REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE A. MIRA-BEJAIA
FACULTE DE TECHNOLOGIE
DEPARTEMENT GENIE ELECTRIQUE

MEMOIRE

EN VUE DE L'OBTENTION DU DIPLOME DE MASTER

Domaine : Sciences et Technologies

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème

Etude et planification d'un réseau Wi-Fi sécurisé Cas : Entreprise RTC Sonatrach de Bejaia

Réalisé par :

MOULLA Badrezzine-salah

TADJINE Samir

Encadré par :

Mr. BERRAH.S

Mr. BENAMIROUCHE.N

Soutenu devant le jury composé de :

Président : Mr. ALLICHE.A

Examinateur : Mr. MEKHMOUKH.A

- Promotion 2018/2019 -

- REMERCIEMENT -

Avant tout, nous remercions Dieu tout puissant de nous avoir donné le courage et la patience de terminer ce travail.

Nous tenons à exprimer notre gratitude à nos promoteurs Mr BERRAH.S, et Mr BENAMIROUCHE.N, pour leurs encouragements, et leurs conseils afin de terminer ce travail.

Nos sincères remerciements au personnel de l'entreprise Sonatrach de Bejaïa, et spécialement à Mr ARKOUB.M notre encadreur de stage pour sa patience, son sérieux, et sa grande disponibilité tout au long de notre stage au sein de l'entreprise.

Nous remercions également, les membres du jury qui ont accepté d'examiner et de juger ce modeste travail.

Sans oublier de remercier tous les enseignants et enseignantes qui, pendant notre cursus universitaire, ont veillé à notre formation et réussite.

Tous les mots restent faibles pour exprimer notre profonde reconnaissance à tous ceux qui nous ont aidé de près ou de loin pour la réalisation de ce travail

DEDICACE

Je dédie ce travail qui n'aura jamais pu voir le jour sans le soutien indéfectible et sans limite de ma chère mère, elle qui ne cesse de me donner avec amour le nécessaire pour que je puisse arriver à ce que je suis aujourd'hui. Tu trouveras ici le témoignage de ma profonde reconnaissance. Que dieu te protège et que la réussite soit toujours à ma portée pour que je puisse te combler de bonheur.

A mes grands-parents, mes oncles, mes tantes et leur famille, à tous mes cousins et cousines et à tous mes proches qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de réussite et de succès.

Merci à vous tous et que Dieu vous protège.

SAMIR.

DEDICACE

Je dédie ce travail et ma profonde gratitude à ma mère et mon père pour l'éducation qu'ils m'ont prodigué, au prix de tous les sacrifices qu'ils ont consentis à mon égard, pour le sens du devoir qu'ils m'ont enseigné depuis mon enfance, pour leur amour, leur soutien et leurs prières tout au long de mes études.

Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

À mon cher frère Safy-Eddine et à ma chère sœur Ghozlane, je vous souhaite une vie pleine de réussite, de santé, et de bonheur.

À la mémoire de ma très chère grand-mère Zohra.

À mes grand parents Mourad et Kheira.

À mes tantes et oncles.

À mes cousins et cousines qui ont toujours été là pour moi.

À mes très chers amis qui m'ont toujours soutenu dans les bons et les mauvais jours.

Merci à vous tous et que Dieu vous protège.

BADRI.

Table des matières

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

A:

ACK: Acknowledgement.

ACL: Access control list

ADSL: Asymmetric **D**igital **S**ubscriber **L**ine.

AES: Advanced **E**ncryption **S**tandard.

ANF: **A**gence **N**ationale des **F**réquences.

AP: Access **P**oint.

B:

BIT: BInary digi**T.**

Bps: Bit **p**ar **s**econde.

BRAN: Broadband **R**adio **A**ccess **N**etworks.

BSA: Basic **S**ervice **A**rea.

BSS: Basic **S**ervice **S**et.

BSSID: Basic **S**ervice **S**et **I**dentifier.

BTS : Base **T**ransceiver **S**tation (station émetteur-récepteur de base).

C :

CCMP : Counter-Mode/CBC-Mac Protocol

CF : Contention **F**ree.

CID : Confidentialité **I**ntegrité **D**isponibilité.

CRC : **C**yclic **R**edundancy **C**heck.

CSMA/CA : Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance.

CSMA/CD: Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etect.

CTS: Clear **T**o **S**end.

D:

DA: Destination **A**ddress.

DECT: Digital **E**nhanced **C**ordless **T**elecommunication.

DHCP: Dynamic **H**ost **C**onfiguration **P**rotocol).

DIFS: Distributed **I**nter **F**rame **S**pace.

DoS: **D**enial **o**f **S**ervice.

DS: **D**istribution **S**ystem.

DSAP: Destination **S**ervice **A**ccess **P**oint.

DSSS: Direct **S**equence **S**pread **S**pectrum.

E:

EAP: Extensible Authentication Protocol.

ESA: Extended **S**ervice **A**rea.

ESS: Extented **S**ervice **S**et.

ESSID: Extended **S**ervice **S**et **I**dentifier.

ETSI : European **T**elecommunications **S**tandards **I**nstitute.

F:

FDM: Frequency Division Multiplexing.

FHSS: Frequency **H**opping **S**pread **S**pectrum.

G:

Gbps: Giga **b**it **p**ar **s**econde.

GI: Guard **I**nterval.

GMK: group master Key

GPO : Group **P**olicy **O**bject

GPRS: General **P**acket **R**adio **S**ervice.

GPS: Global **P**ositioning **S**ystem.

GSM: Global **S**ystem for **M**obile Communications.

GTK: Group temporal Key.

H:

HEC: Header **E**rror **C**heck.

Hiperlan: High **Pe**rformance **R**adio **LAN**.

HomeRF: Home **R**adio **F**requency.

HR-DSSS: High **R**ate **D**irect **S**equence **S**pread **S**pectrum.

HSRP: Hot **S**tandby **R**outing **P**rotocol.

I:

IBSS: Independent **B**asic **S**ervice **S**et.

ICI : Inter-**C**arrier **I**nterference.

IEEE : Institute of **E**lectrical and **E**lectronics **E**ngineers (Institut des ingénieurs électriciens et électroniciens).

IoT: Internet **o**f **T**hings.

IP: Internet **P**rotocol.

irDA: infrared **D**ata **A**ssociation.

IRL: In **R**eal **L**ife.

ISM : Industriel, **S**cientifique et **M**édical.

ISO: International **S**tandard **O**rganisation.

K:

Kbps: Kilo bps.

Km: Kilo**m**ètre.

L:

LAN: Local Area Network.

LDAP: Light **W**ight **D**irectory **A**ccess **P**rotocol.

LED: Light-**E**mitting **D**iode.

Li-Fi: Light **Fi**delity.

LLC: Logical **L**ink **C**ontrol.

LoRaWAN: LOw **RA**nge **W**ide **A**rea **N**etwork.

LPWAN: Low **P**ower **W**ide **A**rea **N**etwork.

LSAP: Logical **S**ervice **A**ccess **P**oint.

LTE: Long **T**erm **E**volution.

LTT : Laboratoire de **T**élécommunications de **T**lemcen.

M:

MAC: Medium **A**ccess **C**ontrol.

Mbps : Mega bps.

MD5 : Message **D**igest 5.

MIC: Message integrity code

MPDU: Mac **P**rotocol **D**ata **U**nit.

N:

NAV: Network **A**llocation **V**ector.

NIC: Network **I**nterface **C**ard.

NS: Nano **S**econde.

O:

OF: Orthogonal **F**requency.

OFDM: Orthogonal **F**requency **D**ivision **M**ultiplexing.

OSI: Open **S**ystems **I**nterconnection.

P:

PBKDF2: Password-Based Key Derivation Function 2 **.**

PCF: Point **C**oordination **F**unction.

PCI: Peripheral **C**omponent **I**nterconnect.

PCMCIA: Personal **C**omputer **M**emory **C**ard **I**nternational **A**ssociation.

PIFS: PCF Inter **F**rame **S**pace.

PLCP: Physical **L**ayer **C**onvergence **P**rotocol.

PLCP-PDU: Physical **L**evel **C**ommon **P**rotoco – **P**rotocol **D**ata **U**nit.

PMD: Physical **M**edium **D**ependent.

PMK: Pairwise Master Key

PSF: PLCP **S**ignaling **F**ield.

PSK: Pre-shared key

PTK: Pairwise Transient Key

Q:

QoS: Quality **o**f **S**ervice.

R:

RA: **R**eceveir **A**ddress.

RADIUS: remote authentification dial-in user service.

RIP: Routing **I**nformation **P**rotocol.

RSB: Rapport **S**ignal sur **B**ruit.

RTS: Ready **T**o **S**end.

S:

SA: Source **A**ddress.

SFD: Start **F**rame **D**elimiter.

SIFS: Short **I**nter **F**rame **S**pace.

SMS: Short **M**essage **S**ervice.

SONATRACH : SOciété **Na**tionale pour le **TR**Ansport par **C**analisation des **H**ydrocarbures)

SPH: Short **P**reamble and **H**eader.

SSAP: Source **S**ervice **A**ccess **P**oint.

SSID: Service **S**et **I**dentifier.

T:

TA: Transmitter **A**ddress.

TDM: Time division multiplexing.

TKIP: Temporal Key Integrity Protocol.

TTL: Time **T**o **L**ive.

U:

UDP : User **D**atagram **P**rotocol

UHF : Ultra **H**autes **F**réquences.

UMTS: Universal **M**obile **T**elecommunication **S**ystem.

UNB: Ultra **N**arrow **B**and.

U-NII: Unlicenced-**N**ational **I**nformation **I**nfrastructure.

V:

VLAN: Virtual Local Area Network.

VLC: Visible **L**ight **C**ommunication.

VTP: Virtal **T**runking **P**rotocol.

W:

WAN: Wide **A**rea **N**etwork.

Wardriving : Wireless **A**ccess **R**esearch **D**riving.

WECA : Wireless **E**thernet **C**ompatibility **A**lliance

WEP: Wired Equivalent Privacy.

WI-FI: WIrless **FI**delity.

WLAN: Wireless **L**ocal **A**rea **N**etwork.

WMAN: Wireless **M**etropolitan **A**rea **N**etwork.

WPA: Wi-Fi **P**rotected **A**ccess.

WPAN: Wireless **P**ersonal **A**rea **N**etwork.

WWAN: Wireless **W**ide **A**rea **N**etwork.

Introduction Générale

Durant ces quarante dernières années [12], la nécessité à pouvoir partager ou échanger l'information de manière numérique et à tout moment n'a eu de cesse d'augmenter.

Peu à peu, un besoin de mobilité s'est fait ressentir, et des réseaux sans fils sont venu pour y répondre en libérant de la nécessité de se connecter physiquement au réseau, tout en apportant des débits permettant d'avoir accès à des services divers.

À l'échelle d'un réseau local, de nombreuses technologies ont ainsi vu le jour, rivalisant entre elles en apportant sans cesse de nouvelles fonctionnalités et une meilleure qualité de service.

On peut dire sans se tromper que la technologie à s'être démarqué à ce niveau, est la norme IEEE 802.11, plus connue du public sous le nom Wi-Fi.

Elle est rapidement devenue une référence en la matière et a été adopté par la grande majorité des constructeurs de matériel informatique. Depuis la première spécification (1997) jusqu'à la norme IEEE 802.11ac, une augmentation conséquente de débit a été obtenue avec chaque nouvelle génération. Aujourd'hui, elle rivalise même avec les débits des technologies filaire tel que la fibre optique.

Même si cette technologie semble parfaite et sans soucis au premier abord, la réalité est bien plus nuancée. En effet, la nature intrinsèque des signaux électromagnétiques fait qu'il est difficile, voire impossible, de maitriser la propagation de ces derniers. Par conséquent, il est facile d'espionner, et même de modifier les informations échangées si le réseau n'est pas correctement sécurisé.

Face à ce genre de risques, les entreprises étaient, dans un premier temps, très réticentes à l'adoption de ce genre de technologies au sein de leurs locaux. Heureusement, l'évolution du Wi-Fi ne s'est pas seulement faite sur les critères de débit et de portée du signal, beaucoup de travaux et d'efforts ont été consentis [1] ces dernières années afin d'aboutir à des solutions pour sécuriser ces réseaux, chaque norme apportant son lot de nouveautés pour garantir confidentialité et intégrité des données.

Aujourd'hui, chaque entreprise possède un réseau informatique permettant une optimisation meilleure des ressources (temps, budget ...), et une certaine aisance pour les employés dans l'exécution de leurs tâches journalières.

Pendant la durée de notre stage au sein de l'entreprise RTC SONATRACH de Bejaïa, nous avons remarqué que leur réseau est uniquement constitué d'une architecture de type filaire. Après avoir minutieusement étudier les différents aspects et besoins de cette entreprise, notre objectif sera donc de concevoir une architecture sans fil basé sur la norme 802.11, et adaptée au site de l'entreprise. Elle servira d'extension à leur réseau existant afin de combler les multiples manques de celui-ci.

Au cours de ce mémoire, nous allons traiter du réseau Wi-Fi, comment est-il structuré ? Quels équipements pour la mise en place d'un tel réseau ?

Nous allons aborder en détail la problématique de sécurité des réseaux Wi-Fi. Compte tenu des vulnérabilités des standards de sécurité Wi-Fi, et face à toutes les failles de sécurité et la diversité des attaques qu'il est possible de monter contre les mécanismes de sécurité dans les réseaux 802.11, quelles sont les meilleures pratiques architecturales et protocolaires en matière

de sécurisation Wi-Fi ? Comment assurer une sécurité optimale, compte tenu de l'hétérogénéité des équipements Wi-Fi existants actuellement dans les entreprises ?

Ce mémoire est structuré en cinq chapitres comme suit :

Le premier chapitre s'intitule "Généralités sur les réseaux sans fil". Il va traiter des réseaux sans fil en général, les différentes catégories existantes, ainsi que leurs avantages et inconvénients.

Le second chapitre nommé " La technologie Wi-Fi" est une étude détaillée de la technologie Wi-Fi, ou l'on va exposer la famille des différentes normes de ce réseau, son architecture cellulaire et en couche, et une vue d'ensemble des différentes technologies Wi-Fi.

Le troisième chapitre est consacré à la partie sécurité dans le réseau Wi-Fi. On verra les potentielles attaques que peuvent subir les équipements de la norme 802.11, ainsi que les différentes solutions apportées à ces problèmes.

Le quatrième chapitre nommé "Organisme d'accueil" aura pour but de mieux comprendre l'entreprise ou nous avons effectué notre stage, sa structure hiérarchique, son réseau informatique ainsi que les différentes technologies utilisées. Nous évoquerons les différentes problématiques rencontrées et les solutions que nous pensons être les plus adéquates.

Le cinquième et dernier chapitre s'intitulera " Planification & Réalisation ". Dans ce chapitre, nous abordons la configuration et la mise en œuvre des différentes solutions retenues.

Enfin, nous finiront par une conclusion générale qui récapitulera les points forts de notre projet ainsi que quelques perspectives futures.

CHAPITRE I

Généralités sur les réseaux sans fil

I. Généralités sur les réseaux sans fil

Introduction

Les progrès en matière de technologies nous permettent d'analyser et de partager de l'information d'une manière ubiquitaire ce qui les a rendus indispensables dans notre vie professionnelle ou personnelle. Toutes ces innovations ont mené au développement des réseaux sans fil. En matière d'infrastructure, on peut enfin se passer des liaisons filaires donc chaque machine n'est plus reliée aux autres par un câble permettant ainsi la mobilité dans l'espace de celle-ci.

Ainsi, la majorité des stations (ordinateurs et appareils mobiles comme les ordinateurs portables, tablettes, Smartphones, …etc.) jouissent de moyens de connexion à un ou plusieurs types de réseaux sans fil comme le Wi-Fi ou le Bluetooth et ce n'est pas très compliqué (du moins pour un connaisseur) de créer un réseau « sans fil » permettant ainsi à tous ces appareils de correspondre. Les gains sont considérables et les avantages notables, mais le développement continu de ces réseaux n'est pas sans déplorables conséquences, ce qui a donné naissance à de nouvelles règles et normes pour mieux joindre les stations entre elles.

I.1. Définition des réseaux sans fil

De l'anglais « wireless network » ou bien tout simplement réseau sans fil dit en français, est un système de communication véhiculant les informations sans contrainte de câblage entre deux terminaux au minimum, si la connexion de l'utilisateur au réseau est assurée même si ce dernier est en mouvement, on parle alors de « mobilité ».

Les réseaux sans fil se sont développés pour mettre en place des transmissions dans les endroits où la pose de câble est difficile, voire impossible et assurer la transmission de données pour des applications mobiles [22], tout cela a servi au développement rapide de ce type de technologies car cela répond à la motivation classique de l'économie des coûts et de l'effort.

I.2. Types de liaison :

Dans les réseaux sans fil, les informations sont transmises par liaison infrarouge ou par onde radioélectrique (onde radio ou onde hertzienne) en lieu et place des câbles habituels.

I.2.1. Liaison de type onde radio :

- Les ondes radio sont émises d'une manière omnidirectionnelle.
- Possibilité de connecter plusieurs appareils entre eux, en même temps.
- Les ondes hertziennes sont difficiles à confiner dans un espace restreint ce qui les rend idéales pour les communications longues distances (plusieurs Km).
- Un mode de communication-modèle pour les liaisons avec les objets mobiles, piétons, automobiles, bateaux, trains, avions, fusées, satellites.
- Les perturbations extérieures peuvent affecter la communication par l'utilisation de la même fréquence par exemple.

I.2.2. **Liaison de type infrarouge :**

- Possibilité de mettre en place des réseaux sans fil de quelques dizaines de mètres.
- Des débits de quelques mégabits par seconde.
- Visibilité des appareils, aucun obstacle ne doit cacher l'émetteur du récepteur car la transmission est unidirectionnelle.
- Utilisation d'onde lumineuse pour la transmission de données car la nature non dissipative de ces ondes permet un degré de sécurité plus élevé.
- Exemple d'utilisation : Télécommande de télévision, de jouet, de voiture..., etc.

Néanmoins, la transmission par onde radio est la méthode la plus utilisée due à sa plus large couverture géographique et son débit plus élevé.

I.3. **Les différents types de réseaux sans fil :**

Plusieurs technologies ont vu le jour, classées suivant la fréquence d'émission, le débit et la portée [2] des transmissions, tout en maintenant les communications et la connexion entre ces derniers.

Ces distances forment « des zones géographiques », elles offrent une connectivité aux terminaux, on les appelle aussi « zones de couverture » ou encore « cellule ». La figure I .1 décrit ces différentes catégories en fonction de la taille de leur zone de couverture.

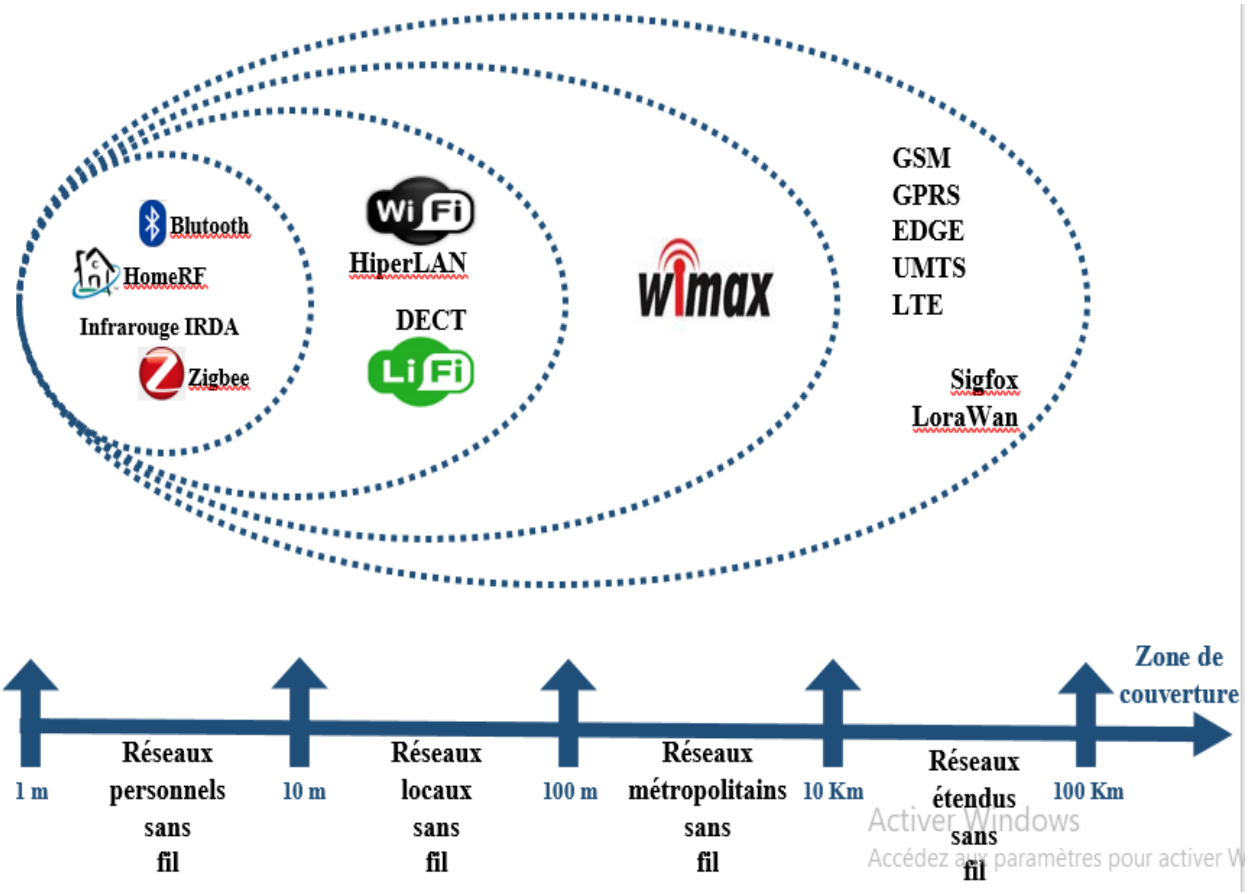

Figure I-1: Les différentes catégories des réseaux sans fil

I.3.1. **Réseaux personnel sans-fil (WPAN)**

Le réseau personnel sans fil (noté WPAN) désigne les réseaux à usage personnel d'une portée de quelques dizaines de mètres autour de l'utilisateur. Ce type de réseau relie d'une manière générale des périphériques très peu distants. Plusieurs technologies sont utilisées pour les WPAN, on cite :

I.3.1.1. **Le Bluetooth :**

Le Bluetooth (nom tiré du surnom anglicisé du roi danois Harald à la dent bleue) est le nom commercial de la norme IEEE 802.15.1. Démarré en 1994 par Ericsson, c'est la technologie maîtresse des WPAN et met à son profit des ondes radio sur la bande de fréquence de 2,4 GHz (c'est la même que pour le Wi-Fi) pour connecter des équipements entre eux. La majorité des périphériques (ordinateurs portables, appareils photos, Smartphones, montres connectées, manettes de jeux vidéo sans fil, ..., etc.) disposent de la technologie Bluetooth, car elle est peu gourmande en énergie.

Officiellement, la première version du Bluetooth a vu le jour en 1999, avec un débit théorique de 1Mbps et une portée maximale plus au moins égale à 30 mètres. En 2009, vint la version 3.0, permettant un débit théorique de 24 Mbps. En 2017 [26], apparaît le Bluetooth 5, la dernière génération élargissant plus la portée à 200 mètres.

I.3.1.2. **ZigBee :**

ZigBee est un protocole de haut niveau développé par l'IEEE, autorisant les échanges entre de petites radios et basée sur la norme IEEE 802.15.4 pour les réseaux à dimension personnelle (WPAN). La spécification initiale de ZigBee propose un protocole dont le rayon d'activité est relativement faible (une dizaine de mètres) et qui est passé à une centaine aujourd'hui, mais très résistant aux interférences, le prix devient faible et la consommation en électricité réduite grâce aux faibles temps de connexion entre les appareils inférieurs à 25 ms et les cycles d'émissions/réceptions très rapides.

Les débits varient selon la bande de fréquence, en Europe c'est la 868 MHz (20 Kbps), aux US c'est la 915 MHz (40 Kbps) et dans le reste du monde la 2.4GHz (250 Kbps) [27].

On retrouve le protocole ZigBee là où la consommation est un critère de sélection (dans les contrôles industriels, les applications médicales, les détecteurs de fumée et d'intrusion, ..., etc.).

I.3.1.3. **HomeRF :**

C'est un standard de télécommunication à haut débit destinée à un usage domestique lancé en 1998 par le HomeRF Working Group incluant entre autres : Motorola, Intel, Microsoft et plus de cent autres. HomeRF utilisait la bande de fréquence de 2,4 GHz avec un débit maximum de 1.6 Mbps dans sa version 1.0 contre 10 Mbps dans sa version 2.0. La distance entre deux

points d´accès varie de 50 à 100 mètres [4]. La norme permettait le transport simultané des données numériques et des signaux de voix provenant de téléphones.

Bien que le HomeRF fût une des meilleures solutions avec sa version 2.0 à son époque néanmoins il fut peu utilisé par les fabricants de matériel et donc peu de produits étaient compatibles, c'est alors que le groupe fut rompu en mois de janvier 2003 lorsque la norme Wi-Fi IEEE 802.11 fut mise à la disposition des besoins domestiques et que Microsoft a choisi d´intégrer Bluetooth, compétiteur direct de HomeRF, dans ses systèmes d´exploitation Windows, ce qui a causé le déclin, puis l´abandon de cette spécification [28].

I.3.1.4. **Infrarouge irDA :**

Les liaisons infrarouges permettent de créer des connexions sans fils de quelques mètres (2 m) avec des débits atteignant quelques mégabits par seconde (4 Mbps max). Cette technologie est majoritairement utilisée pour des communications courte distance, elle est omniprésente dans la maison, par exemple, on peut citer les télécommandes et elle est très simple et pas cher [3].

Par contre, sa sensibilité aux perturbations lumineuses et à l'emplacement des appareils (qui doivent être en vue directe, et sans obstacle entre l'émetteur et récepteur) empêche la progression de cette technologie dans les réseaux sans fil ayant une portée dépassant une dizaine de mètres. L'association irDA formée en 1995 regroupe plus de 150 membres [4].

I.3.2. **Réseaux locaux sans-fils (WLAN)**

Le réseau local sans fils couvre l'équivalent d'un réseau local d'entreprise, environ une centaine de mètres, c'est devenu la solution la plus courante de nombreuses entreprises et de particuliers, on la retrouve dans les campus universitaires, les zones publiques, …, etc. Ainsi, toute personne munie d'un ordinateur portable ou d'un Smartphone peut accéder à des services publics d'information ou encore à se connecter sur Internet à travers le réseau local [2].

Plusieurs normes de WLAN ont été développées, nous citons dans ce qui suit les 3 principales :

I.3.2.1. **Wi-Fi :**

Le réseau Wi-Fi est un réseau sans fil dont les caractéristiques correspondent à celles décrites par la norme IEEE802.11, ce réseau fera l'objet d'étude de ce mémoire et il sera développé en détails dans le chapitre 2.

I.3.2.2. **Hiperlan :**

Hiperlan est une norme européenne créée par l'ETSI et développée par le groupe technique BRAN, concurrent du groupe IEEE802.11 (Wi-Fi) qui lui est américain. Il est composé de deux normes haut débit : HiperLAN 1 et HiperLAN 2.

Hiperlan 1 a été définie en juillet 1998. Elle exploite la bande de fréquence 5 à 5,3 GHz en offrant un débit théorique maximum de 23.5 Mbps. Cette norme est complètement axée sur une architecture réseau ad hoc (qui sera plus détaillé dans le chapitre 2).

Hiperlan 2 fait écho à la norme IEEE 802.11a et elle est axée sur le mode infrastructure (cf. chapitre 2). Cette norme a défini différents débits pour établir des communications allant de 6, 9, 12, 18, 27, 36 et jusqu'à 54 Mbps. L'Hiperlan2 permet de transmettre de la vidéo haute qualité, des paquets IP et de la voix numérisée des cellulaires [2].

I.3.2.3. **DECT :**

DECT « téléphone sans-fil numérique amélioré », anciennement « Digital European Cordless Telephone », est une norme de téléphones sans fil domestiques consacrée aux entreprises et aux particuliers utilisant une gamme de fréquence allant de 1.88 GHz jusqu'à 1.92 GHz [30].

Alcatel et Ascom (deux entreprises de télécommunication) développent ces téléphones pour les environnements industriels, comme les centrales nucléaires, basés sur cette norme qui limite les interférences. Les points d'accès résistent à la poussière et à l'eau. En plus de leur principale utilité qui est le transport des communications vocales, ces téléphones peuvent aussi assurer la surveillance des appareils de sécurité 24/24 afin d'avertir en cas de panne ou de problème en se connectant directement au réseau téléphonique de l'entreprise par exemple.

Figure I-2: GIGASET C430HXD Téléphone DECT[25]

I.3.2.4. **Li-Fi :**

Le Li-Fi ou communication lumineuse visible (VLC) est un système de communication sans fil qui se sert de la lumière visible avec une bande de fréquence allant de 385 à 790 THz [74] pour véhiculer des informations. Il fonctionne grâce aux ampoules LED qui possèdent une

intensité lumineuse variables à très grande vitesse imperceptible à l'œil nu. Ces leds sont de plus en plus utilisées, ce qui en fait de potentiels points d'accès.

Ces changements d'intensité sont captés par un photo-détecteur, elles seront converties en signal électrique puis au format binaire pour pouvoir être interprétées par nos équipements. En théorie, Li-Fi permet des transmissions théoriques de 10 Gbps, bien au-delà de ce que permettent les liaisons radio.

Pour fonctionner, la lumière doit toujours être allumée et visible du récepteur, mais contrairement à son homologue Wi-Fi, la lumière ne traverse pas les murs. Il sera donc plus facile de protéger l'accès à son réseau.

Mais le Li-Fi est actuellement une technologie unidirectionnelle. Il doit donc être couplé avec une autre technologie (CPL, Wi-Fi) ou être utilisé dans des cas particuliers (besoin uniquement de débit descendant), néanmoins les possibilités d'utilisation sont nombreuses (réseau routier, géolocalisation, communication sous-marine, etc.).

I.3.3. **Réseaux métropolitain sans fil (WMAN)**

Les réseaux métropolitains sans fil (WMAN) appelé aussi « Boucles Locales Radio », sont une technologie basée sur la norme IEEE 802.16. Ces réseaux permettant des débits utiles de 1 à 10 Mbps pour une portée variante de 4 à 10 Km, ce type de connexion est plutôt orienté vers les besoins des opérateurs de télécommunication [31].

I.3.3.1. **Wimax :**

C'est la norme la plus populaire du WMAN, fourni une connexion Internet à haut débit avec en théorie, des débits montants et descendants de 70 Mbps avec une portée de 50 kilomètres, mais dans la pratique ce débit dépasse de peu les 20 Mbps à cause des nombreux obstacles comme de grands immeubles ou même des collines.

Certes le standard Wimax assure une connexion sans fil entre une BTS et de très nombreux abonnés sans nécessiter de ligne visuelle directe, il n'en est moins qu'il n'endure pas les gros obstacles. La BTS, cœur de la technologie Wimax est une antenne centrale communiquant avec celles des abonnés. Ce mode de communication est désigné par le terme « liaison point-multipoint » [27].

Il existe deux catégories pour le standard Wimax :

- **Wimax fixe**, aussi noté IEEE 802.16 - 2004, est réservé pour les usagers fixes. Ce standard utilise les bandes de fréquences 2.5 GHz et 3.5 GHz qui nécessitent une licence, ainsi que la bande libre des 5.8 GHz, on peut avoir des débits de 75 Mbps sur une zone de 10 Km plus ou moins.
- **Wimax mobile**, également baptisé IEEE 802.16e, possibilité de connecter des clients mobiles au réseau Internet sur une portée de 3.5 Km avec des débits de 30 Mbps ouvrants ainsi la voie à la téléphonie mobile sur IP ou plus largement à des services mobiles haut débit.

I.3.3.2. **Applications du Wimax**

Accès à Internet haut débit pour les zones non couvertes par les technologies filaires (ADSL, Câble, …etc.), ces zones sont souvent nommées zones du « dernier kilomètre ».

Sert de réseau de « collecte », le WimAX pourra relier plusieurs AP utilisant par exemple le standard Wi-Fi entre eux pour créer un réseau plus étendu.

I.3.4. **Réseau étendu sans-fil (WWAN)**

Les réseaux étendus sans fil (WWAN) ou « réseaux cellulaires mobiles » permettent l'utilisation simultanée de dizaines de millions de téléphones sans fil, qu'ils soient en immobilité ou en mouvement et ce même à grande vitesse et sur de très vastes distances.

Ce type de réseaux est le plus fréquent, car tous les téléphones mobiles sont reliés à un réseau étendu sans fil si ce n'est plus avec les actuels Smartphones à double puce [30]. Les principales technologies utilisées dans les WWAN sont les suivantes :

I.3.4.1. **GSM :**

Le GSM est la norme initiale des téléphones sans fil qui est passée au numérique, ce réseau achemine les informations sur deux bandes de fréquence : une première bande s'étalant de 880 MHz jusqu'à 915 MHz pour la voie montante et une seconde bande de 925 MHz à 960 MHz pour la voie descendante. Le standard GSM achemine de la parole avec un débit de 9 600 Bps, permet aussi la correspondance entre un poste mobile et un autre fixe.

L'autre fonctionnalité est le transfert de messages alphanumériques courts (les SMS, avec 160 caractères seulement), de plus, la fiabilité de transfert de la parole fut aussi améliorée, mais les faibles débits que fournissait ce standard ne lui ont pas permis de suivre le rythme de l'évolution des services à haut débit comme la vidéophonie ou simplement Internet, du coup le GSM a évolué en la norme GPRS et plus tard EDGE [7].

I.3.4.2. **GPRS [8] :**

À ce stade de l'évolution des réseaux mobiles, c'est la capacité de transmission de données qui se développe dans le réseau GSM. Ainsi, le GPRS a pris naissance. Ce nouveau service exploitant la technique de commutation de paquets et l'augmentation des débits ouvre la porte à Internet et aux applications mobiles multimédias.

Dans des conditions optimales, des débits maximums réels de 50 Kbps sont possibles alors que le débit théorique est de 144 Kbps. L'ajout de la capacité de transmission de données au réseau GSM est le GPRS ; ainsi l'architecture mixte GSM et GPRS a débouché sur la 2.5 G. Dans ce nouveau réseau 2.5 G, la voix continue de transiter sur le réseau GSM, alors que le transport des données et l'accès à Internet sont disponibles via GPRS.

I.3.4.3. **EDGE :**

Avec l'EDGE, on était aux portes de la 3G, car cette technologie portée le nom de 2.75 G. La combinaison (GPRS/EDGE) faisait en sorte de « doper » le réseau (GSM/GPRS), les clients bénéficiaient des débits presque 10 fois plus rapides que ceux du GSM et trois fois plus que le GPRS.

Sans rentrer dans les détails, l'encodage de données avec l'EDGE se fait de manière plus performante qu'avec le GPRS, ce qui a accru grandement le débit dans la zone de couverture, ainsi on pouvait atteindre des débits max de 384 Kbps (100 Kbps en pratique) [32], les abonnées jouissaient alors d'une qualité de transmission plus profitable, cependant même si l'envoi de messages et les transferts d'appels se faisaient sans soucis, il était difficile d'insérer des images dans un mail par exemple [33].

I.3.4.4. **UMTS :**

L'UMTS est la norme qui vient après l'EDGE, elle appartient donc à la 3e génération de la téléphonie mobile. Le réseau UMTS est passé sur une nouvelle gamme de fréquence, plus distante et surtout plus large que celle du GSM, cette bande s'étendait de 1885 MHz à 2200 MHz [30].

Ce standard fut une véritable révolution à son époque, lors de la sortie de la version initiale en 2004, les utilisateurs bénéficiaient d'un débit atteignant les 384 Kbps de débits théoriques de l'EDGE et en 2006, vint la version suivante qui a vu son débit max avoisiné les 2Mbps, ouvrant les portes vers de nombreux services multimédia comme l'Internet haut débit, le téléchargement de films et de musiques, la visiophonie et possibilité de jouer à des jeux vidéo en ligne, …, etc. [3]

I.3.4.5. **LTE :**

4e et dernière génération des réseaux mobiles (la 5e encore en stade de développement), LTE utilise une « plage » de fréquences s'étendant de 450 MHz jusqu'à 3.8 GHz (En Algérie, nos opérateurs exploitent la bande de fréquences des 1800MHz [35]). Cette plage est divisée en plusieurs canaux dont l'évasure fluctue de 1.4 MHz jusqu'à 20 MHz, et pour les 20 MHz, on a un débit de 300 Mbps théorique (100 Mbps IRL) pour la liaison descendante.

Un téléphone mobile avec un débit de réception limité à 20 Mbps ne pourra pas profiter des 100 Mbps fournies par la technologie LTE donc si l'on veut télécharger un jeu vidéo de 3 gigas de taille, il faudra jusqu'à 2 minutes et demie pour un Smartphone d'un débit de 20 Mbps et 30 seconde pour un débit de 100 Mbps, en supposons que ce débit ne fluctue pas avec le temps (on appelle ça la théorie.).

Deux évolutions ont suivi la version primaire de la 4G, la 4G LTE Advanced (4G+) : 330 Mbps et la 4G++ : 600 Mbps. Aujourd'hui, la plupart des Smartphones sont compatibles avec

les débits de la 4G (toutes versions confondues) afin de profiter amplement des services offerts par ce réseau [36].

I.3.5. **Réseaux étendu sans fil à faibles puissance (LPWAN)**

Les réseaux LPWAN sont des réseaux émergent dédiés et développés pour l'IoT et la 5G, à très bas débit et une très longue portée (de 5 km à 40 km), cette technologie permet d'émettre et recevoir des messages de petites tailles. Les composants utilisés pour émettre ces messages sont très peu coûteux et très peu énergivores (avec une simple batterie, on peut émettre quelques messages par jour pendant 10 ans.) [9].

Les solutions de surveillance qui échangent de petits volumes de données comme les capteurs ou les compteurs d'énergie communicants, sont les applications type qui s'appuient sur les LPWANs pour les échanges de communication.

Les LPWAN utilisent les bandes de fréquences libres ISM disponibles mondialement, contrairement aux opérateurs mobiles qui utilisent des bandes sous licence. L'utilisation des bandes ISM implique le partage des ressources avec d'autres technologies (Wi-Fi, Bluetooth, etc.). Toutefois, ces bandes sont régulées par des autorités organisatrices.

Compte tenu des faibles débits et de la faible occupation spectrale des signaux, il faut en moyenne, pour un réseau LPWA, 10 fois moins d'antennes pour couvrir la même surface qu'un réseau cellulaire traditionnel.

Exemples d'applications : e-santé, agriculture de précision, villes intelligentes.

Voici quelques technologies :

I.3.5.1. **Sigfox :**

Sigfox est l'une des premières sociétés sur le marché des LPWAN, arrivée en 2009 avec une technologie basée sur la transmission de signaux sur une bande ultra étroite (UNB) d'une centaine de Hz, elle utilise les bandes ISM : autour de 868 MHz pour l'Europe et 915 MHz pour les USA pour une portée de 30 à 50 km en zones rurales et de 3 à 10 km en zones urbaines. Les appareils consomment très peu d'énergie pour envoyer les données, mais en très faibles quantités, entre 10 et 100 bps par maximum [10].

I.3.5.2. **LoRaWAN :**

Un protocole de communication par radio, des objets à faible consommation électrique connectés à Internet, qui permet de transmettre des données à des distances de 2 à 5 km en milieu urbain et jusqu'à 20 km en milieu rural. Seuls 0,3 à 50 kbps peuvent transiter sur ce réseau, qui est (tout comme Sigfox) idéal pour des capteurs émettant périodiquement une faible quantité de données de température, de géo localisation ou de pression par exemple.

Ce protocole peut être développé en réseau privé pour qu'une entreprise puisse en assurer elle-même la gestion.

I.4. Les avantages et les inconvénients des réseaux sans fil

I.4.1. **Avantages :**

Les réseaux sans fil présentent de multiples avantages, ils sont faciles à utiliser et rapide à mettre en place, mais on va voir dans ce qui suit qu'il ne s'agit pas que de ça :

- **Une souplesse de la topologie :** la flexibilité d'un réseau sans fil autorise l'ajustement de son architecture pour l'adapter aux besoins, en fonction du nombre de stations qui vont se connecter ou se déconnecter ainsi que par l'étendue de la zone de couverture des points d'accès (en rajoutant des répéteurs pour accroître l'étendue de la zone de couverture) [39].
- **Fiabilité :** les transmissions sans fil sont très efficaces dans les domaines civil et militaire. Une distance limitée entre les équipements radio (station, AP) et une bonne conception du réseau, permettent une transmission correcte du signal sans chevauchement et autorisent des performances similaires à celles d'un réseau local filaire [3].
- **Facilité :** la connexion au réseau sans fil est très simple, en général un réseau bien configuré nous demandera une autorisation (un mot de passe l'authentification). Une fois cela fait, il suffira de se trouver, la prochaine fois, dans la zone d'émission de l'AP, la liaison au réseau se fait alors automatiquement.
- **Coût :** les frais d'installation et de maintenance sont presque nuls, il n'y a pas de câbles à poser (les APs, répéteurs ou autres antennes sont simplement posées), ainsi l'installation se fait sans le moindre outillage et les modifications de la topologie n'entraînent pas de dépenses supplémentaires [39].
- **Inter connectivité avec les réseaux locaux :** les réseaux sans fil tels que les WLAN sont compatibles avec les LANS (vu qu'ils sont considérés comme des extensions de ces derniers) le Wi-Fi permet d'atteindre des zones difficilement accessibles pour l'Ethernet.
- **Mobilité :** les réseaux sans fil accordent une connexion à Internet et un partage de données sans liaison filaire entre les appareils, ainsi les utilisateurs se meuvent à leur guise dans la zone de couverture du réseau. La mobilité est donc l'avantage maître qui fait toute la force du réseau sans fil face au réseau câblé [3].
- **Évolutivité :** un réseau sans fil est plus facile à mettre en place et à allonger et encore plus à réduire ou à retirer, on peut façonner sa topologie en fonction de nos besoins et du nombre des équipements connectés [39].
- **Simplicité d'installation :** les réseaux sans fil sont des candidats de choix pour la couverture d'évènements à durée limitée comme une conférence, une réunion ou un match de foot. L'installation de ces réseaux est facile et rapide et ne demande pas de lourds aménagements des infrastructures (creuser des tranchées pour acheminer les câbles, équiper des bâtiments en câblages, goulottes et connecteurs).

I.4.2. **Inconvénients :**

Cependant, comme rien n'est jamais parfait, on a le droit à la médaille et au revers de la médaille, voici donc quelques inconvénients :

- Les ondes radio sont très affectés par les interférences, les radiations ou autres émissions radio ce qui cause des dysfonctionnements des réseaux et des taux d'erreurs élevées.
- La qualité des signaux est mise à rude épreuve, des missions provenant d'autres réseaux (radars de gendarmerie ou émetteurs Bluetooth) perturbent la continuité du signal d'un réseau comme le Wi-Fi même si ce dernier est bel et bien configuré et installé [39].
- Effets multi-trajets, les ondes radio se propagent dans tous les sens, le signal peut être capté par tout le monde autour, au-dessus et en dessous de nous.
- Un monde gavé de rayonnement, n'est pas sans mauvaises conséquences sur la santé des gens qui sont exposés aux ondes radio provenant de leurs Smartphones ou autres micro-ondes [3].
- N'importe quelle station même non autorisée à disposer d'une information peut accéder aux données émises sur une cellule (il suffit que cette station soit à la portée du signal.) même si l'information est bien protégée par un code de chiffrement. La question de sécurité doit être prise extrêmement au sérieux si l'on veut éviter des fuites d'informations ou des écoutes indésirables de données. [39]
- Divers produits et solutions selon le propriétaire, il est assez compliqué d'avoir une solution globale et la normalisation prend du temps [3].
- Les réseaux sans fil disposent de bandes passantes réduites par rapport aux réseaux filaires, cela réduit les vitesses de transmission (jusqu'à 10 fois moins rapides qu'avec le câble).

I.5. **Conclusion**

Dans cette première partie, nous avons établi une vue assez générale sur les réseaux sans fil, en définissant ces réseaux et les modèles de liaisons, ensuite, on a présenté les différentes variétés de technologie sans fil et mobile, quelques-unes se complètent tandis que d'autres sont en concurrence (comme le Bluetooth et le HomeRF), et nous avons terminé avec les opportunités que nous offrent les réseaux sans fil, mais aussi les inconvénients dont ils nous encombrent.

Notre conclusion est que les réseaux sans fil ont su trouver leurs places non seulement chez les particuliers mais dans différents domaines comme l'armée (le militaire), l'industrie ou encore la santé, se rendant presque indispensable dans ces secteurs grâce aux avantages et améliorations qu'ils apportent notamment la mobilité, le cout, la simplicité d'installation ou encore la facilité d'accès au réseau, servant par la même occasion d'extensions et non de remplaçants aux réseaux câblés.

CHAPITRE II

La Technologie WI-FI

II. La technologie Wi-Fi

Introduction

En ce début du 21e siècle [21], les réseaux locaux informatiques ont connu deux évolutions importantes. D'une part, l'utilisation courante du réseau local chez les particuliers, due en grande partie à Internet, et d'autre part, l'arrivée en masse des ordinateurs et autres matériels mobiles. Pour cela, il fallait trouver une technologie permettant de simplifier le câblage du réseau chez un particulier et de préserver la mobilité des produits portables. Un seul principe permet de concilier les deux, le sans-fil.

La technologie sans fil s'est largement répandue ces derniers temps et maintenant l'on peut se connecter de presque n'importe où... À la maison, au travail, dans les bibliothèques, les écoles, les aéroports, les hôtels, et même dans certains restaurants.

L'objectif de ce chapitre est de présenter en détail le standard 802.11 qui est le plus utilisé dans les réseaux locaux sans fil.

II.1. Qu'est-ce que le Wi-Fi ?

La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil. Le nom Wi-Fi correspond initialement au nom donné à la certification délivrée par la « Wi-Fi Alliance » anciennement appelée WECA [1]. La mission de WECA [83] est de certifier l'interopérabilité des produits Wi-Fi (IEEE 802.11) et de promouvoir le Wi-Fi en tant que norme LAN sans fil dans tous les segments du marché.

Le Wi-Fi ou norme de réseau 802.11, est un réseau sans fil local proposé par l'organisme de standardisation Américain IEEE. Il correspond aux caractéristiques décrites par le standard IEEE 802.11 et désigne un système de connexion qui permet d'alléger un utilisateur lambda d'un câble entre sa station et son point d'accès à Internet. L'accès se fait avec la transmission d'ondes radioélectriques.

Grâce au Wi-Fi, on peut créer des réseaux locaux sans fil à haut débit pour peu que l'appareil à connecter ne soit pas trop distant du point d'accès. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs de bureau, les tablettes, des Smartphones [30], certaines imprimantes ou tout type de périphérique à une liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur (d'une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert.

La technologie 802.11 est généralement considérée comme la version sans fil de 802.3 (Ethernet). De nos jours et par abus de langage, le terme IEEE 802.11 désigne par la même occasion la première norme du Wi-Fi (802.11 legacy).

Le principal avantage de la connexion Wi-Fi est qu'il est compatible avec presque tous les systèmes d'exploitation, dispositifs de jeu et imprimantes avancées.

II.2. **Les différentes normes du standard IEEE 802.11**

La norme IEEE 802.11 est le standard qui décrit les caractéristiques des réseaux sans fil et elle est l'équivalente de la norme IEEE 802.3 (Ethernet) pour les réseaux filaires.

La première version de la norme IEEE 802.11 est définie en 1997. Des transmissions infrarouges étaient envisagées, les versions les plus récentes du standard sur la base desquelles sont construites l'essentiel des cartes d'interface commercialisées, s'adressent principalement à des transmissions radiofréquences. Pour définir cette norme, les concepteurs ont pris en considération les points suivants :

- Robustesse et simplicité de la technologie contre les défauts de communication afin de pouvoir transmettre dans les meilleures conditions, tenant compte des considérations que le canal de transmission (l'air) est moins fiable que le câble, et qu'il est plus difficile à gérer.
- Utilisation du WLAN mondialement. C'est-à-dire le respect des différentes règles en usage dans les différents pays du monde.
- Totale compatibilité avec les anciens produits et les produits actuels qui composent les réseaux LAN. C'est-à-dire que le passage du WLAN au LAN et vice-versa devra être transparent à l'utilisateur.
- Le choix d'une sécurité acceptable pour le passage de l'information dans l'air vu le peu de fiabilité de ce canal de transmission.

802.11 (version 1997) : La norme IEEE 802.11 n'est en fait que la norme initiale, cette dénomination désigne actuellement tous les protocoles de la série donc il ne faut pas confondre entre l'actuel 802.11 qui désigne tous les standards du 802.11 et le 802.11 publié en 1997 qui lui n'est que la première norme à partir de laquelle un certain nombre de normes dérivées ont été créées afin de répondre à des objectifs d'interopérabilité ou de sécurité, d'ailleurs cette norme initiale est souvent appelée 802.11 **legacy** (en français hérité ou historique) [30].

La norme 802.11 legacy décrit les couches physiques et mac pour un débit allant jusqu'à 2Mbps (max) en radio, dans la bande des 900 MHz. Des extensions ont été publiées depuis qui viennent lui ajouter des améliorations et des modes de fonctionnements plus performants, les principales extensions sont les suivantes :

802.11 (version de 1999) : elle permet toujours d'obtenir un débit de 1 jusqu'à 2Mbps max pour une portée de 20 m en intérieur et jusqu'à 100m en extérieur dans la bande de fréquence radio ISM des 2.4 GHz et une largeur de bande de 83.5 MHz (2.4 GHz – 2.4835 GHz) [30].

802.11a: publiée en septembre 1999 ; elle permet d'obtenir un haut débit (dans un rayon d'environ 35 mètres : 54 Mbit/s théoriques, 27 Mbps réels) dans la bande de fréquence radio SHF des 5 GHz. La norme 802.11a spécifie 8 canaux d'une largeur de bande de 20 MHz (de 5,150 GHz à 5,350 GHz) ; chaque canal est subdivisé en 52 sous-porteuses. Cette norme n'est pas compatible avec 802.11b et 802.11g.

802.11b : la norme 802.11b était la norme Wi-Fi la plus répandue en base installée au début des années 2000. Elle propose un débit théorique crête de 11 Mbps (6 Mbps réels) avec une portée d'une cinquantaine de mètres en intérieur et pouvant aller jusqu'à 300 mètres (en théorie)

dans un environnement dégagé. Fonctionne dans la bande des 2,4 GHz (de 2,4 à 2,4835 GHz) avec une largeur de bande 83.5 MHz [30].

802.11g (Wi-Fi 3) : le Wi-Fi 3 a remplacé à lui seul les Wi-Fi 1 et 2 en 2003. La norme IEEE 802.11g associe effectivement la modulation OFDM plus performante du Wi-Fi 1 à la bande de fréquences 2,4 GHz du Wi-Fi 2, ce qui permet d'offrir au grand public le débit maximal théorique de 54 Mbps [41] (25Mbps en réel) du Wi-Fi 1, avec la portée supérieure du Wi-Fi 2, tout en assurant la rétrocompatibilité avec les équipements Wi-Fi 2 préexistants.

802.11n (Wi-Fi 4) : l'IEEE 802.11n est une révision majeure apparue en 2009 qui décuple littéralement le débit maximal théorique. La norme apporte pour ce faire deux évolutions : la technologie MIMO et une bande passante doublée. Le 802.11n a été conçu pour pouvoir utiliser les bandes de fréquences de 2,4 GHz et/ou 5 GHz.

Pour la bande de fréquence de 2.4 GHz, on avait un débit théorique allant de 72 jusqu'à 288 Mbits/s pour une portée de 70m avec une largeur de bande de 20 MHz, et pour la bande des 5GHz, on pouvait atteindre des débits théoriques de 150 jusqu'à 600 Mbits/s pour une portée de 35m avec une largeur de bande de 20 MHz offrant le débit max de 150Mbits/s et une autre largeur de bande de 40MHz qui nous permet le fameux débit théorique de 600Mbits/s [41].

Les premiers adaptateurs 802.11n disponibles étaient souvent simple-bande à 2,4 GHz, mais des adaptateurs double-bande (2,4 GHz ou 5 GHz, au choix) ou double-radio (2,4 GHz et 5 GHz simultanément) sont également disponibles.

802.11ac (Wi-Fi 5) : IEEE 802.11ac est la dernière évolution « grand public » du standard de transmission sans fil 802.11 ; elle est arrivée par étapes, en 2013 c'est la première vague d'appareils équipés de cette norme qui voient le jour, quelques années plus tard la seconde vague équipe les Smartphones et dépasse la première génération. Elle permet une connexion Wi-Fi haut débit dans la bande des 5 GHz ») sur des largeurs de bande de 20, 40, 80 ou 160 MHz (160 MHz uniquement sur la vague 2) [42], ainsi le 802.11ac offre jusqu'à 1 300 Mbps de débit théorique en utilisant des canaux de 80 MHz et jusqu'à 2600 Mbps/s en utilisant des canaux de 160MHz, soit jusqu'à 7 Gbit/s de débit global dans la bande des 5 GHz (de 5170 MHz à 5835 MHz). Cette norme a été ratifiée en janvier 2014.

802.11ad (WiGig) : Apparut en 2012, l'IEEE802.11ad jouit de sa propre WiGig Alliance, littéralement « alliance pour le sans-fil Gigabit ».

Le WiGig atteint avec un seul flux des débits exprimés en gigabits par seconde. Il fonctionne sur la bande des 60 GHz (donc non compatible avec les normes 802.11 précédentes et les équipements compatibles ont rencontré une faible diffusion), avec une largeur de canal de 2160 MHz offrant ainsi un débit théorique de 6750 Mbps [42] (En pratique 4,6 Gbps, il peut exploiter aussi les bandes 2,4 et 5 GHz pour offre un débit maximal de 7,2 Gbps. Le 802.11ad ne traverse donc pas les murs, il peut tout juste se réfléchir contre les surfaces pour atteindre des appareils en vue indirecte. Sa portée maximale est de 10 mètres. Cette norme est une alternative aux câbles HDMI et USB.

802.11ax : La version définitive de la norme 802.11ax n'est pas attendue avant 2019, cette nouvelle évolution du Wi-Fi doit permettre de dépasser les 10 Gbps tout en gardant une compatibilité avec les deux fréquences des précédentes versions : 2,4 et 5 GHz [41].

Développée avec l'IoT et les smartphones en tête, cette norme doit réduire la consommation énergétique et donc augmenter l'autonomie de nos appareils.

802.11	Bande de fréquence	Débit théorique maximal	Portée	Largeur canal	MIMO
Version 1997	900 MHz	2 Mbps	Faible	-	Non
Version 1999	2.4 GHz	2 Mbps	20 m en intérieur/ 100 m en extérieur	83.5 MHz	Non
a (1999)	5 GHz	54 Mbps	35 m	20 MHz	Non
b (fin 1999 début 2000)	2.4 GHz	11 Mbps	35 à 50 m en intérieur/ 300 m (en théorie) en extérieur	83.5 MHz	Non
g (2003)	2.4 GHz	54 Mbps	38 m	20 MHz	Non
n (2009)	2.4 GHz	72 à 288 Mbps	70 m	20 MHz	Oui
n (2009)	5 GHz	150 à 600 Mbps	35 m	20 ou 40 MHz	Oui
ac (2013)	5 GHz	433 à 2600 Mbps	35 m	20, 40, 80 ou 160 MHz	Oui
ad (2012)	2.4 , 5 ou 60 GHz	6.75 Gbps et jusqu'à 7.2 Gbps avec modulation OFDM	10 m	2160 MHz	Non
ax (courant voir fin 2019)	2.4 et 5 GHz	10.53 Gbps	-	20, 40, 80 ou 160 MHz	oui

Tableau II-1: Récapitulatif des différentes normes et évolution du 802.11.

II.3. Les règles de transmission des ondes radio

Quelques rappels :

La puissance d'un signal est généralement exprimée en Watt ou milliwatt, si l'on veut l'exprimer en rapport de puissance en décibels (dBm) on procède comme suit :

$$P(dBm) = 10 \times log[\, P(mW)]$$

Le RSB est un indicateur de la qualité de la transmission d'une information. C'est le rapport entre la puissance d'émission d'un signal et la puissance du bruit, calculé comme suit :

$$RSB = Ps/Pb$$

Rappelons aussi une caractéristique propre au logarithme :

$$\boldsymbol{Log(a \div b) = log(a) - log(b)}$$

II.3.1. **La portée du signal**

Ce que l'on entend par « porté » est la distance que parcourt une onde radio au fur et à mesure que ça puissance d'émission diminue due aux nombreux obstacles qu'elle rencontre avant de s'évanouir et de disparaître complètement.

Plus la portée est grande et plus l'onde pourra traverser les obstacles, pour augmenter la portée du signal (la doublée) il faut quadrupler sa puissance à l'émission (2×portée = 4×puissance mW), par exemple un émetteur à 100 mW portera 2 fois plus loin qu'un émetteur à 25 mW.

En dBm, quadrupler la puissance revient à rajouter 10 x log (4) ≈ 6.02 dBm à notre puissance initiale elle-même en dBm bien sûr. Le calcul se fait alors comme suit :

$$\begin{aligned} \boldsymbol{QuadruplePPuissance_{dBm}} &= \boldsymbol{10 \times log(QuadruplePuissance_{mW})} \\ &= \boldsymbol{10 \times log\,(4 \times Puissance_{mW})} \\ &= \boldsymbol{10 \times log\,(4) + 10 \times log\,(Puissance_{mW})} \\ \boldsymbol{QuadruplePuissance_{dBm}} &= \boldsymbol{10 \times log\,(4) + Puissance_{dBm}} \qquad \textbf{(1)} \end{aligned}$$

Pour l'exemple de tout à l'heure, si l'on prend le 25 mW, nous trouverons 20 dBm.

Un autre facteur qui détermine la portée c'est la sensibilité du récepteur, c'est-à-dire la puissance (en dBm) minimale captée à la réception nécessaire pour maintenir la connexion, en dessous de ce seuil la communication est perdue.

II.3.2. **Bruit et interférences**

Le rapport signal-bruit s'exprime aussi en dB et dans ce cas il exprime la différence entre la puissance du signal reçu et la puissance du bruit (en dBm) :

$$\boldsymbol{RSB_{dBm} = log(Ps_{mW} \div Pb_{mW})}$$

$$\boldsymbol{RSB_{dBm} = log(Ps_{mW}) - log(Pb_{mW})}$$

$$\boldsymbol{RSB_{dBm} = Puissance\ du\ signal\ reçue_{dBm} - Puissance\ du\ bruit_{dBm}} \qquad \textbf{(2)}$$

Les sources de bruit sont multiples, cela peut être des réseaux sans fil et tous les équipements radio situés à proximité, il y a aussi l'activité humaine (industrielle, militaire, radios, télévision, antennes de téléphonie mobile...) et le bruit électromagnétique naturel. La puissance du bruit naturel est en général de l'ordre de −100 dBm pour les fréquences du Wi-Fi.

Si le bruit est de −100 dBm et que le signal reçu est de −65 dBm, alors le RSB est de +35 dB, en général plus le RSB est important et plus la réception est bonne et permet des débits importants.

II.3.3. **Le débit**

C'est le nombre de bits qui transitent dans le canal de transmission chaque seconde et il dépend de la largeur de ce canal, on peut le calculer avec la formule suivante :

$$\boldsymbol{C = H \times \log_2(1 + \frac{Ps}{Pb})} \quad \textbf{(3)}$$

- **C** : la capacité maximale du canal de communication en bits par seconde.
- **H** : est la largeur de la bande de fréquences utilisées, en hertz.
- **Log**$_2$ (Ps/Pb) = log(Ps/Pb) / log (2).
- **Ps** : c'est la puissance du signal exprimée en Watt.
- **Pb** : c'est la puissance du bruit exprimée aussi en Watt.

Le débit maximal dépend de la largeur de la bande de fréquences utilisées, plus on se situe dans des fréquences élevées et plus on a de la place pour exploiter des bandes de fréquences larges et donc le débit sera plus important. Mais en ce qui concerne le Wi-Fi, les canaux de communication définis pour le 2,4 GHz ont une largeur de 22 MHz et les canaux de 5 GHz ont une largeur de 20 MHz. Le débit maximal que l'on peut atteindre (en théorie) est plus ou moins identique dans les deux cas. Cela explique le fait que le 802.11a et le 802.11g offrent tous les deux le même débit maximal, malgré le fait que le 802.11a exploite des fréquences plus élevées que le 802.11g. Mais le plus dans la bande des 5 GHz c'est qu'il y a plus de canaux pour communiquer qu'avec les 2.4 GHz.

Pour obtenir un bon débit, il est aussi nécessaire d'avoir un bon rapport signal-bruit, plus on s'écarte de l'émetteur plus le RSB diminue et plus le débit diminue lui aussi, exemple : avec un émetteur 802.11g à 15 dBm et un bon récepteur on peut en théorie (sans bruit ou obstacles) obtenir un débit de 11 Mbps jusqu'à 100 mètres, au-delà le débit tombera à 5,5 Mbps, puis à 2 Mbps et enfin à 1 Mbps jusqu'à plus de 300 m. Mais dans la pratique, il en est autrement, la portée est plus faible (la moitié ou le tiers de la portée théorique) à cause du bruit.

II.3.4. **Bandes de fréquences**

Le standard IEEE802.11 utilise des bandes de fréquences dites libres ou sans licences, ces bandes sont exploitées sans autorisation administrative par d'innombrables utilisateurs et ne nécessitent ni déclaration préalable ni paiement [63] contrairement aux bandes de fréquences réservées à des utilisateurs spécifiques comme les opérateurs et qui nécessitent l'obtention d'une autorisation « licences » auprès de l'organisme chargé de l'attribution de la délivrance des autorisations d'utilisation des fréquences (ANF en Algérie).

Les bandes libres, malheureusement, ne garantissent aucune protection contre les phénomènes de brouillage et d'interférence des signaux due au nombre et à l'emplacement indéterminés des stations exploitant ces bandes [70].

Mais le standard IEEE802.11 apporte des protections lors de la transmission des données grâce à des processus de codage et de modulation, ces bandes sont :

II.3.4.1. **La bande ISM :**

Les bandes ISM, les UHF et situées autour des 2.4 GHz, sont utilisées par presque toutes les normes du standard 802.11 avec une la largeur de 83.5 MHz (2.4 GHz – 2.4853 GHz) [17], c'est sur ces fréquences que le Bluetooth et les WLAN émettent leurs données.

- Pour la bande 2400 à 2454 MHz en intérieur ou en extérieur, la puissance d'émission autorisée est de 100 mW.
- Pour la bande 2454 à 2483.5 MHz en intérieur c'est 100 mW et en extérieur 10 mW.

II.3.4.2. **La bande U-NII :**

Ces bandes sont situées autour de 5GHz et sont utilisaient par les normes IEEE802.11 (a, n et ac) [30]. Elles nous offrent une largeur de bande de 300 MHz et qui est fragmentée en trois sous-bandes, deux sont utilisées pour les transmissions en intérieur et une utilisée pour les transmissions en externe.

II.3.5. **Les canaux de transmission**

Une ligne ou canal de communication est une bande de fréquences étroites permettant de transmettre des quantités d'informations, cette quantité, que le canal transporte, est appelée capacité du canal et elle est bien sûr limitée et souvent l'information transmise par ce canal subit des modifications (altérations) dues à un bruit aléatoire (un autre signal ou juste à cause des bruits de l'environnement)

La même ligne de transmission est allouée à deux stations, une émettrice et une autre réceptrice, pour permettre le transfert de données. [17]

II.4. **Les équipements d'un réseau Wi-Fi :**

Un réseau WI-FI peut être composé d'un ou de plusieurs points d'accès, chacun ayant une ou plusieurs stations connectées.

Les points d'accès ou les cartes clientes possèdent le même type d'éléments actifs Wi-Fi : leur fonction principale est de convertir les données numériques en signaux analogiques destinés à l'antenne. C'est à son niveau que les protocoles de modulation/démodulation des signaux interviennent. En réception, il décode les signaux transmis par l'antenne en données IP pour le réseau. Les caractéristiques principales d'un élément actif sont sa puissance d'émission et sa sensibilité en réception (puissance minimale admissible pour interpréter les données et assurer la liaison), toutes deux exprimées en mW ou dBm et qui sont réglables sur ce matériel Wi-Fi le débit de liaison souhaité, parfois le niveau de puissance de sortie, ainsi que plusieurs protocoles liés à la sécurité et à l'identification des autres AP connectées.

Les principaux équipements d'un réseau Wi-Fi sont : des points d'accès, des cartes Wi-Fi et des antennes.

II.4.1. **Les points d'accès :**

Le point d'accès (AP) est un des éléments essentiels de l'architecture WI-FI. C'est lui qui permet à des clients Wi-Fi de communiquer entre eux. Le choix d'un point d'accès se fait en fonction des fonctionnalités qu'il propose.

Ils ne nécessitent pas un ordinateur pour fonctionner, car ils sont totalement autonomes. Leur configuration se fait via un ordinateur relié au réseau sur lequel se trouve le point d'accès. Bien entendu, il peut être directement relié à l'ordinateur par un câble, mais cela n'est pas nécessaire.

Le rôle des points d'accès est similaire à celui que tient le hub dans les réseaux filaires. [43]

Ils peuvent aussi être reliés à un réseau filaire tel un réseau local. Si en plus ils permettent de gérer ce réseau filaire, alors ce sont des routeurs.

Les APs permettent aux stations équipées de cartes Wi-Fi d'obtenir une connexion au réseau. On parle alors d'association entre l'AP et chaque station connectée (ordinateur ou Smartphone par exemple). Les trames d'information envoyées par un client sont réémises par l'AP, ce qui permet à la station de joindre un autre client qu'elle ne peut pas forcément voir directement (à cause de l'éloignement, ou de la présence d'obstacle). Le support physique étant les ondes radio, on ne peut pas empêcher les stations non-destinataires de recevoir les trames émises, d'où l'analogie avec le hub.

Les points d'accès proposés actuellement sur le marché sont plus ou moins complexes.

On trouve des points d'accès simples et d'autres plus avancés comportant des options, notamment un firewall pour se protéger des attaques extérieures, un serveur DHCP [3].

Figure II-1: EXEMPLE D'APS, LE « AC1200R ALFA NETWORK 802.11 AC » A DROITE ET LE « TP-LINK TL-WA801ND » A GAUCHE [45] [43].

II.4.2. **Les cartes Wi-Fi :**

La carte Wi-Fi est une norme de communication permettant la transmission de données numériques sans fil. Elle est appelée carte réseau compatible avec la norme WI-FI et elle est également appelée NIC. Elle constitue l'interface physique entre l'ordinateur et le modem ou AP. Sa fonction est de préparer, d'envoyer et de contrôler les données sur le réseau [46].

Une carte réseau Wi-Fi doit être installée sur chaque station du réseau sans fil (que cela soit un ordinateur portable ou fixe, Smartphone, tablette, …, etc.) et dans de nombreux cas d'appareils mobiles, cette carte est déjà incluse dans la carte-mère, mais elle peut également se trouver sous la forme d'une carte PCI ou d'une clé USB. Une ou plusieurs antennes

(émettrices/réceptrices), parfois intégrées dans la carte, parfois amovibles, permettent l'envoi et la réception des signaux.
Il est possible de relier deux machines directement par Wi-Fi (on parle alors d'architecture ad hoc).

L'ordinateur et la carte doivent communiquer pour faire passer les données. La carte Wi-Fi les traduit en code numérique (à la réception), plus précisément en bits, afin que l'unité centrale puisse les comprendre et les traiter ; quant à l'émission, elle se charge de transformer les données numériques en onde radio afin de les envoyer à l'aide d'antennes à travers le canal hertzien. Son rôle d'identificateur [47] fait qu'elle :

1- Traduit les données et indique son adresse au reste du réseau afin de pouvoir être distinguée des autres cartes du réseau.

2- A une adresse MAC unique sur le réseau, définies par l'IEEE qui attribue des plages d'adresses à chaque fabricant de cartes réseau, ces adresses sont inscrites sur les puces des cartes, une procédure appelée « Gravure de l'adresse sur la carte ». Par conséquent, chaque carte a une adresse MAC unique sur le réseau.

3- Envoi et contrôle des données : avant que la carte émettrice envoie les données, elle dialogue électroniquement avec la carte réceptrice pour s'accorder sur les points suivants :

- Taille maximale des groupes de données à envoyer.
- Volume de données à envoyer avant confirmation.
- Intervalles de temps entre les transmissions partielles de données.
- Délai d'attente avant l'envoi de la confirmation.
- Quantité que chaque carte peut contenir avant débordement.
- Vitesse de transmission des données.

Si une carte plus récente, donc plus perfectionnée, communique avec une carte plus lente, elles doivent trouver une vitesse de transmission commune. Certaines des cartes plus récentes ont des circuits leur permettant de s'adapter au débit d'une carte plus lente afin de communiquer avec.

Nous avons 3 types de cartes Wi-Fi :

II.4.2.1. **PCMCIA :**

C'est une carte de la taille d'une carte de crédit ou un périphérique d'entrée/sortie qui se connecte à un ordinateur personnel, généralement un ordinateur portable.

Tout bon ordinateur portable dispose donc d'un emplacement PC Card (PCMCIA) au niveau de sa carte-mère. L'avantage : une fois placée, on n'y touche plus sauf en cas de dysfonctionnement. Intégrée à un ordinateur, une telle carte sera plus pratique qu'un adaptateur USB, car elle ne dépassera pas ou peu de cet ordinateur et elle ne monopolisera pas un port USB.

La carte ne possède pas une antenne extérieure, mais comporte plutôt une partie bombée (à gauche de l'image) permettant de loger l'antenne interne plate qui assurera les transmissions

(émission/réception) entre le PC portable et le point d'accès (réseau en mode infrastructure) ou bien avec une autre station elle-même équipée d'une carte Wi-Fi (réseau en mode Ad-hoc).

La plupart des fabricants d'ordinateurs portables intègrent une interface WI-FI interne (interface mini-PCI) dans les PC, comme cela a été le cas pour l'interface Ethernet il y a quelques années. Il n'y a plus besoin de cartes PCMCIA actuellement.

Figure II-2: exemple d'une carte Wi-Fi PCMCIA [49].

II.4.2.2. **Les cartes PCI :**

Elle est généralement utilisée dans les ordinateurs de bureau. Même si les ordinateurs bureaux sont câblés au réseau, les cartes PCI sans fil peuvent être installées dedans pour leurs donner la capacité sans fil. Ceci est bénéfique lors du déplacement des ordinateurs autour de la maison ou dans un autre bureau par exemple ou une connexion routeur-filaire est gênante, les adaptateurs PCI donnent donc aux ordinateurs de bureau des capacités « mobiles ». Les cartes PCI ont une antenne située à l'extérieur de la carte, et elles sont installées directement sur la carte-mère de l'ordinateur.

Figure II-3: exemple de carte Wi-Fi pci [50] .

II.4.2.3. **Les cartes adaptatrices PCMCIA :**

Les cartes adaptatrices PCMCIA, avec une interface PCI pour l'insertion de la carte, sont les plus courantes. L'avantage de cette solution est qu'elle utilise les mêmes cartes Wi-Fi PCMCIA

sur la station fixe et sur un ordinateur portable. Il est donc possible de retirer la carte PCMCIA de son berceau et de l'emmener en déplacement avec son portable [3].

Figure II-4: exemple de carte adaptatrice pcmcia [51] .

II.4.2.4. **USB :**

Ce format s'est rapidement popularisé pour sa simplicité d'utilisation et les constructeurs n'ont pas tardé à proposer également des cartes Wi-Fi avec ce format [43].

Les ports USB sur les ordinateurs sont utilisés pour les claviers, souris, disques durs externes et même des cartes réseau sans fil. Les cartes sans fil USB ressemblent à de petites clés USB, et l'antenne est interne. Branchez la carte sans fil USB à un ordinateur, installez les pilotes et l'ordinateur est prêt pour une connexion sans fil.

Figure II-5: exemple de clés Wi-Fi USB [52] [53] .

II.4.3. **Les antennes :**

Une antenne est un dispositif permettant de rayonner les ondes électromagnétiques, sa puissance d'émission de signaux appelée "Gain", est mesurée en "dBi" et plus ce gain est élevé, plus la portée sera grande.

Chaque carte Wi-Fi est équipée d'une antenne interne. Si une station se trouve cachée par un obstacle tel qu'un mur, meuble, ou une personne, ..., etc. Ou qu'elle soit assez éloignée du point d'accès, il se peut qu'elle ne puisse accéder au réseau. La figure suivante illustre la zone (d'émission/réception) de l'antenne d'une carte WI-FI sous forme PCMCIA.

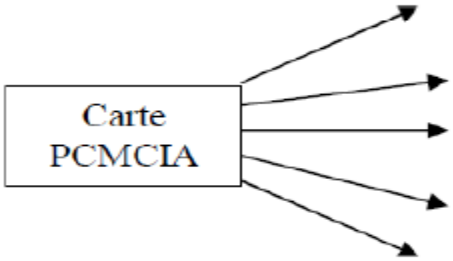

Figure II-6: Zone d'émission et de réception de l'antenne d'une carte PCMCIA [3]

Cette zone ne permet pas à la carte de recevoir des informations de toutes parts, sur 360°. En effet, le Wi-Fi permet de récupérer les transmissions issues des réflexions des ondes radio dans l'environnement. Suivant l'environnement, ces réflexions peuvent être plus ou moins fortes, mais cela permet à certaines stations de fonctionner malgré leurs contraintes spatiales.

Si la carte ne fonctionne pas bien voire pas du tout, l'ajout d'une antenne est indispensable.

L'antenne intégrée à l'AP ou à la carte Wi-Fi peut être remplacée par une antenne externe plus puissante, et souvent, l'antenne peut se trouver à des dizaines de mètres du point d'accès ou de la carte Wi-Fi, alors on peut la relier à ces derniers par un câble d'antenne, la plupart du temps avec un parafoudre pour protéger l'appareil, mais les câbles peuvent générer des pertes dans le signal plus au moins importantes suivant le diamètre du câble, ainsi plus son diamètre est important plus les pertes sont réduites et vice-versa comme on peut le constater dans le tableau suivant qui nous présentes différents types de câbles :

Type de câble	Diamètre en centimètre	Perte en dB sur 10m
LMR-200	**0.5**	**5.543**
LMR-300	**0.7**	**3.42**
LMR-400	**1.03**	**2.23**
LMR-500	**1.27**	**1.8**
LMR-600	**1.29**	**1.443**
LMR-900	**2.21**	**0.984**
LMR-1200	**3.05**	**0.754**
Belden9913	**1.03**	**2.69**
LDF1-50	**0.64**	**2.001**
LDF4-50A	**1.27**	**1.279**
LDF5-50A	**2.22**	**0.754**
LDF6-50	**3.18**	**0.558**
LDF7-50A	**4.13**	**0.459**
RG58	**0.5**	**10**

Tableau II-2: Caractéristiques des différents câbles [54] [55] [56].

Le choix d'une antenne est important et doit être déterminé par le rôle qu'elle devra assurer, c'est-à-dire les interactions souhaitées avec les autres éléments Wi-Fi distants. En fonction des caractéristiques du terrain et des zones à couvrir, il pourra par exemple être décidé de réaliser des liaisons point à point via deux antennes directionnelles ou utiliser un élément omnidirectionnel en cas de clients plus dispersés et rapprochés.

Il y a 3 grandes familles d'antennes :

II.4.3.1. **Les omnidirectionnelles :**

Le signal des antennes omnidirectionnelles rayonne de la même façon en ligne droite [56] dans toutes les directions à la fois (leur rayonnement s'effectue sur 360°.). Elles sont idéales pour une diffusion large du signal Wi-Fi, mais la distance maximale depuis l'AP en revanche reste limitée en comparaison des autres antennes.

Elles ont un gain variant de 0 à 15 dBi environ. Elles sont utilisées pour établir un réseau urbain de type client–serveur, permettant de fournir un accès au réseau, lorsque les stations peuvent être n'importe où par rapport à l'AP dans un parc par exemple.

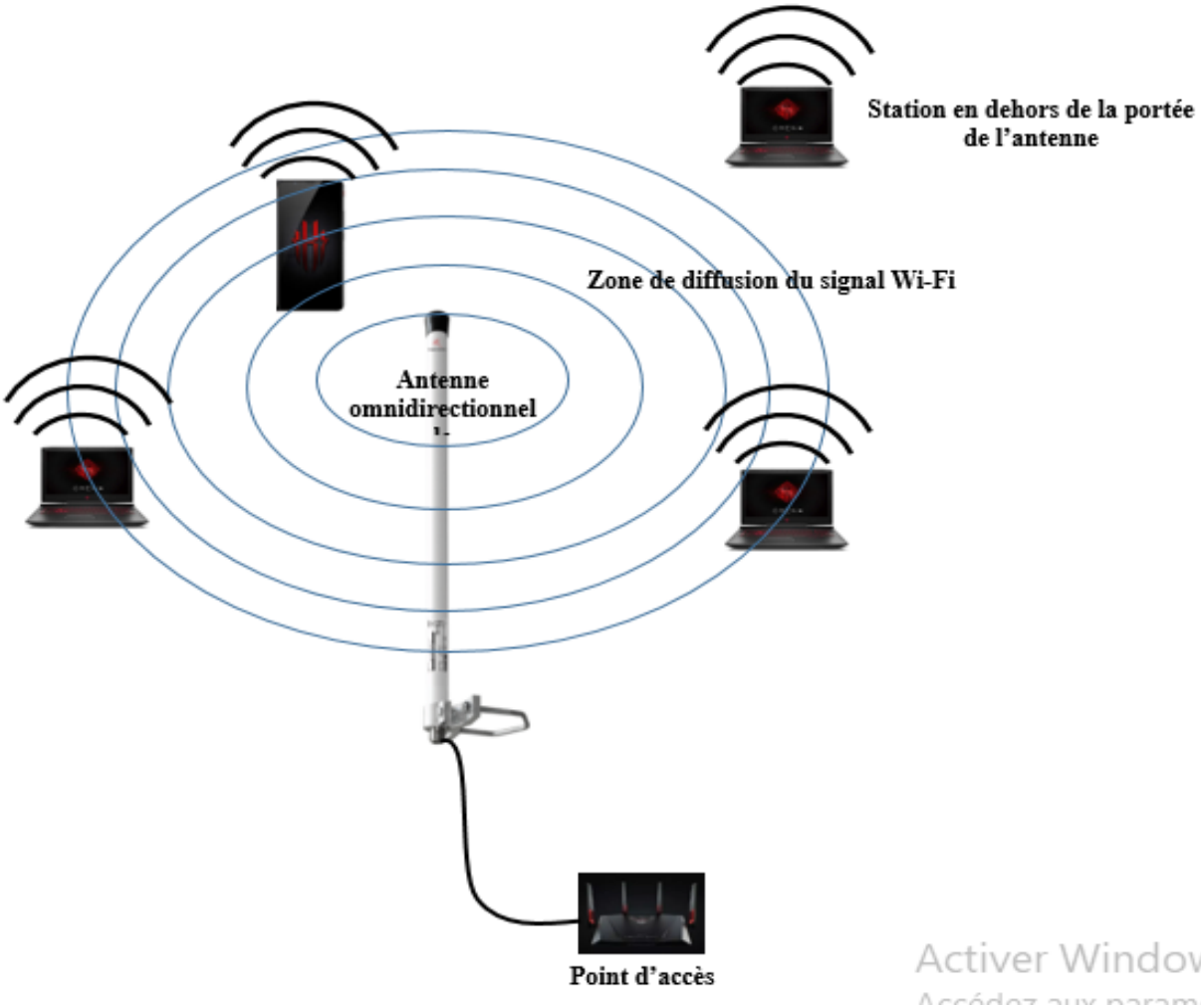

Figure II-7: Zone de diffusion du signal Wi-Fi avec une antenne omnidirectionnelle.

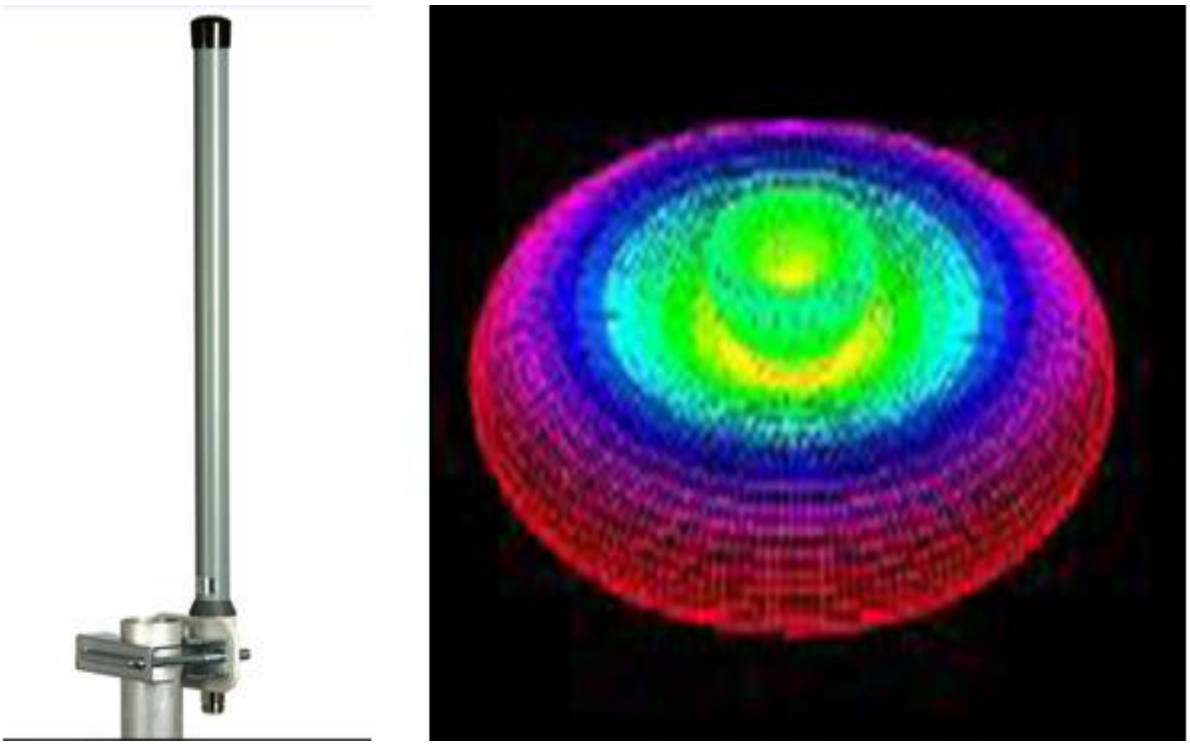

Figure II-8: Antenne omnidirectionnelle [57] avec simulation 3D de la propagation de ses ondes [11]

II.4.3.2. **Les directionnelles :**

Ces antennes ont un fort gain, c'est-à-dire qu'elles peuvent capter un signal à plus grande distance qu'une antenne omnidirectionnelle, mais dans une zone très restreinte, car le signal rayonne de la même façon en ligne droite dans une seule direction. En général, plus le gain est fort, plus longue est la portée du signal, mais hélas plus faible sera l'angle démission et la zone couverte rétrécie, mais on peut capter le même signal depuis un point encore plus éloigné.

Typiquement, les antennes directionnelles sont employées pour créer des liaisons point à point où seulement deux appareils Wi-Fi sont associés l'un à l'autre car elles rayonnent dans une direction bien précise. Ce type de lien est nécessaire pour parcourir de longues distances (environ > 500 m).

Elles se caractérisent par leur gain élevé (de 5 dB minimum jusqu'à 24 dB maximum [11]), cf. ci-dessus, et par un rayonnement directif (donc son angle d'ouverture) : une antenne de 10 dB et 60° d'ouverture [11], pourra tout à fait convenir pour couvrir, par exemple, une place en centre-ville, voir un quartier complet. Une antenne de 14 dB avec 40° d'ouverture couvrira elle une zone plus longue, mais plus étroite. Chaque application nécessite par conséquent une étude sérieuse, de façon à utiliser l'antenne la plus adaptée.

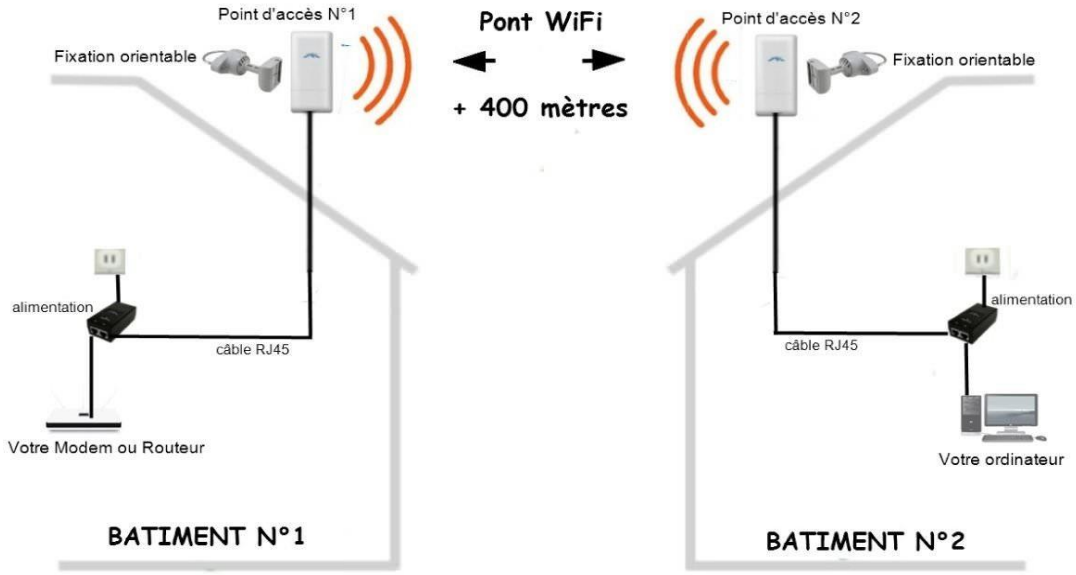

Figure II-9: Zone de diffusion du signal Wi-Fi avec une antenne directionnelle [56].

Types d'antennes directionnelles : Panneau, parabole

Figure II-10: A gauche une antenne Yagi et à droite une antenne parabole

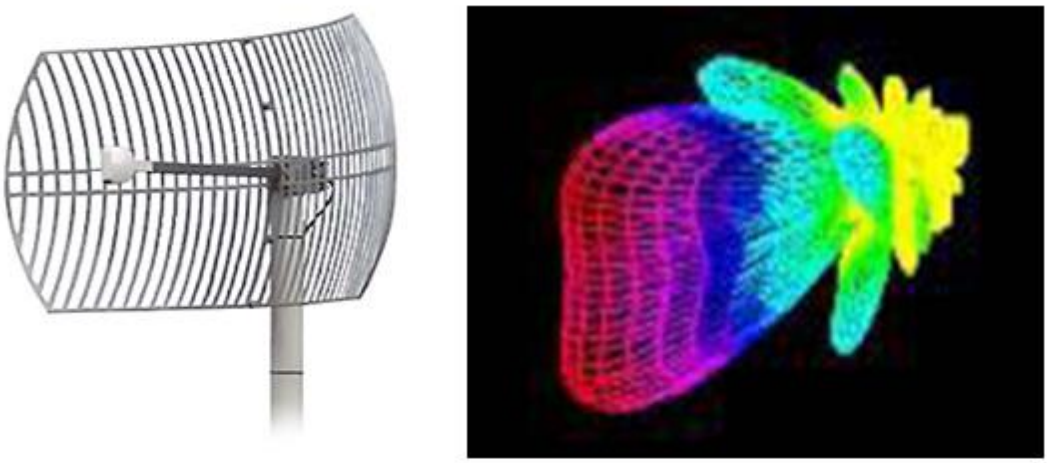

Figure II-11: Antenne directionnelle [58] avec simulation 3D propagation de ses ondes [11].

II.4.3.3. **Les patchs ou antennes sectorielles :**

Il s'agit d'un compromis entre les deux types précédents. On les emploiera lorsque la zone à couvrir est relativement confinée (on peut la voir entièrement sans tourner la tête ou les yeux.) mais elle peut être plus éloignée que pour une antenne omnidirectionnelle. L'angle d'ouverture est généralement de 60°, 90° ou 120° [43].

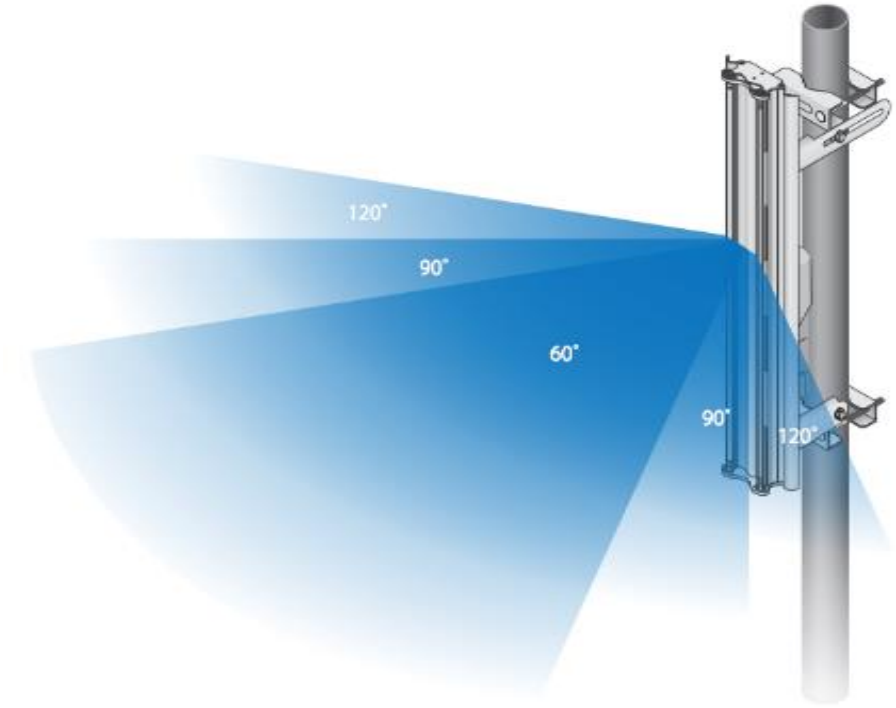

Figure II-12: exemple d'antenne Wi-Fi de type panneau.

II.5. **Les topologies de la norme 802.11**

Les réseaux WI-FI sont fondés sur une architecture cellulaire. Comme celle utilisée dans la téléphonie mobile, où des téléphones mobiles utilisent des stations de base pour communiquer entre eux.

Un réseau WI-FI est composé d'un ou de plusieurs points d'accès, auquel un certain nombre de stations de bases équipées de cartes Wi-Fi s'associent pour s'échanger des données. Le rôle du point d'accès consiste à unifier le réseau et à servir de pont entre les stations du réseau et un réseau extérieur.

La taille d'un réseau dépend de la zone de couverture du point d'accès, aussi appelé cellule. Cette zone peut varier, car l'utilisation des ondes radio ne permet pas de couvrir constamment une même zone. Un grand nombre de facteurs peut faire varier la taille de zone de couverture du point d'accès, tels les obstacles, les murs ou personnes situées dans l'environnement où les interférences liées aux équipements sans fil utilisant les mêmes fréquences, ou encore la puissance du signal [3].

La norme 802.11 définit deux modes de topologies : le mode infrastructure et le mode ad hoc.

II.5.1. **Le mode infrastructure :**

Dans les réseaux de type infrastructure, un ou plusieurs périphériques sont reliés au réseau via le point d'accès Wi-Fi. On dit que le périphérique est le « client » et l'AP le « maître ». Un réseau de ce type s'appelle un BSS [12] ou bien encore ensemble de services de base. Le BSS couvre un espace qu'on appelle une « cellule » ou BSA, cette zone couverte par le signal d'un point d'accès (AP) permet à toutes les stations se trouvant dans la zone géographique d'un BSS d'émettre et de recevoir des trames de l'AP.

Chaque BSS est identifié par un nombre composé de 48 bits : c'est le BSSID. En mode infrastructure, ce BSSID correspond tout simplement à l'adresse MAC du point d'accès, de ce fait, c'est un identifiant unique. L'AP sert de relais entre les périphériques, mais il peut aussi servir de relais vers un réseau filaire, par exemple un réseau d'entreprise.

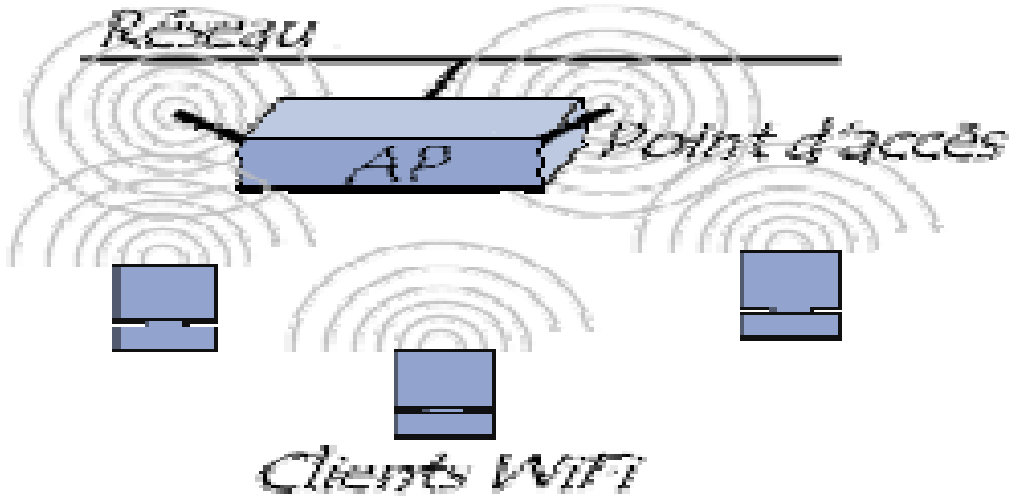

Figure II-13: Un réseau Infrastructure composé d'une seule cellule (BSS) [4].

Plusieurs points d'accès peuvent être déployés pour atteindre une plus large couverture Wi-Fi. Ces BSS multiples peuvent être reliés par un système de distribution (DS) de façon à former un unique réseau sans fil étendu. Le DS peut être un réseau filaire Ethernet (le cas le plus fréquent), un câble de point à point, mais on peut construire un DS également sur du Wi-Fi et donc avec une liaison sans fil.

Il est alors possible à un utilisateur de se déplacer dans l'ensemble de la zone de couverture sans qu'il souffre de ralentissement ou d'interruption de sa connexion : en cas de besoin, la liaison bascule automatiquement (c'est le hand-over) vers le point d'accès offrant la meilleure connexion.

II.5.1.1. **Le Handover en Wi-Fi**

Le roaming, ou handover, ou encore appelé l'itinérance en Wi-Fi est lorsqu'une station change de AP [13] et donc de BSS pour être redirigée vers une autre, car l'utilisateur est sortie de la BSA couverte par le signal du premier AP.

On parle dans ce cas d'ESS ou bien ensemble de services étendus qui couvrent naturellement un espace appelé ESA. Un ESS correspond à la réunion de plusieurs BSS qui sont reliés par un lien réseau (Wi-Fi ou filaire). Chaque ESS est identifié par un nom stocké sur 32 octets maximum qui s'appelle l'ESSID (ou simplement le SSID, c'est un code envoyé avec toutes les trames Wi-Fi à des fins d'identification).

II.5.1.2. **Beacon (balise)**

C'est une trame envoyée régulièrement par l'AP pour signaler sa présence, tout point situé dans le BSS reçoit le beacon à intervalles réguliers [13].

II.5.1.3. **Station (STA)**

Cela correspond à tout matériel équipé d'une carte Wi-Fi autre qu'un AP. Il peut s'agir d'un PC avec une antenne Wi-Fi, mais également des Smartphones, ou de tout autre type d'équipement [13].

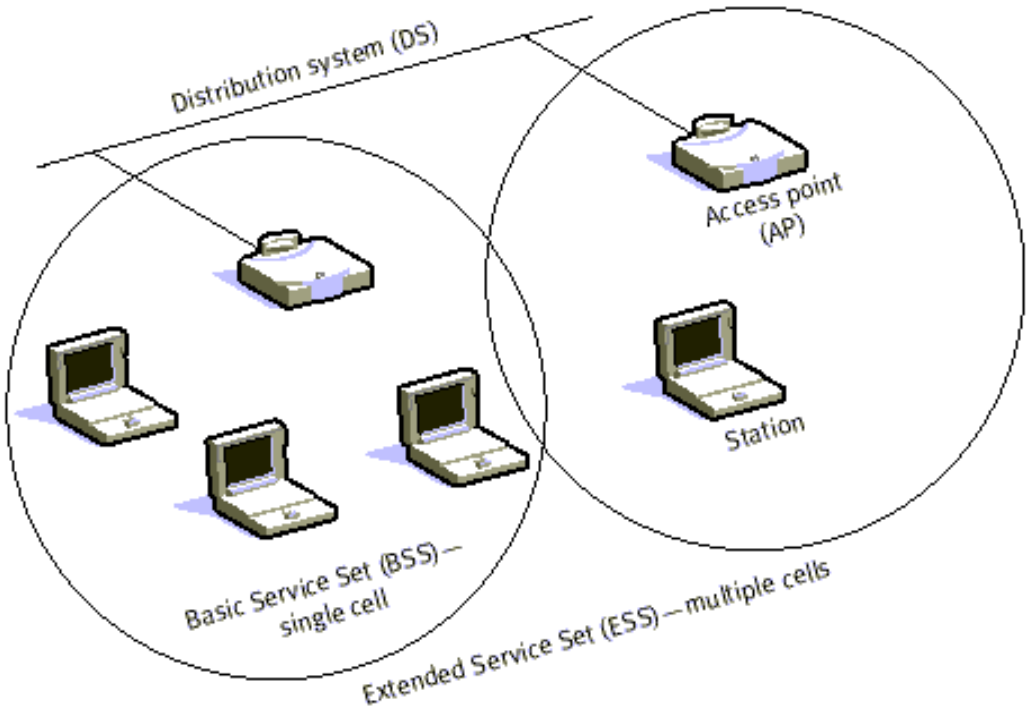

Figure II-14: Un réseau Infrastructure comportant plusieurs cellules (ESS) [59].

II.5.1.4. **Connexion à un réseau Wi-Fi en mode infrastructure :**

La connexion d'une station à un AP s'effectue en deux phases. La première correspond à une phase d'authentification, la seconde à l'association [13].

Authentification : la station désirant entrer sur le réseau Wi-Fi doit s'authentifier sur l'AP. Si le réseau est ouvert, cette phase est obligatoirement un succès.

Association : une fois authentifiée, une station est associée et peut commencer à émettre des trames sur le réseau. L'AP relaiera ces informations aux destinataires concernés.

II.5.1.5. **La communication avec le point d'accès :**

Quand une station rentre dans une cellule, celle-ci diffuse sur chaque canal une requête de sondage (probe request) contenant l'ESSID pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun ESSID n'est configuré, la station écoute le réseau à la recherche d'un SSID.

En effet chaque point d'accès diffuse régulièrement (à raison d'un envoi toutes les 0.1 seconde environ) une trame balise donnant des informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option [4].

À chaque requête de sondage reçue, le point d'accès vérifie l'ESSID et la demande de débit présent dans la trame balise. Si l'ESSID correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger la distance à laquelle il se situe. En effet d'une manière générale, plus un point d'accès est proche meilleur est le débit [4].

Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même SSID) pourra ainsi choisir le point d'accès offrant le meilleur compromis de débit et de charge.

II.5.2. **Le mode ad hoc :**

Dans les réseaux de type Ad Hoc, chaque machine sans fil cliente communique directement avec les périphériques situés à sa portée, sans passer par un intermédiaire comme un point d’accès ou une connexion à un réseau, afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d’accès. Ces réseaux ont été étudiés au début des années 1970 [14] à des fins militaires sous le nom de réseaux en mode paquet.

Ce mode est pratique pour l’échange de données entre quelques stations en l’absence d’un quelconque point d’accès. Le réseau ainsi constitué s’appelle un (IBSS) ou bien un ensemble de services de base indépendants.

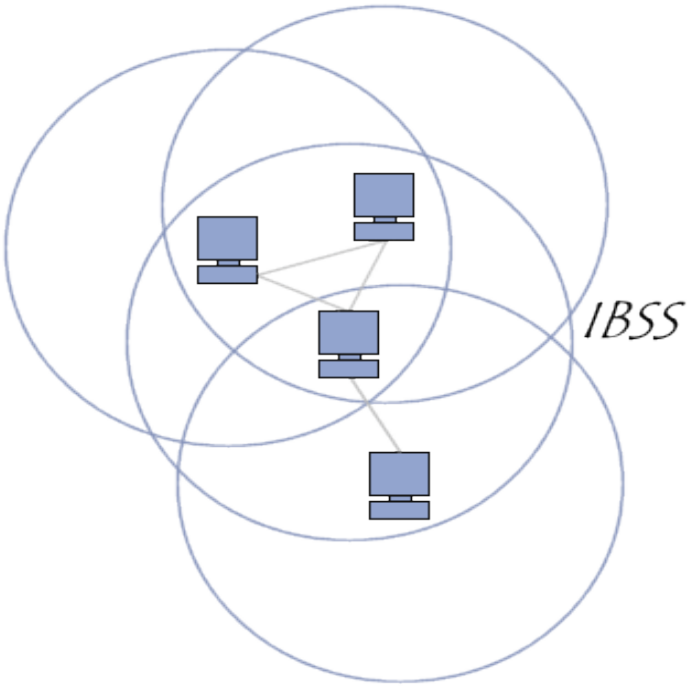

Figure II-15:Exemple d'une structure d'un réseau IBSS [60].

L'IBSS constitue donc un réseau permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure, par conséquent, toute station désirant se connecter au réseau étendu doit connaître au préalable la valeur du SSID**.**

Dans un réseau ad hoc, la portée du BSS indépendant est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi, un IBSS est par définition un réseau sans fil restreint.

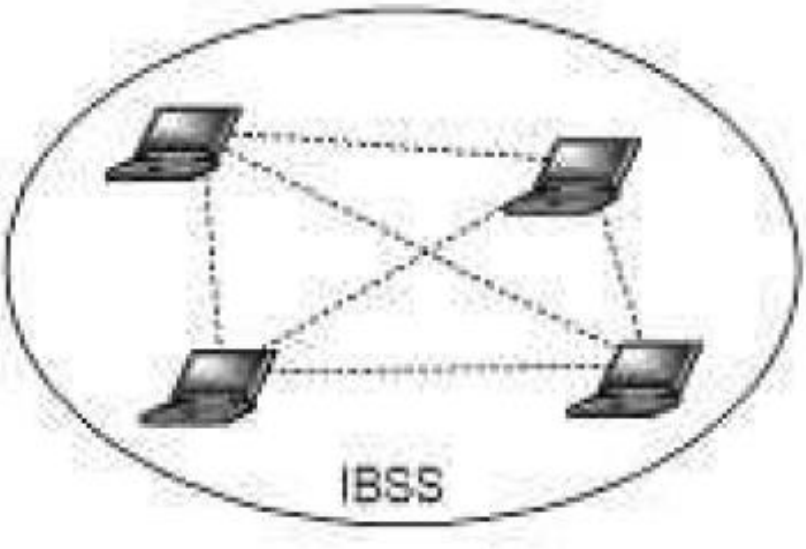

Figure II-16:Plusieurs stations reliées directement entre elles en mode Ad Hoc (IBSS) [12].

II.5.2.1. **Les caractéristiques des réseaux Ad Hoc :**

Les réseaux Ad Hoc sont caractérisés principalement par :

- **Une topologie dynamique :** la topologie des réseaux ad hoc change rapidement et aléatoirement, ceci est causé par la mobilité arbitraire des stations du réseau. Le changement de la topologie change les routes entre les clients.
- **Bande passante limitée :** les réseaux basés sur la communication sans fil utilisent un médium (canal) de communication partagée (ondes radio). Ce partage fait que la bande passante réservée à un hôte soit modeste.
- **Contraintes d'énergie :** les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries. Le paramètre d'énergie doit être pris en considération.
- **Sécurité physique limitée :** les réseaux mobiles Ad Hoc sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques. À cause des limitations physiques qui font que le contrôle des données transférées est minimisé.
- **Erreur de transmission :** les erreurs de transmission radio sont plus fréquentes due à la mobilité des stations (les clientes et celles qui ont un rôle de point d'accès).
- **Interférences :** les liens radios ne sont pas isolés, deux transmissions simultanées sur une même fréquence utilisant des fréquences proches peuvent interférer entre elles.
- **Nœuds cachés :** les nœuds ou stations ne s'entendent pas à cause d'un obstacle qui empêche la propagation des ondes, ainsi ces nœuds pourront commencer leurs émissions simultanément ce qui peut engendrer des collisions au niveau du nœud.
- **La qualité de service :** de nombreuses applications nécessitent certaines garanties relatives par exemple au débit, ou à la gigue (latence ou délai de transmission des données). Dans ces réseaux Ad Hoc, ces garanties sont très difficiles à obtenir à cause de la nature du canal radio d'une part (interférences et taux d'erreur élevés) et au fait que des "liens" entre des mobiles peuvent avoir à se partager les ressources (alors qu'en filaire, deux liens sont indépendants).

II.6. **Description des couches Wi-Fi**

Pour que des utilisateurs puissent communiquer entre eux dans un réseau sans fil, leurs équipements doivent respecter deux règles : d'une, ils doivent se servir d'un média de communication adapté comme les ondes radio dans le cas du Wi-Fi. La seconde contrainte est la synchronisation des communications pour que les échanges se fassent correctement dans l'ordre et sans problème. On a alors spécifié des standards pour pallier à ces problèmes de communication en définissant des protocoles pour gérer les échanges entre les stations du réseau par exemple : comment savoir quand la station peut émettre des informations ou vers quelle station il faut les envoyer, sur quelle fréquence il faut transmettre les informations…etc. [12]

II.6.1. **Le modèle OSI et la norme 802.11 :**

L'ISO est une organisation internationale, non-gouvernementale siégée à Genève en Suisse, formée de plus de 150 pays [16]. Elle développe des protocoles et des standards techniques. L'OSI est l'un de ses modèles développés pour les réseaux informatiques en 1979 [12], il définit des « couches réseaux », leur fonctionnement et les organisent de manière hiérarchique pour un bon déroulement d'une communication dans ces réseaux.

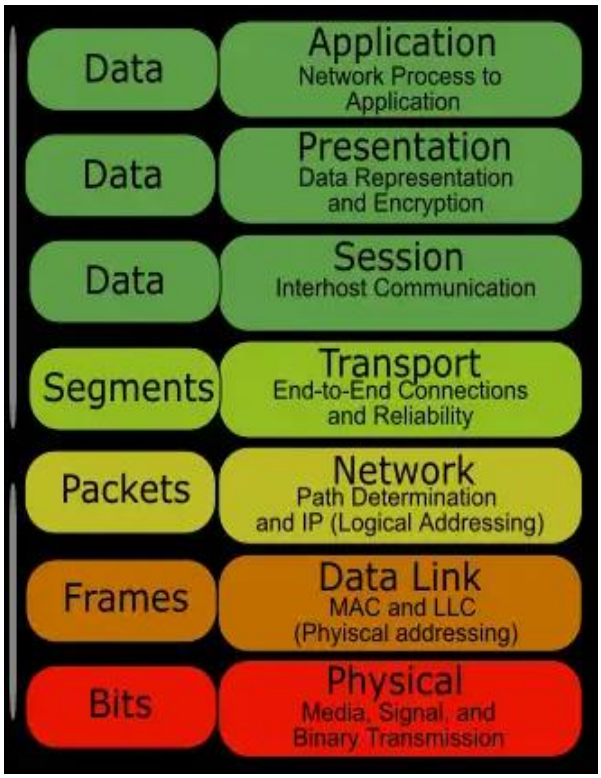

Figure II-17: Les sept couches du modèle OSI [62]

Chaque couche du réseau fournit des services à des couches plus ou moins hiérarchisées pour que deux entités de même niveau échangent des informations, tout ça grâce à un ensemble de règles indispensables pour réaliser ces services et réguler les échanges entre les couches de même niveau. Ainsi lorsqu'un périphérique A est en liaison avec un autre périphérique B, et bien la couche de niveau N de l'ordinateur A communique avec la couche N du périphérique B. Toute communication réussie nécessite utilise un protocole compréhensible des deux côtés.

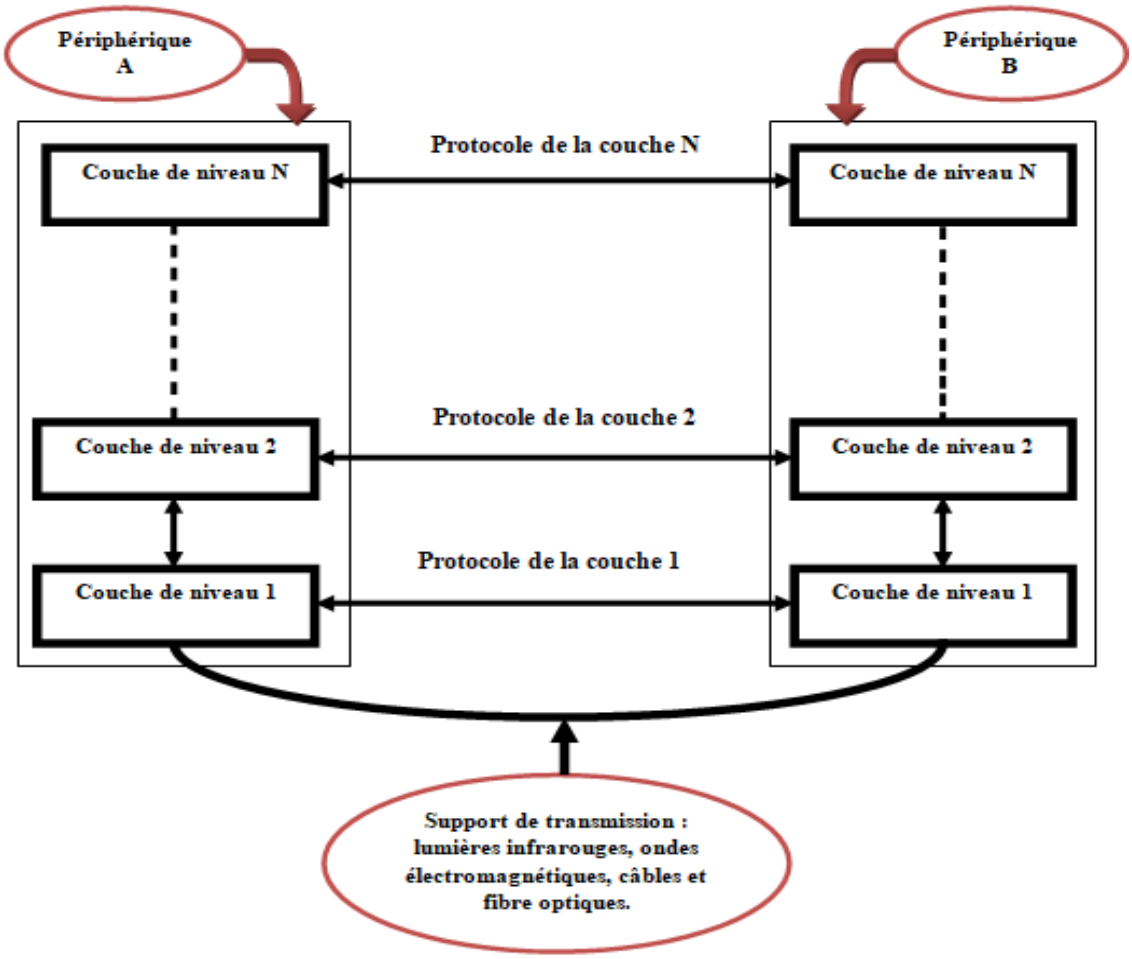

Figure II-18: Représentation de la communication entre couches dans un réseau.

Niveau 1 : la couche physique

Définis la manière dont les données (bits) sont physiquement converties en signaux et les transmet de l'émetteur vers le récepteur en précisant le type du support de communication (câble ou sans fil) [15]. Les modems (modulateurs), les répéteurs ou la connectique des cartes réseaux se placent à ce niveau.

Niveau 2 : la couche liaison de données

Ici, les données sont envoyées sous forme de trames (une succession de bits) d'un nœud [16] (une station) du réseau vers un autre nœud en se servant des adresses MAC de chaque machine, contrôle aussi les erreurs.

Niveau 3 : la couche réseau

La couche de niveau 3 qui gère l'adressage et guide les données via le réseau (LAN) ou même entre différents réseaux (WAN) [12], c'est le « routage » ou acheminement qui consiste à choisir un itinéraire et trouver un chemin sur lequel les paquets vont transiter.

Niveau 4 : la couche transport

Cette couche reçoit des données de la couche « session », les segmente en paquets les fait transiter vers la couche inférieur « réseau » [12], à la réception, c'est l'inverse.

Assure un contrôle des erreurs de transmission si jamais il y en a, veille à ce que le bon transfert de données se fasse de bout en bout avec l'utilisation de données d'acquittement des

échanges (le fameux accusé de réception), introduit la notion de qualité de service (QoS) en déterminant quels flux sont prioritaires comme la vidéo ou la parole et donc ils vont transiter en premier.

Niveau 5 : la couche session

Elle organise, gère et synchronise des dialogues entre diverses stations. Tout d'abord, il y a authentification [16] des utilisateurs puis négociation de la création des sessions entre eux, crée ces sessions et les fermes une fois la communication terminée (un ordre de la couche présentation.). Aussi, la synchronisation est nécessaire pour la demande d'une retransmission en cas d'éventuelle erreur de transfert.

Niveau 6 : la couche présentation

Fait passer les informations, mais se charge aussi de chiffrer, de compresser et de coder [12] les données provenant de la couche applicative grâce aux différents types de codage comme le : MIME, ASCII ou ASN1.

Niveau 7 : la couche application

Cette couche est l'interface utilisateur qui permet l'accès aux ressources du réseau, elle offre des services aux utilisateurs comme le transfert de fichiers, l'envoi ou la réception de courrier électronique, ou encore la navigation sur Internet (lectures des pages web) [12].

En gros, on peut rassembler ces couches en 3 [16] groupes :

- **Les couches hautes :** applications, présentation et session qui offrent les services de gestion de session, de connexion et présentent les informations.
- **Les couches moyennes :** qui gèrent les circuits, assurent le routage et la fragmentation des données.
- **Les couches basses :** liaison de données et physique, s'occupent de l'accès au média.

La norme 802.11 ne concerne que la couche 1 et 2 du modèle OSI, ainsi le Wi-Fi définit quel support de transmission sera utilisé (couche physique) et comment les paquets d'informations doivent être échangés.

Pour ce faire, de nouvelles couches physiques sont mises en œuvre au niveau de la couche 1 ainsi que de nouvelles techniques d'accès au réseau au niveau de la couche 2 comme on peut le voir avec la figure de la page suivante :

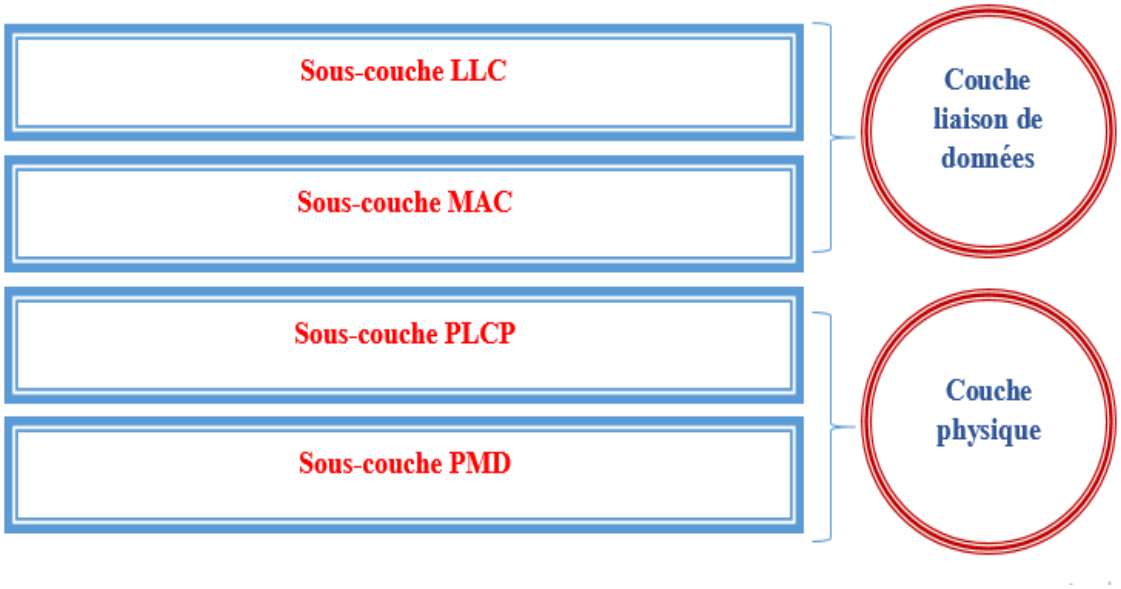

Figure II-19: Couches Liaison et Physique du 802.11

II.6.2. **La couche physique :**

La couche physique transmet les données numériques bit à bit de l'émetteur vers le récepteur [16], mais l'IEEE 802.11 repose sur les ondes radio pour transmettre ces informations et un signal binaire transmit tel quel, c'est-à-dire en bande de base ne sera pas adapté au canal de transmission hertzien, donc l'interface d'accès (carte réseau...) doit transformer le signal numérique en signal radio et réciproquement à la réception.

On s'oriente alors vers les bandes de fréquences ISM et U-NII dont la longueur d'onde permet l'utilisation d'antennes, de taille réduite, intégrées dans les équipements sans fil et mobiles, pour des puissances entre 10 et 100 mW [17], notre signal peut atteindre une portée de 500 mètres.

Dans le standard 802.11, on allie des aptitudes de communication radio et des capacités informatiques. Ainsi, deux sous-couches prennent chacune en charge une partie de ces fonctions, ces sous-couches sont : PLCP et PMD.

- **La sous-couche PMD :** gère l'encapsulation et la décapsulation des trames. Elle spécifie le type de support de transmission, le type d'émetteur-récepteur, gère l'encodage de données à l'aide de diverses stratégies de codage comme : le FHSS, DSSS ou l'OFDM.
- **La sous-couche haute PLCP :** elle permet la liaison entre la couche PMD et la couche MAC, elle « écoute » le support de transmission pour signaler l'état du support à la couche MAC avec un service de notification appelé CCA, si le support est occupé ou libre pour émettre les données.

II.6.3. **Les techniques de transmission :**

II.6.3.1. **FHSS :**

FHSS est basée sur le saut de fréquence. La bande ISM (2.4 à 2.4835 GHz) est divisée en 79 canaux d'une largeur de 1 MHz chacun et on peut définir jusqu'à 26 ensembles de 3 séquences de sauts (soit 78 séquences au total). Les données seront transmises par l'intermédiaire d'un saut d'un canal à un autre toutes les 300 ms selon une séquence prédéfinie par l'émetteur et le récepteur [19], ce choix est important si l'on veut réduire, voir annuler les collisions entre plusieurs transmissions.

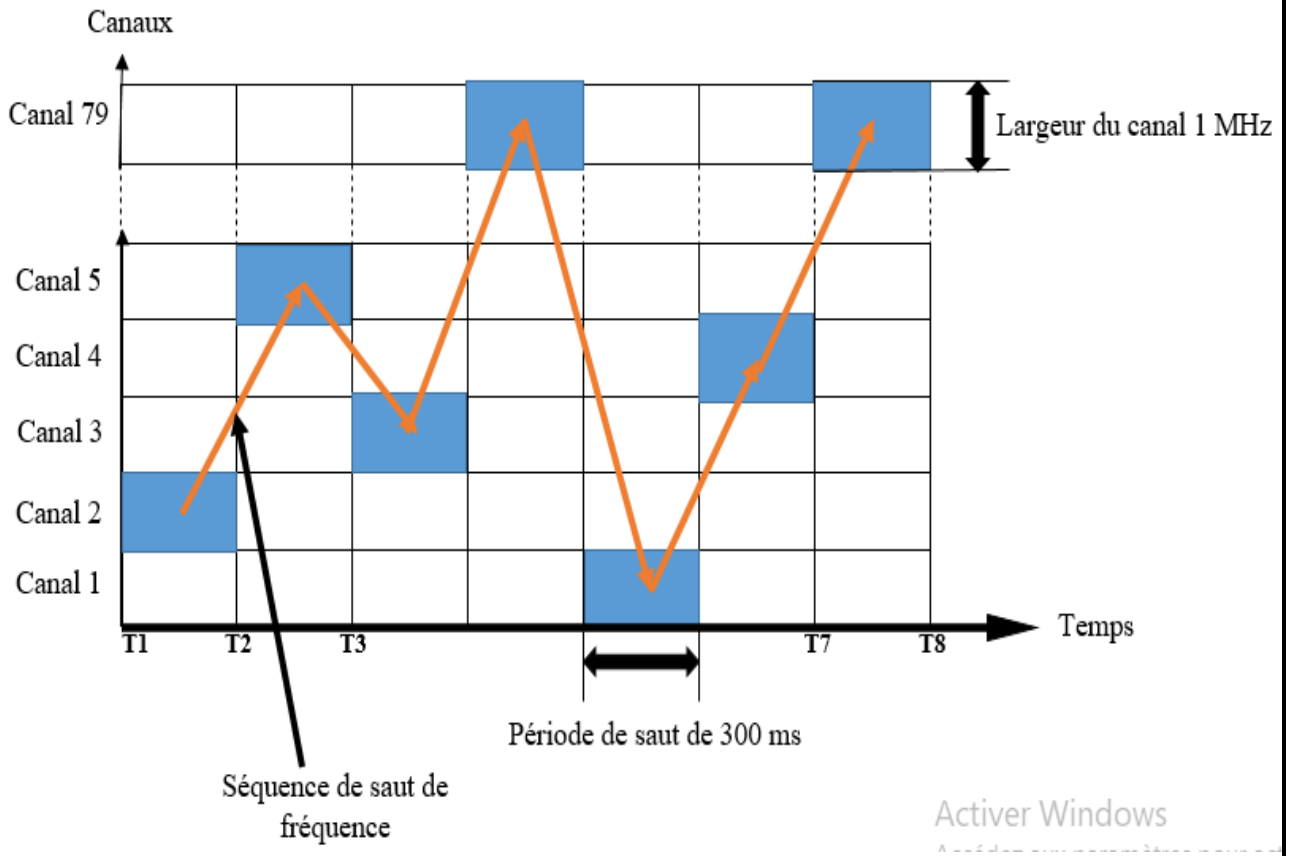

Figure II-20: Exemple de transmission avec la technique FHSS

En mode FHSS, on peut faire fonctionner 26 réseaux 802.11 (3 stations émettrices par réseau) en même temps se trouvant dans une même zone et chaque réseau ayant une des 78 séquences prédéfinies. L'inconvénient majeur est le débit qui ne dépasse pas les 2 Mbps à cause de la largeur des canaux qui est de 1 MHz.

Aussi des transmissions provenant de plusieurs stations peuvent transiter simultanément sur la même bande de fréquence, il faut juste éviter d'utiliser les mêmes séquences de canaux pour éviter des collisions, la transmission 1 pourra utiliser la séquence suivante : 123, 123, 123, …, etc. Pendant qu'une autre transmission utilise cette séquence : 312, 312, 312 [12], …, etc.

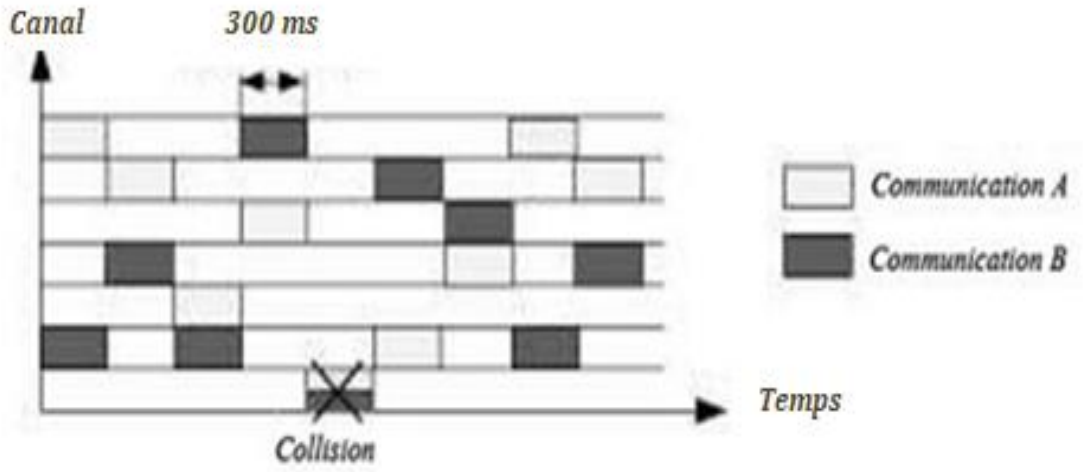

Figure II-21: Exemple de partage des ondes avec le FHSS [12]

II.6.3.2. **DSSS**

La communication via la technique DSSS ne se fait que sur un seul canal pour chaque utilisateur, elle divise la bande ISM en 14 canaux, de 22 MHz de largeur [16] pour chacun, numérotés à partir de 2.4 GHz (Suivant le théorème de Shanon : Fe ≥ 2×fmax), avec une bande passante de 22 MHz on aura 22Mbps. Donc, en respectant le théorème de Shanon, cela fait que pour avoir 11Mbps, il nous faut une bande passante de 22MHz.). À cause la largeur de la bande ISM (83.5 MHz), les canaux sans s'entremêlent, comme on le constate dans la figure dessous :

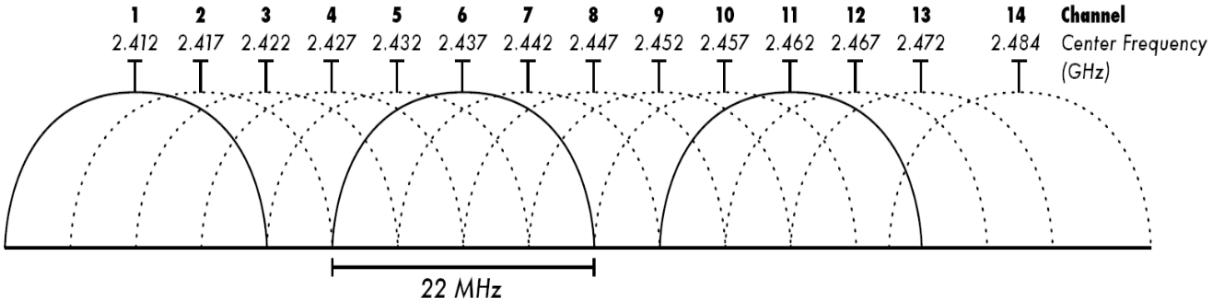

Figure II-22: La décomposition de la bande ISM en sous canaux de 22 MHz [64]

Les centres des sous-canaux sont espacés entre eux de 5 MHz de sorte à ce qu'ils se recouvrent en partie, comme on peut le voir dans la figure II-22.

L'utilisation d'un seul canal pour transmettre des informations posera des problématiques si plusieurs réseaux DSSS se superposent, ce qui fait que les systèmes DSSS sont plus sensibles aux interférences. Pour pallier ce problème et assurer une bonne transmission, il faut allouer aux stations des canaux appropriés espacés de 5 unités et qui ne se chevauchent pas, si un réseau utilise le canal 6, le canal 5 et 7 seront interdits pour un autre réseau trop proche, c'est pareil avec les canaux 2, 3, 4, 8, 9 et 10 [19], qui ne peuvent pas aussi être alloués à cause de l'étalement de la bande passante du canal 6. Les canaux qui peuvent être utilisés sont les canaux 1, 11, 12,

13 et avec une largeur de 83.5 MHz, on ne peut avoir que 3 réseaux qui émettent sur une cellule sans risque de chevauchement.

Dans le DSSS, chaque bit est codé avec une séquence de bit « chip » et plus le code est long, plus il sera mieux protégé face au bruit, mais le débit sera lui aussi démultiplié.

Si l'on code un 0 avec 10011 et le 1 avec 01100, donc même si à la réception l'on reçoit la séquence 00111, on pourra l'interpréter comme étant 10011 car c'est plus proche de cette séquence et que l'on a reçu un 0 en fait.

II.6.3.3. **OFDM**

Elle est apparue dans les années 60 et elle permet des débits allant au-delà de 11 Mbps et on la retrouve à la fois dans le 802.11g, le 802.11a et dans le 802.11n, mais aussi dans des technologies comme le WIMAX [12] et certaines communications de la téléphonie mobile.

L'OFDM permet la transmission de diverses communications sur une même bande de fréquences en même temps grâce au multiplexage et il y en a 2 types :

- **TDM :** la communication dispose d'un certain lapse de temps pour émettre des données sur l'ensemble du spectre.
- **FDM :** Le spectre est partagé en plusieurs sous-porteuses et chaque communication émet sur une de celles-ci, mais avec un risque d'interférence entre les sous-porteuses (ICI).

En Wi-Fi, 52 sous-porteuses d'environ 312,5 KHz chacune, permettent de couvrir un spectre de 20 MHz formant ainsi un canal de communication OFDM. Sur les 52 sous-porteuses, 48 sont utilisées pour transférer les données. Les autres servent à la synchronisation et aux corrections associées. [16]

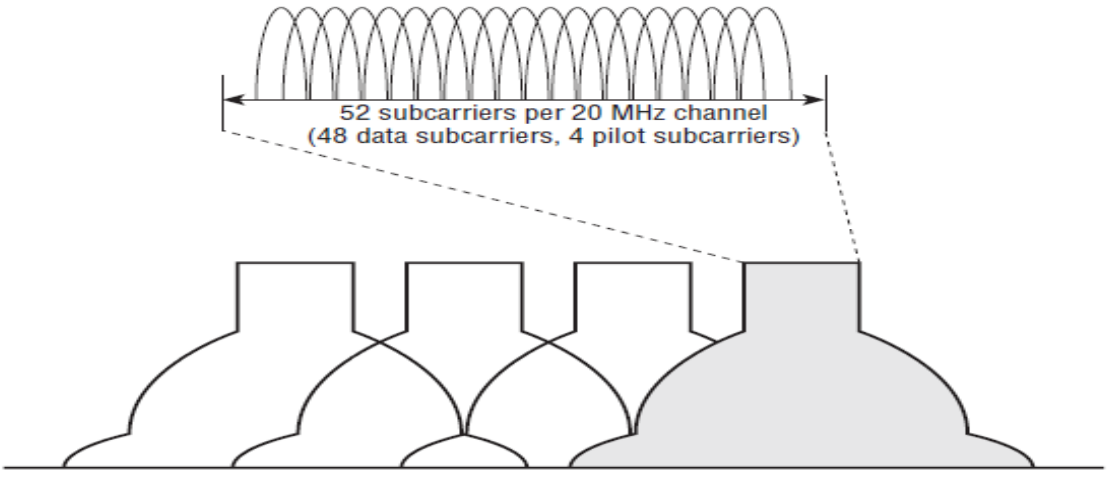

Figure II-23: Le partage de fréquence dans l'OFDM [65].

Pour éviter l'interférence entre symboles, arrivant en même temps au récepteur, un délai d'attente doit être respecté entre deux envois. Appelé intervalle de garde (GI) de 800 ns en 802.11a et 802.11g. Si l'environnement le permet, ce paramètre peut être réduit à 0,4 s en

802.11n. Ainsi, par exemple, le temps total d'envoi du symbole, incluant le GI passe de 4 s à 3.6 s, ce qui augmente encore un peu plus le débit possible.

II.6.3.4. **MIMO** :

Le MIMO désigne toutes les techniques reposant sur des antennes multiples à la fois du côté de l'émetteur et du récepteur pour l'émission et la réception des signaux sur un unique canal radio (Diverses APs et stations sont équipés de plusieurs antennes [12]), cette diversité d'antennes améliore la portée, la fiabilité et surtout le débit de communication. Ces techniques sont représentées dans la figure II-24 :

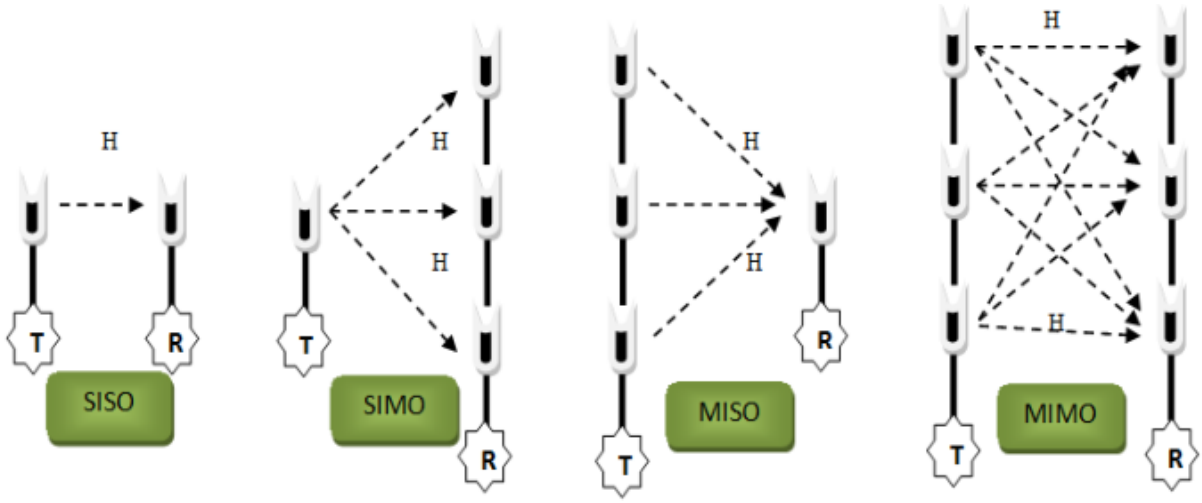

Figure II-24: Les quatre configurations SISO, SIMO, MISO et MIMO [66]

Notre signal est divisé en plusieurs flux d'une fréquence semblable (le nombre de flux dépend de celui des antennes à l'émission et à la réception.).

II.6.4. **La couche liaison de données :**

- ✓ Elle gère l'échange de trames entre les nœuds d'un réseau via un support (on appelle un « nœud » tout périphérique réseau connecté à un support physique, dans notre cas support hertzien.).
- ✓ Elle permet aux couches supérieures d'accéder à ce support.
- ✓ Elle encapsule les paquets provenant de la couche réseau en des unités appelées trames qu'elle envoie ensuite à la couche physique.
- ✓ Elle contrôle aussi la manière dont ces données sont placées et reçues grâce à des systèmes de contrôle d'accès au support et détecteurs d'erreur.

La couche liaison de données est divisée en deux sous-couches :

- **La sous couche LLC :**

C'est le lien logique entre la couche MAC et la couche réseau [68]. Son but est de permettre aux protocoles de niveau 3 de reposer sur une couche unique (LLC), quel que soit le protocole

sous-jacent utilisé. Elle permet aussi de renvoyer une trame s'il y a un problème sur la ligne de transmission.

- **La sous couche MAC :**

Cette sous-couche est le « cœur » d'un réseau 802.11 [16], elle intègre diverses fonctions comme le contrôle d'erreur par CRC, la sécurité, adressage et formatage des trames, qualité de service, la fragmentation et le réassemblage des trames. …, etc.

La sous-couche MAC gère le partage du support de communication pour cela avec une méthode pour accéder au canal de transmission : PCF. Pour éviter qu'il y ait des collisions entre les communications sur le support hertzien et améliorer la qualité de service, MAC utilise un mécanisme d'esquive de collision : le protocole CSMA/CA.

La couche MAC définit aussi « les adresses MAC ». C'est un identifiant unique sur 48 bits (6 octets) que possède chaque périphérique, prenant l'exemple suivant noter en hexadécimal : 00-04-23-8B-B5-0B, le 00-04-23 [12] désigne le constructeur de matériel et dans notre cas cet identifiant est celui d'INTEL, le 8B-B5-0B est assigné à la carte réseau et donc unique. Lors d'une transmission, une trame contient au moins l'adresse de la station émettrice et celle réceptrice.

Unicast, Multicast et Broadcast [12] : « Unicast », une information est destinée à un récepteur unique, en vrai ce message est reçu par tout le monde sur le réseau, mais comme sur la trame MAC leur adresse n'est pas la destination alors il l'ignore.

« Broadcast ou diffusion d'informations », le paquet est adressé à tout le monde sur le réseau. Pour ça, on utilise l'adresse suivante : FF:FF:FF:FF:FF:FF. Idéal lorsque plusieurs stations sont intéressées par les mêmes données émises (une vidéoconférence).

Un paquet peut être adressé à un groupe de stations, grâce à certaines adresses MAC particulières destinées à cet effet (Par exemple : 01:00:5E:00:00:01). Ainsi, les stations intéressées par ce paquet le prendront en compte, les autres l'ignoreront. Ce mode de transmission est dit « Multicast », c'est un cas particulier du « Broadcast ».

II.6.4.1. **La trame MAC :**

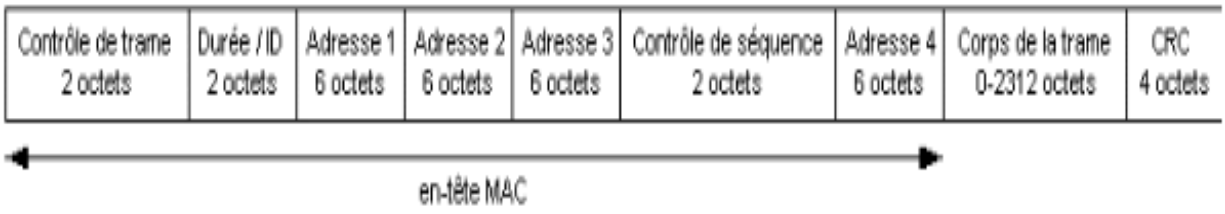

Figure II-25: Format général d'une trame MAC [67].

- **Contrôle de trame (2 octets) :**

Le champ de contrôle de la trame est lui-même divisé en plusieurs sous-champs :

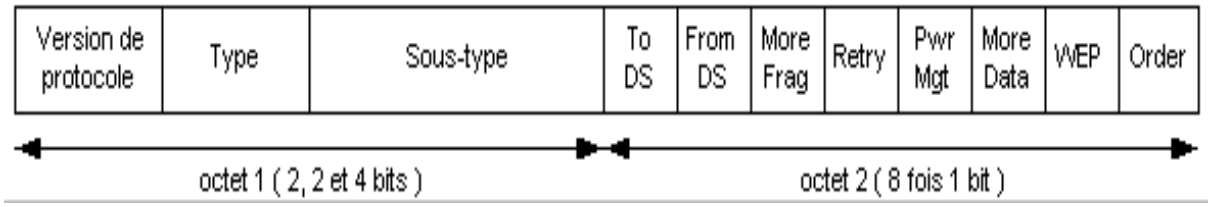

Figure II-26: Schéma du champ de contrôle d'une trame MAC [67].

Version du protocole : 2 bits qui donnent la version du protocole utilisé, dans le cas du 802.11 cette valeur est fixée à 0 [72].

Types et sous-type : 6 bits qui décrivent le type des trames (trames de contrôle, de données et de gestion) sur 2 bits et les sous-types (RTS, CTS, ACK, CF pool, CF End, …, etc.) sur 4 bits [72].

Type	Description du type	Subtype	Description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Annoucement traffic indication message
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	ACK
01	Control	1110	Contention Free (CF)-end

01	Control	1111	CF-end + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack+CF-Poll
10	Data	0100	Null function (no Data)
10	Data	0101	CF-Ack
10	Data	0110	CF-Poll
10	Data	0111	CF-Ack + CF-Poll
10	Data	1000-1111	Reserved
11	Data	0000-1111	Reserved

Tableau II-3: Types et sous types de trames MAC [75]

To DS et **From DS :** 1 bit chacun, ils sont utilisés pour définir le sens de la trame.

To DS	From DS	Signification
0	**0**	Trame entre deux stations d'un réseau ad-hoc .
1	**0**	Trame issue d'une station sans fil et à destination d'un AP
0	**1**	Trame issue d'un AP et à destination d'une station sans fil.
1	**1**	Trame issue d'un AP vers un autre AP, utilisé pour l'interconnexion de réseaux locaux par un pont sans fil.

Tableau II-4: Valeurs des champs To DS et From DS [72].

More Fragment : 1 bit, est positionné à 1 lorsque d'autres fragments de la trame sont à suivre et à 0 lorsqu'il est le dernier fragment ou que la donnée ne fut pas fragmentée.

Retry : 1 bit, il est positionné à 1 s'il s'agit d'une réémission (la trame a déjà été envoyée précédemment.).

Power Management : 1 bit, s'il est à 1, la station passe en mode veille à la fin de la trame et si elle est active, le bit est à 0. Si la trame vient d'un AP, le bit est toujours à 0 [67].

More Data : 1 bit, est un champ positionné à 1 lorsque d'autres trames restent à transférer depuis un point d'accès vers une station.

WEP : 1 bit, il est positionné à 1 si le contenu de la trame est crypté par le mécanisme de clé WEP.

Order : 1 bit, est à 1 lorsque les trames sont transférées en utilisant le mode strictement ordonné [72].

Temps de réservation (durée/ID, 2 octets) :

Il indique la durée d'utilisation du canal de transmission en µs et donc utiliser pour le calcul du NAV.

Types d'adresses :

Dans un réseau 802.11, les adresses MAC source et destination ne suffisent pas pour déterminer le cheminement d'une trame. C'est pour cela qu'il peut y avoir jusqu'à 4 adresses nécessaires pour définir le cheminement de la trame. [72]

- **BSSID :** en mode infrastructure c'est l'adresse MAC de l'AP, et en mode Ad-Hoc il s'agit de l'adresse MAC locale du BSSID (générée lors de la création de l'IBSS).
- **DA** : adresse, individuelle ou de groupe, identifie-le ou les destinataires.
- **SA :** adresse individuelle de la station ayant transmis la trame.
- **RA :** BSSID destination (point d'accès récepteur).
- **TA :** BSSID source (point d'accès émetteur).

Les bits To DS et From DS définissent le type de réseau dans lequel la trame est acheminée. Le tableau suivant résume l'utilisation des 4 adresses d'une trame et des bits To DS et From DS :

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	Aucun
0	1	DA	BSSID	SA	Aucun
1	0	BSSID	SA	DA	Aucun
1	1	RA	TA	DA	SA

Tableau II-5: Utilisation des adresses d'une trame 802.11 [72]

Contrôle de séquence (2 octets) :

La valeur de ce champ est utilisée dans le cas d'envoi de trames fragmentées et est codée sur 16 bits.

- Numéro de séquence (12 bits) : numéro assigné à chaque trame, initialisé à 0 puis incrémenté pour chaque nouvelle trame [67].
- Numéro de fragment (4 bits) : numéro assigné à chaque fragment, si la trame est fragmentée. Il est initialisé à 0 puis incrémenté pour chaque nouveau fragment [68].

Corps de la trame (0 à 2312 octets) :

Il s'agit du message, la taille peut être supérieur à 1500 octets. Il n'y a pas de données pour les trames de contrôle et de gestion [67].

CRC :

C'est un champ de contrôle de 32 bits pour vérifier qu'il n'y a pas eu de problème durant la transmission des trames [72].

II.6.4.2. **Les méthodes d'accès**

CSMA/CA

Dans un réseau local Ethernet classique, on utilise le CSMA/CD. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine sur le canal de transmission. Si, en effet il y a information qui transite su le canal, les deux machines patientent un temps aléatoire avant de retenter l'émission [19].

Ce procédé n'est pas possible dans le sans-fil, car deux stations communiquant avec un récepteur peuvent ne pas s'entendre mutuellement en raison de leur rayon de portée, et même si la station émettrice teste l'état du support, cela ne veut pas dire que le support est libre autour du récepteur.

- Le problème des stations cachées : deux stations peuvent ne pas s'entendre à cause de la distance les séparant : car elle est trop grande ou qu'un obstacle les empêche de communiquer même si elles ont des zones de couverture qui se recoupent [19].

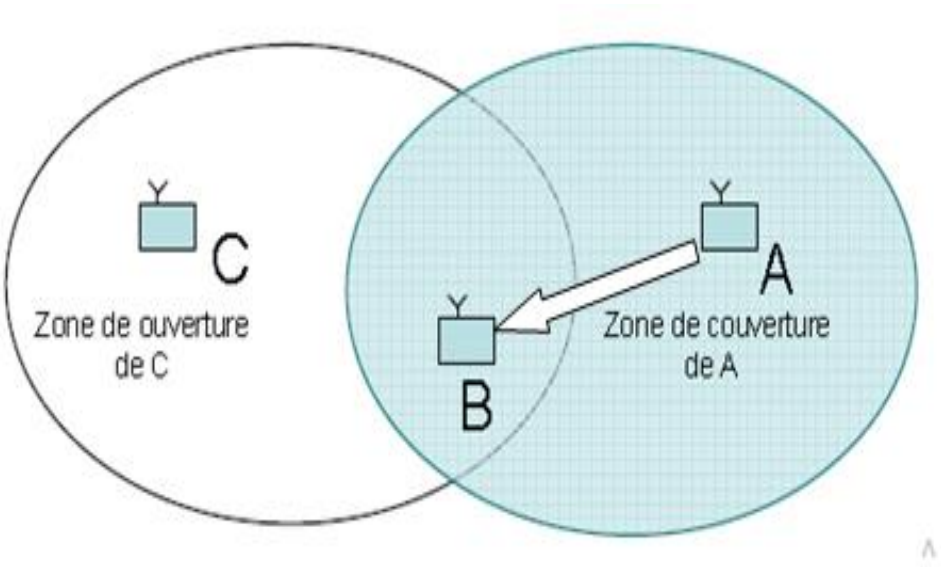

Figure II-27: Le problème des stations cachées [19]

Si les stations A et C ne peuvent pas entendre les émissions de l'une et de l'autre, elles émettront des paquets en même temps à une station B située dans l'intersection des zones de couverture, il va y avoir collision entre les paquets et B ne pourra recevoir aucune des communications.

- Le problème des stations exposées [19] : Une station A transmet des données à une station D. Si une station C écoute le canal radio et entend la communication entre A et D, elle conclut qu'elle ne peut pas transmettre des paquets à une station B, or si C transmettait, cela créerait des collisions seulement dans la région entre B et C et non dans les régions où D et A se situent.

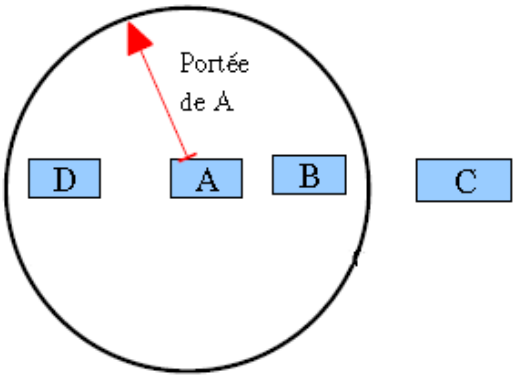

Figure II-28: Le problème des stations exposées [23].

Pour combler ces problèmes, 802.11 utilise le mécanisme « d'esquive de collision » ou CSMA/CA. La station émettrice écoute le réseau, s'il est encombré, la transmission est différée, elle utilise un timer appelé NAV [70] qui suspend toutes les transmissions sauf celles des stations émettrices et réceptrices. Le NAV est calculé par rapport au champ TTL des trames envoyées, ainsi les stations situées autour des stations source et destination sauront la durée de la transmission à venir. Les stations émettront après la fin du NAV.

Mais si le canal est libre pendant un temps donné appelé DIFS, la station va émettre. Elle commence par la transmission d'un message RTS (prêt à émettre en français) qui contient des informations sur le volume des données à émettre et la vitesse de transmission de la station.

Le récepteur répond par CTS que le champ est libre, la station va alors émettre les données. Le récepteur envoie un accusé de réception (ACK) après avoir reçu toutes les données [19].

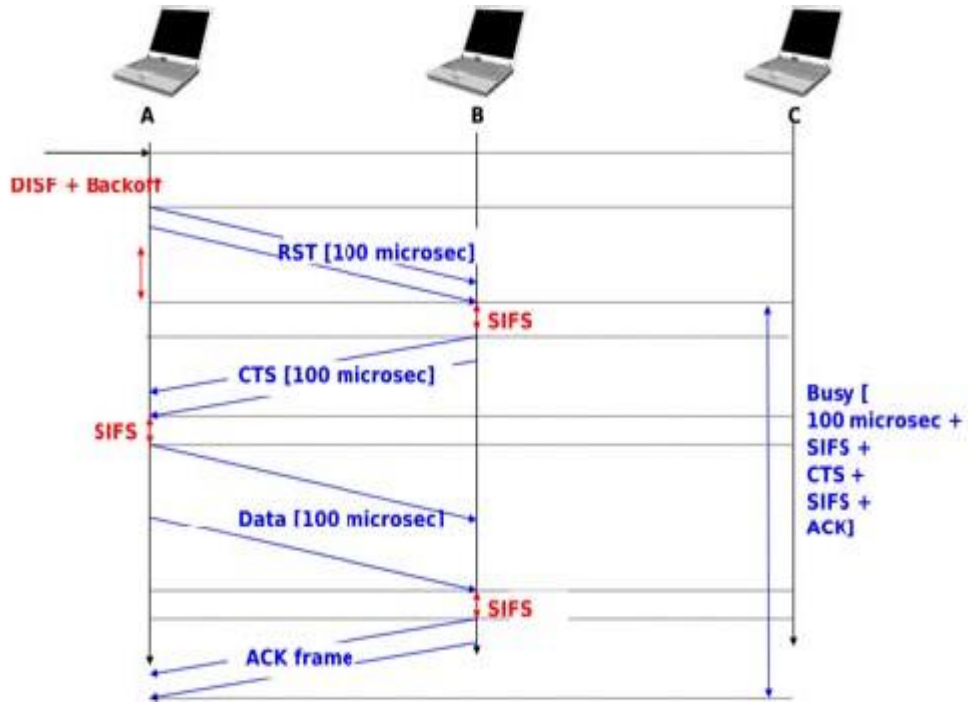

Figure II-29: Exemple détaillé avec CSMA / CA [71].

Le SIFS est un court espace entre deux trames IFS. Il est utilisé pour la transmission des trames ACK, CTS ou encore des rafales de trames issues d'une même station.

La valeur du DIFS est calculée comme suit : **DIFS = SIFS +2 × Slot Time**, le Slot Time est la durée minimale pour déterminer l'état du canal + temps aller-retour + temps de propagation [19]

Standard	Temps SIFS
802.11	28 us
802.11b	10 us
802.11a	16 us
802.11g	10 us

Tableau II-6: Durées du délai SIFS [64]

Standard	Slot Time	Temps DIFS
802.11	50 us	128 us
802.11b	20 us	50 us
802.11a	9 us	34 us
802.11g	9 ou 20 us	28 ou 50 us
802.11n (2.4 GHz)	9 ou 20us	28 ou 50 us
802.11n (5 GHz)	9 us	34 us
802.11ac (5GHz)	9 us	34 us

Tableau II-7: Durée du délai DIFS [30]

Le débit peut chuter considérablement s'il y a beaucoup d'équipements communiquant en même temps, si une station communique à bas débit, elle va ralentir les autres.

Les stations attendent le silence pour communiquer, la présence d'une interférence continue peut interrompre 100 % du trafic. Ceci arrive par exemple à cause d'un four à micro-ondes en fonctionnement car utilisant les mêmes bandes de fréquences, cela peut même être un brouillage volontaire.

Un autre problème du CSMA/CA est qu'il ne garantit pas une fluidité de transfert de données, car la station attend un temps aléatoire avant de transmettre les données (C'est gênant pour la vidéo ou le son car les informations doivent arriver à des intervalles réguliers.

Pour remédier à ces problèmes, le standard 802.11 utilise une autre méthode de partage du média de communication : le mode PCF.

Le mode PCF

La méthode PCF est idéale pour des données vidéo ou voix [16].

Toutes les stations sont reliées à un point d'accès, l'AP distribue la parole à chacune des stations, ce système est dit libre de toute dispute (CF) car il n'y a plus de collisions possibles.

L'AP commence par générer une balise appelée « beacon frame » pour indiquer qu'il passe en mode PCF puis il se tourne successivement vers chacune des stations et leur alloue un « temps de parole » plus ou moins long, grâce à une requête CF-Poll (interrogation).

Si la station prend la parole, elle répond avec un paquet CF-ACK. Elle peut alors émettre un ou plusieurs paquets pendant cette période. Si elle n'a toujours rien émis au bout d'un court intervalle appelé PIFS, alors l'AP passe à la station suivante. Les autres stations attendent patiemment [12].

Pour qu'une station sache quand parler librement, il faut qu'elle soit synchronisée avec l'AP, ce dernier envoie régulièrement des trames « balises » pour assurer la synchronisation. Chaque balise indique le début d'une séquence PCF et indique la durée de la séquence totale ainsi que la durée maximale de la phase PCF.

Le mode PCF divise le temps de parole plus équitablement entre les stations il est donc idéal pour l'envoi de données multimédias.

La valeur du PIFS est calculée comme suit : **PIFS = SIFS + Slot Time [30].** La durée des SIFS est la même que celles du tableau [64].

Standard	Slot Time	Temps PIFS
802.11	50 us	78 us
802.11b	20 us	30 us
802.11a	9 us	25 us
802.11g	9 ou 20 us	19 ou 30 us
802.11n (2.4 GHz)	9 ou 20 us	19 ou 30 us
802.11n (5 GHz)	9 us	25 us
802.11ac	9 us	25 us

Tableau II-8: Durée du délai PIFS [30]

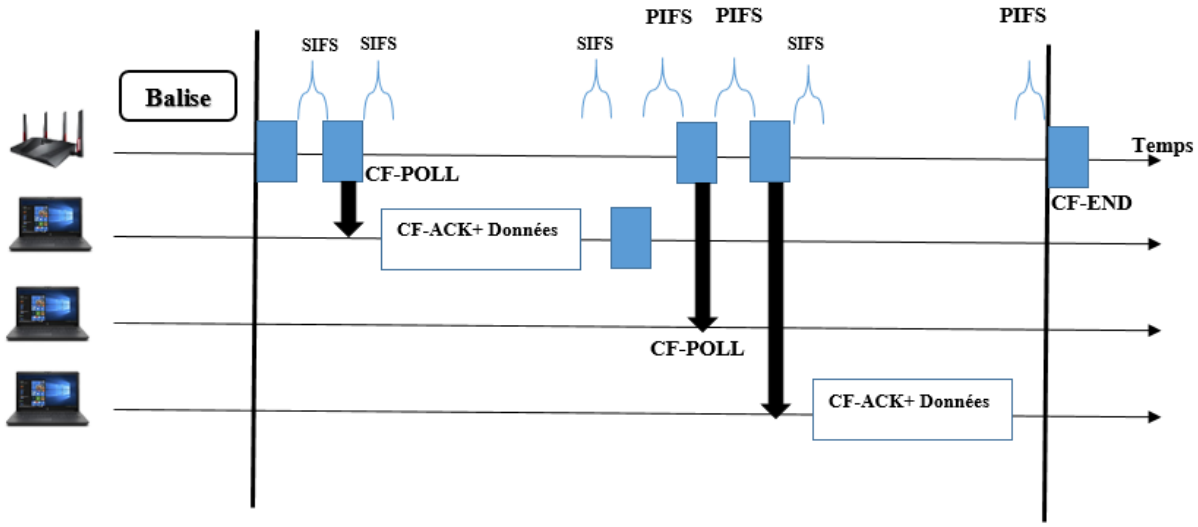

Figure II-30: Le fonctionnement du mode PCF.

II.7. Conclusion

Après une vue d'ensemble sur les réseaux sans fil du chapitre précédent, l'étude dans ce second chapitre s'est focalisée sur l'un des standards des WLAN : le Wi-Fi et ses différentes technologies. En premier lieu, nous avons défini le réseau Wi-Fi ensuite nous avons présenté la famille de l'IEEE 802.11 (les standards) qui ne sont en fait que des évolutions de la norme initiale 802.11 de 1997, des évolutions faites grâce à diverses techniques de multiplexage et de modulation, ces normes ne cessent d'évoluer avec prochainement le 802.11 ax.

Après nous sommes passés aux équipements physiques nécessaires pour la mise en place d'un réseau Wi-Fi, comme les cartes Wi-Fi (différentes selon l'équipement utilisé), les antennes aussi différentes mais selon leur direction d'émission, et les points d'accès qui sont nécessaires à l'installation d'un réseau Wi-Fi en mode infrastructure que nous avons présenté aussi, sauf que ces APs ne sont pas requis pour mettre en place un réseau en mode ad hoc. En dernier lieu, nous avons décrit les couches dans lesquelles opère un réseau Wi-Fi, qui sont les deux couches basses du modèle OSI (couche physique et couche liaison de données)

La technologie Wi-Fi est vaste et nous avons énormément de possibilité pour la mise en place de ce réseau selon nos besoins et nos moyens (un particulier n'aura pas besoin d'autant d'effectifs qu'une entreprise).

Néanmoins la transmission par ondes radio est sujette à controverse, l'utilisation de bandes de fréquences libres ne garantit aucune sécurité pour les données, une personne indésirable peut intercepter notre signal si elle se trouve dans la zone d'émission de notre station. Il est difficile d'envisager une limite absolue au réseau, car les ondes radio se propagent dans tous les sens dans une trajectoire sphérique et sur une grande superficie. Le sans-fil permet donc à un malveillant de profiter de la connexion (si le réseau de l'entreprise est connecté au réseau Internet), et pourra même s'introduire dans le réseau pour produire des actions illégales. Mais les choses ne sont pas restées telles quelles, il faut dire que la sécurité dans le réseau Wi-Fi est un sujet pris très au sérieux et plusieurs solutions existent, cela fera l'objet de notre troisième chapitre.

CHAPITRE III

Sécurité des réseaux Wi-Fi

III. Sécurité des réseaux Wi-Fi

Introduction

Les chapitres précédents nous ont permis de voir à quel point les réseaux sans fil, et en particulier la technologie Wi-Fi intéressante. Cependant, un problème majeur est né en même temps qu'elle : comment protéger son réseau des intrus ? Après tout, n'importe qui peut capter une onde électromagnétique. Donc n'importe qui peut lire le contenu de vos communications Wi-Fi. Néanmoins, il existe de nos jours des solutions très robustes pour rendre un réseau sans fil presque aussi sécurisé qu'un réseau filaire. Cependant, elles sont loin d'être parfaites. Nous allons voir dans ce chapitre les différents types d'attaques que peut subir un réseau Wi-Fi ainsi que les solutions proposées pour y remédier.

III.1. Définitions

III.1.1. Définir la sécurité

Un système d'informations permet le stockage et permet l'échange de données. Alors sécuriser un système d'information est une priorité absolue si l'on veut réduire le risque que les données soient compromises ou qu'elles ne puissent plus être échangées.

Il faut prendre en compte tous les risques possibles tels que : les défauts des logiciels et matériels, les attaques volontaires ou encore les erreurs humaines et les réduire le plus possible si l'on veut parler de sécurité dans un réseau.

III.1.2. Les principes de la sécurité informatique

La sécurité d'un système d'information, et plus particulièrement d'un réseau, s'appuie sur cinq thèmes clés. Si chaque point est assuré, on peut dire que le système est sécurisé.

- **La confidentialité :** l'accès aux ressources gérées par le système et donc aux données doit être réservé aux personnes autorisées. Le but est d'éviter toute divulgation d'information.
- **L'intégrité :** les données ne doivent pas être modifiées ou perdues. Il faut en particulier pouvoir s'assurer que ce qui est reçu correspond bien à ce qui a été envoyé.
- **La disponibilité :** permet de garantir l'accès à un service ou à des ressources en toutes circonstances.
- **L'authentification :** c'est l'assurance que chaque utilisateur du réseau est bien celui qu'il prétend être.
- **La non-répudiation :** c'est la garantie qu'aucun des deux partis d'un échange ne pourra nier la transaction.

Les actions seront ensuite entreprises en toute connaissance de cause. Le risque évalué peut-être :

- Assumé, on choisit de ne pas s'en protéger malgré la connaissance des conséquences.
- Limité, en le réduisant ou diminuant ses causes au maximum.
- Transféré, en le déportant à un autre niveau.

- Evité, et donc après sa mise en évidence, le système d'information est protégé à ce niveau.

III.2. **Attaque d'un réseau Wi-Fi [12] [76] [77]**

Les réseaux Wi-Fi peuvent être attaqués de plusieurs façons, et à différents niveaux. Pour pouvoir faire face à ces attaques, nous devons préalablement les définir et connaître qu'elles sont les composantes matérielles et logicielles qu'elles visent.

III.2.1. **Les attaques passives**

Les attaques passives sont les attaques où le pirate se met en écoute non autorisée, en surveillant simplement les transmissions sans modifier les données, ou le fonctionnement du réseau. Leurs dangerosités résident dans le fait qu'elles sont souvent indétectables, mais une prévention est possible.

III.2.1.1. **Le sniffing (espionnage) :**

L'attaque la plus utilisée car cela consiste à écouter les transmissions des différents utilisateurs du réseau sans fil, et de récupérer n'importe qu'elles données transitant sur le réseau si celles-ci ne sont pas cryptées efficacement. Il s'agit d'une attaque sur la confidentialité.

Il suffit pour cela de disposer d'un adaptateur Wi-Fi capable de lire toutes les trames qui circulent, et pas uniquement celles qui lui sont adressées (le mode monitor). Ensuite, il faut utiliser un logiciel d'analyse du réseau comme « wireshark » ou « Kismet » afin de capturer et afficher les paquets.

L'espionnage conduit à la divulgation d'informations confidentielles (Mots de passe, documents secrets, numéros de cartes bancaires…, etc.) ou bien prépare une attaque active de plus grande envergure.

La Figure suivante illustre le schéma classique d'une attaque de type sniffing.

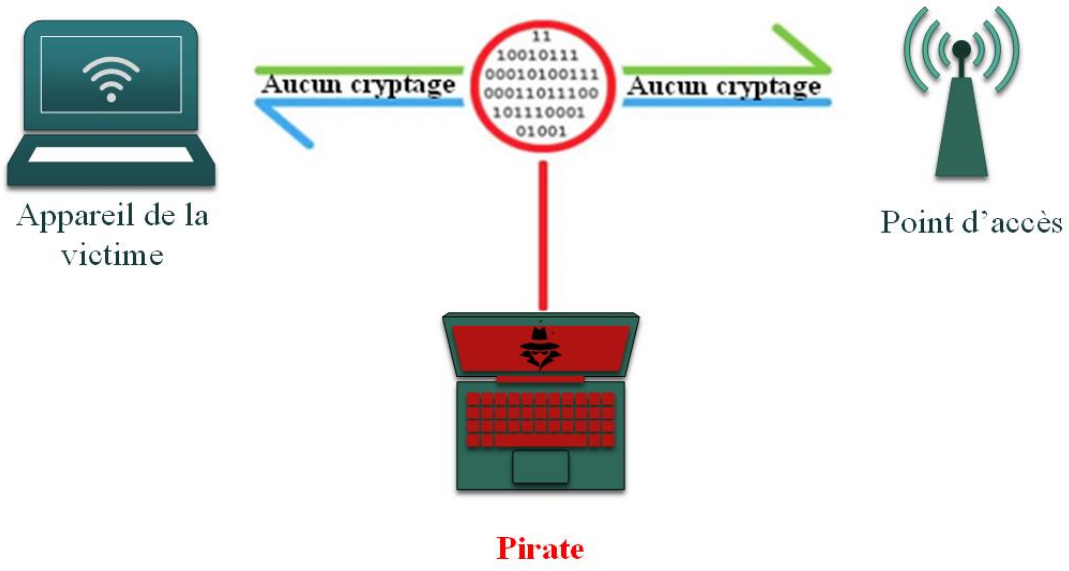

Figure III-1: L'attaque d'écoute passive sur un réseau sans fil non sécurisé.

III.2.2. **Les attaques actives**

Les attaques actives sont les attaques où le pirate modifie des données, s'introduit dans des équipements du réseau ou perturbe le bon fonctionnement de ce dernier. Elles se basent généralement sur des vulnérabilités aux niveaux physique et protocolaire.

Parmi les principales attaques actives :

III.2.2.1. **Spooffing (usurpation) :**

Le spooffing consiste à usurper soit l'adresse MAC, soit l'adresse IP (après l'intrusion) d'une autre machine. En modifiant l'adresse source dans l'en-tête du paquet, le récepteur croira avoir reçu un paquet de cette machine. Si le serveur considérait cette machine comme une machine de confiance, beaucoup de données sensibles pourront être consultées, modifiées, voir même supprimées.

III.2.2.2. **Le DOS (Déni de service) :**

Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, et empêcher les utilisateurs légitimes d'un service de l'utiliser. Elle est souvent utilisée sur Internet afin de rendre inutilisable un site web, et peut parfois s'accompagner d'une demande de rançon pour cesser l'attaque.

Sur les réseaux Wi-Fi, ce type d'attaque peut s'opérer de différentes manières au niveau des couches 1 et 2 du modèle OSI. Le facteur commun étant leur efficacité et la facilité de leur mise en œuvre.

- **Attaque par brouillage radio sur la couche physique :**

Les ondes radio sont très sensibles aux interférences, la bande ISM 2,4 GHz implémentée dans la majorité des périphériques Wi-Fi a aussi d'autres usages (Four à micro-onde, Bluetooth…, etc.), ce qui peut occasionner des conflits accidentels tels que des déconnexions ou des baisses de débit. Cependant, un pirate peut exploiter cette faille afin de brouiller toutes les communications d'un réseau Wi-Fi en utilisant un puissant émetteur radio sur la fréquence de celui-ci.

La dangerosité de cette attaque réside dans le fait qu'elle est quasiment imparable, bien qu'il existe des équipements radio qui permettent de localiser l'emplacement de l'émetteur du signal parasite.

- **Attaque de désauthentification au niveau de la couche MAC :**

Cette faille vient du fait que rien n'est prévu dans le standard 802.11 pour sécuriser les trames de management. Un pirate peut alors usurper l'identité d'un AP et utiliser des trames de désauthentification pour déconnecter un utilisateur précis du réseau, ou alors envoyer un flux continu de ces trames à toutes les stations connectées au point d'accès pour empêcher l'utilisation de ce dernier.

Le but de cette attaque peut être la capture de mot de passe lors de la réauthentification, ou la redirection des clients vers un point d'accès pirate (Attaque evil twin, MitM…, etc.).

III.2.2.3. **Man in the middle (Homme au milieu):**

Le principe de cette attaque est d'intercepter les communications entre deux entités du réseau en se mettant au milieu. Dans les réseaux Wi-Fi, le pirate joue le rôle de relais entre la victime et le point d'accès légitime. Tout le trafic passe ainsi par sa machine avant d'être redirigé vers le réseau, ce qui lui laisse le loisir d'espionner les échanges ainsi que de pouvoir modifier le contenu de ces derniers (voir Figure III-2: L'attaque MitM sur Wi-Fi).

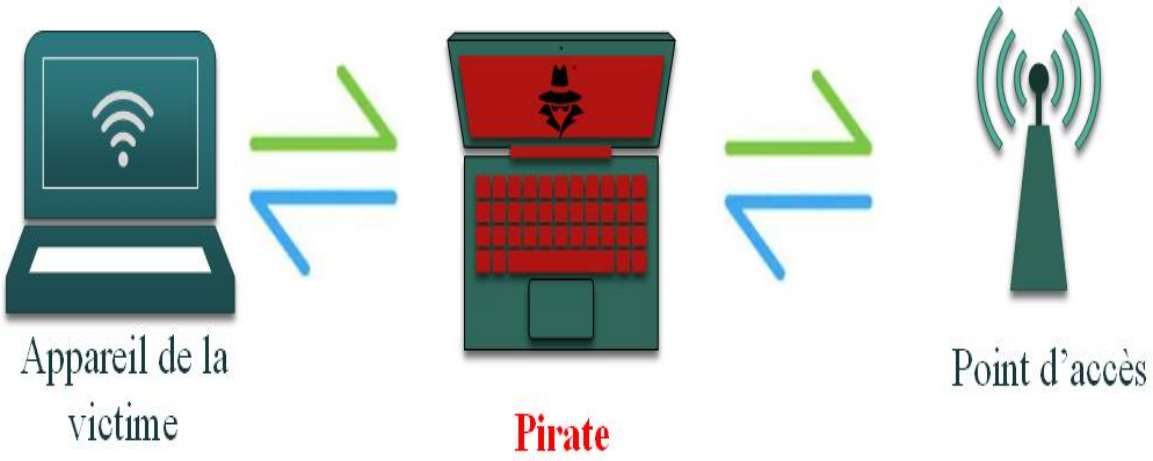

Figure III-2: L'attaque MitM sur Wi-Fi

III.2.2.4. **Wiphisher Evil Twin (Jumeau maléfique) :**

C'est une attaque qui allie la technique de spoofing d'adresse MAC, l'attaque par déni de service, et le social engineering.

Dans un premier temps, le pirate effectue une écoute afin de récolter les informations de L'AP cible. Il crée un point d'accès pirate identique (en usurpant son adresse MAC BSSID et le nom du réseau Wi-Fi SSID) mais non sécurisé.

Après ça, il utilise une attaque DOS (Généralement un flux de désauthentification) sur l'AP légitime afin de forcer la déconnexion des clients et les pousser vers l'AP frauduleux.

Une fois le client connecté, le pirate redirigera ses requêtes web vers un portail fictif préalablement configuré qui demandera à l'utilisateur des informations sensibles (tel que le mot de passe du Wi-Fi légitime) qui seront directement communiquées au pirate. La figure suivante illustre un exemple de portail fictif pouvant être utilisé par un pirate pour le vol d'identifiants.

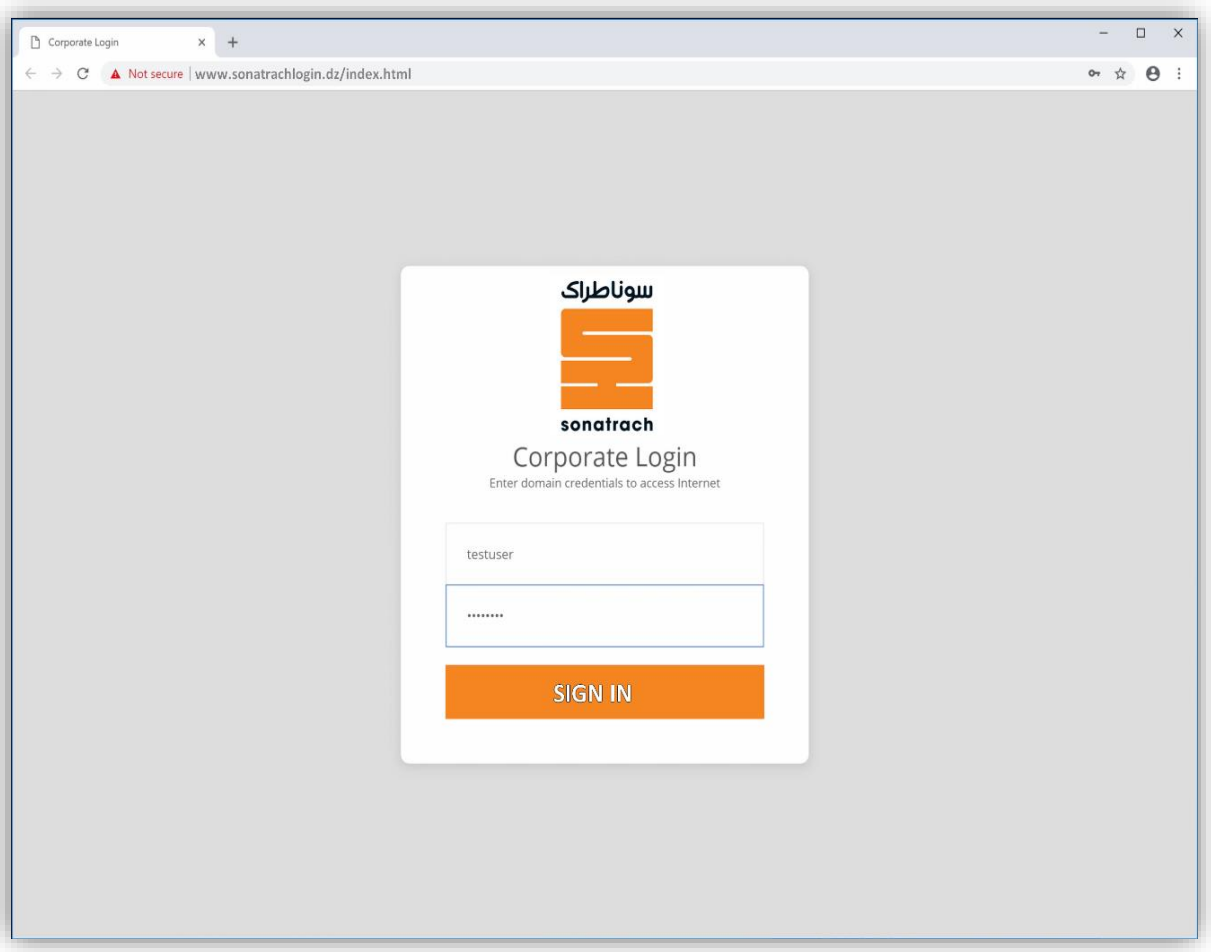

Figure III-3: Exemple de portail captif utilisé dans l'attaque Evil Twin.

III.2.2.5. **Attaques sur la clé chiffrement :**

Le principe de ce genre d'attaque est de déchiffrer la clé de sécurité du réseau Wi-Fi afin de s'y introduire. L'objectif étant de profiter des ressources de celui-ci ou de procéder à d'autres types d'attaques cités précédemment.

a) Attaque par dictionnaire :

Le principe est de tester énormément de mots de passe se trouvant dans un fichier (dictionnaire) les uns après les autres en espérant tomber sur le bon. Il existe une variante en ligne et hors ligne de cette attaque, la deuxième étant beaucoup plus sournoise, car après avoir capturé l'échange de clés crypté, le pirate aura tout le temps hors connexion d'essayer des millions de mots de passe.

b) Attaque statistique :

C'est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé, cette attaque utilise des failles dans les algorithmes de chiffrement assez faible comme RC4 utilisé pour le WEP. Ainsi, si le pirate capture assez de trames transitant par le réseau Wi-Fi, il pourra effectuer une attaque statistique pour calculer la clé.

III.3. Mécanismes préliminaires de sécurité

III.3.1. Limiter les débordements

Une première mesure pour sécuriser les réseaux Wi-Fi consiste à s'assurer que les ondes radio ne débordent pas hors des locaux. Cette protection doit être pensée au moment de la planification en choisissant un positionnement optimal des AP pour que le niveau du signal soit très faible à l'extérieur de l'entreprise.

III.3.2. Masquer le SSID

Par défaut, un réseau Wi-Fi diffuse périodiquement son SSID en clair via les trames balise (beacon). Les périphériques à proximité peuvent ainsi le capter et s'associer avec.

L'utilisation d'un SSID fermé permet d'interdire cette diffusion. La station voulant s'associer devra entrer manuellement le SSID pour se connecter à ce réseau. Toutefois, il s'agit d'une protection très faible, car l'SSID est toujours transmis en clair dans les requêtes d'association. Un pirate effectuant un sniffing peut donc facilement intercepter celui-ci.

III.3.3. Filtrage par adresse MAC

Ce mécanisme consiste à limiter l'accès à un réseau sans-fil a une liste de périphériques. On peut par exemple refuser tous les paquets provenant d'une adresse donnée, ou alors autoriser seulement une liste d'adresses à pouvoir communiquer. Malheureusement, le filtrage par adresse MAC peut être facilement contourné en usurpant l'adresse MAC d'un hôte légitime du réseau cible (Spooffing MAC).

III.3.4. Les VLANs

Les réseaux locaux virtuels (Virtual Local Area Network) permettent la segmentation logique des réseaux dont le but est d'augmenter le niveau de sécurité. Si les APs le permettent, il est bon d'associer le trafic sans-fil à un VLAN particulier. Ainsi les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.

III.3.5. Les ACLs

Une liste de contrôle d'accès est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

- L'adresse d'origine.
- L'adresse de destination.
- Le numéro de port.
- Les protocoles de couches supérieures.

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Elles sont associées à une interface physique ou virtuelle du switch/routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès.

III.4. **Le WEP**

C'est le premier protocole sécuritaire à avoir vu le jour pour la norme 802.11, le but était de sécuriser les échanges radio, afin d'assurer la confidentialité des données.

Il est basé sur l'algorithme RC4, mais est aujourd'hui obsolète, car certaines attaques permettent de casser le chiffrement en moins de 15 min.

III.4.1. **Utilisation de RC4 :**

Dans le cas du WEP, l'algorithme RC4 génère une série de bits pseudo-aléatoire à partir de la clé partagée (PSK) constituée de 40,104 ou 232 bits, concaténés à un vecteur d'initialisation (IV) aléatoire de 24 bits. On l'appellera la clé RC4.

Pour chiffrer un message, on utilise l'opération du OU exclusif (XOR) entre le message en clair et notre clé RC4.

Pour déchiffrer le message crypté, on utilise une fois de plus l'opération XOR entre la clé RC4 et le message crypté.

III.4.2. **Principe de l'authentification :**

- L'authentification commence par une requête d'association du client.
- L'AP envoie une séquence aléatoire de 128 bits appelée challenge.
- Une fois reçu, le client chiffre la séquence avec sa clé RC4 (IV+PSK), et renvoi une trame contenant l'IV utilisé ainsi que le résultat du chiffrement.
- Le point d'accès chiffre la même séquence aléatoire(challenge) avec la clé RC4 (IVclient + PSKap). Il compare le résultat obtenu avec le résultat du client.
- S'il y a correspondance il accepte la demande d'authentification, autrement, il rejette celle-ci.

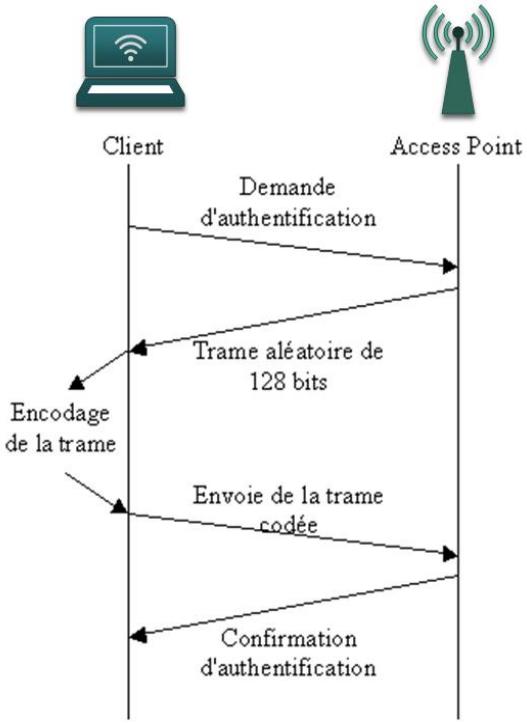

Figure III-4 : Etapes d'authentification WEP.

III.4.3. **Faiblesses du WEP :**

De nombreuses failles ont été trouvés quelques mois seulement après l'apparition du protocole WEP. La principale faiblesse du WEP se trouve au niveau du vecteur d'initialisation. L'IV est un nombre de 24 bits qui est combiné avec la clé PSK pour créer la clé RC4. Un nouveau vecteur est utilisé pour chaque trame émise, or nous n'avons que 2^{24} possibilités. Le réseau émettra donc régulièrement des trames chiffrées avec le même IV.

Sachant que le vecteur d'initialisation est communiqué en clair dans la trame, un pirate peut alors sniffer le réseau Wi-Fi jusqu'à obtenir un bon nombre de trames chiffrées avec le même IV. Un algorithme d'attaque statistique peut alors trouver la clé PSK en quelques secondes.

III.5. **Le WPA**

Devant aux énormes failles contenues dans le WEP, l'IEEE a commencé un programme baptisé IEEE 802.11i, pour définir un standard d'authentification et de chiffrement pour les communications sur des réseaux sans fil. Face aux longs délais de développement de 802.11i, et face à la pression d'un marché fortement demandeur de solutions, une première version a vu le jour. Il s'agit de WPA. En 2004, 802.11i a été finalisé et a pris le nom de WPA2.

III.5.1. **Le WPA-PSK**

Le WPA-PSK aussi appelé WPA personnel a été conçu pour les réseaux individuels et les petites sociétés, il se distingue par rapport à la version d'entreprise au niveau de l'authentification. En effet, ce premier utilise une phrase secrète partagée par tous les utilisateurs pendant que le WPA entreprise utilise une authentification 802.1x.

La phrase secrète peut contenir de 8 à 63 caractères ASCII. Elle sera convertie par la machine via un algorithme de hachage connu en une clé PSK de 256 bits tel que :

PSK = PMK = PBKDF2 (phrase secrète, SSID).

Par la suite, elle servira de clé maîtresse durant la phase d'échange et de dérivation de clé 4-way handshake (Voir §III.5.3).

III.5.2. **Le WPA entreprise**

Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, et d'un contrôleur d'accès.

Chaque client utilisera un nom d'utilisateur et un mot de passe unique, voir des certificats de confiance. Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification.

III.5.2.1. **L'architecture 802.1x :**

Le standard 802.1x utilise un modèle qui s'appuie sur trois entités fonctionnelles :

- **Le système à authentifier (supplicant) :** c'est un client demandant un accès au réseau. Dans le contexte des réseaux Wi-Fi, le système à authentifier n'est autre que le client 802.11.

- **Le contrôleur d'accès (authenticator) :** c'est l'unité qui contrôle et fournit la connexion. Un port contrôlé par cette unité peut avoir deux états : non autorisé ou autorisé. Par défaut, le trafic est autorisé sur le port du contrôleur d'accès, mais uniquement en direction du serveur d'authentification. Dans le contexte d'un réseau Wi-Fi, selon l'architecture utilisée, le contrôleur d'accès peut être soit un AP autonome, soit un contrôleur Wi-Fi.
- **Le serveur d'authentification (Authentication Server) :** ses capacités sont résumées par l'acronyme AAA qui lui est souvent associé. Cette expression exprime les trois fonctions prises en charge : identification et authentification (Authentication), gestion des autorisations d'accès (Authorization) et comptabilisation des connexions (Accounting). Le serveur généralement utilisé est RADIUS.

L'authentification repose sur deux protocoles : EAP et RADIUS.

III.5.2.2. **Les mécanismes d'authentification EAP :**

Le protocole Extended Authentication Protocol sert pour le transport entre le supplicant et l'authenticator des données nécessaires à l'authentification.

Les principales procédures d'authentification utilisées par EAP sont :

- **EAP-MD5 :**

Cette version est la moins sûre d'EAP, authentification simple via le nom d'utilisateur + le mot de passe haché avec la fonction MD5.

- **EAP-TLS :**

C'est la version la plus fiable d'EAP. Elle s'appuie sur le protocole TLS qui utilise une infrastructure à clés publiques pour sécuriser les communications d'identification entre les clients et le serveur.

Concrètement, deux certificats sont utilisés (un côté serveur et un autre côté client) pour la création d'un tunnel sécurisé, qui permettra ensuite la distribution des clés de chiffrement. Ce qui veut dire que même si le mot de passe est découvert, il ne servira à rien sans le certificat client.

Le seul inconvénient de cette version est l'obligation de disposer d'un certificat client unique pour chaque poste. Pour une entreprise disposant d'un grand parc de machines, il peut s'avérer difficile et assez coûteux de gérer un certificat par machine.

- **EAP-TTLS :**

Version allégée de TLS, elle utilise des certificats uniquement côté serveur, celui côté client étant optionnel. Elle permet n'importe quelle méthode d'authentification au sein du tunnel TLS. Offre un très bon niveau de sécurité, mais n'est pas présent sur les systèmes Microsoft et Cisco.

- **PEAP :**

Le Protected EAP utilise un certificat uniquement côté serveur et un chiffrement asymétrique pour créer un tunnel TLS sécurisé. Ce tunnel véhiculera une autre méthode d'authentification EAP plus simple (MD5 par exemple).

Cette méthode présente l'avantage d'être installée nativement sur la plupart des systèmes, simple à mettre en œuvre, tout en offrant un niveau de sécurité très important.

III.5.2.3. **Le Protocole RADIUS**

Le protocole RADIUS est utilisé entre le contrôleur d'accès et le serveur d'authentification, il utilise une clé partagée entre les deux entités appelée Shared-Secret pour chiffrer le trafic et communique via UDP.

Pour l'authentification, il y a quatre types de paquets :

- **Access-Request** : envoyé par le contrôleur d'accès, contenant les informations sur le client (login/mot de passe, ...).
- **Access-Challenge** : envoyé par le serveur pour demander des informations complémentaires, et donc la réémission d'un paquet Access-Request.
- **Access-Accept** : envoyé par le serveur dans le cas où l'authentification est un succès.
- **Access-Reject** : envoyé par le serveur dans le cas où l'authentification est un échec.

La figure III-7 illustre le processus complet d'authentification 802.1x dans le cas d'une architecture centralisée par contrôleur Wi-Fi.

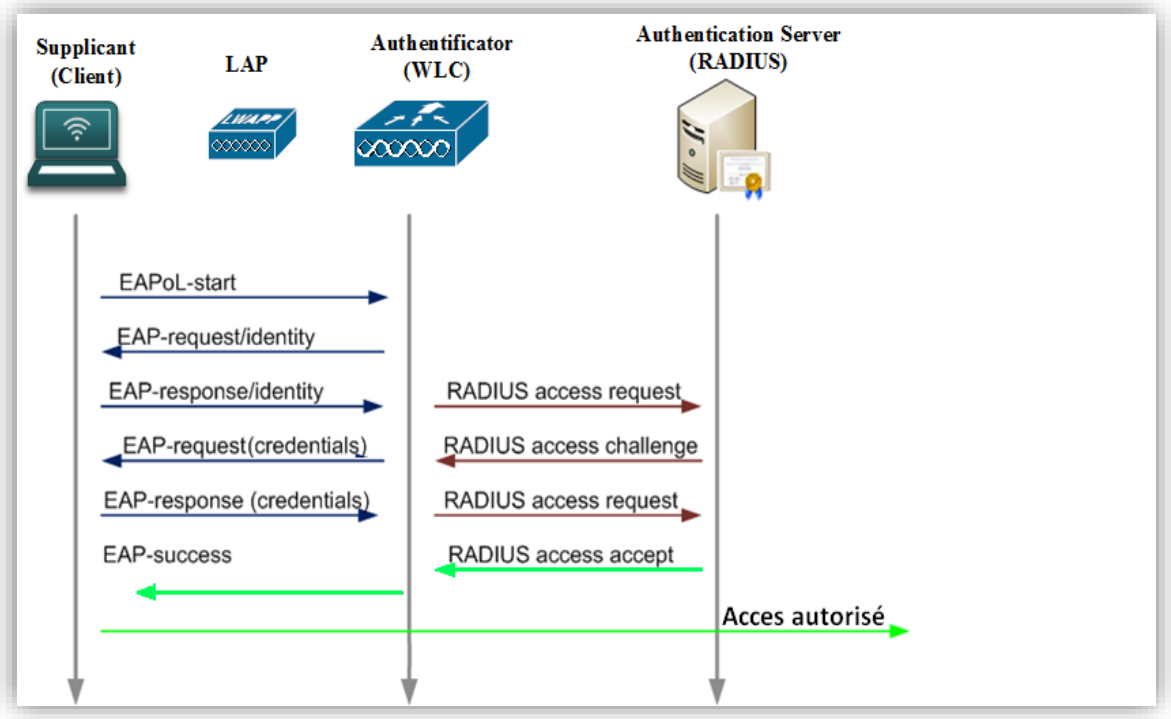

Figure III-5: L'authentification 802.1x EAP.

Remarque :

Après une authentification 802.1x réussie, Une clé maitresse PMK est calculée et échangée entre le supplicant et le serveur d'authentification par le biais d'un canal sécurisé, établi en fonction de la méthode d'authentification EAP utilisée.

Comme pour le WPA personnel, cette clé maitresse sera utilisée durant la phase de dérivation de clés 4-way handshake.

III.5.3. **Le 4-way Handshake**

Le WPA utilise des clés de chiffrement différentes pour chaque paquet transmis sur le réseau, on en déduit aisément que ce n'est pas la clé maîtresse qui sera directement utilisée.

En effet, il existe un système de dérivation de clé appelé 4-Way Handshake initialisé à chaque demande d'association, qui se chargera de l'échange et du calcul des clés temporaires de sessions.

Quand un client se connecte sur un AP, il y a un échange de 4 messages grâce auxquels l'échange et l'installation de clés à lieu :

[**message 1**] : le point d'accès envoie une séquence aléatoire en clair appelée ANonce, ainsi que son adresse MAC au client.

Après la réception, le client génère à son tour une séquence aléatoire appelée SNonce.

Il peut maintenant calculer la clé temporaire de session PTK via une fonction de hachage qui aura comme arguments :

- La PMK.
- AP MAC adresse.
- Client MAC adresse.
- ANonce.
- SNonce.

[**message 2**] : le client envoie ensuite le SNonce en clair à L'AP, ainsi qu'un code d'intégrité MIC calculé à partir de la PTK.

L'AP reçoit le SNonce et l'utilise pour calculer sa PTK.

Grâce au MIC du client, L'AP est en mesure de vérifier si le client connaît la PMK et a correctement dérivé la PTK.

[**message 3**] : si la vérification est un succès, l'AP envoie un accusé de réception au client, et lui demande d'installer sa clé PTK.

[**message 4**] : le client installe sa PTK et notifie le point d'accès que l'échange de données peut commencer.

Nous avons maintenant une clé temporaire commune PTK qui servira à chiffrer la suite des communications durant toute la session.

La figure suivante illustre les étapes de ce processus.

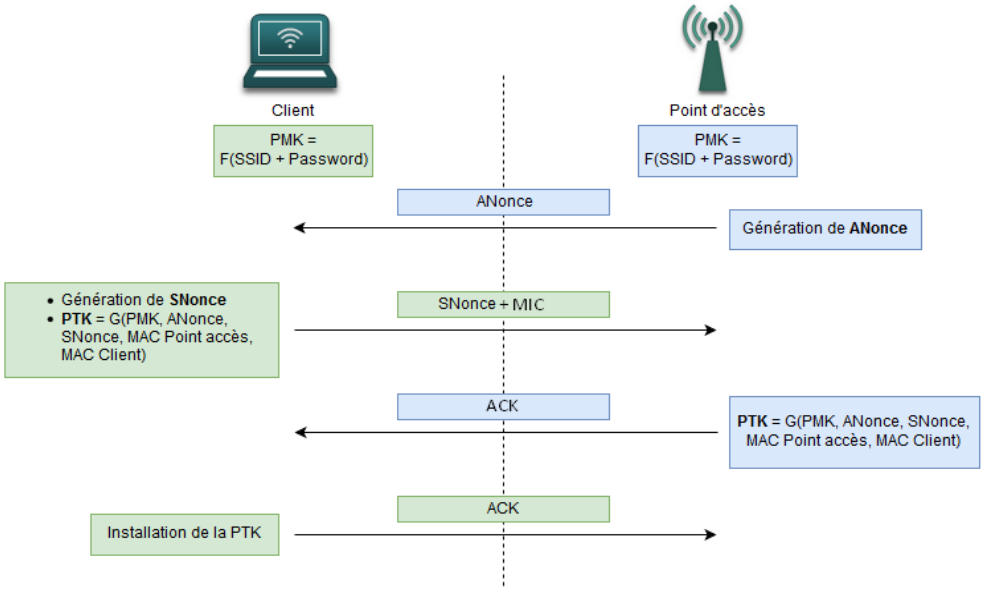

Figure III-6: Le processus d'authentification 4-way Handshake.

À noter qu'au début de chaque 4-way Handshake, un compteur PN (packet number) est initialisé. Il sera ensuite incrémenté à chaque échange, et sera utilisé dans le vecteur d'initialisation lors du chiffrement des communications, garantissant ainsi l'unicité de chaque chiffrement de paquet.

Remarque :

La clé temporaire de chiffrement PTK est utilisée pour chiffrer le trafic Unicast. Il y aura en parallèle l'échange d'une clé de temporaire de groupe GTK, pour chiffrer le trafic Multicast et Broadcast.

III.5.4. **Chiffrement et intégrité**

Toutes les clés générées précédemment seront utilisées dans les protocoles de chiffrements intégrés au WPA.

III.5.4.1. **WPA TKIP**

Il est venu pour combler les faiblesses du WEP, c'est en fait une mise à jour de celui-ci, ce qui présente l'avantage de compatibilité avec le matériel existant.

TKIP utilise lui aussi le chiffrement RC4, mais d'une manière beaucoup plus robuste :

- Vecteur d'initialisation de 48 bits, ce qui permet d'éviter complètement la réutilisation des clés.
- La clé de cryptage change à chaque paquet.
- Vérification de l'intégrité des données à l'aide d'un champ appelé Message Integrity Code. Chaque partie peut ainsi vérifier que le contenu d'un paquet n'a pas été modifié pendant son transfert.

III.5.4.2. **WPA 2 CCMP**

CCMP est un protocole basé sur l'algorithme AES, qui est considéré comme étant le plus sûr et le plus utilisé des algorithmes de chiffrement (il est notamment utilisé au niveau gouvernemental.). Ce changement marque une rupture de compatibilité avec le matériel existant, en grande partie parce que les calculs de chiffrement nécessitent beaucoup plus de puissance que ceux de RC4.

Le protocole CCMP assure entre autres :

- Le mécanisme de roulement des clés de chiffrement pour chaque paquet.
- Un chiffrement de type AES par bloc de 128bits.
- Un algorithme de contrôle d'intégrité CBC.

III.5.5. **Vulnérabilité du WPA**

La faille la plus exploitable est une attaque de type dictionnaire contre la clé PSK utilisée dans le 4-way Handshake.

Pour effectuer cette attaque, le pirate devra soit sniffer passivement les échanges de trames dans le réseau en attendant qu'un client s'authentifie, soit utiliser l'attaque de désauthentification sur un client déjà connecté (voir §III.2.2.2). Une fois les deux premiers messages du Hanshake capturés, le pirate connaît le ANonce (en clair dans le 1er message) et le SNonce (en clair dans le 2ème message). Il pourra ainsi calculer des PTK à partir des PSK contenues dans un fichier dictionnaire.

Si la PSK choisie correspond, le code MIC du second message peut être obtenu avec la PTK correspondante. Sinon, une autre PSK doit être testée.

Le mot de passe exact doit se trouver dans le dictionnaire, sinon l'attaque échouera. Voilà pourquoi il est conseillé d'utiliser de longues combinaisons aléatoires.

III.6. **Conclusion**

Dans ce chapitre, nous sommes partis d'une vue globale sur la sécurité informatique.

Nous avons expliqué quelques attaques capables de porter atteinte à celle d'un réseau Wi-Fi, avant de donner les mécanismes, ainsi que les dispositifs de sécurité qu'on peut envisager de mettre en place dans différents contextes. En détaillant chaque protocole de sécurité, nous connaissons maintenant les avantages et les inconvénients de chacun.

Nous pouvons à présent choisir quelles solutions adoptées et mettre en œuvre dans la suite de notre travail pour sécuriser efficacement un réseau d'entreprise.

CHAPITRE IV

Organisme d’accueil

IV. Organisme d'accueil

Introduction

Afin d'améliorer nos connaissances dans le domaine des réseaux, il est indispensable de développer nos capacités professionnelles. Pour cela, nous avons suivi un stage pratique au centre informatique de l'entreprise SONATRACH de Béjaïa (RTC) que nous allons vous présenter ci-dessous.

Ce chapitre constitue pour nous l'une des parties essentielles de notre étude qui consiste à analyser les éléments qui composent la base du réseau local de l'entreprise.

IV.1. Présentation de l'organisme d'accueil

IV.1.1. Présentation de SONATRACH

SONATRACH est une entreprise publique algérienne et un acteur majeur de l'industrie pétrolière. C'est une compagnie nationale d'envergure internationale, c'est la clé de voûte de l'économie algérienne. Le groupe pétrolier et gazier SONATRACH intervient dans l'exploration, la production, le transport par canalisation, la transformation et la commercialisation des hydrocarbures et de leurs dérivés.

IV.1.1.1. Historique et missions

L'entreprise SONATRACH a été créé le 31 décembre 1963 par le décret n°63/491, les statuts ont été modifiés par le décret n°66/292 du 22 septembre 1966, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures», cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, de ces principes SONATRACH a donné naissance à 17 entreprises : (NAFTAL, ENIP, ENAC,..., etc.).

Les activités de base de SONATRACH furent fixées en 1992, afin d'atteindre ses objectifs en :

- L'exploitation et la recherche.
- L'exploitation des gisements d'hydrocarbures.
- La liquéfaction et la transformation du gaz.
- Le transport par canalisation.
- La commercialisation.

Pour la réalisation de ces objectifs, l'entreprise est divisée en 5 branches représentées dans la figure suivante :

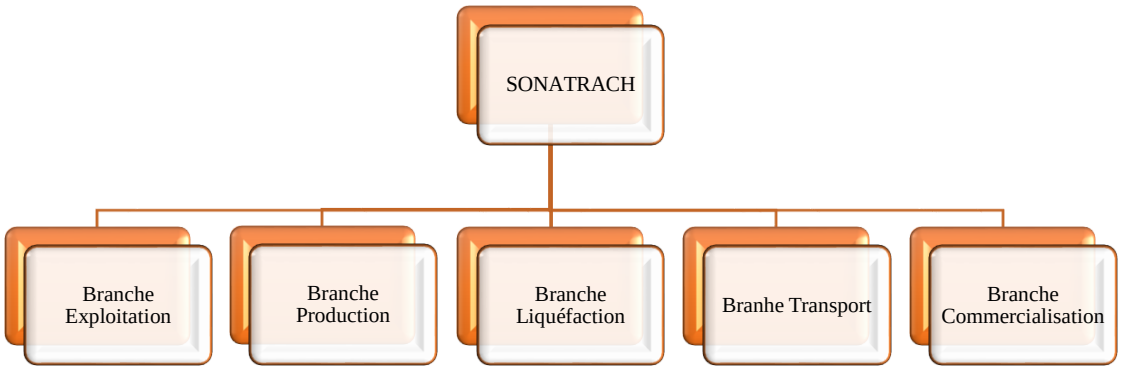

Figure IV-1: Organigramme de la SONATRACH en Algérie.

À travers cette transformation structurelle et fractionnelle, un schéma de groupes a évolué en constituant des branches d'activités autonomes et leurs filiations. Dans la branche « activité de transport par canalisation » se trouve la Direction Régionale de Béjaïa (DRGB) où s'est déroulé notre stage pratique.

IV.1.2. **Activité de la branche transport par canalisation (TRC)**

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation.

Les missions affectées à la branche transport par canalisation sont :

- La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures.
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.
- La maintenance, l'entretien et la protection des ouvrages et canalisation.
- L'exécution des révisions générales, des machines tournantes et équipements.
- Les installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement.
- La conduite des études, la réalisation et la gestion des projets de développement des ouvrages et canalisations.
- Gère l'interface transport des projets internationaux du groupe ou en partenariat.

IV.1.2.1. **Organigramme TRC :**

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

- La direction régionale Est (Skikda).
- La direction régionale Centre (Béjaïa).

- La direction régionale Ouest (Arzew).
- La direction régionale de Haoud-EL-Hamra.
- La direction régionale d'Ain Amenas.

IV.1.3. **Présentation de la direction régionale de transport de Béjaïa (DRGB)**

La DRGB est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (TRC). Elle a pour mission de transporter, stocker et livrer les hydrocarbures liquides et gazeux. Elle est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

IV.1.4. **Structure de la DRGB**

La direction régionale de Béjaïa comporte plusieurs constituants illustrés dans l'organigramme ci-dessous :

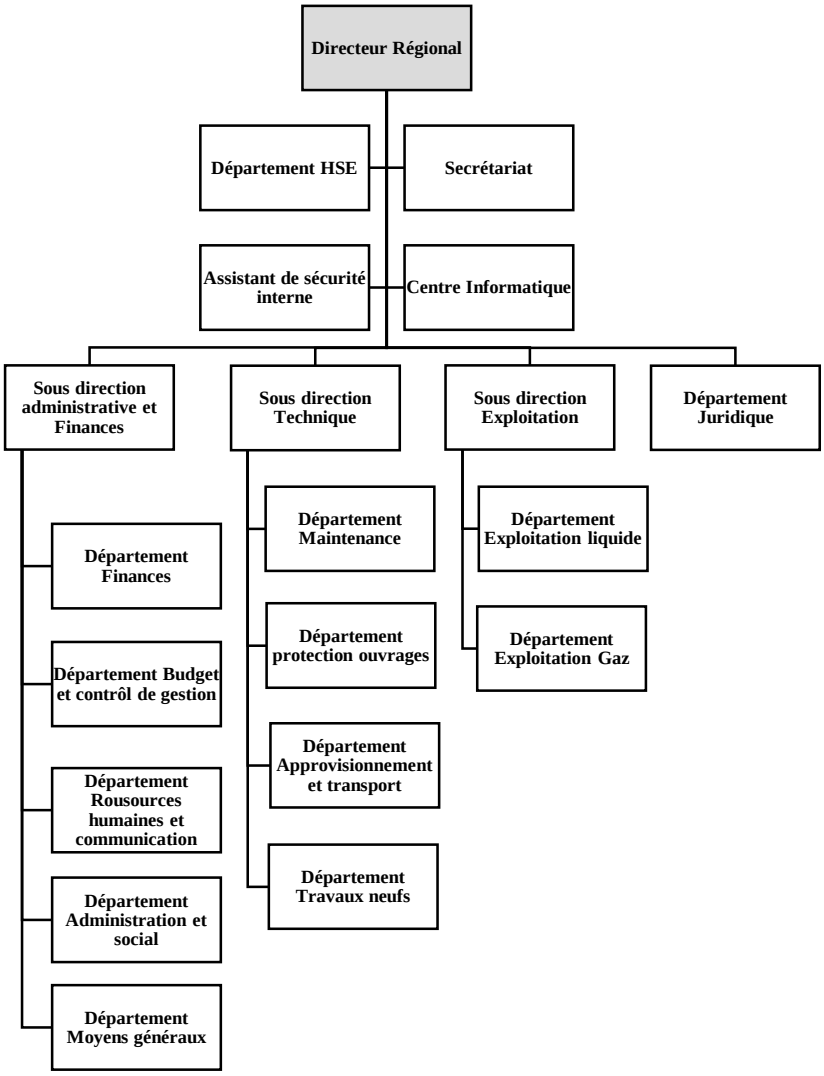

Figure IV-2: Structure de la DRGB

IV.1.4.1. **Définition des services**

- **Direction régionale** : elle est dirigée par un directeur régional aidé par des assistants et un secrétariat.
- **Assistant de sécurité interne** : sa mission est de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.
- **Centre informatique** : il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.
- **Sous-direction technique** : elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements : département maintenance, département protection des ouvrages, département approvisionnement et transport et département des travaux neufs.
- **Sous-direction exploitation** : elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements : le département exploitation liquide et le département exploitation gaz.
- **Sous-direction administrative et finances** : elle a pour mission la gestion des ressources humaines et les moyens généraux, ainsi que d'effectuer la gestion financière, le budget et le contrôle de gestion. Elle est organisée en 5 départements : département administration et social, département ressources humaines et communication, département moyens généraux, département finances, département budget et contrôle de gestion.
- **Département juridique** : prendre en charge les affaires juridiques de la DRGB.

IV.1.5. **Présentation du centre informatique**

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte de la direction régionale de Béjaïa (DRGB) et des autres régions.

IV.1.5.1. **Organisation structurelle**

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.

Le centre informatique se constitue de 3 services gérés par un chef de centre. Ces derniers sont illustrés dans le diagramme suivant :

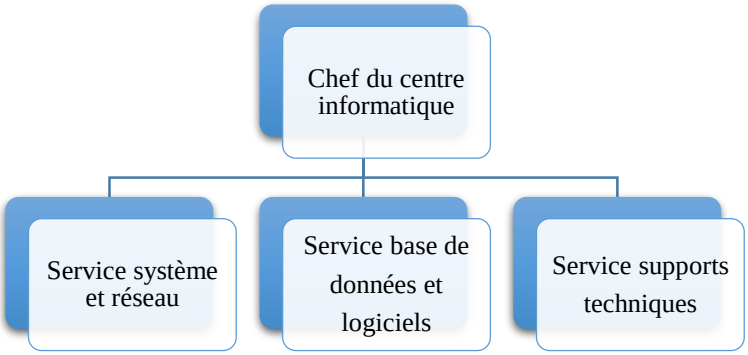

Figure IV-3: Organigramme du centre informatique

IV.1.5.2. **Organisation fonctionnelle**

Chaque service a une mission spécifique, nous allons définir et citer les différentes tâches de chacun ci-dessous :

- **Service système et réseaux**
  - **Système :**
    - Choix des équipements informatique et logiciel de base.
    - Mise en œuvre des solutions matérielles et logicielles retenues.
    - Installation et configuration des systèmes.
    - Orientation des travaux de l'équipe de développement avec une bonne utilisation des ressources de l'ordinateur.
    - Mise en œuvre des nouvelles versions de logiciels.

  - **Réseau :**
    - Assurer le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organise l'évolution de sa structure.
    - Conduite de l'étude pour le choix de l'architecture du réseau à installer.
    - Participation à la mise en place des réseaux.
    - Définition des droits d'accès à l'utilisation du réseau.
    - Assurer la surveillance permanente pour détecter et prévenir les pannes.
    - Traitement des dysfonctionnements et incidents survenant sur le réseau.

- **Service base de données et logiciels :**
  - **Base de données :**
    - Conception des bases de données, optimisation et gestion des données informatiques.
    - Installation, configuration et exploitation du SGBD et de ses bases.
    - Mise en œuvre et gestion des procédures de sécurité (accès, intégrité).
    - Gestion de la sauvegarde, de la restauration et de la migration des données.
    - Assurer la cohérence et la qualité des données introduites par les utilisateurs.

  - **Logiciels :**
    - Etude et conception des systèmes d'information.
    - Développement et maintenance de l'application informatique pour TRC.

- Déploiement des applications et formation des utilisateurs.

- **Service supports techniques :**
  - Assistance aux utilisateurs en cas de problèmes software et hardware.
  - Installation des logiciels, technique et bureautique.
  - Formation aux nouveaux produits installés.

IV.2. **Réseau informatique de l'entreprise**

IV.2.1. **Principales technologies utilisées**

IV.2.1.1. **Contrôleur de domaine**

Un contrôleur de domaine est un serveur informatique hébergeant l'annuaire Active Directory.

La RTC dispose de deux serveurs contrôleurs de domaine : un serveur principal et un autre secondaire qui s'active en cas de saturation ou de panne de serveur principal. Les deux serveurs sont des machines DELL Power Edge 2800 sous le système Windows 2003 Server Entreprise Edition 32x.

Dans ses contrôleurs de domaines, on a hébergé :

- Un annuaire Active Directory.
- Un DNS.
- Un serveur DHCP.
- Et on a défini des stratégies de groupes.

IV.2.1.2. **Active directory**

Active Directory est un service d'annuaire de type LDAP créé par Microsoft et destiné à être installé sur les systèmes d'exploitation Windows Server. Son objectif principal est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs.

Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations.

Chez la RTC, chaque utilisateur possède un compte présenté par un nom d'utilisateur et un mot de passe.

IV.2.1.3. **DNS**

Le Domain Name System (ou DNS, système de noms de domaines) est un service permettant d'associer un nom à une adresse IP, plus simple à retenir, appelé nom de domaine. Et plus généralement, de trouver une information à partir d'un nom de domaine.

DNS est un service indispensable pour le bon fonctionnement de toute l'architecture Active Directory, localisation des contrôleurs de domaine, réplication, etc.

Le nom domaine correspondant à la RTC est RTC_TRC.SH.

IV.2.1.4. **DHCP**

Le serveur DHCP permet d'attribuer des adresses IP dynamiques à station, et ainsi de pallier les ennuis d'une gestion rigoureuse de ces adressages. Le serveur DHCP permet alors d'éviter les conflits d'adresses et donc les problèmes sur le réseau.

IV.2.1.5. **Les stratégies de groupes**

Les stratégies de groupe ou GPO sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Cela inclut la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté.

Les utilisateurs enregistrés dans l'Active Directory de la RTC appartiennent à des groupes selon la hiérarchie de l'organisation (département de travail), leurs droits d'accès aux fichiers et aux applications distribuées, et selon d'autres privilèges définis (accès à Internet…, etc.).

Par exemple, le compte d'un utilisateur est programmé pour ne pouvoir accéder qu'aux applications dont il a besoin, et aux partitions partagées qui le concernent, en fonction son département.

IV.2.1.6. **Serveur de messagerie**

- **Définition**

C'est un logiciel serveur qui a pour vocation de transférer les messages électroniques entre clients. Il est utilisé pour maintenir les boîtes aux lettres et conserver une trace de tous les messages échangés entre ses clients.

- **Mise en œuvre chez RTC**

La solution adoptée par RTC est Microsoft exchange server 2004. Chaque employé enregistré dans l'annuaire Active Directory possède un compte de messagerie et peut échanger

des messages avec les autres utilisateurs, ou bien partager des messages publics dans des dossiers partagés. La taille maximale autorisée par utilisateur est de 250 Mo.

IV.2.1.7. **Serveur antivirus**

- **Définition**

Un serveur antivirus est serveur qui a pour rôle protéger le réseau contre les virus et d'autres menaces, empêcher les machines infectées de propager leurs virus sur le reste du réseau. Ce serveur doit fonctionner de manière transparente en tâche de fond pour empêcher les ralentissements du réseau, la baisse de productivité et les menaces sur les données confidentielles.

- **Mise en œuvre chez RTC**

La solution adoptée par RTC est F-Secure v9 qui intègre une fonctionnalité antispyware pour protéger les serveurs de fichiers et de stockage. Ce serveur permet de programmer des analyses et des mises à jour, visualiser l'état de chaque machine et permettre d'effectuer les mises à jour téléchargées par le serveur localement.

IV.2.1.8. **HSRP**

- **Définition**

Dans un réseau local, utiliser un seul switch fédérateur pour acheminer le trafic à travers tous les sous-réseaux est une idée peu ingénieuse, car si ce switch tombe en panne, c'est tout le réseau qui est hors-service. Pour remédier à ce problème, il est plus judicieux de placer un autre (voir plusieurs) switch dans le réseau pour qu'il se charge de router les données si le principal est endommagé. L'un des protocoles qui permet d'assurer cette redondance est le HSRP, il est implémenté nativement sur les équipements CISCO, mais n'est pas activé par défaut.

- **Principe de fonctionnement**

Tous les switchs fédérateurs émulent une adresse IP virtuelle qui sera utilisée comme passerelle par les équipements du réseau LAN, mais ces équipements n'utilisent que la passerelle du switch actif (car les autres sont en mode standby « en attente ou en mode veille »). Pour cela, sur chacun des switchs fédérateurs dois être configuré le protocole HSRP, mais avec des niveaux de priorités différents. Celui qui disposera du plus grand se verra élu et sera actif. Les autres seront passifs jusqu'à ce que le switch principal tombe en panne. C'est à ce moment-là que le switch disposant du niveau de priorité 2 prendra le relais et ainsi de suite (s'il y a encore d'autres routeurs disposant du protocole HSRP).

IV.2.2. **L'architecture réseau de l'entreprise**

IV.2.2.1. **Architecture physique du réseau**

L'entreprise SONATRACH RTC de Béjaïa utilise principalement des équipements de marque CISCO. Ils sont réputés pour leurs fiabilités et leurs performances ainsi que la disponibilité de la main-d'œuvre qualifiée, ceci permet d'éviter des formations coûteuses pour l'entreprise. Ses équipements sont répartis sur les deux infrastructures.

Le LAN de la RTC se divise en effet en deux réseaux interconnectés :

- Le réseau de l'ancien bâtiment : il a une topologie hybride imposée par l'architecture de l'immeuble.
- Le réseau du nouveau bâtiment : il a une topologie en étoile.

Ancien bâtiment :

La commutation est articulée autour de deux niveaux :

- Un niveau accès et distribution. À ce niveau-là, les équipements utilisés sont : des Switchs simples Catalyst 2950/2960 ainsi que des Switchs multicouches Catalyst 3550.
- Un niveau nommé Core (ou noyau), avec deux Switchs fédérateurs multicouches Catalyst 6509 plus performants que les 3550, pour amortir la charge liée aux différentes sollicitations des serveurs (messagerie, antivirus, DHCP, DNS…, etc.).

La redondance est assurée grâce au protocole HSRP.

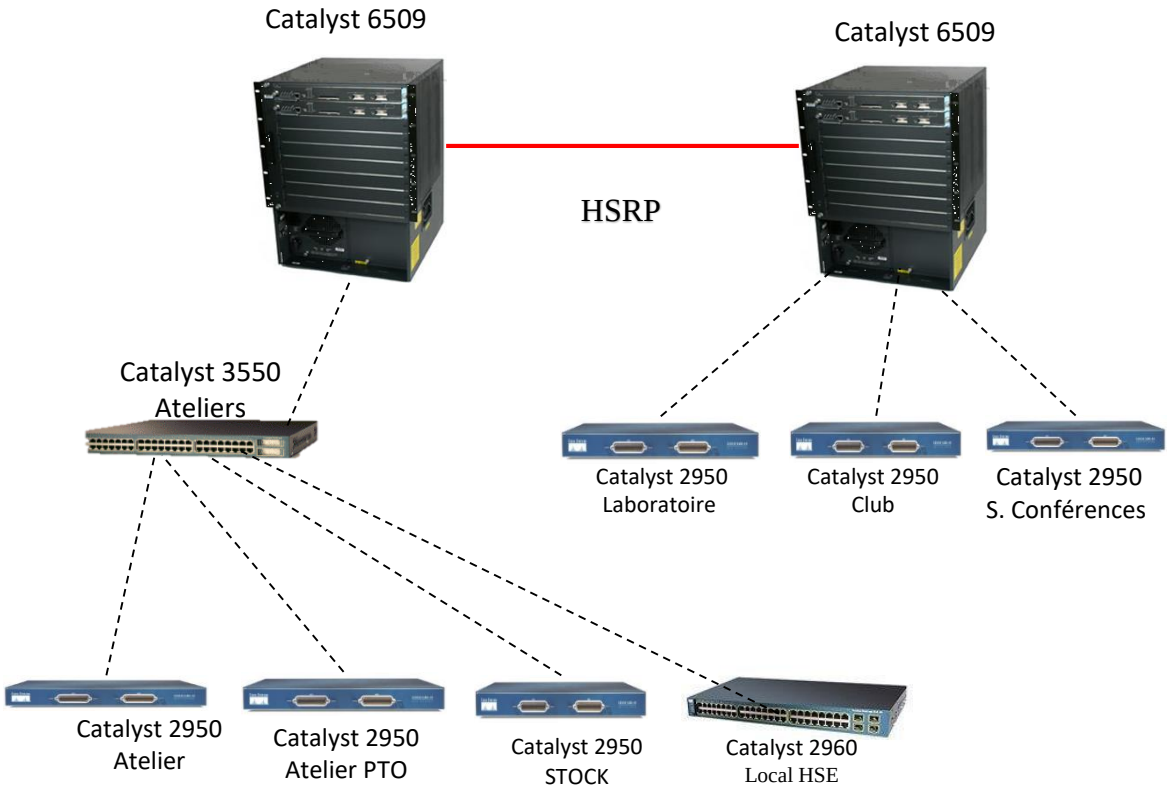

Figure IV-4: La hiérarchie réseau de l'ancien bâtiment

Nouveau bâtiment :

La commutation est articulée autour de deux niveaux :

- Un niveau accès et distribution. À ce niveau-là, les équipements utilisés sont des Switch multicouches 3750 (moins performants que les 6509).
- Un niveau Core, avec deux switchs fédérateurs multicouches Catalyst 6509.

Les deux switchs fédérateurs sont configurés pour une redondance par câble contrairement à ceux de l'ancien bâtiment.

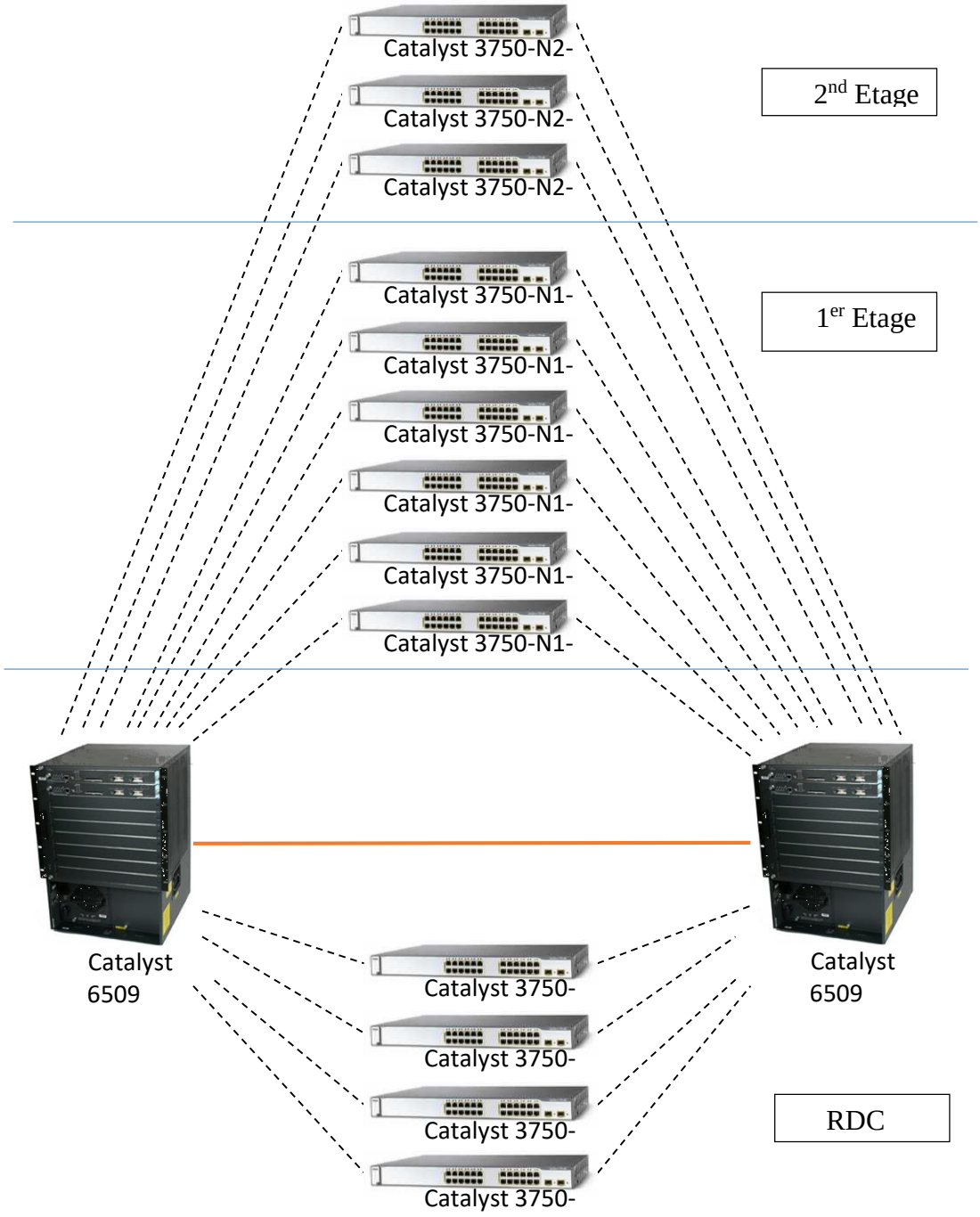

Figure IV-5 La hiérarchie réseau du nouveau bâtiment

Les switchs fédérateurs de l'ancien et du nouveau bâtiment sont reliés entre eux via une fibre optique, pour former l'intranet de l'entreprise.

IV.2.2.2. **Architecture logique du réseau**

Pour faciliter la gestion du réseau, l'entreprise utilise une segmentation de ce dernier en plusieurs VLANs dont chacun est assigné en fonction du port et par service comme représenté dans le tableau ci-dessous. Concernant l'adressage IP, le serveur DHCP assignera chaque utilisateur à un sous-réseau particulier selon le VLAN d'appartenance.

Pour des raisons de sécurité exigées par l'entreprise, on ne va pas divulguer le vrai adressage.

Vlan	Description	Adresse IP	Passerelle
2	Direction	192.168.2.0/24	192.168.2.254
3	Informatique	192.168.3.0/24	192.168.3.254
4	HSE	192.168.4.0/24	192.168.4.254
5	Sûreté interne	192.168.5.0/24	192.168.5.254
6	Sous-direction exploitation	192.168.6.0/24	192.168.6.254
7	Sous-direction technique	192.168.7.0/24	192.168.7.254
8	Sous-direction administrative	192.168.8.0/24	192.168.8.254
9	Sous-direction finance et juridique	192.168.9.0/24	192.168.9.254
10	Les serveurs (DC, EXCH, patte Juniper)	192.168.10.0/24	192.168.10.254
11	Les serveurs base de données	192.168.11.0/24	192.168.11.254
12	Salles (Conférence, formation, technique)	192.168.12.0/24	192.168.12.254
13	WAN	192.168.13.0/24	192.168.13.254
14	Internet	IP Public	--
20	Manager	172.17.0.0/24	172.17.0.254

Tableau IV-1 : Les VLANs et l'adressage IP de l'entreprise.

IV.3. **Problématique et solutions proposées**

IV.3.1. **Critique du réseau et problématique**

Après l'étude de l'architecture réseau de la DRGB, on constate que l'entreprise utilise exclusivement un réseau filaire. Ce qui peut pénalisant de multiples manières :

- Les câbles subissent des dommages répétitifs pour maintes raisons (climatiques ou bien humaines) engendrant des frais additionnels pour les réparations, et un retard sur le travail des employés concernés par la panne.
- L'installation de nouvelles machines requiert l'achat de câble supplémentaire, voir un réaménagement de l'infrastructure.
- Un réseau filaire impose une contrainte importante de mobilité. Cette dernière étant devenue un véritable enjeu au cœur de l'espace de travail, les employés ne pouvant pas bénéficier d'un accès réseau hors de leurs bureaux verront leur productivité fortement limitée, et ainsi celle de l'entreprise.

Enfin, on déplore l'absence d'un accès réseau pour visiteurs, pouvant être utile pour les stagiaires, les invités, ou les collaborateurs de l'entreprise.

IV.3.2. **Les solutions proposées**

Afin de pallier ces différents manques, notre proposition est de passer au sans fil avec l'implémentation d'un réseau Wi-Fi au sein de l'entreprise. L'intérêt étant la compatibilité avec le réseau flaire existant, garantissant une grande souplesse sur la topologie du réseau.

IV.3.2.1. **Architecture du réseau Wi-Fi**

Après l'étude et la comparaison de différentes architectures, celle que nous pensons être optimale est une architecture centralisée avec point d'accès léger et un contrôleur Wi-Fi

Point d'accès léger :

On parle de « Lightweight access point » car assurant uniquement les fonctions de base sans fil :

- Couche physique (DSSS, OFDM, MIMO, …).
- Une partie de la couche liaison :
  - CSMA/CA.
  - Balises de signalisation (beacons).
  - Chiffrement de niveau 2.
  - Encapsulation/décapsulation, fragmentation.

Les fonctions avancées de la couche liaison sont déportées au contrôleur.

Contrôleur Wi-Fi :

C'est le cerveau de notre architecture :

- Il pilote les points d'accès (politiques de sécurité, gestion des fréquences radio, Qos…).

- Il gère la mobilité, notamment les handovers.
- Il définit la configuration applicable aux LWAP (SSID, VLAN, norme 802.11 utilisée…).

Avantages de cette architecture :

- Facilité d'administration.
- Système intelligent de détection et d'évitement des interférences entre les AP, en adaptant les bandes de fréquences, et la puissance d'émission.
- Possibilité de détection des points d'accès pirates qui ne font pas partie de l'ESS légitime.

IV.3.2.2. **Détails de notre solution**

Notre solution se basera sur l'émission par chaque AP de deux SSID distincts :

- **SSID ENTREPRISE :**

C'est le réseau dédié aux employés de l'entreprise, il permettra d'accéder à distance aux différentes ressources et applications de l'entreprise, répondant ainsi aux besoins de connectivité et de confort de chacun.

La sécurité de ce réseau sera assurée via le WPA entreprise. Nous mettrons donc en place une architecture 802.1x (voir Figure III-5), avec un serveur AAA de type RADIUS, et une méthode d'authentification PEAP.

Chaque employé aura son propre nom d'utilisateur et mot de passe stockés dans le serveur RADIUS, ce qui permettra une gestion dynamique des identifiants et des droits de chacun.

Le chiffrement des données se fera grâce au protocole CCMP-AES.

- **SSID VISITEUR :**

C'est un second réseau émis en parallèle du réseau principal. L'avantage ici est de pouvoir mettre à disposition un accès à Internet sans pour autant compromettre la sécurité du réseau principal de l'entreprise.

Que les visiteurs soient dans le cadre d'un stage, ou dans le cadre professionnel (clients, partenaires, fournisseurs). Ce réseau leur fournira un moyen de communication électronique efficace.

La sécurité de ce réseau sera apportée via le protocole WPA-2 Personnel. Tous les visiteurs partageront le même mot de passe, qui devra être régulièrement changé afin de prévenir tout risque de sécurité. Le chiffrement des données sera assuré grâce au protocole CCMP-AES.

Nous utiliserons également une segmentation virtuelle du réseau par VLAN. Ainsi, chaque SSID sera acheminé dans un VLAN différent afin de réduire les domaines de diffusions, et d'assurer une sécurité supplémentaire.

Le protocole DHCP se chargera d'attribuer des adresses IP dynamiquement sur des sous-réseaux définis en fonction du VLAN.

Le fait d'être connecté au réseau ne doit pas impliquer que toutes les données soient accessibles. Nous utiliserons les listes de contrôle d'accès afin d'autoriser ou d'interdire le transit de certains paquets.

CHAPITRE V

Planification & Réalisation

V. Planification & Réalisation

Introduction

Ce chapitre consistera en la réalisation de notre projet avec les solutions proposées précédemment. Nous exposerons les différentes configurations nécessaires à implémenter sur le LAN, en se basant sur le simulateur Cisco Packet Tracer.

Pour présenter les configurations que nous avons réalisées, nous nous sommes servi des captures d'écran qui illustrent les étapes de la configuration.

V.1. Présentation du simulateur Cisco Packet Tracer 7.2.1

Packet tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel. Il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques.

L'objectif principal de simulateur, est de schématiser, configurer et de voir toutes les possibilités d'une future mise en œuvre réseau.

Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituants un réseau informatique.

V.2. Architecture de mise en œuvre

Afin de configurer le nouveau réseau local de SONATRACH, nous l'avons simulé sous Cisco Packet tracer. Nous nous sommes contentés de la partie en relation avec le réseau sans-fil vu que le reste du réseau filaire ne sera pas impacté.

La figure V-1 montre la topologie reproduite avant la configuration des équipements.

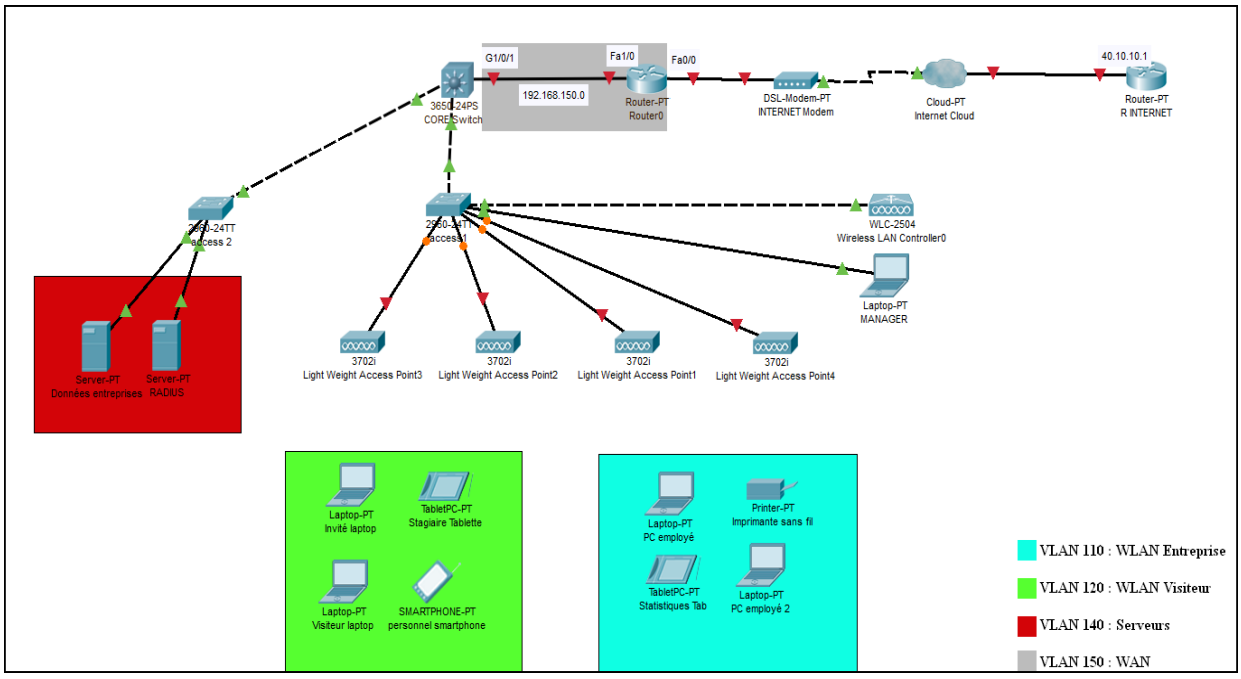

Figure V-1 Topologie simulée du réseau

- Nous nous sommes servis à titre d'exemple de quatre Points d'accès légers, chacun diffusant nos deux SSID.
- Un contrôleur Wi-Fi de type WLC-2504.
- Un serveur AAA de type RADIUS contenant les identifiants des employés.
- Un switch multicouche reliant les différentes parties du réseau LAN ainsi que la partie WAN.
- Des switchs d'accès reliant les différents équipements au switch multicouche.
- Un routeur interne et un routeur externe reliés par une connexion DSL afin de simuler un accès à INTERNET.
- Différents périphériques sans fil qui seront reliés à nos SSID selon leurs appartenances.

V.3. **VLANs à implémenter et leurs plans d'adressage**

L'adresse du réseau est 192.168.0.0/24, son masque de sous-réseau est 255.255.255.0.

Chaque sous-réseau pourra donc contenir 254 adresses IP utilisables.

Les machines affiliées à un VLAN, vont prendre des adresses IP d'un même sous-réseau.

Le tableau V.1 montre la liste des VLANs à implémenter ainsi que leurs paramètres IP.

VLAN-ID	Description	Adresse IP du sous réseau	Passerelle par défaut
1	**Par défaut**	**192.168.1.0/24**	**192.168.1.100**
110	**WLAN Entreprise**	**192.168.110.0/24**	**192.168.110.100**
120	**WLAN Visiteur**	**192.168.120.0/24**	**192.168.120.100**
140	**Les serveurs base de données**	**192.168.140.0/24**	**192.168.140.100**
150	**WAN**	**192.168.150.0/24**	**192.168.150.100**

Tableau V-1: Liste des VLANs à implémenter et leur plan d'adressage.

V.4. **Configuration des équipements**

V.4.1. **Configuration des Commutateurs**

V.4.1.1. **Configuration du protocole VTP [82]**

Le protocole VTP permet à un administrateur réseau de configurer un commutateur pour qu'il propage des configurations VLAN à d'autres commutateurs du réseau. Le commutateur peut être configuré dans le rôle d'un serveur VTP ou d'un client VTP.

- VTP simplifie l'administration de réseaux locaux virtuels sur plusieurs commutateurs en répliquant les configurations VLAN entre les commutateurs.
- Un domaine VTP détermine quels switchs du réseau doivent être paramétrés de la même manière concernant la configuration VLAN.
- Le mode serveur VTP permet de créer, supprimer, et de modifier les VLANs.
- Le mode client VTP empêche la modification des réseaux locaux virtuels et permet uniquement de recevoir des informations VLAN par l'intermédiaire d'annonces VTP.

- **Configuration du protocole VTP sur le Switch Cœur**

Le commutateur CORE Switch sera configuré comme serveur VTP. C'est lui qui va gérer l'administration de l'ensemble des VLANs.

La figure V-2 représente la configuration du serveur VTP au niveau du switch multifonction.

```
CORE>en
CORE#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#vtp mode server
Device mode already VTP SERVER.
CORE(config)#vtp domain sonatrach
Changing VTP domain name from NULL to sonatrach
CORE(config)#vtp password sonatrach123
Setting device VLAN database password to sonatrach123
```

Figure V-2: Configuration du VTP-Server

- **Configuration du protocole VTP sur les autres switchs**

La figure V-3 représente la configuration VTP-client qui se fera au niveau des autres commutateurs.

```
access>
access>
access>en
access#config t
Enter configuration commands, one per line.  End with CNTL/Z.
access(config)#vtp mode client
Setting device to VTP CLIENT mode.
access(config)#vtp domain sonatrach
Changing VTP domain name from NULL to sonatrach
access(config)#vtp password sonatrach123
Setting device VLAN database password to sonatrach123
access(config)#
```

Figure V-3: Configuration des VTP-Clients

V.4.1.2. **Création des VLANs**

La création des réseaux locaux virtuels se fera au niveau du CORE Switch, et cette configuration sera par la suite automatiquement propagée aux autres commutateurs grâce au protocole VTP.

La figure V-4 illustre les commandes de base pour la création des VLANs.

```
CORE>en
CORE#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#vlan 110
CORE(config-vlan)#name WLAN-entreprise
CORE(config-vlan)#exit
CORE(config)#vlan 120
CORE(config-vlan)#name WLAN-visiteur
CORE(config-vlan)#exit
CORE(config)#vlan 140
CORE(config-vlan)#name Serveurs
CORE(config-vlan)#exit
CORE(config)#
CORE(config)#vlan 150
CORE(config-vlan)#name WAN
CORE(config-vlan)#end
CORE#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure V-4: Création des VLANs

V.4.1.3. **Configuration des ports physiques**

- **Le commutateur CORE Switch :**

  - Le port Gig1/0/1 : c'est le port relié au routeur, il sera configuré en mode Access pour le VLAN 150 (WAN).
  - Le port Gig1/0/3 : c'est le port connecté au switch qui relie les serveurs, il sera configuré en mode Access pour le VLAN 140 (serveurs base de données.).
  - Le port Gig1/0/2 : il est connecté au switch du réseau sans fil, il sera configuré en mode Trunk en autorisant les VLANs 110,120 ainsi que le VLAN 1 à transiter par ce port.

Les commandes nécessaires sont illustrées dans la Figure V-5.

```
CORE>en
CORE#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#interface gig1/0/1
CORE(config-if)#
CORE(config-if)#switchport access vlan 150
CORE(config-if)#switchport mode access
CORE(config-if)#exit
CORE(config)#interface gig1/0/3
CORE(config-if)#switchport access vlan 140
CORE(config-if)#switchport mode access
CORE(config)#interface GigabitEthernet1/0/2
CORE(config-if)#
CORE(config-if)#switchport trunk allowed vlan 110,120,1
CORE(config-if)#switchport trunk encapsulation dot1q
CORE(config-if)#switchport mode trunk
```

Figure V-5: Configuration des interfaces sur le CORE Switch.

- **Le Commutateur Access 2 :**

Les trois ports de ce switch sont configurés en mode Access pour le VLAN 140 (voir figure V-6).

```
access>en
access#config t
Enter configuration commands, one per line.  End with CNTL/Z.
access(config)#interface range fa0/1-3
access(config-if-range)#switchport access vlan 140
access(config-if-range)#switchport mode access
access(config-if-range)#no shutdown
access(config-if-range)#end
access#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure V-6: Configuration des interfaces sur le switch Access 2.

- **Le Commutateur Access 1 :**
  - Le port Fa0/7 : c'est le port relié au Laptop Manager. Il sera configuré en mode Access pour le VLAN 1 (par défaut).
  - Les ports Fa0/1 jusqu'à Fa0/6 : ils seront configurés en mode Trunk en autorisant le transit des VLANs 1,110, et 120.

```
access1(config)#interface range fa0/1-6
access1(config-if-range)#switchport trunk allowed vlan 110,120,1
access1(config-if-range)#switchport mode trunk

access1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

access1(config-if-range)#exit
access1(config)#interface fa0/7
access1(config-if)#switchport access vlan 1
access1(config-if)#switchport mode access
access1(config-if)#end
access1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure V-7: Configuration des interfaces sur le switch Access 1

V.4.1.4. **Interfaces VLANs et Routage inter-VLAN** [80]

La création d'interfaces VLANs sur le switch fédérateur et l'assignation d'adresses IP à ces dernières permet de les utiliser comme passerelles par défaut pour chaque VLAN du réseau.

Nous pourrons par la suite activer le routage inter-VLAN grâce à la commande **« ip routing ».**

La figure V-8 illustre les commandes nécessaires à cette configuration.

```
CORE#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#interface vlan 110
CORE(config-if)#
%LINK-5-CHANGED: Interface Vlan110, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan110, changed state to up
CORE(config-if)#ip address 192.168.110.100 255.255.255.0
CORE(config-if)#no sh
CORE(config-if)#interface vlan 120
CORE(config-if)#
%LINK-5-CHANGED: Interface Vlan120, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state to up

CORE(config-if)#ip address 192.168.120.100 255.255.255.0
CORE(config-if)#no sh
CORE(config-if)#interface vlan 140
CORE(config-if)#
%LINK-5-CHANGED: Interface Vlan140, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan140, changed state to up

CORE(config-if)#ip address 192.168.140.100 255.255.255.0
CORE(config-if)#no sh
CORE(config-if)#interface vlan 150
CORE(config-if)#
%LINK-5-CHANGED: Interface Vlan150, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan150, changed state to up

CORE(config-if)#ip address 192.168.150.100 255.255.255.0
CORE(config-if)#no sh
CORE(config-if)#interface vlan 1
CORE(config-if)#ip address 192.168.1.100 255.255.255.0
CORE(config-if)#no sh
CORE(config-if)#exit
CORE(config)#ip routing
CORE(config)#end
```

Figure V-8: Configuration des interfaces VLANs et routage inter-VLAN

V.4.1.5. **Configuration du protocole DHCP** [30] [79]

Un serveur DHCP a pour rôle de distribuer automatiquement des paramètres IP à des clients pour une durée déterminée, notamment en lui attribuant une adresse IP, un masque de sous-réseau, une passerelle par défaut…, etc.

Nous pouvons configurer notre switch fédérateur comme relais pour un serveur DHCP externe, ou le programmer en tant que serveur DHCP.

Pour notre simulation, nous utiliserons la deuxième option. Le CORE Switch pourra ainsi attribuer des adresses IP selon le VLAN d'appartenance du périphérique (voir Figure V-9).

```
CORE(config)#ip dhcp excluded-address 192.168.1.100
CORE(config)#ip dhcp excluded-address 192.168.110.100
CORE(config)#ip dhcp excluded-address 192.168.120.100
CORE(config)#ip dhcp excluded-address 192.168.140.100
CORE(config)#ip dhcp excluded-address 192.168.150.100
CORE(config)#ip dhcp pool WLAN-entreprise
CORE(dhcp-config)#default-router 192.168.110.100
CORE(dhcp-config)#network 192.168.110.0 255.255.255.0
CORE(dhcp-config)#exit
CORE(config)#ip dhcp pool WLAN-visiteur
CORE(dhcp-config)#default-router 192.168.120.100
CORE(dhcp-config)#network 192.168.120.0 255.255.255.0
CORE(dhcp-config)#exit
CORE(config)#ip dhcp pool Serveurs
CORE(dhcp-config)#default-router 192.168.140.100
CORE(dhcp-config)#network 192.168.140.0 255.255.255.0
CORE(dhcp-config)#exit
CORE(config)#ip dhcp pool LWAP
CORE(dhcp-config)#default-router 192.168.1.100
CORE(dhcp-config)#network 192.168.1.0 255.255.255.0
CORE(dhcp-config)#option 43 ip 192.168.1.254
CORE(dhcp-config)#end
CORE#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure V-9: Configuration du serveur DHCP

La création du pool LWAP servira à l'attribution de paramètres IP aux points d'accès léger. La commande **« option 43 »** spécifie l'adresse IP du contrôleur Wi-Fi.

V.4.2. **Configuration du serveur RADIUS**

- Premièrement, on configure les paramètres IP du serveur en statiques afin qu'il soit toujours accessible à la même adresse. Dans l'onglet Desktop du serveur > IP Configuration (voir figure V-10).

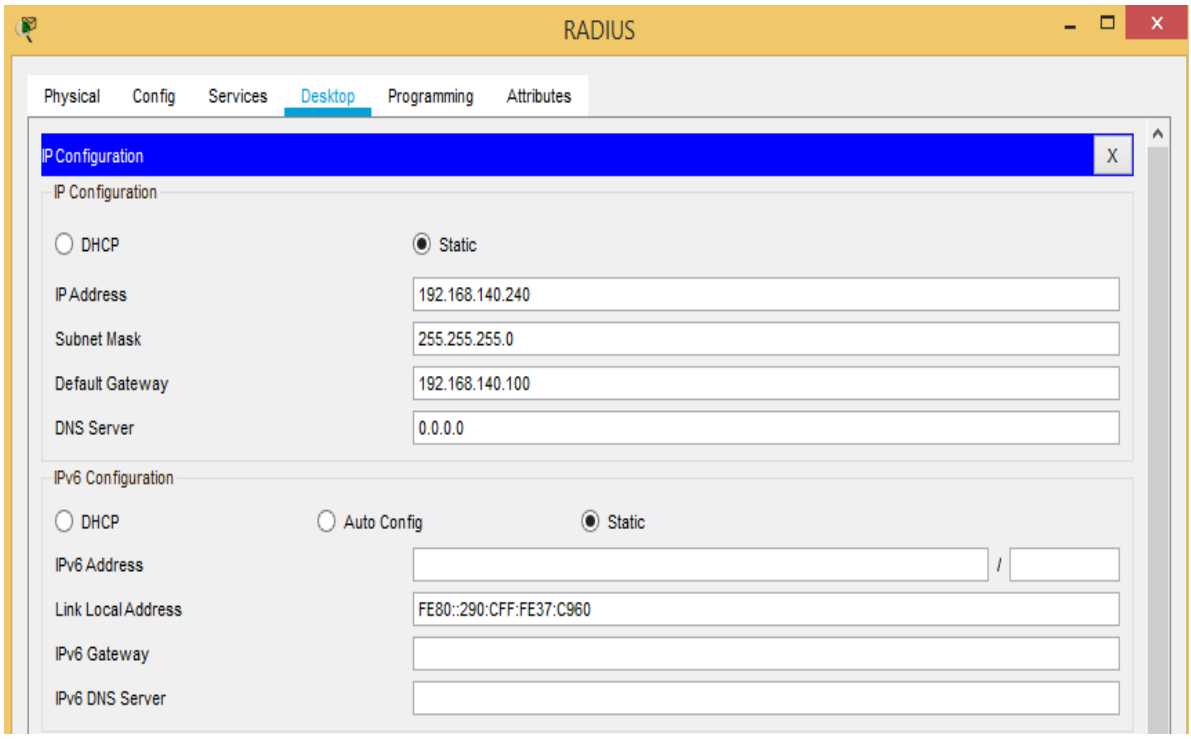

Figure V-10: Adressage IP du serveur RADIUS

- Deuxièmement, il faut créer un profil pour le client radius dans l'onglet Services > AAA. Dans notre cas, le client radius est le WLC.

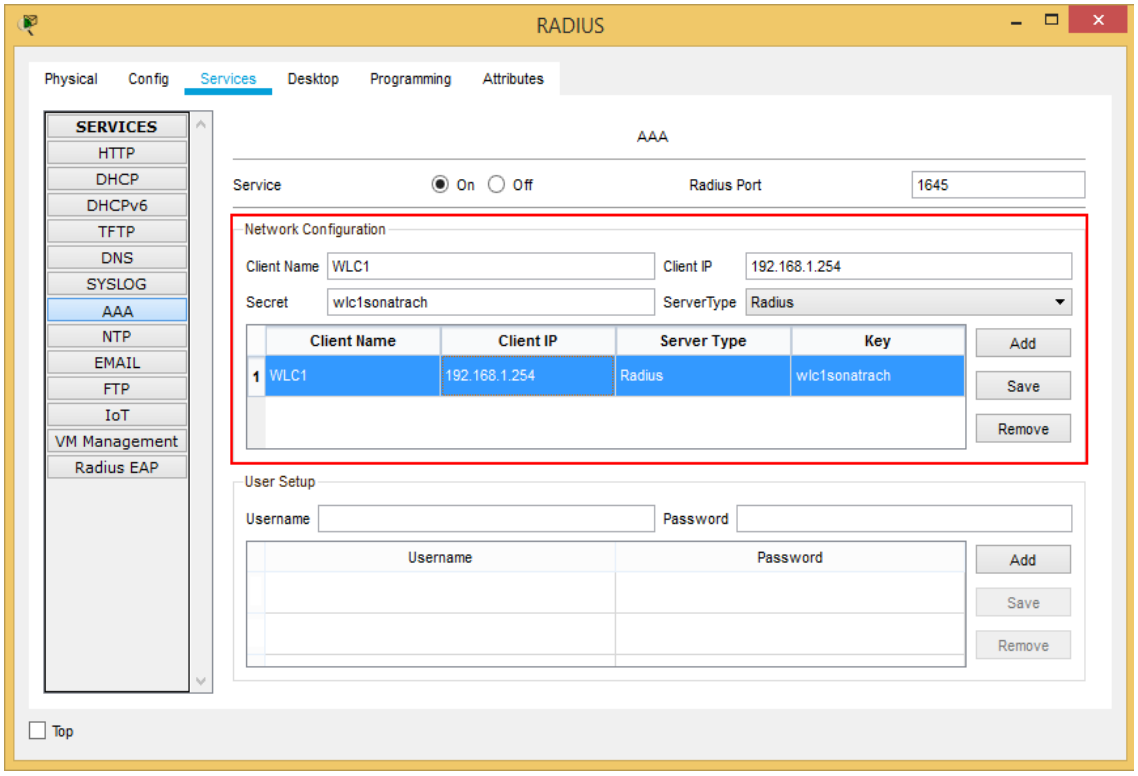

Figure V-11: Création d'un profil de client RADIUS

- Enfin, on programme les identifiants des utilisateurs qui pourront s'authentifier via notre serveur RADIUS (voir figure V-12).

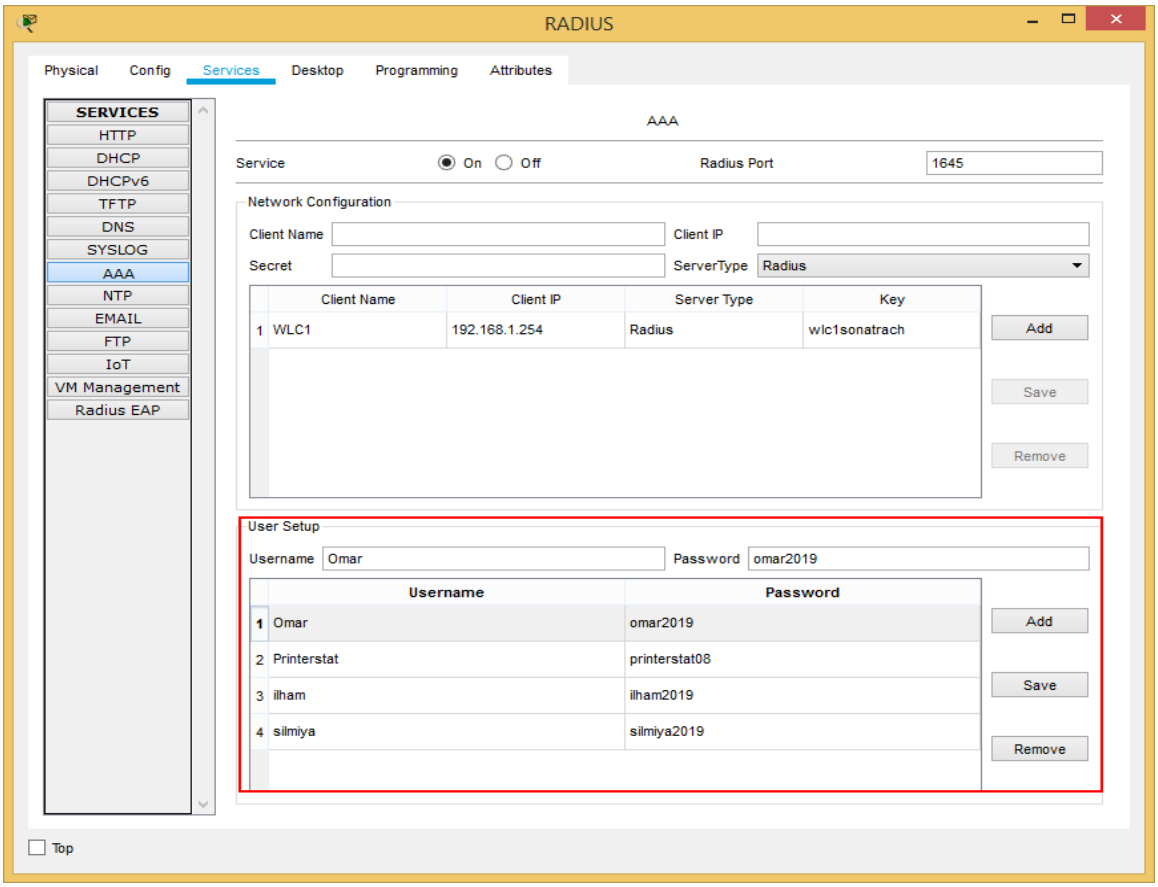

Figure V-12: Configuration des profils utilisateurs

V.4.3. **Configuration du WLC**

V.4.3.1. **Management**

L'intégralité de la configuration du WLC se fera via son interface graphique accessible par navigateur à l'adresse IP de l'interface Management. Nous devons donc préalablement configurer deux choses :

- Les paramètres IP du PC MANAGER : dans l'onglet DESKTOP > IP configuration : on active le DHCP.
- L'interface management du WLC : dans l'onglet CONFIG > Management : on définit les paramètres IP statiques (voir figure V-13).

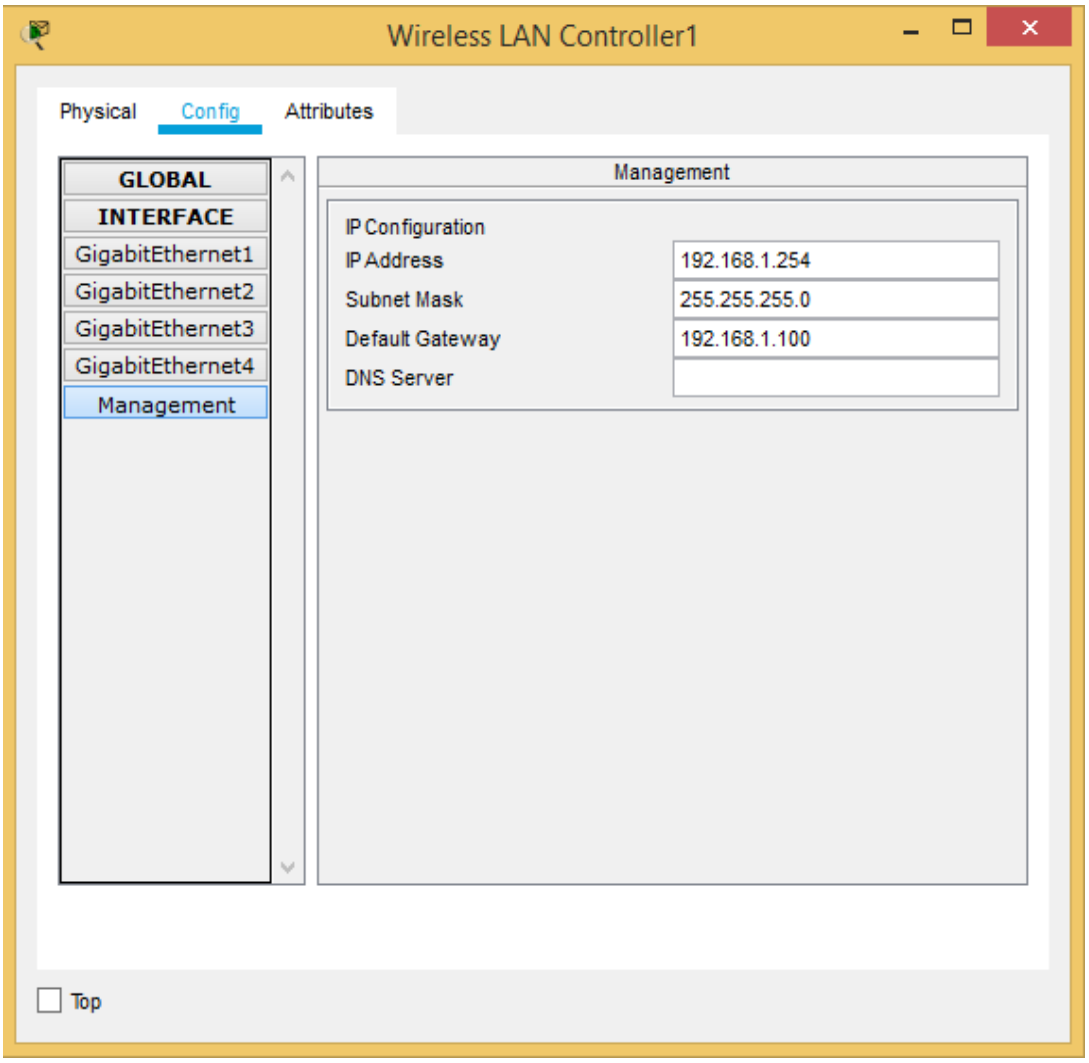

Figure V-13: Configuration de l'interface Management du WLC

V.4.3.2. **Création d'un compte Administrateur**

Après avoir entré l'adresse IP du WLC dans le Web Browser du PC MANAGER, il nous affiche l'interface graphique qui nous demande de créer le nom d'utilisateur et le mot de passe (complexe) de l'administrateur (voir figure V-14).

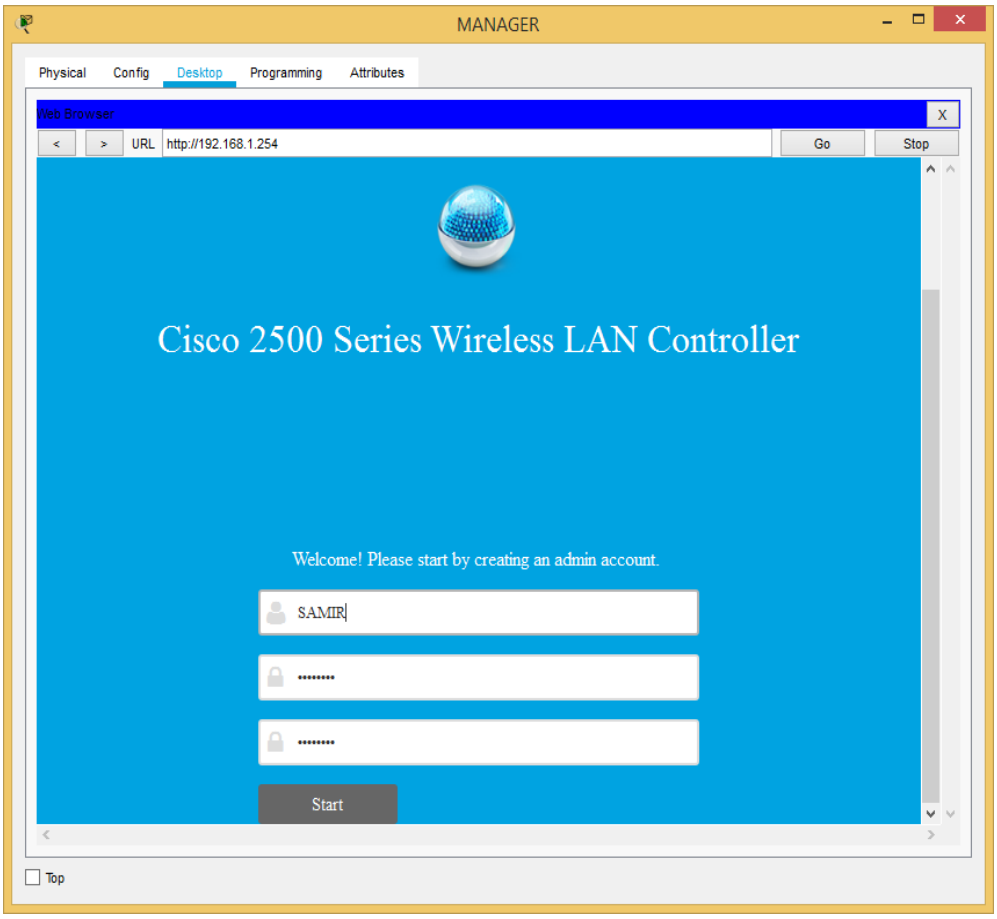

Figure V-14: Création d'un administrateur sur le WLC

Par la suite, nous rentrons soigneusement les informations demandées comme cité précédemment, et on applique.

V.4.3.3. **Configuration du client RADIUS**

Afin que l'authentification puisse avoir lieu, le serveur RADIUS doit être accessible par le client RADIUS. Nous allons configurer ce dernier via l'onglet SECURITY > AAA > RADIUS > Authentification > New… (voir figure V-15).

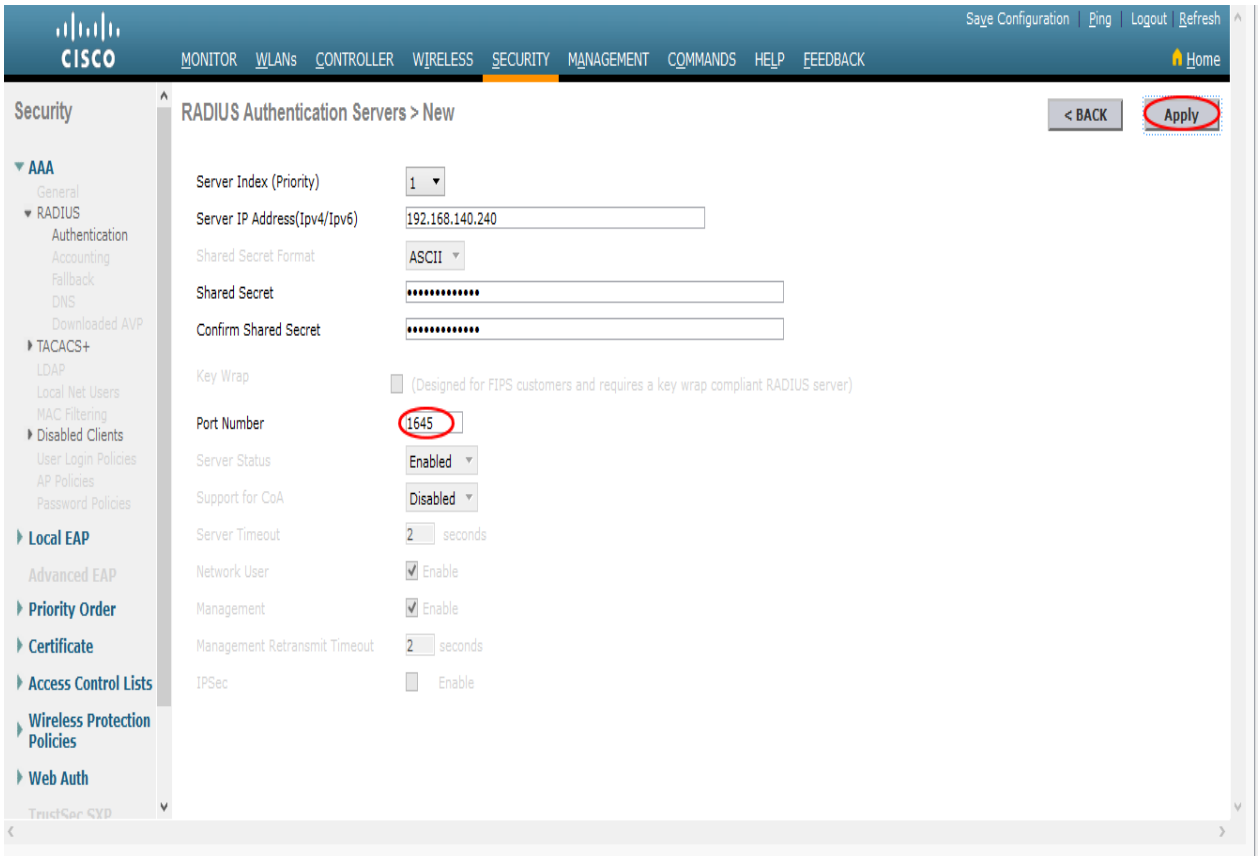

Figure V-15: Configuration du client RADIUS

V.4.3.4. **Configuration des interfaces virtuelles**

Avant de créer nos réseaux sans-fil, nous devons préalablement configurer des interfaces virtuelles associées à des VLANs spécifiques.

On ouvre à nouveau l'interface graphique du WLC sur le Web Browser[1].

Après authentification, on se dirige vers l'onglet CONTROLLER > Interfaces > New…

On doit créer une interface pour chaque SSID, les paramètres de chaque interface sont résumés dans le tableau V-2.

Interface Name	VLAN Id	Physical Port Number	IP Address	Netmask	Gateway	Primary DHCP Server
Visiteur	**120**	**1**	**192.168.120.254**	**255.255.255.0**	**192.168.120.100**	**192.168.120.100**
Entreprise	**110**	**1**	**192.168.110.254**	**255.255.255.0**	**192.168.110.100**	**192.168.110.100**

Tableau V-2: Paramètres des interfaces virtuelles du WLC

[1] Le protocole **HTTPS** devra obligatoirement être utilisé cette fois, au lieu de **HTTP.**

V.4.3.5. **Configuration des SSID**

- **SSID Entreprise :**

Dans l'onglet WLANs > Create New > On spécifie le nom du profil, et le SSID > Apply.

Dans l'onglet General > on coche Statut sur Enabled, et on définit interface sur « Entreprise ».

Dans l'onglet Advanced > on coche FlexConnect Local Switching sur Enabled.

Dans l'onglet Security > Layer 2 : on spécifie les paramètres tels que montré dans la figure V-16.

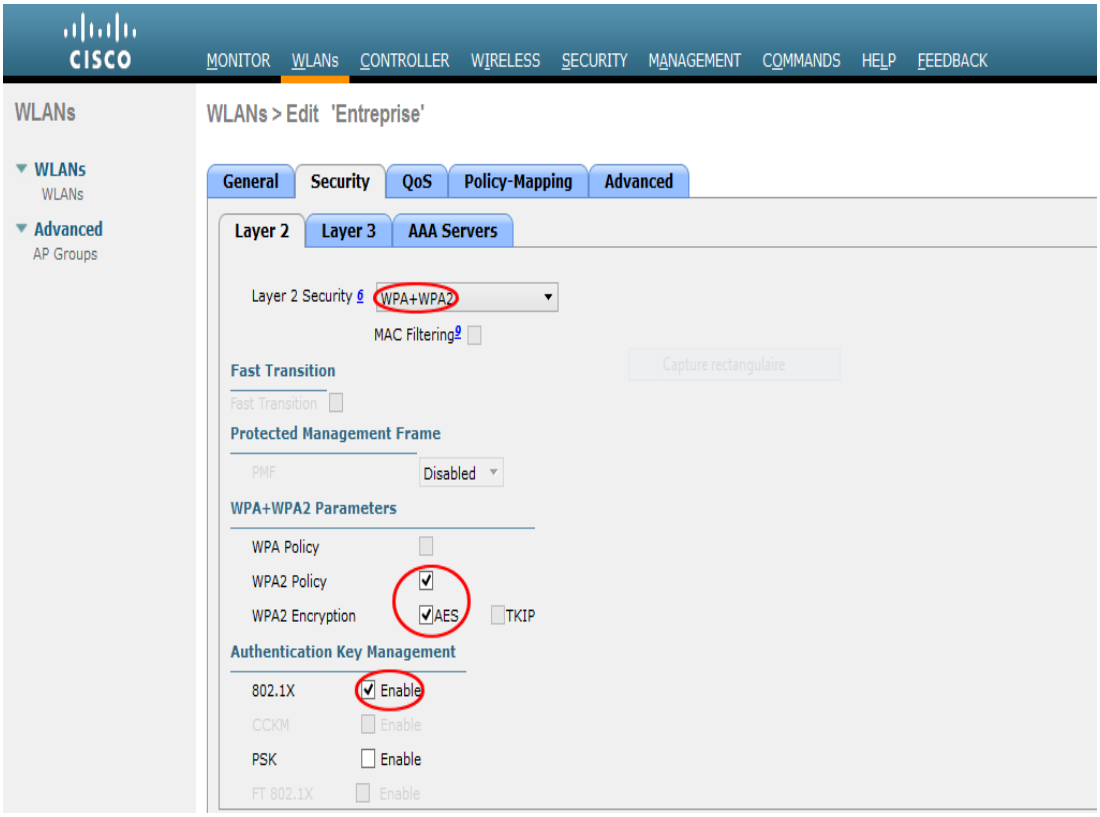

Figure V-16: Sécurité du SSID Entreprise.

Dans l'onglet Security > AAA Servers : on sélectionne le serveur RADIUS précédemment configuré > Apply.

- **SSID Visiteur :**

Dans l'onglet WLANs > Create New > On spécifie le nom du profil, et le SSID > Apply.

Dans l'onglet General > on coche statut sur Enabled, et on définit interface sur « **Visiteur** ».

Dans l'onglet Advanced > on coche FlexConnect Local Switching sur Enabled.

Dans l'onglet Security > Layer 2 : on spécifie les paramètres tels que montré dans la figure V-17 > Apply.

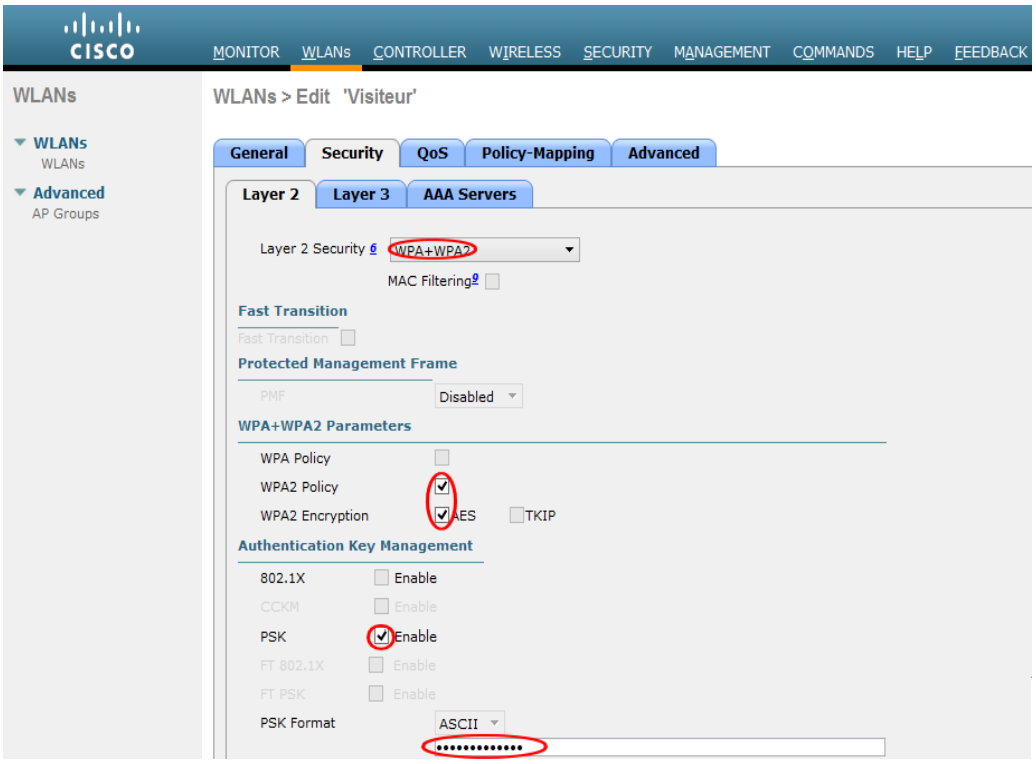

Figure V-17: Sécurité du SSID Visiteur.

V.4.4. **Configuration des périphériques Wi-Fi**

V.4.4.1. **Interfaces physiques**

Dans un premier temps, on doit ajouter des interfaces Wi-Fi aux périphériques qui n'en sont pas dotés (voir la figure V-18).

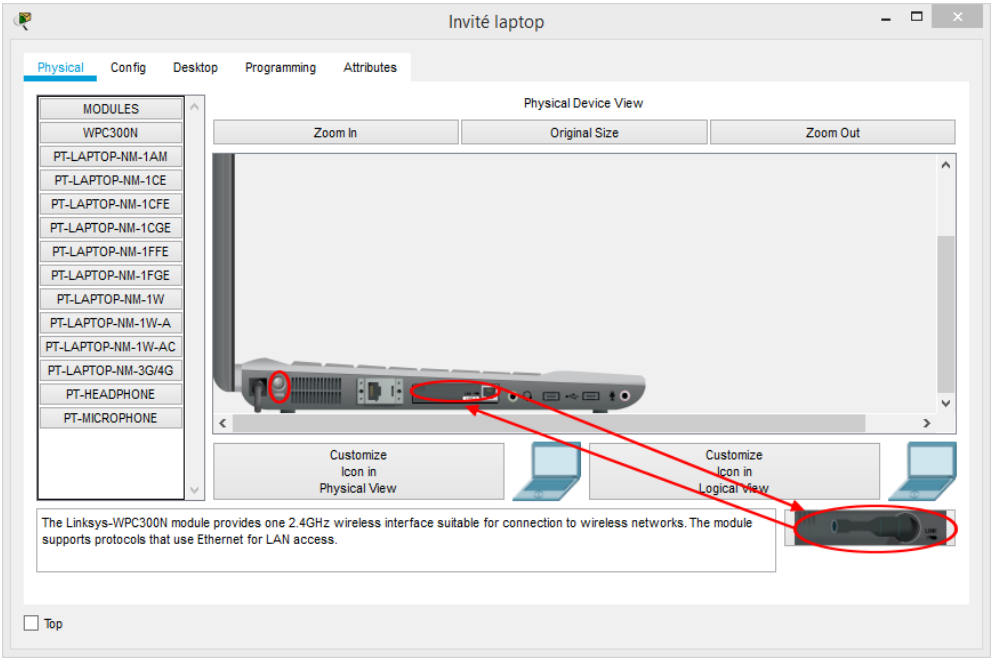

Figure V-18: Exemple d'ajout d'interface Wi-Fi.

V.4.4.2. **Paramètres d'authentification**

Chaque périphérique sera configuré en fonction du SSID auquel il sera connecté.

- **SSID Visiteur :**

Les clients de ce réseau seront configurés via l'onglet Config > Wireless0 (voir figure V-19).

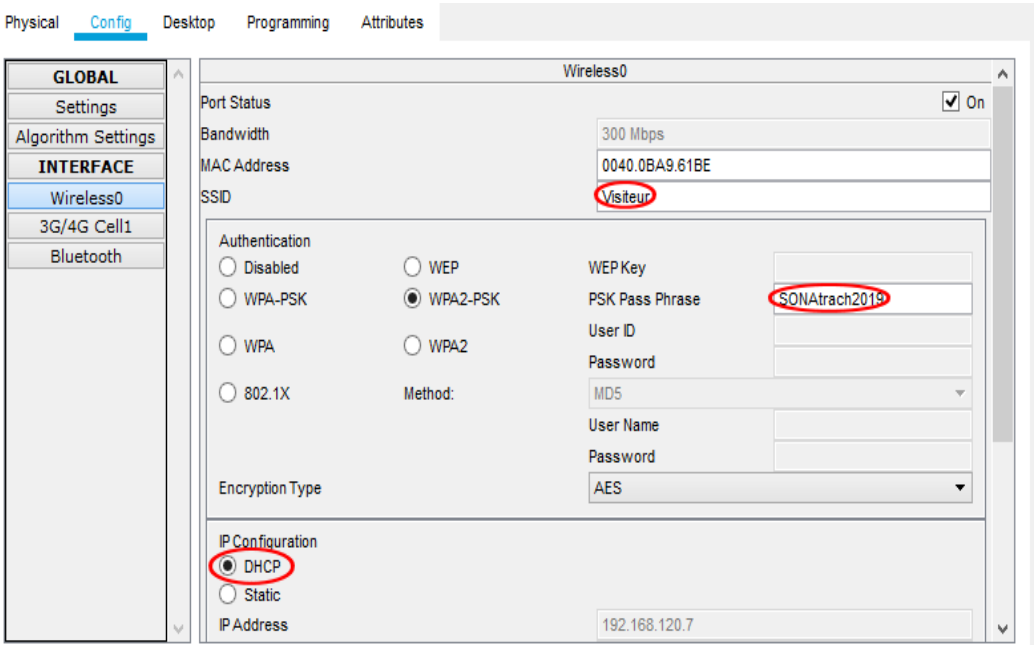

Figure V-19: Configuration d'un client du réseau Visiteur.

- **SSID Entreprise :**

Les clients de ce réseau seront configurés avec les identifiants créés précédemment dans le serveur RADIUS (voir figure V-20).

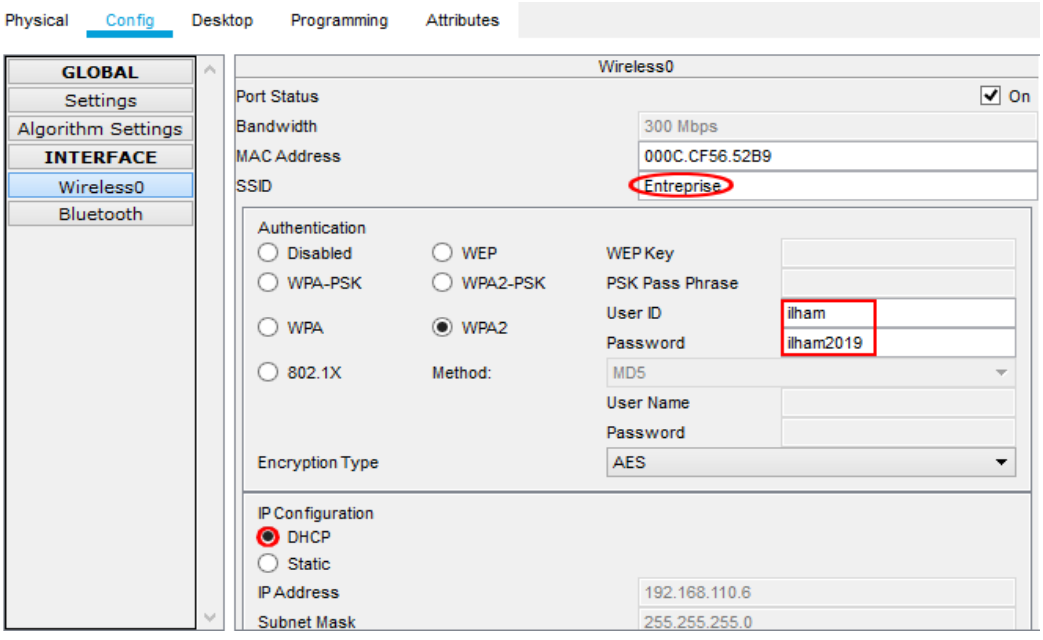

Figure V-20: Configuration d'un client du réseau Entreprise.

V.4.5. **Configuration des interfaces des Routeurs**

- **Router-Sonatrach :**

La configuration se fait grâce aux commandes suivantes :

Router-Sonatrach(config)#interface FastEthernet0/0
Router-Sonatrach(config-if)#ip address 40.10.10.2 255.0.0.0
Router-Sonatrach(config-if)#no shutdown
Router-Sonatrach(config-if)#exit
Router-Sonatrach(config)#interface FastEthernet1/0
Router-Sonatrach(config-if)#ip address 192.168.150.2 255.255.255.0
Router-Sonatrach(config-if)#no shutdown

- **Router-Internet :**

La configuration se fait grâce aux commandes suivantes :

Router-INTERNET(config)#interface FastEthernet0/0
Router-INTERNET(config-if)#ip address 40.10.10.1 255.0.0.0
Router-INTERNET(config-if)#no shutdown

V.4.6. **Configuration du Routage RIP** [78]

RIP est un protocole de routage dynamique. La table de routage est mise à jour de manière automatique toutes les 30 secondes par échange de paquets RIP entre les entités du réseau configurées avec ce protocole.

Dans notre cas, il servira à créer les routes reliant notre réseau local au réseau externe.

- **Router-Internet :**

La configuration se fait grâce aux commandes suivantes :

Router-INTERNET(config)#router rip
Router-INTERNET(config-router)#version 2
Router-INTERNET(config-router)#network 40.0.0.0
Router-INTERNET(config-router)#exit

- **Router-sonatrach :**

La configuration se fait grâce aux commandes suivantes :

Router-Sonatrach(config)#router rip
Router-Sonatrach(config-router)#version 2
Router-Sonatrach(config-router)#network 40.0.0.0
Router-Sonatrach(config-router)#network 192.168.150.0
Router-Sonatrach(config-router)#exit

- **CORE-Switch :**

La configuration se fait grâce aux commandes suivantes :

```
CORE(config)#router rip
CORE(config-router)#version 2
CORE(config-router)#network 192.168.110.0
CORE(config-router)#network 192.168.120.0
CORE(config-router)#network 192.168.150.0
CORE(config-router)#exit
```

V.4.7. **Configuration des ACL** [81]

Les listes de contrôle d'accès permettent de gérer le trafic en autorisant ou en refusant des paquets en fonction de certains critères.

Dans notre cas, elles serviront à interdire le transit de paquets vers les VLANs 110 et 140 quand ces paquets ont une adresse IP source appartenant au sous-réseau Visiteur (192.168.120.0).

- **1ère étape** : Création de l'ACL :

```
CORE>en
CORE#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#access-list 20 deny 192.168.120.0 0.0.0.255
CORE(config)#access-list 20 permit any
CORE(config)#end
CORE#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure V-21: Création de l'ACL sur le CORE Switch.

- **2nd étape** : Affectation de l'ACL aux interfaces :

Nous allons maintenant affecter notre liste de contrôle d'accès aux interfaces VLAN 110 et VLAN 140 avec l'option **« out »**, afin de bloquer tout paquet sortant par ces interfaces et dont l'adresse IP source appartient au sous-réseau Visiteur.

```
CORE(config)#interface vlan 110
CORE(config-if)#ip access-group 20 out
CORE(config-if)#exit
CORE(config)#interface vlan 140
CORE(config-if)#ip access-group 20 out
CORE(config-if)#end
CORE#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure V-22: Affectation de l'ACL aux interfaces VLANs.

V.5. Tests de fonctionnement de notre solution

V.5.1. Vérifications

V.5.1.1. Vérification de la création des VLANs

On utilise la commande « **show vlan brief** » sur chaque commutateur afin de vérifier que la configuration des VLANs a bien été distribuée par le serveur VTP.

La figure V-23 illustre les résultats sur le commutateur Access 1.

```
access1#
access1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
110  WLAN-entreprise                  active
120  WLAN-visiteur                    active
140  Serveurs                         active
150  WAN                              active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
access1#
```

Figure V-23: Vérification de la création des VLANs sur le client VTP.

V.5.1.2. Vérification des SVI

Grâce à la commande « **show ip interface brief** » on peut voir la configuration des interfaces virtuelles du switch (SVI) sur le CORE Switch (voir figure V-24).

```
GigabitEthernet1/0/16  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/17  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/18  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/19  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/20  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/21  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/22  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/23  unassigned      YES NVRAM  down                    down
GigabitEthernet1/0/24  unassigned      YES NVRAM  down                    down
GigabitEthernet1/1/1   unassigned      YES NVRAM  down                    down
GigabitEthernet1/1/2   unassigned      YES NVRAM  down                    down
GigabitEthernet1/1/3   unassigned      YES NVRAM  down                    down
GigabitEthernet1/1/4   unassigned      YES NVRAM  down                    down
Vlan1                  192.168.1.100   YES manual up                      up
Vlan110                192.168.110.100 YES manual up                      up
Vlan120                192.168.120.100 YES manual up                      up
Vlan140                192.168.140.100 YES manual up                      up
Vlan150                192.168.150.100 YES manual up                      up
```

Figure V-24: SVI du CORE Switch.

V.5.1.3. **Vérification de la distribution des adresses IP dynamiques**

On peut utiliser la commande « **show ip dhcp binding** » sur le CORE Switch pour vérifier que chaque poste a bien reçu une adresse IP DHCP.

```
CORE#show ip dhcp binding
IP address      Client-ID/              Lease expiration        Type
                Hardware address
192.168.120.5   00E0.F7B1.6EB4          --                      Automatic
192.168.120.6   0001.6425.E018          --                      Automatic
192.168.120.7   0040.0BA9.61BE          --                      Automatic
192.168.120.8   00D0.D38D.BD98          --                      Automatic
192.168.110.3   0002.1624.3653          --                      Automatic
192.168.110.4   000C.CF56.52B9          --                      Automatic
192.168.110.5   00E0.F7BD.4E50          --                      Automatic
192.168.110.6   0002.17E2.6C28          --                      Automatic
CORE#
```

Figure V-25: Distribution des adresses IP par le protocole DHCP.

Ou par vérification directement au niveau des postes :

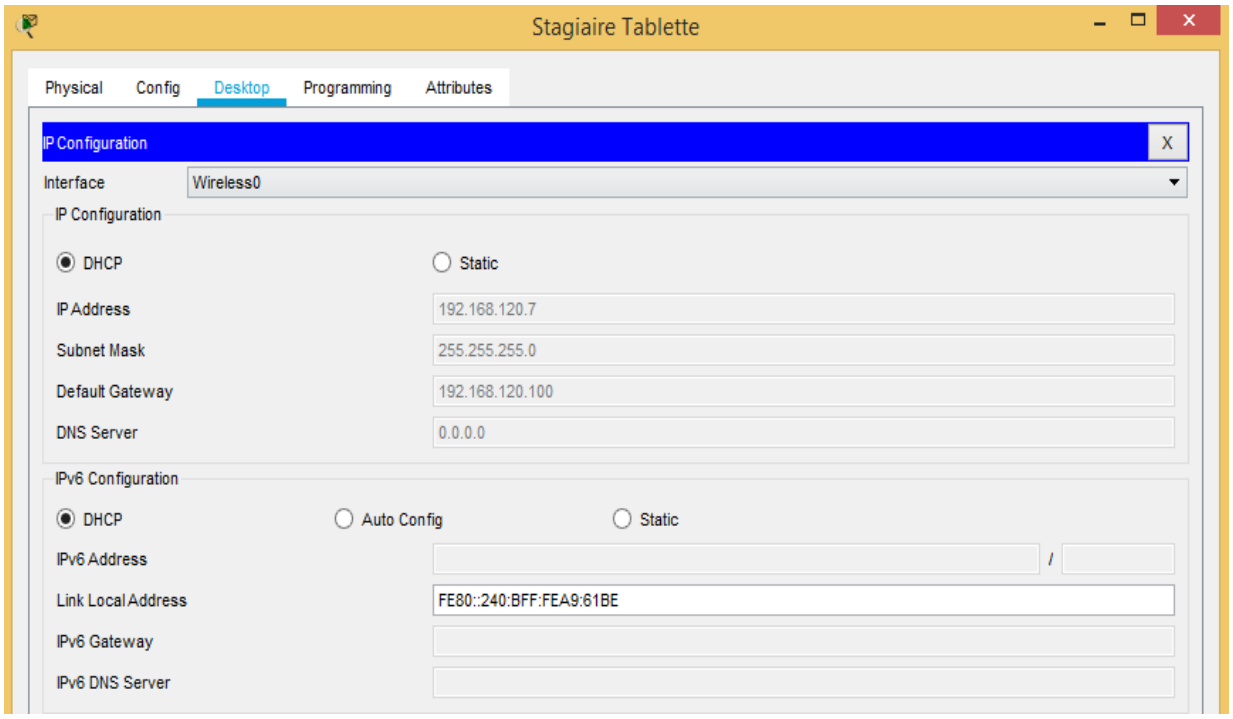

Figure V-26: Vérification des paramètres IP de Stagiaire Tablette.

L'attribution par DHCP marche correctement, et chaque poste obtient des paramètres IP selon le VLAN auquel il appartient.

V.5.2. **Tests de validation**

Dans cette partie, l'ensemble des tests de validation consiste à vérifier l'accessibilité de l'ensemble des équipements en utilisant la commande « **Ping** » qui teste la réponse d'un équipement sur le réseau. Donc, si un équipement veut communiquer avec un autre, le Ping permet d'envoyer des paquets au destinataire. Si l'équipement récepteur reçoit ces paquets, la communication est réussie.

- **Entre le CORE Switch et les routeurs :**

```
CORE>ping 192.168.150.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

CORE>ping 40.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/51/60 ms
```

Figure V-27: Ping entre le CORE Switch et les routeurs.

- **Entre les routeurs :**

```
Router-Sonatrach>ping 40.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.10.10.1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 49/60/82 ms

Router-Sonatrach>
```

Figure V-28: Ping entre les routeurs.

- **Poste avec SSID Entreprise et serveur de données (Test du routage inter-VLAN) :**

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.140.1

Pinging 192.168.140.1 with 32 bytes of data:

Reply from 192.168.140.1: bytes=32 time=10ms TTL=127
Reply from 192.168.140.1: bytes=32 time=4ms TTL=127
Reply from 192.168.140.1: bytes=32 time=7ms TTL=127
Reply from 192.168.140.1: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.140.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 10ms, Average = 6ms
```

Figure V-29: PING d'un poste avec SSID Entreprise vers serveur de données.

- **Poste avec SSID Entreprise et Router-INTERNET :**

```
Packet Tracer PC Command Line 1.0
C:\>ping 40.10.10.1

Pinging 40.10.10.1 with 32 bytes of data:

Reply from 40.10.10.1: bytes=32 time=58ms TTL=253
Reply from 40.10.10.1: bytes=32 time=51ms TTL=253
Reply from 40.10.10.1: bytes=32 time=55ms TTL=253
Reply from 40.10.10.1: bytes=32 time=68ms TTL=253

Ping statistics for 40.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 68ms, Average = 58ms
```

Figure V-30: PING d'un poste avec SSID Entreprise vers le Router-INTERNET.

Les utilisateurs du WLAN Entreprise ont bel et bien un accès à Internet.

- **Poste avec SSID Visiteur et Router-INTERNET :**

```
Packet Tracer PC Command Line 1.0
C:\>ping 40.10.10.1

Pinging 40.10.10.1 with 32 bytes of data:

Reply from 40.10.10.1: bytes=32 time=96ms TTL=253
Reply from 40.10.10.1: bytes=32 time=60ms TTL=253
Reply from 40.10.10.1: bytes=32 time=65ms TTL=253
Reply from 40.10.10.1: bytes=32 time=64ms TTL=253

Ping statistics for 40.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 96ms, Average = 71ms
```

Figure V-31: Ping d'un poste avec SSID Visiteur vers le Router-INTERNET.

Les utilisateurs du WLAN Visiteur ont bel et bien un accès à Internet.

- **Poste avec SSID Visiteur et Imprimante sans-fil (SSID Entreprise) :**

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.110.5

Pinging 192.168.110.5 with 32 bytes of data:

Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.

Ping statistics for 192.168.110.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure V-32: Ping d'un poste avec SSID Visiteur vers l'imprimante sans-fil.

- **Poste avec SSID Visiteur et les Serveurs (VLAN140) :**

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.140.240

Pinging 192.168.140.240 with 32 bytes of data:

Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.

Ping statistics for 192.168.140.240:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.140.1

Pinging 192.168.140.1 with 32 bytes of data:

Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.
Reply from 192.168.120.100: Destination host unreachable.

Ping statistics for 192.168.140.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure V-33: Ping d'un poste avec SSID Visiteur vers les serveurs.

Les utilisateurs du WLAN Visiteur n'ont accès ni aux périphériques du WLAN Entreprise, ni aux serveurs de l'entreprise, et ceci grâce à la segmentation du réseau en VLANs, et à la configuration des listes de contrôle d'accès (ACL).

V.6. Conclusion

Dans ce chapitre, nous avons mis en place un réseau sans-fil d'entreprise performant, et configuré une solution robuste pour y contrôler l'accès.

Nous avons expliqué la configuration de chacun des éléments pour la réalisation de ce projet. Pour finir, on a opté pour des vérifications et des tests de validations afin de prouver l'efficacité de l'infrastructure.

Notre solution peut être optimisée d'avantage, en l'alliant avec d'autres procédés complémentaires existant dans l'entreprise tel que l'annuaire LDAP, pour les identifiants des utilisateurs afin d'offrir une solution véritablement sécurisée et optimale.

Lors de la mise en place de cette architecture, il est fortement conseillé de penser à l'aspect redondance, en introduisant un contrôleur Wi-Fi secondaire qui prendra le relai du contrôleur principal, si ce dernier tombe en panne.

Enfin, un réseau Wi-Fi bien sécurisé est aussi un réseau bien supervisé. La mise en place d'un mécanisme de monitoring permettra de détecter toute activité suspecte pour y remédier rapidement.

Conclusion générale

L’objectif de notre projet était la réalisation d’un réseau Wi-Fi pour l’entreprise RTC SONATRACH de Béjaïa. Pour ce faire, il nous a fallu penser à une issue qui s’adapte avec l’architecture du réseau existant, tout en tenant compte de la durabilité, l’évolution et la fiabilité de cette solution, tant sur le plan technique que sur le plan économique.

Pour entamer ce travail, il nous a fallu faire des recherches sur divers supports bibliographiques et plateformes en ligne, demander de l’aide, et bien sûr faire d’innombrables tentatives de simulation, pour bien comprendre les mécanismes de fonctionnement des réseaux Wi-Fi. Nous avons ainsi pu obtenir le savoir nécessaire à la création d’un réseau d’entreprise efficace et extensible.

Notre stage pratique nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique et qui sera utile pour nous à l’avenir, tout en apportant une contribution à l’entreprise.

Ce fut l’occasion de nous familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir nos connaissances, et de les appliquer aux diverses réalités du terrain. Nous y avons également approfondi notre compréhension sur les fonctionnalités des commutateurs de niveau 2 et multicouches tels que les VLANs, l’agrégation des ports, le routage inter-VLAN, et les listes de contrôle d’accès.

Ce projet nous a permis de mettre en pratique les principes théoriques acquis durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d’avoir une idée plus profonde et plus pragmatique sur l’importance du réseau dans une entreprise.

Nos propositions font partie des solutions les plus fiables actuellement. Mais ça ne sera pas le cas pour toujours. En effet, un système parfaitement sécurisé aujourd’hui ne le sera sans doute plus tout à fait dans un an, si on ne le met pas à jour. De nouvelles failles auront été découvertes, à tous les niveaux et surtout au niveau logiciel. D’où la nécessité de toujours rester informé sur les progrès dans le domaine.

BIBLIOGRAPHIE

[1] **MAHER Gaha, « Sécurité dans les réseaux Wi-Fi : étude détaillée des attaques et proposition d'une architecture Wi-Fi sécurisée »,** UNIVERSITÉ DU QUÉBEC, MONTRÉAL, Mars 2007.

[2] **ZIDANI Ferroudja, « Solution d'authentification et de gestion de clés pour le standard 802.11i des réseaux WiFi »,** faculté des Sciences de l'Ingénieur département d'Informatique, Universite Ferhat Abbas – Sétif UFAS Algérie.

[3] **BELABDELLI Abdelheq et OUKAZ Mokhtar, « Dimensionnement D'un Réseau Sans Fil Wifi »,** faculté de technologie département de génie électrique et électronique, universite Abou Bekr Belkaid Tlemcen, 01 juillet 2012.

[4] **DI GALLO Frédéric, « WiFi L'essentiel qu'il faut savoir… »**, synthèse publié le 23/11/2003.

[5] **CHEIKHROUHOU Omar, « Sécurité des réseaux adhoc »**, Département d'Informatique et de Mathématiques Appliquées, Ecole Nationale d'Ingénieurs de Sfax, le 4 juillet 2005.

[6] **BOUCHOUCHA Lydia et TOUCHI Ibtissam, « Développement des Méthodes de Sécurité des Réseaux Mobiles »**, département Automatique, Télécommunication et Électronique, Université A. Mira de Bejaïa, 2014/2015.

[7] **GUISSI Yasmine, « Etude de la technique de gestion d'un réseau sans fil basé sur le standard 802.16 »**, département de Génie électrique, université A. MIRA – BEJAIA, 2012/2013.

[8] **TADJINE Samir, MEHNAOUI Samir et Aouchiche Thiziri, « Réseau 5G »,** département Automatique, Télécommunication et Électronique, Université A. Mira de Bejaïa, 2016/2017.

[9] **KARA Nadjah, « Conception d'un réseau de communication pour une maison intelligente en utilisant la technique d'internet des objets »**, Faculté des Sciences Exactes Département d'Informatique, 2016/2017.

[10] **TIZZAOUI Youva, « Internet des Objets « IoT » »,** Application : Industrie 4.0 », Faculté de Technologie Département Génie Électrique, Université A. Mira de Bejaïa, 2016/2017.

[11] **GERTHOFFERT François et al, « 802.11 les réseaux sans fil »**, livre achevé le 29/03/2003.

[12] **GERON Aurélien, « WIFI PROFESSIONNEL. La norme, le déploiement, la sécurité. 3ème édition » ;** éditeur : Dunod en Malakof, France ; paru le 23/09/2009 ; Collection InfoPro - Réseaux et télécoms.

[13] **BELKADI Salim et ABAIDIA Abdelmadjid, « Planification des réseaux Wi-Fi par usage d'une approche heuristique : Recherche Tabou »,** Faculté des Sciences Exactes

et des Sciences de la Nature et de la Vie, Département Mathématiques et Informatiques, Université A. Mira de Bejaïa, 2015/2016.

[14] **RIAHI Mohammed Nadjib, « CONCEPTION DES RESEAUX LOCAUX SANS FIL AVEC LOGICIEL OPNET »,** Faculté de Technologie, Département du Génie Electrique et Electronique, Laboratoire de Télécommunications, Juin 2014.

[15] **BOUABID Amel, « Choix d'un protocole de routage dynamique dans un réseau d'entreprise : Cas de CEVITAL »,** Faculté de Sciences Exactes, Département d'Informatique, Université A. Mira de Bejaïa, 2012/2013.

[16] **ATELIN Philippe , « Wi Fi. Réseaux sans fil 802.11 _ Technologie - Déploiement - Sécurisation. Résumé. Philippe ATELIN. ENI Editions - All rigths reserved, 2ème édition »** ; éditeur : Eni à Saint-Herbin en France ; paru le 11/08/2008 ; Collection Ressources informatiques.

[17] **DRIDI Khaled, « Spécification du protocole MAC pour les réseaux IEEE 802.11e à différentiation de services sous contrainte de mobilité »,** Réseaux & Télécoms, Université Paris Est, Décembre 2011.

[18] **GRUNENBERGER Yan, « Réseaux sans fil de nouvelle génération : architectures spontanées et optimisations inter-couches »**, École Doctorale « Mathématiques, Sciences et Technologies de l'Information, Informatique », Institut Polytechnique de GRENOBLE, 03/12/2008.

[19] **TERRÉ Michel, « Le Standard 802.11 Couche physique et couche MAC »,** Mars 2007.

[20] **BENDIMERAD Fethi Tarik, « MIMO ET ACCÈS MULTIPLES AVANCÉS POUR RÉSEAUX SANS FIL »,** Laboratoire de Télécommunications, Université Abou Bekr Belkaid, Tlemcen, programme national de recherche 2011-2013.

[21] **KHERBACHE Zeyneb, LARIBI Amina « Étude de la Qualité de Service (QoS) dans les réseaux WIFI »**, Facultés des Sciences Département de l'Informatique, Université Abou Bekr Belkaid, Tlemcen, 2010/2011.

WEBOGRAPHIE

[22] **PILLOU Jean-François, « Réseaux sans fil - Wireless Networks »**, publié dans le site commentçamarche.net le 14/10/2008

[23] **HADDACHE,** « 03-Les-réseaux-sans-fils », publié dans le site univ-bouira en 2010/2011.

[24] **KHELIFI Hakima et KERBOUAI Feyrouz, « Le WIFI sur les VANETs »,** publié dans slideplayer.fr.

[25] **« GIGASET C430HXD Téléphone DECT, 2 combinés avec socle de chargement »**, publié dans le site reichelt.com.

[26] **« Le Bluetooth : qu'est-ce que c'est et comment ça marche ? »,** publié dans le site prixtel.com le 13/11/2018.

[27] **DESSUREAULT Alain, « les réseaux sans fil »,** publié dans le site icriq.com en avril 2006.

[28] **« HomeRF domestique les réseaux sans fil jusqu'à 50 mètres »,** publié dans le site 01net.com le 08/01/2001.

[29] **« HomeRF »,** publié dans la page lansansfil.free.fr.

[30] Extrait depuis le site de Wikipédia.

[31] **PILLOU Jean-François, « WMAN - Réseaux métropolitains sans fil »,** publié dans le site commentçamarche.net le mardi 14 octobre 2008,

[32] **« 5G, 4G, 3G, GPRS, EDGE : que signifient ces appellations ? »**, publié dans le site prixtel.com le 9 novembre 2018.

[33] **Aurélien, « G, Edge, H, H+, 3G, 4G : les réseaux mobiles passés au crible »**, publié dans le site fnac.com le 13/10/2016.

[34] **MEURISSE Eric, « L'UMTS et le haut-débit mobile »**, publié dans univ-mlv.fr en November 2006.

[35] **TEMARI Fares, « 4G : Une information importante à savoir avant d'acheter un Smartphone »**, publié dans android-dz.com le 30/11/2016.

[36] **« 4G LTE, 4G LTE Advanced et 4G+ UHD, quelle différence ? »**, publié dans prixtel.com le 17/01/2019.

[37] **BENFATTOUM Ali « LES LPWAN - CES NOUVEAUX RÉSEAUX DE L'INTERNET DES OBJETS »**, publié dans le site frugalprototype.com le 26/12/2015,

[38] **« Le LiFi : explication, avantages et contraintes »**, publié dans le site kyos.ch le 11/07/2014.

[39] **DOLAN Roxane et IONAS Matthieu, « Réseaux filaire et Wifi: Avantages et inconvénients »,** publié dans le blog over-blog.com le 13/08/2013.

[40] **PLANUS Yannis, ROCHEDY Adrien et SALIQUE Yoann, « PI11 - Solution de géo localisation indoor basée sur l'utilisation du ZigBee »,** publié dans le site grenoble-inp.fr le 03/04/2014.

[41] **« Wi-Fi n, ac, ad, ax… : tout savoir sur le réseau sans fil et ses débits »**, publié dans le site frandroid.com le 15/11/2018.

[42] **« Normes Wi-Fi 802.11a/b/g/n/ac : Comprendre le Wifi et ses normes »**, publié dans le site le-routeur-wifi.com le 18/04/2019.

[43] **« WIFI : le matériel (synthèse : centre Erasme »**, publié dans le site erasme.org le 12/06/2003.

[44] **« ALFA NETWORK ROUTEUR/AP AC1200R DUAL BAND »**, publié dans le site wifi-algerie.com.

[45] **« TP-LINK TL-WA801ND »**, publié dans le site ldlc.com le 19/03/2019,

[46] **PILLOU Jean-François, « Carte réseau »**, publié dans le site commentçamarche.net 08/01/2014,

[47] **« Carte wifi : quel est son rôle ? »,** publié dans le site ihunt4u.net.

[48**] « Types de cartes réseau sans fil »**, publié dans le site ordinateur.com.

[49] **« Carte PCMCIA TENDA WIFI 802.11g (54MBPS) »**, publié dans le site amazon.fr le 05/01/2017.

[50] **« TP-Link TL-WDN4800 Adaptateur PCI Express »**, ceci est publié dans le site amazon.fr le 09/01/2012.

[51] **« Adaptateur module PC Card (PCMCIA) vers port PCI »**, publié dans le site grosbill.com le 20/05/2018.

[52] **« CLÉ WIFI USB D-LINK »,** publié dans le site tunisianet.com.

[53] **HABIBOU AbouIslam, « Débloquer ou desimlocker une clé usb ooredoo (nedjma) »**, publié dans le site e-monsite.com le 19/12/2018.

[54] **« CDF300 COAXIAL CABLE »**, publié dans le site wellshow.com.

[55] **« LMR-500 Low Loss Flexible Coax Cable »,** publié dans le site fairviewmicrowave.com.

[56] **Fredo, « Le WI-FI »** publié dans le blog ciw.blog.free.fr, date de création du document le 31/07/2017.

[57] **« Antenne exterieure, 5 Ghz Omnidirectionnelle 11 dbi »,** publié dans le site antennes-wifi.com.

[58] **« 2.4 GHz 24dBi WIFI grille carrée antenne parabolique »,** publié dans le site aliexpress,

[59] **BOUCHAIB Nassereddine , « Évaluation des performances du protocole Hybrid Wireless Mesh Protocol du standard IEEE 802.11s »**, publié dans le site researchgate.net en Juin 2009,

[60] **PILLOU Jean-François**, **« Les modes de fonctionnement du Wifi (802.11 ou Wi-Fi) »,** publié dans le site commentçamarche.net le 13/12/2016,

[61] **« WiFi - Réseau sans fil et sécurité »,** publié le 04/11/2009 dans le site cocmmentçamarche.net.

[62] **« Communication in Industrial Networks »,** publié dans le site digikey.fr le 04/04/2012.

[63] **« bandes libres »,** publié dans le site de l'Arcep.fr le 31/05/2018,

[64] **SKOK Tomas, « 802.11 PHYSICAL LAYER STANDARD »,** publié dans le site vseprozvuk.cz le 15/03/2015

[65] **NAYARASI, « CWAP – 802.11n Introduction »,** publié dans le site mrncciew.com le 19/10/2014.

[66] **GHAYOULA Elies et al, « SISO, SIMO, MISO, MIMO Channels »,** publié dans le site researchgate.net en juillet 2014.

[67] **Jess, « Trame WIFI »,** publié dans le blog guide-wifi.blogspot.com le 07/01/2004.

[68] **FRATI Stéphane**, **« Couches MAC et physique »,** publié dans le site <iutsa.unice>,

[69] **BOUJU Alain, « Transmission, Système, Réseaux »,** publié dans le site pageperso.univ-lr.fr.

[70] **Rodrigues, « La transmission par onde radio »,** publié dans le site reseau-wifi.blogspot.com le 01/11/2006.

[71] **« Carrier Sense Multiple Access with Collision Avoidance »,** publié dans le site le opentextbooks.org 19/01/2016.

[72] **« Fonctionnement du réseau 802.11 : Couche Liaison de données »**, publié sans le site d.bilo.free.fr.

[73] **ADRAR, « Les technologies sans fil : le Wi-Fi et la securité »,** publié dans le site memoireonline.com.

[74] **« La technologie Li-Fi »**, publié dans le site lyceecolbert-tg.org.

[75] **HOUSNI-ALAOUI Imad et DEGLIN Stéphane**, **« Les réseau locaux sans fils : Un aperçu de la norme 802.11»**, publié dans le site karpok.com.

[76] **KONDAH Hamza, « Formation Hacking et Sécurité, Expert : Réseaux sans Fil »,** publié dans le site alphorm.com le 14/03/2016.

[77] **« Différence entre attaque active et attaque passive »**, publié dans le site waytolearnx.com le 28/07/2018

[78] **MEIER Yohan, « Cisco : configuration du routage RIP »,** publié dans le site it-connect.fr le 07/06/2017.

[79] **EMPSON Scott et ROTH Hans, « CCNP SWITCH Portable Command Guide: Implementing Inter-VLAN Routing »**, publié dans le site ciscopress.com le 06/04/2010.

[80**] SIMENE Samuel, « configuration du routage inter-vlan sur un layer 3 switch Cisco »,** publié dans le site supinfo.com le 21/10/2015.

[81] **OUZAI Houssine, « Les ACL, listes de contrôle d'accès »,** publié dans le site academia.edu.

[82] **« Understanding VLAN Trunk Protocol (VTP) »**, publié dans le site cisco.com le 29/09/2014.

[83] **Ericsson, « IEEE 802.11 and WECA Status Updates »,** Munich, Germany, publié le 11/10/2002 dans le site 3gpp.org.