République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira
Faculté de la Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications.
Spécialité : Réseaux et Télécommunications

Thème

Conception et déploiement d'un réseau Wi-Fi sécurisé avec contrôle d'accès et authentification basée sur les certificats

Préparé par :

- Melle BENATSOU TAFATH
- Melle AIT OUALI KAHINA

Dirigé par :

M. Diboune Abdelhani

Examiné par :

Mme Mezhoud Naima

M. Bellahsene Hocine

Année universitaire : **2024/2025**

Remerciements

Avant tout, on tient à remercier Dieu le tout puissant, pour nous avoir donné la force et la patience.

On tient particulièrement à remercier **Monsieur Diboune Abdelhani** pour nous avoir fait l'honneur d'être notre promoteur, de nous avoir fait confiance, nous avoir encouragées et conseillées tout en nous laissant une grande liberté, pour son soutien et sa grande générosité.

On tient remercie également **Monsieur Said Henchouche**, notre encadreur à la Pharmacie Centrale des Hôpitaux, pour sa confiance, ses conseils professionnels et l'opportunité qu'il nous a offerte d'enrichir nos compétences dans un environnement réel.

On tient à remercie aussi les **Membre du jury** d'avoir accepté d'examiner notre travail et pour le temps qu'ils y consacrent.

On tient également à exprimer notre reconnaissance et notre sincère gratitude à tous les enseignants qui nous ont accompagnées durant ce cursus universitaire.

Nous tenons aussi à remercier également tous les enseignants qui ont

Assurées notre formation durant notre cycle universitaire. Ainsi, que tout le personnel du département ATE.

Nous remercions aussi le personnel de l'entreprise Pharmacie Centrale des Hôpitaux, pour leurs accueils en stage pratique.

Merci à toute personne ayant contribué à l'élaboration de ce

Modeste travail.

Merci à tous

Dédicace

Au nom d'ALLAH, le tout Miséricordieux le très Miséricordieux

Je remercie Allah Le tout puissant, clément et Miséricordieux de m'avoir motivé à réaliser Ce modeste travail,

Ensuite je remercie infiniment ***mes parents*** *qui m'ont encouragée et aidée à arriver à ce Stade de formation.*

Je dédie ce modeste travail à ***ma mère*** *Fatiha, qui a sacrifié sa vie afin de réussir dans le Parcours de l'enseignement, celle qui est restée toujours à mes côtés dans les moments rudes de ma vie.*

Je dédie ce modeste travail à ***mon père*** *Lahlou, qui m'a accompagnée durant les moments les plus pénibles de ce long parcours de mon éducation.*

A mon très ***cher frère*** *Saad*

A ***mes sœurs*** *Tassadit, Faiza, Feta, Thiziri, Lahena*

A ***mes amis*** *Amina, Thanina, Lina, Lydia, Lynda, Zineb, Ferroudja, Ouiza, Yassemine*

A ***mon binome*** *Kahina*

À tous ***mes collègues*** *de la classe de* ***Réseaux et Télécommunications*** *pour les partages, les rires et les souvenirs.*

Tafath

Dédicaces

Avec toute la sincérité de mon cœur et l'humilité de mes mots, je dédie ce mémoire à celles et ceux dont l'amour, la présence et le soutien ont été mes piliers tout au long de ce parcours.

A ma maman adorée, *Toi qui es l'origine de tout, tes prières murmurées, ton amour discret, quelles que soient les paroles, elles resteront toujours insuffisantes pour exprimer toute ma gratitude.*

A mon père, *ta force, ton regard et tes conseils qui résonnant encore dans mes choix. Tu m'as appris à croire en mes capacités même dans les moments de doute***.**

A mes sœurs, *qui sont toujours pour me redonner énergie et sourire même dans les silences votre tendresse est un refuge.*

A mes frères, *Vos encouragement et votre respect m'ont toujours portée.*

A mes amies chères *Nesrine, Sofia, Badri, Romila, Votre amitié n'a pas seulement accompagné ce parcours, elle l'illuminé, merci pour votre écoute, vos rires, vos partages.*

A mon binôme Tafath *Ton soutien moral, ta patience et ta compréhension tout au long de ce projet.*

A toute la promotion RT 2024/2025 *Pour votre soutien mutuel et votre camaraderie ont rendu cette expérience enrichissante et inoubliable.*

Et à tous ceux qui m'aiment de proche ou de loin.

Kahina

A

- AAA: Authentication, Authorization, Accounting (ou Auditing)
- ACK: Acknowledge (Accusé de Réception)
- ACL: Access Control List
- AES: Advanced Encryption Standard
- AP: Access Point
- APPRO : Approvisionnement

B

- BSS: Basic Service Set

C

- CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- CHAP: Challenge-Handshake Authentication Protocol
- CRC: Cyclic Redundancy Check
- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance
- CSMA/CD: Carrier Sense Multiple Access with Collision Detection
- CTS: Clear To Send

D

- DGA: Direction Générale de l'Administration
- DCF: Distributed Coordination Function
- DIFS: DCF Inter-Frame Spacing
- DES: Data Encryption Standard
- DES3: Triple DES
- DHCP: Dynamic Host Configuration Protocol
- DISI: Direction de l'Informatique et des Systèmes d'Information
- DLL: Dynamic Link Library
- DM/RCD: Déclaration de Matériel / Rapport de Conformité Déclarée
- DNS: Domain Name System
- DoS: Denial of Service
- DS: Distribution System
- DSSS: Direct Sequence Spread Spectrum
- DTR: Direction Technico-Réglementaire

E

- EAP: Extensible Authentication Protocol
- EAP-AKA: Extensible Authentication Protocol - Authentication and Key Agreement
- EAP-FAST: Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling
- EAP-MD5: Extensible Authentication Protocol - Message-Digest Algorithm 5
- EAP-SIM: Extensible Authentication Protocol - Subscriber Identity Module
- EAP-TLS: Extensible Authentication Protocol - Transport Layer Security
- EAP-TTLS: Extensible Authentication Protocol - Tunneled Transport Layer Security
- EPIC : Établissement Public à Caractère Industriel et Commercial
- ESS: Extended Service Set
- ESSID: Extended Service Set Identifier

F

- FHSS: Frequency Hopping Spread Spectrum

G

- 5G: 5e Génération
- Gb/s: Gigabits par seconde
- GHz: Gigahertz
- GSM: Global System for Mobile Communications

H

- HiperLAN2: High-Performance Radio Local Area Network 2
- HR-DSSS: High Rate Direct Sequence Spread Spectrum
- HMAC: Hash-Based Message Authentication Code

I

- IBSS: Independent Basic Service Set
- IDEA: International Data Encryption Algorithm
- IEEE: Institute of Electrical and Electronics Engineers
- IP: Internet Protocol
- IPsec: Internet Protocol Security
- IR: Infra Rouge
- IT: Information Technology

L

- LDAP: Lightweight Directory Access Protocol
- LLC: Logical Link Control
- LTE: Long-Term Evolution

M

- MAC: Medium Access Control
- Mbps: Megabits par seconde
- MD5: Message-Digest Algorithm 5
- MHz: Megahertz
- MIC: Message Integrity Code
- MITM: Man-in-the-Middle
- MU-MIMO: Multi-User Multiple Input Multiple Output

N

- NAS: Network Access Server
- NAV: Network Allocation Vector

O

- OFDM: Orthogonal Frequency Division Multiplexing
- ORSEC: Organisation des Secours
- OSI: Open Systems Interconnection

P

- PAC: Protected Access Credential
- PAP: Password Authentication Protocol
- PBKDF2: Password-Based Key Derivation Function 2
- PCF: Point Coordination Function
- PCH: Pharmacie Centrale des Hôpitaux
- PEAP: Protected Extensible Authentication Protocol
- PHY: Physical Layer
- PMD: Physical Medium Dependent
- PMI: Physical Medium Independent
- PSK : Pre-shared Key

Q

- QHSE: Qualité Hygiène Sécurité Environnement
- QoS: Quality of Service

R

- RADIUS: Remote Authentication Dial-In User Service
- RC4: Rivest Cipher 4
- RH : Ressources Humaines
- RSA: Rivest-Shamir-Adleman
- RSF : Réseau Sans Fil
- RTS: Request To Send

S

- SAP: Service Access Point
- SHA: Secure Hash Algorithm
- SIFS: Short Interframe Space
- SIE: Système d'Information d'Entreprise
- SNAP: Subnetwork Access Protocol
- SQL: Structured Query Language

T

- TACACS+: Terminal Access Controller Access-Control System Plus
- TKIP: Temporal Key Integrity Protocol

U

- UDP: User Datagram Protocol
- UMTS: Universal Mobile Telecommunications System

V

- VLAN: Virtual Local Area Network
- VPN: Virtual Private Network

W

- WEP: Wired Equivalent Privacy
- Wi-Fi: Wireless Fidelity
- WPA: Wi-Fi Protected Access
- WPA2: Wi-Fi Protected Access 2
- WPA3: Wi-Fi Protected Access 3

Liste des figures

Liste des figures

Liste des tableaux

Table des matières

Chapitre 2 : Sécurité des réseaux sans-fil

Chapitre 3 : Présentation de l'organisme d'accueil

Chapitre 4 : Mise en œuvre d'une solution de sécurisation d'un réseau sans fil basée sur le contrôle d'accès et l'authentification.

Introduction générale

D'après une étude récente, près de 60 % des entreprises ont subi une attaque visant leur réseau Wi-Fi [62]. Dans un contexte de dépendance croissante aux technologies numériques pour leurs activités quotidiennes, les entreprises sont confrontées à une diversité de menaces [63]. Les cyberattaques sont en nette augmentation, allant de l'écoute clandestine à des attaques actives telles que le déni de service (DDoS) ou l'usurpation d'identité [64].

Les risques associés aux réseaux sans-fil sont accentués par la complexité croissante des architectures réseau, la diversité des terminaux connectés et l'évolution des techniques d'attaque. La sécurité des réseaux représente un enjeu stratégique majeur, d'autant plus que les cybercriminels peuvent agir à distance sans accès physique, dès lors que le réseau sans-fil est accessible [65].

Les réseaux sans-fil, notamment ceux conformes à la norme IEEE 802.11, offrent une flexibilité et une mobilité accrues en permettant la transmission de données sans câblage physique. Cette technologie facilite l'interconnexion des dispositifs au sein des entreprises, réduisant les contraintes d'installation et favorisant la connectivité dans des environnements variés. Toutefois, la nature même des communications sans-fil, basées sur des transmissions par ondes hertziennes accessibles à tout appareil à portée, les rend particulièrement vulnérables [66].

Par conséquent, les solutions de sécurité sans-fil sont de plus en plus sollicitées afin de garantir la confidentialité, l'intégrité, la disponibilité, la traçabilité, le contrôle d'accès et l'authentification des données.

Par ailleurs, les protocoles de sécurité des réseaux jouent un rôle essentiel dans la protection des données circulant sur les réseaux. Leur mise en œuvre a permis de faire face aux nombreuses menaces et vulnérabilités potentielles [66]. Des protocoles spécifiques tels que RADIUS (Remote Authentication Dial-In User Service) développé par Livingston Enterprises [67], ainsi que des standards de sécurité comme WPA2 (Wi-Fi Protected Access 2), accompagnés de solutions cryptographiques avancées, sont aujourd'hui indispensables pour répondre aux exigences des environnements professionnels. Ils renforcent la sécurité des réseaux d'entreprise en centralisant la gestion des politiques de sécurité et en assurant une authentification centralisée. Cela signifie que les utilisateurs doivent s'identifier une seule fois pour accéder à l'ensemble des ressources du réseau d'entreprise. Le protocole RADIUS est utilisé pour authentifier et autoriser l'accès aux ressources réseau [68], y compris les serveurs, les routeurs, les contrôleurs LAN sans-fil (WLC) et les points d'accès (AP) sans-fil. Il facilite la gestion des règles de sécurité et l'attribution des ressources.

Le choix d'une méthode et d'une architecture d'authentification peut s'avérer complexe en raison du grand nombre de solutions disponibles [69]. Ce choix peut être fortement influencé par les informations préexistantes relatives aux utilisateurs. Dans ce mémoire, nous nous intéressons spécifiquement à l'authentification basée sur RADIUS. Cette thématique est développée en quatre chapitres.

- Dans le premier chapitre, nous présentons les principes généraux des réseaux sans-fil, notamment leur architecture et leurs modes de fonctionnement, tels que les modes ad hoc et le mode infrastructure. Nous explorons également la pile protocolaire d'un RSF avec la couche liaison de données (LLC) et la couche physique (PMD).

- Le deuxième chapitre est dédié à la sécurité des réseaux sans-fil. Nous analysons les risques et les attaques auxquels ces réseaux sont exposés, en distinguant notamment les attaques passives et actives. Ensuite, nous présentant des solutions visant à renforcer la sécurité de ces réseaux sans-fil, en assurant l'intégrité des données, la non-répudiation, la confidentialité, la traçabilité, contrôle d'aces et l'authentification.
- Dans le troisième chapitre, nous présentons l'organisme d'accueil de ce mémoire, la Pharmacie centrale des hôpitaux (PCH). Nous définissons la PCH en décrivant sa localisation, ses objectifs, ses missions et ses principales activités. Nous abordons également l'architecture du réseau de son client et les problématiques auxquelles il est confronté.
- Le quatrième chapitre concerne la réalisation et les tests. Nous détaillons l'environnement de développement utilisé, ainsi que les différentes étapes de simulation du réseau réalisée avec Cisco Packet Tracer. Nous présentons également les tests effectués pour vérifier le bon fonctionnement de l'authentification basée sur serveur RADIUS.

Enfin, une conclusion générale résumera les principaux apports de ce mémoire.

Chapitre 1 : Généralité sur les réseaux sans fil

Introduction

Un réseau sans fil (en anglais Wireless network) est une infrastructure de communication qui permet la transmission de données entre des appareils électroniques sans avoir besoin de câbles physiques [1] ce qui facilite l'installation et la maintenance dans des environnements où le câblage est difficile ou impossible.

Les communications s'effectuent à l'aide d'ondes hertziennes dans laquelle le client est quasi immobile dans la cellule où il se trouve. S'il sort de sa cellule, la communication est interrompue [2, p. 395]. Toutefois, la notion de ***roaming*** qui permet de contourner ce problème par la norme ***IEEE 802.11f***, en assurant une continuité de service entre plusieurs points d'accès (APs).

Lorsqu'un appareil se connecte à un réseau sans fil, une liaison est établie entre l'appareil et le point d'accès sans fil, qui assure la transmission et la réception des signaux radio [1].

De plus, il existe de nombreux types différents de réseaux sans fil sur une gamme de technologies telles que ***Bluetooth, ZigBee, LTE et 5G***, tandis que le Wi-Fi est spécifique au protocole sans fil défini par l'Institute of Electrical and Electronic Engineers (IEEE) dans la norme 802.11 et ses amendements [3]. Cette technologie permet aux particuliers, aux entreprises et aux opérateurs de télécommunications de réduire, voire d'éliminer, l'usage de câbles pour connecter différents emplacements.

Ce chapitre se concentre sur divers aspects fondamentaux des réseaux sans fil, notamment leur architecture. Nous examinerons également les différents modes de topologie sans fil, à savoir le mode infrastructure et le mode ad-hoc. Nous aborderons la pile protocolaire des réseaux sans fil composée d'une physique (PHY) et d'une couche liaison de données (DLL), et en détaillant leurs sous-couches. Enfin, nous examinerons l'importance de la méthode d'accès dans un environnement sans fil, en mettant l'accent sur la norme IEEE 802.11.

Figure 1 : Composition d'un réseau wifi [16, p. 8].

1. Architecture des Réseaux sans fil IEEE 802.11

L'architecture d'un réseau sans fil est cellulaire. Elle est essentielle pour concevoir, déployer et gérer efficacement d'un réseau sans fil. Elle définit la structure et l'organisation des composantes qui le constituent comme elle englobe les différents éléments matériels et logiciels, ainsi que leurs interactions. Un groupe de terminaux munis d'une carte d'interface réseau 802.11, s'associent pour établir des communications directes et forment un BSS (Basic Set Service). Figure 1.1 illustre l'architecture réseau sans fil :

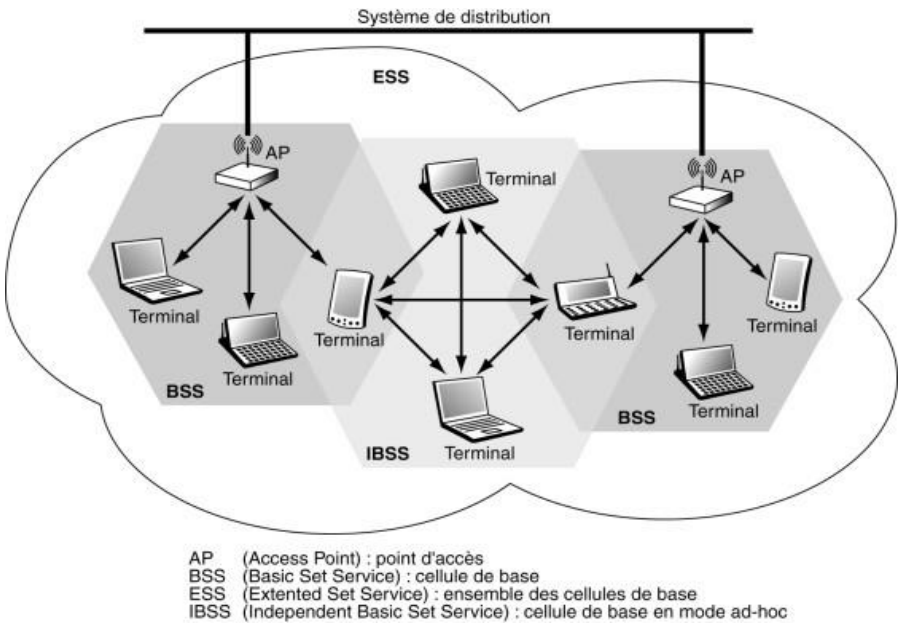

Figure1.1 : Architecture Réseau sans fil [2, p. 398].

Lorsque le réseau est composé de plusieurs BSS, chacun d'eux est relié à un système de distribution, ou DS (Distribution System), via un point d'accès (AP). Le DS, généralement un réseau Ethernet avec câble métallique, transfère des paquets entre les stations de base. Un ensemble de BSS interconnectés par un DS forme un ESS (Extended Service Set).

Le DS est indépendant de la structure hertzienne et peut utiliser des connexions hertziennes. Il peut également inclure une passerelle vers un réseau fixe (ex. Internet), permettant de connecter le réseau 802.11 à d'autres réseaux IEEE 802.x.

Le système de distribution (DS) est responsable du transfert des paquets entre les différentes stations de base. Dans les spécifications du standard, le DS est implémenté de manière indépendante de la structure hertzienne et utilise un réseau Ethernet métallique. Il pourrait tout aussi bien utiliser des connexions hertziennes entre les points d'accès. Sur le système de distribution il est possible de placer une passerelle d'accès vers un réseau fixe, tel qu'Internet. Cette passerelle permet de connecter le réseau 802.11 à un autre réseau. Si ce réseau est de

type IEEE 802.x, la passerelle incorpore des fonctions similaires à celles d'un pont [2, p. 395].

2. Les modes de fonctionnement

Les réseaux sans fil peuvent être configurés pour opérer de différentes façons, dont les plus communs sont les modes « ad hoc » et « infrastructure ». Ces deux modes peuvent se diviser en trois configurations différentes :

- « Independent Basic Service Set » (IBSS)
- « Basic Service Set » (BSS)
- « Extended Service Set » (ESS) [4].

2.1 Ad Hoc

Mode Ad-Hoc aussi connu sous le nom de Mode IBSS (Independent Basic Service Set) est un réseau sans infrastructure (aucune station fixe) qu'est un réseau autonome de nœuds mobiles dans ce mode chaque ordinateur fait office d'émetteur et de récepteur. La connexion entre chaque ordinateur ne nécessite aucun matériel particulier à part une carte réseau Wifi [5]. Ce mode est très pratique dans le cas d'une connexion rapide entre ordinateurs.

Cependant, ce mode est moins sécurisé que le mode infrastructure, car il n'existe pas de point central pour contrôler la sécurité du réseau. Chaque périphérique sans fil doit donc être configuré individuellement pour garantir des niveaux de sécurité élevés, ce qui peut être difficile et fastidieux. En outre, le mode Ad-hoc a une portée limitée, ce qui implique que les périphériques doivent être situés à proximité les uns des autres pour se connecter [6]. Figure 1.2 illustre l'architecture du mode Ad-Hoc :

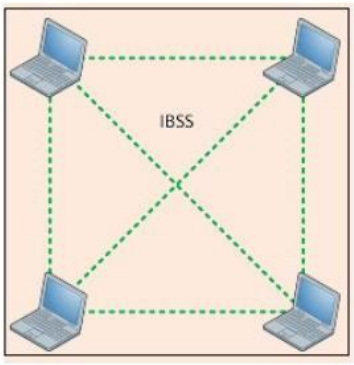

Figure 1.2: Architecture Ad-Hoc [17, p. 4].

2.2 Infrastructure

Mode infrastructure aussi connu sous le nom de Mode BSS (Basic Service Set) : Réseau avec station de base fixes (Mobiles Station Support) couvrant chacune une zone géographique limitée. Pour fonctionner, ce mode a besoin d'un point d'accès (AP) [2, p. 398] qui peut par exemple être un routeur Wifi. Chaque ordinateur à l'aide de sa carte réseau va se connecter à cet AP.

Le mode infrastructure, en revanche, offre une meilleure sécurité que le mode Ad-hoc, car tous les périphériques sans fil sont reliés à un point central de contrôle. Cela permet de configurer et de gérer les paramètres de sécurité de manière centralisée, ce qui facilite la mise en place de niveaux de sécurité élevés. Par ailleurs, le mode infrastructure a une portée plus large, permettant aux appareils de communiquer sur une plus grande distance comparée au le mode Ad-hoc [6]. Figure 1.3 illustre l'architecture du mode infrastructure :

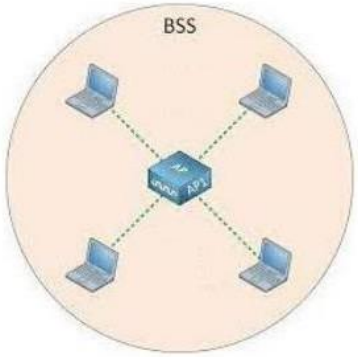

Figure 1.3 : Architecture Infrastructure [17, p. 4].

3. Pile protocolaire

3.1 Définition

Une pile de protocoles est un groupe de protocoles réseau organisés qui collaborent pour faciliter la communication entre divers appareils connectés à un réseau. Cette pile est divisée en différentes couches, chacune ayant un rôle spécifique dans l'envoi et la réception de données. Cette structuration en couches permet une transmission efficace, ordonnée et fiable des informations, tout en garantissant une séparation claire des différentes fonctions [7].

3.2 Structure de la Pile de Protocoles

La pile de protocole repose sur un ensemble de protocoles organisés en différentes couches, où chacune ayant un rôle spécifique. Cette structuration en couches facilite la collaboration entre les niveaux afin d'assurer une transmission fiable des données entre les appareils. Les données circulant par une série d'étapes lors de l'émission pour s'assurer qu'elles sont bien transmises et reçues correctement [7].
La norme IEEE 802.11 définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Cette dernière est divisée en deux sous-couches complémentaires, la sous-couche LLC (Logical Link Control) et la sous-couche MAC (Medium Access Control) [8]. La figure 1.4 représente le modèle en couches de IEEE 802.11 :

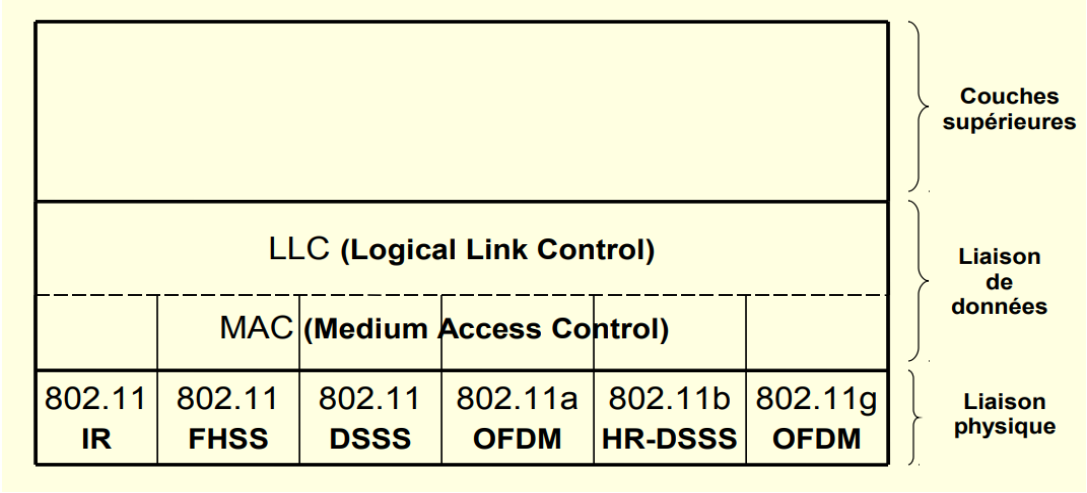

Figure1.4 : Modèle en couches de IEEE 802.11 [11, p. 66].

3.2.1 Couche liaison de données

La couche de liaison de données (DLL) permet de transférer des données sur le support physique en le divisant en paquets. Elle ajoute des en-têtes, qui contient notamment les adresses physiques des dispositifs, ainsi que des queues, qui comportent un code de contrôle d'erreur appelé CRC, ajouté par la sous-couche MAC. Ces ajouts permettent de fournir un mécanisme efficace de contrôle des erreurs et de gestion du flux.

a. Sous couche MAC

Couche de contrôle d'accès au support, elle gère l'accès au support physique pour les stations sans fil et les points d'accès [9]. Elle utilise le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pour éviter les collisions de paquets lors de l'accès simultané au support physique [10].

i. **Méthode d'accès**

Dans le domaine filaire d'Ethernet, le protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) est utilisé pour réguler les accès au support et de détecter les collisions qui se produisent. Dans les réseaux Wi-Fi, la détection des collisions n'est pas possible, en raison de la nature du support de transmission. En effet, la détection de collision exige de la station la simultanéité de l'émission et de la réception [11]. Si une collision se produit, la station continuera à transmettre la trame au complet, ce qui entraîne une forte baisse de performance du réseau.

Le protocole CSMA/CA : Utilise un mécanisme d'évitement de collision basé sur un principe d'accusés de réception (ACK) réciproques entre l'émetteur et le récepteur. Il gère très efficacement les interférences et autres problèmes radio. Deux méthodes d'accès au canal basées sur CSMA/CA ont été mises en œuvre pour les réseaux 802.11: la DCF (Distributed Coordination Function) et la PCF (Point Coordination Function).

La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors la station peut émettre. La station transmet un message appelé Ready To Send (ou Request To Send, noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un Clear To Send (CTS, signifiant le champ est libre pour émettre), puis la station commence l'émission des données.

À réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent alors pendant un temps qu'elles considèrent être nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée [12, pp. 294-295]. La figure 1.5 illustre le processus de transmissions des trames :

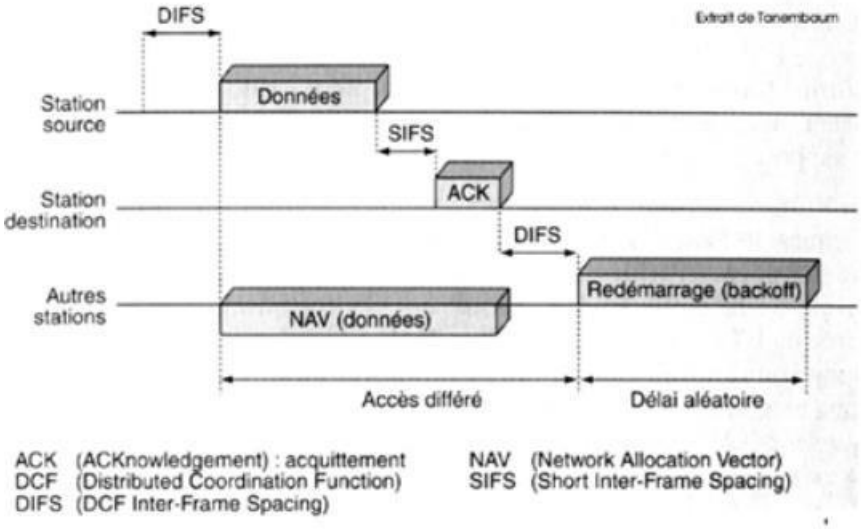

Figure 1.5: Processus de transmission des trames [18].

b. Sous couche LLC

Offre les mêmes fonctionnalités, quel que soit la sous-couche MAC, permet l'´établissement d'un lien logique [9]. Principalement, elle joue le rôle de SAP (Service Access Point), ce qui permet d'assurer le multiplexage des protocoles en utilisant l'encapsulation SNAP (Subnetwork Access Protocol), i.e. permettre à plusieurs protocoles de communiquer sur le même support physique.

3.2.2. Couche physique

La couche physique a pour rôle principal d'établir et de maintenir le lien radio ou infrarouge pour permettre la transmission de données sans fil entre les stations composant le réseau. Pour ce faire, elle propose certaines primitives à la couche supérieure. En particulier, elle offre à la couche MAC des primitives lui permettant de tester l'état – occupé ou disponible – du canal

radio ou infrarouge ou bien encore de savoir si une transmission ou une réception vient de commencer ou de se terminer, etc.

Afin de garantir à la couche MAC une dépendance moindre vis-à- vis de la couche physique, une sous-couche de convergence servant d'interface entre les deux a été définie. La couche physique se décompose en deux parties : la sous couche PMD et la sous-couche PMI.

a. **La sous-couche basse (sous-couche PMD, Physical Medium Dependent)** : assure la transmission des données (bits) sur les supports.
b. **La sous-couche supérieure (PMI, Physical Medium Independent)** : assure la détection de présence d'un signal, le codage et la récupération de l'horloge (synchronisation) [13].

La norme IEEE 802.11 utilise trois techniques de transmission : Infra rouge, FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) et elle utilise deux techniques additionnelles haut-débit : OFDM (Orthogonal Frequency Division Multiplexing) jusqu'à 54 Mbps et HR-DSSS (High Rate Direct Sequence Spread Spectrum) jusqu'à 11 Mbps [11, p. 67]

4. Les différentes normes IEEE802.11

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Tableau (1.1) présente les différentes révisions de la norme 802.11 et leur signification [14] [15] :

Nom de la norme	Nom	Description
802.11be	Wifi7	Les fonctionnalités du Wi-Fi 7 de la norme 802.11be s'appuient et améliorent les générations Wi-Fi antérieures. Cela signifie donc des vitesses encore plus rapides, jusqu'à 46 Gb/s, mais aussi une réactivité et une fiabilité considérablement améliorée. Il utilise des canaux de 320 MHz, ce qui permet de rassembler encore plus de données lors de chaque transmission (débit théorique doublé).
802.11ax-2021	Wi-Fi 6E	La norme 802.11ax-2021 elle utilise une troisième bande de fréquences Wi-Fi, avec une bande passante de 500 MHz dans les 6 GHz. Il s'agit de la plus grande allocation de spectre et elle triple presque le spectre disponible pour le Wi-Fi. Grâce à cette incursion dans la bande des 6 GHz, la connectivité Wi-Fi franchit un nouveau palier, avec plus de capacités, des canaux plus larges et moins d'interférences.
802.11ax	Wi-Fi 6	La norme 802.11ax est compatible avec les deux bandes de fréquences 2,4 GHz et 5 GHz, il a une meilleure portée que le Wi-Fi 5, de l'ordre de 70 mètres. En outre, grâce à l'OFDMA, une technique qui permet de diviser le canal Wi-Fi lorsqu'il communique avec plusieurs appareils, et aux améliorations apportées à la technologie MU-MIMO (8 flux), il permet de faire passer le débit maximum théorique en Wi-Fi jusqu'à 9,6 Gb/s, soit une augmentation de 40% du débit en Wi-Fi.
802.11a	Wifi5	La norme 802.11a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence de 5 GHz.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d (bridging)	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d en pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.

802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau.
802.11g		La norme 802.11g offrira un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. Cette norme vient d'être validée. La norme 802.11g a une compatibilité ascendante avec la norme b.
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose le chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11IR		La norme 802.11j a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme 802.11j est à la réglementation japonaise ce que le 802.11 est à la réglementation européenne.

Tableau 1.1 : Les différentes révisions de la norme 802.11 et leur signification.

Conclusion

Dans ce chapitre, nous avons examiné en détail la norme 802.11, qui forme la base d'un réseau sans fil. Nous avons abordé les notions fondamentales, soulignant les modes de fonctionnements. Nous avons également étudié le modèle protocolaire en décrivant les couches physiques et liaison de données, avec leurs sous-couches respectives. La méthode d'accès CSMA / CA a été examinée dans le cadre des normatives IEEE 802 .11, qui est cruciale pour la gestion des collisions dans les communications sans fil. Alors que nous entamons le deuxième chapitre axé sur la sécurité des réseaux IEEE 802.11, il est essentiel de comprendre que la maîtrise des bases techniques des réseaux sans fil est cruciale pour relever les défis de sécurité qui en découlent. Protéger les données et assurer la sécurité des communications sans fil. Ainsi, dans le prochain chapitre, nous analyserons sur les attaques et les risques auxquels ces réseaux sont exposés ainsi que les solutions visant à garantir l'intégrité, la confidentialité, l'authentification et le contrôle d'accès

Chapitre 2 : Sécurité dans les réseaux IEEE.802.11

Introduction

La sécurité des réseaux sans fil repose sur l'ensemble des technologies, protocoles et règles mises en place pour protéger les échanges et garantir que seules les personnes autorisées puissent accéder au réseau. Elle vise à préserver la confidentialité, l'intégrité et la disponibilité des données face aux menaces et les accés non autorisés.Cette sécurisation inclut l'élaboration et l'application de politiques de sécurité, le déploiement de solutions cryptographiques avancées [19].

1. Risques et Attaques

Les risques et attaques informatiques désignent les menaces visant à compromettre la sécurité des systèmes et des données, et pour se protéger contre ces menaces, il est crucial de mettre en place des stratégies de cybersécurité efficaces.

1.1 Les Risques

Les risques informatiques représentent l'ensemble des menaces provenant de techniques, de pratiques et de programmes informatiques malveillants et ayant pour seul but de saboter, brouiller, détruire nuire ou voler les données et les ressources d'un système informatique d'une entreprise [20].

- **Risques physiques :** L'accès non autorisé aux câbles d'un réseau informatique peut entraîner l'interception de données sensibles, la manipulation des câbles pour altérer le trafic et l'injection de données malveillantes. Ces risques sont liés à l'accès physique aux infrastructures réseau et peuvent affecter la confidentialité, l'intégrité et la disponibilité des données.
- **Risques réseau :** Il désigne les menaces qui affectent la sécurité des données lorsqu'elles circulent sur un réseau informatique comme l'espionnage, l'interception, la modification ou le blocage des informations.
- **Risques système (exploitation) :** Ils concernent la sécurité des systèmes d'exploitation et des logiciels associés. Ils incluent les vulnérabilités logicielles, les erreurs de configuration, les failles de sécurité connues, les faiblesses des mots de passe et d'autres problèmes qui peuvent compromettre la sécurité des systèmes.
- **Risques d'information :** Ils touchent la confidentialité et l'intégrité des données stockées et échangées. Ils incluent l'accès non autorisé aux données sensibles, les fuites d'informations, le vol d'identité, et la divulgation d'informations confidentielles, mettant ainsi en danger la protection des données personnelles et d'entreprise.
- **Risques d'application :** Ils sont spécifiques aux applications logicielles utilisées dans les systèmes informatiques. Ils incluent les vulnérabilités des applications, les erreurs de programmation, les attaques par injection de code (comme les attaques par SQL injection), et les failles dans les interfaces utilisateur, qui peuvent être exploitées pour compromettre la sécurité des applications [21].
- **Risques organisationnels :** Ces risques sont liés à la gestion de la sécurité au sein d'une organisation. Ils incluent des politiques de sécurité inefficaces, des procédures de sauvegarde et de récupération inadéquates**,** des erreurs une formation insuffisante du personnel**,** humaines, et le non-respect des politiques de sécurité**,** qui peuvent affaiblir la protection de l'ensemble de l'organisation.

1.2 Les Attaques

Les réseaux sans fil, tels que le Wi-Fi et le Bluetooth, permettent la transmission de données entre différents dispositifs sans recours à un câblage physique. Ils sont encadrés par des normes spécifiques, notamment la norme IEEE 802.11 pour le Wi-Fi. Leur fonctionnement repose principalement sur un point d'accès, qui assure la connexion des appareils à Internet ou à un autre réseau, sans liaison filaire. Bien que cette architecture flexible facilite leur utilisation, elle les expose davantage aux risques de sécurité. Sur le plan conceptuel, ces attaques peuvent être classées en deux catégories : les attaques actives et les attaques passives [22].

1.2.1 Les attaques actives

L'attaquant tente de modifier l'information ou crée un faux message. La prévention de ces attaques est assez difficile en raison d'un large éventail de vulnérabilités physiques, de réseaux et de logiciels. Au lieu de la prévention, la stratégie de sécurité met l'accent sur la détection de l'attaque et la récupération de toute perturbation ou retard causé par celui-ci. Figure 2.1 Illustration d'une attaque active

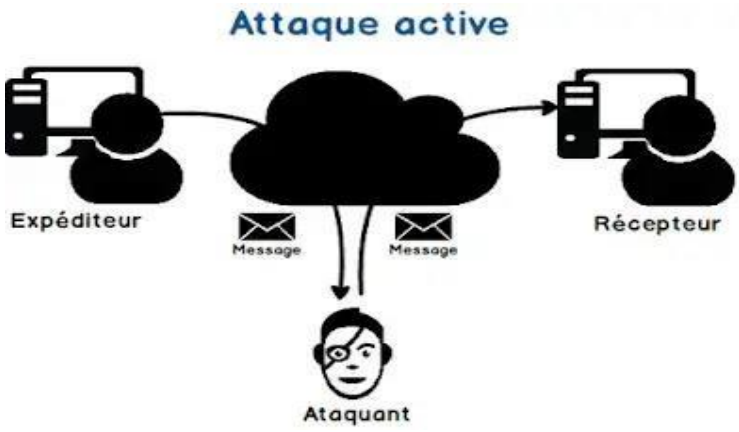

Figure 2.1 : Illustration d'une attaque active [22].

- **Exemples d'attaques actives dans les réseaux sans-fil**

- **DoS wifi :** est une attaque de dénis de service (Denial of Service ou DoS en anglais), elle consiste à rendre un service inutilisable par ses utilisateurs potentiels. Le service généralement fourni par le Wi-Fi est la mise à disposition d'une connectivité réseau à des appareils. Une attaque DoS va ainsi viser à rendre ce lien de connectivité inopérant et peut être implémentée de différentes manières, par exemple en épuisant une ressource nécessaire à fournir le service, ou en exploitant des fonctionnalités du service [23]. Figure 2.2 Principe d'une attaque DoS sur le Wi-Fi

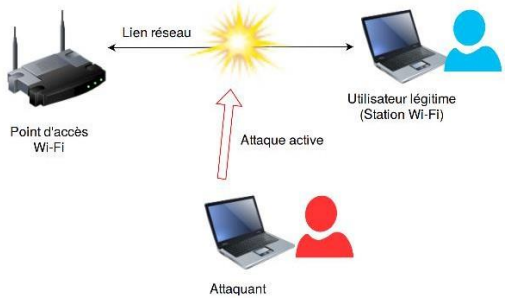

Figure 2.2 *:* Principe d'une attaque DoS sur le Wi-Fi [23].

- **Injection des paquets (modification DNS) :** Permet aux utilisateurs d'injecter des paquets personnalisés dans les réseaux sans fil. En injectant ces paquets, les utilisateurs peuvent effectuer différents types d'attaques et de tests de sécurité sur les réseaux sans-fil. C'est une forme d'attaque de MITM : écoute du port UDP 53, l'attaquant intercepte les paquets et injecte des réponses DNS falsifiées [24].

- **Rogue DHCP :** Une attaque DHCP (Dynamic Host Configuration Protocol) est une menace informatique où un attaquant compromet un serveur DHCP ou manipule le protocole pour distribuer des adresses IP malveillantes ou des paramètres de configuration aux dispositifs du réseau. Cela peut entraîner divers risques de sécurité, notamment l'interception de trafic, le vol de données et l'accès non autorisé à des informations sensibles [25].

- **Craquage des mots de passe :** est le processus qui consiste à obtenir un accès non autorisé à des systèmes restreints en utilisant des mots de passe communs ou des algorithmes qui devinent les mots de passe [26].

1.2.2. Les Attaques Passives

Sont les attaques où l'attaquant se met en écoute non autorisée, en surveillant simplement la transmission ou la collecte d'informations. L'oreille indiscrète n'apporte aucun changement aux données ou au système [22]. Figure 2.3 Illustration attaque passive

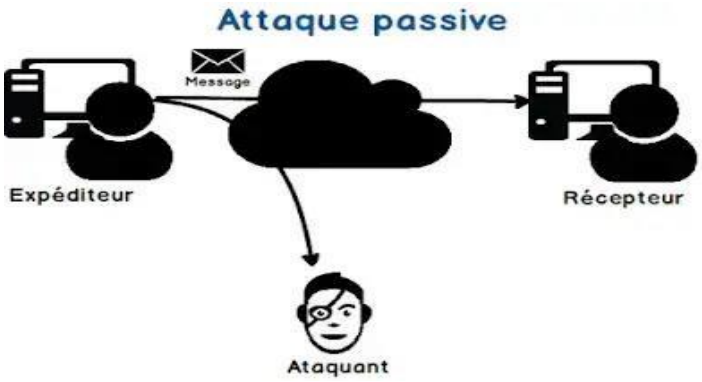

Figure 2.3 : Illustration attaque passive [22].

- **Exemples d'attaques passives dans les réseaux sans-fil**

• **MAC Spoofing :** est une attaque cybernétique où un attaquant se fait passer pour un dispositif légitime sur un réseau en falsifiant son adresse Media Access Control (MAC). L'adresse MAC est un identifiant unique attribué à une interface réseau, et en la falsifiant, les attaquants peuvent contourner les mesures de sécurité du réseau et obtenir un accès non autorisé au réseau [27].

• **Man in the middle (MITM) :** est un type de cyberattaque où les attaquants interceptent une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime. Pour la victime, il semblera qu'un échange standard d'informations est en cours, mais en s'insérant au « milieu » de la conversation ou du transfert de données, l'attaquant peut discrètement détourner des informations [28].

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. Figure 2.4 Attaque Man-in-the-middle (MITM)

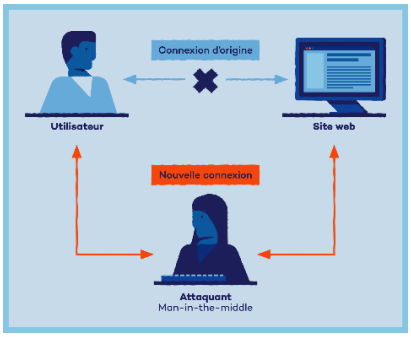

Figure 2.4: Attaque Man-in-the-middle (MITM) [28].

Critères de comparaison	Attaque active	Attaque passive
De base	Une attaque active tente de modifier les ressources du système ou d'effectuer leur fonctionnement.	L'attaque passive tente de lire ou d'utiliser les informations du système mais n'influence pas les ressources du système.
Nuire au système	Cause toujours des dommages au système.	Ne provoque aucun mal.
Modification de l'information	Se produit	N'a pas lieu
Menace à	Intégrité et disponibilité	Confidentialité
Tache effectuée par l'attaquant	La transmission est capturée en contrôlant physiquement la partie d'un lien.	Juste besoin d'observer la transmission.

Tableau 2.1 : Table de comparaison entre attaque active et passive [22].

2. Les solutions :

Dans cette partie, nous allons aborder les aspects essentiels de la sécurité des réseaux sans fil pour se protéger des menaces.

2.1 Intégrité des données :

Dans certains cas, il peut être nécessaire d'assurer simplement que les données sont intégrés, c'est-à-dire qu'elles n'ont pas été au passage falsifiées par un intrus. Ces données restent claires, au sens où elles ne sont pas secrètes [29].Pour assurer l'intégrité des données dans les réseaux sans fil, différentes techniques peuvent être utilisées, telles que :

2.1.1 Cryptage (chiffrement) :

Le chiffrement consiste à rendre un texte incompréhensible en le codant. On code (crypte ou chiffre) le texte en effectuant une opération sur le texte en clair à partir d'une règle appelée clé de chiffrement. Le texte codé (cryptogramme) peut alors être envoyé à son destinataire, cryptage symétrique et asymétrique sont les deux techniques utilisées pour préserver la confidentialité de votre message [30].

- **Le cryptage symétrique** utilise toujours une seule clé pour le cryptage et le décryptage du message.
- **Le cryptage asymétrique** l'expéditeur utilise la clé publique pour le cryptage et la clé privée pour le déchiffrement [30].

	Cryptage Symétrique	**Cryptage Asymétrique**
Définition	Le cryptage symétrique utilise une seul clé pour le cryptage et déchiffrement.	Le cryptage asymétrique utilisé une clé différent pour le cryptage et décryptage.
Performance	Le cryptage symétrique est rapide en exécution.	Le cryptage asymétrique est lent à l'exécution en raison de la charge en calcul élevée.
Algorithmes	AES, DES, DES3 et RC4	Diffie-Hellman, RSA
Objectif	Le cryptage symétrique est utilisé pour la transmission des données en masse.	Cryptage asymétrique est souvent utilisé pour l'échange des clés secrètes.

Tableau 2.2 : Comparaison des deux types de Cryptage symétrique et asymétrique [30].

2.1.2 Hashage : en anglais (hashing), ou hachage en français, est une méthode utilisée en informatique pour convertir n'importe quelle donnée en une chaîne de caractères de taille fixe, appelée empreinte numérique ou encore « hash ». Cette technique permet d'assurer l'intégrité des données transmises ou stockées [31]. De nombreux types de programmes différents peuvent transformer le texte en hachage, et ils fonctionnent tous de manière quelque peu différente. Parmi les algorithmes de hachage les plus répandus**,** on trouve :

- **MD5 :** Est l'abréviation de 'Message-Digest algorithme 5'. Un algorithme MD5 est une fonction de hachage cryptographique qui prend une chaîne de n'importe quelle longueur en entrée et produit une valeur de hachage de 128 bits en sortie. La valeur de hachage est une chaîne de 32 caractères de chiffres hexadécimaux qui peut être utilisée pour représenter les données d'entrée [32].

- **SHA :** (acronyme de Secure Hash Algorithm), Le terme “SHA” fait référence à un algorithme de hachage sécurisé. Il s'agit d'une version modifiée de MD5 et est utilisée dans le but de hacher des données et des certificats [33].
- **PBKDF2 :** (Password-Based Key Derivation Function) est une fonction de dérivation de clé, appartenant à la famille des normes Public Key Cryptographic Standards, Cette norme est aujourd'hui utilisée pour le hachage de mot de passe (associé à des fonctions comme SHA-256) ou la génération de clé de chiffrement de données [34].
- **HMAC :** (Hash-Based Message Authentication Code) est une technique d’authentification cryptographique qui utilise une fonction de hachage et une clé secrète [35].

2.2 Confidentialité : Empêcher la divulgation d’informations à des entités non autorisées à les connaître. Les entités peuvent être des sites, organisations, personnes, etc [36].

2.2.1 Chiffrement : Le processus de transformation d’une information de manière à la rendre incompréhensible. Il existe deux classes principales d’algorithmes de chiffrement :

- **Le chiffrement symétrique :** Est un algorithme cryptographique qui utilise la même clé secrète pour le chiffrement et pour le déchiffrement d’un message [37]. Il s’agit d’une clé partagée. Figure 2.5 illustre le chiffrement symétrique,
  Voici quelques exemples d’algorithmes de chiffrement symétrique
  :

  - **DES (Data Encryption Standard)** : Est un algorithme de chiffrement par bloc. Il s’agit d’une ancienne méthode de cryptage qui a été remplacée par AES et 3DES. Elle utilise une clé de 56 bits [38].

  - **AES (Advanced Encryption Standard**) Est l’un des algorithmes de chiffrement symétrique les plus répandus pour protéger les données sensibles. L’algorithme AES repose sur le chiffrement de blocs de données de 128 bits [39].

  - **IDEA (International Data Encryption Algorithm) :** Un algorithme de chiffrement symétrique par blocs utilisé pour chiffrer et déchiffrer des données. Il manipule des blocs de texte en clair de 64 bits. Une clé de chiffrement longue de 128 bits (qui doit être choisie aléatoirement) est utilisée pour le chiffrement des données [40].

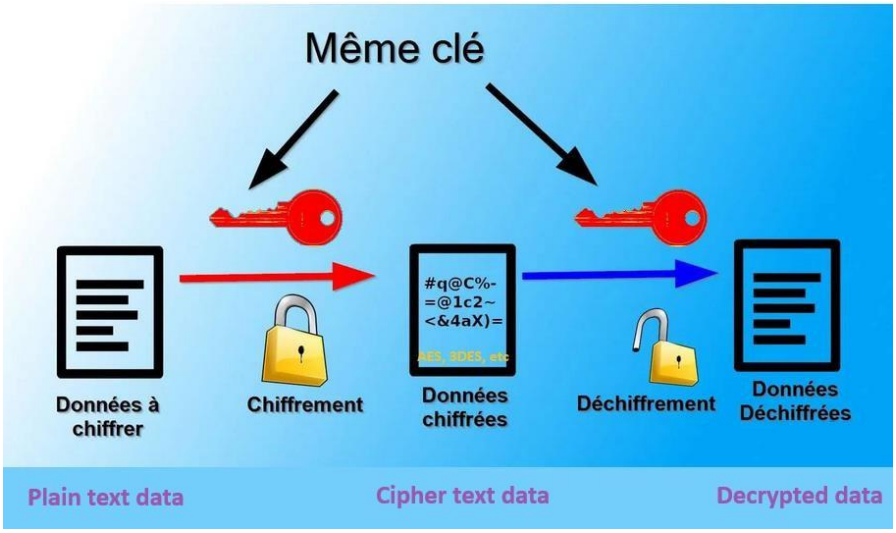

Figure 2.5 : Chiffrement symétrique [43].

Le Chiffrement asymétrique : est un algorithme cryptographique qui repose sur une clé privée et sur une clé publique. La clé publique est utilisée pour chiffrer un message, mais le message chiffré ne sera déchiffré que par la personne qui possède la clé privée. La clé publique est donc connue des tous, tandis que la clé privée doit rester secrète [41]. Figure 2.6 illustre le chiffrement asymétrique, L'un des algorithmes de cryptage asymétrique les plus répandus :

- **RSA :** RSA Security (Rivest-Shamir-Adleman) est un algorithme de chiffrement asymétrique largement utilisé basé sur les propriétés mathématiques des grands nombres premiers. Il est l'un des systèmes de cryptage à clé publique les plus courants, connu pour sa sécurité et sa polyvalence. Il est très sécurisé car il est très difficile de trouver les nombres premiers p et q à partir de n connu [42].

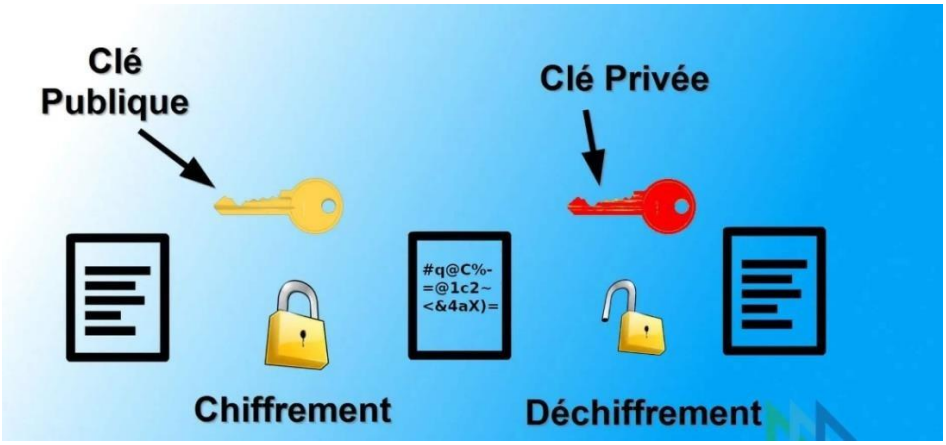

Figure 2.6 : Chiffrement asymétrique [43].

2.3 Traçabilité et non-répudiation

La traçabilité des données fait référence à la capacité de suivre l'origine, les mouvements et les modifications des données tout au long de leur cycle de vie. Elle permet de créer un historique détaillé des activités sur la collecte, le stockage, la transformation et le partage des données [44], Non-répudiation c'est empêcher les entités de démentir (nier) leurs actions

précédentes ou leurs engagements [36].

2.4 Authentification : Pour utiliser un réseau sans fil, les clients doivent d'abord découvrir ce qu'on appelle un ensemble de services de base, le BSS (Basic Service Set), afin de demander l'autorisation de s'y associer. Une fois cette découverte effectuée, les clients devront être « authentifiés » par le point d'accès. Cette authentification a pour but de vérifier l'identité de l'utilisateur ou de l'appareil qui se connecte au réseau [45].

L'authentification est un processus crucial dans la sécurité des réseaux sans fil, car elle permet de vérifier que l'entité qui souhaite se connecter au réseau est bien celle qu'elle prétend être. Dans ce cadre, le protocole AAA (Authentication, Authorization, Accounting ou Auditing) est un protocole ou un mécanisme servant à renforcer la sécurité d'accès aux ressources de l'entreprise en se passant par trois étapes :

- **Authentification :** Qui est autorisé à accéder ?
- **Autorisation :** Que peut faire la personne autorisée ?
- **Accounting** : Auditer en détail tout ce qui s'est passé [46].

Les deux principaux protocoles pour la communication entre un client et un serveur triple-A sont RADIUS et TACACS+. Toutefois nous pouvons mentionner d'autres, notamment DIAMETER, TACACS et LDAP [47].

2.4.1 Kerberos : Kerberos est un protocole d'authentification réseau qui utilise des « tickets » pour authentifier les utilisateurs et les services. IL est utilisé pour valider les clients/serveurs sur un réseau utilisant une clé cryptographique. Il est conçu pour exécuter une authentification forte tout en rendant compte aux applications [48].

2.4.2 DIAMÈTRE : Diameter est un protocole AAA plus récent, conçu pour remplacer RADIUS. Il offre des fonctionnalités plus avancées, notamment en termes de fiabilité, de sécurité et d'extensibilité [49].

2.4.3 LDAP : Signifie Lightweight Directory Access Protocol, est un protocole léger d'accès à l'annuaire. Il permet d'identifier les individus, les organisations et les autres appareils d'un réseau, qu'ils soient sur Internet public ou d'entreprise. Utilisé comme service d'annuaire, il constitue notamment la base du service Active Directory de Microsoft.

2.4.4 TACACS+ (Terminal Access Controller Access-Control System Plus) : ce système permet d'effectuer une authentification basée sur les adresses IP. Les dernières versions de ce protocole incluent le chiffrement. Il offre une plus grande sécurité et une plus grande flexibilité que RADIUS. TACACS+ sépare les fonctions d'authentification, d'autorisation et d'audit, ce qui permet une gestion plus fine des accès [49].

2.4.5 RADIUS : RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau qui centralise la gestion de l'authentification, de l'autorisation et de la comptabilité (***AAA***) pour les utilisateurs qui se connectent et utilisent un service réseau. RADIUS est principalement utilisé par les fournisseurs d'accès à Internet (***FAI***) et les organisations pour gérer l'accès à leurs réseaux, VPN et autres services d'accès à distance [50].

Le protocole RADIUS repose sur un modèle ***client-serveur***. Dans ce modèle, le *serveur RADIUS* gère les identifiants des utilisateurs, les règles d'accès et les informations de comptabilité, tandis que les *clients RADIUS*, également appelés serveurs d'accès réseau (***NAS***), sont les périphériques qui fournissent l'accès au réseau, tels que les routeurs, les commutateurs ou les passerelles VPN.

Le protocole RADIUS a trois fonctions principales :

- **Authentification :** processus de vérification des informations d'identification de l'utilisateur, telles que les noms d'utilisateur et les mots de passe. Lorsqu'un utilisateur tente de se connecter au réseau, le NAS envoie une demande d'accès au serveur RADIUS, qui vérifie les informations d'identification dans sa base de données. Si les informations d'identification sont valides, le serveur envoie un message d'acceptation d'accès au NAS, accordant l'accès à l'utilisateur ; sinon, il envoie un message de refus d'accès.
- **Autorisation :** Une fois l'utilisateur authentifié, le serveur RADIUS fournit au NAS un ensemble d'attributs définissant ses autorisations et ses paramètres d'accès réseau, tels que les adresses IP, les attributions de VLAN ou les paramètres de qualité de service (QoS). Le NAS applique ces politiques d'accès pendant la session de l'utilisateur.
- **Comptabilité :** le NAS envoie des informations de comptabilité, telles que la durée de la session, l'utilisation des données et les horodatages de connexion, au serveur RADIUS tout au long de la session de l'utilisateur. Ces informations sont utilisées pour la facturation, l'allocation des ressources et la surveillance de l'utilisation du réseau [50].

a. Principe de fonctionnement de Radius

RADIUS repose principalement sur un serveur (*le serveur RADIUS*) relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé *NAS* (Network Access Server) faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré. Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS, il traite les demandes d'authentification en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateurs, de machines ou de domaines. Il dispose pour cela d'un certain nombre d'interfaces ou de méthodes [51].

b. Scénario de fonctionnement

1. L'utilisateur souhaite accéder au réseau et envoie une demande de connexion contenant le nom d'utilisateur et le mot de passe au client RADIUS « Si PAP (Password Authentication Protocol) est adopté, sinon lance le défi si CHAP (Challenge Handshake Authentication Protocol) est adopté ».
2. Le client RADIUS envoie un paquet de demande d'accès contenant le nom d'utilisateur et le mot de passe au serveur RADIUS.
3. Le serveur RADIUS vérifie l'identité de l'utilisateur et peut répondre de plusieurs manières, selon la validité de l'identité de l'utilisateur et les besoins du processus d'authentification. Il retourne ainsi une des quatre réponses suivantes :

- Si l'identité de l'utilisateur est valide, le serveur RADIUS répond au client RADIUS par un paquet d'acceptation d'accès, autorisant l'utilisateur à effectuer d'autres opérations. Ce paquet contient les informations d'autorisation, car RADIUS assure à la fois l'authentification et l'autorisation.
- Si l'identité de l'utilisateur n'est pas valide, le serveur RADIUS répond avec un paquet Access-Reject au client RADIUS, rejetant la demande d'accès de l'utilisateur.

_ Le serveur RADIUS souhaite collecter des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge »).

_ Le serveur Radius demande à l'utilisateur un nouveau mot de passe.

4. Le client RADIUS informe l'utilisateur du résultat de l'authentification.
5. Le serveur RADIUS accepte ou rejette la demande d'accès utilisateur en fonction du résultat de l'authentification. Si la demande est acceptée, le client RADIUS envoie un paquet de demande de comptabilité (démarrage) au serveur RADIUS.
6. Le serveur RADIUS répond avec un paquet Accounting-Response (Start) et démarre la comptabilité.
7. L'utilisateur commence à accéder aux ressources du réseau.
8. L'utilisateur envoie une demande de déconnexion pour arrêter d'accéder aux ressources réseau.
9. Le client RADIUS envoie un paquet de demande de comptabilité (Stop) au serveur RADIUS.
10. Le serveur RADIUS répond avec un paquet Accounting-Response (Stop) et arrête la comptabilité.
11. Le client RADIUS informe l'utilisateur que l'accès au réseau se termine et que l'utilisateur cesse d'accéder aux ressources réseau [52].

Voici la figure 2.7 qui représente le fonctionnement du protocole RADIUS :

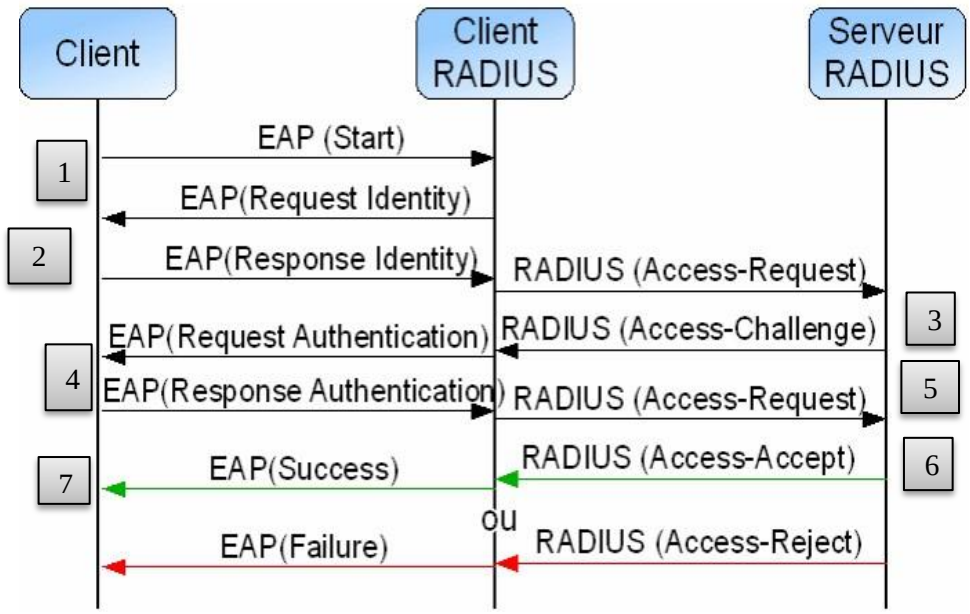

Figure 2.7 : Fonctionnement du protocole RADIUS [53].

c. Protocoles de mots de passe

RADIUS prend en charge deux protocoles d'authentification par mots de passe : PAP (***Password Authentication Protocol***), qui transmet le nom d'utilisateur et le mot de passe en clair, et CHAP (***Challenge Handshake Authentication Protocol***) qui repose sur un mécanisme de hachage avec échange d'un challenge. Le protocole prévoit deux attributs séparés : *User-Password* et *CHAP-Password [51].*

d. Problèmes de sécurité de RADIUS

Bien que RADIUS soit largement utilisé pour gérer l'accès au réseau, ce protocole joue un rôle central de la protection du réseau d'entreprise contre les connexions frauduleuses, il vérifie l'identité de l'utilisateur en utilisant les informations d'identification stockées dans sa base de données d'utilisateurs, en empêchant les accès non autorisés, donc en garantissant que seuls les utilisateurs légitimes puissent se connecter. En regroupant au même endroit les utilisateurs, il facilite le suivi de ce qui se passe sur le réseau, il présente plusieurs problèmes de sécurité dont les organisations doivent être conscientes :

1. **Vulnérabilité de secret partagé** : La sécurité repose sur un secret partagé, dont la compromission peut affecter l'ensemble du système.
2. **Chiffrement insuffisant** : RADIUS ne chiffre que le mot de passe, laissant d'autres données vulnérables à l'interception.
3. **Attaques par force brute et par dictionnaire** : Les méthodes d'authentification comme PAP et CHAP sont susceptibles à ces attaques.
4. **Point de défaillance unique** : Les serveurs RADIUS représentent un point de défaillance qui peut perturber l'authentification si le serveur est indisponible.

Pour atténuer ces problèmes de sécurité les organisations peuvent mettre en œuvre des mesures de sécurité supplémentaires, telles que l'utilisation de secrets partagés forts et uniques pour chaque paire client/serveur RADIUS, déploiement de protocoles de chiffrement réseau comme IPsec (**Internet Protocol Security**), mise en œuvre de méthodes d'authentification robustes, telles que EAP (***Extensible Authentication Protocol***), qui prend en charge des mécanismes d'authentification plus forts et Assurer des mises à jour et des correctifs réguliers pour le logiciel serveur RADIUS afin de remédier aux vulnérabilités connues. Les organisations avec des exigences de sécurité élevées pourraient envisager des protocoles alternatifs tels que Diameter, qui offrent de meilleures fonctionnalités de sécurité [54].

e. Importance de l'utilisation du RADIUS

Le protocole RADIUS est largement adopté dans les environnements professionnels pour plusieurs raisons clés, que nous détaillons ci-dessous :

Centralisation de l'authentification : RADIUS permet de gérer l'authentification des utilisateurs à partir d'un serveur central. Cela simplifie la gestion des utilisateurs et des droits d'accès, notamme **Sécurité renforcée :** RADIUS prend en charge des méthodes d'authentification robustes via l'utilisation de protocoles EAP (***Extensible Authentication Protocol***) qu'est un protocole conçu pour étendre les fonctions du protocole Radius à des types d'identification plus complexes, notamment :

- EAP-TLS (***Transport Secure Layer***) : utilise TLS pour établir un canal sécurisé permettant l'authentification mutuelle par certificats et l'échange sécurisé de clés.
- PEAP (***Protected EAP***) : une méthode très semblable dans ses objectifs et voisine dans la réalisation à EAP-TTLS, qui renforcent la sécurité des échanges. Cela réduit considérablement les risques d'accès non autorisé et d'usurpation d'identité.

Gestion des accès granulaires : Grâce à RADIUS, il est possible de définir des règles d'accès spécifiques selon le profil de l'utilisateur (rôle, groupe, type de périphérique).
Suivi et comptabilité (Accounting) : Le protocole permet d'enregistrer dans une base de données les connexions, les déconnexions, la durée des sessions, etc. Ces informations sont utiles pour :

- Auditer les accès.
- Détecter des activités suspectes.
- Facturer les services (pour les FAI).

Compatibilité avec de nombreux appareils : RADIUS est un protocole standardisé et compatible avec une grande variété d'équipements réseau pour la facilite de son intégration, (Commutateurs, routeurs, bornes Wi-Fi, contrôleurs, etc.).
Scalabilité : RADIUS est capable de gérer efficacement des milliers d'utilisateurs simultanés, ce qui le rend adapté sans perturber les performances [55].
nt dans les grands réseaux.

f. Limitation du protocole RADIUS

Malgré ses avantages pour la gestion de l'accès au réseau. Les principales limites incluent :

1. **Sécurité limitée** : La dépendance à un secret partagé peut compromettre l'ensemble du système si ce dernier est exposé, et le chiffrement ne protège que le mot de passe de l'utilisateur.
2. **Point de défaillance unique** : Si le serveur RADIUS devient indisponible, l'authentification et l'autorisation peuvent être interrompues, bien que des mécanismes de redondance puissent atténuer ce risque.
3. **Problèmes d'évolutivité** : La gestion d'un grand nombre d'utilisateurs et d'appareils peut devenir complexe, affectant les performances.
4. **Prise en charge limitée des attributs** : RADIUS ne prend en charge qu'un ensemble prédéfini d'attributs d'autorisation, ce qui peut être insuffisant pour certaines organisations, et la création d'attributs personnalisés peut compliquer l'intégration.
5. **Manque de fonctionnalités avancées** : Développé dans les années 1990, RADIUS n'offre pas certaines fonctionnalités modernes que des protocoles comme Diameter proposent, ce qui le rend moins adapté aux besoins contemporains. **Problèmes de compatibilité** : Tous les dispositifs ne prennent pas en charge RADIUS nativement, ce qui peut compliquer son intégration, notamment avec des implémentations personnalisées.

Malgré ces limites, RADIUS demeure un choix populaire pour les organisations recherchant une solution simple, efficace et largement compatible pour l'authentification centralisée. Sa bonne intégration avec des services tels que FreeRADIUS, LDAP ou Active Directory en fait une option pragmatique dans de nombreux cas. Pour des infrastructures complexes nécessitant des garanties de sécurité renforcées et une grande flexibilité, un protocole plus moderne comme Diameter peut toutefois s'avérer plus adapté [54].

2.5 Contrôle d'accès

Le contrôle d'accès est une mesure de sécurité fondamentale qui permet à une organisation de se protéger contre les violations et l'exfiltration de données. Il définit précisément qui est autorisé à accéder à certaines données, applications et ressources. Le contrôle d'accès empêche le vol d'informations confidentielles, telles que les données des clients et la propriété intellectuelle, que ce soit par des acteurs malveillants externes ou d'autres utilisateurs internes non autorisés. De plus, il contribuer à réduire les risques d'exfiltration de données par les employés et prévient les menaces émanant du web. Pour optimiser la gestion des autorisations, des nombreuses organisations axées sur la sécurité utilisent des solutions de gestion des identités et des accès (IAM) telles que Microsoft Azure Active Directory ou Okta, mettant ainsi en œuvre des stratégies de contrôle d'accès efficaces [56].

2.5.1 Méthode de contrôle d'accès

a. Filtrage MAC

Le filtrage par adresse MAC est un mécanisme de sécurité utilisé dans les réseaux sans fil pour restreindre l'accès au réseau à des appareils spécifiques. la figure 2.8 illustre ce mécanisme fonctionne en autorisant uniquement les stations dont l'adresse MAC figure dans une liste préalablement définie sur le point d'accès , parfois combinée à d'autres mesures de sécurité comme l'ESSID fermé ou les Listes de Contrôle d'Accès (ACL). Cependant, cette méthode présente plusieurs vulnérabilités importantes. La première est qu'il s'agit d'un mécanisme optionnel, souvent non activé dans les réseaux sans fil. De plus, le filtrage MAC peut être facilement contourné par un attaquant en usurpant l'adresse MAC d'un appareil légitime [57].

Figure 2.8 : Filtrage des adresses mac [60].

b. Protocol WPA

Nous allons étudier dans cette partie le WPA (WPA et WPA2, en particulier la version personnelle la plus utilisée, mais aussi la version Enterprise utilisant un serveur d'authentification type radius donc plus compliquée) son fonctionnement (protocole de cryptage, authentification ses faiblesses et ensuite quels sont les moyens utilisés pour le craquer. Le Wi-Fi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux de type WiFi [58].

i. WPA entreprise

Le mode "Enterprise" utilise une infrastructure d'authentification 802.1x avec un serveur RADIUS et un contrôleur réseau (point d'accès). Le protocole EAP (Extensible Authentification Protocol) identifie les utilisateurs avant de les autoriser à accéder au réseau, via diverses méthodes d'authentification (mot de passe, carte à puce, certificats électroniques, etc.).
Voici la figure 2.7 expliquant comment marche la connexion Wifi en mode WPA entreprise, le client commence par envoyer une requête d'authentification, qui est vérifiée par le serveur via un échange de clés et la négociation d'un protocole de cryptage. Une fois l'authentification réussie, l'échange se poursuit dans un tunnel sécurisé et le client est autorisé à s'associer au point d'accès [58].

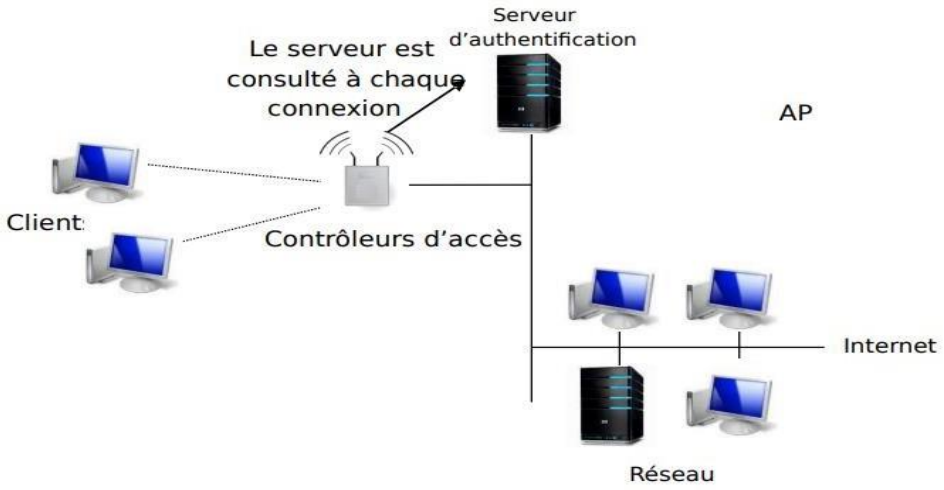

Figure 2.9 : Le fonctionnement du Wi-Fi avec un serveur d'authentification [60].

Figure 2.15 décrit une connexion WiFi utilisant un serveur d'authentification EAP avec un certificat. Le serveur envoie d'abord une requête d'authentification au client, qui peut répondre avec un mot de passe, une carte à jeton ou un certificat. Comme le client n'a pas de carte à jeton, il propose un certificat, qui est choisi par le serveur. Après vérification, le client demande à s'associer au point d'accès, et s'il est accepté, il se connecte au réseau [58].

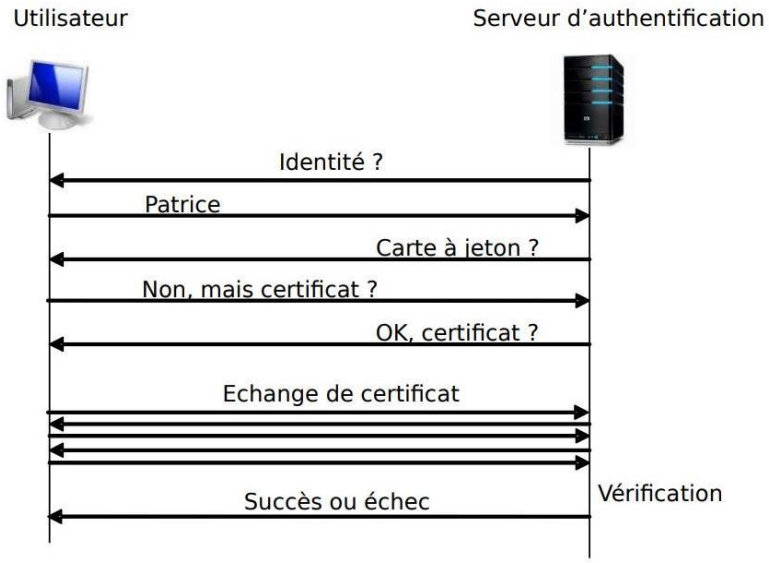

Figure 2.10 : Dialogue avec EAP [60].

1. Méthodes et types courants de EAP

Le protocole d'authentification extensible (EAP) prend en charge diverses méthodes, chacune conçue pour répondre à différents besoins et environnements de sécurité. Ces méthodes offrent flexibilité et adaptabilité, permettant aux organisations de choisir le mécanisme d'authentification le plus approprié pour leurs scénarios d'accès au réseau. Voici quelques-unes des méthodes EAP courantes [59].

- **EAP-TLS** : Méthode très sécurisée basée sur TLS **(Transport Layer Security)** avec authentification mutuelle via certificats numériques. Utilisée dans les réseaux à haute sécurité (ex : entreprises, VPN).
- **EAP-TTLS (Tunneled Transport Layer Security)** : Crée un tunnel sécurisé TLS ; seul le serveur a besoin d'un certificat, le client peut s'authentifier par mot de passe. Plus flexible et facile à déployer.
- **PEAP (Protected Extensible Authentication Protocol)** : Semblable à EAP-TTLS, crée aussi un tunnel TLS ; protège des méthodes EAP moins sécurisées. Couramment utilisé en WPA2-Enterprise.
- **EAP-MD5 (Extensible Authentication Protocol - Message Digest 5)** : Méthode simple avec hachage MD5 ; pas de chiffrement ni d'authentification mutuelle, donc peu sécurisé. Utilisé dans des environnements à faible exigence de sécurité.
- **EAP-SIM (Extensible Authentication Protocol - Subscriber Identity Module)** : Utilisé dans les réseaux mobiles GSM, s'appuie sur les informations de la carte SIM pour l'authentification.
- **EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement)** : Variante de EAP-SIM pour UMTS et LTE. Offre meilleure sécurité et prise en charge des clés de chiffrement
- **EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)** : Développé par Cisco, propose un tunnel sécurisé sans certificat, utilisant une PAC (Protected Access Credential). Idéal dans les environnements où la gestion de certificats est difficile [59].

2. Cryptages

Il existe 2 types de cryptage, le protocole TKIP pour le WPA, et le protocole AES pour le WPA2.

2.1 WPA-TKIP

TKIP ***(Temporal Key Integrity Protocol)*** est un protocole de sécurité pour les réseaux Wi-Fi, utilisé dans WPA pour protéger et authentifier les données est basé sur un moteur WEP ***(RC4)*** et améliorant la méthode de gestion des clés et le contrôle d'intégrité grâce à MIC ***(Message Integrity Control)*** **[61]**.

2.2 WPA2: TKIP (Temporal Key Integrity Protocol) et AES (CCMP)

CCMP (Counter-Mode/CBC-Mac protocol) est une méthode de chiffrement qui utilise AES (Advanced Encryption Standard), un algorithme de chiffrement. La combinaison des deux est la sécurité la plus performante [58].

ii. Faiblesses

- **Celles du PSK :** elle ne convient qu'aux petits réseaux infrastructure ou les réseaux Ad Hoc. Ces défauts sont dus aux mots de passe trop court, au partage de la clé avec tous les utilisateurs ce qui diminue la sécurité et le fait que tous les utilisateurs peuvent espionner le trafic des autres et dans le cas où le nombre d'utilisateurs est grand, le système devient lourd à gérer.
- **Celles de TKIP :** Par exemple celle du protocole Michael qui dispose d'un code d'intégrité MIC (Message Integrity Protocol) trop court et donc qui peut être attaquable en quelques heures.
- **Celles d'EAP :** La sécurité du 802.1x peut être compromise de 3 façons différentes : en attaquant la méthode EAP utilisée (contre la méthode d'authentification il existe l'attaque de dictionnaire en ligne ou hors ligne), en détournant une session après sa création ou encore en s'interposant entre le client et le serveur d'authentification (attaque MiM) [58].

iii. Solutions

- **Celles de PSK :** Il est conseillé d'utiliser un mot de passe long, idéalement d'une vingtaine de caractères, ou au minimum d'une douzaine si celui-ci est composé de lettres aléatoires. De plus, de ne pas avoir trop d'utilisateur à gérer sur un même point d'accès.

- **Celles de TKIP :** La contre mesure de Michael est que si un paquet est modifié par un pirate le contrôle d'intégrité Michael le détectera et l'AP sera bloquée pendant 60 secondes. Ceci permet d'éviter qu'un pirate modifie des millions de paquets dans l'espoir que l'un d'entre eux passera le contrôle d'intégrité.

- **Celles d'EAP :** Il faut créer un tunnel sécurisé, améliorer la validité du certificat (exemple : un par poste) et avoir une bonne sécurité interne du type carte à jeton en utilisant un cryptage puissant du type WPA et WPA2 [58].

Conclusion

La sécurité des réseaux sans fil est un enjeu crucial dans un monde de plus en plus connecté. À travers ce chapitre, nous avons exploré les différents types de risques et d'attaques, qu'elles soient actives ou passives, et leurs impacts potentiels sur la confidentialité, l'intégrité et la disponibilité des données. Face à ces menaces, plusieurs solutions techniques ont été mises en avant, telles que le chiffrement, le hachage, les certificats numériques. Les méthodes de contrôle d'accès, bien que fondamentales, doivent être renforcées par des technologies avancées et des pratiques de sécurité rigoureuses. En intégrant des solutions telles que WPA2 et des pratiques de gestion des identités, les organisations peuvent mieux se protéger contre les attaques. Cependant, il demeure essentiel de rester informé des nouvelles vulnérabilités et des techniques d'attaque émergentes afin d'adapter continuellement les stratégies de sécurité. La sensibilisation et l'éducation des utilisateurs jouent également un rôle clé dans la prévention des incidents de sécurité.

Chapitre 3 : Présentation de l’entreprise la Pharmacie Centrale des Hôpitaux

Introduction

Ce chapitre sera réservé à la présentation de l'entreprise pharmacie centrale des hôpitaux (PCH) où nous effectuons notre stage, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs.

1. Présentation de la Pharmacie Centrale des Hôpitaux

La Pharmacie Centrale des Hôpitaux (PCH), Établissement Public à Caractère Industriel et Commercial (EPIC) sous tutelle du Ministère de la Santé, est un acteur clé dans l'approvisionnement des établissements publics de santé à l'échelle nationale. Elle a pour s'assurer la distribution des produits pharmaceutiques sur tout le territoire Algérienne, tout en remplissant des missions de service public liées à la constitution d'un stock stratégique et d'un stock ORSEC (organisation des secours). La PCH son réseau de distribution couvre six régions : Alger, Oran, Annaba, Biskra et Béchar, Tamanrasset, elle garantit la disponibilité de produit pharmaceutique de plus de 1000 références clients dans des conditions optimale de livraison, de stockage et de coût. Cet établissement elle collabore avec près de 250 fournisseurs, 89 locaux et 158 internationaux, pour répondre aux besoins des établissements de santé et autres clients. Engagée dans une démarche industrielle, la PCH projette de renforcer sa participation dans la production pharmaceutique afin de réduire la dépendance nationale vis-à-vis du marché mondial. L'établissement est dirigé par un directeur général. Elle est soumise à un organe de contrôle, mission, assuré par un Conseil d'Administration présidé par Monsieur le Ministre de la santé et dont les membres sont des représentants des différents ministères. Dans la figure 3.1 représente le logo de la PCH.

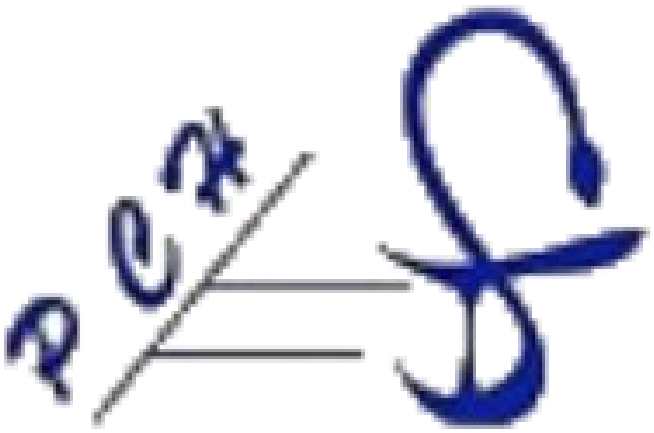

Figure 3.1 : Logo de la pharmacie centrale des hôpitaux.

2. La localisation de l'entreprise

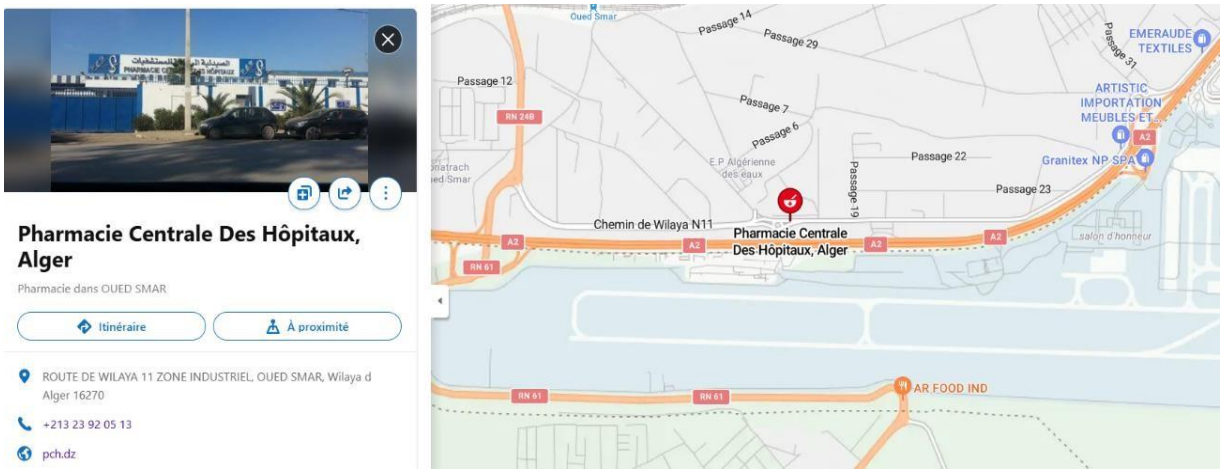

Figure 3.2 : Localisation de l'entreprise PCH.

3. Fiche technique

La figure ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude. Voici la figure 3.3 présente de manière globale les informations de l'entreprise.

Adresse:	11, Route de Wilaya. Zone Industrielle Oued Smar. Bp 354. Dar El Beida,Alger,Algérie
Email:	pch@sante.dz contact@pch.dz
Téléphone portable:	Il n'y a pas de téléphone mobile principal
Téléphone fixe:	023 92 05 10 023 92 05 11 023 92 05 12 023 92 05 13
Fax:	023 27 90 01
Viber:	Pas de Viber
Horaires de travail	Nous n'avons pas cette information.
Site Web:	http://www.pch.dz

Figure 3.3 : Information sur l'entreprise.

4. Les Missions de la Pharmacie Centrale des Hôpitaux

4.1. Missions générales

- Approvisionner les établissements publics de santé en produits pharmaceutiques et dispositifs médicaux selon la liste ministérielle.
- Approvisionner les établissements publics de santé en produits pharmaceutiques et dispositifs médicaux selon la liste ministérielle et d'importation basée sur les besoins exprimés par le ministère de la santé.
- Commercialiser ces produits aux établissements publics, privés, et aux Commercialiser ces produits aux établissements publics, privés, et aux distributeurs agréés (officines).
- De procéder à l'exécution des actions de régulations des approvisionnements conformément à la législation et à la réglementation en vigueur.
- Fabriquer notamment des médicaments génériques et assurer leur conditionnement.
- Mettre en place des points de vente au détail pour assurer la disponibilité nationale.
- Apporter une assistance technique, dans le cadre d'un partenariat, à tout opérateur intervenant dans l'industrie pharmaceutique.
- Réaliser des sujétions de service public définies par décret.

4.2. Mission services publiques

- Détenir un stock stratégique et un stock ORSEC arrêté par le ministère chargé de la santé.
- Approvisionner les établissements publics destinés au traitement de maladies rares et pathologies à pronostic vital et les programmes nationaux de prévention et des plans nationaux de santé.
- Détention d'un droit exclusif en matière d'importation et commercialisation des produits hémodérivés et stupéfiants.

5. La vision de PCH

La PCH vise de renforcer son plan commercial en satisfaisant les besoins des établissements de santé publique et en augmentant sa part de marché, est envisagé à améliorer la gestion de son approvisionnement en optimisant coûts, délais et qualité, en favorisant la production nationale pour réduire les importations, optimiser les stocks, maîtriser les coûts de transit et moderniser les sites et moyens matériels. Sur le plan qualité, elle souhaite garantir la conformité réglementaire des produits pharmaceutiques. Enfin, elle s'engage à développer une culture de sécurité, moderniser les systèmes existants et renforcer les dispositifs de protection.

6. Stratégies

La PCH est la centrale d'achat et de gestion des produits pharmaceutiques en charge d'assurer leur disponibilité, qualité et transport des produits pharmaceutiques sur l'ensemble du territoire national, en alignement avec la stratégie du Ministère de la Santé à savoir celle de garantir la disponibilité des médicaments et dispositifs médicaux. Elle maintient un stock stratégique et ORSEC pour les besoins de service public. Face à la concurrence, elle

encourage la production locale via des appels d'offres pour réduire la dépendance aux importations, tout en continuant à s'approvisionner à l'international pour les produits non fabriqués localement. La PCH vise à moderniser sa distribution grâce aux technologies pour passer d'une gestion à un management pharmaceutique efficace.

7. Directions

- La **Direction Technico-Réglementaire (DTR)** : La maîtrise des enjeux techniques et réglementaires revêt un intérêt fondamental pour la PCH. La DTR garantit la qualité et la conformité des produits pharmaceutiques commercialisés en Algérie. Elle collabore étroitement avec les autorités sanitaires pour s'assurer du respect des normes techniques et réglementaires, notamment le contrôle qualité, la traçabilité et la gestion des réclamations depuis la passation de commande des produits jusqu'à la livraison aux clients.
- **Approvisionnement :** La PCH gère ses achats locaux et étrangers via des directions spécialisées par familles de produits. Ces directions assurent le suivi des commandes, la gestion des contrats, les aspects bancaires, et veillent à la bonne coordination avec les commissions et le Bureau des Marchés.
- **Activité Commerciale :** La direction commerciale, essentielle à la PCH, veille à la rentabilité économique tout en répondant aux besoins des clients. Elle suit l'évolution du marché, la concurrence, et maintient une coordination fonctionnelle avec les autres activités comme l'approvisionnement, la distribution et le stockage.
- **Stockage :** La gestion des stocks est cruciale pour assurer la disponibilité et la qualité des produits, optimiser l'espace d'entreposage, éviter la rupture ou le sur-stockage, et planifier les stocks stratégiques.
- **Logistique :** La Direction Moyens et Logistique, composée de trois sous-directions, soutient les besoins matériels et de transport de la PCH. Elle gère aussi les achats de matériel, le parc roulant, et les inventaires des biens.
- **IT et Système d'Information (DISI) :** La DISI est le système nerveux de la PCH, divisée en gestion des systèmes d'information et exploitation des réseaux. Elle assure la sécurité informatique, le développement d'applications, l'harmonisation des outils, la veille technologique, et le traitement analytique des données pour appuyer la prise de décision.

7.1. Métiers et fonctions transversales

La PCH s'organise autour de métiers clés (approvisionnement, stockage, distribution) soutenus par des fonctions transversales (technico-réglementaire, commerciale, contrôle de gestion, communication, informatique, ressources humaines, finance, audit qualité) afin d'optimiser son efficacité et la qualité du service aux établissements hospitaliers.

8. Produits

La Pharmacie Centrale des Hôpitaux (PCH) fournit aux établissements de santé de toute l'Algérie toute une gamme de produits ce qui contribue réellement à maintenir les gens en bonne santé. Il s'agit de :

- **Médicaments** Le médicament n'est pas un produit comme les autres. Pour être appelé comme tel, il doit correspondre à une définition précise donnée par le Code de la Santé Publique. Ainsi, un médicament est un produit qui peut :

  - Soigner une maladie.
  - La prévenir.
  - Aider à faire un diagnostic.
  - Modifier une fonction de l'organisme.
  - Dispositifs médicaux.

- **Produits dentaires** sont des matériaux et des instruments utilisés pour les soins et les traitements dentaires tels que les dentifrices, les brosses à dents et les shampoings.
- **Réactifs chimiques** Il s'agit de substances ou de composés chimiques utilisés pour effectuer des réactions, des tests ou des expériences en laboratoire. Ils sont les agents de changement dans la recherche en laboratoire, permettant aux scientifiques d'observer, de mesurer et d'étudier toute une série de phénomènes pour fournir des résultats précis et reproductibles.
- **Consommables de laboratoire** incluent des équipements tels que des balances, des chauffages, des évaporateurs rotatifs, des étuves ou incubateurs, et des micropipettes. Les principaux consommables de laboratoire sont le barreau aimanté, le bécher, la burette, l'éprouvette et la fiole comme les pansements, les bandages, les produits d'hygiène et de protection.
- **Médicaments radio-pharmaceutiques** qui permettent aux médecins d'observer l'activité des organes en temps réel et de traiter certaines pathologies grâce aux effets de la radiation sur les cellules malades. Ils sont particulièrement utilisés en oncologie, en cardiologie et en neurologie et d'autres choses dont les hôpitaux ont besoin pour fonctionner correctement.

Elle est très importante car elle veille à ce que tout le monde reçoive ce dont il a besoin, en toute sécurité et dans le respect des règles en vigueur en Algérie. Elle répond aux nombreux besoins du monde médical.

9. Organigramme

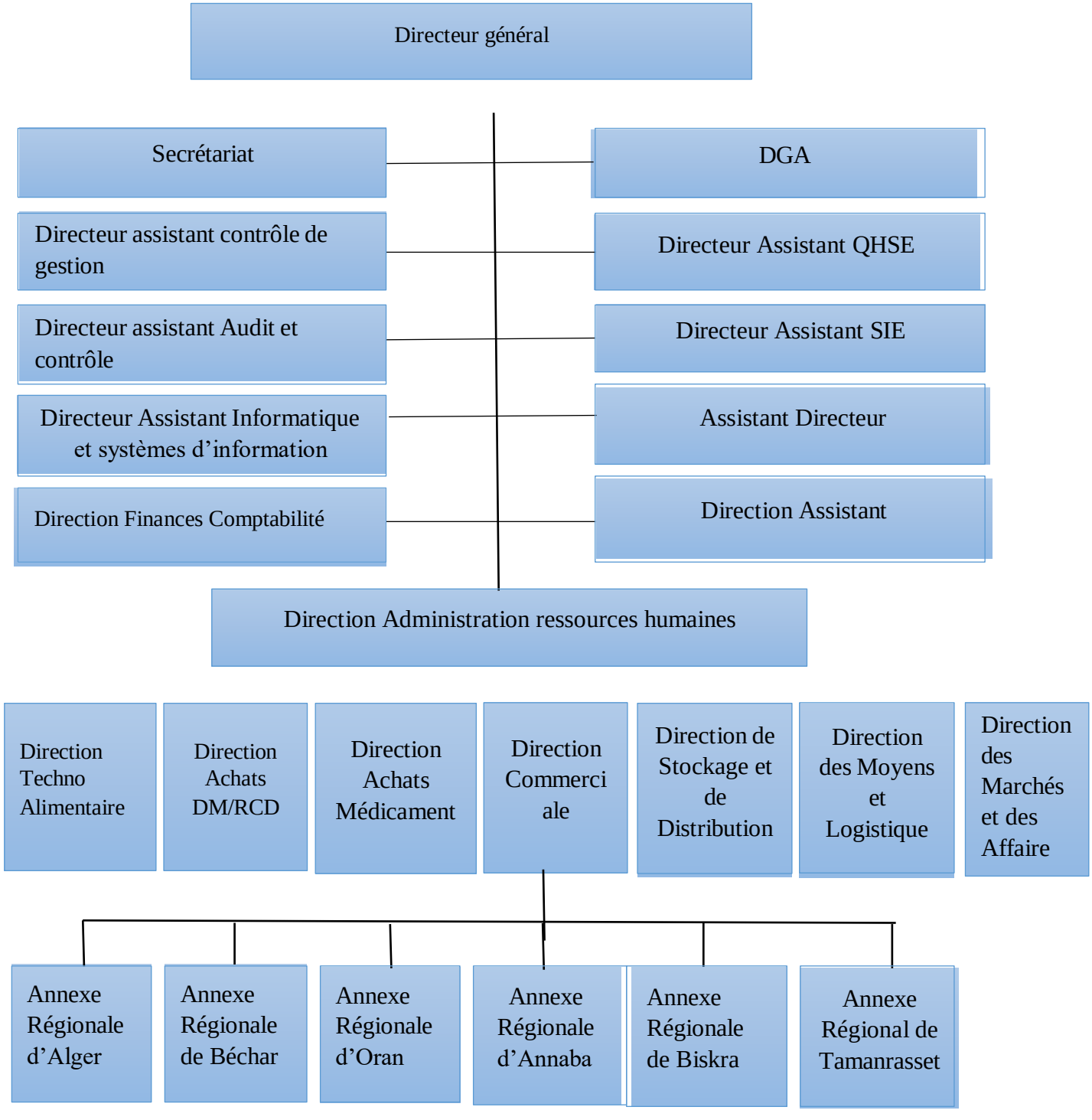

Figure 3.4 : L'organigramme de la pharmacie centrale des hôpitaux.

10. Conclusion

Dans ce chapitre, nous avons donné un aperçu général de l'entreprise de pharmacie centrale des hôpitaux, puis nous avons découvert un problème qui nous a amenés à rechercher de mettre en œuvre une architecture qui puisse améliorer la sécurité des réseaux sans fil. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

Chapitre 4 : Mise en œuvre d'une solution de sécurisation d'un réseau sans fil basée sur le Contrôle d'accès et l'authentification.

Introduction

Avec l'évolution constante des technologies de l'information, les réseaux sans-fil sont devenus des composantes essentielles des infrastructures informatiques, notamment dans les établissements publics et les entreprises. Toutefois, cette flexibilité s'accompagne de vulnérabilités spécifiques, notamment en ce qui concerne d'authentification, de confidentialité des données échangées et de contrôle d'accès.
Au sein de l'établissement d'accueil de stage, la Pharmacie Centrale des Hôpitaux (PCH), certaines failles ont été détectées. Face à ces menaces, la mise en place d'une solution de sécurisation du réseau Wi-Fi s'impose comme une nécessité.
À cette fin, une architecture réseau local sans-fil a été proposée, modélisée et mise en œuvre. Afin de mettre en évidence les configurations essentielles ainsi que les manipulations techniques réalisées, l'outil Cisco Packet Tracer a été utilisé comme environnement de simulation.

1. Contexte du stage et étude de l'infrastructure existante

Le travail s'inscrit dans le cadre de la mise en place d'une solution de sécurisation du réseau sans-fil au sein de la Pharmacie Centrale des Hôpitaux (PCH). L'objectif principal est de concevoir et de déployer un réseau Wi-Fi fiable, intégrant des mécanismes d'authentification et de contrôle d'accès basés sur des certificats. Afin de proposer une solution adaptée, une étude de l'infrastructure existante a été réalisée. Cette section présente donc l'état actuel du réseau, les équipements en place ainsi que les types de connexion utilisés.

1.1. Description de l'infrastructure réseau existante

L'architecture réseau de la Pharmacie Centrale des Hôpitaux (PCH) est structurée autour de trois blocs fonctionnels : le bloc administratif (DG), le bloc commercial et le dépôt. Ces blocs sont interconnectés via des liaisons en fibre optique (FO), avec un point de concentration situé dans la salle technique du bloc DG, comme illustré dans Figure 4.1 et Figure 4.2.
L'infrastructure repose sur une hiérarchie classique :

- **Commutateurs d'accès et de distribution :** Cisco Catalyst 2960, déployés dans les baies réseau de chaque étage et de chaque bloc.
- **Switch cœur de réseau :** Cisco Catalyst 3850, situé dans la baie principale du bloc DG, jouant le rôle de switch de distribution de niveau 3.
- **Connexion Internet :** assurée via un équipement dédié connecté au cœur de réseau avec une liaison cuivre redondante.

Toutefois, cette infrastructure présente certaines limites, notamment l'absence de segmentation VLAN entre les services, ainsi que l'absence d'un service d'authentification centralisée (tel qu'un serveur Radius) rend les accès au réseau sans fil vulnérables aux connexions non autorisées.

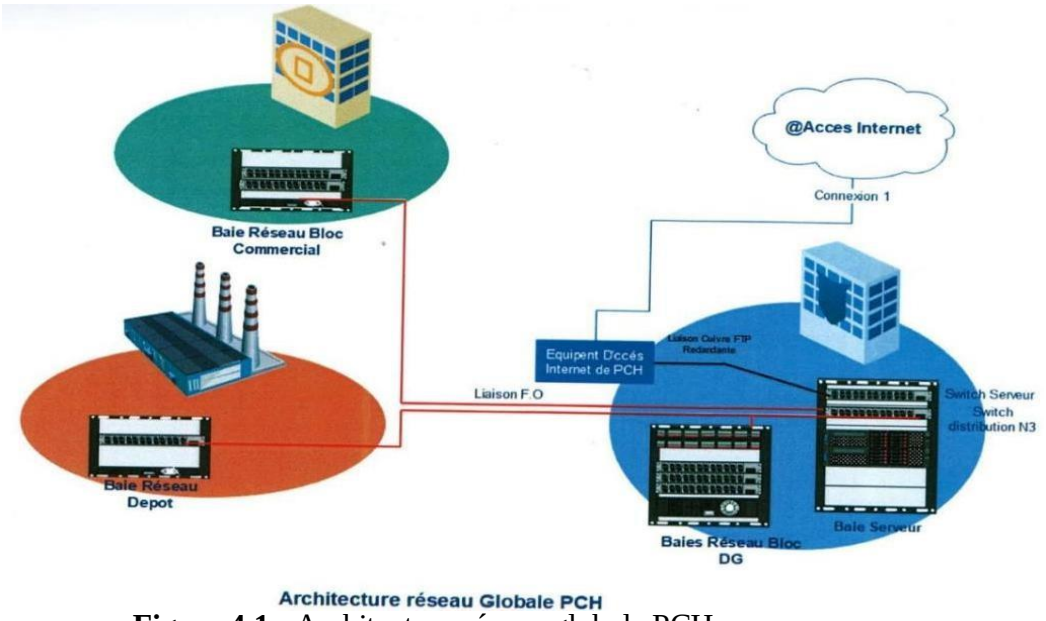

Figure 4.1 : Architecture réseau globale PCH.

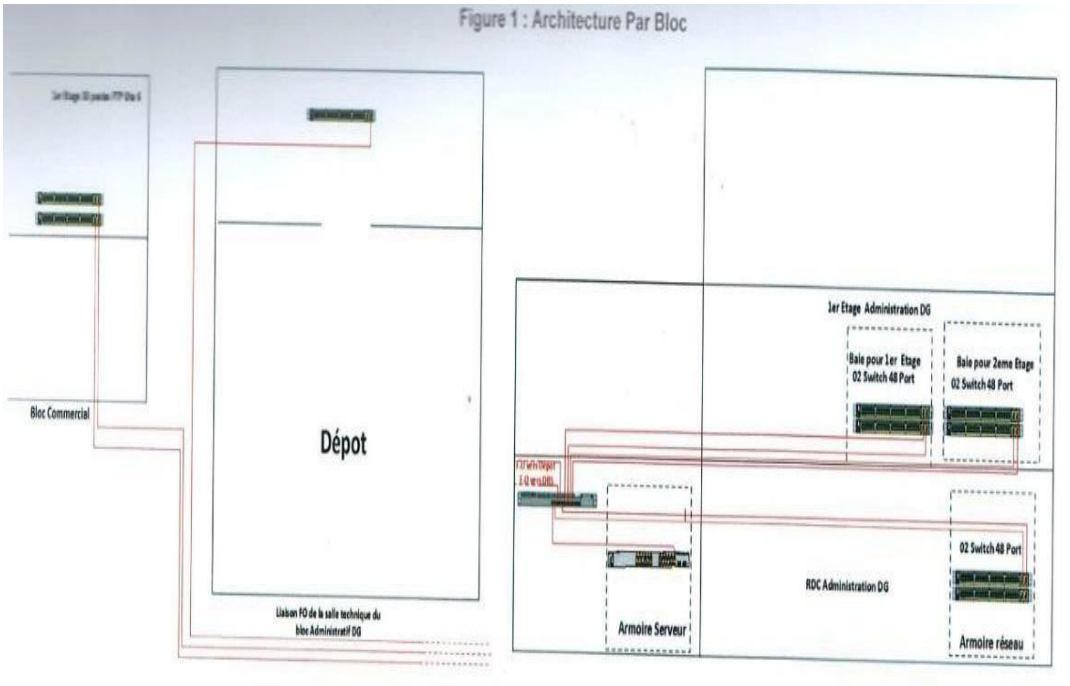

Figure 4.2 : Architecture réseau par bloc.

1.2. Les vulnérabilités et failles conceptuelles de l'infrastructure réseaux sans fil existante

- Partage d'un mot de passe unique (WPA2 : tous les utilisateurs utilisent la même clé (PSK – Pre-Shared Key).

Ainsi, si le mot de passe est divulgué, n'importe qui peut accéder au réseau.

- La traçabilité n'est pas assurée : impossible d'identifier l'utilisateur est responsable d'une activité spécifique.

- Absence d'identification individuelle des utilisateurs : aucun mécanisme ne permet de lier un appareil ou une activité réseau à une identité précise.
- Manque de contrôle granulaire des accès : impossible d'attribuer des droits spécifiques par utilisateur ou par groupe. Ainsi, tous les utilisateurs possèdent le même niveau d'accès, quel que soit leur rôle (invité, employé, administrateur, etc.).
- Risque d'attaques par rebond ou usurpation d'identité : un attaquant peut usurper l'adresse MAC d'un appareil Autorisé.
- Absence de support natif pour l'attribution dynamique de VLANs, les politiques d'accès conditionnelles, ou l'intégration avec un annuaire central (comme LDAP ou Active Directory).

1.2.1 Les mécanismes de sécurité implémentés

Afin de corriger les failles de sécurité observées dans l'infrastructure réseau existante, nous avons mis en œuvre une politique de sécurité essentielle basée principalement sur deux aspects :

- **Mise en place de VLAN (segmentation du réseau)**

Nous avons créé plusieurs VLAN pour séparer les différents services (APPRO, RH, IT, WLC) et défini des règles de communication inter-VLAN.

- **Authentification centralisée via un serveur RADIUS**

Le serveur RADIUS vérifie l'identité de chaque utilisateur avant d'autoriser l'accès au réseau.

1.3. Mise en œuvre d'une approche de sécurisation du réseau sans-fil

1.3.1. Description générale de la solution proposée

La solution proposée vise à sécuriser un réseau sans fil en mettant en œuvre un mécanisme d'authentification forte et un serveur RADIUS basée sur les VLANs.

Le schéma général d'architecture réseau sécurisée présenté dans Figure 4.3 repose sur une architecture en mode infrastructure avec un réseau Wi-Fi sécurisé par l'authentification WPA2-Enterprise, elle intègre un contrôleur WLC, un serveur RADIUS et un serveur mail. L'infrastructure est répartie sur plusieurs VLANs (10, 20,30, 88) et sur trois niveaux de réseau : cœur, distribution, accès. Les utilisateurs se connectent via des points d'accès contrôlés par le WLC. Figure 4.3 illustre la topologie réseau proposée.

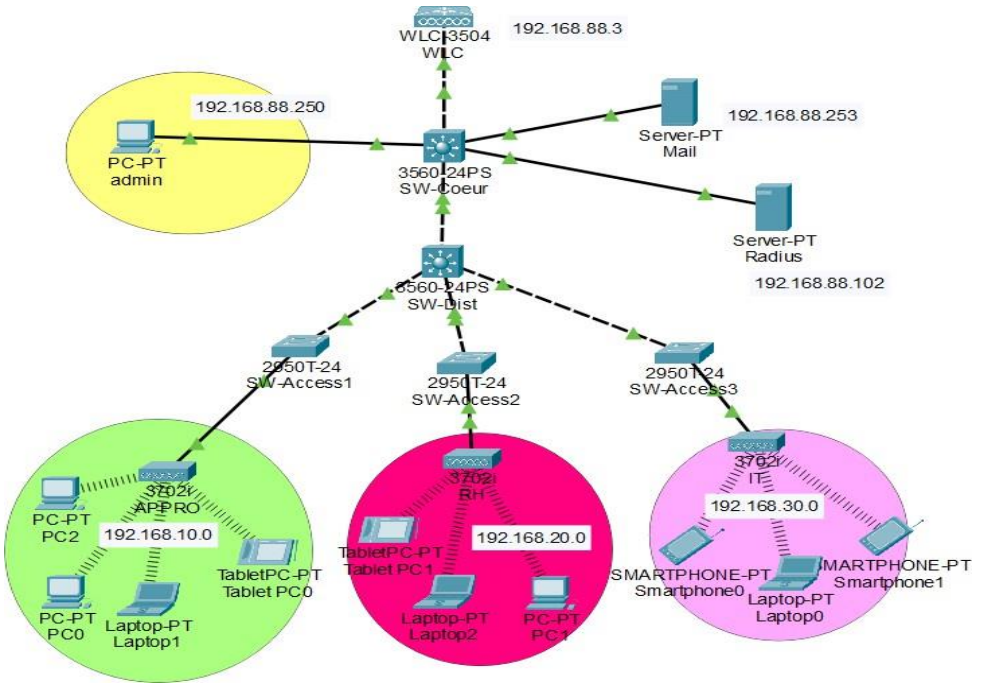

Figure 4.3 : la topologie réseau proposée.

1.3.2. Approche basée sur les VLANs

a. Objectifs :

Attribuer un VLAN spécifique à un groupe de clients Wi-Fi permet de créer un réseau virtuel distinct au sein de l'infrastructure physique existante, ce qui présente les avantages suivants :

- ✓ Une plus grande flexibilité dans l'administration et l'évolution du réseau, car l'ensemble de l'architecture peut être ajusté simplement en configurant les commutateurs.
- ✓ Une amélioration de la sécurité grâce à l'isolation logique des données (domaines de diffusion), ce qui permet de les séparer du reste du trafic.
- ✓ Une réduction significative de la diffusion du trafic dans le réseau.

b. Principe de la solution :

Cette séparation logique du réseau basé sur les VLANs, s'appuie principalement sur trois critères de différenciation :

Selon l'activité réseau du client 802.11 après l'authentification. Ce niveau de différenciation

- ✓ permet d'établir un VLAN par profil d'utilisateur (APPRO, RH, IT, WLC).
- ✓ Selon le type du trafic, notamment le trafic d'administration réseau (WLC, IT) et celui du Système d'information (RH, APPRO).
- ✓ Eventuellement, en fonction de la technologie des équipements : cette classification permet d'ajuster les mécanismes de sécurité et d'authentification en tenant compte des vulnérabilités propres aux standards supportés par chaque type de matériel (WEP, WPA, WPA2).

Nom de VLAN	Description	Privilèges
APPRO	Approvisionnement	Lecture sur les données de configuration
RH	Ressources Humaines	Modification des informations des employés
IT	Informatique	Modification des configurations réseau
WLC	Contrôleur Wi-Fi	Lecture seule sur les données de trafic Wi-Fi

Tableau 4.1 : Tableau des privilèges des VLANs.

1.3.3. Intégration de l'authentification centralisée avec RADIUS

a. Objectifs

L'intégration d'une authentification centralisée basée sur le protocole RADIUS dans le cadre de ce projet vise principalement à :

- ✓ Renforcer l'authentification des utilisateurs accédant au réseau Wi-Fi.
- ✓ Mettre en œuvre un contrôle d'accès basé sur des certificats numériques.
- ✓ Assurer une traçabilité des connexions.
- ✓ Garantir la confidentialité et l'intégrité des données échangées.

L'objectif final est de déployer une architecture sécurisée, fiable et évolutive, répondant aux exigences de l'établissement en matière de sécurité réseau.

b. Justification du choix de RADIUS

Pour répondre à ces objectifs, le protocole RADIUS (Remote Authentication Dial-In User Service) a été retenu comme cœur de la solution d'authentification. Ce choix se justifie par plusieurs raisons :

- ✓ RADIUS est un protocole approuvé, largement utilisé pour gérer l'authentification, l'autorisation et la journalisation des accès réseau.
- ✓ Il permet une intégration facile avec les points d'accès Wi-Fi via le protocole 802.1X.
- ✓ Il supporte des méthodes d'authentification sécurisées comme PEAP, basées sur des certificats numériques.
- ✓ Il offre une centralisation de la gestion des utilisateurs, ce qui simplifie l'administration du réseau et renforce la cohérence de la politique de sécurité.

Ainsi, l'adoption de RADIUS constitue une réponse efficace aux besoins de sécurité du réseau sans fil de la PCH, tout en assurant une meilleure gestion des accès et une protection accrue contre les intrusions.

2. Détails d'implémentation de la solution proposée

2.1 Description des composants principaux

Dans le cadre de la sécurisation du réseau Wi-Fi à l'aide du protocole RADIUS, plusieurs composants interconnectés interviennent pour assurer l'authentification, l'autorisation et la gestion des accès :

- **Point d'accès Wi-Fi :** un point d'accès (PA) ou Access Point en Anglais est un appareil de mise en réseau, permettant à tout périphérique smartphone, ordinateur de se connecter au réseau local [70].
- **Serveur RADIUS :** le serveur RADIUS utilise un protocole client-serveur conçu pour centraliser les informations d'authentification des utilisateurs.
- **Contrôleur WLC (Wireless LAN Controller) :** c'est un dispositif centralisé chargé de la gestion et du contrôle des points d'accès (AP) dans les réseaux sans fil.

2.2 Équipements réseau utilisés

L'architecture de test et de simulation repose sur les outils suivants :

Composants / Équipements	Rôle
Wireless LAN Controller	Un contrôleur du réseau local sans fil (WLC) est un équipement réseau chargé d'administrer les points d'accès Wi- Fi, facilitant la connexion des périphériques sans fil. Il assure une gestion centralisée de l'infrastructure réseau sans fil.
Switch	Le commutateur facilite la communication entre les différents périphériques d'un réseau, tout en assurant la connexion à d'autres réseaux. Il permet ainsi un partage efficace des ressources au sein de l'infrastructure, en assurant notamment la gestion des VLANs et la séparation des flux selon les privilèges et les technologies.
Point d'accès	Il s'agit d'un composant fondamental dans un réseau sans fil, servant d'interface entre les dispositifs mobiles (tels que les ordinateurs portables, les smartphones ou les tablettes) et l'infrastructure réseau.
Serveur Mail	Il envoie et reçoit des courriels en s'appuyant sur des protocoles spécifiques de messagerie, tels que ceux dédiés à l'envoi (comme SMTP) et à la réception (comme le POP3 ou l'IMAP).
Serveur RADIUS	Il contrôle l'accès au réseau en vérifiant l'identité des utilisateurs.

Tableau 4.2 : Le rôle du chaque équipement réseau.

3. Mise en œuvre de la solution

3.1 Environnement de simulation / implémentation

3.1.1 Cisco Packet Tracer

Packet Tracer est un logiciel de CISCO permettant la mise en œuvre d'un réseau, et de simuler le comportement
des protocoles de communication sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. La figure suivante représente le logo de Cisco packet tracer [71].

Figure 4.4: Logo Cisco Packet Tracer [71].

a. Le plan d'adressage :

Le réseau est segmenté en quatre VLANs, chacun avec une plage d'adresse dédiée utilisant le protocole IEEE 802.Q pour l'encapsulation des trames.

Nom de VLAN	Son numéro	Adresse réseau et masque	Adresse passerelle	Technologies et normes utilisées
APPRO	VLAN 10	192.168.10.0/24	192.168.10.1/24	Vlan IEEE 802.1Q
RH	VLAN 20	192.168.20.0/24	192.168.20.1/24	Vlan IEEE 802.1Q
IT	VLAN 30	192.168.30.0/24	192.168.30.1/24	Vlan IEEE 802.1Q
WLC	VLAN 88	192.168.88.0/24	192.168.88.1/24	Vlan IEEE 802.1Q

Tableau 4.3 : Table d'adressage des VLANs.

Les équipent réseau sont configurés avec des adresse IP statique, chacune correspondant à une fonction spécifique, facilitant la gestion du réseau.

Equipement	Interface	IP adresse	Masque	Gateway
Serveur Mail	Fa0	192.168.88.253	255.255.255.0	192.168.88.1
Serveur Radius	Fa0	192.168.88.102	255.255.255.0	192.168.88.1
Contrôleur WLC	Management	192.168.88.3	255.255.255.0	192.168.88.1
Pc Administrateur	Fa0	192.168.88.250	255.255.255.0	192.168.88.1

Tableau 4.4 : Table d'adressage des interfaces.

4. Mise en œuvre de la sécurité Wi-Fi

4.1 Configuration des Switches

Etape 1 : Les configurations de base des équipements

1. **Au niveau de chaque commutateur**

Configurer chaque switch en suivant les instructions indiquées. Un exemple de configuration du switch cœur est donné ci-dessous :

- Désactiver la recherche DNS :

```
Switch(config)#no ip domain-lookup
```

Figure 4.5 : Désactiver la recherche DNS.

- Configurer les noms d'hôte des périphériques comme c'est indiqué dans la topologie de la figure 4.3 puis activer le cryptage des mots de passe, Enfin sécuriser le mode privilégié par un mot de passe (switch-dist : PCHdist2025, trois switches d'accès 1,2 ,3 comme suit : PCHAccess2025, PCHAccess22025, PCHAccess32025).

```
Switch(config)#hostname SW-Coeur
SW-Coeur(config)#service password-encryption
SW-Coeur(config)#banner motd #Acces reserve aux personnes autorisees#
SW-Coeur(config)#enable password PCHcoeur2025
```

Figure 4.6 : Nommer switch cœur et définir un mot passe.

2. **Au niveau des commutateurs**

- **Activer le SSH sur chaque commutateur de la couche cœur et distribution, accès :**

Nous avons mis en place la configuration du protocole SSH, cela inclut la création d'un utilisateur avec un mot de passe, la définition d'un nom de domaine, la génération d'une clé RSA et l'activation de l'accès SSH sur les lignes VTY.

```
SW-Coeur(config)#username Admin password PCHcoeur2025
SW-Coeur(config)#ip domain-name cisco.com
SW-Coeur(config)#crypto key generate rsa
SW-Coeur(config)#line vty 0 4
*Mar 1 0:7:6.775: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:7:6.775: %SSH-5-ENABLED: SSH 1.5 has been enabled
SW-Coeur(config-line)#transport input ssh
SW-Coeur(config-line)#LOGIN
```

Figure 4.7 : Les commandes d'activation SSH sur switch cœur.

Etape 2 : Configuration des VLANs

1. **Créations des VLANs**

- Créer les quatre VLANs (VLAN 10, VLAN 20, VLAN 30, VLAN 40) au niveau du switch cœur en référant au Tableau 4.3.

Un exemple de création de VLAN (cas VLAN 10) est donné par le script suivant :

```
SW-Coeur(config)#vlan 10
SW-Coeur(config-vlan)#name APPRO
SW-Coeur(config-vlan)#ex
```

Figure 4.8 : Création de VLAN 10.

- Enregistrer les configurations :

```
SW-Coeur#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Figure 4.9 : Enregistrer les configurations.

- Vérifier la configuration des VLANs :

Pour vérifier que tous les VLANs sont attribués et configurés correctement, nous exécutons la commande "show vlan brief ".Cela nous fournira un aperçu des VLANs avec leurs paramètres.

```
SW-Coeur#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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
                                                Gig0/2
10   APPRO                            active
20   RH                               active
30   IT                               active
88   WLC                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 4.10 : La commande show vlan brief sur switch cœur.

- Configuration des interfaces virtuelles des commutateurs

Configurer chaque VLAN (10, 20, 30 et 88) en attribuant une adresse IP virtuelle en suivant Tableau 4.3, un exemple de configuration de l'interface virtuelle du VLAN 10 sur switch cœur est donné par le script suivant :

```
SW-Coeur#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Coeur(config)#interface vlan10
SW-Coeur(config-if)#ip address 192.168.10.1 255.255.255.0
SW-Coeur(config-if)#exit
```

Figure 4.11 : Configuration de l'interface vlan 10.

2. Configuration des liaisons d'agrégation et des liaisons d'accès

a) Au niveau de la couche cœur :

- Configurer des interfaces du switch cœur en mode accès pour connecter à des utilisateurs

```
SW-Coeur(config)#interface range f0/1-4
SW-Coeur(config-if-range)#switchport mode access
SW-Coeur(config-if-range)#switchport access vlan 88
SW-Coeur(config-if-range)#ex
```

Figure4.12 : La commande de configuration en mode accès sur switch cœur.

- Une interface en mode trunk pour permettre l'acheminement des paquets émanant de plusieurs VLAN (APPRO, RH, IT, WLC) afin de permettre la communication inter VLANs

```
SW-Coeur(config)#int gig0/1
SW-Coeur(config-if)#switchport trunk encapsulation dot1q
SW-Coeur(config-if)#switchport mode trunk
SW-Coeur(config-if)#switchport trunk allowed vlan 10,20,30,88
```

Figure4.13 : Les commandes de configuration en mode trunk sur switch cœur.

- Enregistrer les configurations **:**

```
SW-Coeur#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Figure 4.14 : Enregistre les configurations.

b) Au niveau de la couche distribution

- Configurer les interfaces en mode trunk

```
SW-Dist(config)#interface GigabitEthernet0/1
SW-Dist(config-if)# switchport trunk encapsulation dot1q
SW-Dist(config-if)#switchport mode trunk
SW-Dist(config-if)#switchport trunk allowed vlan 10,20,30,88
SW-Dist(config-if)#ex
SW-Dist(config)#interface FastEthernet0/2
SW-Dist(config-if)#switchport trunk encapsulation dot1q
SW-Dist(config-if)# switchport mode trunk
SW-Dist(config-if)# switchport trunk allowed vlan 10,88
SW-Dist(config-if)#ex
SW-Dist(config)#interface FastEthernet0/3
SW-Dist(config-if)#switchport trunk encapsulation dot1q
SW-Dist(config-if)# switchport mode trunk
SW-Dist(config-if)# switchport trunk allowed vlan 20,88
SW-Dist(config-if)#ex
SW-Dist(config)#interface FastEthernet0/4
SW-Dist(config-if)#switchport trunk encapsulation dot1q
SW-Dist(config-if)# switchport mode trunk
SW-Dist(config-if)#switchport trunk allowed vlan 30,88
```

Figure 4.15 : Configuration en mode trunk sur switch distribution**.**

c) Au niveau de couche accès

- Configurer les interfaces suivant en mode trunk sur les switches accès 1, 2,3

```
SW-Access1(config)#interface FastEthernet0/1
SW-Access1(config-if)#switchport access vlan 10
SW-Access1(config-if)#switchport mode trunk
SW-Access1(config-if)#switchport trunk allowed vlan 10,88
SW-Access1(config-if)#ex
SW-Access1(config)#interface FastEthernet0/2
SW-Access1(config-if)#switchport access vlan 88
SW-Access1(config-if)#switchport mode trunk
SW-Access1(config-if)#switchport trunk native vlan 88
SW-Access1(config-if)#switchport trunk allowed vlan 10,20,30,88
```

Figure 4.16 : Configuration en mode trunk sur switch d'accès 1.

```
SW-Access2(config)#interface FastEthernet0/1
SW-Access2(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-Access2(config-if)#switchport mode trunk
SW-Access2(config-if)#switchport trunk allowed vlan 20,88
SW-Access2(config-if)#ex
SW-Access2(config)#interface FastEthernet0/2
SW-Access2(config-if)#switchport access vlan 88
SW-Access2(config-if)#switchport mode trunk

SW-Access2(config-if)#switchport trunk native vlan 88
SW-Access2(config-if)#switchport trunk allowed vlan 10,20,30,88
```

Figure 4.17 : Configuration en mode trunk sur switch d'accès 2.

```
SW-Access3(config)#interface FastEthernet0/1
SW-Access3(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
SW-Access3(config-if)#switchport mode trunk
SW-Access3(config-if)#switchport trunk allowed vlan 30,88
SW-Access3(config-if)#ex
SW-Access3(config)#interface FastEthernet0/2
SW-Access3(config-if)#switchport access vlan 88
SW-Access3(config-if)#switchport mode trunk
```

Figure 4.18 : Configuration en mode trunk sur switch d'accès 3.

Etape 3 : Attribution dynamique des adresses IP

Pour chaque VLAN (10, 20,30 et 88) créer les plages d'adresse DHCP conformément au tableau 4.3 Exemple : Figure 4.19 illustre la configuration de la plage DHCP pour le VLAN 10.

```
SW-Coeur(config)#ip dhcp pool vlan10
SW-Coeur(dhcp-config)# network 192.168.10.0 255.255.255.0
SW-Coeur(dhcp-config)# default-router 192.168.10.1
SW-Coeur(dhcp-config)#dns-server 192.168.1.1
```

Figure 4.19 : Les commandes de configuration DHCP pour VLAN 10.

- Exclusions des intervalles d'adresses IP sont suivants :

Cela permet d'éviter les conflits d'adresses entre les équipements configurées statiquement et les clients configurés dynamiquement via DHCP. Ces exclusions assurent une gestion réseau plus fiable.

```
SW-Coeur(config)#ip dhcp excluded-address 192.168.10.2 192.168.10.10
SW-Coeur(config)#ip dhcp excluded-address 192.168.20.2 192.168.20.10
SW-Coeur(config)#ip dhcp excluded-address 192.168.30.2 192.168.30.10
SW-Coeur(config)#ip dhcp excluded-address 192.168.88.2 192.168.88.10
```

Figure 4.20 : Exclusion des intervalles d'adresses IP.

4.2 Configuration des Points d'accès

Les points d'accès (APPRO, RH et IT) sont configurés en mode DHCP afin d'obtenir automatiquement une adresse IP depuis le serveur.

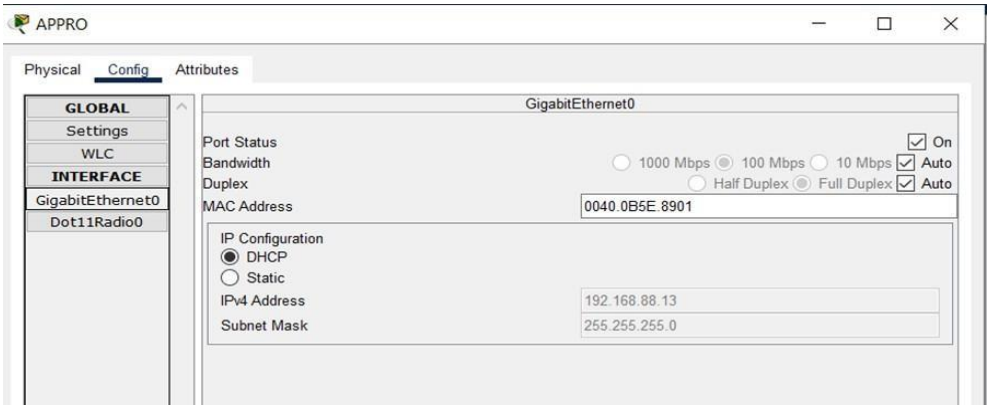

Figure 4.21 : L'adresse attribuée au point d'accès APPRO par DHCP.

4.3 Configuration des clients

Les terminaux (laptot, Pc et tablette) sont configurés en mode DHCP afin de recevoir automatiquement une adresse IP, une passerelle et des serveurs DNS depuis le réseau, comme illustré ci-dessous

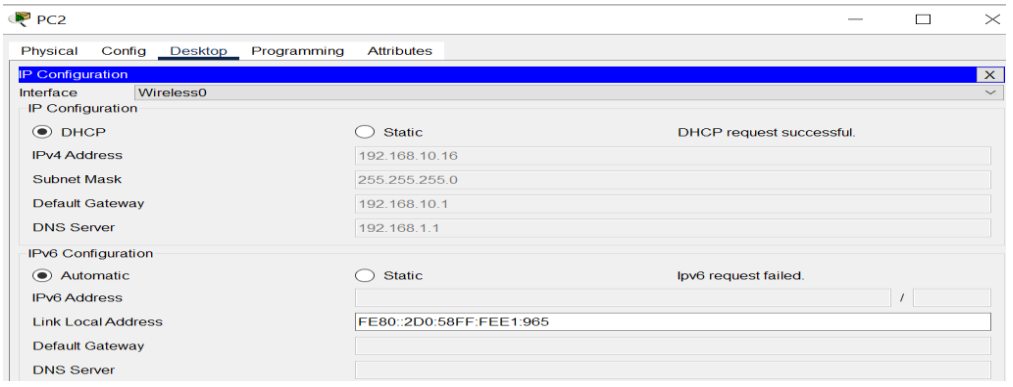

Figure 4.22 : L'adresse attribuée aux Pc2 par DHCP.

4.4 Configuration des utilisateurs

Dans chaque utilisateur créer les quatre profile, l'interface nous propose alors une liste de réseau sans fil disponibles, nous sélectionnons le nom de réseau souhaité, puis choisissons le mode infrastructure, Ensuite nous choisissons WPA2-Enterprise, Pour faire cela il faudrait suivre les commandes suivants :

Tout d'abord, nous avons créé un nouveau profil nommée APPRO-WIFI.

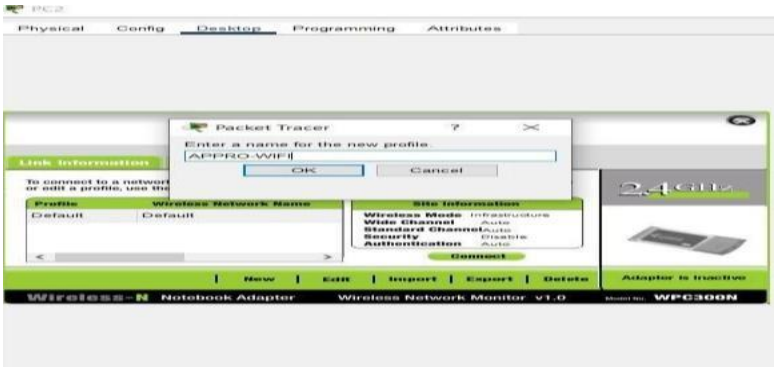

Figure 4.23 : Création du profil APPRO-WIFI.

Puis, nous avons sélectionné le réseau sans fil APPRO dans la liste des réseaux disponibles, et aussi nous avons cliqué sur connect pour établir la connexion.

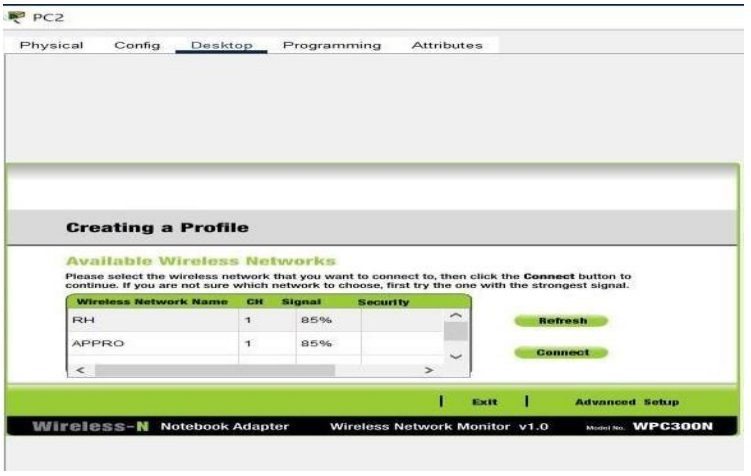

Figure 4.24 : Liste des réseaux sans fil disponible.

Ensuite, nous avons choisi le mode infrastructure pour une Connexion au réseau APPRO, et nous avons sélectionné l'option obtenir les paramètres réseau automatiquement (DHCP), dans sécurité nous avons choisi WPA2- Enterprise, puis nous avons saisi le nom d'utilisateur et le mot passe associer pour l'authentification Wi-Fi.

Figure 4.25 : Saisie des identifiants d'authentification.

Ainsi, une confirmation du profile APPRO validé

Figure 4.26 : Confirmation des nouveaux paramètres du profil.

Enfin, la connexion entre point d'accès et pc

Figure 4.27 : Connexion au point d'accès réussie.

4.5 Configuration Serveur Radius

Pour la configuration du serveur radius, nous avons d'abord attribué une adresse IP statique, un masque et une passerelle par défaut via l'onglet IP configuration.

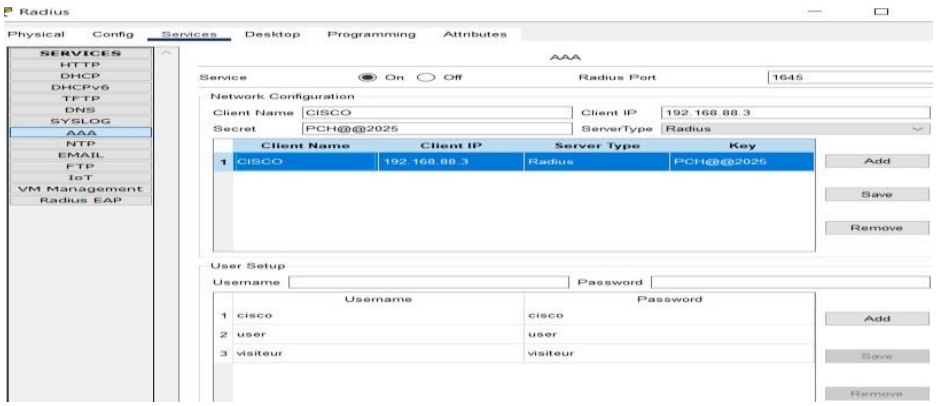

Figure 4.28 : Activation du service AAA sur le serveur RADIUS.

Ensuite, dans l'onglet services, nous avons activé le service AAA (Authentication, Authorization, Acounting) et aussi les services HTTP et HHTPS.

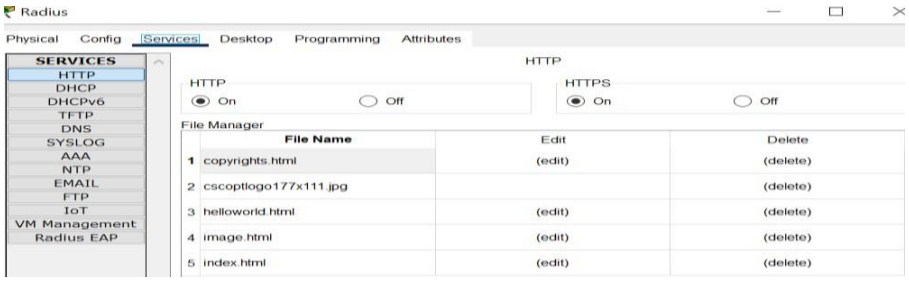

Figure 4.29 : Activation des services web (HHTP/HTTPS) sur le serveur radius.

Enfin, le serveur RADIUS a été configuré pour fournir le service DHCP, en définissent des pools d'adresse IP pour différents VLANs du réseau.

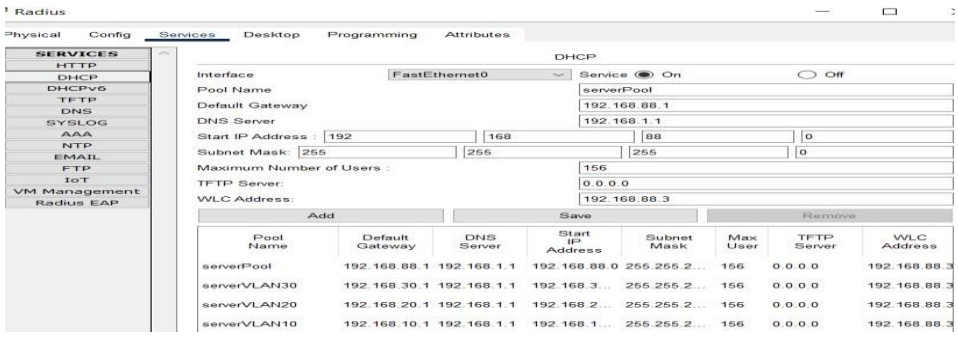

Figure 4.30 : Activation du service DHCP sur le serveur radius.

4.6 Serveur Mail

Dans cette partie, nous avons commencé par configurer le serveur mail avec les paramètres nécessaires puis nous avons créé des comptes utilisateurs (user, admin, visiteur, mail) pour les équipements ce qui leur permis d'échanger des emails entre eux de manière sécuriser et fiable.

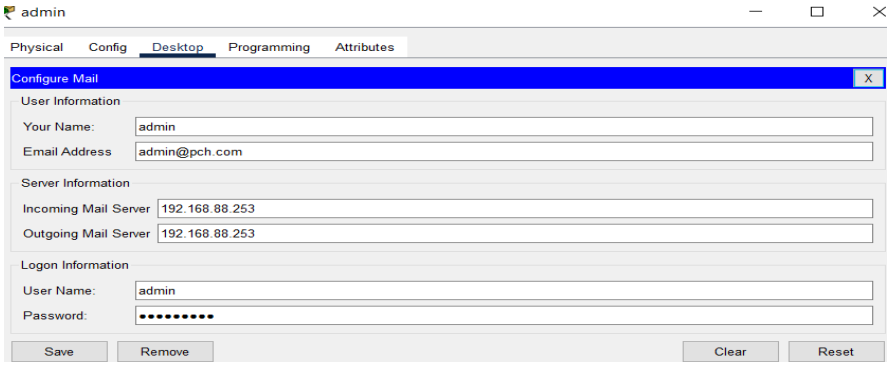

Figure 4.31 : Configuration du compte messagerie sur pc admin.

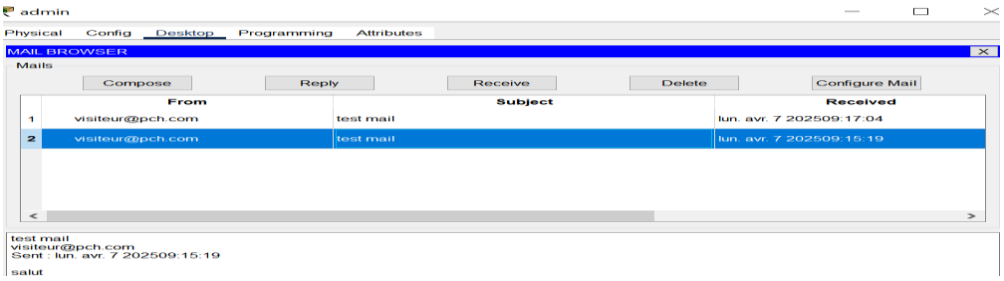

Figure 4.32 : Pc admin reçoit l'e-mail de la part smartphone.

4.7 Configuration Contrôleur WLC

Nous allons ajuster l'adresse IP du contrôleur en fonction du VLAN auquel il est associé, plus précisément VLAN 88.

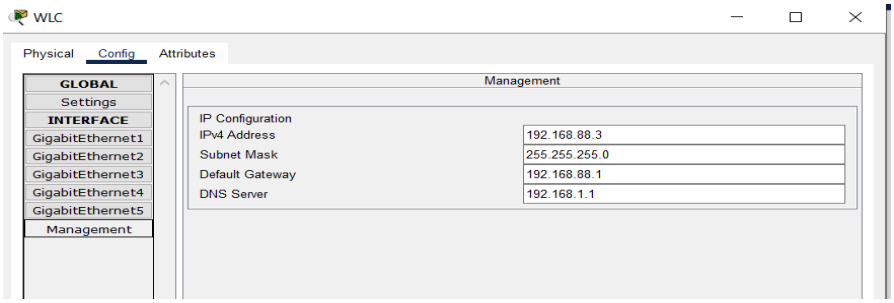

Figure 4.33 : Attribution des adresses IP au contrôleur.

D'abord nous avons lancé un Ping sur pc admin

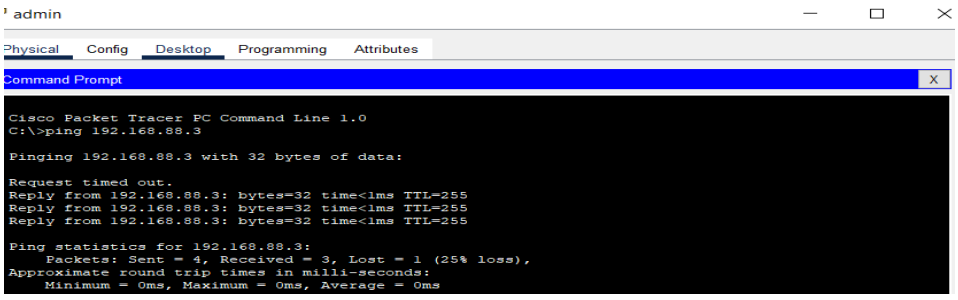

Figure 4.34 : Ping de l'adresse IP contrôleur WLC sur pc admirateur.

Dans la page de connexion d'un contrôleur (WLC), nous avons saisi le nom d'utilisateur et un mot de passe afin d'accéder à l'interface de gestion et configurer le réseau Wi-Fi.

Figure 4.35 : Demande d'authentification.

a. Configuration de l'authentification RADIUS

Dans cette partie nous avons configuré serveur d'authentification Radius avec un port 1645

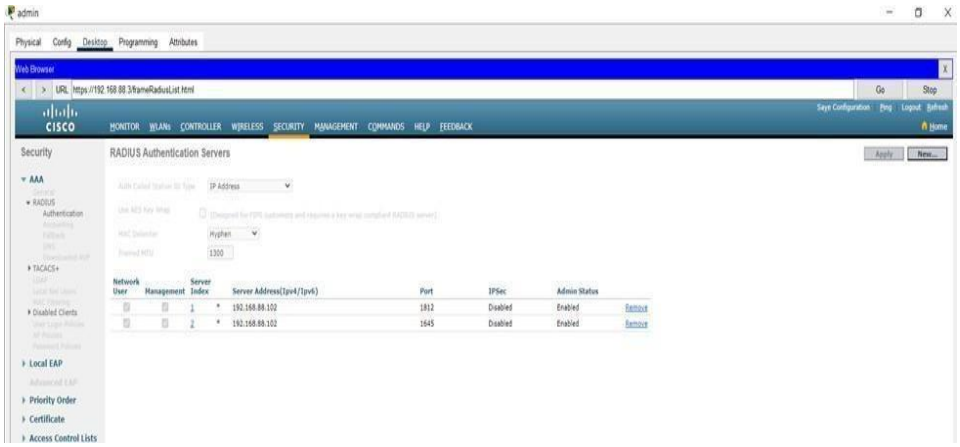

Figure 4.36 : Intégration serveur radius.

b. Controller

Dans la case Contrôleur nous avons configuré les interfaces (APPRRO, RH, IT)

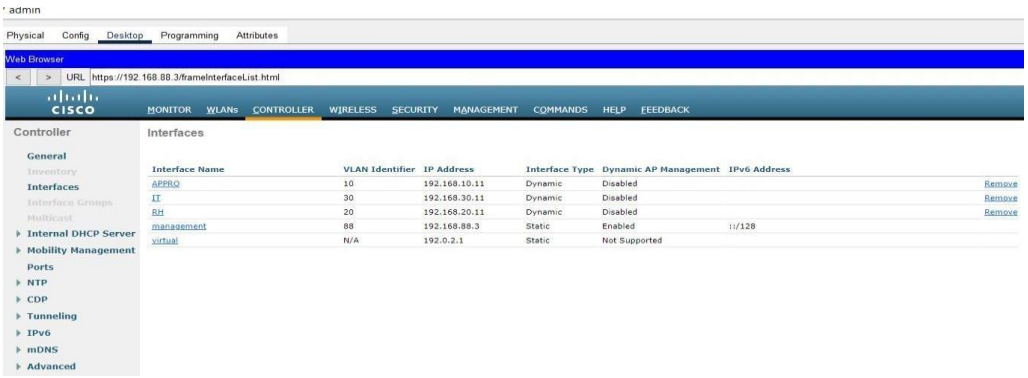

Figure 4.37 : Liste des interfaces.

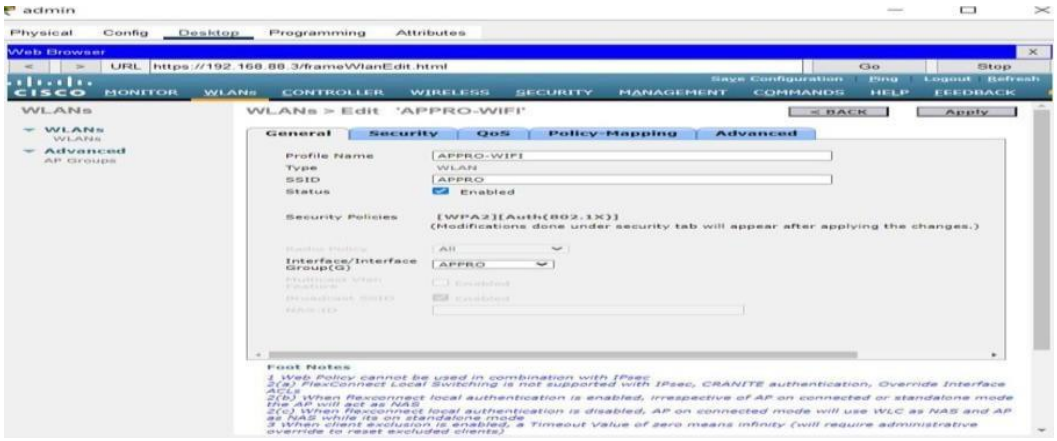

Figure 4.38 : Paramètres d'accès APPRO-WIFI.

Nous avons configuré le WLAN « APPRO-WIFI » est configuré en mode WPA2-Enterprise avec Authentification 802.1X. Ce mode utilise le protocole PEAP pour authentifier les utilisateurs via un serveur radius, l'encryptions est assurée par AES, garantissant la confidentialité des données transmises.

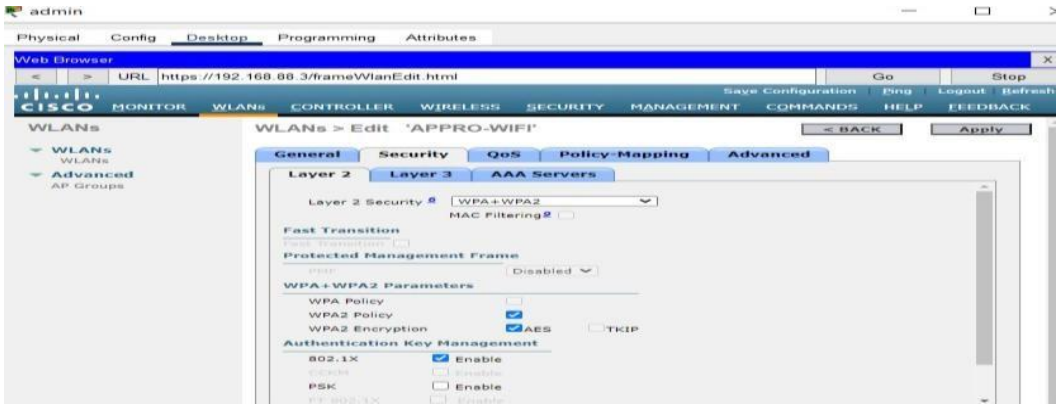

Figure 4.39 : Sécurité APPRO-WIFI.

Nous avons configuré le serveur radius pour l'authentification des utilisateurs du WLAN.

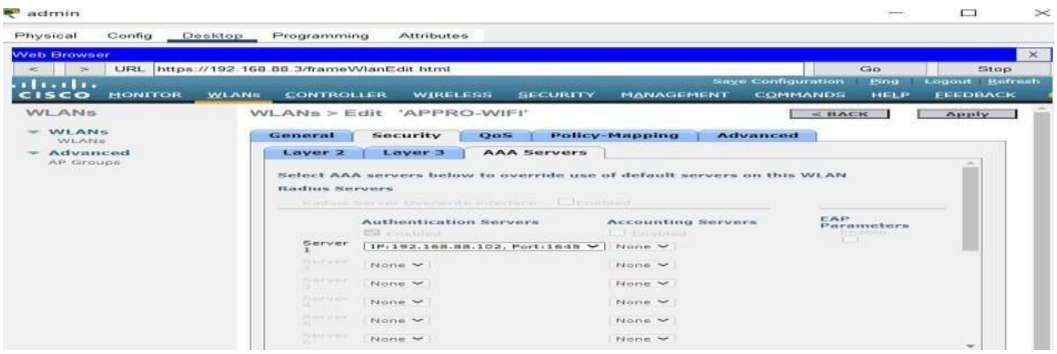

Figure 4.40 : Sécurité AAA servers.

Nous avons créé trois WLANs (APPRO-WIFI, RH-WIFI, IT- WIFI) pour assurer une sécurité renforcée via un serveur RADIUS.

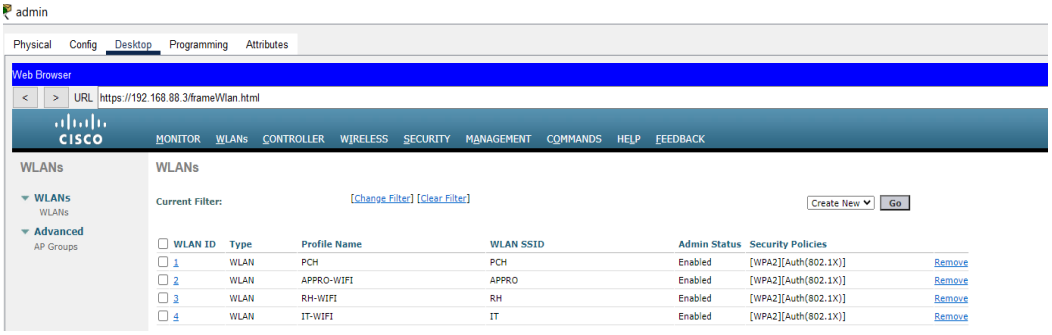

Figure 4.41 : Liste WLans.

Maintenant, nous allons former trois groupes (APPRO, IT, RH). Pour créer un groupe, il suffit de cliquer sur "Ajouter un nouveau groupe AP "pour l'ajouter.

Figure 4.42 : Liste des AP Groups configurés.

5. Partie Analyse

i. Tests et validation de la solution

- **Scénarios de tests réalisés :**

Nous avons effectué des tests de connectivité en envoyant des requêtes ICMP entre les différents équipements du réseau. Figure (4.43) Tester la connectivité.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Laptop1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Tablet ...	Laptop2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Smartp...	Laptop0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	Multilayer Swit...	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC0	Multilayer Swit...	ICMP		0.000	N	4	(edit)	(delete)
	Successful	Radius	Multilayer Swit...	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Laptop1	Mail	ICMP		0.000	N	6	(edit)	(delete)
	Successful	Tablet ...	Radius	ICMP		0.000	N	7	(edit)	(delete)
	Successful	Tablet ...	Mail	ICMP		0.000	N	8	(edit)	(delete)
	Successful	PC1	Radius	ICMP		0.000	N	9	(edit)	(delete)
	Successful	Radius	admin	ICMP		0.000	N	10	(edit)	(delete)
	Successful	Laptop0	Mail	ICMP		0.000	N	11	(edit)	(delete)
	Successful	PC1	admin	ICMP		0.000	N	12	(edit)	(delete)
	Successful	Tablet ...	admin	ICMP		0.000	N	13	(edit)	(delete)
	Successful	PC1	Radius	ICMP		0.000	N	14	(edit)	(delete)
	Successful	Laptop0	Mail	ICMP		0.000	N	15	(edit)	(delete)
	Successful	Tablet ...	Radius	ICMP		0.000	N	16	(edit)	(delete)

Figure 4.43 : Tester la connectivité.

ii. Avantages de la solution proposée

- **Sécurisation des échanges Wi-Fi :** grâce à l'authentification WPA2-Enterprise, les communications sont sécurises.
- **Centralisation de l'authentification** : le serveur Radius permet de gérer tous les accès.
- **Traçabilité et gestion fine des accès :** Chaque connexion est authentifie et enregistrée et associe à un profil utilisateurs (via les VLANs)

iii. Limites et pistes d'amélioration

✓ **Limite :**

Dépendance à l'infrastructure : La solution repose sur la disponibilité continue de services tels que le serveur Radius et le contrôleur WLC. Toute panne ou défaillance de ces composants peut affecter l'accès au réseau.

✓ **Amélioration :**

Redondance des services critiques : mise en place des serveurs Radius et WLC redondants en cas de panne.

Conclusion

En conclusion, ce chapitre a permis de mettre en place un réseau sans-fil sécurisé basé sur le contrôle d'accès et l'authentification, à l'aide de l'outil de simulation Packet tracer nous avons configuré le contrôleur WLC, les points d'accès, le serveur Radius, le serveur mail ainsi que équipements clients, les tests réalisés ont confirmé la bonne connectivité, l'authentification réussie et le bon fonctionnement de l'infrastructure.

Conclusion générale

En conclusion, le travail présenté dans ce mémoire porte sur l'étude des réseaux sans fil, en particulier la norme IEEE 802.11 (Wi-Fi). Nous avons analysé les différents types de risques et d'attaques auxquels ces réseaux sont exposés. Dans ce contexte , il est essentiel de mettre en place des mesures de sécurité adéquates pour protéger l'intégrité des données, garantir la confidentialité des informations, contrôler l'accès au réseau et authentifier les utilisateurs de manière fiable.

Le mémoire a examiné en détail les différentes dimensions de la sécurité des réseaux sans fil, en mettant l'accent sur l'authentification centralisée via un serveur RADIUS. Il a exploré les risques et les attaques potentielles auxquels les réseaux Wi-Fi sont exposés, tout en proposant des solutions et des techniques de sécurité pour se protéger de ces menaces.

De plus, ce mémoire a présenté une étude de cas sur l'entreprise « Pharmacie Centrale des Hôpitaux », mettant en évidence les problématiques de sécurité auxquelles elle est confrontée. Des solutions spécifiques ont été proposées pour améliorer la sécurité de ce réseau, en mettant en œuvre une authentification basée sur le serveur Radius. Pour mettre en place notre solution, on a utilisé un logiciel de simulation Cisco Packet tracer et nous avons configuré un contrôleur LAN sans fil pour gérer un réseau WI-FI sécurisé en utilisant un serveur RADIUS et la méthode d'authentification est WPA2-Entreprise avec PEAP.

En appliquant ces solutions, ce mémoire a mis en évidence la faisabilité et l'efficacité de l'authentification centralisée à l'aide de serveur RADIUS pour renforcer la sécurité des réseaux Wi-Fi. Il a également souligné l'importance de maitriser les principes fondamentaux des réseaux sans-fil et de la sécurité informatique pour concevoir et déployer des architectures réseau sécurisées.

Pour conclure, ce mémoire a permis de proposer et de mettre en œuvre une solution de sécurisation d'un réseau sans fil basée sur le contrôle d'accès et l'authentification via un serveur RADIUS afin de renforcer la sécurité et la fiabilité du réseau.

Références bibliographiques

Référence bibliographies

Livres et Documents Académiques

[2] G. Pujolle, Cours réseaux et télécoms : Avec exercices corrigés, 3e éd., Paris: Eyrolles, 2008, p. 395

[11] F. Dupont, Réseaux sans-fil et réseaux de mobiles, pp. 280-284.

[57] M. Gaha, Sécurité dans les réseaux Wi-Fi : étude détaillée des attaques et proposition d'une architecture Wi-Fi sécurisée, mémoire de maîtrise, Université du Québec à Montréal, 2007. [En ligne]. Disponible sur : https://archipel.uqam.ca/4850/1/M9822.pdf. [Consulté le : 30-mai-2025]

[58] M. Monnier, WPA, projet de cryptographie, MIF30, Université Claude Bernard Lyon 1, 2008/2009. [En ligne]. Disponible sur : https://laure.gonnord.org/pro/teaching/MIF30/projets2009/monnier_rapport.pdf

Présentations universitaires

[10] "ETUDE ET SIMULATION DES TECHNOLOGIES," 2023 - 2024. [En ligne]. Disponible sur : https://polytechnique.mg/these/194800.

Articles et documents en ligne

[1] TecnoDigital, "Réseau sans fil Qu'est-ce que c'est : tout ce que vous devez savoir," [En ligne]. Disponible sur : https://informatecdigital.com/fr/r%C3%A9seau-sans-fil-c'est- tout-ce-que-vous-devez-savoir/#google_vignette. [Accessed 07 JUL 2023]

[3] Fortinet, "Qu'est-ce qu'un réseau sans fil ? Types de réseaux sans fil," [En ligne]. Disponible sur : https://www.fortinet.com/fr/resources/cyberglossary/wireless-network

[4] D. Wiki, "Réseau WiFi Ad-hoc," 22 Fev 2012, [En ligne]. Disponible sur : https://wiki.debian.org/fr/WiFi/AdHoc

[5] CommentOuvrir, "Différence entre le mode Ad-hoc et le mode infrastructure : avantages et inconvénients," [En ligne]. Disponible sur : https://commentouvrir.com/tech/difference-entre-le-mode-ad-hoc-et-le-mode- infrastructure-avantages-et-inconvenients/

[6] "VPN Unlimited," [En ligne]. Disponible sur : https://www.vpnunlimited.com/fr/help/cybersecurity/protocol-stack

Référence bibliographies

[7] T. Michel, "Le Standard 802.11 Couche physique et couche MAC," Mars 2007. [En ligne]. Disponible sur : https://fr.doczz.net/doc/131614/le-standard-802.11-couche- physique-et-couche-ma

[8] 2023 [En ligne].Disponible sur : https://elearning.univ-bejaia.dz/pluginfile.php/985140/mod_resource/content/1/main.pdf

[9] StudySmarter, "Protocoles MAC," [En ligne]. Disponible sur : https://www.studysmarter.fr/resumes/ingenierie/ingenierie-des- telecommunications/protocoles-mac/

[12] J.-P. Lips, "Les réseaux sans fils," 2009 - 2010. [En ligne]. Disponible sur : https://fr.scribd.com/document/561561134/Les-Reseaux-Sans-Fils

[14] "Réseau sans fil technologie wi-fi," 07 Feb 2014. [En ligne]. Disponible sur : https://de.slideshare.net/slideshow/rseau-sans-fil-technologie-wifi/30953268

[15] L. R. DegroupTest, "Wi-Fi : normes, débit, portée et sécurité," [En ligne]. Disponible sur : https://www.degrouptest.com/guide/wi-fi . [Accessed 2025 Mai 15]

[16] Y. Tijani, "Réseaux domestiques : Comment mettre en réseau les ordinateurs de votre maison," 03 10 2012. [En ligne]. Disponible sur : https://cimbcc.org/wp- content/uploads/Notes-2012-10-03-1.pdf

[17] T.M, "Introduction aux RSF & Rx mobiles," 2027-2028. [En ligne]. Disponible sur : https://elearning.univ-bejaia.dz/pluginfile.php/1080314/mod_resource/content/1/Slides%20Cours%20WPAN_ NB.pdf

[18] "La norme IEEE 802.11," 6 Décembre 2013. [En ligne]. Disponible sur : https://msir004.wordpress.com/2013/12/06/la-norme-ieee-802-11/

[19] Cursa, "Sécurité du réseau sans fil," [En ligne]. Disponible sur : https://cursa.app/fr/page/securite-du-reseau-sans-fil

[20] digiSchool, "Les risques informatiques," [En ligne]. Disponible sur : https://www.digischool.fr/cours/les-risques-informatiques.

[21] "Qu'est-ce que la sécurité des application," [En ligne]. Disponible sur : https://www.f5.com/fr_fr/glossary/application-security.

[22] WayToLearnX, "Différence entre attaque active et attaque passive," [En ligne]. Disponible sur : https://waytolearnx.com/2018/07/difference-entre-attaque-active-et- attaque-passive.html

Référence bibliographies

[23] Connect-Editions Diamond, "Attaque par déni de service dans le Wi-Fi," [En ligne]. Disponible sur : https://connect.ed-diamond.com/GNU-Linux-Magazine/glmfhs- 099/attaque-par-deni-de-service-dans-le-wi-fi

[24] Technobrice, "aireplay-ng:inject packets into a wirelless network-command examples," [En ligne]. Disponible sur : https://www.technobrice.com/tech/tbg/aireplay-ng-inject- packets-into-a-wireless-network-command-examples/

[25] VPN Unlimited, "Attaque DHCP," [En ligne]. Disponible sur : https://www.vpnunlimited.com/fr/help/cybersecurity/dhcp-attack.

[26] Un Téléphone, "Comment cracker un mot de passe," [En ligne]. Disponible sur : https://untelephone.com/comment-cracker-un-mot-de-passe/

[27] VPN Unlimited, "MAC Spoofing," [En ligne]. Disponible sur : https://www.vpnunlimited.com/fr/help/cybersecurity/mac-spoofing

[28] Panda Security, "Attaque Man-in-the-Middle," [En ligne]. Disponible sur : https://www.pandasecurity.com/fr/mediacenter/attaque-man-in-the-middle/

[29] Clicours, "Cours : Les mécanismes de sécurité des réseaux sans fil Wi-Fi," [En ligne], Disponible sur : https://www.clicours.com/cours-les-mecanismes-de-securite-des- reseaux-sans-fil-wi-fi/.

[30] WayToLearnX, "Différence entre le cryptage symétrique et asymétrique," [En ligne]. Disponible sur : https://waytolearnx.com/2018/07/difference-entre-le-cryptage- symetrique-et-asymetrique.html

[31] Secret Defense, "Le hashage expliqué : fondamentaux pour la sécurité des données," [En ligne]. Disponible sur : https://www.secret-defense.org/cybersecurite/le-hashage- explique-fondamentaux-pour-la-securite-des-donnees/#:~:text=Le%20hashage%2C%20ou%20hachage%20en%20fran%C3%A7ais%2C%20est%20une,permet%20d%27assurer%20l%27int%C3%A9grit%C3%A9%20des%20donn%C3%A9es%20tr

[32] Dataconomy, "Qu'est-ce qu'un algorithme MD5 et comment fonctionne-t-il ?," [En ligne]. Disponible sur : https://fr.dataconomy.com/2023/07/11/quest-ce-quun- algorithme-md5-et-comment-fonctionne-t-il-leconomie-des-donnees/

[33] HowToHosting.Guide, "What is SHA(Secure Hash Algorithm) ?," [En ligne]. Disponible sur : https://howtohosting.guide/fr/definitions/what-is-sha-secure-hash- algorithm/

Référence bibliographies

[34] Wikipédia, "PBKDF2," [En ligne]. Disponible sur : https://fr.wikipedia.org/wiki/PBKDF2

[35] Okta, "HMAC," [En ligne]. Disponible sur : https://www.okta.com/fr/identity- 101/hmac/

[36] Z.Farah, "Sécurité informatique," [En ligne]. Disponible sur : Z. Farah, Sécurité informatique [en ligne], Université de Béjaïa, s.d. Disponible sur : https://elearning.univbejaia.dz/pluginfile.php/603267/mod_resource/content/0/Cours_FARAH%20Zoubeyr_ SECURITE%20INFORMATIQUE.pdf

[37] Kiteworks, "Public vs Private Key Encryption," [En ligne]. Disponible sur : https://www.kiteworks.com/fr/partage-securise-de-fichirs/public-vs-private-key-encryption/#Chiffrement_symetrique

[38] Geekflare, "Types de cryptographie," [En ligne]. Disponible sur : https://geekflare.com/fr/cryptography-types/

[39] Cybersecurite-Management.fr, "L'Advanced Encryption Standard (AES) : un gardien discret de la sécurité numérique," [En ligne]. Disponible sur : https://cybersecurite-management.fr/ladvanced-encryption-standard-aes-un-gardien-discret-de-la-securite-numerique/

[40] Wikipédia, "International Data Encryption Algorithm," [En ligne]. Disponible sur : https://fr.wikipedia.org/wiki/International_Data_Encryption_Algorithm

[41] Kiteworks, "Public vs Private Key Encryption," [En ligne]. Disponible sur : https://www.kiteworks.com/fr/partage-securise-de-fichirs/public-vs-private-key- encryption/

[42] Progresser en Maths, "Le chiffrement RSA : cours et exercice," [En ligne]. Disponible sur : https://progresser-en-maths.com/le-chiffrement-rsa-cours-et-exercice/

[43] Malekal, "Chiffrement, cryptage des données : comment ça marche ?," [En ligne]. Disponible sur : https://www.malekal.com/chiffrement-cryptage-donnees-comment-ca- marche/

[44] ITI, "Sécurité de l'information : traçibilité des données," [En ligne]. Disponible sur : https://iti.ca/fr/blogue/securite-sauvegarde/securite-information-tracabilite-des- donnees/

[45] D. SO, “Sécurisation des réseaux sans fil,” FORMIP, 23-oct-2023. [En ligne]. Disponible sur : https://www.formip.com/pages/blog/sécurisation-des-réseaux-sans-fil/ [Consulté le : 29-mai-2025]

[46] M. Souilah, “Le protocole AAA,” LinkedIn, [En ligne]. Disponible sur : https://www.linkedin.com/pulse/le-protocole-aaa-mohamed-souilah/ [Consulté le : 30-mai- 2025]

Référence bibliographies

[47] B. Belkhir, Introduction Générale – Généralités sur les réseaux et sécurité informatique. Scribd, transféré par H. Ssan, 08-sept.-2024. [En ligne]. Disponible sur : https://fr.scribd.com/document/767034930/Introduction-generale-belkhir [Consulté le : 29- mai-2025]

[48] Wikipédia, "Kerberos (protocole)," Wikipédia, 27-mai-2025. [En ligne]. Disponible sur : https://fr.wikipedia.org/wiki/Kerberos_(protocole) [Consulté le : 30-mai-2025]

[49] ORSYS, "AAA : Authentication, Authorization, Accounting," ORSYS Le Mag - Glossaire, [En ligne]. Disponible sur : https://orsys-lemag.com/Glossaire/aaa-authentication-authorization-accounting/ [Consulté le : 30-mai-2025]

[50] "Remote Authentication Dial-In User Service (RADIUS)," F5 Glossary, [En ligne]. Disponible sur : https://www.f5.com/fr_fr/glossary/remote-authentication-dial-in- user-service-radius [Consulté le : 30-mai-2025]

[51] C. Duvallet, "Le protocole RADIUS – Remote Authentication Dial-In User Service," Université du Havre, [En ligne]. Disponible sur : https://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/CNAM/CNAM-Cours-ServeurRadius.pdf. [Consulté le : 30-mai-2025]

[52] Huawei, "What Is RADIUS? How Does RADIUS Work?", Huawei Technical Support, [En ligne]. Disponible sur : https://info.support.huawei.com/info-finder/encyclopedia/en/RADIUS.html. [Consulté le : 30-mai-2025]

[53] D. Roussel, " RADIUS : Remote Authentication Dial-In User Service," Université Gustave Eiffel – IGM, [En ligne]. Disponible sur : https://igm.univ-mlv.fr/~dr/XPOSE2007/jgauth02_RADIUS/802_1x.html. [Consulté le : 30-mai-2025]

[54] WireX Systems, "What Is RADIUS? Understanding Network Protocols," WireX Systems, [En ligne]. Disponible sur : https://wirexsystems.com/resource/protocols/radius. [Consulté le : 30-mai-2025]

[55] B. B. Isaac, "Pourquoi utiliser RADIUS dans un réseau ? " Bushtech, 27 février 2025. [En ligne]. Disponible sur : https://bushtechno.blogspot.com/2025/02/pourquoi-utiliser- radius-dans-un-reseau.html

[56] Microsoft, "Qu'est-ce que le contrôle d'accès ?", Microsoft Security, [En ligne]. Disponible sur : https://www.microsoft.com/fr-ca/security/business/security-101/what-is-access-control [Consulté le : 30-mai-2025]

Référence bibliographies

[57] M. Gaha, Sécurité dans les réseaux Wi-Fi : étude détaillée des attaques et proposition d'une architecture Wi-Fi sécurisée, mémoire de maîtrise, Université du Québec à Montréal, 2007. [En ligne]. Disponible sur : https://archipel.uqam.ca/4850/1/M9822.pdf. [Consulté le : 30-mai-2025]

[58] M. Monnier, WPA, projet de cryptographie, MIF30, Université Claude Bernard Lyon 1, 2008/2009. [En ligne]. Disponible sur : https://laure.gonnord.org/pro/teaching/MIF30/projets2009/monnier_rapport.pdf

[59] phoenixNAP, "Qu'est-ce que le protocole d'authentification extensible (EAP) ?", phoenixNAP Glossaire, 4 juin 2024. [En ligne]. Disponible sur : https://www.phoenixnap.fr/glossaire/protocole-d%27authentification-extensible-eap

[60] G. Lehembre, WPA / WPA2 : Une sécurité fiable pour le Wi-Fi ?, Groupe Sécurité Unix et Réseau, Hervé Schauer Consultants, 14 juin 2005. [En ligne]. Disponible sur : https://www.ossir.org/sur/supports/2005/ossir_wpa_wpa2.pdf

[61] Auteur inconnu, Sécurité des réseaux Sans Fil. [En ligne]. Disponible sur : https://d1n7iqsz6ob2ad.cloudfront.net/document/pdf/5385d48cd1c5a.pdf. [Consulté le : 30- mai-2025]

[62] PR Newswire, « Une nouvelle étude révèle une hausse des cyberattaques visant les infrastructures critiques », 19 sept. 2023. [En ligne]

[63] Action Telecom, « Sécurité des réseaux sans fil : Les meilleures pratiques pour protéger votre entreprise contre les cyberattaques », Action Telecom, 28 juin 2023. [En ligne]. Disponible sur : https://www.actiontelecom.fr/securite-des-reseaux-sans-fil-les-meilleures-pratiques-pour-proteger-votre-entreprise-contre-les-cyberattaques/. [Consulté le : 2 juin 2025]

[64] Sysdau, « Quels sont les principaux protocoles de sécurité réseau et comment les mettre en place ? », Sysdau Extranet, 2023. [En ligne]. Disponible sur : https://sysdau-extranet.fr/quels-sont-les-principaux-protocoles-de-securite-reseau-et-comment-les-mettre-en-place/ [Consulté le : 2 juin 2025]

[65] Fortinet, "Wireless Security Tips," Fortinet, [En ligne]. Disponible sur : https://www.fortinet.com/fr/resources/cyberglossary/wireless-security-tips. [Consulté le : 2 juin 2025]

[66] IONOS, « Sécurité wifi : comment renforcer son réseau sans fil », Digital Guide, 22 février 2024. [En ligne]. Disponible sur : https://www.ionos.fr/digitalguide/serveur/securite/securite-wifi-mesures-de-protection-pour-votre-reseau/

[67] "Remote Authentication Dial-In User Service (RADIUS)," F5, https://www.f5.com/glossary/remote-authentication-dial-in-user-service-radius (consulté le 2 juin 2025)

[68] B. Duval, « Les avantages du RADIUS informatique », Citypassenger, 27 février 2020. [En ligne]. Disponible sur : https://citypassenger.com/les-avantages-du-radius/

[69] 1A247d01, Scribd, [En ligne]. Disponible sur : https://fr.scribd.com/document/509690497/1A247d01. [Consulté le : 2 juin 2025].

[70] Orange, «Qu'est-ce qu'un point d'accés?,» [En ligne]. Disponible sur : https://iotjourney.orange.com/fr-FR/connectivite/qu-est-ce-qu-un-point-d-acces. [Consulté le : 3 juin 2025].

[71] M.-U. C. d'Azur, «Utilisation de Packet Tracer,» [En ligne]. Disponible sur : https://webusers.i3s.unice.fr/~map/Cours/LPSILADMIN/UtilisationPacketTracer.pdf.[Consulté le : 3 juin 2025].

Article

[13] T. Daniel, "Standard pour réseaux sans fil : IEEE 802.11," Techniques de l'Ingénieur, 10 Mai 2002.

Résumé

Résumé

Les réseaux sans fil sont aujourd'hui au cœur des infrastructures de communication, offrant mobilité et connectivité indispensables dans de nombreux usages personnels et professionnels. Leur sécurité est cruciale, car ils sont particulièrement vulnérables à diverses attaques telles que les accès non autorisés, par des intrusions exploitant des failles ou des points d'accès malveillants.

Dans ce mémoire, nous proposons une solution efficace pour atténuer ces risques, basée sur un service d'authentification à distance des utilisateurs, communément appelé serveur RADIUS (Remote Authentication Dial-In User Service) ou serveur AAA (Authentication, Authorization, and Accounting). Ce protocole assure la validation sécurisée des utilisateurs à distance, offrant un contrôle d'accès basé sur les rôles et permettant l'authentification sur plusieurs bases de données via différentes méthodes.

Le serveur RADIUS authentifie chaque utilisateur souhaitant se connecter au réseau sans-fil. Il doit d'abord fournir le mot de passe du réseau wifi. Ensuite, le système lui demande ses informations de connexion. Le client RADIUS envoie ces informations au **serveur RADIUS** via le **protocole RADIUS**. Le serveur vérifie alors l'exactitude des informations de connexion en comparant l'identifiant et le mot de passe. Si les informations sont correctes, le serveur répond positivement au client et la connexion établie. Dans le cas contraire, le point d'accès (AP) bloque la connexion et refuse l'accès au réseau, permettant ainsi de mettre en place un réseau sans fil sécurisé par RADIUS basé sur WLC.

Mots clés : Réseaux sans fil, Serveur Radius, WLC, Authentification.

Summary

Wireless networks are at the heart of today's communications infrastructures, offering mobility and connectivity that are indispensable in many personal and professional applications. Their security is crucial, as they are particularly vulnerable to various attacks such as unauthorized access, through intrusions exploiting loopholes or malicious access points.

In this dissertation, we propose an effective solution to mitigate these risks, based on a remote user authentication service, commonly known as a RADIUS (Remote Authentication Dial-In User Service) or AAA (Authentication, Authorization, and Accounting) server. This protocol ensures secure remote user validation, offering role-based access control and enabling authentication on multiple databases via different methods.

The RADIUS server authenticates each user wishing to connect to the wireless network. The user must first provide the wifi network password. Then, the system asks for the user's login information. The RADIUS client sends this information to the RADIUS server via the RADIUS protocol. The server then checks the correctness of the connection information by comparing the login and password. If the information is correct, the server responds positively to the client and the connection is established. If not, the access point (AP) blocks the connection and denies access to the network, making it possible to set up a RADIUS-secured wireless network based on WLC.

Keywords: Wireless networks, Radius server, WLC, Authentication.