INSTITUT UNIVERSITAIRE DES SCIENCES

(IUS)

Faculté des Sciences et Technologies

(FST)

Projet – Réseaux I

Sujet : « *L'authentification et la gestion des identités dans les réseaux sans fil sécurisés.* »

Elaboré par :

Kendy BICHOTTE

Frantzdy ALEXANDRE

Niveau :

L3

Sous la direction du professeur :

Ismaël SAINT-AMOUR

Date : Janvier 2026

Table des matières

Introduction

À une époque où communication et technologie sont les maîtres mots de notre société, nous ne pouvons douter que l'avenir des réseaux informatiques soit de grandir et de se développer. Cet avenir est pour une bonne part liée aux techniques et aux supports de communication utilisés dans les réseaux. À l'heure actuelle, la tendance est à la transmission numérique et à l'utilisation de la communication sans fil. De plus, la technologie actuelle permet d'accroître les volumes et les vitesses de transfert des données tout en diminuant les coûts. Les interconnexions de réseaux sont innombrables et pratiquement tous les réseaux se trouvent aujourd'hui imbriqués les uns dans les autres. En particulier, Internet est le réseau fédérateur des réseaux de la planète. L'intégration des réseaux locaux et grande distance dans le système d'information et de communication de l'entreprise a conduit au concept de *réseau d'entreprise*, dans lequel l'utilisateur a accès à toutes les ressources informatiques, grâce à une réelle distribution des applications.

Pendant longtemps, les réseaux sans fils traditionnels (TWK : Traditional Wireless Networks) tel que les réseaux cellulaires de téléphonie (GSM : Global System for Mobile Communications) et UTMS (Universal Mobile Telecommunications System) étaient l'exemple prédominant des réseaux de télécommunication conçus pour transmettre la voix. Fin des années 90, une nouvelle technologie sans fil surgit : les réseaux locaux sans fil (Wireless Area Network, WLAN), qui étaient adaptés aux transmissions des données. De nos jours cette technologie est en plein essor. En effet les ordinateurs portables, un nombre croissant de téléphones mobiles, les consoles de jeux et même des véhicules sont dotés de cette technologie ainsi que les fournisseurs d'accès à internet qui proposent des solutions domestiques sans fil. En raison de la généralisation des ordinateurs portables, des tablettes et des smartphones cela veut dire tout simplement que les connexions wifi jouent un rôle central dans la connectivité, l'innovation et la productivité des PME, des institutions gouvernementales et publiques, des institutions privées, des centres d'enseignement, des centres industriels.

Avec l'avènement de la 5G en 2019, les réseaux sans fil se développent rapidement tant en disponibilité qu'en cas d'utilisation. Elle est considérée comme une technologie de rupture en raison des changements qu'elle promet d'apporter au même titre que l'intelligence artificielle (AI), l'internet des objets (IoT), le Machine Learning (ML). Grâce aux progrès technologiques, la 5G est reconnue pour son potentiel à transformer de nombreux secteurs, notamment en permettant de transférer de grandes quantités de données de manière rapide et sécurisée entre des appareils connectés, à des vitesses inédites. Depuis l'invention du haut débit mobile et sa généralisation dans tous les aspects de la vie professionnelle et privée, le volume de données généré par les réseaux et les appareils mobiles a augmenté de manière exponentielle.

L'homme, de nature paresseux, est un animal technique et rationnel, cherchant toujours à économiser du temps en créant ou en innovant pour faciliter sa vie et celle des autres. Avec cette curiosité accrue d'apprendre et d'expérimenter, a ouvert la porte à une montée technologique de partages des ressources, de communication et autres au sein de toute entreprise qui veut rester au top dans ce monde concurrentiel. Toutefois, cette facilité de connectivité et d'exploitation des ressources, présente aussi des dangers quant à la sécurité notamment liée à l'intrusion et à la perte de données. En ce sens, l'authentification et la gestion de tout utilisateur ou équipement du réseau mérite d'être traitées avec la plus grande importance possible. Que ce soit dans la mise en place d'une politique de sécurité, d'un contrôle d'accès ou en définissant le rôle, le statut de tout utilisateur et autre.

Dans ce projet, les différents types de réseaux sans fil, les normes, les protocoles de sécurité, ainsi que les moyens de gestion des identités seront présentés pour comprendre combien les réseaux wifi bien qu'ils soient indispensables dans la vie au quotidien montre des risques de sécurité énormes où dans un environnement le nombre d'utilisateurs peut augmenter en un clin d'œil.

Listes des abréviations

Abréviations	Significations
AAA	Authentication, Authorization, Accounting
IA	Artificial Intelligence
AP	Access Point
BSS	Basic Service Set
BLR	Boucle Locale Radio
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data rates for GSM Evolution
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
HIPERLAN	High Performance Radio Local Area Network
IAM	Identity and Access Management

IAPP	Inter-Access Point Protocol
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IOS	Internetwork Operating System (Cisco)
IR	Infrared
IS-95	Interim Standard 95 (CDMA-based mobile network)
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MITM	Man In The Middle
ML	Machine Learning
OFDM	Orthogonal Frequency Division Multiplexing
PAP	Password Authentication Protocol
PCMCIA	Personal Computer Memory Card International Association
PHY	Physical Layer
P2P	Peer-to-Peer
RFID	Radio Frequency Identificatio
SSID	Service Set Identifier
TWK	Traditional Wireless Networks
UWB	Ultra Wide Band
UMTS	Universal Mobile Telecommunications System

VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
ZIGBEE	Protocole de communication sans fil basse consommation

Chapitre I- Réseau mobiles et réseaux sans fil

Les systèmes de communications sans fil- tels que les réseaux cellulaires mobiles, réseaux locaux sans fil (ex. WiFi), réseaux de capteurs, réseaux véhiculaires, et réseaux Bluetooth- sont aujourd'hui incontestablement omniprésents dans notre vie. Avec l'utilisation massive de l'Internet en utilisant des dispositifs sans fil, l'arrivée de l'Internet des objets (IoT pour Internet of Things en anglais) ainsi que l'incontrôlable augmentation du nombre de dispositifs de communication sans fil, de la diversité de leurs applications, l'apparition de nouvelles applications multimédia, et les nouvelles exigences de capacité élevée et/ou de qualité de service, une connaissance approfondie des systèmes et réseaux de communications sans fil, devient nécessaire pour tous les scientifiques.

L'objectif principal des réseaux mobiles est de permettre à leurs utilisateurs de se déplacer tout en restant connecté dans une zone géographique plus ou moins étendu (zone de couverture), et d'accéder au réseau de n'importe où et à n'importe quel moment (communication ubique). Les environnements sans fil offrent une grande flexibilité d'emploi. En particulier, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible.

I.2-Réseaux de mobiles et réseaux sans fil

Les termes mobiles et sans fil sont souvent utilisés pour décrire les systèmes existants, tels que le GSM, IS-95, IEEE 802.11, Bluetooth, et autres. Toutefois, il est important de distinguer les deux catégories de réseaux que recoupent les concepts de mobile et de sans fil, de façon à éviter toute confusion.

Les réseaux de mobiles : Un utilisateur mobile est défini théoriquement comme un utilisateur capable de communiquer à l'extérieur de son réseau d'abonnement tout en conservant une même adresse. Un réseau mobile permet à tout appareil connecté, notamment les smartphones et les tablettes, d'établir des communications avec d'autres appareils. Un réseau mobile offre une grande flexibilité tout en permettant la communication même étant en mouvement.

Les réseaux sans fil : Le concept de sans fil est étroitement associé au support de transmission. Un système est dit sans fil s'il propose un service de communication

totalement indépendant de prises murales. Dans cette configuration, d'autres moyens d'accès sont exploités, tels que les ondes radio, l'infrarouge ou les ondes hertziennes. Un réseau sans fil (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

I.3- Réseaux sans fil vs réseaux filaire

Un réseau sans fil permet aux appareils de rester connectés au réseau sans câbles encombrants. Les points d'accès amplifient les signaux Wi-Fi, de sorte qu'un appareil peut être toujours connecté au réseau bien qu'il soit éloigné d'un routeur.

Un réseau filaire utilise des câbles pour connecter des appareils tels que des ordinateurs portables ou de bureau à Internet ou à un autre réseau. Le principal inconvénient est que votre appareil doit être attaché à un routeur.

Auparavant, on pensait que les réseaux filaires étaient plus rapides et plus sécurisés que les réseaux sans fil. Toutefois, les améliorations continuelles apportées aux technologies de réseau sans fil, telles que le standard Wi-Fi 6, ont réduit les différences de vitesse et de sécurité entre les réseaux filaires et sans fil.

I.4-Réseau sans fil et réseau satellitaire

Les réseaux satellites sont des systèmes de communication qui utilisent des satellites en orbite autour de la Terre pour transmettre des données entre différents points géographiques. Ces réseaux offrent une couverture globale, rendant possible l'accès à Internet et aux services de communication dans des zones éloignées ou peu desservies. Grâce à leurs capacités de transmission rapide et stable, ils jouent un rôle crucial dans les télécommunications modernes, la navigation et la surveillance environnementale.

Un réseau sans fil utilise des radiofréquences (ondes électro-magnétiques) comme porteuse d'un signal. Une bonne connexion sans fil (par exemple, Wi-Fi 6 avec un signal fort ou cellulaire 5G) sera presque toujours plus rapide qu'une connexion satellite. Cependant, si une bonne connexion filaire ou sans fil n'est pas une option, le satellite fournit une connectivité là où les autres options échouent.

I.5- Avantages et inconvénients des réseaux sans fil

A-Les avantages des réseaux sans fil

1. **Portabilité** : avec seulement un ordinateur portable, ou un smartphone suffisent pour se connecter ;
2. **Mobilité** : l'utilisateur n'est pas obligé de rester dans un lieu fixe, par exemple à son bureau, il peut se déplacer ;
3. **Facilité** : moins encombrant car pas de fil ou de câble, il peut se connecter facilement ;
4. **Productivité** : aide l'utilisateur à faire son travail et peut collaborer facilement ;
5. **Extensibilité/scalabilité/évolutivité** : peut facilement être déployé avec des équipements existants tandis que pour un réseau filaire, il faut du câble supplémentaire ;
6. **Sécurité** : offre des protections de sécurités robustes grâce aux avancées des réseaux sans fil ;
7. **Coût** : moins couteux à mettre en place qu'un réseau filaire.

B-Les inconvénients des réseaux sans fil

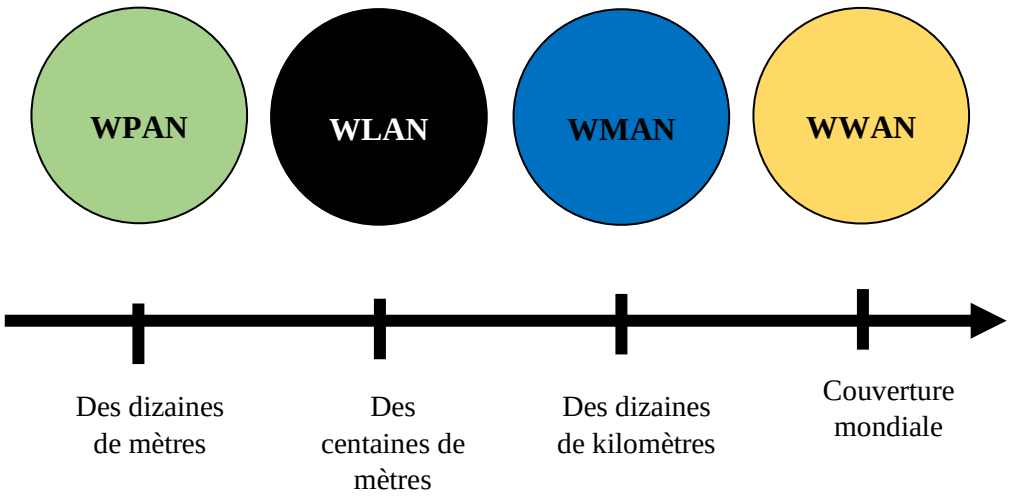
1. **Energie** : les applications relatives aux réseaux sans fils ont un caractère nomade et tirent leur autonomie de batterie, émission et réception des informations consomment beaucoup d'énergie ;
2. **Débit** : souvent plus faible qu'un réseau filaire ;
3. **Distance** : atténuation rapide du signal qui induit l'impossibilité pour un émetteur de détecter une collision ;
4. **Interférence** (latence) : Les transmissions radios ne sont pas isolées, et le nombre de canaux disponibles est limité, ce qui force le partage. Les interférences peuvent être de natures diverses à savoir des émetteurs travaillant à des fréquences trop proches ; des bruits parasites dus à l'environnement ; des phénomènes d'atténuation, de réflexion et de chemins multiples dus à l'environnement

5. **Faible Sécurité** : il est facile d'espionner passivement un canal radio, il y a un risque de piratage et de perte de données ;
6. **Portée limitée** : distance entre l'appareil et le routeur.

I.6- Classification des réseaux sans fil

On distingue habituellement plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) ou selon le mode opératoire.

I.6.1- Classification des réseaux en fonction de la taille



Une classification des réseaux sans fil selon leur taille

a) **Les WPAN (Wireless Personal Area Networks)**

Nous retrouvons les réseaux sans fil à l'échelle humaine dont la portée maximale est limitée à quelques dizaines de mètres autour de l'usager (bureaux, salles de conférence...). Nous y trouvons les standards tels que le Bluetooth, l'Ultra Wide Band (UWB), ZIGBEE, RFID et HomeRF ;

b) Les WLAN (Wireless Local Area Networks)

Nous avons des réseaux locaux sans fil dont la portée va jusqu'à 500 m, pour les applications couvrant un campus, un bâtiment, un aéroport, un hôpital, etc. On y trouve les standards tels que le Wi-Fi (Wireless Fidelity) et les HIPERLAN ;

c) Les WMAN (Wireless Metropolitan Area Networks)

Plus connus sous le nom de Boucle Locale Radio (BLR), ce type de réseau utilise le même matériel que celui qui est nécessaire pour constituer un WLAN mais peut couvrir une plus grande zone de la taille d'une ville avec une portée pouvant aller jusqu'à 50 Km. C'est dans cette catégorie que l'on classe le WiMAX et les HIPERMAN ;

d) Les WWAN (Wireless Wide Area Networks)

C'est la catégorie de réseaux cellulaires mobiles dont la zone de couverture est très large, à l'échelle mondiale. Dans cette catégorie, on peut citer le GSM et ses évolutions (GPRS, EDGE), le CDMA et l'UMTS.

I.6.2- Classification des réseaux suivant le mode opératoire

En réseau sans fil, nous retrouvons deux modes opératoires :

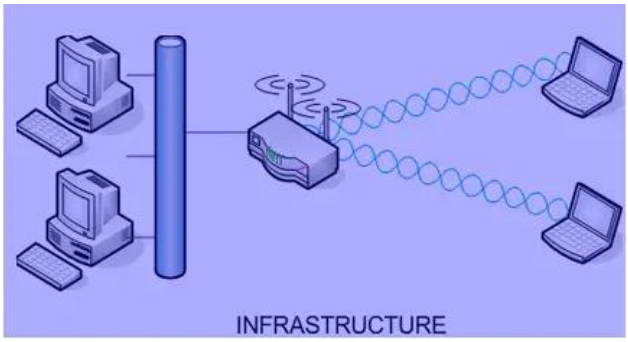
A. Le mode avec infrastructure

B. Le mode sans infrastructure (Ad hoc)

A. Le mode infrastructure

En mode infrastructure, le réseau est composé de plusieurs cellules et chacune d'elles comprend une station de base (ou un point d'accès) par laquelle toutes les autres stations de la cellule accèdent au réseau intra et intercellulaire. Les différents points d'accès sont reliés entre eux et/ou au réseau Internet à l'aide d'une

technologie supplémentaire qui peut être filaire ou hertzienne. Dans cette catégorie, on trouve les réseaux WLAN (Wi-Fi), WMAN (WiMAX) et WWAN (GSM).



Dans le mode infrastructure, nous retrouvons deux sous-mode :

- Le mode BSS (Basic Service Set), où l'on utilise qu'une seule borne d'accès ;
- Le mode ESS (Extended Service Set), où l'on utilise au moins deux bornes d'accès. Dans ce mode, le client peut faire du roaming en passant d'une borne à une autre sans couper la communication réseau.

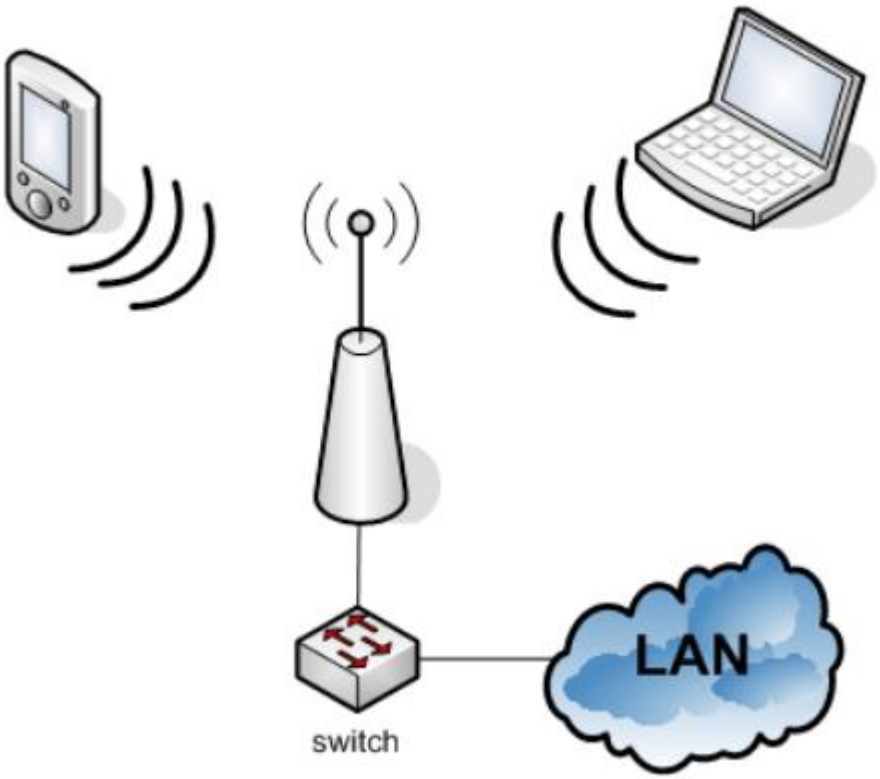
Borne d'accès lourde ou légère

Que vous soyez en mode BSS (Basic Service Set) ou ESS (Extended Service Set), vous avez deux possibilités pour la configuration des bornes d'accès :

a) Configurer la borne en mode **lourd** ou « **standalone** »

b) Configurer la borne en mode **léger** ou « **lightweight** »

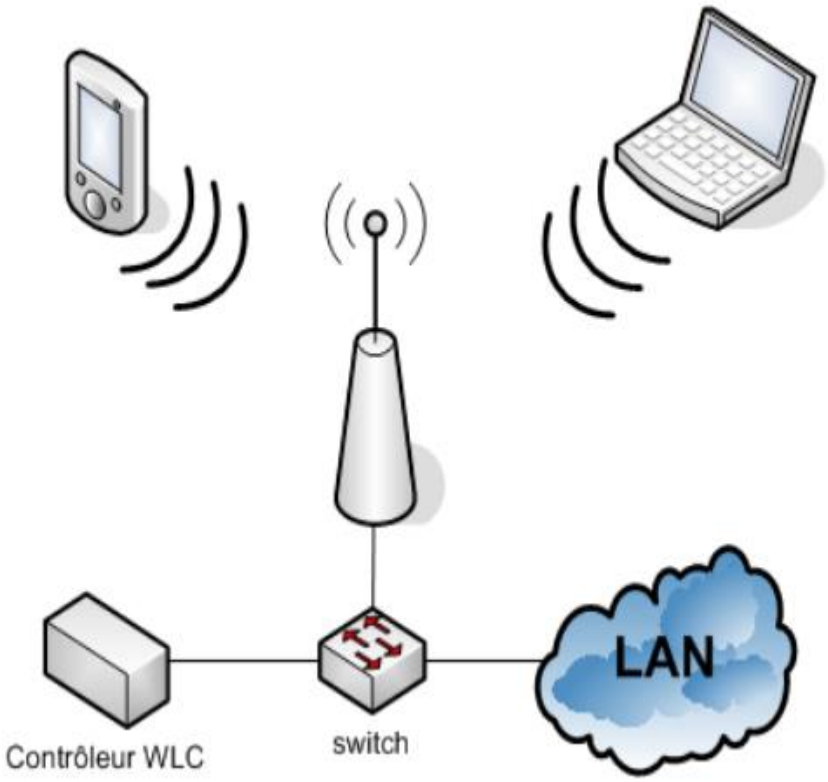
a) Borne lourde ou standalone



Dispositif de réseau pouvant fonctionner de manière indépendante

- Les premières bornes d'accès étaient en mode lourd/standalone
- Gère la commutation
- Au sein de leur système d'exploitation se trouvait toute la configuration (comme un IOS pour un switch ou routeur)
- Dispose de ports WAN et LAN
- Peut prendre en charge des fonctions de sécurité telles que le serveur DHCP, DNS, clonage d'adresses MAC, accès VPN et pare-feu.
- Connexion en console ou telnet/ssh/http à la borne pour lui configurer différents paramètres comme le SSID, le canal à utiliser, la puissance.

b) Borne légère ou lightweight



- L’émission/réception du trafic radio
- La gestion des accès (MAC)
- Le chiffrement du trafic
- Pas de routage, DNS, serveur DHCP et de nombreuses autres fonctions de chargement et ne conserve que la partie accès sans fil
- Reçoit/envoi des trames vers un boitier intelligent, le WLC (Wireless LAN Controller). *Note : les points d’accès légers se gèrent uniquement avec un contrôleur (WLC)*

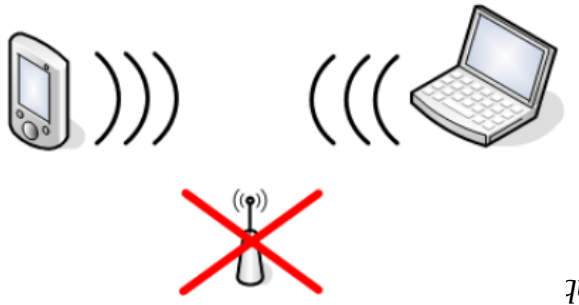
Fonctionnement

1. La borne démarre électriquement
2. Son interface filaire va envoyer une requête DHCP pour récupérer une adresse IP
3. Une fois reçue, elle va contacter son WLC

4. Le WLC va lui envoyer sa configuration minimale avec tous les paramètres au bon fonctionnement (SSID, puissance, canal…)
5. Une fois configurée, la borne envoi tout le trafic des clients WiFi au contrôleur qui se chargera de les envoyer vers les bonnes destinations

B. Le mode Ad hoc

En mode ad hoc, il n'y a pas de point d'accès fixe, l'infrastructure n'est composée que des stations elles-mêmes, ces dernières jouant à la fois le rôle de terminaux et de routeurs pour permettre le passage de l'information d'un terminal vers un autre sans que ces terminaux soient reliés directement ; on parle aussi de communication **point à point** (**point-to-point / P2P**). La caractéristique essentielle d'un réseau ad-hoc est l'existence de tables de routage dynamiques dans chaque nœud. C'est la catégorie des réseaux WPAN tels que le Bluetooth. Ce mode peut être aussi appelé IBSS (Independent Basic Service Set).



Les images montrent le mode opératoire *quent entre eux sans point d'accès (AP).*

Chapitre II- Réseaux Wi-Fi

Le Wi-Fi (contraction de **Wireless Fidelity**) 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. Le WI-FI répond à la norme IEEE 802.11. La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Un réseau Wifi est en réalité un réseau répondant à la norme 802.11. Ainsi, un réseau wifi permet de relier plusieurs appareils informatiques par ondes radios afin de favoriser le partage des ressources ou la transmission des données.

La connectivité Internet est rendue possible grâce à un routeur sans fil. Dans ce chapitre, je vais mettre l'accent sur la norme 802.11 comprenant les topologies et les couches, les équipements wifi.

II.1-Normes et différents types de wifi

Les réseaux WiFi se déclinent en plusieurs types, chacun offrant des caractéristiques distinctes adaptées à divers besoins. Chaque nouvelle génération de Wi-Fi apporte des améliorations en termes de **vitesse**, de **fiabilité**, de **sécurité** et de **capacité**, permettant ainsi de mieux répondre aux besoins croissants des utilisateurs en matière de connectivité sans fil. Sur le plan technique, la norme IEEE 802.11 définit les protocoles qui permettent les communications avec les dispositifs dotés du Wi-Fi, y compris les routeurs sans fil et les points d'accès sans fil.

Les différentes versions du Wi-Fi ont longtemps porté des noms compliqués via **la norme 802.11**, mais, pour tenter de dissiper toute confusion, la Wi-Fi Alliance a renommé les versions actuelles, passées et futures du Wi-Fi.

Date	Standard IEEE 802.11	Génération	Bande de fréquence	Vitesse négociée
1997	IEEE 802.11		2,4GHz	2Mbps
1999	IEEE 802.11b	Wifi 1	2,4GHz	11Mbps
1999	IEEE 802.11a	Wifi 2	5GHz	54Mbps
2003	IEEE 802.11g	Wifi 3	2,4GHz	54Mbps
2009	IEEE 802.11n	Wifi 4	2,4GHz (5GHz)	150Mbps
2014	IEEE 802.11ac (vague 1)	Wifi 5	5GHz	866Mbps
2016	IEEE 802.11ac (vague 2)	Wifi 5	5GHz	1,73Gbps
2019	IEEE 802.11ax	Wifi 6	2,4GHz-5GHz	2,4Gbps
2024	IEEE 802.11be	Wifi 7	2,4GHz-5GHz-6GHz	46 Gbps

II.2-Caractéristiques de l'IEEE 802.11

La norme 802.11 fournit des fonctionnalités des couches MAC et PHY pour une connectivité sans fils des postes fixes, portables et mobiles, se déplaçant à une vitesse de piéton ou de véhicule dans une zone locale. Elle prend en compte les différences suivantes qui existent entre un réseau filaire et un WLAN :

- **Gestion de l'alimentation :** La plupart des interfaces réseaux sans fils se trouvent sous forme de cartes PCMCIA, qui permet aux équipements mobiles et portables d'avoir un accès aux WLAN. Cependant, ces dispositifs doivent souvent dépendre des batteries afin d'alimenter leurs composantes électroniques. L'un des objectifs était de trouver des solutions pour économiser l'alimentation par batterie, en introduisant des techniques permettant aux cartes réseaux sans fil, de passer au mode de veille périodiquement quand il n'y pas de transmission.
- **Bande passante** : Pour optimiser l'utilisation de la bande passante, 802.11 offre des mécanismes de compression des données transmises favorisant une meilleure exploitation de la bande passante disponible.

- **Sécurité** : Le groupe de travail 802.11 travaillait en coopération avec le comité des standards 802.10 responsable du développement des mécanismes de sécurités pour toute la série 802.
- **Adressage** : La topologie d'un réseau sans fil est dynamique. Autrement dit, l'adresse de destination ne correspond pas toujours à l'emplacement de la destination. Ceci soulève un problème de routage des paquets à travers le réseau vers la destination. La norme 802.11f fournit le protocole Inter Access Point Protocol (IAPP) pour remédier à ce problème.

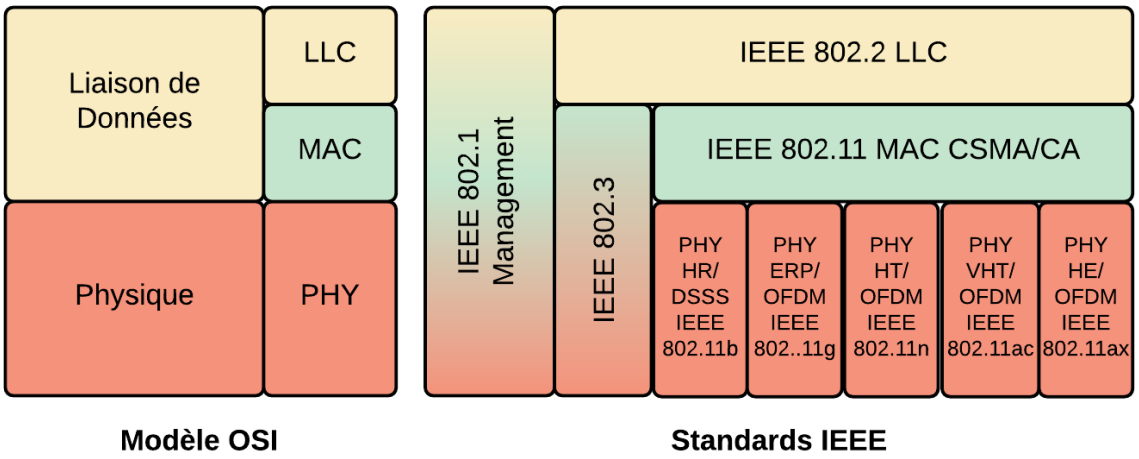
II.3-Architecture du réseau 802.11

Du point de vue de l'architecture, 802.11 définit deux modes d'opération : le mode infrastructure BSS (Basic Service Set) et le mode ad-hoc IBSS (Independant Basic Service Set). La topologie du mode ad-hoc est très simple et l'ensemble des stations communique directement par paires, sans aucune fonction de relais de messages. Le mode infrastructure est beaucoup plus répandu que le mode ad-hoc et il définit un élément central, le point d'accès (AP).

Quoiqu'un LAN sans fil puisse être constitué par une seule cellule, avec un seul point d'accès, (et peut également travailler sans point d'accès), la plupart des installations seront constituées par plusieurs cellules, où les points d'accès sont reliés ensemble par un système de distribution (DS). Ce DS est dans la majorité des cas un LAN Ethernet. Les communications entre points d'accès peuvent aussi être hertziennes, on parle dans ce cas de WDS (Wireless DS). Généralement les réseaux sans fil 802.11 sont déployés en regroupant plusieurs points d'accès rapprochés, pour former une zone de couverture étendue composée des cellules de couverture contiguës. Ce réseau étendu est appelé ESS (Extended Service Set) et les points d'accès qu'il contient coopèrent entre eux pour acheminer les messages entre les cellules desservies.

II.4-Modèle en couche

La norme 802.11 couvre les deux premières couches du modèle OSI à savoir « Physique » (L1) et « Liaison de données » (L2).

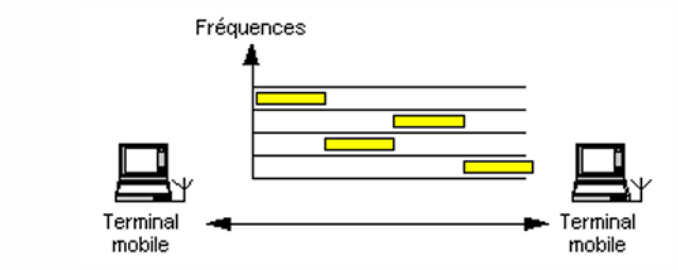


II.4.1-La couche physique

La norme IEEE 802.11 définit Initialement, trois techniques de transmission (FHSS, DSSS et IR), auxquelles 802.11a a ajouté OFDM :

---FHSS: Frequency Hoping Spread Spectrum

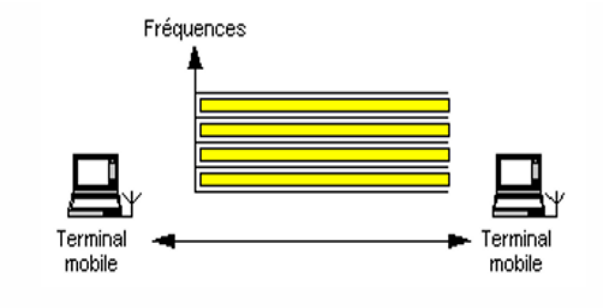
La plupart des interférences nuisibles aux transmissions radio n'agissent que sur des bandes de fréquence assez étroites. Notre signal sera fortement dégradé si des interférences ont lieu au moment où l'on transmet. Une technique pour protéger notre signal consiste à changer régulièrement de fréquence. Certes que les paquets envoyés sur la bande perturbée seront affectés, toutefois ils ne représenteront plus qu'une minorité des transmissions et leur retransmission sera moins couteuse. L'émetteur et le récepteur doivent connaitre préalablement le séquencement des sauts de fréquence.



---DSSS: Direct Sequence Spread Spectrum

Toujours pour lutter contre les interférences importantes qui n'affectent que des plages de fréquences assez étroites, il y a la technique de l'étalement de spectre. Des manipulations sur le signal vont le faire occuper un spectre plus large. À la réception,

une manipulation inverse est effectuée. Cette technique est moins sensible aux interférences dues aux fréquences parasites à faible largeur spectrale.



---IR Infra Red :

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission des données. Cette transmission se fait de façon unidirectionnelle. Il est possible grâce à la technologie infrarouge qui offre un niveau de sécurité plus élevé d'obtenir des débits allant de 1 à 2 Mbit/s par l'utilisation d'une modulation appelée Pulse Position Modulation (PPM). Cette dernière consiste à transmettre des impulsions à amplitude constante et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de 16-PPM tandis que le celui de 2 Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles.

---OFDM : Orthogonal Frequency Division Multiplexing

Lorsqu'un signal radio est émis, l'onde va se diviser sur les divers obstacles rencontrés. À l'arrivée plusieurs chemins pourront avoir été empruntés, et leur temps de parcours n'étant forcément les mêmes ; ainsi les multiples réfractions entre les réfractions/réflexions d'une même onde vont interférer entre elles. Plus la différence de temps de parcours sera grands vis-à-vis de la durée de transmission totale du symbole, plus les chances que les réflexions/réfractions de symboles consécutifs se chevauchent. Ceci est appelé le problème des chemins multiples. OFDM propose

d'utiliser des symboles plus longs mais envoyés en parallèle. C'est une méthode qui préconise qu'en présence de chemins multiples, l'utilisation de plusieurs canaux lents donne de meilleurs résultats qu'un seul canal très rapide.

II.4.2-La couche Liaison de données

Réaliser un acheminement sans erreur de blocs d'informations sur la liaison physique est l'objectif de la couche liaison de données. Elle attache des en-têtes et des caractères aux paquets de données à transmettre afin d'effectuer une transmission correcte. Les messages communiqués sont appelés MPDU (MAC Protocol Data Unit) ou bien trames MAC. Par la suite, les messages seront encapsulés dans des trames de niveau physique appelées PLCP-PDU (Physical Level Control Protocol-PDU). La couche de liaison de données contient essentiellement deux sous-couches :

1. **La sous-couche LLC (Logical Link Control)** : Elle représente une partie de la couche de liaison de données, elle est indépendante des mécanismes d'accès au support physique. Elle présente des caractéristiques de fiabilité grâce au séquencement et à la retransmission des données en cas de détection d'erreurs.
2. **La sous-couche MAC (Medium Access Control)** : Elle est responsable de la procédure d'allocation du canal, l'adressage de l'unité de fragmentation du processus inverse à savoir le réassemblage. Elle effectue des fonctionnalités essentielles pour la retransmission en cas de perte ou de trame erronée, l'envoi d'accusé de réception et la fragmentation des données, la réalisation d'une transmission correcte point à point à savoir la détection d'erreur. Ainsi, deux modes d'accès au medium au niveau MAC sont définis par la norme IEEE 802.11 : mode distribué (DCF) et mode centralisé (PCF).

2.1- DCF (Distributed Coordination Function) : c'est un mode qui peut être utilisé par tous les mobiles, et qui permettent un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès. Il peut être aussi utilisé lorsqu'il n'y a pas des stations de base (mode ad hoc) que lorsqu'il y en a (mode infrastructure).

2.2-PCF (Point Coordination Function) : c'est un mode dans lequel les stations de base (ou AP) ont la charge de la gestion de l'accès au canal dans leur zone de couverture pour les mobiles qui leur sont attachés.

II.5-Les équipements wifi

Il existe différents types d'équipements pour la mise en place d'un réseau Wi-Fi :

1. Les adaptateurs ou cartes d'accès : ce sont des cartes réseaux permettant de se connecter à un réseau WiFi. Ces adapteurs sont disponibles dans de nombreux formats (carte PCMCIA, carte PCI, adaptateur USB, carte Compact Flash SD). On appelle station tout équipement possédant une telle carte.



2. Les bornes d'accès ou AP (Access Point). Elles se comportent comme des routeurs et peuvent être reliées au réseau filaire ou à une connexion ADSL.



3. Les ponts (bridge) : ils permettent de relier deux réseaux entre eux.


4. Les antennes : elles servent à amplifier le signal et se connectent aux points d'accès.
    - Antennes omnidirectionnelles
    - Antenne Parabole
    - Antennes Patch
    - Antenne Yagi




Chapitre III- Sécurité dans les réseaux Wi-Fi

Le Wi-Fi bien qu'il soit très pratique, comporte son lot de problèmes, de vulnérabilités. Des attaquants peuvent intercepter vos données, perturber les services et même prendre le contrôle de tout équipement connecté sur un réseau. La cybersécurité est devenue un enjeu majeur dans notre société, dans toute entreprise où nous sommes connectés pour exploiter ou profiter des ressources d'un réseau. De cette façon, il est crucial de comprendre les vulnérabilités qui représentent les faiblesses exploitables dans un système mais aussi les moyens ou méthodes et les protocoles à utiliser pour contrecarrer toute attaque que ce soit de l'intrusion, de la perte ou vol de données, de l'interruption de services, de l'accès non-autorisé.

Objectifs principaux de la sécurité réseau

La sécurité des réseaux est devenue une préoccupation centrale avec l'expansion d'internet et l'usage croissant de systèmes connectés. L'objectif est de garantir la disponibilité, l'intégrité, et la confidentialité des données. Ce chapitre sera axé sur la sécurité, les attaques dans un réseau Wi-Fi, les protocoles d'authentification et la gestion des identités répartis en plusieurs sections.

Section A- Les attaques d'un réseau wifi

Les malwares /virus/ cheval de trois/ vers

Ce sont des programmes malveillants utilisés par les attaquants pour voler données, ou même rendre dysfonctionnel le réseau.

L'Homme du milieu (MITM :Man in the middle)

L'attaquant espionne la conversation, le trafic des paquets en déviant toutes communications entre deux ordinateurs, pour les faire transiter par sa machine, et peut même y jeter du code malveillant pour déstabiliser le réseau.

Le War driving

Le War Driving (la guerre en voiture) est une forme de piratage qui consiste à se promener en voiture avec une antenne Wi-Fi et à repérer la position et les caractéristiques de tous les points d'accès disponibles.

Cette pratique permet d'exploiter les endroits où se trouvent les réseaux afin de réaliser toute catégorie d'attaques contre le Wi-Fi : espionnage, intrusion, modification de messages, déni de services.

Le Deni de service (DoS/DDoS)

Dans ce type d'attaques qui consiste à rendre un service, un réseau indisponible ; l'attaquant peut rendre un serveur saturé en le bombardant d'un trafic excessif de données ou en brouillant les signaux dans un réseau sans fil pour empêcher l'accès à internet.

Le reniflement (Sniffing)

Le « reniflement » (sniffing) désigne la surveillance du trafic Internet en temps réel. Les renifleurs sont des programmes ou appareils utilisés par les attaquants pour espionner l'activité du réseau, collecter des informations et exploiter les vulnérabilités. Ainsi on y retrouve des Sniffeurs de paquets, de wifi pour ne citer que ceux-là.

Le phishing (l'hameçonnage) / ingénierie sociale

Par cette forme d'attaque, les attaquants incitent l'utilisateur à fournir des informations personnelles sensibles ou confidentielles souvent par voie électronique (email) qui seront ensuite utilisées à des fins néfastes (*pour voler des données, entrer dans le réseau, et autres*).

L'intrusion et le piratage

L'attaquant s'introduit dans le système, dans le réseau sans autorisation (accès non autorisé) pour voler, pour supprimer ou modifier des informations.

Section B-Cryptographie et services de sécurité

La cryptographie est une science basée sur les mathématiques pour crypter et décrypter des informations considérées comme confidentielles pour enfin les stocker et les transmettre d'une manière sécurisée.

Le cryptage appelé aussi chiffrement est la fonction permettant de transformer un texte en clair et lisible en un texte incompréhensible ou crypté ou chiffré en utilisant une clé. L'inverse appelée décryptage n'est possible que par le destinataire possédant la clé adéquate.

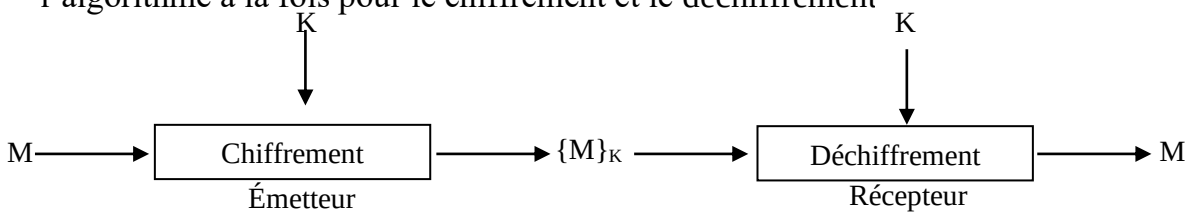
Les protocoles cryptographiques ont pour objectif de sécuriser un échange tout en respectant les propriétés fondamentales suivantes :

- **Confidentialité** : seul le destinataire d'un message peut en prendre connaissance.
- **Intégrité** : un message ne peut être modifié à l'insu du destinataire.
- **Authentification** : l'identité de l'expéditeur est vérifiée.
- **Non-répudiation** : lier une personne à un document c'est-à-dire l'expéditeur ne peut pas nier avoir émis un message une fois celui-ci reçu par son destinataire.

1. **Confidentialité** : Elle a pour rôle d'assurer le secret du message afin que seul son destinataire légitime puisse en prendre connaissance. Elle s'appuie sur différents types d'algorithmes comme : symétriques ou à clé secrète, asymétriques ou à clé publique et hybrides.

   1.1- Chiffrement à clé secrète

   Appelé aussi chiffrement symétrique, repose sur le partage entre deux interlocuteurs en communication d'une même clé secrète qui sert à paramétrer l'algorithme à la fois pour le chiffrement et le déchiffrement



Deux interlocuteurs qui veulent communiquer des données confidentielles doivent partager une clé secrète K, l'émetteur envoie par exemple un message M chiffré avec la clé K, à la réception, le récepteur récupère le message M en déchiffrant le message reçu avec la clé K.

Le chiffrement symétrique a l'avantage d'être rapide. Toutefois, il peut être assez onéreux en raison de la difficulté de la distribution sécurisé de la clé. On y trouve les algorithmes DES, IDEA, AES et RC4.

DES (Data Encryption Standard) : C'est un algorithme de chiffrement symétrique considéré obsolète, non adapté aux usages actuels.

IDEA (International Data Encryption Algorithm): C'est un algorithme de chiffrement par blocs conçu par Xuejia Lai et James Massey en 1991. Il est censé remplacer le DES.

AES (Advanced Encryption Standard) : une méthode de chiffrement à clé symétrique, est aujourd'hui considérée comme étant l'une des méthodes de chiffrement les plus fiables disponibles. Elle est très couramment utilisée dans les protocoles de sécurité Wi-Fi, tels que WPA2 et WPA3 pour chiffrer les données transmises sur les réseaux sans fil. En plus certaines applications de messagerie comme Signal ou WhatsApp ainsi que le programme d'archive de fichiers Win Zip utilisent cet algorithme.

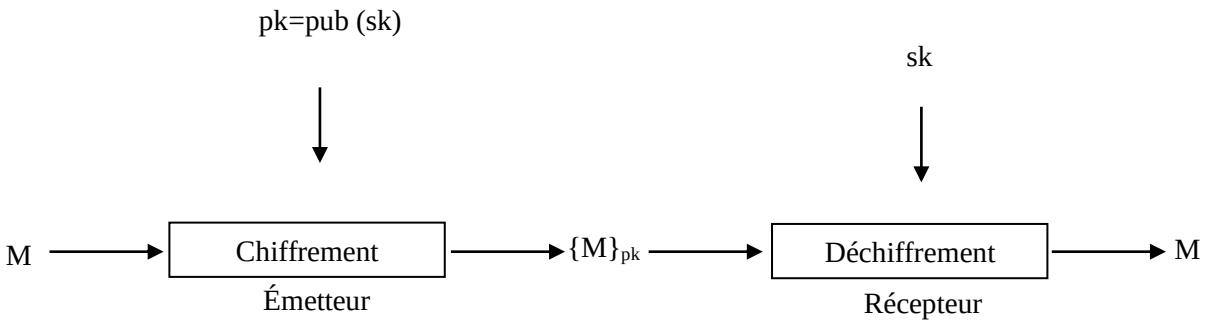
RC4

Cet algorithme est utilisé dans les protocoles de chiffrement WEP et WPA, généralement appliqués dans les routeurs sans fil.

1.2- Chiffrement à clé publique

Introduite en 1975 par Diffie et Hellman avec l'algorithme connu sous le nom de Diffie-Hellman, ce chiffrement utilise deux clés : une publique à partager pour le cryptage et l'autre privée à garder secrète pour le décryptage

Un émetteur qui envoie des données confidentielles. Chiffre le message à envoyer en utilisant la clé publique $\{M\}_{pk}$ de récepteur. Ce dernier est le seul à pouvoir récupérer le message en le déchiffrant avec sa clé privée (sk).



Chiffrement asymétrique

L'intérêt du chiffrement asymétrique réside dans la possibilité de diffuser la clé de cryptage sans renoncer à la confidentialité des messages. Les algorithmes utilisés par la cryptographie asymétrique sont : RSA (Rivest Shamir Adelman), Elgamel, Diffie-Hellman, DSA (Digital Signature Algorithm).

1.3- Cryptographie hybride

C'est une combinaison des meilleures fonctionnalités des deux types de cryptographie susmentionnés. Elle consiste à créer d'abord une clé de session qui est une clé secrète à usage unique. La clé de session est utilisée pour le cryptage et le décryptage par un algorithme symétrique donnant ainsi une rapidité aux deux processus.

La clé de session associée à l'algorithme à clé secrète est soit créée par l'expéditeur aléatoirement, soit par les deux parties en même temps tandis que les deux clés

associées à l'algorithme à clé publique (clé publique et clé privée) sont créées par le propriétaire ou par une autorité à laquelle ce dernier se rattache.

Les algorithmes utilisés : PGP (Pretty Good Privacy), GnuPG (GNU Privacy Guard) et SSL (Secure Socket Layer) qui est plus un protocole plus qu'un algorithme.

2. **Intégrité du message :** Une des conditions les plus élémentaires pour une communication sécurisée est que les messages échangés ne doivent, en aucun cas, faire l'objet de modification ou d'altération durant la communication.

Le rôle de cette fonctionnalité est de détecter toute modification apportée au message. À cette fin, l'utilisation des fonctions de hachage est nécessaire.

Fonction de hachage

Une fonction de hachage appelée aussi fonction de hachage à sens unique est une fonction mathématique permettant de transformer une chaine de longueur variable en une chaine de taille inférieure et fixe appelée empreinte. Elle assure que, si l'information était échangée en qui que ce soit, même d'un seul bit, une sortie totalement différente serait produite. Il existe deux types de fonction de hachage : **les fonctions de hachage sans clé** (peuvent être calculées par n'importe quelle entité) et **les fonctions de hachages avec clé** (seuls ceux qui possèdent la clé peuvent calculer la valeur de hachage correspondante). Les fonctions de hachage les plus utilisées : MD5 (Message Degest 5), SHA-1 (Standard Hash Algorithm-1).

3. **Authentification** : Elle nous permet de nous assurer de l'identité des parties concernées. Il existe plusieurs techniques :
   - **3.1-** ***Avec un algorithme à clé publique*** : chaque partie possède une paire de clés publique/privée. Le fait que l'expéditeur crypte le message M avec sa clé secrète *skA* est un moyen d'affirmer qu'il est le propriétaire de la clé publique *pkA*.

3.2- Avec un algorithme à clés symétriques

3.3- Avec un MAC (Message Authentification Code) : c'est un code qui peut être généré de deux manières avec :

a) *une clé symétrique* : le code de hachage signé avec la clé secrète est une manière de s'assurer de l'identité de l'expéditeur, car il détient la bonne clé secrète.

b) *une fonction de hachage* : c'est le même principe sauf que dans ce cas on ne crypte pas avec la clé k, mais elle entre avec un message M dans la composition du code de hachage MAC.

3.4- ***Avec une signature digitale*** : l'utilisation de la cryptographie à clé publique permet l'établissement des signatures numériques qui offrent au destinataire la possibilité de vérifier l'authenticité de l'expéditeur. Elles sont difficiles à falsifier. Elles apportent aussi l'authentification et l'identification des parties concernées et la non-répudiation en cas de désaveu de la part de l'expéditeur.

Section C-Protocoles d'authentification / de sécurité dans les réseaux Wi-Fi

Avec la quantité croissante d'informations fiables accessibles sur le réseau, la nécessité d'empêcher l'accès à ces données par des personnes non autorisées s'est imposée. L'usurpation d'identité étant aisée dans le monde informatique, des méthodes de vérification spécifiques ont dû être mises au point pour s'assurer que la personne ou l'ordinateur demandant des données est bien celle qu'il prétend être. Le rôle du protocole d'authentification est de spécifier la séquence exacte d'étapes nécessaires à l'exécution de l'authentification. Les Protocoles d'authentification sont une série de procédures permettant de vérifier l'identité d'un utilisateur dans un système informatique et sont essentiels pour garantir la sécurité des données et empêcher tout accès non autorisé. Avant d'entamer les différents protocoles d'authentification, nous allons d'abord définir quelques concepts de base.

a) **Authentification** : L'authentification est un processus de sécurité utilisé pour s'assurer que seuls les utilisateurs autorisés peuvent accéder aux informations, aux systèmes ou à d'autres ressources afin de protéger contre les activités frauduleuses ou les failles de sécurité.

b) **Autorisation** : L'autorisation est l'étape suivante après l'authentification. Il s'agit de déterminer ce qu'un utilisateur authentifié a le droit de faire. Par exemple, un utilisateur peut avoir l'autorisation de visualiser des données mais pas de les modifier. Les autorisations sont généralement attribuées en fonction du rôle de l'utilisateur dans l'organisation ou le système.

c) **Gestion des identités et des accès :** C'est un cadre de processus, de technologies permettant aux entités vérifiées d'obtenir un accès sécurisé aux ressources d'un réseau (comme courriels, bases de données, données et applications). L'objectif est de gérer l'accès afin que les utilisateurs, les collaborateurs autorisés puissent travailler et que les personnes mal intentionnées comme les pirates se voient refuser l'accès.

d) **Importance de l'authentification et de l'autorisation dans un réseau wifi sécurisé**

L'authentification et l'autorisation fonctionnent différemment et offrent des couches de sécurité distinctes pour les réseaux, les données et d'autres ressources. Elles doivent être utilisées en tandem pour créer un environnement entièrement sécurisé. Elles sont nécessaires pour assurer la séparation et la sécurité des données utilisateur. L'authentification invite les utilisateurs à terminer un processus de vérification d'identité pour accéder au réseau, et après cela, l'autorisation détermine les systèmes, les données ou les ressources auxquels le client, l'utilisateur peut accéder.

D’une part, l’authentification est importante car :

- Elle sécurise l’accès pour chaque utilisateur et protège ses données ;
- Elle offre une expérience utilisateur améliorée, souvent en proposant des méthodes de vérifications simples ;
- Avec la simplification de la gestion des utilisateurs par l’authentification unique (SSO), elle permet d’accéder à de nombreux services cloud avec un seul ensemble d’informations d’identification.

D’autre part, l’autorisation est importante car :

- Elle applique le principe du privilège minimum afin que les utilisateurs aient accès uniquement aux ressources nécessaires à leur rôle ;
- Elle permet un contrôle d’accès dynamique afin que les administrateurs puissent modifier les stratégies d’accès en temps réel, offrant une sécurité plus souple.

1-Types d’authentification

Les organisations s’appuient sur différents types d’authentification pour préserver leurs ressources et leurs sites de la cybercriminalité et d’autres atteintes à la sécurité. Certaines institutions peuvent n’utiliser qu’un seul type d’authentification ou une combinaison de ces méthodes en fonction du niveau de sécurité souhaité.

a) **Authentification à un seul facteur** : également appelée authentification par mot de passe, l’authentification à un seul facteur est couramment utilisée et offre la protection la plus faible en termes de sécurité. Il suffit de saisir un mot de passe pour obtenir l’accès.

b) **Authentification à deux facteurs** : il faut saisir deux des trois catégories d’authentification. Par exemple, en plus d’un mot de passe les utilisateurs peuvent également devoir répondre à une question de sécurité, saisir un code d’accès à usage unique ou fournir un code envoyé par email ou SMS.

c) **Authentification multifactorielle** : lorsque l'authentification nécessite trois étapes ou plus, on parle de processus d'authentification multifactorielle. Elle exige des utilisateurs qu'ils fournissent plusieurs moyens de prouver leur identité.

d) **Authentification par jeton :** L'authentification par jeton est une forme d'authentification à deux facteurs qui exige des utilisateurs qu'ils fournissent un jeton physique ou numérique pour prouver leur identité et obtenir l'accès. Le jeton est généralement un code généré à partir de techniques de cryptage, qui sert de signature numérique à l'utilisateur. Un exemple d'authentification basée sur un jeton est un code à usage unique ou un mot de passe. La validité du code est généralement limitée à un laps de temps.

e) **L'authentification basée sur un certificat (CBA)** : S'appuyant sur un certificat numérique pour vérifier l'identité, ce type d'authentification requiert quelque chose que l'utilisateur possède et qu'il connait. L'utilisateur signe un morceau de données générées de manière aléatoire. Il envoie ensuite ces données signées et le certificat numérique d'authentification via le réseau serveur. La CBA est souvent utilisée lorsque les utilisateurs veulent accéder à un serveur intranet, à l'email de l'entreprise ou à certaines applications basées sur le cloud.

f) **L'authentification biométrique** : Elle exige que vous utilisiez une partie de votre corps, comme votre empreinte digitale, votre voix, votre visage ou vos yeux, pour obtenir un accès. Méthode couramment utilisée pour l'authentification à deux facteurs, l'authentification biométrique est plus sûre que les autres méthodes car elle exige que vous fournissiez quelque chose de totalement unique à vous-même.

2- Protocoles d'authentification

Les protocoles sont principalement utilisés par les serveurs PPP (Point-to-Point Protocol) pour valider l'identité des clients distants avant de leur accorder l'accès aux données du serveur.

2.1- Protocole d'authentification par mot de passe (PAP)

Le protocole d'authentification par mot de passe est l'un des plus anciens. L'authentification est initialisée par l'envoi, par le client d'un paquet contenant les identifiants (nom d'utilisateur et mot de passe) au début de la connexion. Ce qui le rend très vulnérable aux attaques les plus simples comme l'écoute clandestine et les attaques MITM (homme du milieu).

2.2- Protocole d'authentification par échange de défi (CHAP)

Dans ce protocole, l'authentification est toujours initiée par le serveur et peut être effectuée à tout moment de la session, même de manière répétée. Le serveur envoie une chaine aléatoire. Le client utilise le mot de passe et la chaine reçue comme entrées d'une fonction de hachage, puis envoie le résultat ainsi que son nom d'utilisateur en clair. Le serveur utilise le nom d'utilisateur pour appliquer la même fonction et compare le hachage calculé avec celui reçu. L'authentification est réussie lorsque les hachages calculé et reçu correspondent.

2.3-Protocole d'authentification extensible (EAP)

Le protocole EAP a été initialement développé pour le protocole PPP (Point-to-Point Protocol), mais il est aujourd'hui largement utilisé dans les normes IEEE 802.3, IEEE 802.11 (Wifi) et IEEE 802.16. Sa version la plus récente est normalisée dans la RFC 5247. L'avantage d'EAP réside dans le fait qu'il s'agit d'un cadre d'authentification client-serveur ; le mode d'authentification est défini dans ses nombreuses versions, appelées méthodes EAP. Il existe plus de 40 méthodes EAP dont les plus courantes sont : EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-PEAP.

2.4-Protocoles d'architecture AAA (Authentification, Autorisation, Comptabilisation)

Protocoles complexes utilisés dans les grands réseaux pour vérifier l'utilisateur (authentification), contrôler l'accès aux données du serveur (autorisation) et surveiller les ressources réseau et les informations nécessaires à la facturation des services (comptabilité).

2.4.1-TACACS, XTACACS et TACACS+

Le plus ancien protocole AAA utilisait une authentification basée sur le protocole IP sans chiffrement (nom d'utilisateur et mot de passe étaient transmis en clair). La version XTACACS (Extended TACACS) a ajouté l'autorisation et la comptabilisation. Ces deux protocoles ont été remplacés par TACACS+ qui sépare les composants AAA, pour permettre leur isolement et leur gestion sur des serveurs distincts. Il utilise le protocole TCP (Transmission Control Protocol) pour le transport et le chiffre l'intégralité du paquet. C'est une technologie propriétaire Cisco.

2.4.2-RAYON

RADIUS (Remote Authentification Dial-In User Service), est un protocole AAA complet couramment utilisé par les FAI. Les informations d'identification sont principalement basées sur une combinaison nom d'utilisateur / mot de passe et utilise les protocoles NAS et UDP pour le transport.

2.4.3-DIAMÈTRE

Diameter (protocole) a évolué à partir de RADIUS et comprend de nombreuses améliorations telles que l'utilisation d'un protocole de transport TCP ou SCTP plus faible et une sécurité plus élevé grâce à TLS.

3- Protocoles de sécurité du réseau Wi-Fi

Les protocoles de sécurité du réseau Wi-Fi sont, en fait, un ensemble de règles qui protègent les réseaux sans fil en chiffrant les données et en contrôlant les accès. Ils assurent la confidentialité des informations et la non infiltration dans le réseau par les pirates.

La vulnérabilité dû à la transmission des données transmises par les réseaux sans fil, les protocoles de sécurité sans fil robustes se révèlent essentiels pour assurer la sécurité en ligne. Ces protocoles sont certifiés par la Wi-Fi Alliance, une organisation à but non lucratif propriétaire de la marque commerciale Wi-Fi. On y retrouve quatre protocoles de sécurité sans fil :

3.1-WEP (Wired Equivalent Privacy)

Le plus ancien protocole de sécurité Wi-Fi et est considéré de nos jours comme obsolète. La norme de sécurité WEP a été ratifiée en 1999 par le groupement Wi-Fi Alliance. Le WEP a connu plusieurs problèmes parmi lesquels, on retrouve des failles cryptographiques dans l'algorithme RC4 et une vulnérabilité aux attaques. Devenu très simple à pirater avec l'amélioration de la puissance de calcul moderne ; il a été officiellement retiré en 2004 par la Wi-Fi Alliance et tous les systèmes qui l'utilisent encore doivent être mis à niveau ou remplacés.

Vulnérabilités :

- Truffe de failles de sécurités
- Uniquement des clés 64 bits et 128 bits pour le chiffrement
- Chiffrement à clé fixe
- Difficile à corriger

3.2-WPA (Wi-Fi Protected Access)

C'est un protocole de sécurité sans fil lancé en 2003 pour résoudre les vulnérabilités du WEP. Il est plus sûr que le WEP car il utilise une clé de chiffrement 256 bits c'est-à-dire qu'il existe tellement de combinaisons possibles qui faudrait des millions d'années pour la déchiffrer.

Il utilise aussi le protocole TKIP (Temporal Key Integrity Protocol), qui génère une nouvelle clé pour chaque paquet réseau, c'est-à-dire pour chaque unité de données.

Cependant le WPA présente aussi des failles. Le TKIP, composant principal du WPA, a été conçu pour être mis en œuvre dans les systèmes WEP via la mise à jour du firmware. Cette approche fait que le WPA repose encore sur des éléments facilement exploitables.

Vulnérabilités :

- Lorsqu'il est appliqué aux appareils WEP, le TKIP peut faire l'objet d'un exploit
- Failles similaires à celles du WEP

3.3-WPA2 (Wi-Fi Protected Access 2)

La deuxième génération de protocole de sécurité sans fil du WPA. Il chiffre le trafic sans fil et limite l'accès aux personnes possédant le mot de passe du réseau. Le TKIP a été remplacé par le système AES (Advanced Encryptions System). Cette norme de chiffrement robuste est utilisée par les gouvernements, les institutions financières et les entreprises internationales pour sa grande sécurité. Pour éliminer des failles de sécurité, il faut d'une part désactiver le WEP/WPA sur les appareils fonctionnant avec WPA2 et d'autre part il faut mettre à niveau tous les appareils reposant uniquement sur le WEP.

3.3.1-WPA2 Personal

Rencontré dans les réseaux Wi-Fi domestiques est également appelé mode Clé pré-partagée (PSK), qui utilise un code d'accès partagé qui doit être saisi à la fois sur l'appareil client et sur le point d'accès

3.3.2-WPA2 Entreprise

Généralement rencontré dans les entreprises ou les institutions, il utilise le protocole EAP ainsi qu'un serveur d'authentification centralisé. Ce qui permet à chaque utilisateur ou appareil de se connecter avec des informations d'identification uniques.

Vulnérabilité

- Présente encore quelques failles en termes de sécurité

3.4-WPA3 (Wi-Fi Protected Access 3)

C'est le protocole de sécurité le plus récent, conçu pour chiffrer les données de manière plus sûre et protéger les sessions passées, même si un mot de passe est compromis par la suite : une fonctionnalité connue sous le nom de Confidentialité persistante (PFS). WPA3 repose sur AES-GCMP (Galois/Counter Mode Protocol), un mode de chiffrement très puissant qui renforce à la fois la sécurité et la rapidité. Par rapport au mode AES-CCMP utilisé dans le WPA2, GCMP offre une meilleure intégrité des données et une meilleure efficacité globale.

Caractéristiques techniques

	WEP	**WPA**	**WPA2**	**WPA3**
Année de sortie	1999	2003	2004	2018
Protocole de chiffrement	Clé fixe	TKIP	CCMP	AES-GCMP
Taille de clé de session	64 bits / 128 bits	256 bits	256 bits	192bits/256bits
Type de chiffrement	Chiffrement de flux RC4	TKIP (basé sur RC4)	AES	Chiffrement par blocs GCMP
Intégrité des données	Contrôle de redondance cyclique	Contrôle d'intégrité des message	CCMP	GMAC
Méthode d'authentification	Système ouvert/Clé partagée	PSK	PSK + PMK	SAE + EAP
Gestion des clés	Chiffrement à clé symétrique	WPA+WPA-PSK	PMK + PSK	RSN + PMF
Sécurité	Faible	Moyenne	Elevée	Très élevée

Section D-Politique de sécurité sans fil et mobiles

Les appareils sans fil et mobiles sont essentiels pour le travail et la communication. Toutefois, ils présentent des risques de sécurité importante pour un réseau. Il est nécessaire de mettre en place des politiques de sécurités efficaces.

1. Chiffrement et authentification

L'une des étapes les plus élémentaires et plus importantes consiste à utiliser des protocoles de cryptage et d'authentification pour protéger les appareils et les utilisateurs. Le chiffrement favorise la lecture seulement par les parties concernées ou autorisées tandis que l'authentification vérifie l'identité des appareils et des utilisateurs. Le WPA et le WPA3 peuvent être utilisés pour un cryptage fort et s'il le faut une authentification multi facteur peut être mise en place pour la protection du réseau.

2. Gestion et contrôle des appareils

Il faut un système de gestion et de contrôle pour surveiller, configurer et mettre à jour les appareils. Il facilite le verrouillage, la suppression ou la localisation d'appareils perdus ou volés. Une solution WLC, contrôleur LAN sans fil, est nécessaire.

3. Segmentation et isolation du réseau

La sécurité sans exige la segmentation et l'isolation du réseau en différentes zones en fonction du niveau de confiance et d'accès requis. Ceci aide à la disponibilité et à l'amélioration des performances du réseau. Le pare-feu, les listes de contrôle d'accès et les VLAN peuvent être employés pour appliquer la stratégie de segmentation et d'isolation du réseau.

4. Protection et sauvegarde des données

À cette étape, il est crucial d'utiliser des outils pour empêcher la fuite ou le vol des données sensibles comme les informations personnelles, les identifiants et autres. La protection et la sauvegarde des données se montrent indispensable pour une meilleure sécurité dans les réseaux mobiles et sans fil.

5. Education et débilisation des utilisateurs

Les utilisateurs doivent être sensibilisé et éduqués aux meilleures pratiques et politiques d'utilisation des appareils sans fil. Des formations régulières et des conseils sont encouragés sur les sujets aussi sensibles sur la sécurité comme la gestion de mot de passe, la prévention du phishing, la sécurité des appareils, la sécurité du réseau et la protection des données. Il est conseillé de demander aux utilisateurs de signaler toute activité suspecte ou inhabituelle.

6. Test et audits de sécurité

Il est de faire des évaluations de vulnérabilités, des tests de pénétration et des audits de conformité pour identifier et corriger les lacunes ou les faiblesses de sécurité. Le trafic réseau doit être surveillé et analysé pour anticiper toute anomalie ou toute attaque.

Chapitre IV- Gestion des identités

De nos jours, la sécurité de l'information joue un rôle important dans notre vie numérique où chaque jour nos données sont exposées à des attaques, des violations de sécurité. Dans les organisations, des ressources sont mises à la disposition des utilisateurs qui en ont besoin pour travailler efficacement. Souvent cette gestion des ressources s'avère très difficile pour des centaines voire des milliers d'utilisateurs. La gestion des identités et des accès contribue à renforcer la sécurité en assurant un suivi, une gestion et la sécurisation des identités des utilisateurs et des données qui leur sont attribuées ou associées.

1. Identité

Une identité numérique est une collection d'identificateurs uniques ou d'attributs qui représentent une personne, un composant logiciel, une machine, une ressource ou une ressource dans un système.

Les identités sont classées en trois types :

- Identités humaines, elles représentent des personnes, y compris des employés et des utilisateurs externes ;
- Identités de charge de travail, elles représentent des charges de travail logicielles telles qu'une application, un service, un script ou un conteneur ;
- Identités d'appareil, elles représentent des appareils, notamment des ordinateurs de bureau, des téléphones mobiles, des capteurs IoT et des appareils gérés par IoT.

2. Gestion de l'identité

La gestion de l'identité couvre le processus de gestion des identités des utilisateurs et des droits d'accès de manière centralisée. Elle implique l'enregistrement et le contrôle des identités au sein d'une organisation et l'application de politiques de gouvernance des identités.

3. Différence entre gestion des identités et gestion des accès

En termes plus simples, la gestion des identités consiste à établir et à gérer des identités numériques, tandis que la gestion des accès consiste à contrôler et réglementer les droits d'accès et les autorisations associées à ces identités. IDM (Identity Management) est responsable de la création et de la maintenance des identités, tandis que IAM (Identity and Access Management) se concentre sur la gestion et l'application des contrôles d'accès basés sur ces identités.

La gestion des identités se concentre sur l'établissement et la gestion des identités numériques des individus ou des entités au sein de l'écosystème d'une organisation. Cela implique de créer des identités uniques et de les associer à des attributs et des informations d'identification tels que des noms d'utilisateur, des mots de passe et des certificats numériques. L'IDM englobe des activités telles que l'intégration, la désintégration des utilisateurs et la gestion du cycle de vie des identités. Son objectif principal est de garantir que chaque utilisateur ou entité dispose d'une identité numérique bien définie et unique au sein du système IAM de l'organisation. IDM fournit une base pour le contrôle d'accès et établit la base de la gestion des privilèges et autorisations des utilisateurs.

La gestion des accès, quant à elle, s'occupe du contrôle et de la gestion des autorisations et privilèges d'accès associés à l'identité numérique d'un individu ou d'une entité. La gestion des accès se concentre sur l'application des processus d'authentification et d'autorisation pour garantir que les utilisateurs disposent du niveau d'accès approprié à des ressources spécifiques ou effectuent certaines actions au sein du système. L'authentification vérifie l'identité revendiquée de l'utilisateur, tandis que l'autorisation détermine à quelles ressources l'utilisateur peut accéder et quelles actions il peut effectuer. La gestion des accès comprend des activités telles que les politiques de contrôle d'accès, le contrôle d'accès basé sur les rôles (RBAC) et l'application de la politique de sécurité.

Aspect	Gestion des identités (IDM)	Gestion des accès (IAM)
Focus	Etablir et gérer les identités numériques	Contrôler et gérer les autorisations d'accès
Activités	Intégration et désintégration des utilisateurs, gestion du cycle de vie des identités	Politiques d'authentification, d'autorisation et de contrôle d'accès
Objectif	Créer et maintenir des identités numériques	Appliquer des contrôles d'accès basés sur les identités
Composants clés	Identités, attributs, informations d'identification uniques	Mécanismes d'authentification, politiques de contrôle d'accès
Responsabilités	Création et gestion d'identité	Application des droits d'accès

Tableau récapitulatif de IDM et IAM

4. Fonctionnalités de la gestion des identités et des accès

Le processus d'IAM commence par l'authentification de l'utilisateur en vérifiant l'identité de l'utilisateur via diverses méthodes telles que mot de passe, données biométriques, et autres. Détermine ensuite le niveau d'accès de l'utilisateur authentifié. L'IAM fournit aussi des fonctionnalités d'audit permettant de suivre l'activité d'un utilisateur et de surveiller tout comportement suspect afin d'identifier menaces potentielles pour la sécurité et prendre les mesures appropriées. Les étapes générales de IAM sont les suivantes :

1. **Gestion d'identité** : L'IAM commence par la gestion des identités, impliquant l'établissement et la gestion d'identité numériques uniques pour les individus ou les entités de l'écosystème d'une organisation. Chaque identité est associée

à un ensemble d'attributs et d'informations d'identification comme : nom d'utilisateur, mot de passe, certificat numérique.

2. **Approvisionnement et déprovisionnement des utilisateurs** : L'IAM permet de créer et de gérer des comptes utilisateur, notamment en spécifiant quels utilisateurs peuvent accéder aux ressources et attribuer des autorisations et des niveaux d'accès.

3. **Authentification des utilisateurs** : L'authentification est le processus de vérification de l'identité revendiquée d'un utilisateur ou d'une entité. Les système IAM utilisent diverses méthodes d'authentification pour garantir la légitimité des utilisateurs avant d'accorder l'accès. Des mécanismes d'authentification peuvent être mis en œuvre selon le niveau de risque : le SSO (Single Sign-On) pour se connecter une seule fois pour accéder à plusieurs ressources, le MFA (Multi-Factor Authentification) pour sécuriser les accès sensibles ou encore l'authentification adaptative pour moduler le niveau de contrôle selon le contexte (lieu, terminal, horaire).

4. **Autorisation des utilisateurs :** Une fois l'identité d'un utilisateur établie et authentifiée, IAM détermine le niveau d'accès et les autorisations qui doivent être accordées. Les stratégies d'autorisation définissent les ressources auxquelles un utilisateur peut accéder et les actions qu'il peut effectuer.

5. **Contrôle de l'accès** : des contrôles d'accès sont appliqués par les systèmes IAM en agissant comme intermédiaire entre les utilisateurs et les ressources. Les mécanismes de contrôle d'accès peuvent inclure un contrôle d'accès basé sur les rôles **RBAC** (Role-Based Access Control), dans lequel les droits d'accès sont attribués en fonction des rôles prédéfinis. Le **ABAC** (Attribute-Based Access Control) tient compte des critères contextuels comme la localisation, le type données ou le statut d'un projet. Il existe d'autres modèles comme **DAC** (Discretionary Access Control) où le propriétaire des données

définit qui peut y accéder, ou **MAC** (Mandatory Access Control) basé sur des politiques d'accès strictes imposées par l'organisation.

6. **Rapport et surveillance** : Pour la traçabilité et l'audit des accès, l'IAM gère des rapports sur les actions de plateforme pour garantir la conformité et évaluer les risques de sécurité.

5.Intégration de l'IAM

a) Avec RADIUS (Remote Authentification Dial-In User Service)

RADIUS est un protocole largement utilisé qui facilite l'authentification, l'autorisation et la comptabilité centralisées (AAA) pour les utilisateurs accédant à des services réseau tels que les VPN, le Wi-Fi et d'autres systèmes critiques. MFA avec votre serveur RADIUS, vous garantissez que l'accès à votre réseau est sécurisé en demandant aux utilisateurs de fournir non seulement leurs informations d'identification, mais également un deuxième facteur d'authentification, tel qu'un mot de passe à usage unique (OTP), une notification push ou une vérification biométrique.

RADIUS exécute trois fonctions de base :

- **Authentification** : il authentifie les appareils ou les utilisateurs avant de leur permettre d'accéder à un réseau ;
- **Autorisation** : il autorise les appareils ou les utilisateurs ;
- **Comptabilité** : il représente le nombre de ressources utilisées, telles que les paquets, les octets et le temps consacré, pendant la session.

b) Avec LDAP

Annuaire joue un rôle essentiel dans le recensement et le stockage des informations d'identité et d'authentification. Il permet aussi la gestion des accès aux ressources et la configuration des paramètres de sécurité tant pour les utilisateurs que pour les postes.

Le protocole LDAP (Lightweight Directory Access Protocol) est une interface standardisée permettant d'accéder aux différents services d'un annuaire. Il se structure autour de quatre modèles fondamentaux :

- **Modèle d'information** : définit le type d'information stocké dans l'annuaire
- **Modèle de nommage** : organise les informations et précise leur désignation
- **Modèle fonctionnel** : décrit les méthodes d'accès et de modification des informations
- **Modèle de sécurité** : établit les mécanismes d'authentification et de droits d'accès.

Avec Active Directory

L'Active Directory ou AD représente le pilier de la gestion des identités et des accès. C'est un annuaire LDAP créé par Microsoft et fourni par les systèmes d'exploitation Windows Server. Cet annuaire centralise deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information. Il est devenu l'outil de référence pour la gestion des comptes et identités.

c) Avec TACACS+ (Terminal Access Controller Access-Control System Plus)

TACACS+ facilite la communication entre un client et un serveur. TACACS+ donne aux utilisateurs plus de contrôle sur la manière dont les commandes sont autorisées. De plus, avec TACACS+, toutes les informations d'authentification, d'autorisation et de comptabilité sont cryptées.

5.Tendance et innovations/ intelligence artificielle en IAM

L’intelligence artificielle (IA) joue un rôle crucial dans la détection de anomalies au sein des systèmes IAM. Grâce à des algorithmes avancés qui analysent les comportements des utilisateurs, les systèmes peuvent identifier en temps réel des activités suspectes, signalant ainsi les menaces potentielles avant qu’elles ne deviennent des incidents de sécurité.

Cette capacité à réagir rapidement est essentielle dans un paysage de menaces en constante évolution. Intégration de l’IA dans les solutions IAM est indispensable pour toute organisation voulant maintenir une posture de sécurité proactive.

L'automatisation intelligente est une autre tendance majeure qui transforme la gestion des accès et des identités. En utilisant des algorithmes d'apprentissage machine, les entreprises peuvent rationaliser leurs processus de gestion des identités, réduisant ainsi le risque d'erreurs humaines tout en augmentant l'efficacité.

Cette automatisation contribue également à améliorer l'expérience utilisateur, en simplifiant l'accès aux ressources tout en maintenant des niveaux de sécurité élevés. En adoptant des solutions d'automatisation, les entreprises peuvent se concentrer sur des tâches à plus forte valeur ajoutée, laissant les processus répétitifs aux machines.

Les solutions basées sur l'IA ne se contentent pas de réagir aux menaces ; elles peuvent anticiper les menaces avancées avant qu'elles ne se produisent. En analysant des données historiques et en observant les comportements des utilisateurs, les systèmes d'IA peuvent prédire et prévenir les incidents de sécurité. En intégrant des outils d'IA dans leur stratégie IAM, les organisations peuvent non seulement renforcer leur sécurité, mais également améliorer leur capacité à détecter et à répondre aux menaces.

Chapitre V- Études de cas

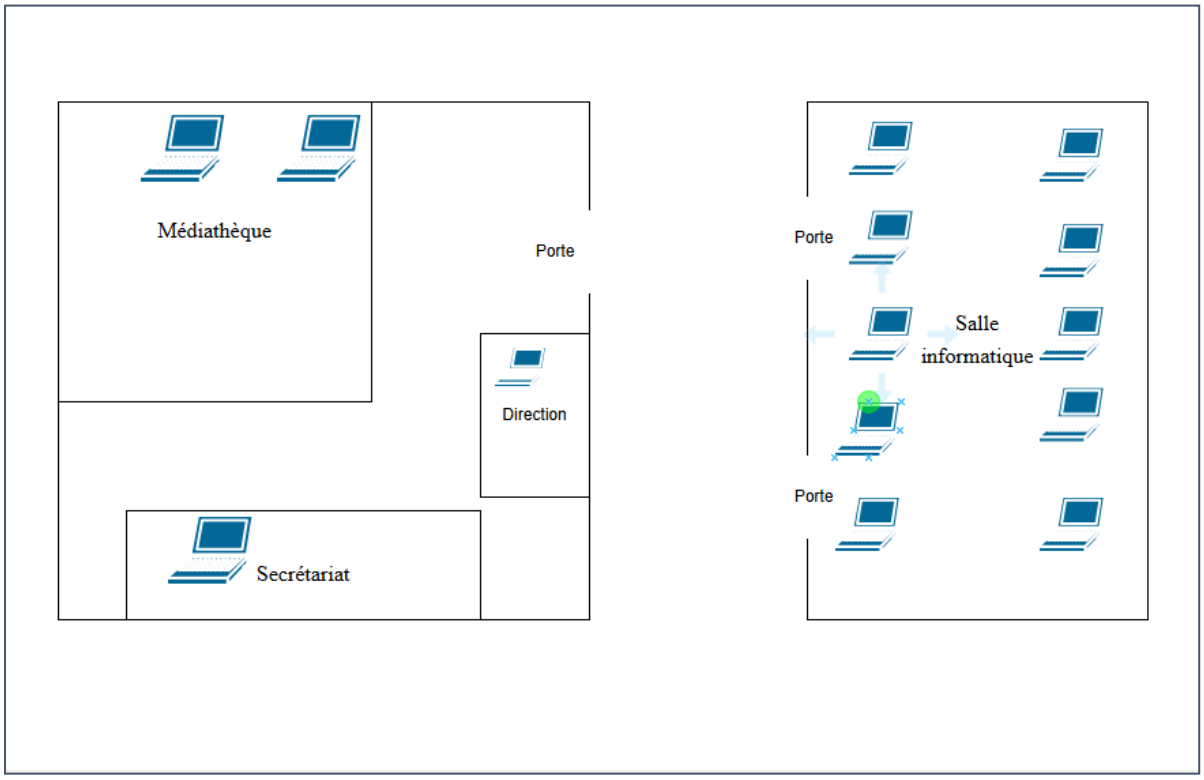
Déploiement d'un système wifi avec l'AAA, serveur RADIUS et un seul point d'accès pour lier les deux bâtiments en utilisant le chiffrement AES.

À propos de l'institution

Créée en 1920, l'Alliance Française de Jacmel est une association de droit haïtien qui participe à la promotion de la langue française, de la diversité culturelle et des cultures francophones. Elle offre des cours de français, de créole, d'anglais, d'espagnol et d'informatique pour tout intéressé désirant se former ou approfondir leur connaissance et monter en compétences.

L'objectif de ce travail pratique est la mise en réseau de plus d'une dizaine de laptops avec le protocole AAA (Radius).

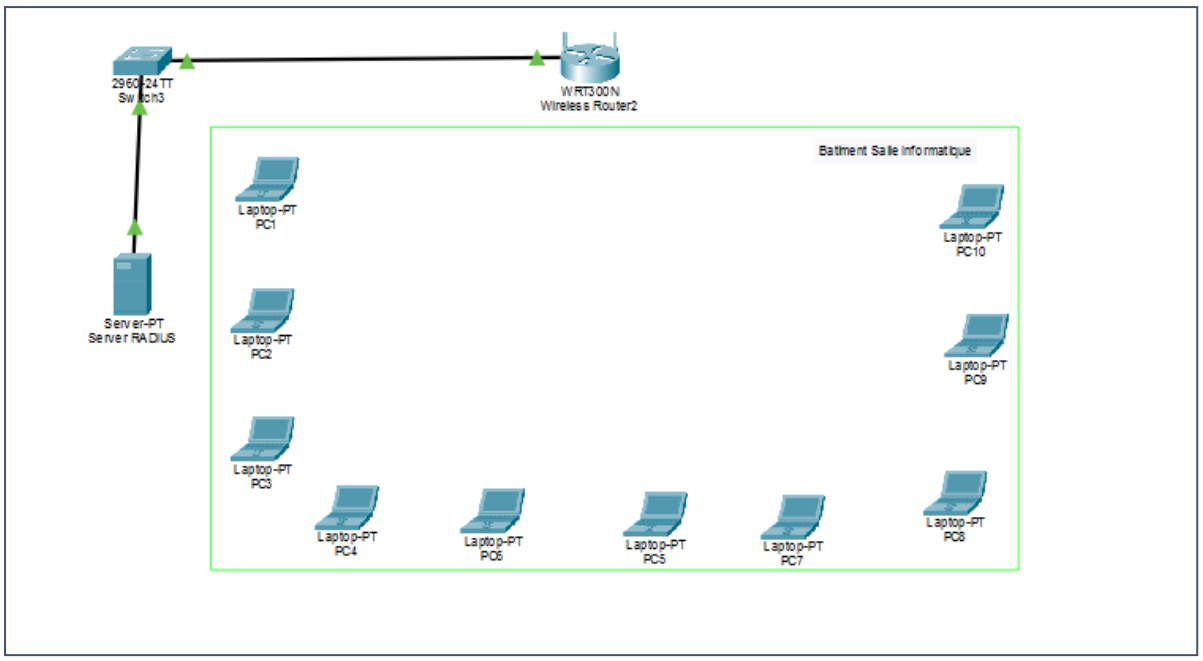
Plan du bâtiment



La direction de l'AFJ souhaite mettre en place un réseau wifi dans le bâtiment 2 où se trouve la salle informatique pour faciliter sa prise en charge et le contrôle des

candidats lors des examens internationaux et écarte le bâtiment principal en raison de l'utilisation excessive et non contrôlée des équipements par les employés.

Topologie du réseau



Matériels utilisés

- 10 laptops
- 1 switch
- 1 routeur
- 1 serveur RADIUS

Pour la mise en place ou le déploiement du réseau, j'ai utilisé le protocole WPA2 avec le chiffrement AES. Le protocole WPA2 est très utilisé et est fiable avec le chiffrement cela renforce encore la sécurité.

IP du routeur : 192.168.0.1

IP du Serveur : 192.168.0.119

IP des laptops sont attribués de façon dynamique

Pour l'authentification et la gestion des identités, le serveur RADIUS a été utilisé pour une centralisation de la vérification et des accès aux ressources du réseau.

Chapitre VI- Recommandations et perspectives

RADIUS a été développé par Livingston Enterprises, Inc. en 1991 et est devenu la norme de l'Internet Engineering Task Force (IETF). RADIUS a été utilisé pour la première fois pour connecter les universités dans l'État du Michigan. La National Science Foundation (NSF) a accordé une subvention à Merit Network, un fournisseur Internet à but non lucratif, et a engagé Livingston Enterprises pour développer un protocole qui a fini par être RADIUS

Le service d'authentification à distance et d'accès à distance (RADIUS) est un protocole réseau qui **autorise et authentifie les** utilisateurs qui accèdent à un réseau distant. Un protocole est un ensemble de règles qui contrôlent la façon dont quelque chose communique ou fonctionne.

RADIUS est utilisé pour établir des connexions entre les ordinateurs et fournit l'authentification, l'autorisation et la comptabilité. RADIUS est un outil important pour gérer l'accès au réseau, car il peut empêcher les utilisateurs non autorisés et les attaquants d'infiltrer votre réseau.

Un protocole RADIUS utilise un client RADIUS ou un serveur d'accès réseau (NAS) et un serveur RADIUS. Il exécute certaines des mêmes fonctions qu'un protocole **LDAP (Lightweight Directory Access Protocol)** et fournit des services d'authentification locaux en maintenant un répertoire actif des informations d'identification des utilisateurs. Ses fonctions de sécurité le placent à la même hauteur que le **TCP (Transmission Control Protocol)**. RADIUS fonctionne sur le port 1812 et le port 1813. RADIUS exécute trois fonctions de base : l'authentification, l'autorisation et la comptabilité.

1. **Authentification** : RADIUS authentifie les appareils ou les utilisateurs avant de leur permettre d'accéder à un réseau.
2. **Autorisation** : RADIUS autorise les appareils ou les utilisateurs, ce qui leur permet d'utiliser des services spécifiques sur le réseau.

3. **Comptabilité** : RADIUS représente le nombre de ressources utilisées, telles que les paquets, les octets et le temps consacré, pendant la session.

Avec RADIUS, vous pouvez empêcher la divulgation d'informations privées à des personnes non autorisées, principalement parce que si leurs identifiants ne correspondent pas à ce qui se trouve dans la base de données du serveur RADIUS, un utilisateur ne peut pas accéder à la connexion. RADIUS est une solution évolutive, car elle peut être mise en œuvre dans une variété de réseaux différents. Il peut également être dupliqué si nécessaire au fur et à mesure que d'autres connexions sont ajoutées. De plus, il s'intègre à la plupart des systèmes de sécurité, tels que le protocole point à point (PPP), le protocole d'authentification par mot de passe (PAP) ou la connexion UNIX.

L'IA une autre facette de la sécurité informatique multiplie à la fois les capacités de défense et les risques, rendant la sécurité périmétrique traditionnelle insuffisante. Le modèle Zéro Trust évolue vers un modèle centré sur les données. L'association de l'IA, du Zéro Trust et des services gérés permet la visibilité, l'automatisation et la réponse en temps réel. L'irruption de l'IA a changé la donne en matière de cybersécurité. La philosophie Zéro Trust est devenue la nouvelle norme. Le défi consiste désormais à l'adapter à un monde où il ne s'agit plus seulement de contrôler les personnes et les appareils, mais aussi les modèles d'IA, les agents autonomes et les flux de données qui circulent à la vitesse de la machine entre les plateformes, les applications et les clouds. Cependant, l'IA est devenue une arme à double tranchant, apporte aussi son lot de problèmes car il est aujourd'hui très facile de générer des campagnes de phishing hyper-personnalisées, des deepfakes vocaux ou vidéos, malware polymorphe ou des fraudes automatisées.

Zéro Trust, ce modèle popularisé en 2010 par Foresster, initié par John Kindervag avec une idée aussi simple que radicale : « Ne faites confiance, vérifiez toujours » peu importe que la connexion provienne de l'intérieur ou de l'extérieur, tout accès doit être authentifié, autorisé et surveillé en permanence. Ses principes fondamentaux

peuvent être résumés en trois piliers : vérification rigoureuse et indépendante de l'origine, accès selon le principe du moindre privilège et engagement permanent. On part du principe que le réseau peut être compromis et que tout utilisateur, même interne, peut devenir une menace.

Conclusion

Nous vivons dans un monde en pleine évolution surtout dans le domaine numérique. Les technologies sans fil se multiplient et nous sommes de plus en plus exposés au risque de cyberattaques. Pour se protéger contre le vol d'informations sensibles, de ressources importantes, l'intrusion ou toute autre vulnérabilité, nous devons mettre en place des techniques, des politiques de sécurités pour contrecarrer ou anticiper toute menace que ce soit venant de l'extérieur ou de l'intérieur surtout des utilisateurs non sensibilisés ou de normes de sécurités obsolètes.

Les administrateurs de réseaux se trouvent parfois face à un dilemme sur le choix de protocole de gestion des identités ou de l'authentification des utilisateurs du réseau sans fil utilisés pour le trafic des paquets de données. Nous avons présenté quelques protocoles dont la sécurité est obsolète ou très élevée. Un réseau wifi sécurisé contient d'abord un SSID (Service Set Identifier), un nom pour l'identifier et un mot de passe ou clé pour sa sécurité. Pour renforcer la sécurité, il faut des mots de passe renforcés et changés régulièrement.

L'authentification et la gestion des identités sont très utiles dans tout système sans fil ou wifi sécurisé car elles permettent d'identifier l'utilisateur et voir s'il sera autorisé à accéder aux ressources disponibles sur le réseau. La gestion de l'authentification et des accès (généralement appelée *IAM*, Identity and Access Management) consiste à accorder aux bonnes personnes l'accès aux bonnes ressources pour les bonnes raisons. Elles assurent la confidentialité, l'intégrité, l'authentification des données.

Les protocoles d'authentification et de gestion des identités ont été vu, avec leurs faiblesses et leurs forces. Des protocoles, WPA2 offre un niveau de sécurité élevé et celui du WPA3 est excellent. Cependant WPA3 n'est pas encore disponible sur certains équipements et certains restent toujours avec le WPA2. AES est un mécanisme de chiffrement symétrique fonctionnant par bloc est ultra fiable, et RADIUS un protocole AAA d'authentification et de gestion d'identité centralisé pour la protection des ressources équipement réseau.

Cependant, face à de nouvelles menaces et à l'économie de temps, il serait très pratique de faire appel à l'IA (intelligence artificielle) pour l'automatisation de certaines tâches dans le réseau et aussi utilisé une solution cloud pour partager des ressources.

Bibliographie

1. Baptiste LEMOINE, 10/10/2024.Les communications sans fil. Comment fonctionnent-ils ? Les communications sans fil : décryptage de leur fonctionnement !
2. Qu'est-ce que la gestion des vulnérabilités, Qu'est-ce que la gestion des vulnérabilités ? | IBM, visité le 30 décembre 2025
3. Concepts fondamentaux de la gestion des identités et des accès. Gestion des identités et des accès (IAM) : Concepts et avantages fondamentaux - Microsoft Entra | Microsoft Learn, visité le 25 décembre à 10h38
4. Qu'est ce que la gestion des identités et des accès (IAM), Qu'est-ce que la gestion des identités et des accès (IAM) ? | OVHcloud France visité le 30 décembre à 9h08
5. Comparaison de sécurité du réseau Wi-Fi : Qu'est-ce que le WEP, le WPA, le WPA2 et le WPA3 ?, Sécurité Wi-Fi : WEP, WPA, WPA2 et WPA3, visité le 30 décembre 2025 à 10h02
6. Qu'est-ce que l'autorisation et l'authentification ? Authentification vs autorisation : quelle est la différence ?
7. Présentation de la gestion de l'authentification et des accès, Présentation de la gestion de l'authentification et des accès | Cloud Architecture Center | Google Cloud Documentation, consulté le 30 décembre 2025 à 14h pm
8. Réseau wifi sécurisé : Comment fonctionne ce principe de sécurité, Réseau Wi-Fi sécurisé : Comment fonctionne ce principe de sécurité ? - Xter, 24 Aout 2025
9. La sécurité du wifi, Centre canadien pour la cybersécurité, itsp80002-f.pdf, consulté le 2 janvier 2026
10. Coursera staff, 1/08/2024, Qu'est-ce que l'authentification, Qu'est-ce que l'authentification ? | Coursera
11. Protocole d'authentification, Protocole d'authentification, visité le 26 décembre 2025

Annexes

Configuration du routeur Wireless

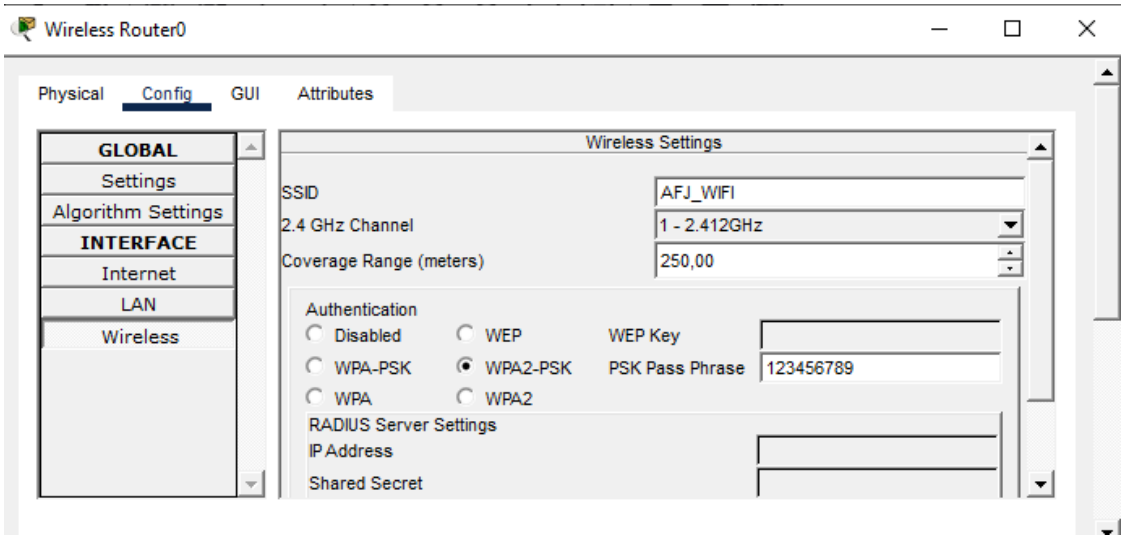
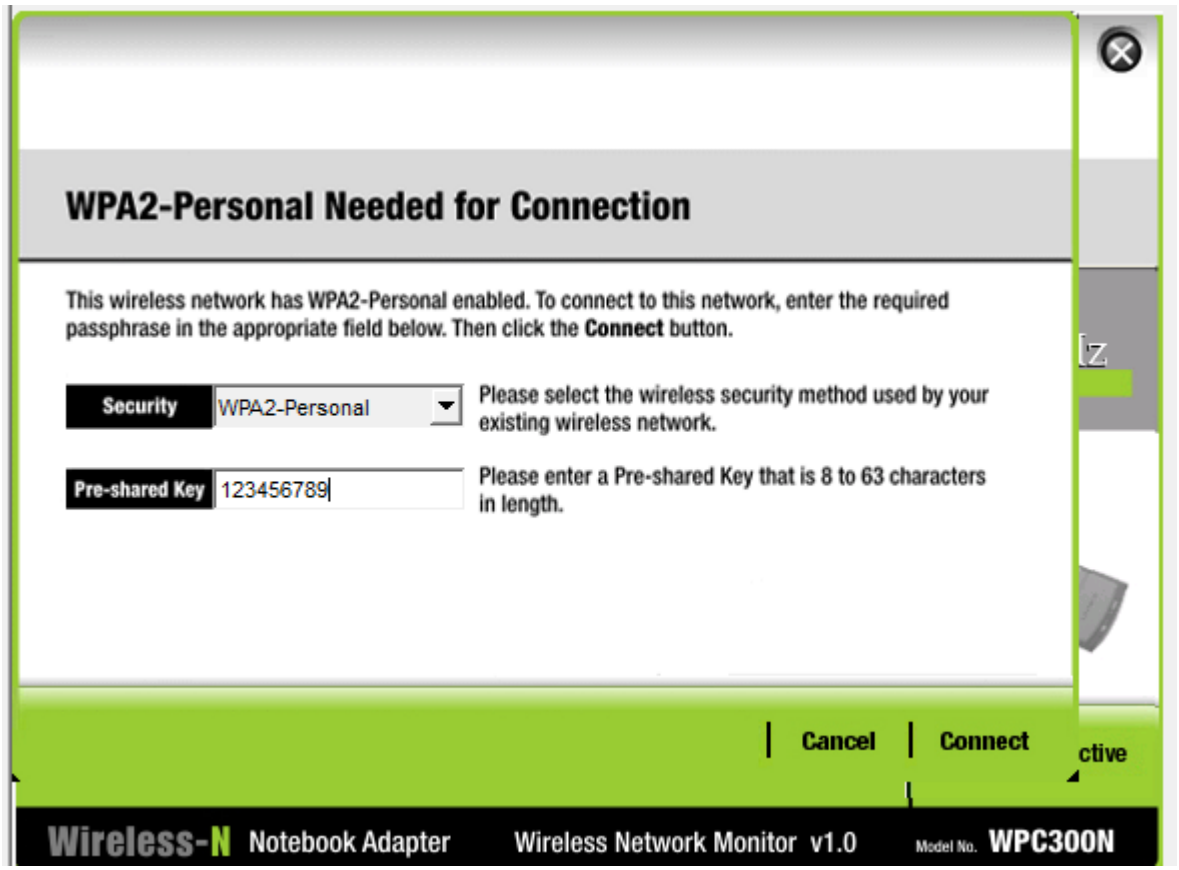


Figure 1-un mot de passe est un SSID est attribué au routeur

Connection d'un PC au routeur



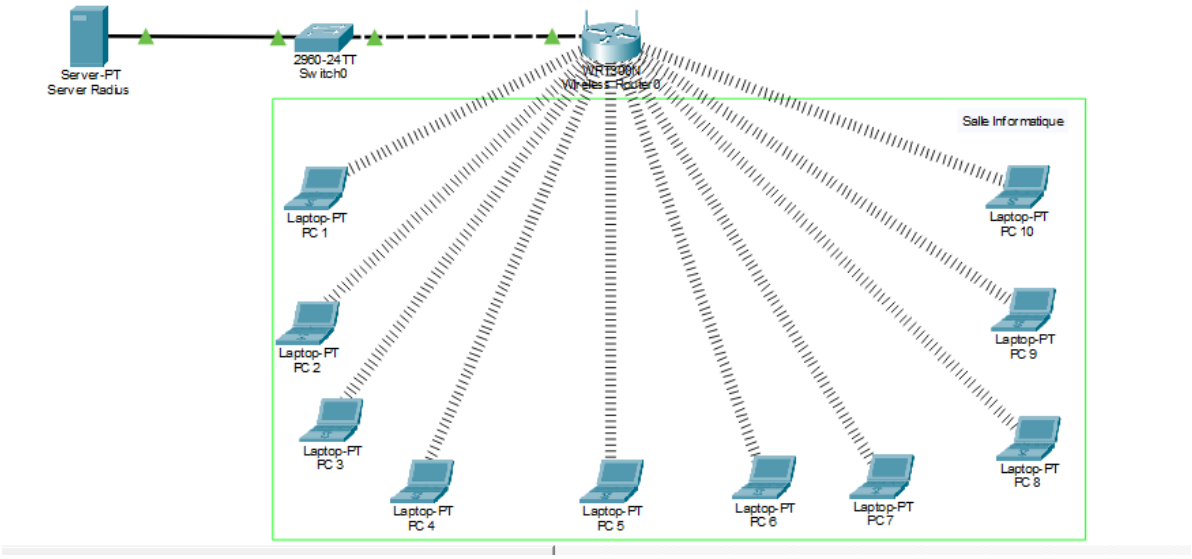


Figure 2-La connexion des PC au Point d'accès

Attribution d'adresse IP au Serveur RADIUS

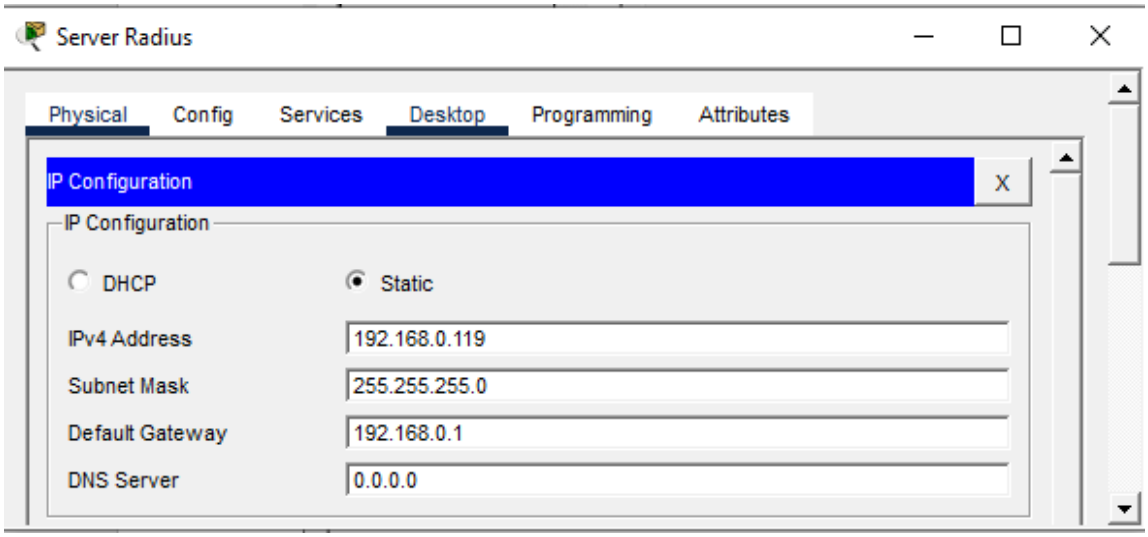
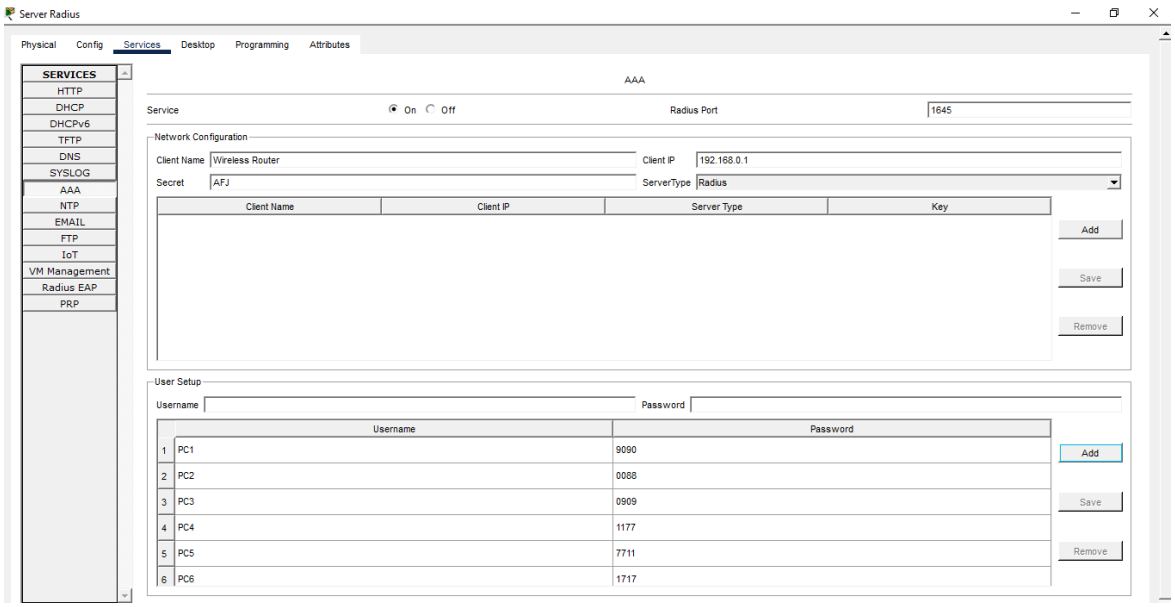


Figure 3-une adresse IP statique a été attribué au serveur ainsi qu'une passerelle 192.168.0.1

Activation des services AAA pour le serveur RADIUS



Test de la connectivité entre le server et le routeur

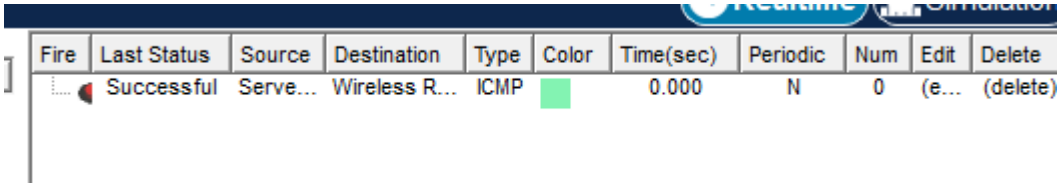


Figure 4-tout se fait avec succès

Connexion des utilisateurs avec les identifiants créés dans le serveur RADIUS

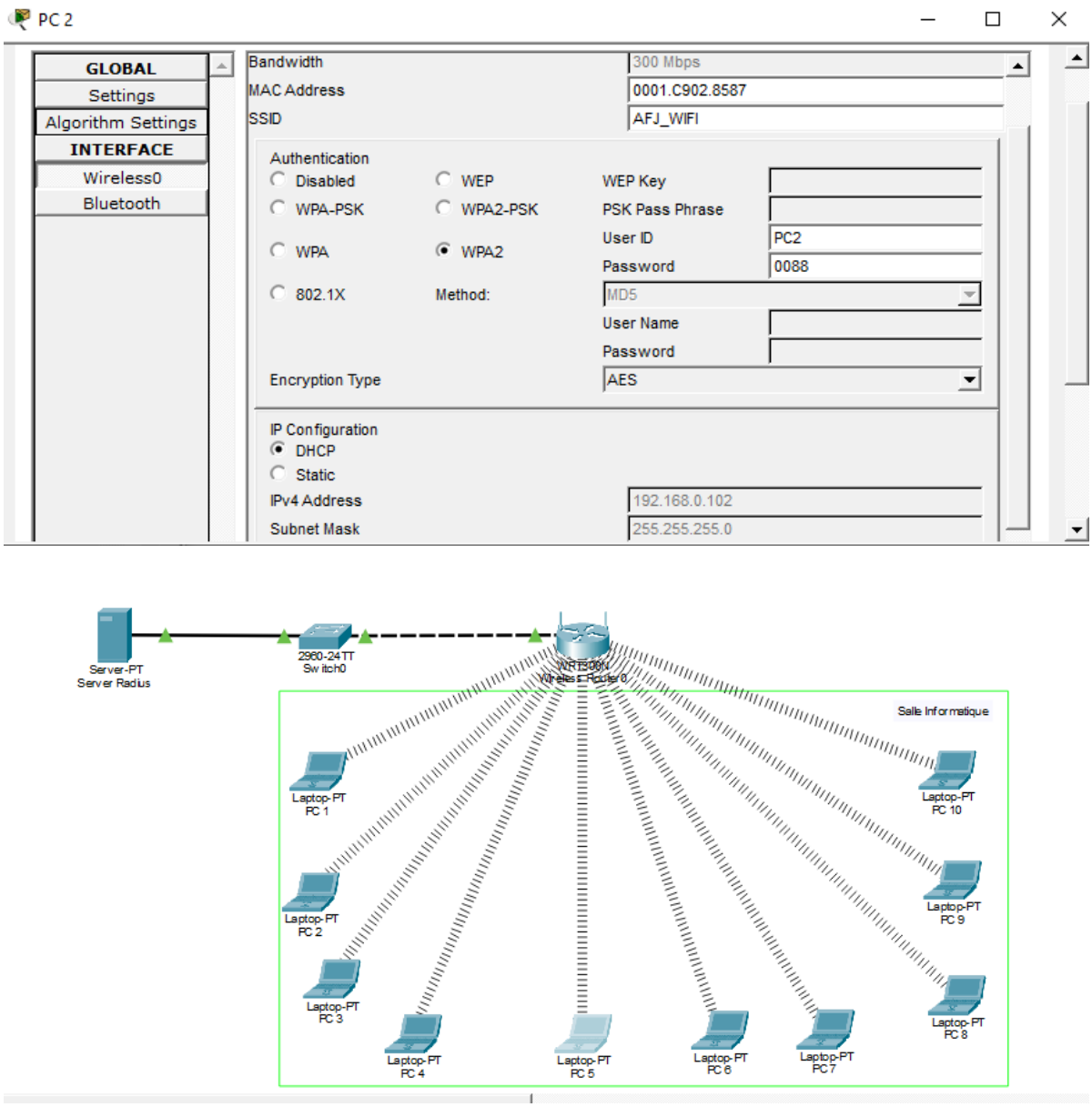


Figure 5-Apres la saisie des identifiants défini dans le serveur RADIUS