Ministère de la formation et de l'enseignement professionnels

Institut National Spécialisé En Formation Professionnelle

«INSFP El-Kseur W.Bejaia »

Mémoire de fin de formation

En vue de l'obtention du Diplôme de Brevet de Technicien Supérieur en INFORMATIQUE ET RESEAUX

Thème

Sécurisation des réseaux sans fil (Wi-Fi)

Organisme d'accueil

Centre de Recherche en Technologies Agro-Alimentaires (CRTAA)

Présenté par :

- **Mr SAIDI Farid**

Encadré par :

- **Mr ZEROUKLANE Salim**

Promotion 2026

Remerciements

***J**'adresse mes sincères remerciements à Madame la Directrice du Centre de Recherche en Technologies Agro-Alimentaires, Pr. BOUCHERBA Nawal, Madame la Sous-Directrice, Pr. DJOUDAD KADJI Hafsa, ainsi que Madame ZETOUT Zohra, pour leur accueil et les conditions de stage favorables mises à ma disposition.*

***M**es remerciements les plus sincères vont à Monsieur ZEROUKLANE Salim, mon encadreur, pour sa patience, sa disponibilité et la qualité de son encadrement. Son accompagnement m'a permis d'avancer avec confiance et rigueur.*

***J**e tiens à adresser un remerciement particulier à Monsieur BOUMARTIT Massinissa, membre du service de gestion et de maintenance des réseaux informatiques du centre, pour son soutien et sa disponibilité tout au long de mon stage.*

***M**es remerciements s'adressent également à l'ensemble du personnel du CRTAA pour leur accueil et leur collaboration.*

***J**'adresse enfin mes remerciements les plus respectueux aux membres du jury pour avoir accepté d'évaluer ce travail.*

Dédicace

C'est avec profonde gratitude et sincère mots que je dédié ce modeste travail de fin de formation :

A mes très chers parents,

A ma chère épouse Wissem qui m'a soutenu tout au long de la période de préparation de ce mémoire.

A Mes chers fils Abderaouf et Aris

A tous les membres de ma famille et de ma belle-famille,

Et enfin à tous mes Amis.

Farid

Table des matières

Chapitre 2 : La sécurité dans les réseaux Wi-Fi

Chapitre 3 : Présentation de l'organisme d'accueil

Chapitre 4 : Mise en œuvre et réalisation

Liste des figures

Liste des tableaux

Liste des abréviations

Abréviation	Signification
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
ACK	Indicateur d'accusé de réception (Acknowledgement)
AP	Access Point (Point d'accès)
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CRTAA	Centre de Recherche en Technologies Agro-Alimentaires
DHCP	Dynamic Host Configuration Protocol
DoS	déni de service
EAP	Extensible Authentication Protocol
EPST	Établissement Public à Caractère Scientifique et Technologique
FAI	Fournisseur Accès Internet
GSM	Groupe Spécial Mobile
GPRS	General Packet Radio Service
IAPAA	Ingénierie des Aliments et des Procédés Agro-Alimentaires
IEEE	Institute of Electrical and Electronics Engineers
IBSS	Independent Basic Service Set
IP	Internet Protocol
IETF	Internet Engineering TASK Force
ISO	International Standards Organization
LAN	Local Area Network
LWAPP	Lightweight Access Point Protocol
MAC	Media Access Control
MITM	Man In The Middle
NAT	Traduction des Adresses de Réseau
NIC	Network Interface Controller
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PEAP	Protected Extensible Authentication Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol

UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WMAN	Wireless Metropolitan Area Networks
WPA 2	Wi-Fi Protected Access 2
WPA 3	Wi-Fi Protected Access 3
WPAN	Wireless Personal Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WWAN	Wireless Wide Area Network

Introduction générale

Les réseaux sans fil, également appelés « Wireless networks », occupent aujourd'hui une place essentielle dans les systèmes de communication modernes. Contrairement aux réseaux filaires traditionnels, ils offrent des avantages considérables tels que la facilité de déploiement, la réduction des coûts d'infrastructure, ainsi qu'une grande mobilité permettant aux utilisateurs d'accéder aux ressources réseau sans contrainte physique.

Cependant, malgré ces atouts, les réseaux sans fil présentent des vulnérabilités importantes liées à la nature même de leur support de transmission. En effet, l'utilisation des ondes radio rend les communications plus exposées aux interceptions, aux écoutes clandestines et aux attaques malveillantes. Cela introduit des risques majeurs en matière de confidentialité, d'intégrité et d'authentification des données échangées, nécessitant ainsi la mise en place de mécanismes de sécurité robustes et adaptés.

Dans ce contexte, la norme IEEE 802.11, communément connue sous le nom de Wi-Fi, s'est imposée comme le standard principal des réseaux locaux sans fil (WLAN). Elle intègre plusieurs protocoles de sécurité tels que WEP, WPA, WPA2 et WPA3, visant à protéger les communications. Toutefois, ces mécanismes présentent certaines limites et vulnérabilités qui peuvent être exploitées par des attaquants à travers diverses techniques, telles que les attaques par interception, l'usurpation d'identité ou encore les attaques de type Man-In-The-Middle.

Face à l'évolution constante des menaces, la sécurisation des réseaux Wi-Fi est devenue une préoccupation majeure pour les administrateurs réseaux. Il est donc essentiel de concevoir des architectures sécurisées capables de garantir un niveau élevé de protection tout en maintenant des performances optimales.

C'est dans ce cadre que s'inscrit ce mémoire, réalisé au sein du Centre de Recherche en Technologies Agro-Alimentaires (CRTAA). L'objectif principal et de concevoir une architecture Wi-Fi sécurisée capable de garantir un niveau élevé de protection tout en maintenant des performances optimales.

Ce mémoire est structuré en deux parties principales répartie on quatre chapitre :

- **La première partie (théorique)** est consacrée aux fondements des réseaux sans fil et à leur sécurisation.

  Le **premier chapitre** présente les généralités sur les réseaux sans fil, leurs catégories, leurs caractéristiques ainsi que la norme IEEE 802.11 et ses différentes spécificités. Le **deuxième chapitre** aborde les principes fondamentaux de la sécurité des réseaux Wi-Fi, les protocoles de sécurisation existants, ainsi que les principales vulnérabilités et attaques associées.

- **La deuxième partie (pratique)** est dédiée à l'étude de cas et à la mise en œuvre. Le **troisième chapitre** présente l'organisme d'accueil (CRTAA), son infrastructure réseau ainsi qu'une analyse du réseau Wi-Fi existant.

  Le **quatrième chapitre** est consacré à la conception, à la simulation et à la mise en œuvre d'une solution de sécurisation du réseau Wi-Fi à l'aide de l'outil Cisco Packet Tracer, suivies d'une évaluation des performances et des limites de la solution proposée.

Chapitre 1 : Généralités sur les réseaux sans fil et le WI-FI

1.1 Introduction

Les réseaux sans fil connaissent actuellement un succès très important dont leur nombre croît très rapidement au sein des entreprises et du grand public. Ils offrent en effet une flexibilité largement supérieure aux réseaux filaires, en s'affranchissant notamment des problèmes de câblage et de mobilité des équipements.

Dans ce chapitre, nous présenterons une étude approfondie des réseaux sans fil, en mettant particulièrement l'accent sur la norme IEEE802.11 (Institute of Electrical and Electronics Engineers). Nous débuterons par une classification des différentes catégories de réseaux sans fil, avant d'analyser leurs principaux avantages ainsi que leurs limites. Nous décrirons ensuite les différentes versions de la norme IEEE 802.11 (a, b, g, n, ac, ax…). De plus, nous détaillant les modes de fonctionnement et nous analyserons l'architecture Wi-Fi. Ce chapitre vise à fournir une compréhension globale des réseaux sans fil et de Wi-Fi.

1.2 Définition

Un réseau sans fil (Wireless network) est, comme son nom l'indique, est un réseau à travers lequel différentes stations ou systèmes peuvent communiquer entre eux au moyen d'ondes radio. Grâce aux réseaux sans fil, l'utilisateur a la possibilité de rester connecté lors de ses déplacements dans un environnement géographique assez étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

Le réseau sans fil permet de connecter facilement des appareils distants de 10 mètres à plusieurs kilomètres. De plus, l'installation de tels réseaux ne nécessite pas d'ajustements majeurs à l'infrastructure existante, comme c'est le cas pour les réseaux filaires, comme creuser des tranchées pour le câblage ou installer des chemins de câbles et des connecteurs dans les équipements, etc.), ce qui conduit au développement rapide du réseau [1].

La norme la plus couramment utilisée pour les réseaux sans fil est la norme IEEE 802.11, mieux connue sous le nom de Wi-Fi (contraction de Wireless Fidelity) désigne l'ensemble des protocoles de communication régis par la norme internationale IEEE 802.11, permet la connexion de dispositifs variés tels que des ordinateurs, smartphones, imprimantes et capteurs, facilitant ainsi l'accès à internet ou aux ressources d'un réseau privé dans un rayon de quelques dizaines de mètres.

1.3 Catégorie des réseaux sans fil

Les réseaux sans fil sont classifiés selon leur étendue et domaine d'application en quatre (4) catégories [2] :

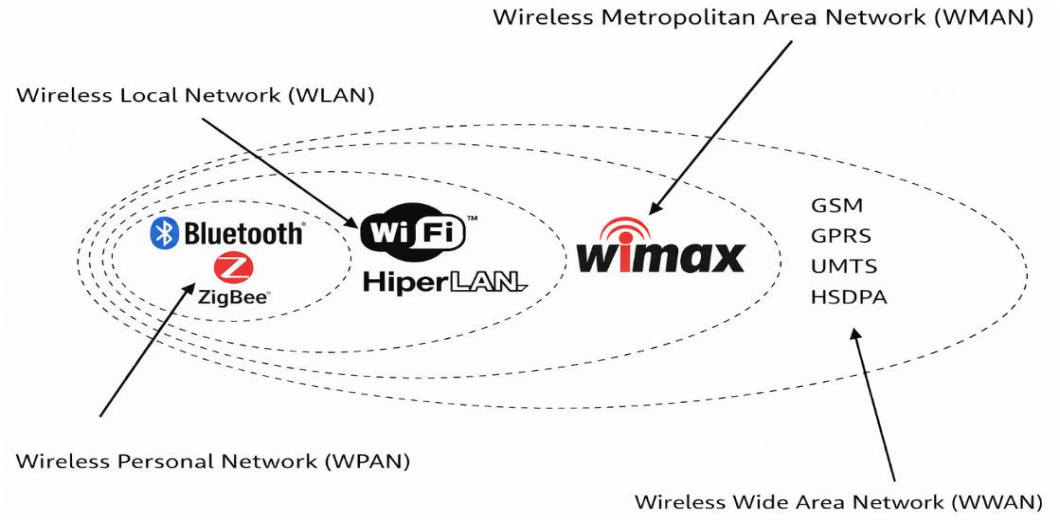

Figure 1 : Classification des réseaux sans fil

1.3.1 Les réseaux personnels sans fil (WPAN)

Le réseau personnel (concerne les réseaux sans fils d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques,) ou un dispositif mobile (smartphone, tablette) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fils entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN, nous citons :

- ✓ La technologie Bluetooth (norme IEEE 802.15.1) : C'est la principale technologie WPAN, lancée en 1994, proposant un débit théorique de 1Mbps pour une portée maximale d'une trentaine de mètres.
- ✓ La technologie ZigBee (norme IEEE 802.15.4) : Elle permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être intégrée dans de petits appareils électroniques.
- ✓ La technologie infrarouge : Les liaisons infrarouges permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde, cette technologie est largement utilisée pour la domotique (télécommandes).

Figure 2 : Les réseaux personnels sans fil (WPAN)

1.3.2 Réseaux locaux sans fil (WLAN)

Le réseau local sans fils (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes. Les WLAN sont basés sur la norme 802.11 et une fréquence radio de 2.4 GHz ou 5 GHz, voici quelques-unes :

- ✓ La technologie Wi-Fi (norme IEEE 802.11) ;
- ✓ La technologie hiperLAN2 (High Performance Radio LAN 2.0) : C'est une norme européenne qui permet d'obtenir un débit théorique de 54 Mbps.

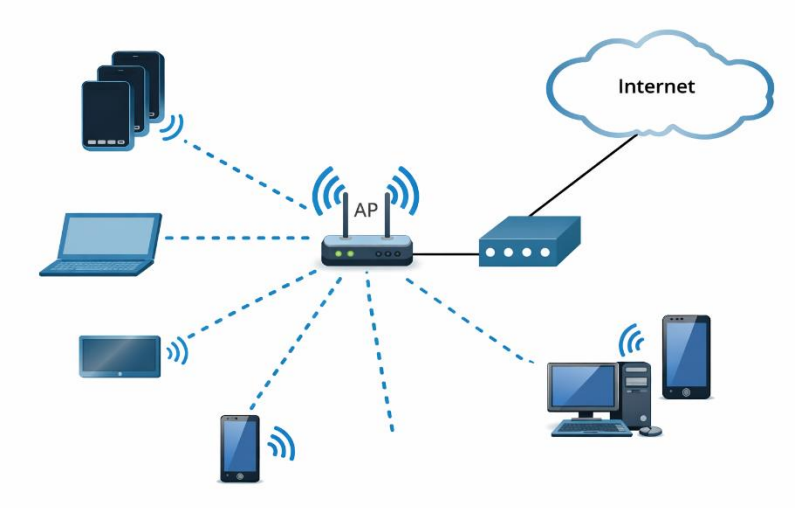

Figure 3 : Réseaux locaux sans fil (WLAN)

1.3.3 Les réseaux métropolitains sans fil (WMAN)

Les WMAN (Wireless Metropolitan Area Networks) couvrent une zone urbaine ou métropolitaine. Des technologies telles que WiMAX permettent une connectivité à haut débit sur plusieurs kilomètres, souvent utilisée par les opérateurs publics pour fournir Internet à grande échelle.

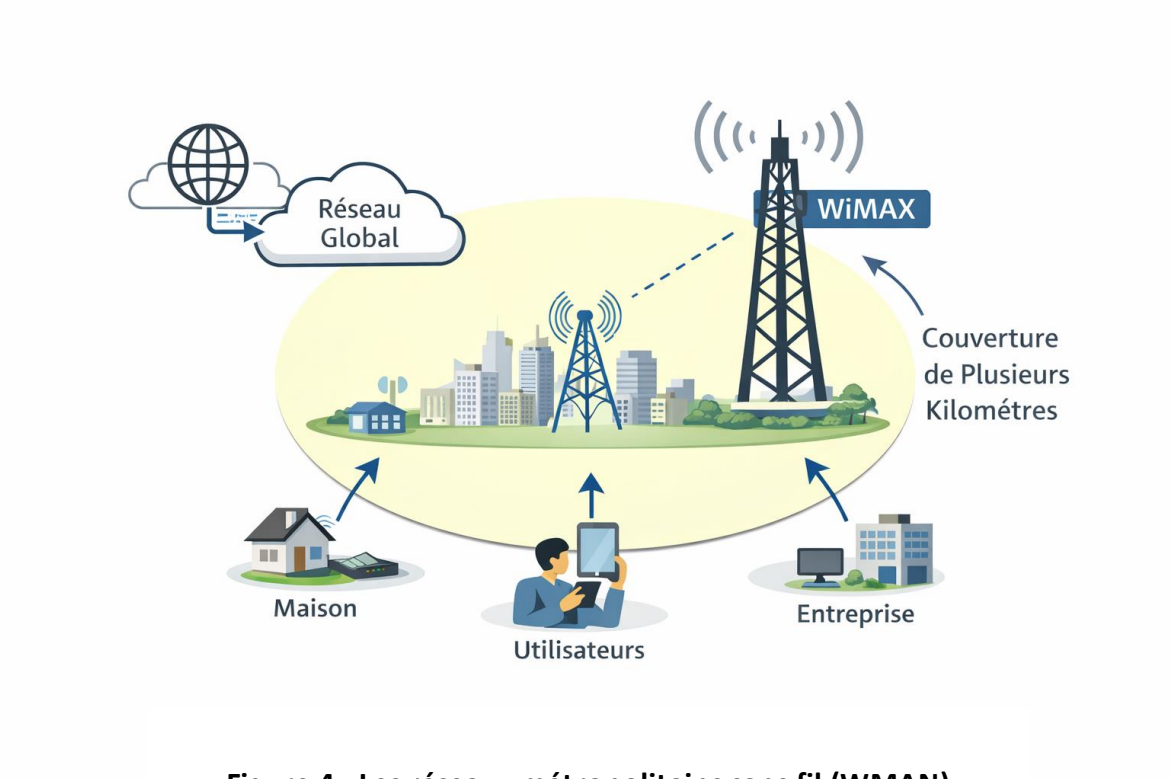

Figure 4 : Les réseaux métropolitains sans fil (WMAN)

1.3.4 Les larges réseaux sans fil (WWAN)

Ce réseau est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus, puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. Les principales technologies sont les suivantes :

- ✓ GSM (global for mobile Communication ou en français Groupe Spécial Mobile) dont le débit est de 9 kbps ;
- ✓ GPRS (General Packet Radio Service) dont le débit est de 20-30 kbps ;
- ✓ UMTS (Universal Mobile Telecommunication System) dont le débit est de 1 Mbps.

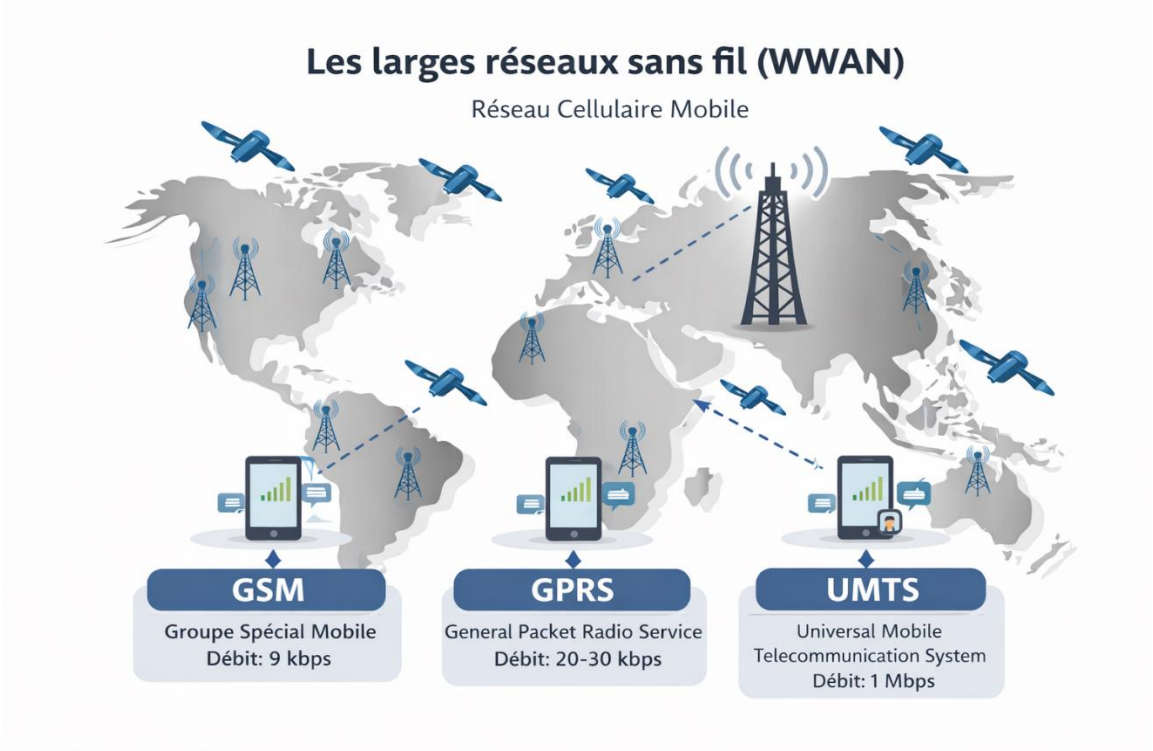

Figure 5 : Les larges réseaux sans fil (WWAN)

1.4 Les Avantages et les inconvénients des réseaux sans fil

Les réseaux sans fil sont devenus une technologie essentielle dans les environnements modernes, permettant la connexion des appareils sans recourir à des câbles physiques. Toutefois, comme toute technologie, ils présentent à la fois des avantages et des inconvénients, à savoir [3] :

1.4.1 Avantages des réseaux sans fil

✓ **Topologie**

Le sans-fil libère des contraintes imposées par les réseaux câblés. Avec un logiciel adéquat, il devient possible de mettre en service un nouvel appareil à n'importe quel moment, ce dernier se connecte, s'identifie, propose ses services et reçoit alors une partie des tâches à exécuter. Tout cela automatiquement, sans aucune connexion physique.

✓ **Mobilité**

Les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.

✓ **Facilité et souplesse**

Un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.

✓ **Evolutivité**

Les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins.

1.4.2 Inconvénient des réseaux sans fil

✓ **Sécurité plus vulnérable**

Les transmissions radio peuvent être interceptées, exposant le réseau aux accès non autorisés si des mécanismes de sécurité robustes ne sont pas mis en place.

✓ **Performances et stabilité inférieures**

Comparés aux réseaux filaires, les WLAN sont plus sensibles aux interférences et aux obstacles, ce qui peut réduire la vitesse et la fiabilité.

✓ **Portée limitée**

La couverture diminue avec la distance et les obstacles physiques, nécessitant parfois plusieurs points d'accès.

1.5 La norme IEEE 802.11 (Wi-Fi)

1.5.1 Historique du Wi-Fi

Le Wi-Fi trouve ses racines dans les travaux de pionniers tels que Hedy Lamarr et George Antheil, qui ont développé une technique de saut de fréquence pour sécuriser les communications sans fil dans les années 1940.

Ce n'est cependant qu'au début des années 1990 que la technologie Wi-Fi a commencé à prendre forme sous l'égide des normes 802.11. Ratifiées par l'IEEE*, ces normes définissent les protocoles de communication, les spécifications techniques des composants et la mise en œuvre des réseaux locaux sans fil (WLAN).

Chaque norme au sein de la famille IEEE 802.11 correspond à une version spécifique de la technologie Wi-Fi, identifiée par une série de lettres.

Créée en 1999, la Wi-Fi Alliance a également joué un rôle crucial en établissant des normes d'interopérabilité, garantissant une compatibilité totale entre les équipements provenant de constructeurs différents. Cette initiative a contribué à la popularisation et à l'essor mondial

du Wi-Fi. Le développement de la technologie et des normes successives associées a été tel que la Wi-Fi Alliance a décidé d'introduire une numérotation en fonction de la génération de Wi-Fi considérée. Cette numérotation apporte une meilleure lisibilité pour les consommateurs et les utilisateurs [4].

1.5.2 Présentation du Wi-Fi

Le terme « Wi-Fi » suggère la contraction de « Wireless Fidelity », est un ensemble de protocoles de communication sans fil régi par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11).

Le Wi-Fi est une technologie de réseau sans fil qui permet aux périphériques tels que des ordinateurs (portables et fixes), des périphériques mobiles (téléphones intelligents et dispositifs portables) et d'autres équipements (imprimantes et caméras vidéo) d'accéder à Internet. Il permet à ces appareils, et à de nombreux autres, d'échanger des renseignements entre eux, ce qui crée un réseau [5].

Figure 6 : Logo officiel du Wi-Fi

1.5.3 Les différentes normes Wi-Fi

Les normes Wi-Fi, définies par l'IEEE dans la famille 802.11, régissent l'évolution des réseaux locaux sans fil en précisant les bandes de fréquences, les débits, les portées et les technologies de transmission. Elles ont évolué pour améliorer les performances, optimiser la gestion multi-utilisateurs et répondre aux besoins croissants en connectivité, en termes de débit, de sécurité, de fiabilité et d'efficacité énergétique. La liste des principales normes Wi-Fi est présentée comme suit [6] :

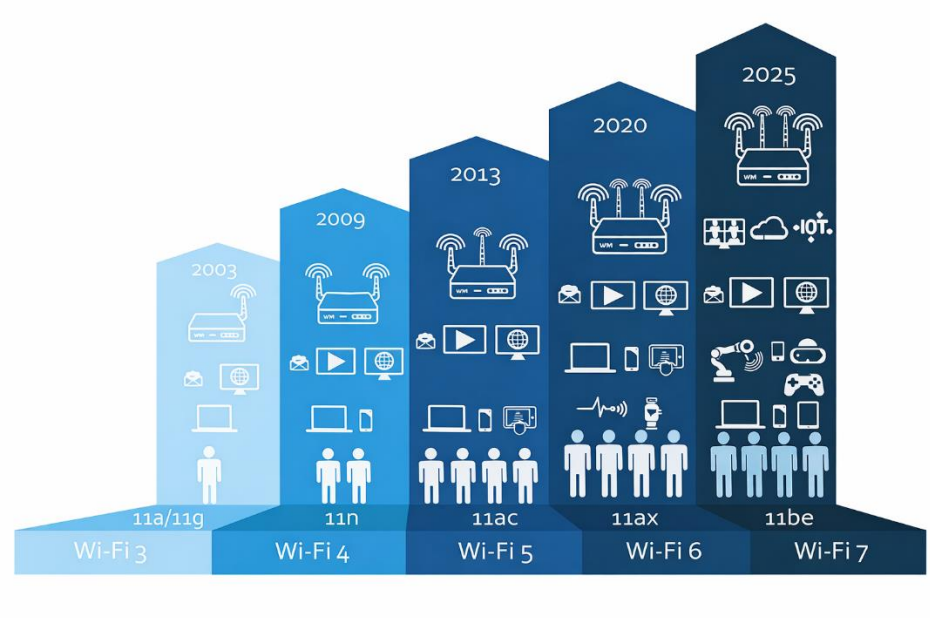

Figure 7 : Évolution des normes Wi-Fi de 2003 à 2025

-IEEE 802.11a : fonctionne dans la bande de fréquences de 5 GHz et permet des débits allant jusqu'à 54 Mbit/s. Cette norme s'appliquant à des fréquences élevées, elle possède une zone de couverture plus petite et est moins efficace pour pénétrer des structures de bâtiments. Il n'y a pas d'interopérabilité entre les périphériques fonctionnant sous cette norme et les normes 802.11b et 802.11g décrites ci-dessous.

-IEEE 802.11b : fonctionne dans la bande de fréquences de 2,4 GHz et permet des débits allant jusqu'à 11 Mbit/s. Les périphériques mettant en oeuvre cette norme ont une portée plus longue et sont davantage capables de pénétrer les structures de bâtiments que les périphériques basés sur la norme 802.11a.

-IEEE 802.11g : fonctionne dans la bande de fréquences de 2,4 GHz et offre des débits allant jusqu'à 54 Mbit/s. Les périphériques mettant en oeuvre cette norme fonctionnent par conséquent aux mêmes portée et radiofréquence que la norme 802.11b mais avec la bande passante de la norme 802.11a.

-IEEE 802.11n : fonctionne dans les bandes de fréquences 2,4 GHz et 5 GHz. Les débits de données standard attendus vont de 150 Mbit/s à 600 Mbit/s sur une distance maximale de 70 mètres. Cette norme est rétro compatible avec les périphériques 802.11a/b/g.

-IEEE 802.11ac : fonctionne dans la bande de fréquence de 5 GHz offrant des débits de données de 450 Mbit/s à 1,3 Gbit/s (1 300 Mbit/s). Cette norme est rétrocompatible avec les périphériques 802.11a/n.

-IEEE 802.11ad : également appelée « WiGig ». Cette norme utilise une solution Wi-Fi tribande sur les bandes de fréquences de 2,4 GHz, 5 GHz et 60 GHz et permet des débits théoriques jusqu'à 7 Gbit/s.

Tableau 1 : Comparaison des principales normes IEEE 802.11 du Wi-Fi

Norme	Génération	Débit maximal	Fréquence	Rétrocompatibilité
802.11a	Wi-Fi 2	54 Mbit/s	5 GHz	Non
802.11b	Wi-Fi 1	11 Mbit/s	2,4 GHz	Non
802.11g	Wi-Fi 3	54 Mbit/s	2,4 GHz	802.11b
802.11n	Wi-Fi 4	600 Mbit/s	2,4 GHz ou 5 GHz	802.11a/b/g
802.11ac	Wi-Fi 5	1,3 Gbit/s (1300 Mbit/s)	2,4 GHz et 5 GHz	802.11a/n
802.11ad	-	7 Gbit/s (7000 Mbit/s)	2,4 GHz, 5 GHz et 60 GHz	802.11a/b/g/n/ac

1.5.4 Les Normes Wi-Fi avancées

Les normes Wi-Fi ont évolué afin de répondre aux besoins croissants en performance, en portée et en efficacité énergétique, donnant naissance à des standards avancés tels que IEEE 802.11ax, 802.11ah et 802.11af.

-IEEE 802.11ax (Wi-Fi 6) : Le 802.11ax ou Wi-Fi 6, surnommé le High Efficiency WLAN (HEW), est prévu pour fonctionner sur les deux bandes de fréquences classiques du Wi-Fi actuelles : le 2,4 GHz et le 5 GHz. Il est donc prévu pour être complètement rétro compatible avec l'ensemble des normes précédentes, contrairement au 802.11ac qui ne fonctionnait que sur le 5 GHz. Ainsi, l'idée du 802.11ax est aussi d'étendre au 2,4 GHz les techniques radios et liaison qui ont été mises en place avec le 802.11ac [7].

-IEEE 802.11ah (Wi-Fi HaLow) : La norme 802.11ah, aussi connu sous le petit nom de Wi-Fi HaLow, elle a été annoncée officiellement en janvier 2016. Elle est principalement pensée pour les objets connectés avec une portée plus importante que du Wi-Fi classique, tout en consommant moins d'énergie. Les débits sont évidemment assez faibles puisqu'il est question de quelques dizaines de Mb/s [8].

-IEEE 802.11af (White-Fi / Super Wi-Fi) : Cette norme est un amendement à la norme de base IEEE 802.11, également connu dans le commerce sous le nom de super Wi-Fi. La principale différence par rapport aux normes bien connues IEEE 802.11a / b / g réside dans le fait que l'IEEE 802.11af est destiné à fonctionner dans les espaces blancs de télévision, c'est-à-dire le spectre déjà attribué aux diffuseurs de télévision mais non utilisé à un endroit et à une heure spécifiques période.

Cette norme utilise la technologie de la radio cognitive pour identifier les espaces blancs qu'elle peut utiliser. Cette technologie cognitive sera basée sur une base de données de géo localisation autorisée. Cette base de données fournit des informations sur la fréquence, l'heure et les conditions de fonctionnement des réseaux [9].

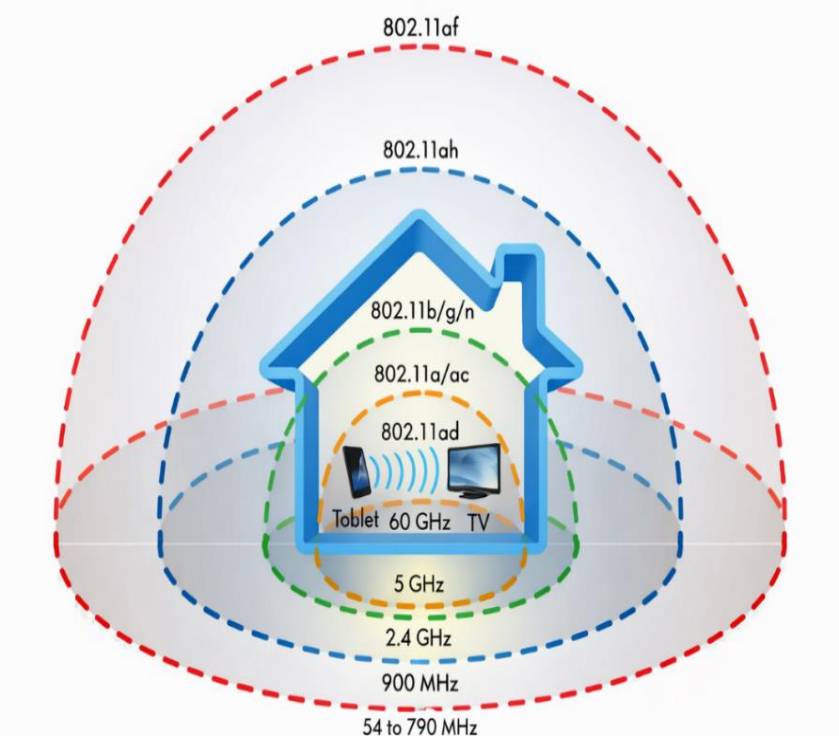

Figure 8 : Les normes Wi-Fi et leurs couvertures

1.5.5 Modes de fonctionnement du Wi-Fi

Le standard IEEE 802.11 définit plusieurs architectures de fonctionnement pour les réseaux locaux sans fil (WLAN), parmi lesquelles le mode infrastructure et le mode ad hoc sont les plus couramment utilisés.

✓ **Le mode infrastructure**

Le mode infrastructure c'est le mode qui permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès (PA) qui agissent comme des concentrateurs (exemple : répéteur ou commutateur en réseau Ethernet). Autrefois ce mode était essentiellement utilisé en entreprise. Dans ce cas, la mise en place d'un tel réseau oblige de poser à intervalles réguliers des bornes « point d'accès » (PA) dans la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau (SSID = Service Set IDentifier) afin de pouvoir communiquer. L'avantage de ce mode, en entreprise, est de garantir un passage obligé par le point d'accès : il est donc possible de vérifier qui accède au réseau. Actuellement les FAI, les boutiques spécialisées et les grandes surfaces fournissent aux particuliers des routeurs sans fil qui fonctionnent en mode « infrastructure », tout en étant très faciles à configurer [10].

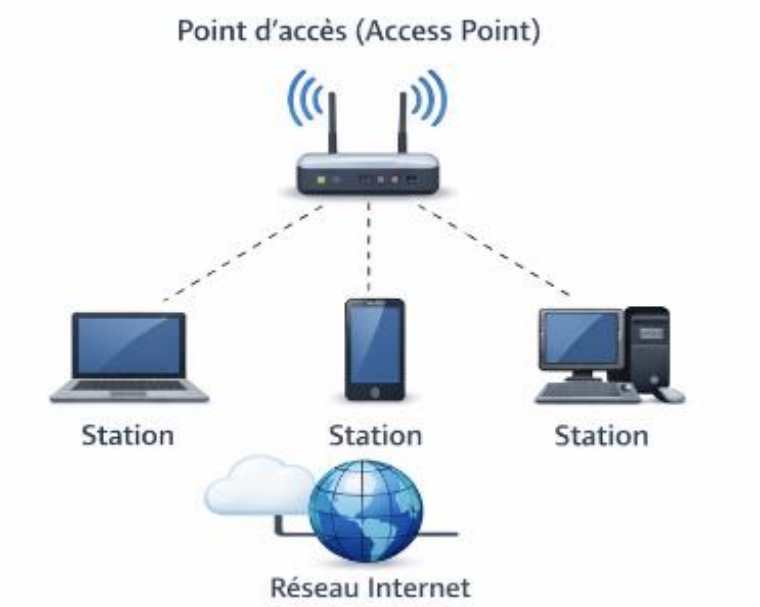

Figure 9 : Mode de fonctionnement infrastructure

✓ **Le mode Ad-hoc**

Cette architecture, aussi connue sous l'appellation IBSS, ne nécessite aucune infrastructure préalablement déployée pour permettre la communication entre ses membres, elle représente simplement un ensemble de station 802.11 autonomes, qui communiquent directement entre elles sans point d'accès ni connexion a un réseau filaire [11].

Le mode Ad-hoc permet de connecter directement les ordinateurs équipés d'une carte Wi-Fi, sans utiliser un matériel tiers tel qu'un point d'accès (en anglais : Access Point, ou AP). Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire (exemple : échange de fichiers entre portables dans un train, dans la rue, au café…). La mise en place d'un tel réseau consiste à configurer les machines en mode « Ad hoc » (au lieu du mode « Infrastructure »), la sélection d'un canal (fréquence), d'un nom de réseau (SSID) communs à tous et si nécessaire d'une clé de chiffrement. L'avantage de ce mode est de s'affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de point d'accès. Des protocoles de routage dynamique (exemples : OLSR, AODV…) rendent envisageable l'utilisation de réseaux maillés autonomes dans lesquels la portée ne se limite pas à ses voisins (tous les participants jouent le rôle du routeur)[12].

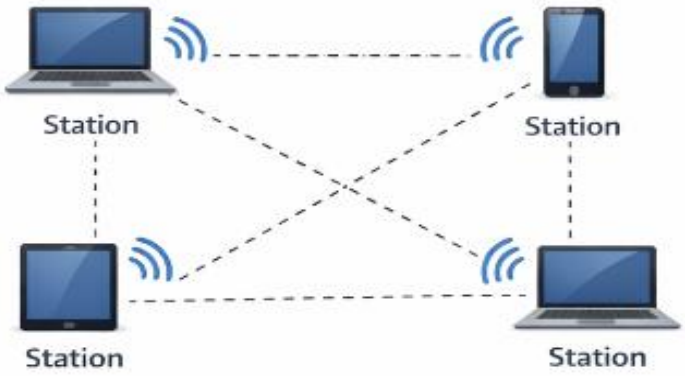

Figure 10 : Mode de fonctionnement Ad-hoc

1.5.6 Les Equipements Wi-Fi

Un réseau Wi-Fi repose sur deux équipements essentiels : les adaptateurs des terminaux et les points d'accès. Leur choix dépend du standard IEEE 802.11, du débit requis et du nombre d'utilisateurs.

✓ Les adaptateurs sans fil

Les adaptateurs sans fils ou cartes d'accès (en anglais wireless adapters ou network interface controller, noté NIC) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs WiFi sont disponibles dans de

nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte Compact Flash, ...). On appelle station tout équipement possédant une telle carte et sont désormais intégrés par défaut dans la majorité des ordinateurs portables [13].

Figure 11 : Catre réseaux sans fil PCI

✓ Les routeurs sans fil

Un routeur sans fil est un appareil multifonction combinant les fonctionnalités d'un routeur et d'un point d'accès sans fil. Il connecte plusieurs appareils (ordinateurs, téléphones et tablettes, par exemple) à un réseau local (LAN) et fournit un accès à Internet via une connexion à un fournisseur d'accès à Internet (FAI). Les routeurs sans fil comprennent généralement :

- ✓ Fonctions de routage : Diriger le trafic de données entre les appareils sur le réseau local et Internet.
- ✓ Accès sans fil : Diffusion de signaux Wi-Fi pour connecter des appareils sans fil.
- ✓ Fonctionnalités de sécurité : Pare-feu, protection par mot de passe et traduction d'adresses réseau (NAT).
- ✓ Connexions filaires : Plusieurs ports Ethernet pour appareils filaires.

Les routeurs sans fil sont idéaux pour les petites entreprises, les particuliers et les environnements où un seul appareil peut gérer à la fois le routage et l'accès sans fil. Faciles à configurer et à gérer, ils constituent un choix populaire pour les réseaux peu complexes. Un routeur sans fil, également appelé routeur Wi-Fi, allie les fonctions de réseau d'un point d'accès sans fil et d'un routeur [14].

.

Figure 12 : Routeurs sans fil

✓ Les points d'accès

Un point d'accès sans fil est un appareil de mise en réseau permettant aux appareils sans fil de se connecter à un réseau filaire. Il est plus simple d'installer un point d'accès sans fil pour connecter tous les ordinateurs ou appareils de votre réseau que d'utiliser des fils ou des câbles [15].

Figure 13 : Point d'accès Wi-Fi

Les clients sans fil utilisent leur carte réseau sans fil pour découvrir les points d'accès à proximité annonçant leur SSID. Les clients tentent ensuite de s'associer et de s'authentifier avec un AP. Une fois authentifiés, les utilisateurs sans fil ont accès aux ressources réseau.

Certains modèles intègrent des fonctionnalités supplémentaires telles qu'un modem, un pare-feu ou des mécanismes de sécurité avancés.

Tableau 2 : Point d'accès sans fil et Routeur sans fil : Principales différences

Critère	Routeur sans fil	Point d'accès sans fil (AP)
Fonction principale	Assure la connexion LAN-Internet et gère le trafic	Étend la couverture Wi-Fi d'un réseau existant
Rôle dans le réseau	Combine routage et point d'accès sans fil	Pont entre réseau filaire et clients Wi-Fi
Interfaces réseau	Plusieurs ports LAN et WAN	Généralement un port Ethernet
Couverture Wi-Fi	Adapté aux petites et moyennes surfaces	Conçu pour grandes zones avec plusieurs AP
Sécurité	Pare-feu, NAT, DHCP, VPN intégrés	Dépend d'un routeur ou contrôleur externe
Gestion	Autonome, configuration simple	Gestion centralisée possible
Évolutivité	Limitée	Très évolutive (ajout de plusieurs AP)

1.6 Catégories des points d'accès

Les points d'accès peuvent être classés comme des points d'accès autonomes ou des points d'accès basés sur un contrôleur, comme suit [16].

1.6.1 Points d'accès autonomes

Il s'agit de périphériques autonomes configurés à l'aide d'une l'interface de ligne de commande ou d'une interface graphique, les points d'accès autonomes sont utiles dans les situations ou seuls quelques points d'accès sont requis dans l'organisation. Un router domestique est un exemple d'AP autonome car la configuration complète de l'AP réside sur l'appareil. Si les demandes sans fil augmentent, plus de points d'accès seraient nécessaires. Chaque AP fonctionnerait indépendamment des autres AP et chaque AP nécessiterait une configuration et une gestion manuelles. Cela deviendrait écrasant si de nombreux points d'accès étaient nécessaires.

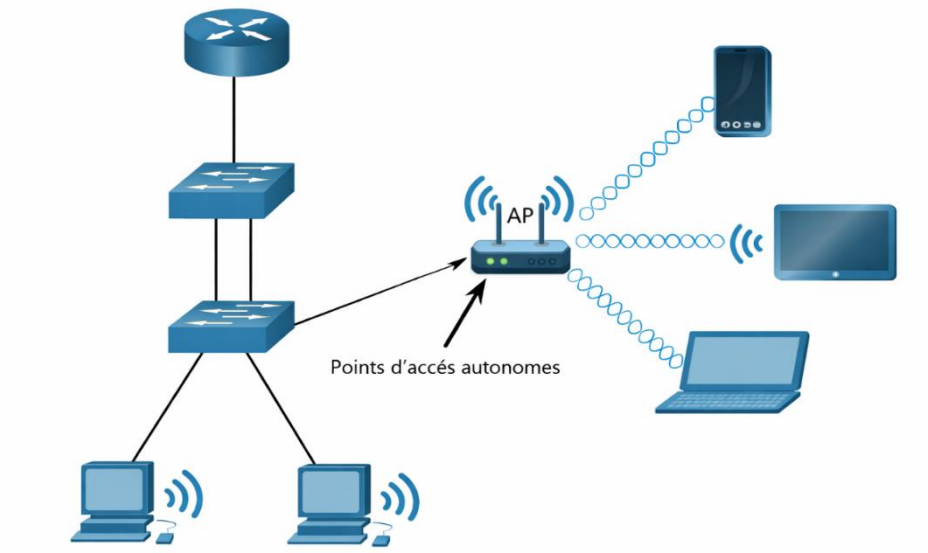

Figure 14 : Points d'accès autonomes

1.6.2 Points d'accès basée sur un contrôleur

Ces périphériques ne nécessitent aucune configuration initiale et sont souvent appelés points d'accès légers (LAP). Les LAP utilisent le protocole LWAPP (Lightweight Access Point Protocol) pour communiquer avec un contrôleur WLAN (WLC) pour (Wireless LAN Controller). Les points d'accès basées sur un contrôleur sont utiles dans les situations où de nombreux points d'accès sont requis dans le réseau. Comme plus d'AP sont ajoutés, chaque AP est automatiquement configuré et gère par le WLC.

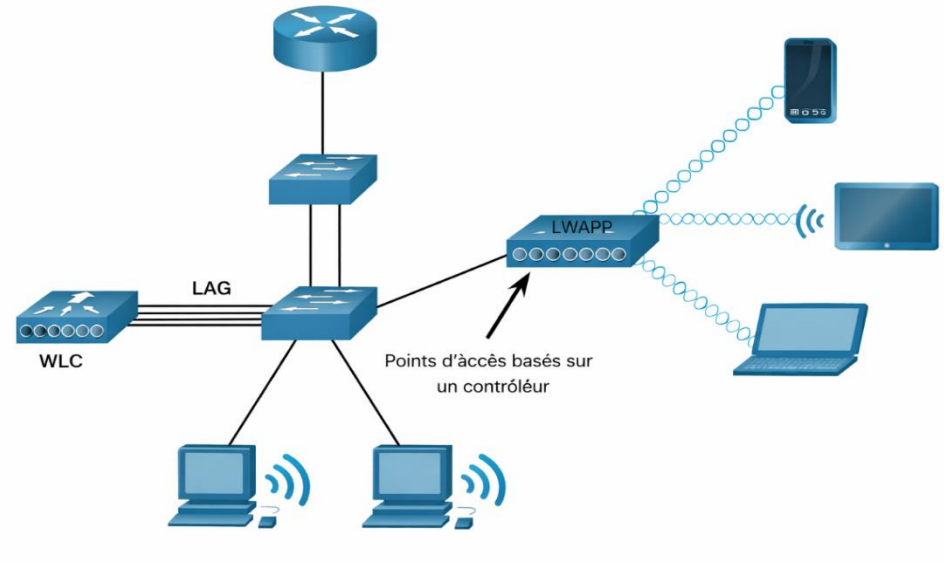

Figure 15 : Points d'accès basée sur un contrôleur (WLC)

1.7 Architecture Wi-Fi

La norme Wi -Fi définit les deux couches basses du modèle OSI d'un réseau sans fil de type WLAN, à savoir la couche liaison de données et la couche physique.

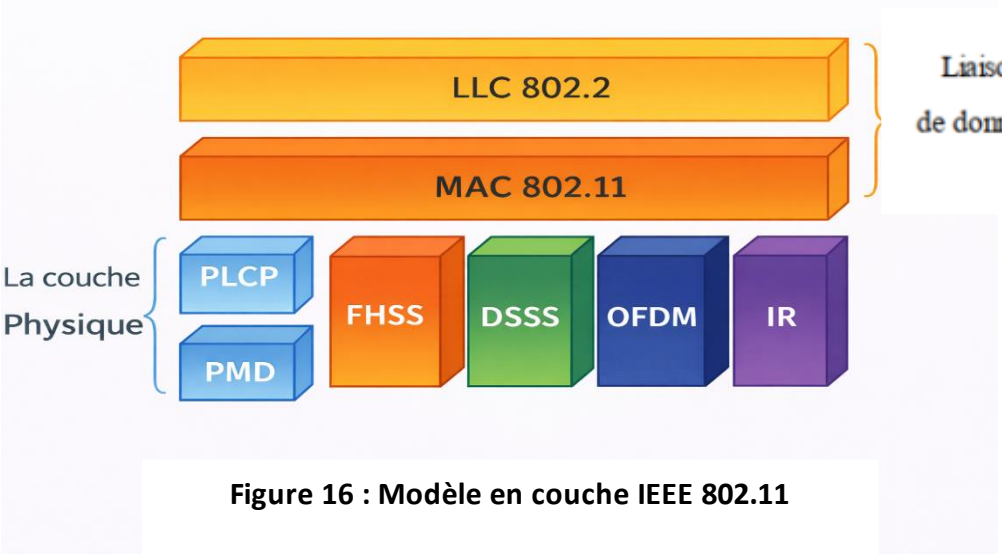

Figure 16 : Modèle en couche IEEE 802.11

1.7.1 Couche physique (PHY)

La couche physique définit la modulation des ondes radioélectrique et les caractéristiques de la signalisation pour la transmission de donnes [17].

Elle est responsable de la transmission des signaux sur le support radio. Elle définit les paramètres techniques liés aux bandes de fréquences (2,4 GHz, 5 GHz, 6 GHz), aux techniques de modulation (OFDM, QAM), aux débits de transmission, à la puissance d'émission, ainsi qu'aux méthodes de codage et de correction d'erreurs.

Cette couche joue un rôle central dans la portée du signal, la robustesse des communications, et la performance globale du réseau sans fil.

1.7.2 Couche liaison de données (MAC)

La couche liaison de données, et plus précisément la sous-couche MAC (Medium Access Control), assure la gestion de l'accès au médium radio partagé. Elle définit les mécanismes permettant d'éviter les collisions, notamment le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), ainsi que l'adressage des trames, le contrôle d'erreurs, la retransmission des paquets et la gestion de la qualité de service (QoS).

La couche MAC intègre également des mécanismes de sécurité essentiels, tels que l'authentification, le chiffrement des données (WEP, WPA2, WPA3) et la gestion des associations entre stations et points d'accès. Elle garantit ainsi la fiabilité, la sécurité et l'efficacité des communications Wi-Fi.

1.7.3 Méthode d'accès de base CSMA/CA

Un protocole CSMA/CA (Carier Sense Multiple Access with Collision Avoidance) utilise un mécanisme d'esquive de collision en imposant un accusé de réception systématique des paquets (ACK), ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception.

Ce protocole fonctionne de la manière suivante : Une station voulant émettre, doit d'abord écouter le support de transmission, s'il est occupé (i.e. une autre station est en train d'émettre), alors, la station remet sa transmission à plus tard. Dans le cas contraire, la station est autorisée à transmettre [18].

1.8 Conclusion

Au cours de ce premier chapitre, nous avons abordé les généralités sur les réseaux sans fil, notamment leurs définitions, leurs différentes catégories ainsi que leurs avantages et leurs inconvénients. Nous avons ensuite présenté le standard IEEE 802.11 (Wi-Fi), en exposant son historique, sa présentation générale, ses principales normes, ainsi que les équipements utilisés, les modes de fonctionnement et son architecture.

Les réseaux sans fil présentent plusieurs avantages par rapport aux réseaux filaires, en particulier la facilité de déploiement, la flexibilité et la mobilité. Toutefois, ils restent confrontés à plusieurs problématiques, notamment en matière de sécurité. Ainsi, le prochain chapitre sera consacré à l'étude de la sécurité dans les réseaux Wi-Fi.

Chapitre 2 : La sécurité dans les réseaux WI-FI

2.1 Introduction

La sécurité des réseaux sans fil représente aujourd'hui un enjeu majeur dans le domaine des technologies de l'information et de la communication. Contrairement aux réseaux filaires, où l'accès au support de transmission est physiquement limité, les réseaux Wi-Fi reposent sur la propagation des ondes radio dans l'air, ce qui les rend plus exposés aux interceptions et aux attaques malveillantes. En conséquence, les informations échangées à travers ces réseaux peuvent être compromises si des mécanismes de sécurité appropriés ne sont pas mis en place.

Dans ce chapitre, nous présenterons tout d'abord les principes fondamentaux de la sécurité des réseaux Wi-Fi. Nous aborderons ensuite les principaux protocoles de sécurité mis en œuvre pour protéger les communications sans fil. Enfin, nous analyserons les différentes menaces ainsi que les vulnérabilités spécifiques aux réseaux Wi-Fi.

2.2 Principes de la sécurité Wi-Fi

La sécurité des réseaux Wi-Fi a pour objectif de protéger les communications sans fil contre les accès non autorisés, l'interception des données et diverses attaques malveillantes. Elle s'appuie sur les principes fondamentaux suivants [19] :

2.2.1 Confidentialité

La confidentialité est importante pour protéger les informations sensibles contre toute divulgation à des parties non autorisées. Cela inclut la protection des données au repos, en transit et en cours d'utilisation. Les techniques courantes utilisées pour maintenir la confidentialité comprennent le cryptage, les contrôles d'accès et le masquage des données.

2.2.2 Intégrité

L'intégrité est importante pour garantir que les informations n'ont pas été falsifiées ou modifiées de manière non autorisée. Cela inclut la protection des données contre toute modification, suppression ou ajout non autorisé. Les techniques courantes utilisées pour maintenir l'intégrité incluent les signatures numériques, les codes d'authentification des messages (MAC) et le hachage des données.

2.2.3 Disponibilité

La disponibilité est importante pour garantir que les informations et les systèmes sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin. Cela inclut la protection contre les attaques par déni de service et la garantie que les systèmes sont disponibles et peuvent résister aux pannes. Les techniques courantes utilisées pour maintenir la disponibilité incluent l'équilibrage de charge, la redondance et la planification de reprise après sinistre.

2.2.4 Authentification

Authentification est importante pour garantir que les informations proviennent d'une source fiable. Cela inclut la protection contre l'usurpation d'identité et d'autres types de fraude à l'identité. Les techniques courantes utilisées pour établir l'authenticité comprennent l'authentification, les certificats numériques et l'identification biométrique.

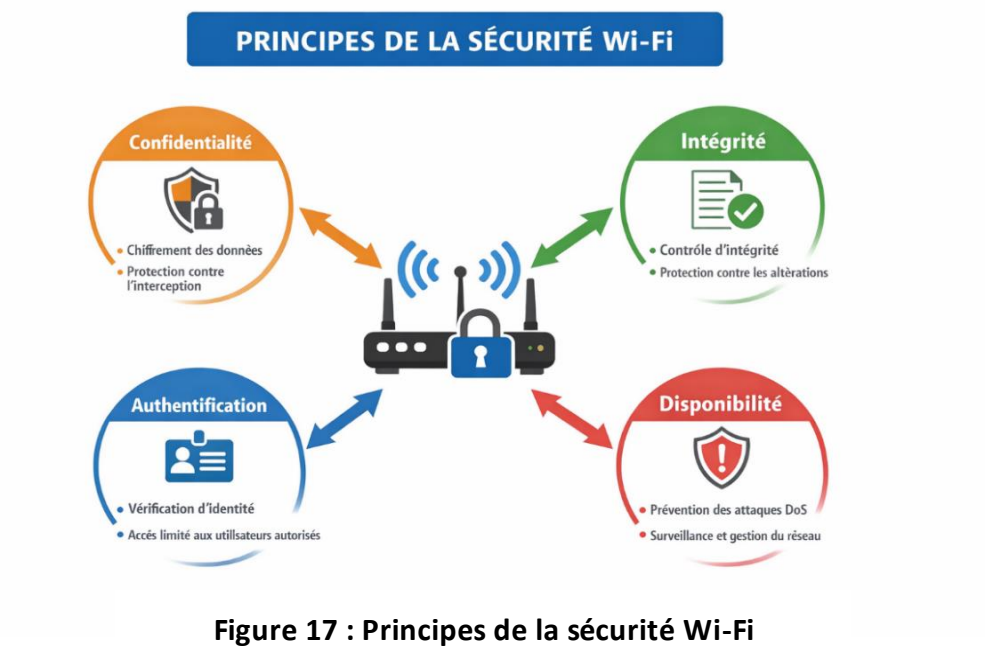

Figure 17 : Principes de la sécurité Wi-Fi

2.3 Protocoles de sécurité Wi-Fi

Les protocoles de sécurité sans fil les plus courants aujourd'hui sont WEP, WPA et WPA2. Chaque protocole utilise un type de chiffrement différent pour renforcer la sécurité du réseau. Les protocoles les plus récents, y compris le tout dernier protocole WPA3, se sont révélés très robustes et les pirates ont beaucoup plus de mal à les déjouer, Les principaux protocoles de sécurité Wi-Fi sont [20] :

2.3.1 WEP (Wired Equivalent Privacy)

Le WEP (Wired Equivalent Privacy) constituait auparavant le chiffrement standard, mais il n'est plus sûr, car la puissance de calcul s'est améliorée et les pirates peuvent désormais le déchiffrer facilement. Le chiffrement WEP s'effectue à l'aide d'une clé statique ; c'est l'une des principales raisons pour lesquelles il n'est plus considéré comme sûr.

Mis en place en 1997, le WEP utilise une clé unique pour assurer la sécurité de l'ensemble d'un réseau. Si un utilisateur est compromis, il entraîne tous les membres du réseau avec lui. Lorsque la sécurité WEP a été introduite, la chaîne de 64 ou 128 bits était difficile à forcer, créant ainsi un formidable mur entre le réseau d'utilisateurs et les pirates qui tentaient d'intercepter les signaux sans fil.

Aujourd'hui, il est facile, même pour un ordinateur grand public, d'effectuer les calculs nécessaires au déchiffrement d'une clé WEP. Le protocole de sécurité WEP a été retiré en 2004, les systèmes qui l'utilisent encore doivent donc être mis à jour.

Avantages

- ✓ La plupart des appareils reconnaissant le WEP, la configuration et l'utilisation étaient simples.
- ✓ Il visait à égaler les avantages des connexions Internet câblées en matière de sécurité.
- ✓ Au moment de sa mise en place, l'algorithme de chiffrement était suffisamment complexe pour empêcher les utilisateurs non-initiés d'y accéder.
- ✓ Le WEP protégeait des attaques dites de l'homme du milieu.

Inconvénients

- ✓ La clé de chiffrement statique devait être modifiée manuellement et mise à jour sur chaque machine individuelle pour bénéficier des avantages de sécurité des protocoles ultérieurs.
- ✓ Une partie de la clé était transmise sous forme de texte brut facilement déchiffrable.
- ✓ Trop de failles de sécurité ont été découvertes au fil du temps.

2.3.2 WPA (Wi-Fi Protected Access)

La sécurité WPA (Wi-Fi Protected Access) a été développée pour résoudre plusieurs des problèmes apparus avec le WEP. Devenu la norme en 2003, le WPA chiffre la clé d'accès au réseau de manière dynamique, en la renouvelant régulièrement par le biais du TKIP (Temporal Key Integrity Protocol). De cette façon, les pirates ne peuvent plus percer la clé en collectant les données transmises sur une longue période.

Le TKIP a créé un environnement de sécurité dynamique, mais ce n'était pas encore suffisant. Les experts en sécurité ont rapidement découvert que le TKIP pouvait être piraté, même avec de petits volumes de données.

En conséquence, un algorithme de chiffrement a été proposé aux cryptographes du monde entier pour remplacer le chiffrement RC4 du WEP et du WPA : l'AES, une création belge, s'étant avéré le plus sûr lors du concours de sélection. L'AES a été largement adopté par le successeur du WPA, le WPA2, que nous aborderons dans la section suivante.

Avantages

- ✓ Introduction du TKIP, ou chiffrement à clé dynamique, qui renouvelle régulièrement la clé d'accès au réseau.
- ✓ Tous les appareils du réseau reconnaissent la nouvelle clé lorsqu'elle est générée.
- ✓ Complexité accrue des clés de sécurité et de leur authentification.

Inconvénients

- ✓ Le TKIP s'est révélé vulnérable et peut être facilement piraté.
- ✓ La complexité de l'algorithme peut désormais être surmontée par la puissance de calcul moderne.
- ✓ Si les utilisateurs et les administrateurs de réseau ne créaient pas de mots de passe forts, les données étaient vulnérables.
- ✓ Si l'on compare le WPA au WEP, les avantages du WPA en matière de sécurité sont considérables, mais ses défauts sont vite apparus.

2.3.3 WPA2 (Wi-Fi Protected Access 2)

Le protocole de sécurité WPA2 a augmenté la complexité de son prédécesseur (WPA) et constitue la norme en matière de sécurité réseau depuis plus de dix ans. Il utilise le chiffrement AES, un mécanisme qui nécessiterait des milliards d'années pour qu'un ordinateur, même avancé, puisse le violer.

Mais le WPA2 comporte également des failles en matière de sécurité. Une attaque KRACK peut forcer l'accès pendant la prise de contact, c'est-à-dire le moment où un réseau authentifie la connexion d'un appareil, ce qui rend possible l'interception des mots de passe et autres données de la victime. Pour réussir une telle attaque, les pirates doivent se trouver à proximité du réseau, ce qui n'est pas aisé, même pour les meilleurs d'entre eux.

Les différences de sécurité significatives entre WPA et WPA2 ont permis au protocole WPA2 de perdurer plus longtemps que tout autre protocole de sécurité précédent.

Avantages

- ✓ Il offre les mêmes avantages que ceux introduits par le WPA.
- ✓ Il utilise généralement le chiffrement AES, extrêmement robuste.
- ✓ Les mots de passe doivent être plus longs, ce qui renforce la sécurité.

Inconvénients

- ✓ Il requiert une plus grande puissance de calcul (désormais négligeable avec la technologie actuelle).
- ✓ Il est vulnérable aux attaques dites de l'homme du milieu.
- ✓ Plus de dix ans après son lancement, une faille a finalement été découverte.

2.3.4 WPA3 (Wi-Fi Protected Access 3)

Le WPA3 a été introduit en 2018 et est devenu un protocole de sécurité standard en 2020, mais son adoption généralisée pourrait prendre un certain temps. La plupart des foyers et des entreprises utilisent encore le WPA2, et le matériel compatible avec le WPA3 peut être coûteux. Avec le WPA3, le chiffrement entre le dispositif d'un utilisateur et le réseau est spécifique et individualisé ; les utilisateurs n'ont pas besoin de saisir un mot de passe.

Avec le WPA2, un appareil et ses données peuvent être compromis dès qu'un pirate parvient à déjouer le chiffrement du réseau. Ce ne sera plus possible avec le WPA3, grâce à la couche supplémentaire de chiffrement individualisé.

Le WPA3 corrige également la faille de sécurité du WPA2 qui permet les attaques KRACK. De plus, l'algorithme de chiffrement est beaucoup plus complexe, à tel point que les ordinateurs modernes auraient besoin de milliards d'années de calculs pour pénétrer dans un seul réseau sécurisé par le WPA3.

Tableau 3 : Méthodes d'Authentification par Clé Partagée

Méthode d'authentification	Description
WEP (Wired Equivalent Privacy)	La spécification 802.11 originale conçue pour sécuriser les données à l'aide de la méthode de cryptage Rivest Cipher 4 (RC4) avec une clé statique. Cependant, la clé ne change jamais lors de l'échange de paquets. Cela facilite le piratage. Le WEP n'est plus recommandé et ne doit jamais être utilisé.
WPA (Wi-Fi Protected Access)	Une norme Wi-Fi Alliance qui utilise le WEP, mais sécurise les données avec le cryptage TKIP (Temporal Key Integrity Protocol), un algorithme beaucoup plus puissant. TKIP change la clé de chaque paquet, ce qui rend le piratage beaucoup plus difficile.
WPA2	WPA2 est la norme industrielle actuelle pour la sécurisation des réseaux sans fil. Elle utilise le standard de chiffrement avancé (AES) pour le chiffrement. AES est actuellement considéré comme le protocole de cryptage le plus puissant.
WPA3	La prochaine génération de sécurité Wi-Fi. Tous les appareils compatibles WPA3 utilisent les dernières méthodes de sécurité, interdisent les protocoles hérités obsolètes et exigent l'utilisation de cadres de gestion protégés (PMF). Cependant, les appareils avec WPA3 ne sont pas encore facilement disponibles.

2.4 Techniques de sécurisation de base des réseaux Wi-Fi

Les réseaux Wi-Fi disposent de plusieurs mécanismes simples permettant de limiter l'accès non autorisé et de renforcer la sécurité de base. Bien que ces techniques ne soient pas suffisantes seules pour assurer une protection complète, elles constituent une première couche de défense.

2.4.1 Masquage du SSID

Le SSID, ou Service Set Identifier, est le nom par lequel un réseau se fait reconnaître. Les SSID par défaut peuvent souvent révéler la marque et parfois même le modèle des routeurs, facilitant l'identification par des personnes mal intentionnées. La dissimulation du SSID ne le sécurise pas directement, mais rend nécessaire une connaissance manuelle pour s'y connecter, renforçant la sécurité en rendant le SSID non identifiable. Masquer le SSID n'ajoute pas automatiquement une sécurité, mais complique l'accès non autorisé [21].

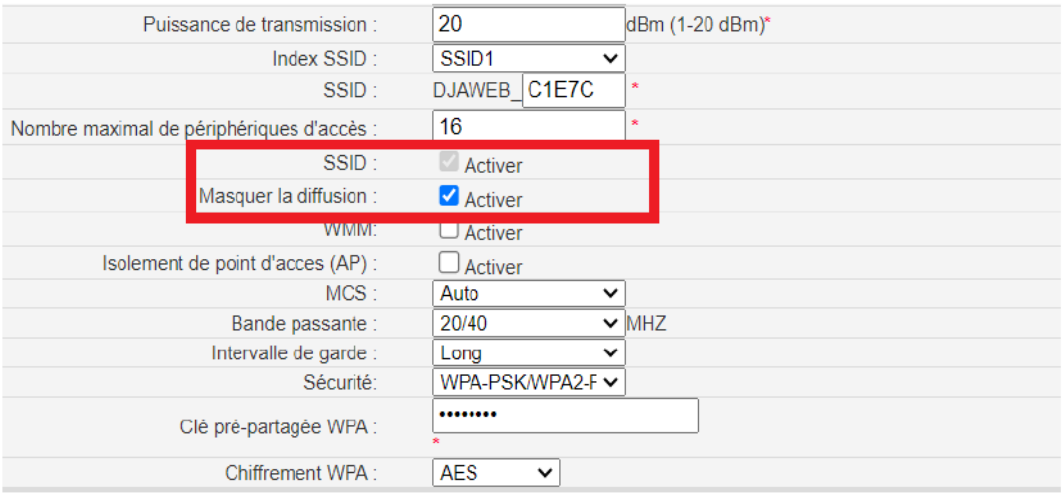

Figure 18 : Masquage du SSID

2.4.2 Filtrage des adresses MAC

L'adresse MAC, unique à chaque carte réseau, est utilisée pour le filtrage d'accès. Ce filtrage restreint les connexions aux seuls appareils avec des adresses MAC spécifiques, renforçant la sécurité en autorisant uniquement les appareils préalablement approuvés à se connecter au réseau.

Il est important de souligner que cette méthode demeure une couche de sécurité supplémentaire pour les réseaux Wi-Fi. Bien qu'elle ne soit pas infaillible et qu'elle puisse être contournée par des attaquants déterminés, elle contribue à la défense en profondeur en ajoutant une barrière supplémentaire que les intrus doivent franchir. Par conséquent, le filtrage des adresses MAC reste une mesure de sécurité valable lorsqu'il est utilisé en complément d'autres mécanismes de protection plus robustes [22].

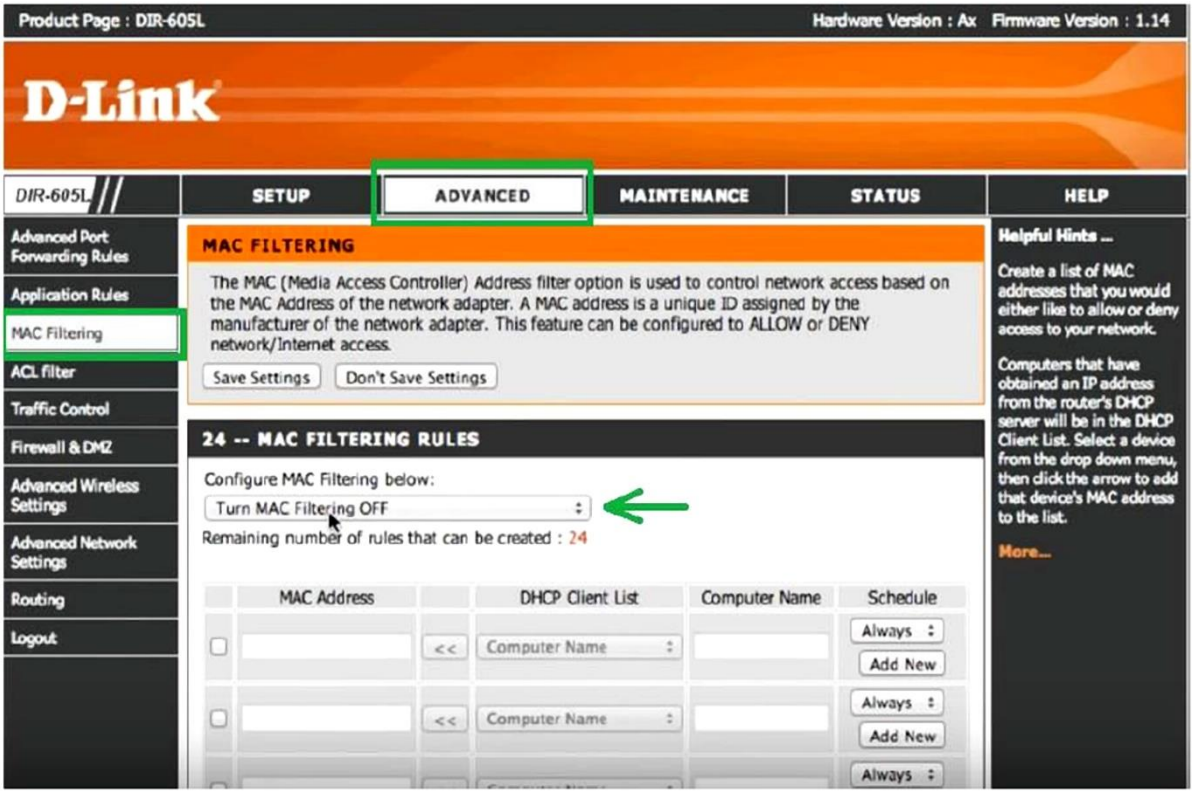

Figure 19 : Filtrage d'adresse MAC

2.5 Mécanismes avancés de sécurisation des réseaux Wi-Fi

Avec l'évolution des menaces et la généralisation des réseaux sans fil dans les environnements professionnels, les mécanismes de sécurité classiques basés uniquement sur des clés pré-partagées (mode personnel) se sont révélés insuffisants. Afin de renforcer la sécurité, des mécanismes avancés d'authentification et de contrôle d'accès ont été introduits, notamment dans les environnements d'entreprise. Ces mécanismes reposent principalement sur l'utilisation du standard IEEE 802.1X et du protocole RADIUS, qui permettent une authentification centralisée, dynamique et sécurisée des utilisateurs.

2.5.1 Architecture d'authentification IEEE 802.1X

Le 802.1X est un mécanisme d'authentification au standard international pour des terminaux dans un LAN (réseau interne câblé) ou un WLAN (réseau interne sans fil). Il est typiquement appliqué au sein d'une entreprise pour sécuriser l'accès à son réseau et ainsi aux données lui appartenant.

L'objectif de 802.1X est de délivrer, ou non, un droit d'accès au réseau, ceci sans se soucier du support physique utilisé. En effet, 802.1X travaille au niveau de la couche 2 du modèle OSI et ne requiert pas l'utilisation de la couche 3 (couche IP).

IEEE 802.1x utilise le protocole EAP (Extensible Authentication Protocol), pour mettre en communication le client et le serveur d'authentification via le contrôleur [23]. Il est largement utilisé dans les réseaux Wi-Fi sécurisés de type entreprise.

Ce protocole repose sur trois entités principales :

- ✓ **Le supplicant** : il s'agit du client (utilisateur ou équipement) souhaitant accéder au réseau
- ✓ **L'authenticator** : généralement un point d'accès Wi-Fi ou un commutateur, qui joue le rôle d'intermédiaire ;
- ✓ **Le serveur d'authentification** : souvent un serveur RADIUS, chargé de vérifier les identifiants.

Le fonctionnement de 802.1X s'appuie sur le protocole EAP, qui permet de supporter différentes méthodes d'authentification (certificats, identifiants, cartes à puce, etc.). Tant que l'utilisateur n'est pas authentifié, l'accès au réseau reste bloqué, ce qui renforce considérablement la sécurité.

2.5.2 Serveur d'authentification RADIUS

RADIUS (Remote Authentication Dial-In User Service) est une norme de l'IETF (Internet Engineering TASK Force). C'est un protocole d'authentification standard Client/Serveur qui permet de centraliser les données d'authentification : les politiques d'autorisations, de droits d'accès, et de traçabilité.

A l'origine, ce protocole a été créé pour permettre aux fournisseurs d'accès à internet (FAI) D'authentifier les utilisateurs distants. Au fil du temps, il a été enrichi et on peut envisager aujourd'hui de l'utiliser pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil [24].

Le RADIUS est un protocole qui répond au modèle AAA qui permet de centraliser les trois fonctions suivantes :

- ✓ Authentication(Authentification) : authentifier l'identité du client.
- ✓ Authorization (Autorisation) : accorder des droits du client.
- ✓ Accounting (Compatibilité) : c'est " journaliser " les accès, les temps de session, les ressources consommées, etc. afin de garantir la traçabilité des informations.

Dans une architecture Wi-Fi sécurisée, le serveur RADIUS joue un rôle central :

- ✓ Il reçoit les requêtes d'authentification envoyées par l'authenticator (point d'accès) ;
- ✓ Il vérifie les informations d'identification de l'utilisateur (login/mot de passe, certificat..
- ✓ Il autorise ou refuse l'accès au réseau en fonction des politiques de sécurité définies.

L'utilisation de RADIUS permet une gestion centralisée des utilisateurs, une traçabilité des connexions, ainsi qu'une meilleure application des politiques de sécurité. De plus, il facilite l'intégration avec des annuaires d'entreprise tels que LDAP ou Active Directory.

2.5.3 Modes Enterprise (WPA2-Entreprise et WPA3-Entreprise)

Les protocoles WPA2 et WPA3 offrent deux modes de fonctionnement : le mode personnel et le mode entreprise. Ce dernier est spécialement conçu pour les environnements professionnels nécessitant un haut niveau de sécurité.

Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS, et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte. Mais attention, toutefois, rien n'est acquis et il y a fort à parier que cette solution ne restera pas à l'abri des hackers très longtemps [25].

- ✓ Chaque utilisateur possède des identifiants uniques ;
- ✓ L'authentification est réalisée de manière centralisée ;
- ✓ Des clés de chiffrement dynamiques sont générées pour chaque session ;
- ✓ Le risque de compromission globale du réseau est fortement réduit.

Tableau 4 : Comparaison entre WPA2-Enterprise et WPA3-Enterprise

Critère	WPA2-Enterprise	WPA3-Enterprise
Niveau de sécurité	Élevé	Très élevé
Chiffrement	AES (128 bits)	Jusqu'à 192 bits
Authentification	802.1X + RADIUS	802.1X + RADIUS
Protection contre-attaques	Bonne	Très renforcée
Compatibilité	Large	Limitée (équipements récents)

Le mode entreprise de WPA2 utilise généralement le chiffrement AES (Advanced Encryption Standard), avec le protocole CCMP (Counter Mode CBC-MAC Protocol), tandis que WPA3-Entreprise introduit des mécanismes de sécurité encore plus robustes, notamment une meilleure protection contre les attaques par force brute et un niveau de chiffrement renforcé.

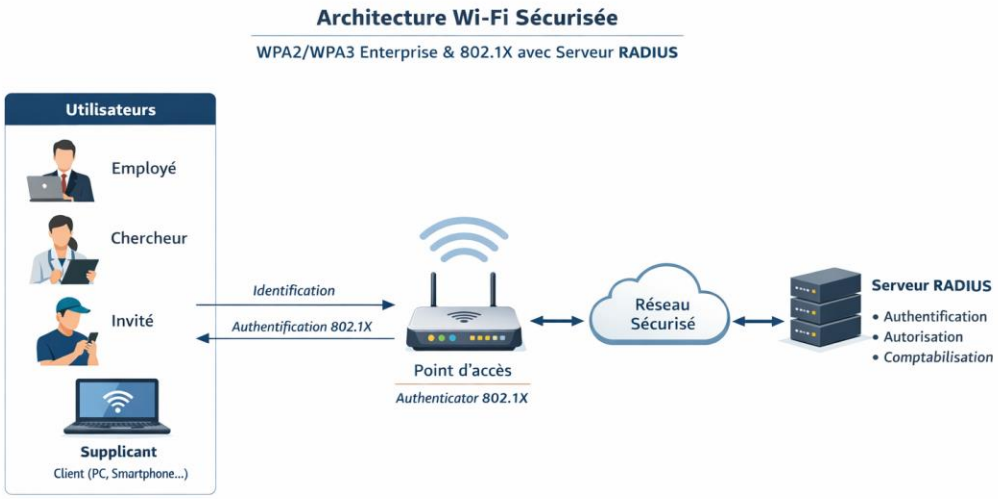

Figure 20 : Architecture Wi-Fi Sécurisé (WPA2/WPA3 Entreprise & 802.1X avec serveur RADIUS)

2.6 Vulnérabilités et attaques des réseaux Wi-Fi

Les réseaux Wi-Fi sont exposés à des risques pouvant compromettre la sécurité des données. Ces risques se traduisent par des attaques exploitant des vulnérabilités des systèmes, protocoles ou pratiques des utilisateurs.

2.6.1 Vulnérabilités des réseaux Wi-Fi

Les vulnérabilités représentent les faiblesses ou lacunes dans les équipements, les protocoles ou les configurations réseau qui peuvent être exploitées par un attaquant. Les principales vulnérabilités des réseaux Wi-Fi sont les suivantes :

- ✓ **Mots de passe faibles ou par défaut** : l'utilisation de mots de passe simples, prévisibles ou fournis par défaut par les équipements constitue une faille majeure, permettant un accès rapide au réseau.
- ✓ **Utilisation de protocoles de sécurité obsolètes** : certains protocoles de sécurité, comme WEP ou certaines versions anciennes de WPA, présentent des failles connues qui facilitent le piratage et l'interception des données.
- ✓ **Absence de segmentation du réseau** : lorsque tous les utilisateurs partagent le même réseau sans fil, une faille exploitée sur un point d'accès peut affecter l'ensemble du réseau. La segmentation du réseau permet d'isoler les ressources sensibles et de limiter l'impact d'une attaque.
- ✓ **Points d'accès mal configurés ou non mis à jour** : les points d'accès dont la configuration est incorrecte ou dont le firmware n'est pas régulièrement mis à jour peuvent présenter des vulnérabilités exploitables par des attaquants, telles que des failles dans le protocole ou dans l'équipement.

Ces vulnérabilités constituent des points d'entrée pour les attaques et doivent être corrigées ou atténuées par des pratiques de sécurité appropriées, telles que le chiffrement robuste, l'utilisation de mots de passe forts et la mise à jour régulière des équipements.

2.6.2 Attaques liées aux réseaux Wi-Fi

Les attaques sur un réseau Wi-Fi prennent différentes formes, visant à compromettre sa sécurité ou à accéder à des informations sensibles. Ces tentatives malveillantes exploitent diverses vulnérabilités pour compromettre la confidentialité, l'intégrité ou la disponibilité des données. Ci-dessous, un aperçu des principales attaques sur les réseaux Wi-Fi :

✓ **Le wardriving**

Le wardriving est une cyberattaque qui consiste à rechercher des réseaux sans fil vulnérables à partir d'un véhicule en mouvement ou d'un autre moyen de transport. Les attaquants utilisent des logiciels et du matériel spécifique pour détecter et enregistrer les emplacements des points d'accès Wi-Fi non sécurisés, souvent pour obtenir un accès non autorisé et voler des données. Cette pratique a évolué à partir du film "WarGames" et implique généralement des outils tels que des renifleurs de paquets, des testeurs de force du signal et des logiciels de cartographie des points d'accès [26].

✓ **L'espionnage**

En raison des caractéristiques des réseaux sans fil, un pirate peut facilement faire l'écoute sur un réseau sans fil : il se poste à proximité et surveille les échanges, on dit qu'il sniffe le réseau [27]. Le sniffing est une technique couramment utilisée dans ce cadre. Elle consiste à capturer et analyser les paquets circulant sur le réseau à l'aide d'un adaptateur Wi-Fi en mode monitor et d'outils spécialisés, tels que Wireshark. Cette méthode permet à l'attaquant de récupérer des informations confidentielles comme des identifiants, des mots de passe ou d'autres données personnelles.

✓ **L'intrusion**

Une intrusion réussie permet au pirate de se comporter exactement comme un utilisateur normal : au point qu'il est souvent difficile de s'apercevoir qu'une intrusion a eu lieu ou même qu'elle est en cours, car tout se passe comme si un utilisateur normal accédait au système. Il s'agit donc d'une attaque extrêmement dangereuse.

L'intrusion est bien sûr tout à fait triviale si aucune sécurité n'est mise en œuvre : il suffit de s'associer normalement à l'un des AP du réseau, et le tour est joué. En revanche, si l'association impose un mécanisme d'identification avant d'autoriser l'ouverture d'une session sur le réseau, le pirate aura essentiellement deux options :

? Ouvrir une nouvelle session en se faisant passer pour un utilisateur légitime ; ? Détourner une session existante (hijacking).

Idéalement, les mots de passe des utilisateurs doivent être assez longs et complexes pour qu'il soit impossible de les deviner en quelques tentatives, le système doit détecter et bloquer

les attaques de dictionnaire en ligne, et il doit également utiliser un protocole d'authentification invulnérable aux attaques de dictionnaire hors ligne [28].

✓ **Les attaques de mots de passe**

Les attaques de mots de passe reposent sur deux méthodes principales :

- **Attaque par dictionnaire**

Dans sa forme la plus simple, une attaque par dictionnaire est un type d'attaque par force brute au cours de laquelle les pirates informatiques essaient de deviner le mot de passe d'un utilisateur pour ses comptes en ligne en parcourant rapidement une liste de mots, de phrases et de combinaisons de chiffres couramment utilisés. Lorsqu'une attaque par dictionnaire a permis de déchiffrer correctement un mot de passe, le pirate peut l'utiliser pour accéder aux comptes bancaires, aux profils de réseaux sociaux et même à des fichiers protégés par un mot de passe. C'est à ce moment-là que la victime du pirate informatique peut être confrontée à un véritable problème [29].

- **Attaque par force brute**

Est une méthode en cryptanalyse pour trouver un mot de passe ou une clé. Il consiste à essayer, une à une, toutes les combinaisons possibles jusqu'à trouver la bonne. Cette méthode en générale considérée comme la plus simple concevable.

En réalité l'incertitude du succès d'une attaque de force brute réside dans le temps qu'il faut pour trouver le bon mot de passe. Cette variable dépend à la fois de la longueur du mot de passe ainsi de la puissance de l'appareil. Cette attaque peut prendre de quelques minutes à plusieurs années en fonction complexité du mot de passe utilisé [30].

- **Le détournement de session**

Le détournement de session (parfois appelé détournement de cookies, détournement de session TCP ou reniflage de paquets) se produit lorsqu'un pirate informatique prend le contrôle de votre session Internet. Une telle situation peut se produire lorsque vous effectuez des achats en ligne, payez une facture ou vérifiez votre solde bancaire. Les pirates de session ciblent généralement les navigateurs ou les applications Internet, et leur objectif est de contrôler votre session de navigation pour accéder à vos informations personnelles ainsi

qu'à vos mots de passe. Les pirates de session se font passer pour vous auprès des sites Web. Ce type d'attaque peut avoir de graves conséquences pour la sécurité des applications, car il permet aux pirates informatiques d'obtenir un accès non autorisé à des comptes protégés (et aux données qu'ils contiennent) en se faisant passer pour un utilisateur légitime [31].

✓ **Le déni de service (Dos)**

Une attaque par déni de service (DoS) est un type de cyberattaque dans lequel un acteur malveillant vise à rendre un ordinateur ou un autre appareil indisponible pour ses utilisateurs prévus en interrompant le fonctionnement normal de l'appareil. Les attaques DoS fonctionnent généralement en submergeant ou en saturant une machine ciblée de requêtes jusqu'à ce que le trafic normal ne puisse plus être traité, ce qui entraîne un déni de service pour les utilisateurs supplémentaires. Une attaque DoS se caractérise par l'utilisation d'un seul ordinateur pour lancer l'attaque [32].

✓ **Man-in-the-middle**

Une attaque de l'homme du milieu (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 [33].

L'objectif d'une attaque MITM est de récupérer des données confidentielles telles que des détails de compte bancaire, des numéros de carte de crédit ou des informations de connexion, qui peuvent être utilisées pour commettre d'autres crimes comme le vol d'identité ou les transferts de fonds illégaux. Parce que les attaques MITM sont menées en temps réel, elles passent souvent inaperçues jusqu'à ce qu'il soit trop tard [34].

L'attaque Evil Twin est une forme d'attaque de type Man-in-the-Middle (MITM) exploitant les réseaux Wi-Fi publics. Son nom, signifiant « jumeau maléfique », vient du fait qu'un pirate crée un faux point d'accès Wi-Fi imitant un réseau légitime pour tromper les utilisateurs. Une fois connectés, les données sensibles telles que les identifiants, mots de passe ou informations bancaires sont interceptées [35].

✓ **Les Points d'Accès Non Autorisés** [36]

- Un point d'accès non autorisé est un point d'accès ou un routeur sans fil qui a été connecté à un réseau d'entreprise sans autorisation explicite et conformément à la politique de l'entreprise.
- Une fois connecté, l'escroc AP peut être utilisé par un attaquant pour capturer des adresses MAC, capturer des paquets de données, accéder à des ressources réseau ou lancer une attaque de type homme-au-milieu.
- Un point d'accès au réseau personnel pourrait également être utilisé comme point d'accès non autorisé. Par exemple, un utilisateur avec un accès réseau sécurisé permet à son hôte Windows autorisé de devenir un point d'accès Wi-Fi.
- Pour empêcher l'installation de points d'accès non autorisés, les organisations doivent configurer les WLC avec des stratégies de points d'accès malveillants et utiliser un logiciel de surveillance pour surveiller activement le spectre radioélectrique des points d'accès non autorisés.

2.7 Conclusion

Au cours de ce chapitre, nous avons tout d'abord présenté un aperçu de la sécurité des réseaux sans fil et de leurs principes fondamentaux. Nous avons ensuite abordé les standards de sécurité, notamment les protocoles WEP, WPA, WPA2 et WPA3, en mettant en évidence leurs avantages et limites. Enfin, nous avons examiné les vulnérabilités des réseaux sans fil et les principales attaques qui en tirent parti. Malgré les avancées en matière de sécurité, les réseaux Wi-Fi restent exposés, ce qui rend indispensable la connaissance des failles et des mesures de protection.

Le troisième chapitre sera consacré à la présentation de l'organisme d'accueil, le Centre de Recherche en Technologies Agro-Alimentaires (CRTAA).

Chapitre 3 : Présentation de l'organisme d'accueil

3.1 Introduction

Dans le cadre de ce mémoire de fin de formation, consacré à la sécurisation des réseaux sans fil (Wi-Fi), il est essentiel de présenter l'organisme d'accueil ayant servi de terrain d'étude et d'expérimentation. Le Centre de Recherche en Technologies Agro-Alimentaires –CRTAA-, constitue un environnement professionnel riche, caractérisé par une infrastructure informatique notamment on réseaux Wi-Fi, en constante évolution et des besoins croissants en matière de sécurité des systèmes d'information.

Ce chapitre a pour objectif de fournir une vue d'ensemble sur cet organisme, en mettant en évidence sa présentation, ses missions principales, son organisation interne ainsi que son parc informatique. Cette présentation permettra de mieux comprendre le contexte dans lequel s'inscrit notre travail, notamment en ce qui concerne les enjeux liés à la sécurisation des réseaux sans fil au sein de l'établissement.

3.2 Présentation générale du CRTAA

3.2.1 Présentation du CRTAA

Le Centre de Recherche en Technologies Agro-Alimentaires (CRTAA) est un établissement public algérien de recherche scientifique et de développement technologique. Situé sur le campus universitaire de Targa Ouzemmour à Bejaïa, il a été officiellement créé en 2019.

Placé sous la tutelle du ministre chargé de la recherche scientifique, est chargé de réaliser des programmes de recherche scientifique et de développement technologique dans le domaine des technologies agroalimentaires portant notamment, sur la promotion de la recherche dans les domaines des technologies appliquées au secteur de l'agroalimentaire.

Il est aussi chargé de la contribution à l'élaboration des procédés visant la maîtrise et la diversification des propriétés d'usage et la fonctionnalité des produits à l'intention des industries de transformation.

Ce centre est aussi appelé à contribuer à l'élaboration de techniques de transformation et de préservation des produits agroalimentaires alternatives et meilleures pour

l'environnement, élaboration de techniques de gestion des ressources, de réduction de la quantité de déchets et de pertes découlant de la détérioration des produits survenant au cours de la production, de la transformation et de la distribution.

La participation au développement et à l'harmonisation de la législation ayant trait à la bioéthique, à la biosécurité et aux normes référentielles en collaboration avec les organismes concernés figurent également parmi les missions de centre de recherche en technologies agroalimentaires [37].

3.2.2 Carte d'identité du CRTAA

- ✓ Statut : Établissement Public à Caractère Scientifique et Technologique (EPST), relevant du secteur de la recherche scientifique en Algérie.
- ✓ Date de création : 29 Avril 2019
- ✓ Directrice : Pr. BOUCHERBA Nawal
- ✓ Siège : Route de Targa Ouzemmour, Campus Universitaire, 06000 Béjaia, Algérie
- ✓ Position GPS : 36.7601° N, 5.0550° E
- ✓ Site web : https://crtaa.dz/

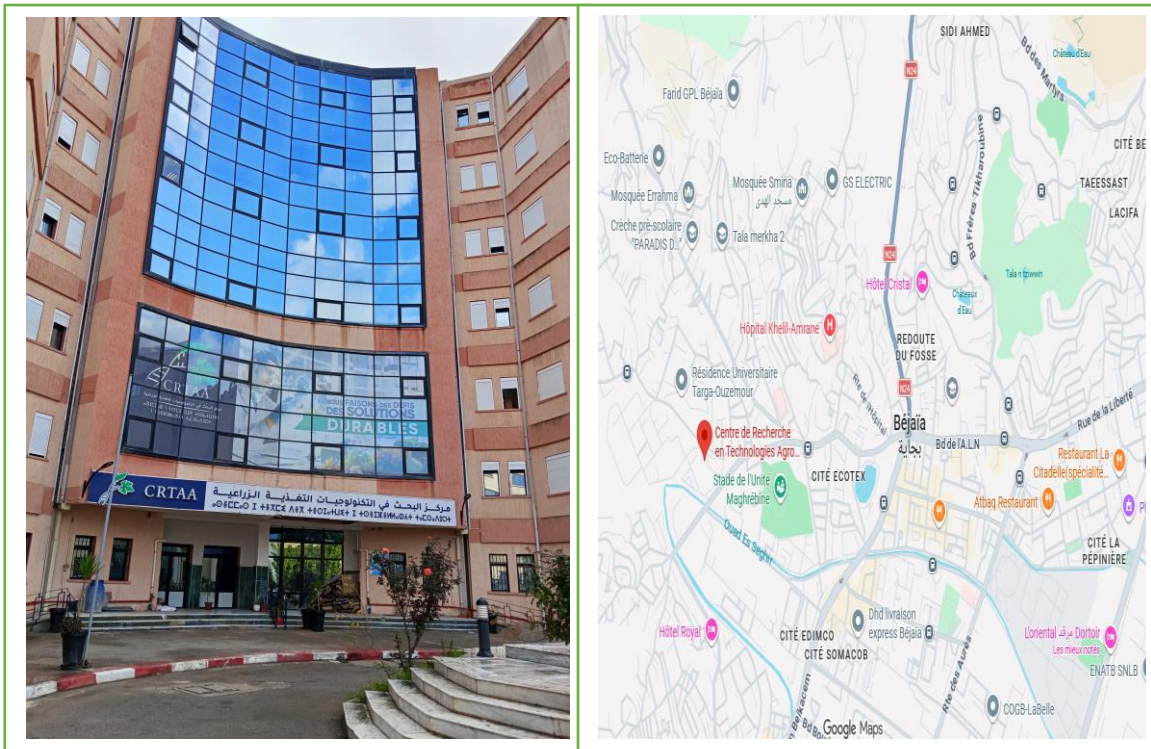

Figure 21 : Vue générale du CRTAA, avec indication de sa localisation

3.2.3 Fondements stratégiques de l'implantation du CRTAA à Bejaïa

L'installation du CRTAA dans la wilaya de Bejaïa s'inscrit dans une démarche stratégique qui prend en compte des dimensions scientifiques, économiques et géographiques.

Cette région se démarque par un potentiel agroalimentaire significatif, avec une production agricole variée et un tissu industriel robuste dédié à la transformation des denrées alimentaires, abritant des entreprises telles que Cevital, Ifri, Soummam et Danone Djurdjura.

La proximité du CRTAA avec les établissements universitaires favorise les échanges scientifiques et le développement de projets de recherche partenariaux, tout en permettant l'accueil d'étudiants pour des stages et des travaux académiques. Cela renforce la coopération entre la formation, la recherche et l'innovation. Par ailleurs, la position géographique avantageuse de Bejaïa, notamment grâce à son port, représente un atout essentiel pour le développement des échanges commerciaux et la mise en valeur des produits agroalimentaires tant au niveau national qu'international. Par conséquent, le choix de Bejaïa comme site pour le CRTAA reflète une volonté de lier la recherche scientifique aux besoins du terrain, tout en soutenant le développement économique local et en mettant en avant le savoir-faire régional.

3.3 Mission et Orientations Scientifiques du CRTAA

3.3.1 Mission du CRTAA

Faire progresser la connaissance et être utile à la société, tel est le rôle confié au CRTAA. Une mission nationale que l'établissement entend accomplir dans le respect des règles d'éthique et en s'engageant pour l'égalité professionnelle.

Une mission qui se décline en sept axes [38]:

1. la promotion de la recherche dans les domaines des technologies appliquées au secteur de l'agroalimentaire ;
2. l'élaboration des procédés visant la maîtrise et la diversification des propriétés d'usage et la fonctionnalité des produits à l'intention des industries de transformation ;

3. la contribution à l'élaboration de processus agroalimentaires rentables et de nouveaux produits et d'ingrédients agroalimentaires possédant de nouvelles caractéristiques sanitaires et fonctionnelles ;
4. la promotion de l'innovation alimentaire (aliments et santé, transformation des aliments et caractéristiques des aliments) en assurant l'innocuité des aliments ;
5. la contribution à l'élaboration de techniques de transformation et de préservation des produits agroalimentaires alternatives et meilleures pour l'environnement ;
6. la contribution à l'élaboration de techniques de gestion des ressources, de réduction de la quantité de déchets et de pertes découlant de la détérioration des produits survenant au cours de la production, de la transformation et de la distribution ;
7. la participation au développement et à l'harmonisation de la législation ayant trait à la bioéthique, à la biosécurité et aux normes référentielles.

3.3.2 Orientations Scientifiques (OS) du CRTAA

Les activités de recherche du CRTAA sont structurées autour de Cinq Orientations Scientifiques (OS) [39] :

OS 1. Répondre aux enjeux de la sécurité alimentaire et gérer les risques associés (environnementaux, sanitaires).
OS 2. Accompagner les mutations agro-écologique et la transition alimentaire, en associant les défis économiques et sociaux.
OS 3. Œuvrer pour une bio-économie basée sur une utilisation rationnelle et recyclante des ressources.
OS 4. Favoriser une approche globale de la notion aliment-santé.
OS 5. Intégrer la Data science et les technologies du numérique au services des décideurs et du grand public.
Cinq Orientations de Politique Générale (OPG)
OPG 1. Placer la Recherche, l'innovation et l'expertise dans nos relations avec la société et l'entreprise.
OPG 2. Etre un acteur engagé auprès des laboratoires universitaires et un leader dans les partenariats nationaux et internationaux.
OPG 3. Faire de la « Responsabilité alimentaire, Environnementale et sanitaire »: une priorité collective.

OPG 4. Le CRTAA s'engage dans des démarches de science participative, Il participera au dynamisme de l'écosystème de recherche et d'enseignement supérieur, en contribuant aux politiques de Tamayouz (en TIAA) et aux alliances de recherche.
OPG 5. Etablissement d'un réseau qui permettra de collaborer avec les meilleures équipes en Algérie et dans le monde (régional, Africain, méditerranéen.....) et l'indexation d'une revue scientifique sur l'aliment.

3.4 Organigramme du CRTAA

3.4.1 Divisions de recherche au niveau du CRTAA [40]

✓ **Division Biologie et Chimie Alimentaire**

La division de Biologie et Chimie Alimentaire se consacre à l'étude de la composition, des propriétés physico-chimiques et biologiques des denrées alimentaires, ainsi qu'à leur transformation, conservation et sécurité. Son objectif est de garantir la qualité des aliments consommés et de promouvoir l'innovation technologique dans le secteur agro-alimentaire. Elle est structurée autour de deux axes majeurs :

-la biologie alimentaire et la chimie alimentaire.
Cette division offre une compréhension approfondie des aliments, essentielle pour garantir leur qualité et leur valeur nutritionnelle. Elle permet d'explorer les interactions biologiques et les réactions chimiques qui surviennent tout au long du cycle de vie des aliments, depuis les processus de fabrication et de conservation jusqu'à la digestion, garantissant ainsi une expertise globale et appliquée dans le domaine de la science alimentaire.

-Ingénierie des Aliments et des Procédés Agro-Alimentaires (IAPAA)
La division « Ingénierie des aliments et des procédés agroalimentaires » se consacre à la recherche et au développement de solutions durables dans la transformation alimentaire. Elle vise à minimiser l'impact environnemental des procédés tout en favorisant l'économie circulaire et la valorisation des sous-produits. En collaboration avec des partenaires industriels, la division innove à travers des technologies de pointe et des techniques minimalistes pour garantir la qualité et la sécurité des produits tout en optimisant l'efficacité industrielle.

✓ **Division de la Sécurité Alimentaire**

La division de la Sécurité Alimentaire veille sur la sécurité et le contrôle de la qualité des aliments. Cette division assure également un contrôle continue de l'hygiène et l'innocuité des aliments ainsi que le maintien.

✓ **Division des Alertes et Veille**

La division des Alertes et Veille Règlementaire pour l'Alimentation a pour mission d'empêcher la fraude alimentaire et protéger le consommateur est parmi les préoccupations du CRTAA.

✓ **Division Ingénierie des Aliments et des Procédés Agro-Alimentaires**

La division « Ingénierie des aliments et des procédés agroalimentaires » se consacre à la recherche et au développement de solutions durables dans la transformation alimentaire. Elle vise à minimiser l'impact environnemental des procédés tout en favorisant l'économie circulaire et la valorisation des sous-produits. En collaboration avec des partenaires industriels, la division innove à travers des technologies de pointe et des techniques minimalistes pour garantir la qualité et la sécurité des produits tout en optimisant l'efficacité industrielle.

✓ **Division d'Agro-Ecologie Alimentaire**

La Division de recherche en Agroécologie Alimentaire se consacre à l'étude des écosystèmes agricoles et de leurs interactions avec l'environnement, en vue d'optimiser la production et la disponibilité alimentaire. Elle vise à développer des approches innovantes pour valoriser durablement les productions végétales et animales, tout en préservant les ressources naturelles et le patrimoine culinaire algérien. La Division s'engage à élaborer des solutions technologiques et des pratiques agroécologiques pour optimiser la gestion des ressources, réduire les déchets et les pertes durant les processus de production, transformation et distribution alimentaires, et renforcer la résilience des systèmes agroalimentaires face aux défis environnementaux.

3.4.2 Organigramme général du CRTAA

Le CRTAA est composé de plusieurs divisions, départements et services ; l'organigramme suivant en présente la structure générale.

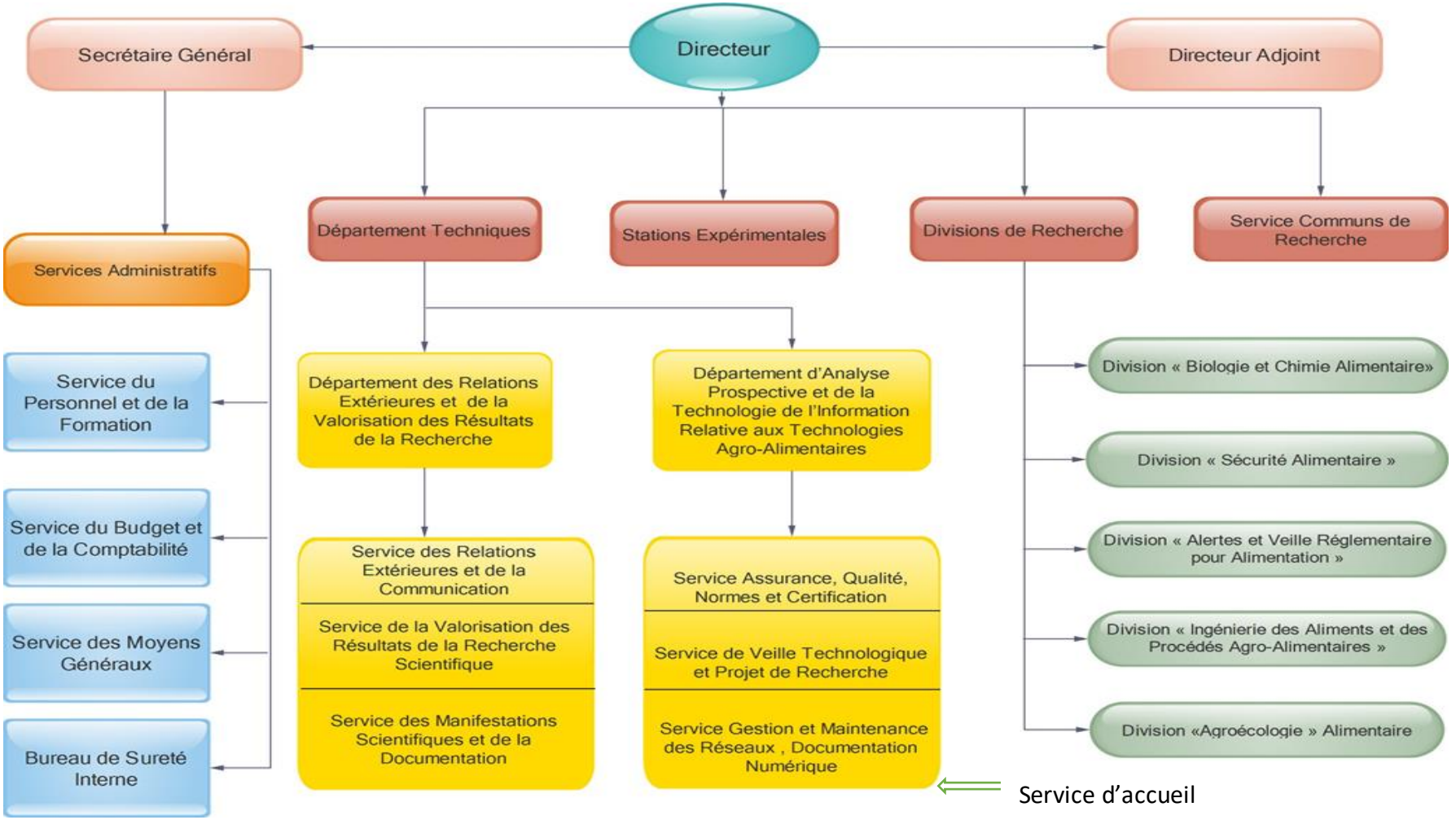

Figure 22 : Organigramme du Centre de Recherche en Technologies Agro-Alimentaires –CRTAA-

3.4.3 Rôle de Service Gestion et Maintenance des Réseaux au niveau du CRTAA

Le Service de Gestion et Maintenance des Réseaux du CRTAA assure la mise en place, l'administration et la maintenance de l'infrastructure réseau de l'établissement. Il veille au bon fonctionnement des réseaux informatiques (filaire et Wi-Fi), garantit la sécurité des systèmes d'information, et assure la disponibilité des services numériques. Ce service prend également en charge la surveillance du réseau, la résolution des incidents techniques, la gestion des équipements (routeurs, switchs, points d'accès) ainsi que l'assistance aux utilisateurs. Il contribue enfin à l'amélioration continue des performances du réseau et à la mise en œuvre des politiques de sécurité adaptées aux besoins du centre.

3.5 L'importance et Analyse des réseaux Wi-Fi au sein du CRTAA

3.5.1 L'importance des réseaux Wi-Fi au sein du CRTAA

Les réseaux Wi-Fi occupent une place essentielle au sein du CRTAA, en facilitant l'accès rapide et flexible aux ressources numériques pour l'ensemble du personnel scientifique, technique et administratif. Ils permettent une connectivité permanente aux systèmes d'information, favorisant ainsi le partage de données, l'accès aux bases de données scientifiques et la communication interne.

De plus, le Wi-Fi offre une grande mobilité aux chercheurs et aux ingénieurs, leur permettant de travailler efficacement dans différents espaces du centre sans contrainte de câblage. Il joue également un rôle clé dans l'intégration des équipements modernes et des dispositifs connectés utilisés dans les activités de recherche.

Enfin, l'utilisation des réseaux Wi-Fi contribue à améliorer la productivité et la collaboration au sein du CRTAA, tout en nécessitant la mise en place de mécanismes de sécurité adaptés pour protéger les données sensibles et garantir la fiabilité du réseau.

3.5.2 Analyse du réseau Wi-Fi du CRTAA

L'analyse du réseau Wi-Fi du CRTAA constitue une étape essentielle dans l'évaluation de son niveau de performance et de sécurité. Elle permet d'identifier les caractéristiques de l'infrastructure existante, ainsi que les éventuelles faiblesses pouvant compromettre son bon fonctionnement.

✓ **Architecture du réseau Wi-Fi**

Le réseau Wi-Fi du CRTAA repose sur une architecture composée de plusieurs points d'accès (Access Points) répartis à travers les différents services et laboratoires. Ces équipements sont interconnectés via le réseau local filaire (LAN), assurant ainsi la distribution de la connectivité Internet et l'accès aux ressources internes.

✓ **Couverture et accessibilité**

La couverture Wi-Fi est conçue pour répondre aux besoins de mobilité du personnel. Toutefois, certaines zones peuvent présenter des faiblesses de signal, notamment en raison des obstacles physiques (murs, équipements) ou d'une mauvaise répartition des points d'accès. Cela peut impacter la qualité de service et la stabilité de la connexion.

✓ **Sécurité du réseau**

Le niveau de sécurité du réseau Wi-Fi dépend des protocoles utilisés (WPA2/WPA3), de la gestion des accès (authentification, mots de passe) et de la configuration des équipements. Une analyse approfondie permet de détecter d'éventuelles vulnérabilités telles que :

- L'utilisation de mots de passe faibles,
- L'absence de segmentation réseau,
- Une mauvaise configuration des points d'accès.

✓ **Performance du réseau**

Les performances du réseau Wi-Fi sont évaluées en termes de débit, de latence et de stabilité. Une surcharge du réseau, un nombre élevé d'utilisateurs connectés ou des interférences peuvent entraîner une dégradation de la qualité de service.

✓ **Gestion et maintenance**

Le Service de Gestion et Maintenance des Réseaux assure le suivi, la supervision et la maintenance du réseau Wi-Fi. Cependant, l'absence d'outils avancés de monitoring ou de politiques de maintenance régulières peut limiter l'efficacité de cette gestion.

✓ **Identification des limites**

L'analyse du réseau met en évidence plusieurs limites potentielles :

- Insuffisance de couverture dans certaines zones,
- Niveau de sécurité perfectible,
- Manque de contrôle des accès utilisateurs,
- Absence de solutions avancées de supervision.

3.6 Présentation des équipements réseaux filaire et Wi-Fi du CRTAA

L'infrastructure réseau et sans fil du CRTAA repose principalement sur des équipements Cisco, reconnus pour leur fiabilité, leur performance et leurs mécanismes avancés de sécurité. Leader dans les technologies de l'information et de la communication, Cisco propose des solutions complètes de commutation, de routage et de réseaux sans fil, largement utilisées dans les environnements professionnels.

3.6.1 Équipements de l'infrastructure réseau filaire

Le réseau filaire du CRTAA est structuré autour de plusieurs équipements stratégiques assurant la distribution, le routage et la sécurité des données.

✓ **Switch fédérateur Cisco Catalyst 4506E**

Le switch cœur de réseau Cisco Catalyst 4506E constitue l'élément central de l'architecture. Il assure l'agrégation des flux réseau, la gestion du trafic et la haute disponibilité du backbone. Grâce à son architecture modulaire, il permet une grande évolutivité et une tolérance aux pannes.

✓ **Routeur Cisco ISR 4431.**

Le routeur Cisco ISR 4431 est utilisé pour l'interconnexion avec les réseaux externes, notamment Internet. Il supporte plusieurs services tels que le VPN, la traduction d'adresses (NAT), ainsi que des mécanismes de qualité de service (QoS).

✓ **Pare-feu Fortinet (FortiGate)**

Le pare-feu Fortinet (FortiGate) assure la sécurité périmétrique du réseau. Il protège l'infrastructure contre les menaces externes grâce à des fonctionnalités avancées telles que le filtrage des paquets, la détection d'intrusion (IDS/IPS) et le contrôle applicatif.

✓ **Switchs Cisco Catalyst 3650 (C-3650)**

Les commutateurs Cisco Catalyst 3650 sont utilisés au niveau de la couche de distribution. Ils offrent des fonctionnalités avancées de niveau 3 (routage inter-VLAN), ainsi que le support du PoE (Power over Ethernet) pour alimenter certains équipements réseau.

✓ **Switchs Cisco Catalyst 2960X**

Les switchs Cisco Catalyst 2960X sont déployés au niveau de la couche d'accès. Ils assurent la connectivité des postes de travail, imprimantes et autres équipements, avec des performances fiables et une gestion simplifiée.

Figure 23 : Équipements de l'infrastructure réseau filaire au sein du CRTAA

3.6.2 Équipements de l'infrastructure Wi-Fi

L'infrastructure sans fil du CRTAA repose sur une architecture centralisée permettant une gestion efficace et sécurisée des points d'accès.

✓ **Contrôleur Wi-Fi Cisco 3504 (WLC)**

Le contrôleur Cisco 3504 Wireless LAN Controller permet la gestion centralisée de l'ensemble des points d'accès Wi-Fi. Il assure des fonctions essentielles telles que l'authentification, la sécurité, la gestion des canaux radio, le roaming et la supervision du réseau sans fil.

✓ **Points d'accès Cisco Aironet Air-AP1832I-E-K9**

Les points d'accès Cisco Aironet 1832I assurent la couverture Wi-Fi au sein du CRTAA. Compatibles avec la norme 802.11ac Wave 2, ils offrent des performances élevées, une connectivité bi-bande (2.4 GHz / 5 GHz) et une capacité adaptée aux environnements professionnels.

Figure 24 : Équipements de l'infrastructure Wi-Fi au sein du CRTAA

3.7 Conclusion

En conclusion, ce chapitre a permis de présenter de manière détaillée l'organisme d'accueil, le Centre de Recherche en Technologies Agro-Alimentaires (CRTAA), en mettant en évidence son cadre institutionnel, ses missions, son organisation interne ainsi que son environnement technique. L'analyse du réseau Wi-Fi a permis d'identifier son importance stratégique au sein du centre, tout en mettant en lumière certaines limites et vulnérabilités liées à sa sécurité et à ses performances. Ces constats justifient pleinement la nécessité de proposer des solutions adaptées pour renforcer la sécurisation du réseau sans fil, qui feront l'objet des chapitres suivants.

Chapitre 4 : Mise en œuvre et réalisation

4.1 Introduction

Ce projet s'inscrit dans le domaine de la sécurité des réseaux Wi-Fi et vise à proposer une solution au problème d'authentification au sein du réseau du Centre de Recherche en Technologies Agro-Alimentaires (CRTAA). Dans ce chapitre, nous présentons la mise en œuvre pratique de l'architecture WLAN sécurisée proposée, réalisée à l'aide de l'outil de simulation Cisco Packet Tracer, afin de valider les choix techniques en matière de sécurité, de segmentation et de gestion des accès. Cette implémentation repose sur un système d'authentification basé sur un serveur RADIUS, s'appuyant sur le mécanisme 802.1X et utilisant le protocole EAP, permettant d'authentifier les utilisateurs avant tout accès au réseau de l'entreprise.

4.2 Analyse du contexte et de l'infrastructure existante

L'analyse du contexte permet d'identifier les besoins réels de l'établissement en matière de connectivité, de sécurité et de gestion des accès, ainsi que de mettre en évidence les limitations de l'architecture actuelle. L'objectif est de proposer par la suite une solution adaptée basée sur une architecture WLAN sécurisée et centralisée.

4.2.1 Analyse de l'existant

L'étude de l'infrastructure actuelle a permis d'identifier plusieurs limitations :

- Un réseau Wi-Fi **lent et instable**, impactant la productivité ;
- Absence de **segmentation réseau** (tous les utilisateurs sur le même réseau) ;
- Faible niveau de sécurité (accès non contrôlé) ;
- Difficulté de gestion et d'administration.

4.2.2 Problématique

La problématique principale de ce projet est de concevoir et de sécuriser une infrastructure WLAN performante au sein du CRTAA, permettant d'assurer une authentification forte des utilisateurs, une segmentation dynamique des accès, une isolation complète des invités ainsi qu'une amélioration des performances globales du réseau.

4.2.3 Objectifs du projet

Dans le but de répondre à la problématique identifiée, ce projet vise à concevoir et à mettre en œuvre une architecture WLAN sécurisée et performante adaptée aux besoins du CRTAA. Les objectifs principaux de ce projet sont les suivants :

- Mettre en place un mécanisme d'authentification forte basé sur un serveur RADIUS et la norme IEEE 802.1X ;
- Assurer une segmentation efficace du réseau à l'aide des VLAN afin de séparer les différents profils d'utilisateurs ;
- Garantir une isolation complète des utilisateurs invités pour limiter leur accès aux ressources internes ;
- Améliorer les performances globales du réseau sans fil ;
- Renforcer la sécurité des communications grâce à l'utilisation de protocoles de chiffrement avancés ;
- Faciliter la gestion et l'administration du réseau à travers une approche centralisée.

La réalisation de ces objectifs permettra d'assurer un accès sécurisé, fiable et optimisé au réseau WLAN du CRTAA.

4.3 Environnement de simulation et techniques de sécurisation

4.3.1 Présentation de l'outil Cisco Packet Tracer

Cisco Packet Tracer est un logiciel de simulation complet dédié à l'enseignement et à l'apprentissage. Il offre une combinaison unique d'expériences de simulation et de visualisation réalistes, de fonctionnalités d'évaluation et de création d'activités ainsi que d'opportunités de collaboration et de mise en concurrence de plusieurs utilisateurs.

Les fonctionnalités innovantes de Cisco Packet Tracer aident les élèves et les enseignants à collaborer, à régler des problèmes et à découvrir des concepts dans un environnement social attrayant et dynamique [41].

4.3.2 Mise en œuvre du mécanisme d'authentification

Comme présenté dans le chapitre 2, le mécanisme d'authentification repose sur un serveur RADIUS, associé à la norme IEEE 802.1X et au protocole EAP. L'objectif est d'assurer un contrôle d'accès sécurisé en exigeant une authentification préalable des utilisateurs. Le point d'accès joue le rôle d'équipement d'authentification en relayant les requêtes vers le serveur RADIUS, chargé de valider les identifiants.

La mise en œuvre sous Cisco Packet Tracer a permis de simuler une authentification centralisée, où chaque accès est contrôlé avant autorisation. Ce mécanisme permet également l'application de politiques d'accès, notamment l'attribution dynamique de VLAN selon le profil de l'utilisateur, renforçant ainsi la sécurité du réseau.

4.3.3 Segmentation du réseau par VLAN

Une segmentation du réseau à l'aide des VLAN (Virtual Local Area Network) a été mise en œuvre afin d'améliorer le contrôle d'accès et l'organisation du réseau. Un VLAN permet de diviser un réseau physique en plusieurs réseaux logiques indépendants, offrant ainsi une meilleure isolation des différents types de trafic.

Cette approche permet de regrouper les utilisateurs selon leurs rôles ou leurs besoins (administrateurs, employés, invités, etc.), tout en limitant les communications entre ces groupes. Ainsi, même si plusieurs utilisateurs sont connectés au même point d'accès sans fil, ils peuvent être affectés à des VLAN distincts, réduisant considérablement les risques liés aux accès non autorisés.

Tableau 5 : Présentation des différents VLANs

VLAN	Nom	Description
20	CRTAA	Employés (STAFF)
50	guest	Invités
200	Management	Administration (Management)

4.4 Conception et fonctionnement de l'architecture WLAN sécurisée

4.4.1 Conception de l'architecture WLAN proposée

Dans le cadre de ce projet, une architecture WLAN centralisée a été conçue et implémentée à l'aide de Cisco Packet Tracer. Cette architecture repose sur l'utilisation d'un contrôleur sans fil (WLC), permettant une gestion centralisée des points d'accès et une meilleure application des politiques de sécurité.

Cette architecture permet de centraliser la gestion du réseau, d'améliorer la sécurité et de simplifier l'administration.

L'architecture proposée comprend les éléments suivants :

- Un **switch fédérateur (Cisco 3560)** assurant la connectivité et le routage ;
- Un **contrôleur WLAN (WLC-3504)** pour la gestion centralisée du réseau sans fil ;
- Un **point d'accès léger (LAP)** permettant la couverture Wi-Fi ;
- Un **serveur RADIUS** pour l'authentification des utilisateurs ;
- Un **poste administrateur (PC)** pour la configuration et la supervision ;
- Des **clients sans fil (ordinateurs portables).**

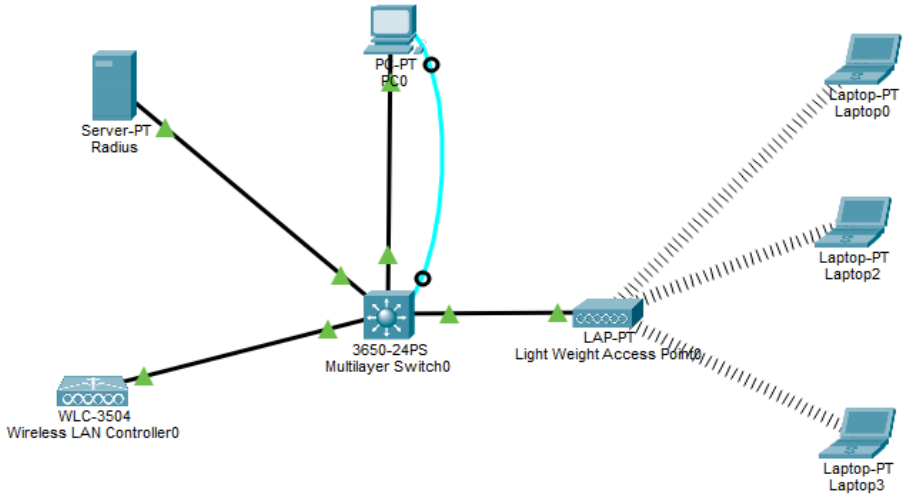

Figure 25 : Architecture de la solution WLAN centralisée avec serveur RADIUS

4.4.2 Description du fonctionnement de la solution

Le fonctionnement de l'architecture WLAN proposée repose sur lorsqu'un utilisateur tente de se connecter au réseau Wi-Fi :

- ✓ Le client détecte le SSID diffusé par le point d'accès ;
- ✓ Le point d'accès transmet la demande d'authentification au contrôleur WLAN ;
- ✓ Le contrôleur WLAN relaie la requête vers le serveur RADIUS ;
- ✓ Le serveur RADIUS vérifie les identifiants de l'utilisateur ;
- ✓ En cas de succès, l'accès est autorisé et une adresse IP est attribuée ;
- ✓ L'utilisateur accède au réseau en fonction de ses droits.

Ce processus garantit une authentification forte et un contrôle d'accès rigoureux.

4.5 Mise en œuvre de la solution sous Packet Tracer

La mise en œuvre de cette architecture a été réalisée en plusieurs étapes, permettant de simuler un environnement réseau réaliste. Les étapes présentées ci-après concernent le cas du WLAN CRTAA (Staff) avec une authentification basée sur un serveur RADIUS. Les mêmes étapes sont suivies pour la création du WLAN Guest (invités), avec toutefois l'utilisation d'une sécurité de type WPA2-Personal.

Tableau 6 : Table d'Adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau
PC- admin	Carte réseau (NIC)	192.168.200.1	255.255.255.0
WLC	Gestion	192.168.200.100	255.255.255.0
Switch fédérateur	VLAN 20	192.168.20.253	255.255.255.0
	VLAN 50	192.168.50.253	255.255.255.0
	VLAN 200	192.168.200.253	255.255.255.0
Serveur RADIUS	Carte réseau	192.168.20.253	255.255.255.0
LAP-PT	G0	le protocole DHCP	255.255.255.0
Laptop sans fil	Carte réseau	le protocole DHCP	255.255.255.0
Laptop sans fil	Carte réseau	le protocole DHCP	255.255.255.0
Laptop sans fil	Carte réseau	le protocole DHCP	255.255.255.0

4.5.1 Configuration de Switch fédérateur Cisco Catalyst

Le switch fédérateur a été configuré afin de :

- Créer les VLAN nécessaires à la segmentation du réseau
- Assurer le routage des flux entre les différentes entités du réseau

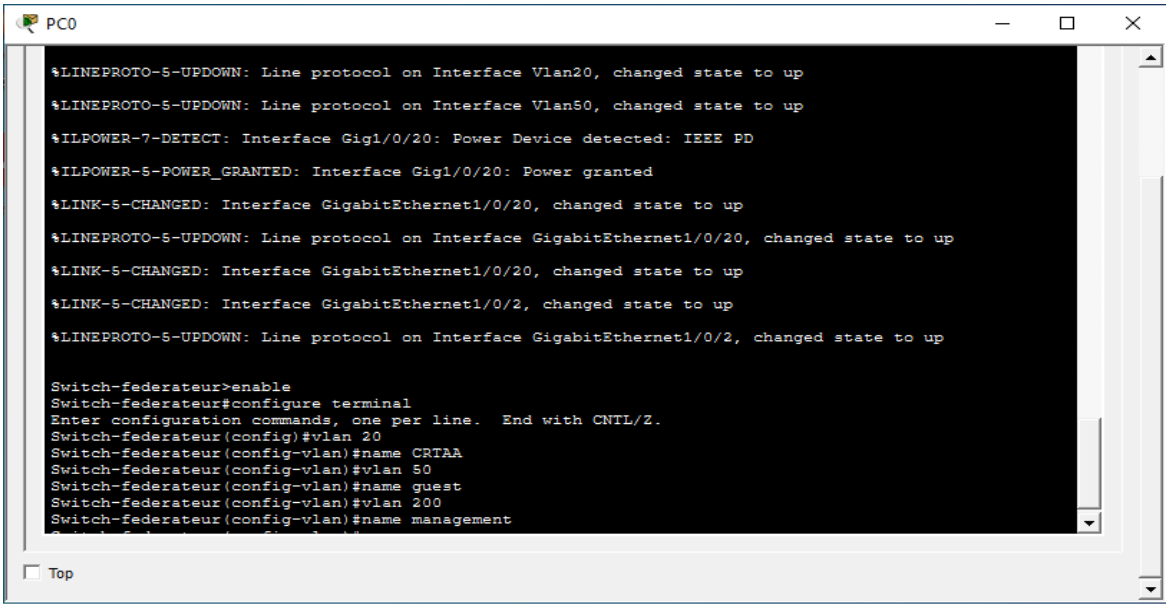

Figure 26 : Création des VLAN sur le switch fédérateur

- Pour confirmer la création des VLAN, la commande `show vlan brief` est utilisée :

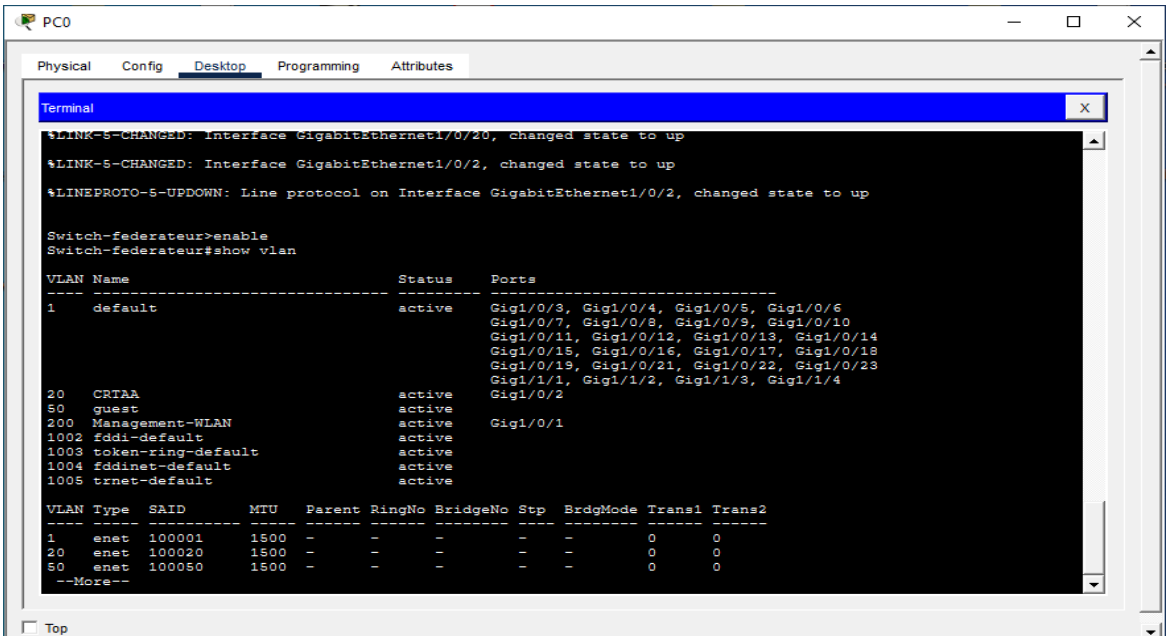

Figure 27 : Vérification des VLAN avec la commande *show vlan brief*

4.5.2 Configuration du contrôleur WLAN (WLC)

Le contrôleur WLAN (WLC) permet de centraliser la gestion des points d'accès et d'offrir des services avancés de configuration et de sécurité. L'accès au WLC s'effectue via une interface web en utilisant les identifiants configurés lors de l'initialisation.

La configuration de base du WLAN sur le WLC comprend les étapes suivantes :

1.Connexion au contrôleur WLC : Se connecter au contrôleur Wi-Fi Cisco 3504 à l'aide d'un navigateur web depuis le PC de l'administrateur, en utilisant l'adresse IP par défaut (192.168.1.1 lors de la première utilisation).

Figure 28 : Interface de connexion au contrôleur WLAN (WLC)

2.Création d'un compte administrateur : Configurer les identifiants d'accès : Nom d'utilisateur : admincrtaa, Mot de passe : Crtaa@2026

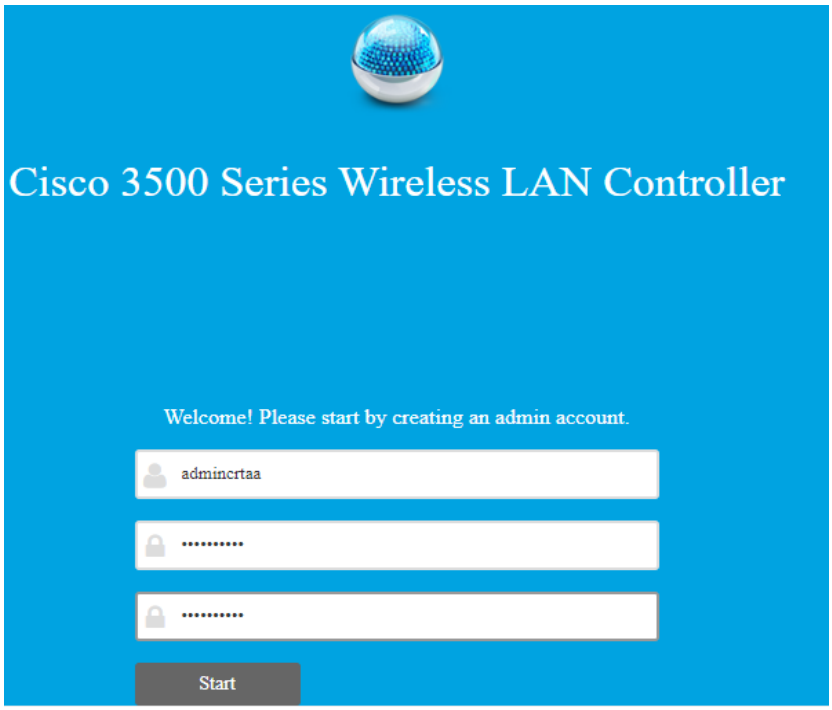

Figure 29 : Création du compte administrateur sur le WLC

3.Configuration du système et de l'adressage IP : Définir le nom du système et modifier l'adresse IP par défaut du contrôleur afin de l'adapter au plan d'adressage du réseau.

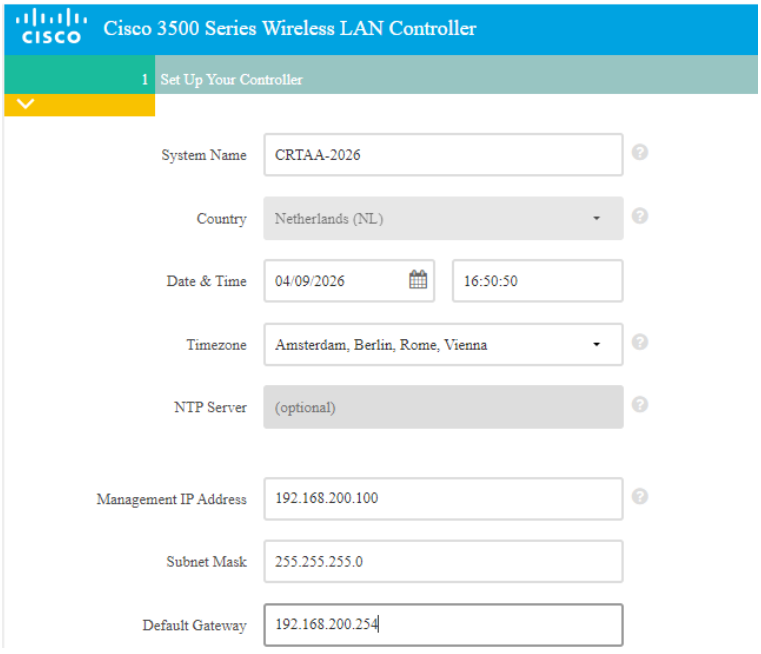

Figure 30 : Configuration initiale du système et de l'adressage IP du WLC

4.Vérification de l'accès au WLC : Se connecter à l'interface web avec les identifiants créés afin de valider la configuration initiale.

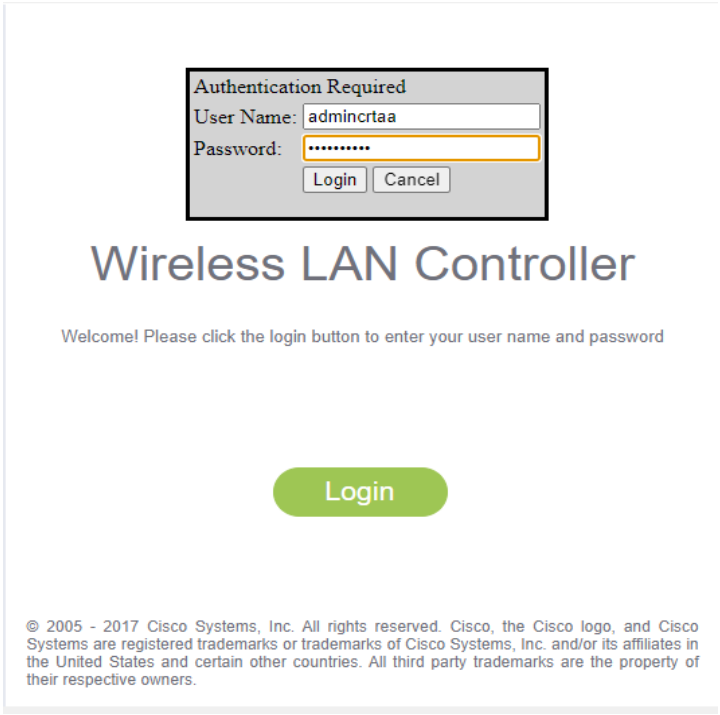

Figure 31 : Interface d'authentification au WLC (login administrateur)

5.Création du WLAN : Créer un nouveau réseau sans fil avec le SSID : **CRTAA**

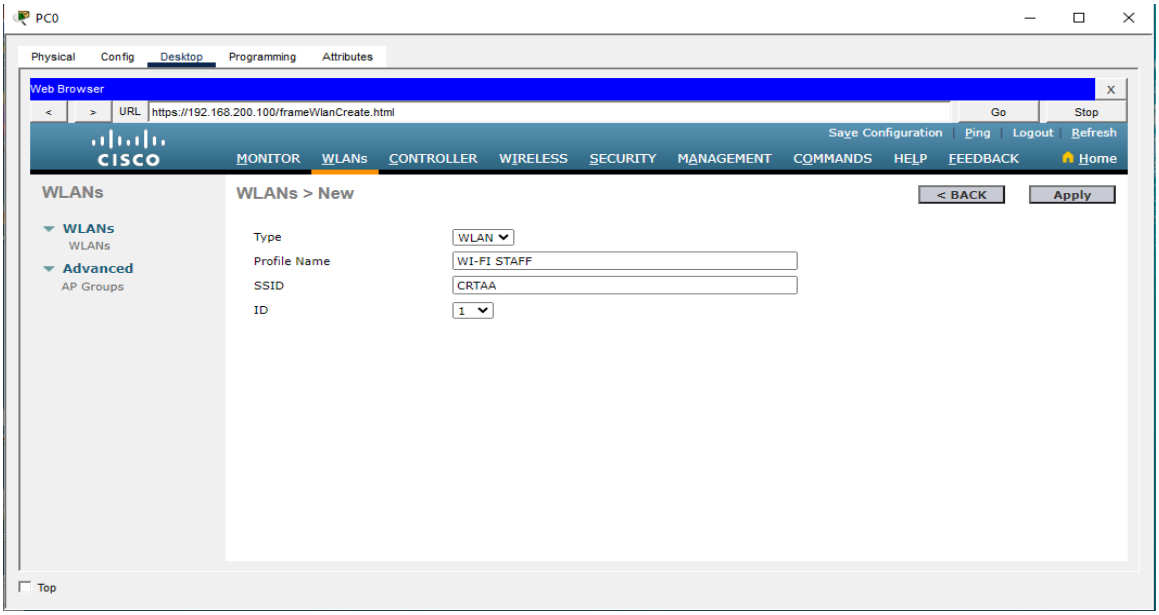

Figure 32 : Création du WLAN (SSID CRTAA)

6.Activation et configuration du WLAN : Activer le WLAN et configurer ses paramètres généraux (SSID, VLAN associé, politiques d'accès).

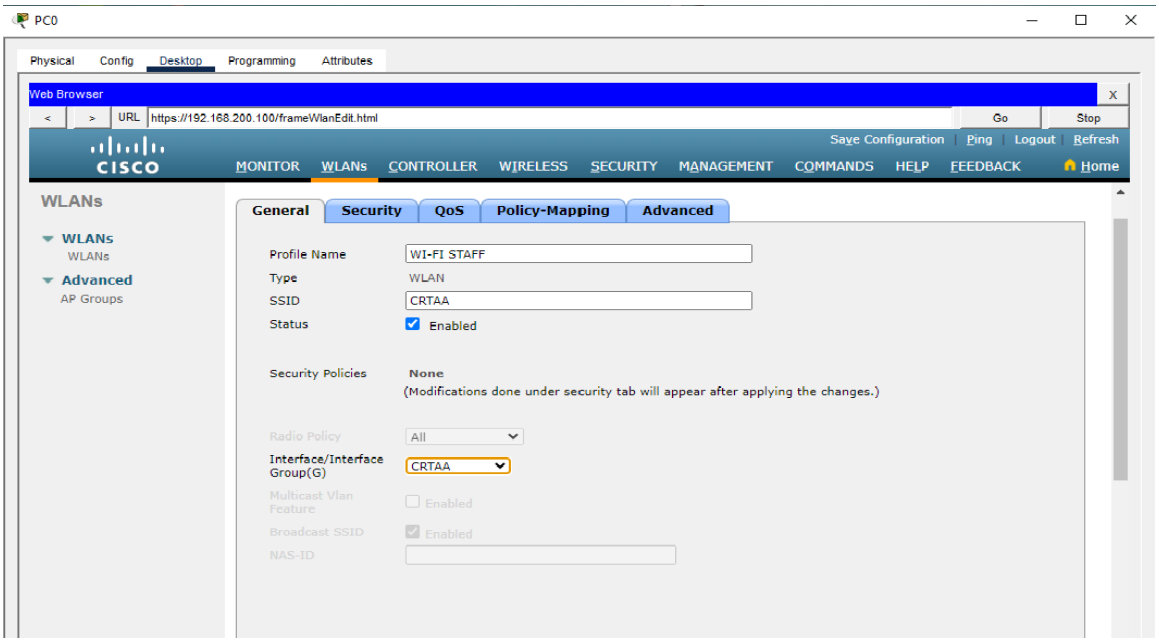

Figure 33 : Activation et configuration des paramètres du WLAN

7.Configuration de la sécurité (AAA) : L'administrateur configure l'utilisation d'un serveur RADIUS pour assurer les services d'authentification, d'autorisation et de comptabilité (AAA).

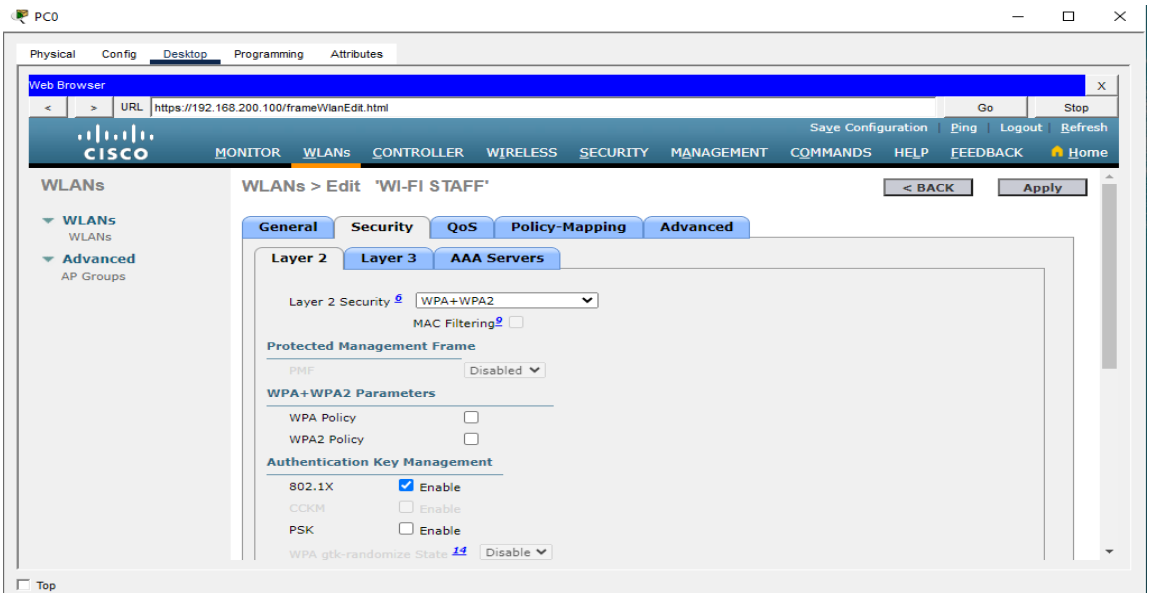

Figure 34 : Configuration de la sécurité WLAN (WPA2-Enterprise)

8.Ajout du serveur RADIUS : Renseigner les paramètres du serveur RADIUS (adresse IP, clé secrète partagée, port).

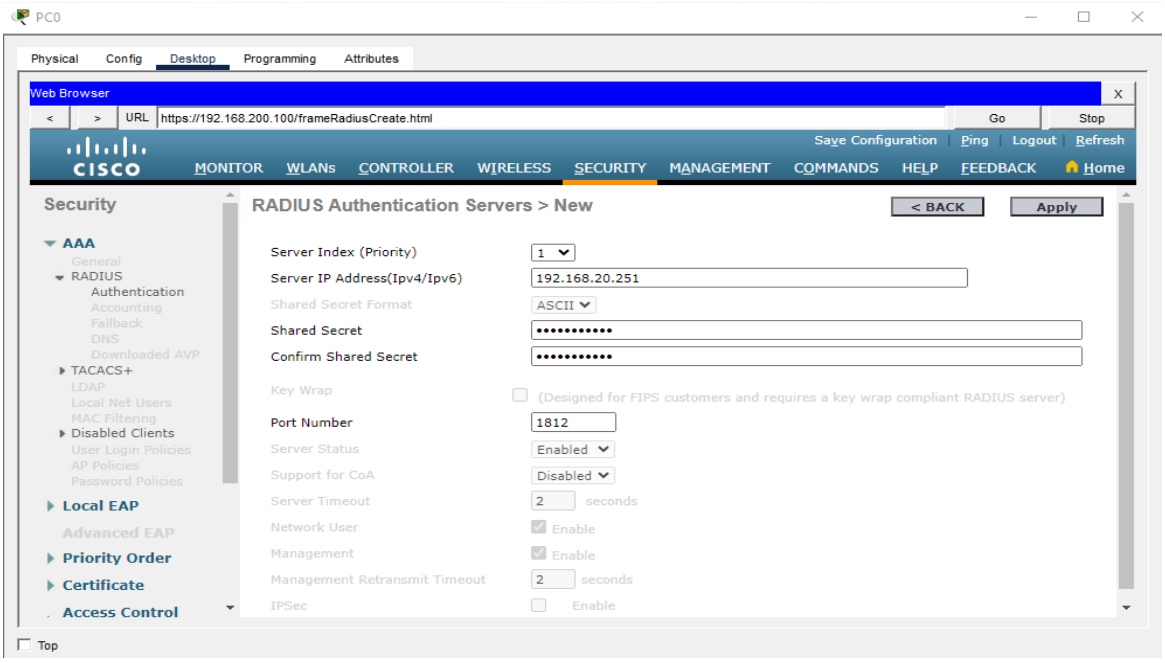

Figure 35 : Ajout du serveur RADIUS sur le WLC

9.Validation du serveur RADIUS : Vérifier que le serveur est bien ajouté et actif dans la liste des serveurs d'authentification.

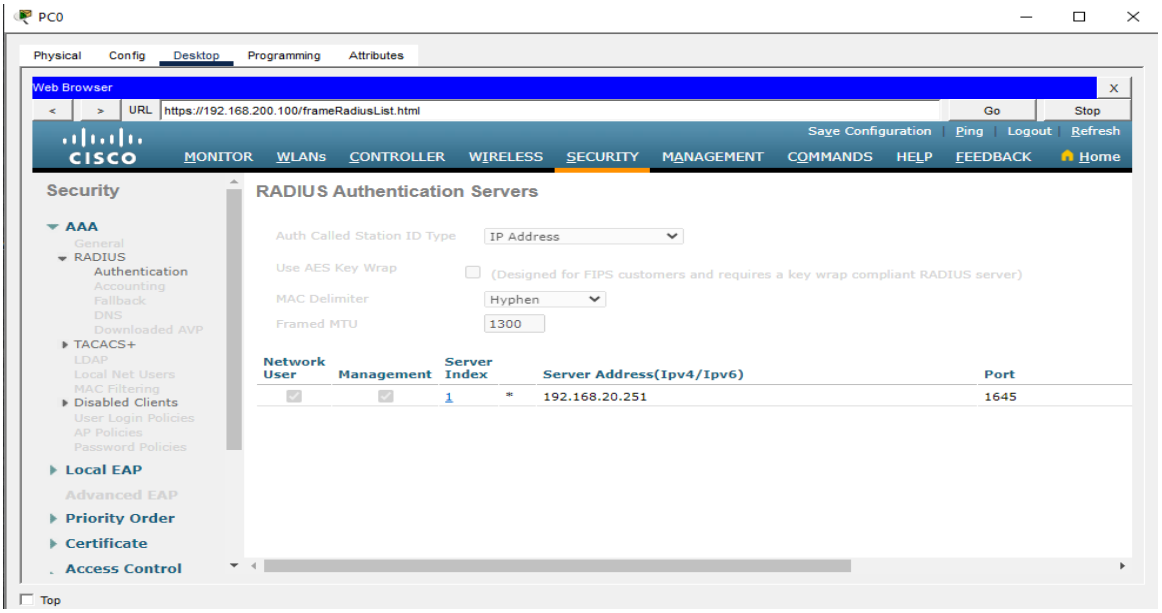

Figure 36 : Vérification de la configuration du serveur RADIUS

10.Vérification du fonctionnement du WLAN : Accéder au menu *WLANs* pour vérifier l'état du réseau sans fil configuré.

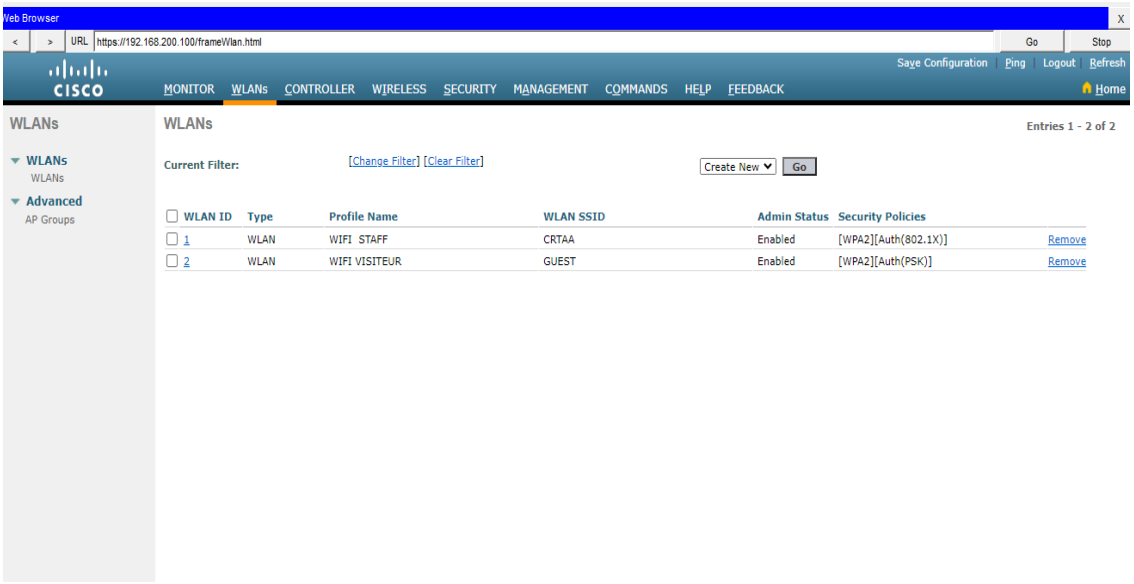

Figure 37 : Affichage du WLAN configuré dans le menu WLANs

11.Création des interfaces VLAN : Chaque WLAN nécessite une interface virtuelle spécifique. Accéder à : **Controller > Interfaces > New** pour créer les interfaces correspondantes.

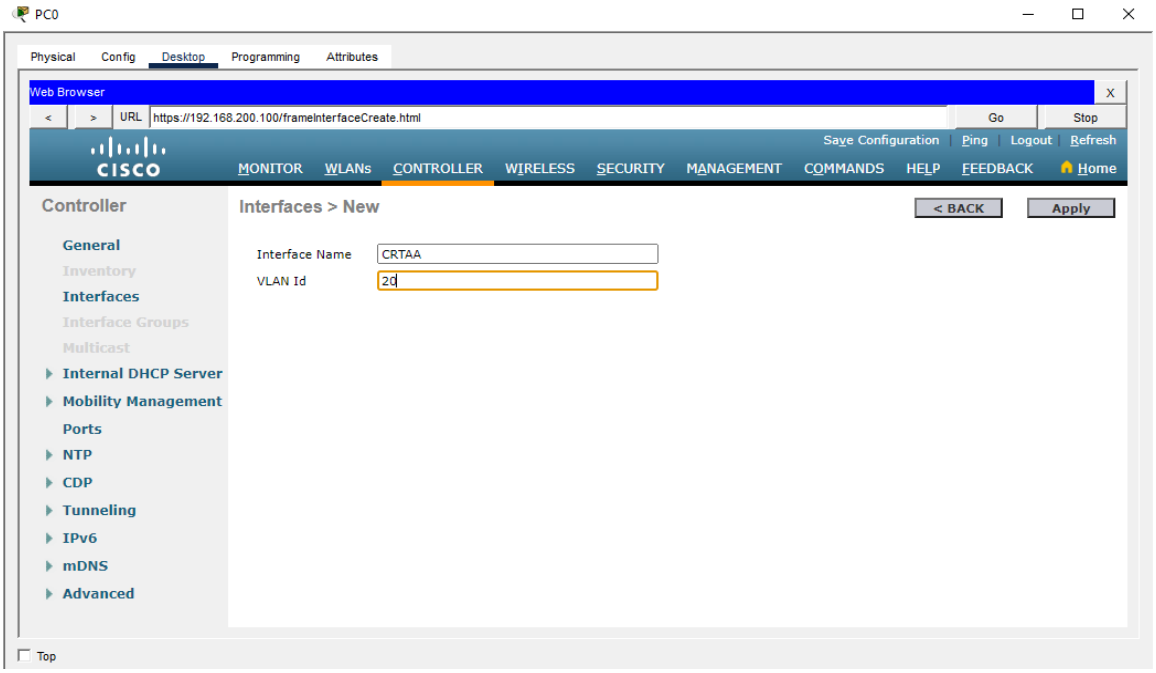

Figure 38 : Création des interfaces VLAN sur le contrôleur WLC

12.Résultat de la configuration des interfaces :(Voir figure correspondante)

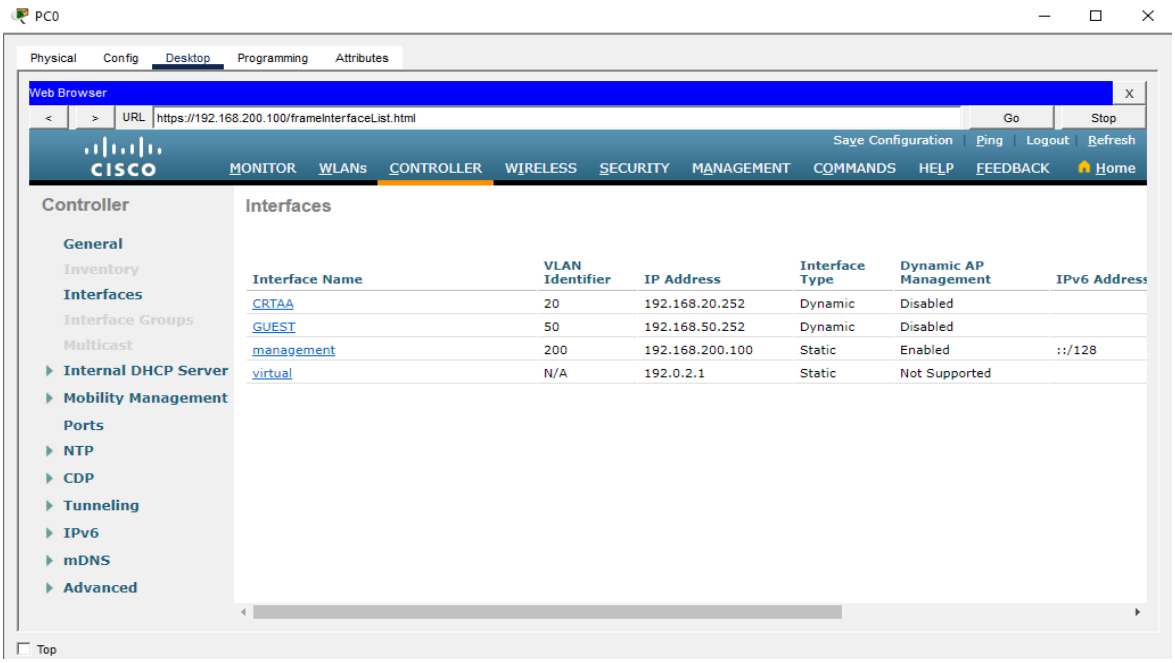

Figure 39 : Résultat de la configuration des interfaces VLAN

13.Configuration du serveur DHCP : Modifier la plage d'adresses IPv4 DHCP afin d'assurer l'attribution automatique des adresses IP aux clients.

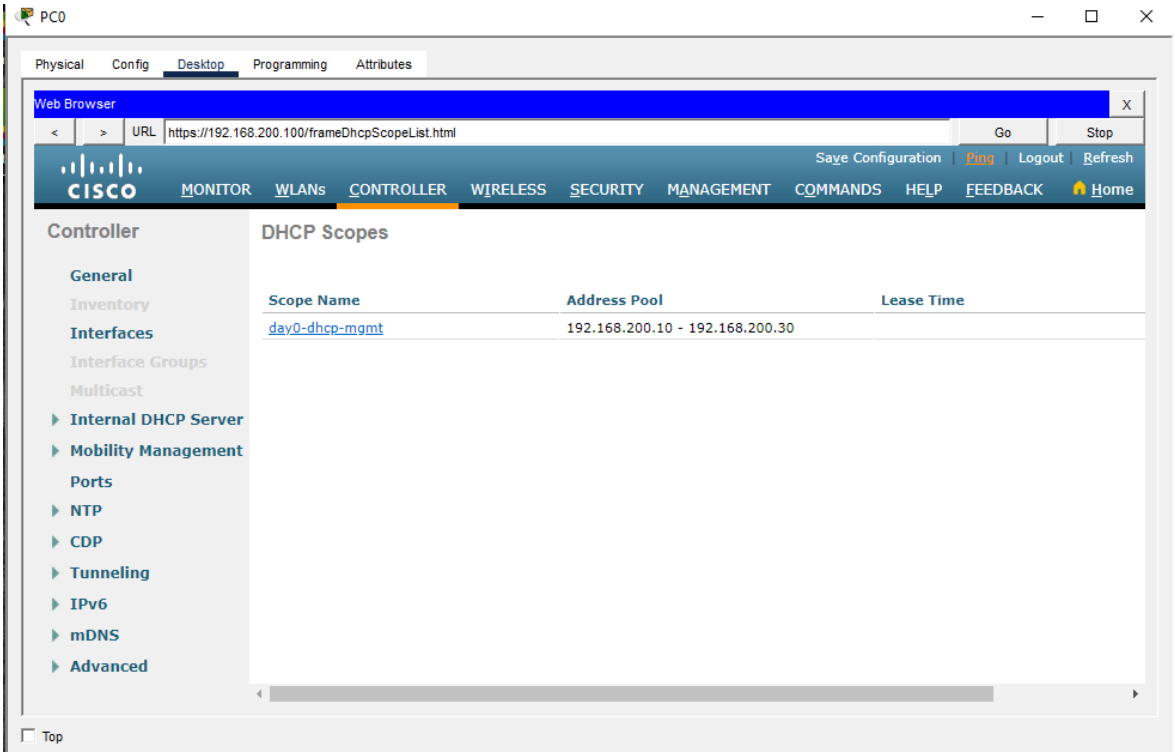

Figure 40 : Configuration de l'étendue DHCP sur le WLC

14.Supervision du WLAN : Utiliser l'onglet *Monitor* pour consulter les statistiques et vérifier le bon fonctionnement du WLAN **CRTAA**.

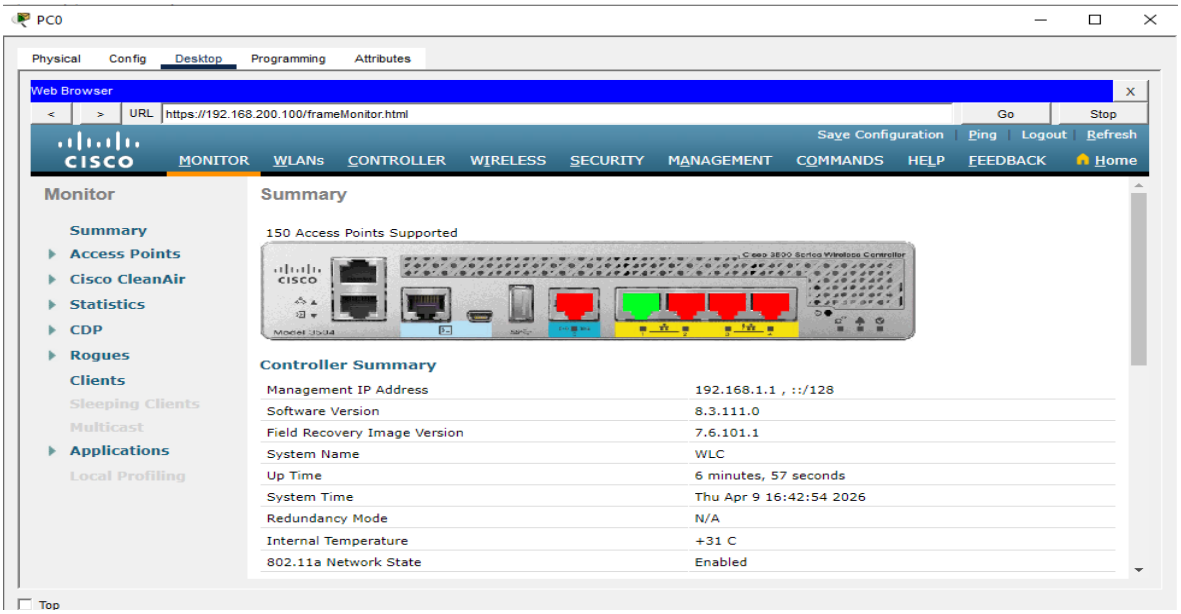

Figure 41 : Supervision du WLAN via l'onglet Monitor

4.5.3 Connexion des clients sans fil

Les clients sans fil (dans notre cas, des PC portables) ont été configurés pour :

- Se connecter au SSID **CRTAA**
- Utiliser une authentification **WPA2-Enterprise**
- S'authentifier via le serveur **RADIUS**

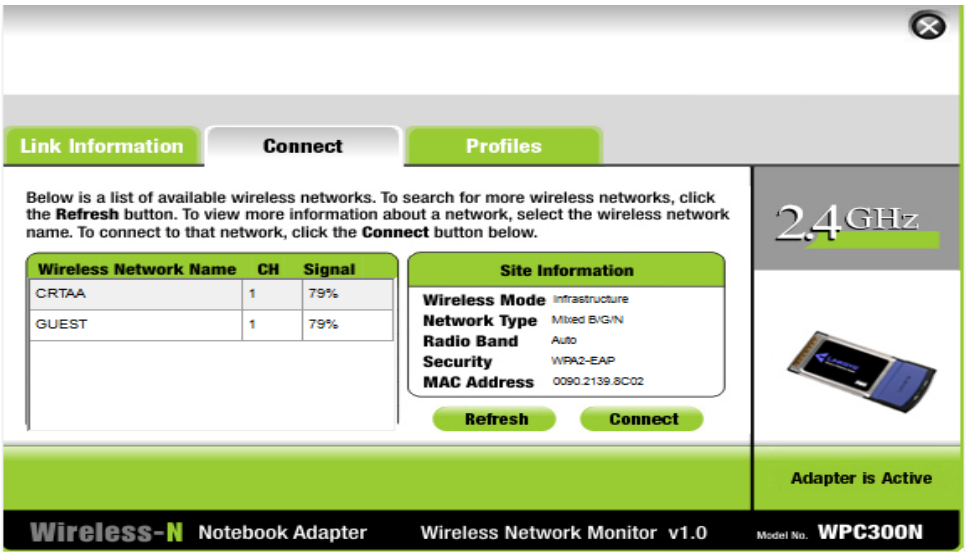

Figure 42 : Connexion d'un client sans fil au réseau CRTAA

4.6 Évaluation des performances et limites de la solution

4.6.1 Évaluation des performances

L'implémentation de cette solution a permis de constater plusieurs améliorations :

- Renforcement de la sécurité grâce à une authentification centralisée via RADIUS ;
- Meilleure gestion du réseau grâce au contrôleur WLAN ;
- Isolation des utilisateurs via la segmentation VLAN ;
- Amélioration de la stabilité et des performances globales.

Ainsi, cette architecture répond efficacement aux besoins du CRTAA en matière de sécurité et de gestion des accès.

4.6.2 Limites de la solution

Malgré les avantages obtenus, certaines limites peuvent être identifiées :

- Les fonctionnalités de simulation de Packet Tracer restent limitées ;
- L'absence de certains protocoles et mécanismes avancés ;
- Un environnement simulé ne reflétant pas totalement les conditions réelles (interférences, charge, mobilité, etc.).

4.7 Conclusion

Ce chapitre a permis de mettre en œuvre une architecture WLAN sécurisée et centralisée adaptée aux besoins du CRTAA. Grâce à l'utilisation du contrôleur WLAN et du serveur RADIUS, il a été possible d'assurer une authentification forte, une gestion efficace des accès et une amélioration globale des performances du réseau.

Conclusion générale

Au terme de ce travail, il apparaît clairement que les réseaux Wi-Fi occupent aujourd'hui une place incontournable dans notre quotidien, que ce soit dans les environnements professionnels, académiques ou personnels. Leur facilité d'utilisation et leur flexibilité en font une solution très attractive, mais ces mêmes avantages peuvent également devenir des points faibles lorsqu'il s'agit de sécurité.

Tout au long de ce mémoire, nous avons pu comprendre que la sécurisation des réseaux sans fil ne se limite pas à l'application de quelques paramètres de base. Elle nécessite une véritable réflexion globale, allant de la compréhension des normes Wi-Fi jusqu'à l'analyse des vulnérabilités et des différentes attaques possibles. L'étude des protocoles comme WEP, WPA, WPA2 et WPA3 a montré que, malgré les améliorations apportées au fil du temps, aucun système n'est totalement à l'abri.

La partie pratique réalisée au sein du CRTAA a été particulièrement enrichissante. Elle nous a permis de passer de la théorie à la pratique, en analysant une infrastructure réelle, en identifiant ses limites, puis en proposant une solution adaptée. La mise en œuvre de mécanismes tels que l'authentification centralisée, la segmentation du réseau et l'utilisation d'un contrôleur WLAN a permis de renforcer significativement la sécurité globale du réseau.

Ce travail nous a également fait prendre conscience que la sécurité est un processus continu et non une solution définitive. Les menaces évoluent constamment, ce qui oblige les administrateurs à rester vigilants et à adapter en permanence leurs stratégies de protection.

En conclusion, ce mémoire a été une expérience à la fois technique et formatrice, qui a permis de consolider nos connaissances tout en développant une approche concrète de la sécurisation des réseaux sans fil.

Bibliographie

Bibliographie

◆ Livres et mémoires

[2] Marcel MUSWILA. ≪ Mise en place d'une politique d'accès à un réseau sans fil avec l'authentification basée sur la norme 802.1x ≫, Mémoire licence. Université Notre-Dame du Kasayi - 2019.

[3] K. BELHADJ & A. ABID. ≪ ETUDE et réalisation d'un réseau WiFi hotspot dans le service public ≫, Mémoire ingénieur en Electronique. Université Mouloud Mammeri, Tizi Ouazou ,2012.

[4] GIGAMEDIA. (2024). Surfer l'ère du Wi-Fi : évolutions & perspectives de la connectivité sans fil. Livre blanc, GIGAMEDIA.

[7], [8] Didi née Lahfa Fedoua. « Qualité de Service dans les réseaux locaux sans fil de type IEEE 802.11 », Thèse doctorat. Université Abou Bekr Belkaid.2010.

[9] Dufresne Loïc. « Quel est l'effet de la QoS sur des petits réseaux de labo ?», Thèse doctorat. Haute école d'ingénierie et d'architecture fribourg.2018.

[11] S. Dieta & M. Yaro. ≪ Mise en place d'un réseau Wi-Fi éxpérimental sécurisé ≫, Mémoire Ingenieur en télécommunicatione. Institut de Télecommunication d'Oran - 2006.

[17] F. Lemainque, « Tout sur les Réseaux sans fil », DUNOD 2009.

[18] N. BATTAT & F. MIMOUNE. ≪ Les technologies sans fil Le Wi-Fi et la Sécurité ≫, Mémoire licence en informatique. Université Abderrahmane Mira - 2007.

[19] N. BENCHERIF & S. STAILI ≪ Sécurité dans les réseaux sans fil (Wi-Fi) ≫, Mémoire master Génie électrique. Université Abdelhamid Ibn Badis Mostaganem- 2024.

[23], [24] BORDÈRES, Serge. Authentification réseau avec Radius : 802.1 x, EAP, FreeRadius.Editions Eyrolles, 2006.

[25] R. HAMADOU & S. BEREBERE. ≪ Sécurisation d'un Wi-Fi via un serveur RADIUS ≫, Mémoire licence professionnelles en Génie électrique. Université Africaine de Technologie et de Management- BENIN. 2018.

[27] G. Aurélien, WiFi Professionnel-3e édition- : La norme 802.11, le déploiement, la sécurité, Dunod, 2009.

[29] Marcel MUSWILA. ≪ Mise en place d'une politique d'accès à un réseau sans fil avec l'authentification basée sur la norme 802.1x ≫, Mémoire licence. Université Notre-Dame du Kasayi - 2019.

[30] A. BENNAI et A. BOUAM, « Ethical Hacking : Étude et réalisation de tests de vulnérabilité », Mémoire de Master en Informatique, Université Abderrahmane Mira Béjaïa, 2017.

[36] Programme Cisco Networking Academy ; Notions de base sur la commutation, le routage et le sans-fil v7.0 ; Contenu Pédagogique de l'instructeur.

◆ Articles web

[1] https://web.maths.unsw.edu.au/~lafaye/CCM/wireless/wlintro.htm

[5] https://www.cisco.com/c/fr_ca/products/wireless/what-is-wifi.html

[6] https://cisco.ofppt.info/ccna1/course/module4/4.2.4.4/4.2.4.4.html

[10], [12] https://fr.wikipedia.org/wiki/Wi-Fi

[13] https://web.maths.unsw.edu.au/~lafaye/CCM/wifi/wifimodes.htm

[14] https://www.come-star.com/fr/blog/wireless-ap-vs-wireless-router/

[15] https://www.cisco.com/c/fr_ca/solutions/small-business/resource-center/networking/what-is-access-point.html

[16] https://www.netacad.com/fr/

[20] https://www.avg.com/fr/signal/wep-wpa-or-wpa2/

[21] https://www.fortinet.com/fr/resources/cyberglossary/service-set-identifier-ssid/

[22] https://www.ionos.fr/digitalguide/serveur/securite/securite-wifi-mesures-de-protectionpourvotre-reseau/

[26] https://www.pandasecurity.com/fr/mediacenter/wardriving/

[31] https://www.kaspersky.fr/resource-center/definitions/what-is-session-hijacking/

[32] https://www.cloudflare.com/fr-fr/learning/ddos/glossary/denial-of-service/

[33], [34] https://www.pandasecurity.com/fr/mediacenter/attaque-man-in-the-middle/

[35] https://www.itrust.fr/focus-attaque-mitm-evil-twin/

[37], [38], [39], [40] https://crtaa.dz/

[41] https://www.netacad.com/fr/cisco-packet-tracer

Résumé

Les réseaux sans fil, notamment le Wi-Fi, sont aujourd'hui largement utilisés en raison de leur flexibilité et de leur facilité de déploiement. Cependant, leur nature ouverte les rend vulnérables à diverses menaces de sécurité. Ce mémoire vise à étudier les mécanismes de sécurisation des réseaux Wi-Fi et à proposer une solution adaptée à un environnement réel. Une première partie théorique présente les concepts des réseaux sans fil, les normes IEEE 802.11 ainsi que les protocoles de sécurité tels que WEP, WPA, WPA2 et WPA3, en mettant en évidence leurs limites.

La partie pratique, réalisée au sein du CRTAA, a consisté à analyser l'infrastructure existante puis à mettre en œuvre une solution basée sur l'authentification centralisée, la segmentation par VLAN et l'utilisation d'un contrôleur WLAN, simulée sous Cisco Packet Tracer.Les résultats montrent qu'une approche combinant plusieurs mécanismes de sécurité permet de renforcer efficacement la protection des réseaux Wi-Fi.

Mots-clés : Réseaux sans fil, Wi-Fi, sécurité, IEEE 802.11, WPA2, WPA3, RADIUS, VLAN, attaques réseau, Cisco Packet Tracer.