République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D' **I**NFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par
Malia TOUMI
Sabrina YAKER

Thème

ETUDE ET MISE EN PLACE D'UN RESEAU WIFI OUTDOOR

Mémoire soutenue publiquement le 04/07/2016 devant le jury composé de :

Mr MOHIA Yacine
Maitre conférence UMMTO, Président
Mr OUALOUCHE Fethi
Maitre conférence UMMTO, Encadreur
Mr LAZRI Mourad
Maitre conférence UMMTO, Examinateur
Mr HAMEG Slimane
Maitre assistant UMMTO, Examinateur

Promotion 2015/2016

Remerciements

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

Nous tenons à exprimer nos plus sincères remerciements à notre promoteur Mr. OUALOUCHE pour ses encouragements et ses orientations qui nous ont beaucoup aidées au cours de notre projet.

Un grand merci à notre Co-promoteur Mr. HADOUS Abdenour (Ingénieur du service réseau et maintenance de Algérie Telecom) qui nous a aidées tout au long du travail.

Nos remerciements les plus vifs s'adressent aussi à messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de Notre cycle universitaire.

Un grand merci également à nos familles et nos amis pour leurs aides considérables.

Dédicaces

Je dédie ce travail

- *A mes très chers parents, pour leurs sacrifices et leurs dévouements pour mon bonheur. Que Dieu les garde*
- *A mes chers frères et mes chères sœurs*
- *A ma grande sœur et son mari et mon cher neveu Mayas a qui je souhaite une longue vie*
- *A toute ma promotion Master II*
- *A tout mes amis (es)*
- *A tous ceux qui me sont chers*

MALIA

Dédicaces

A mes chers parents Qui m'ont tant donné pour faire de moi ce que je suis

A Mes sœurs : Lylia Et Cherifa

A mon frère : Athmane

A mes amis (es) et à tous ceux que j'aime

Je leur dédie ce modeste travail en guise de reconnaissance.

SABRINA

Sommaire

Sommaire

Sommaire

Sommaire

CHAPITRE III : étude et installation d'un AP wifi Outdoor

Sommaire

Sommaire

Glossaire

Glossaire

AP: Access Point.

AES: Advanced Encryption Standard.

BTS: Base Transceiver Station.

BSC: Base Station Controller.

BSS: Basic Service Set.

BDD: Base De Données.

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance.

DHCP: Dynamic Host Configuration Protocol.

DNS: Domain Name System.

DS: Distribution System.

DSSS: Direct Sequence Spread Spectrum.

ESS: Extended Service Set.

FTP: Foiled twisted pair.

FHSS: Frequency Hopping Spread Spectrum.

IEEE: Institute of Electrical and Electronic Engineers.

GSM: Global System for Mobile Communication.

GPRS: General Packet Radio Service.

IP: Internet Protocol.

IBSS: Independent Basic Service Set.

IDS: Intrusion Detection System.

IPS: Intrusion Prevention System.

LLC: Logical Link Control.

LTE: Long Term Evolution.

Glossaire

LOS: Line-of-sight.

MAC: Media Access Control.

MSC: Mobile Switching Center.

MIMO: Multiple-Input Multiple-Output.

NAS: Network Access Server.

NAT: Network Address Translation.

NLOS: Non-line-of-sight.

OSI: Open System Interconnection.

OFDM: Orthogonal Frequency Division Multiplexing.

PLCP: Physical Layer Convergence Protocol.

PMD: Physical Medium Dependant.

POE: Power over Ethernet.

RADIUS: Remote Authentication Dial-In User Service.

SSID: Service Set Identifier.

SSH: Secure Shell.

SSL: Secure Socket Layer.

UDP: User Datagram Protocol.

UTP: Unshielded twisted pair.

TKIP: Temporal Key Integrity Protocol.

UMTS: Universal Mobile Telecommunication System.

VPN: Virtual Private Network.

WEP: Wired Encryption Protocol.

WPA: Wifi Protected Access.

Wifi: Wireless Fidelity.

Glossaire

WiMAX: Worldwide Interoperability for Microwave Access.

WLAN: Wireless Local Area Network.

WMAN: Wireless Metropolitan Area Network.

WPAN: Wireless Personal Area Network.

WWAN: Wireless Wide Area Network.

Wici: Wifi ici.

WISP: Wireless Internet Service Providers.

Introduction

Introduction

Les réseaux informatiques sont devenus ces dernières années, des axes majeurs de communication. Aujourd'hui, les principaux développements de ces réseaux visent à favoriser la mobilité. Pour répondre aux nouveaux besoins des personnes, les différents acteurs dans le domaine des réseaux ont normalisé une nouvelle technologie qui est le Wifi. Celle-ci permet d'avoir une mobilité et d'assurer une compatibilité entre les différents fabricants. **[1]**

En plus de la mobilité, les utilisateurs des réseaux sans fil souhaitent se connecter à internet ou qu'ils aillent à tout moment et avec un très bon débit. Plusieurs technologies peuvent répondre à ce besoin (la 3G / 4G mobile, wimax) **[2],** mais ces dernière ont vite montré leurs limite en débit et en coût. Alors une nouvelle technologie qui allie fiabilité, sécurité et convivialité et offrant un débit appréciable a fait son apparition c'est le wifi outdoor.

Le Wifi Outdoor est un réseau qui permet d'accéder au haut débit à l'extérieur, c'est-à-dire dans la rue, les terrasses de cafés, les universités, les lieux publiques…etc. Pour se connecter à ce réseau, on peut utiliser n'importe quel équipement de connexion (ordinateur, Smartphone, tablette,...). À la différence du Wifi interne, le Wifi Outdoor sort de l'intérieur de l'entreprise pour couvrir un périmètre plus large. De ce fait, il facilite le quotidien des utilisateurs des technologies de communication. **[3]**

Dans le cadre de notre projet de fin d'étude, nous nous sommes intéressés à l'étude et la mise en place de la technologie WICI au niveau de la placette public Mbarek Ait Menguellet (ex gare routière) de Tizi-Ouzou. A cet effet, nous avons effectué un stage pratique au sein d'Algérie Telecom.

Nous avons structuré notre mémoire en trois chapitres:

Le premier chapitre présente des généralités sur les réseaux sans fil et les équipements utilisés lors d'installation d'un réseau sans fil.

Dans le deuxième chapitre, nous exposons le problème de la sécurité dans un réseau sans fil. Nous commençons par citer les attaques contre ce réseau puis nous énumérons les différentes solutions et protocoles proposées pour faire face à ces attaques.

Le troisième chapitre est consacré à la mise en service du réseau Wici. En premier lieu nous avons fait l'étude du site puis nous détaillons les étapes à suivre pour l'installation des équipements. Enfin, nous avons illustré la configuration du AP wifi outdoor et les différents tests.

Nous terminons ce présent mémoire par une conclusion générale et une bibliographie.

Chapitre I

Généralités sur les réseaux sans fil

1. Préambule

Un réseau sans fil (Wireless Network) est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce à ces réseaux, 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". Dans ce chapitre, nous allons présenter les notions de base d'un réseau sans fil ainsi que les différents types d'équipement utilisés.

2. Définition et avantages d'un réseau sans fil

Un réseau est un ensemble des nœuds reliés entre eux par des liens ou canaux de communication dans le but d'échanger des informations **[10].**

Selon le type des nœuds, on distingue : les réseaux de télécommunication dans lesquels les nœuds sont les stations mobiles, les stations de base (BTS), les contrôleurs des stations de base (BSC), les commutateurs (MSC) , et les réseaux informatiques dans lesquels les nœuds sont les ordinateurs, les imprimantes, les routeurs, les Switchs ou tout autre équipement informatique.

Selon le type de canaux de communication, on distingue : les réseaux filaires qui utilisent un canal de transmission matériel (le câble coaxial, les paires torsadées, la fibre optique) et les réseaux sans fils. Ces derniers, utilisent la propagation des ondes pour s'échanger des données. L'utilisation des réseaux sans fil procure plusieurs avantages, notamment :

- L'usage facile dans les endroits à câblage difficile.
- La réduction du temps de déploiement et d'installation.
- La réduction des coûts d'entretien.
- L'augmentation de la connectivité.
- La réduction de l'encombrement.
- La mobilité.

3. Techniques de transmission dans les réseaux sans fil

Il existe principalement deux méthodes pour la transmission dans les réseaux sans fil:

- **Transmission par ondes infrarouges**

La transmission par les ondes infrarouges nécessite que les appareils soient en face l'un des autres et aucun obstacle ne sépare l'émetteur du récepteur car la transmission est directionnelle. Cette technique est utilisée pour créer des petits réseaux de quelques dizaines de mètres. (Télécommande de : télévision, les jouets, ...) **[4].**

- **Transmission par ondes radios.**

La transmission par les ondes radios est utilisée pour la création des réseaux sans fil qui a une étendue de plusieurs kilomètres. Les ondes radios ont l'avantages de ne pas êtres arrêtés par les obstacles car sont émises d'une manière omnidirectionnelle. Le problème de cette technique est perturbations extérieurs qui peuvent affecter la communication à cause de l'utilisation de la même fréquence par exemple **[4].**

4. Classification des réseaux sans fil

4.1. Classification des réseaux selon le mode opératoire

En réseaux sans fil, on retrouve principalement deux modes opératoires :

- le mode infrastructure.
- le mode sans infrastructure (Ad hoc).

4.1.1. Mode infrastructure

Le mode infrastructure se base sur une station spéciale appelée Point d'Accès (AP). L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set). Chaque BSS est identifié par un BSSID (BSS Identifier) de 6 octets qui correspond à l'adresse MAC du AP. Cette architecture permet d'étendre les réseaux parce qu'elle permet à des terminaux de se connecter à n'importe quel réseau via un point d'accès.

C’est une architecture centralisée où toute communication doit passer par le AP même s’il s’agit d’une communication entre deux stations du même BSS.

Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution DS afin de constituer un ensemble de services étendu (Extended Service Set ou ESS).

Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil. Le figure ci-dessous présente deux point d’accès en mode infrastructure.

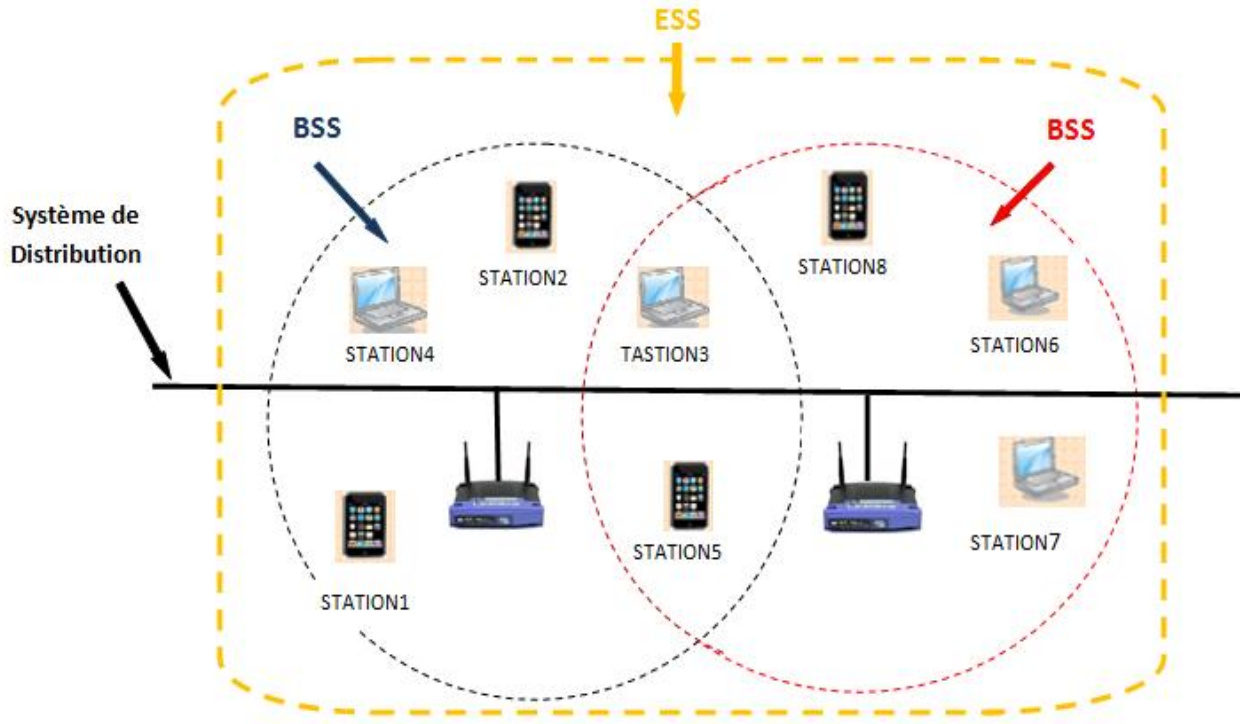

Figure 1 : mode infrastructure.

Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant comportant au maximum 32 caractères de long servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sorte un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès **[3].**

4.1.2. Mode ad hoc

En mode ad hoc les machines sans fils se connectent les unes aux autres afin de constituer un réseau point à point (Peer to Peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès.

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (Independant Basic Service Set : IBSS).

Un IBSS est ainsi un réseau sans fil, qui est constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure.

Dans un réseau ad hoc, la portée du IBSS est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations, par exemple dans la figure2 ci-dessous, la station1 peut seulement communiquer avec les stations2 et 3 mais pas avec la station4 car elle est hors de sa portée. Par contre la station3 peut communiquer avec toutes les stations car elles sont toutes à sa portée.

Contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi un IBSS est par définition un réseau sans fil restreint **[3].**

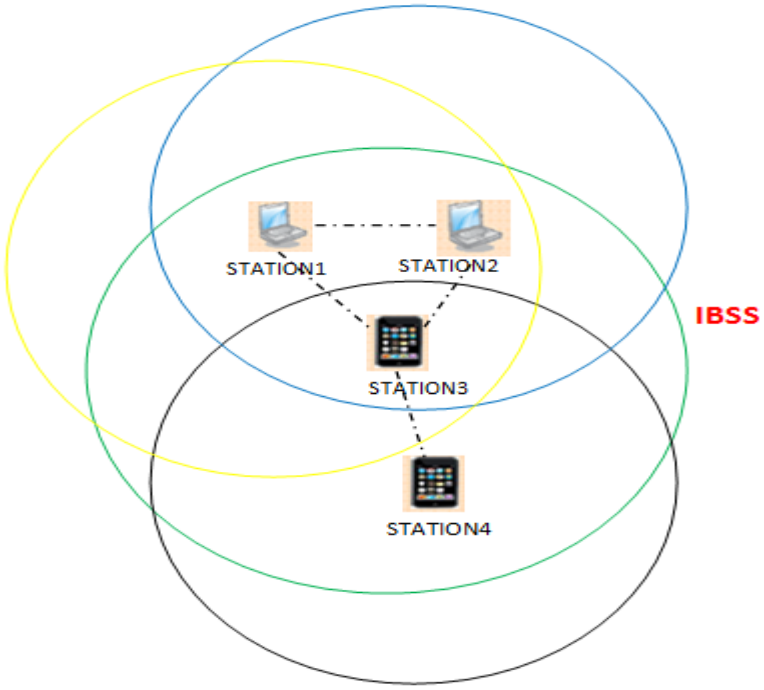

Figure 2 : Mode ad hoc

4.2. Classification des réseaux en fonction de la taille

De manière générale, les réseaux sans fils sont classés selon leur étendue géographique, en quatre catégories offrant une connexion (appelé Zone de couverture).

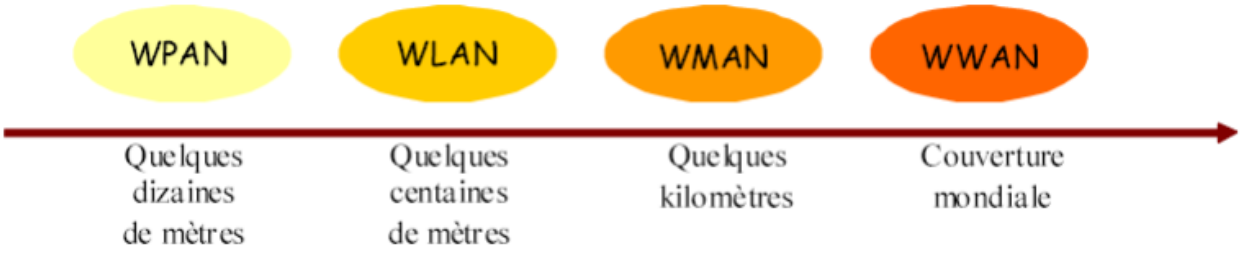

Figure 3 : Classification des réseaux sans fil suivant leur taille

4.2.1. Les WPAN (Wireless Personal Area Networks)

Dans cette catégorie, on retrouve 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...). On y trouve les standards tels que le Bluetooth, l'Ultra Wide Band (UWB), ZIGBEE, RFID et HomeRF.

4.2.2. Les WLAN (Wireless Local Area Networks)

C'est la catégorie 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 Wifi (Wireless Fidelity) et les HIPERLAN.

4.2.3. 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.

4.2.4. 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.

5. Présentation du wifi

5.1. Définition du wifi

L'appellation « Wifi » correspond à l'abréviation de l'expression anglaise Wireless Fidelity, c'est-à-dire « fiabilité du sans fil ». Il s'agit d'une technologie qui permet de transmettre des données numériques sans fil, via des ondes radio**.** Ces ondes sont diffusées sur différentes bandes de très hautes fréquences, dont notamment la bande de 2,4 GHz et la bande de 5 GHz.

Le Wifi repose sur des normes techniques définies, à partir de 1997, par l'association professionnelle IEEE, et correspond plus précisément à la norme IEEE 802.11 **[13]**. Cette dernière a pour objectif de déterminer les principales caractéristiques d'un réseau local sans fil ou « WLAN ».

5.2. Application du Wifi

Les applications du Wifi sont diverses et nombreuses. Il répond aux besoins d'un réseau d'entreprise Ethernet sans fil**.** La première application était donc d'étendre le réseau filaire existant.

Le Wifi s'est ensuite introduit dans les foyers chez le grand public. L'objectif derrière l'installation d'un réseau sans fil est de pouvoir se connecter à l'internet depuis n'importe quel endroit du domicile. Ce réseau semble adéquat parce qu'une seule borne Wifi suffit à couvrir un domicile de moins de 100 m².

La troisième utilisation concerne les hots pots. En effet, un hot spot est un point d'accès sans fil à Internet. D'un terminal mobile personnel, les utilisateurs peuvent se connecter et accéder à internet qu'ils soient dans un café, un hôtel, un aéroport, ou même une salle d'attente. Cette technologie a connu un essor remarquable dès son apparition. De ceci sont créés les WISP (Wireless Internet Service Providers) ou fournisseurs d'accès à internet sans fil **[9].**

5.3. La place du Wifi

Le Wifi a été conçu avant tout pour les réseaux locaux sans fil, les WLAN. Pour les autres usages, il a de sérieux concurrents.

La figure4 résume la place relative des différentes technologies selon deux axes : le débit et l'étendue du réseau.

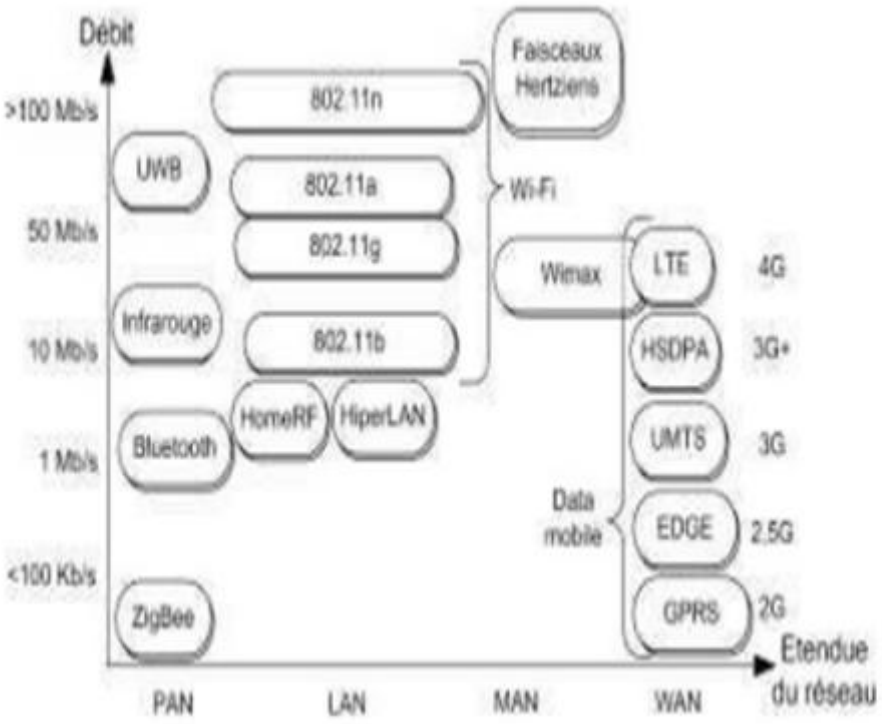

Figure 4: La place du Wifi parmi les autres technologies sans fil **[3].**

6. Les avantages et les inconvénients du Wifi

6.1. Les avantage

Comme les autres réseaux sans fil, le Wifi possède plusieurs avantages :

- **la facilité de déploiement** : un réseau Wifi peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- **le faible coût d'acquisition :** si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.
- **la mobilité** : les utilisateurs peuvent se déplacer sans couper la connexion au réseau.
- **la simplification de la gestion :** L'ajout de nouveaux élément ou le déplacement d'éléments existants peuvent être réalisés rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

De plus, le Wifi est interopérable avec les réseaux filaires existants et garantit une grande souplesse sur la topologie du réseau.

6.2. Les inconvénients

- **Qualité et continuité du signal :** ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.
- **Sécurité :** la sécurité des réseaux sans fil diffère selon les technologies et les équipements utilisés.

7. La technologie 802.11

7.1. Les couches de l'IEEE 802.11

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques **[3]:**

- **la couche liaison de données**, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC**).**
- **la couche physique** (notée couche PHY), constitué aussi de deux sous couche : PLCP et PMD.

Couche Liaison de données(MAC)	LLC
	MAC
Couche Physique(PHY)	PLCP
	PMD

Figure 5 : la technologie 802.11

7.1.1. La couche liaison de données

La couche de liaison de données du protocole 802.11est composée essentiellement de deux sous couches, LLC (Logical Link Control) et MAC.

La couche LLC utilise les mêmes propriétés que la couche LLC 802.2. il est de ce fait possible de relier un réseaux WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC quant à elle, est spécifique de l'IEEE 802.11.

Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre ou occupé, le terminal émet, sinon il se met en attente. Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre

7.1.2. La couche physique 802.11

La couche physique (couche 1 du modèle OSI) est chargée de gérer les connexions matérielles. Elle est divisée en deux parties: PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependant).
La sous couche PLCP concentre les fonctionnalités d'encodage des données, alors que la seconde sous couche PMD se charge de l'écoute de du support et fournit un service de signalisation à la couche MAC, en lui notifiant l'état du support : libre ou occupé.

La couche physique utilise plusieurs techniques de codage et de modulations

- Le FHSS (Frenquency Hopping Spread Spectrum).
- Le DSSS (Direct Sequence Spread Spectrum).
- OFDM (Orthogonal Frequency Division Multiplexing). **[6]**

7.2. Les principales améliorations du 802.11

Au fil des années, des améliorations importantes ont été apportées au standard 802.11. Certaines concernent la couche physique, d'autres concernent la couche MAC. Ces améliorations sont simplement désignées par une lettre rajoutée au nom du standard. Les principales améliorations concernant les couches physiques sont :

• **802.11a** : fréquence radio à 5 GHz au lieu de 2,4 GHz, modulation radio de type OFDM, débit maximal théorique de 54 Mb/s.

• **802.11b** : fréquence radio à 2,4 GHz, modulation DSSS ou HR-DSSS, débit maximal théorique de 11 Mb/s.

• **802.11g** : fréquence radio à 2,4 GHz, modulation DSSS, HR-DSSS ou OFDM, débit maximum théorique 54 Mb/s.

• **802.11n** : elle est disponible depuis le 11 septembre 2009. Compatible avec le 802.11a et le 802.11b/g, il permet, grâce à de nombreuses améliorations techniques telles que le MIMO (Multiple-Input Multiple-Output) et OFDM (Orthogonal Frequency Division Multiplexing d'atteindre des débits très élevés (> 100 Mb/s réels).

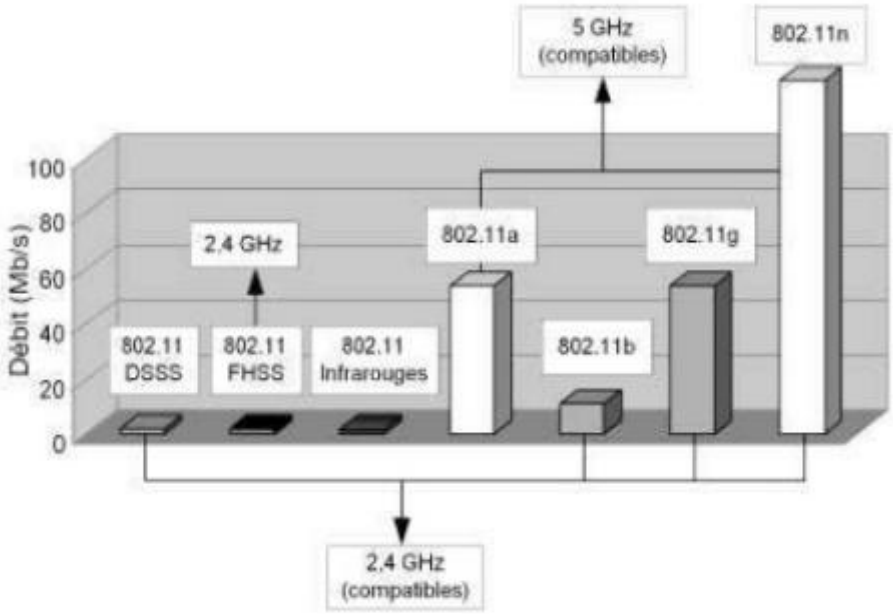

Figure 6 : les couches physiques du wifi (débit, fréquence et compatibilité) **[3].**

8. Les méthodes d'accès

La technique DCF pour l'accès au support de transmission constitue la technique d'acces par défaut. Elle permet la transmission de données en mode asynchrone et best-effort, sans aucune exigence de priorité. La technique DCF s'appuie sur le protocole CSMA/CA6. Dans ce qui suit, nous donnons les caractéristiques principales du protocole CSMA/CA, ainsi que le mécanisme de réservation du support hertzien.

8.1. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

La station voulant émettre écoute le réseau si le réseau est encombré, la transmission est différée. Dans le cas contraire (si le canal est libre pendant un temps donné DIFS : Distributed Inter Frame Sace). Alors la station peut émettre. La station commence par la transmission d'un message RTS (Read To Sen) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur lui répond par CTS (Cledar To Sen) le champ est libre pour émettre puis la station commence l'émission de

données. A la réception de toutes les données émises par la station le récepteur envoie un accusé de réception (ACK).

8.2. PCF (Point Coordination Fonction)

Le point coordination fonction appelé mode d'accès contrôlé. Elle est fondée sur l'interrogation à tour de rôle des stations ou pollings, contrôlée par le point d'accès. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour l'application à temps réelle nécessitant une gestion de délai lors de la transmission de données.

- La base (le point d'accès) contrôle tout le trafic : il n'y a jamais de collisions
- Elle interroge (Pol) les autres stations pour savoir si elles ont des trames à transmettre :
  - ✓ Envoi d'une trame de signalisation (Beacon frame) 10 à 100 fois par seconde.
  - ✓ Cette trame contient des informations système, des informations de synchronisation, etc.
  - ✓ Elle invite aussi les nouvelles stations à se faire connaitre pour rentrer dans la séquence de polling.

9. Le SSID

Le SSID est une abréviation de Service Set Identifier, un identificateur unique pour éviter les interférences sur un réseau sans fil, et il se réfère aussi à ESSID (Extended Service Set Identifier). Le SSID est une valeur de 32 bits ou moins et il est assigné au point d'accès. L'appareil réseau sans fil que vous désirez associer au réseau sans fil doit correspondre au point d'accès.

Le point d'accès et les appareils réseau sans fil envoient régulièrement des paquets d'informations appelées trames de balise, qui contiennent l'information SSID. Lorsque votre appareil réseau sans fil envoie une trame de balise, vous pouvez identifier le réseau sans fil qui est suffisamment proche des ondes radio afin de pouvoir atteindre votre appareil.

❖ **Communication entre un point d'accès et une station**

Voici les trois échanges requis entre une station est un AP pour communiquer:

• Le processus de sondage, ou probe.
• Le processus d'authentification.

• Le processus d'association.

Le processus de sondage, consiste généralement, à émettre une trame de requête probe sur chaque canal. Cette trame contient notamment des informations sur la station émettrice (les plus importantes sont les débits supportés (IE Supported Rates et l'ensemble de services auquel elle appartient (IE SSID)). Ce processus à pour but de permettre à la station de connaître les APs qui se trouvent à proximité.

Lorsque la station reçoit les trames de réponse probe des APs, elle peut, suivant la configuration, se connecter automatiquement à un AP ou alors attendre la décision de l'utilisateur de la station.

Le processus d'authentification est très important dans les WLAN, il permet de déterminer celui qui est autorisé à accéder au réseau. Le standard 802.11 possède deux modes différents: Open System et Shared Key. En résumé, la station envoie une requête d'authentification et l'AP lui renvoie une réponse d'authentification.

Le processus d'association autorise ou non un AP à assigner un port logique à la station sans fil. Il est initié par la station au moyen d'une trame de requête et se termine par une réponse de l'AP lui indiquant le succès ou l'échec.

10. les équipements wifi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil WIFI **[4]** :

10.1. Les adaptateurs sans fil ou carte d'accès :

Les adaptateurs sans fil ou cartes d'accès (en anglais Wireless adapters ou network interface Controller) : 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 **[8].**

- ✓ **La carte réseau sans fil PCI**

Dans un ordinateur de bureau, la carte est habituellement installée à l'intérieur de l'ordinateur, le plus généralement dans un des emplacements de PCI qui sont communs dans la tour ou les configurations de bureau de PC. Sur une carte sans fil, une antenne courte, environ 10cm (4

pouces) dépasse en dehors de l'ordinateur et peut être pivotée environ pour recevoir le meilleur signal.

- ✓ **La carte PCMCIA :**

Dans un ordinateur portable, la carte serait très probablement installée dans une des fentes de PCMCIA dans le coté de l'ordinateur portable. Sur une carte sans fil, environ 2cm (3/4 pouce) de la carte dépasse au delà de la fente pour agir en tant qu'antenne. Sur des ordinateurs d'Apple Macintosh, la carte d'aéroport est installée à l'intérieur de l'ordinateur et n'est pas évidente de l'extérieur.

- ✓ **La carte sans fil connecté à un port USB :**

Une troisième possibilité est de connecter la carte par l'intermédiaire d'un câble d'USB à l'ordinateur. Dans ce cas-ci, l'antenne sera sur la carte, qui peut être placée n'importe où que le câble d'USB lui permettra, qui pourrait être jusqu'à 5 mètres à partir de l'ordinateur. La carte est actionnée bien que le câble d'USB, ainsi aucune alimentation d'énergie supplémentaire ne soit exigée.

Figure 7: Les adaptateurs wifi

10.2. Les points d'accès

Les points d'accès (AP) sont le cœur d'un réseau sans fil de type Infrastructure. Ils gèrent de nombreuses fonctions telles que l'authentification et l'association des stations, ou encore l'acheminement des paquets Wifi entre les stations associées **[8].** D'autres fonctions sont optionnelles mais très fréquentes, par exemple :

- La gestion du hand-over: un utilisateur peut alors passer sans déconnexion d'un AP à un autre. Pour cela, les AP concernés doivent communiquer entre eux Via le système de distribution (DS) qui est le plus souvent un réseau filaire.
- Le filtrage des périphériques autorisés, en fonction de leur adresse MAC.
- Le cryptage des données échangées et l'authentification des périphériques grâce aux protocoles WEP, WPA ou WPA2.

Outdoor AP

Indoor AP

Figure 8: Points d'accès

10.3. Les antennes

Par définition, les antennes sont des dispositifs passifs utilisés pour transformer un signal électrique en ondes électromagnétiques se propageant dans l'espace libre.

Elles permettent aussi de rassembler les ondes électromagnétiques dans l'espace libre, et en les transformant en signaux électriques sur un conducteur.

Il existe principalement deux types d'antennes selon leur type d'utilisation:

- **une antenne omnidirectionnelle :** rayonne dans toutes les directions on les trouve en général sur tout type de matériel réseau Wifi grand public.

- **une antenne unidirectionnelle** : comme son nom l'indique, envoie le signal radio que dans une direction bien précise. Elles sont utilisées pour établir des liaisons point à point longue distance.

11. Les équipements d'interconnexion d'un réseau

11.1. Switch

C'est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permettent de créer des circuits virtuels. La commutation est l'un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage. Dans les réseaux locaux (LAN), il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur (hub). Il existe aussi des commutateurs pour tous les types de réseau en mode point à point.

Figure 9: Le Switch

11.2. Hub

Le hub est un répéteur qui transmet le signal sur plus d'un port d'entrée-sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet sur tous les autres ports. Il présente les mêmes inconvénients que le répéteur. Il assure en fonction annexe une auto-négociation du débit entre 10 et 100 Mbits/s, il est utilisé en extrémité du réseau et doit être couplé en un nombre maximum de 4 entre deux stations de travail

Figure 10: Le hub

11.3. Routeur

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter. Il transforme la connexion internet filaire en connexion sans fil.

11.4. Les Câbles

- **Fibre optique**

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestre et océanique de données. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux. Un réseau « large band » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'information. En permettant les communications à très longe distance et à des débits jusqu'alors impossible, les fibres optiques ont constitué l'un des éléments clef de la révolution des télécommunications optiques. Ses propriétés sont également exploitées dans le domaine des capteurs (température, pression, etc.) et dans l'imagerie.

Un nouveau type de fibre optique , fibres à cristaux photoniques, a également été mis au point ces dernières années, permettant des gains significatifs de performances dans le domaine du traitement optique de l'information par des techniques non linéaires, dans l'amplification optique ou bien encore dans la génération de super continus utilisables par exemple dans le diagnostic médical, dans les réseaux informatiques de type Ethernet, pour la relier à d'autres équipement, on peut utiliser un émetteur-récepteur**[6].**

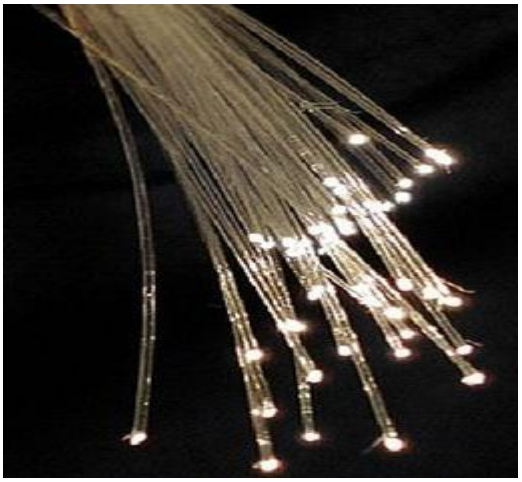

Figure 11: câble optique

- **FTP** (Foiled Twisted Pair) : Egalement d'impédance 100 ohms et écranté ; Il est constitué d'un simple feuillard d'aluminium enroulant les quatre paires torsadées protégées par une gaine externe.

Figure 12: câble FTP

- **UTP** : c'est une paire torsadée non blindé, elle n'est pas entourée d'un blindage protecteur.
- **paires torsadées**

Un câble paires torsadées décrit un modèle de câblage où une ligne de transmission est formée de deux conducteurs enroulés en hélice l'un autour de l'autre, cette configuration à pour but de maintenir précisément la distance entre les fils et de diminuer la diaphonie.

Le maintien de la distance entre fils de paire permet de définir une impédance caractéristique de la paire, afin de supprimer les réflexions de signaux aux raccords et en bout

de ligne. Les contraintes géométriques (épaisseur de l'isolant/diamètre du fil) maintiennent cette impédance autour de 100 ohm.

- 100 ohm pour les réseaux Ethernet en étoile
- 100 ou bien 120 ohm pour les réseaux de téléphonie
- 90 ohm pour les câbles USB.

Plus le nombre de torsades est important, plus la diaphonie est réduite. Le nombre de torsades moyen par mètre fait partie de la spécification du câble, mais chaque paire d'un câble est torsadée de manière légèrement différente pour éviter la diaphonie. L'utilisation de la signalisation différentielle symétrique permet de réduire davantage les interférences.

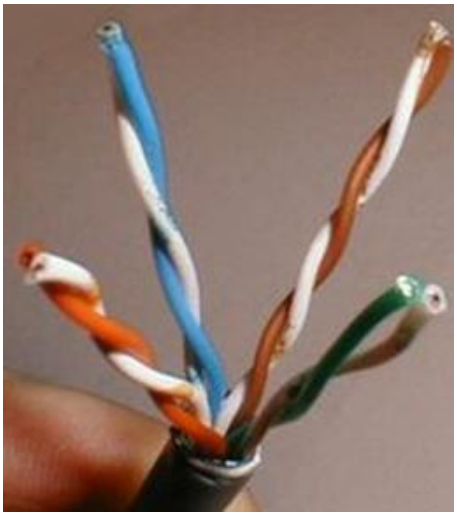

Figure 13: câble paires torsadées

12. Discussion

Dans ce chapitre nous avons présenté les réseaux sans fil, et le Wifi qui sont des technologies intéressantes et très utilisées dans de divers domaines comme l'industrie, la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation (absence de câblage), la disponibilité. Toutefois la sécurité dans ce domaine reste un sujet très délicat, car depuis l'utilisation de ce type de réseaux plusieurs failles ont été détectées.

Chapitre II

Protocoles et sécurité wifi

1. Préambule

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation.

L'objectif de la sécurité a toujours été globalement le même, à savoir préserver l'intégrité, la confidentialité et la disponibilité des ressources informatiques et réseaux. Pour atteindre cet objectif, plusieurs mécanismes de sécurité ont été développés tels que les mécanismes d'authentification, de chiffrement, de contrôle d'accès…

Dans ce chapitre nous commençons par étudier les différents serveurs et protocoles associés au Wifi (Serveur DHCP, RADIUS et les protocoles,….) en étalant leurs principes de fonctionnement, ensuite on va présenter quelques attaques et les solutions nécessaires pour protéger les réseaux sans fil.

2. Serveurs et protocoles

2.1. Serveur DHCP

Le serveur DHCP (Dynamic Host Configuration Protocol) permet la gestion et la distribution des adresses IP dynamiquement à un ordinateur sui se connecte sur un réseau, son but principal étant la simplification de l'administration d'un réseau.

2.1.1. Fonctionnement du protocole DHCP :

Il faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe.

Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.

Quand une machine démarre, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP.

Pour se faire, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va émettre un paquet de broadcast (broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion...) sur le réseau local.

Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast contenant toutes les informations requises pour le client.

Il existe plusieurs types de paquets DHCP susceptibles d'être émis soit par le client pour le serveur, soit par le serveur vers un client :

- **DHCPDISCOVER** : pour localiser les serveurs DHCP disponibles.
- **DHCPOFFER** : réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres.
- **DHCPREQUEST** : requête diverse du client pour par exemple prolonger son bail.
- **DHCPACK** : réponse du serveur qui contient des paramètres et l'adresse IP du client.
- **DHCPNAK** : réponse du serveur pour signaler au client que son bail a expiré ou si le client annonce une mauvaise configuration réseau.
- **DHCPDECLINE** : le client annonce au serveur que l'adresse est déjà utilisée.
- **DHCPRELEASE** : le client libère son adresse IP.
- **DHCPINFORM :** le client demande des paramètres locaux, il a déjà son adresse IP.

2.1.2. La sécurité du DHCP

Le DHCP a été construit directement sur le protocole UDP et le protocole IP (Internet Protocole), respectivement la couche Transport et la couche Réseau du modèle OSI. Ces deux protocoles (UDP et IP), n'étant pas sécurise à 100%, rendent donc le DHCP assez vulnérable et insécurisé.

Des serveurs DHCP non-autorisés peuvent être facilement montés. Des serveurs de ce genre pourraient envoyer de fausses informations aux clients, comme des adresses incorrectes ou déjà utilisées ou bien même des routes erronées, etc.

Un faux client DHCP pourrait se faire passer pour un vrai client et s'accaparer de toutes les ressources disponibles, rendant ainsi l'accès aux connexions, par les clients légitimes, impossible. Pour résoudre ce problème des faux clients, il est possible pour le serveur DHCP de se bâtir une liste de MAC adresse (adresse matérielle individuelle de chaque carte réseau existante), différente pour chaque carte de tous les ordinateurs ayant le droit d'être client DHCP sur ce serveur. Avant d'envoyer une adresse IP, le serveur vérifiera dans sa table pour voir si ce poste est éligible ou pas. L'adresse MAC, étant unique pour

chaque carte réseau, permet donc vraiment de contrôler les postes se connectant au serveur DHCP.

2.2. Le serveur RADIUS

Le protocole RADIUS acronyme de Remote Authentication Dial-In User Service est un protocole client- serveur qui repose principalement sur :

- ✓ un serveur (le serveur RADIUS), relié à une base d'identification (base de données).
- ✓ un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur.

L'ensemble des transactions entre le client RADIUS et le serveur RADIUS sont chiffrés et authentifiée grâce à un secret partagé.

L'identification effectuée par un serveur RADIUS est une vérification de nom d'utilisateur et de mot de passe.

Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée. Enfin, le client final qui se connecte au réseau envoie tout simplement sa demande au point d'accès. Il n'échange aucune donnée avec le serveur radius. Il envoie juste son identifiant et son mot de passe sur le réseau qui est relayé jusqu'au serveur**[3].**

Exemples d'utilisation de RADIUS représenté ci-dessus :

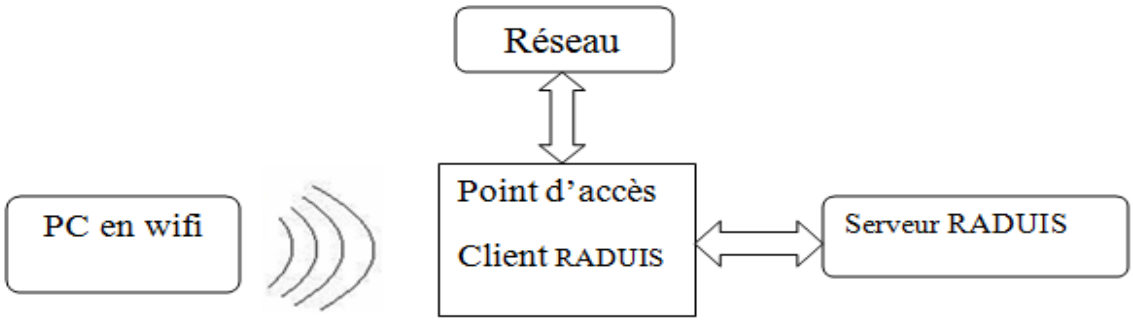

Figure 14: Utilisation de RADIUS

2.2.1. Format des paquets

Les données sont échangées entre un client et le serveur en paquets RADIUS. En fait, un paquet RADIUS est encapsulé dans un paquet UDP (User Datagram Protocole). Chaque paquet contient les informations suivantes :

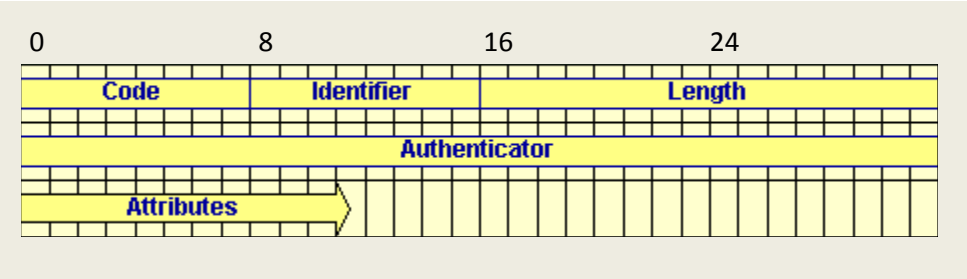

Figure 15: Format d'un paquet RADIUS

Signification des différents champs

Code : indique le type du paquet radius : Access- requet, Access-challenge, Access-accept, Access –reject, Accounting-requet ou Accourting-reponse.

Identifiant (ID) : est inclus dans chaque requête, il s'agit d'un simple compteur qui identifie le paquet. Ceci permet de savoir à quelle requête correspond une réponse radius (car avec le protocole UDP, l'ordre des paquets peut changer entre l'émetteur et le récepteur).

Longueur (lengh) : longueur de paquet en octets en comptant l'en-tête radius et les attributs.

Authentificateur (authentificator) : ce champ est très important du point de vue de la sécurité, il permet :

- Au client d'authentifier la réponse du serveur.
- De contrôler l'intégrité du paquet, pour s'assurer que ce dernier n'a pas été modifié par un pirate entre l'émetteur et le récepteur.
- De masquer le mot de passe en créant l'attribut user-password.

Les attributs (attributes) : ils constituent le principe le plus important du protocole radius. La bonne compréhension de leur signification et de leur rôle est indispensable pour tirer le meilleur parti de radius. Chaque attribut possède un numéro auxquelles est associé un nom, et leur valeur peut correspondre à l'un des types suivant :

- ✓ Adresse IP (4 octets).

- ✓ Date (4 octets).
- ✓ Chaine de caractères (jusqu'a 255 octets).
- ✓ Entier (4 octets).
- ✓ Valeur binaire (1 bit).
- ✓ Valeur parmi une liste des valeurs (4octets).

Le format de chaque attribut précise son type, sa longueur et sa valeur :

Type	Longueur	Valeur
1 octet	1octet	0 à 253 octets

Tableau 1 : les attributs du Protocol radius

2.2.2. Diagramme de séquence :

Ci-dessous un schéma d'un diagramme de séquence lorsqu'un utilisateur accède au réseau à travers un NAS (Network Access Server) et se déconnecte lui-même.

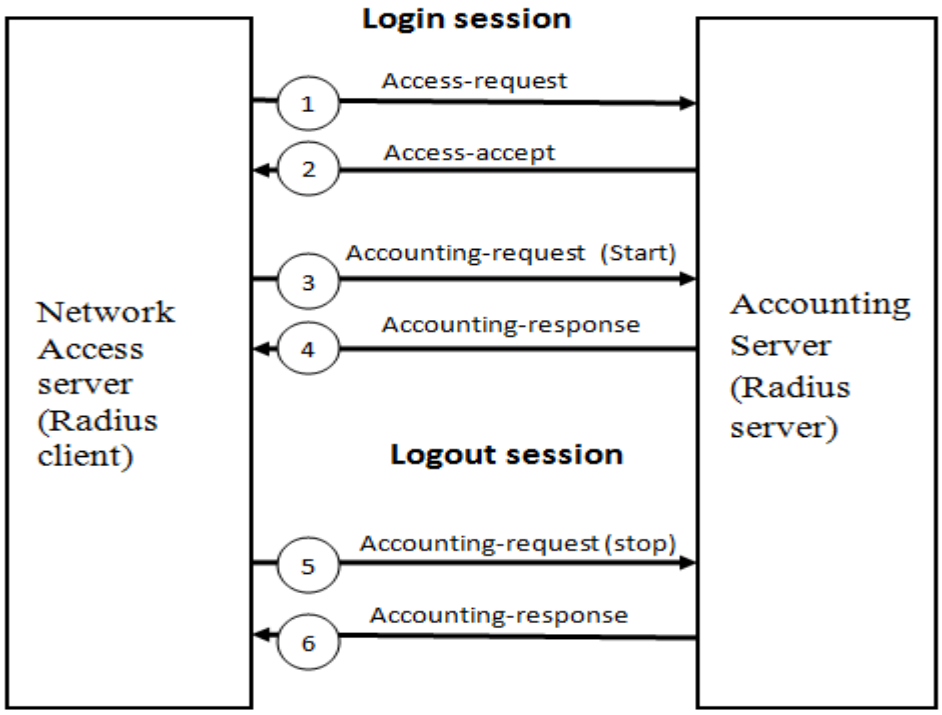

Figure 16: Flux de messages RADIUS.

1. Le NAS récupère le login/password d'un utilisateur à distance, crypte ces informations avec une clé partagée et envoie cela avec une "Access-request" à un serveur (phase Authentification).

2. Lorsque la combinaison login/password est valide, alors le serveur RADIUS envoie un message "accept-accept" avec des informations supplémentaires (par exemple : adresse IP, masque de réseau, etc.) au NAS (phase Autorisation).

3. Le NAS envoie un message "accounting-request (start)" pour indiquer que l'utilisateur est connecté sur le réseau (phase Comptabilité).

4. Le serveur RADIUS répond avec un message "Accounting-response" lorsque l'information de comptabilité est stockée.

5. Lorsqu'un utilisateur se déconnectera, le NAS va envoyer un message "Accounting-request (Stop)" avec les informations suivantes :

- Delay time, le temps d'essai d'envoi de ce message.
- Input octets, le nombre d'octets reçus par le client.
- Output octets, le nombre d'octets envoyés par le client.
- Session time, le nombre de secondes que le client s'est connecté.
- Input packets, le nombre de paquets reçus par le client.
- Output packets, le nombre de paquets envoyés par le client.
- Reason, la raison pour laquelle le client s'est déconnecté.

6. Le serveur RADIUS répond avec un message "accounting-response" lorsque l'information de comptabilité est stockée.

2.3. Le serveur DNS

Le service DNS« Domain Name System », permet de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques, il associe un nom à une adresse IP à chaque machine connectée au réseau.

Pour déployer un serveur DNS dans un réseau, il faut définir l'adresse du réseau. Pour des organisations désirant donner un accès public à leur domaine, il faut acheter un nom de domaine chez un prestataire de services tout en assurant son unicité sur internet. Dans un

réseau subdivisé en plusieurs sous réseaux, il doit y avoir un serveur DNS primaire par zone (sous réseau) et plusieurs serveurs secondaires sur lesquels on effectue des copies régulières des informations primaires pour des mesures de sécurité. Dans ce cas, une configuration des sous-domaines s'impose.

2.4. Le serveur NAT (Network Adresse Translation)

Le NAT permet de partager une connexion internet entre plusieurs ordinateurs sur un réseau local. En effet, les PC sur un réseau local ont des IP locales qui ne sont pas routables sur internet. De ce fait, le NAT est né afin de permettre à tous les PC d'un réseau de se connecter à internet à travers une seule adresse public.
En termes de sécurité, l'équipement (routeur, point d'accès) qui fait du NAT, n'accepte que les adresses IP qui ont été initialisées sur sa table. En effet, s'il ne retrouve pas vers quelle machine il doit envoyer la connexion, cette dernière sera éliminée du réseau. Cet équipement fait donc office de firewall pour le réseau local **[14].**

2.5. Les protocoles de sécurité

2.5.1. Le chiffrement

L'absence de chiffrement dans un réseau sans fil laisse l'ensemble des données qui transitent sur ce réseau à la merci d'une personne munie d'une carte Wifi et située dans le périmètre de réception des ondes émises par les autres équipements.
En raison de la propagation des ondes, il est nécessaire de protéger son réseau par un chiffrement approprié.

a. Le protocole WEP

Le WEP (Wired Equivalent Privacy) est Le protocole initialement proposé pour le chiffrement des communications entre éléments d'un réseau sans fil.

Le cryptage WEP fait partie de la norme 802.11 qui utilise le chiffrement par flot utilisant l'algorithme RC4 et nécessitant un secret partagé appelé clef.

Cette clef peut être de longueur 64 ou 128 bits (compte tenu de l'utilisation d'un vecteur d'initialisation de 24 bits, la longueur réelle de la clé est de 40 ou 104 bits) **[9].**

❖ **Principe de fonctionnement**

Le WEP est un protocole chargé de chiffrement des trames 802.11 utilisant l'algorithme symétriques rc4 avec des clés d'une longueur de 64 ou 128 bits.

Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 128 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé partagée par toutes les sessions est statique, c'est-à-dire que pour déployer un grand nombre de station wifi, il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications car tous les utilisateurs d'un réseau Wifi protégé avec le chiffrement WEP partagent la même clef WEP.

L'inconvénient de cette technique est que tout utilisateurpeut écouter les autres utilisateurs comme si aucun chiffrement n'était en place.

b. Protocole WPA/WPA2

Le WPA (Wifi Protected Access), respecte la norme 802.11i. Ce protocole permet de remédier aux faiblesses du chiffrement WEP.

Les données sont chiffrées de la même façon que pour le WEP mais le WPA utilise le protocole TKIP (Temporal Key Integrity Protocol) permettant de générer des clés différentes, et de les changer plusieurs fois par seconde.

Le WPA2 est à l'heure d'aujourd'hui, la méthode de cryptage la plus fiable, en effet, en plus du WPA, il inclut le chiffrement basé sur AES (Advanced Encryption Standard) qui est un algorithme de chiffrement symétrique. Le protocole précis utilisé par le WPA2 est CCMP.

❖ **Principe de fonctionnement**

La norme IEEE 802.11 définit deux modes de fonctionnement :

- **WPA personnel :** ce mode permet de mettre en œuvre une infrastructure sécurisée basée sur un WPA restreint sans serveur d'authentification.

  Il repose sur l'utilisation d'une clé partagée, appelée PSK, renseigné dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas

nécessaire de saisir une clé de longueur prédéfinie. Le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage **[9].**

- **WPA entreprise :** ce mode impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification généralement un serveur radius, qui permet d'identifier les utilisateurs sur les réseaux et de définir leurs droits d'accès, et d'un contrôleur réseau (point d'accès) **[9].**

2.5.2. Le protocole SSH

Le protocole SSH (Secure Shell) est un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante afin d'envoyer des commandes ou des fichiers de manière sécurisé :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (Spoofing).

2.5.3. Le protocole SSL

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.….).Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité. Le principe d'une authentification du serveur avec SSL est le suivant :

- Le navigateur du client fait une demande de transaction sécurisée au serveur.
- Suite à la requête du client, le serveur envoie son certificat au client.
- Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- Le client choisit l'algorithme.

- Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- Le navigateur vérifie que le certificat délivré est valide.
- Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

3. Les objectifs de la sécurité

Cinq types d'objectifs de sécurité sont définis :

- **La confidentialité des données** : les informations n'appartiennent pas à tout le monde, seule ceux qui en le droit peuvent y accéder.
- **L'authentification** : consiste à assurer que seules les personnes autorisées aient accès aux ressources.
- **L'intégrité** : les services et les informations (fichier, messages…) ne peuvent être modifié que par les personnes autorisées (administrateur, propriétaire…).
- **non-répudiation** : assure qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié.
- **La disponibilité :** les services (PC, réseaux,…) et les informations (donnés, fichier) doivent être accessibles aux personnes autorisées quand elles ont besoin **[5].**

4. Les attaques contre les réseaux wifi

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

4.1. L'interception de donnée

L'interception de donnée veut dire accéder illicitement au contenu d'un message. Il s'agit d'une attaque contre l'intégrité.

Initialement un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement

écouter toutes les communications circulant sur le réseau. Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

4.2. L'intrusion dans le réseau

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une occasion pour ce dernier dans le but de mener des attaques sur Internet.

4.3. Le brouillage radio

L'utilisation des ondes radio comme support de communication sont très sensibles aux interférences.

Un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes, par exemple, peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

4.4. Le déni de service

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets de données. Ces paquets peuvent demander la dissociation de cette station afin de perturber le fonctionnement du réseau sans fil.

De plus que la connexion à des réseaux sans fil est consommatrice d'énergie. L'envoi d'un grand nombre de données (chiffrées) par un pirate peut surcharger une machine. Comme tous les périphériques portables possèdent une autonomie limitée, donc un pirate peut provoquer une surconsommation d'énergie afin de rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie **[8].**

4.5. Le sniffing

Le sniffing est une technologie réseau permettant à un attaquant de compromettre la sécurité d'un réseau d'une manière passive **[11].**

Un « sniffer » est un outil matériel ou logiciel qui surveille, sans se faire repérer, un ordinateur du réseau en vue d'y trouver des informations susceptibles d'intéresser un attaquant.

Dans la plupart des cas, ces informations sont relatives à l'authentification des utilisateurs : couples nom d'utilisateur/mot de passe permettant l'accès à un système ou une ressource.

Un attaquant se place sur des points stratégiques comme la proximité d'une machine. Si le réseau est ouvert sur internet, l'attaquant intercepte les procédures d'authentifications entre deux réseaux.

Le résultat de ces attaques est la désorganisation des informations, la violation de la confidentialité et de l'intégrité des objets ou leur modification.

4.6. Le détournement d'adresse IP (spoofing IP)

C'est une technique utilisé en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Il permet de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper l'adresse IP d'une machine autorisée pour profiter de ses privilèges. Pour éviter ce genre d'attaques, il est recommandé de ne pas utiliser de service se basant sur l'adresse IP pour identifier les clients **[8].**

4.7. Faux point d'accès

Faux point d'accès crée pour permettre à l'attaquant d'effectuer une attaque man in the middle, ce faux point d'accès cible les réseaux qui n'utilisent pas une authentification mutuelle (client-serveur, serveur-client).

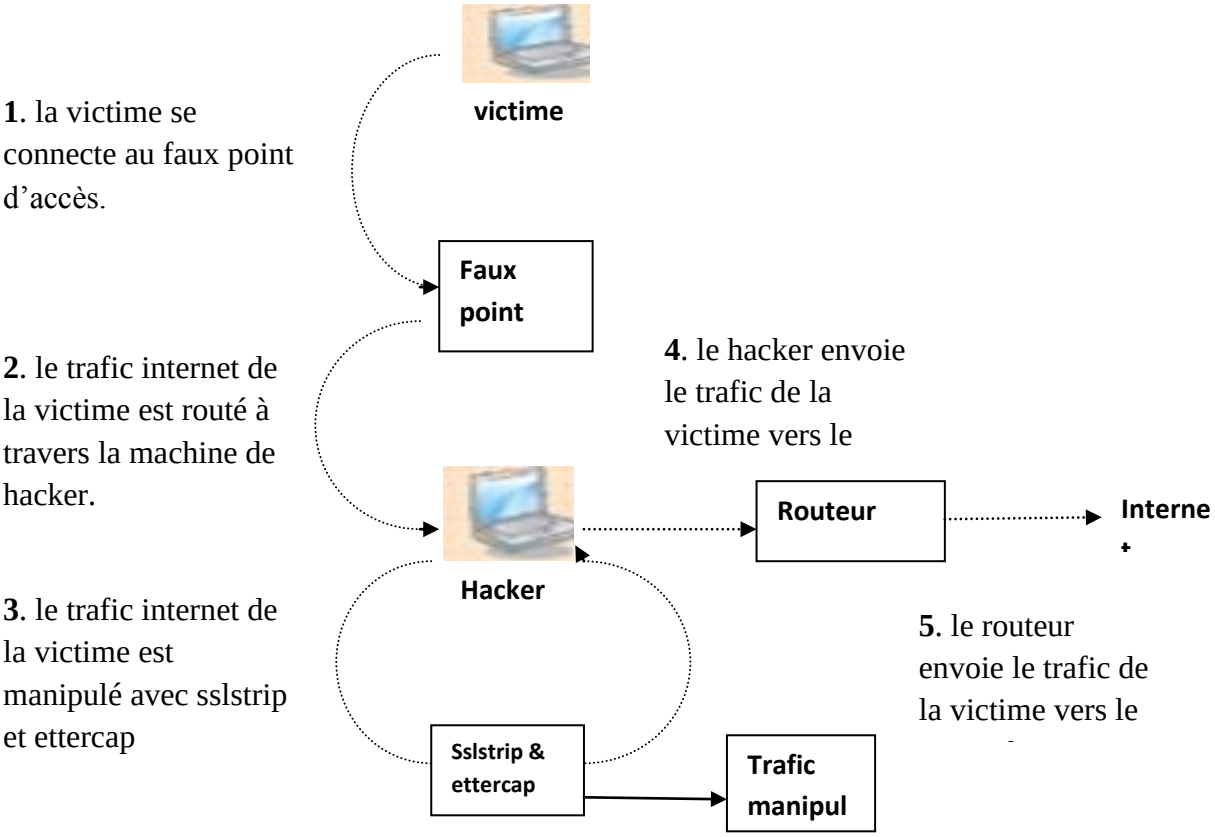

Figure 17 : représentation schématique de procédure du faux point d'accès **[16].**

La machine victime se connecte au faux point d'accès. Le trafic internet de cette dernière est routé à travers l'attaquant. Une fois obtenu, l'attaquant le manipule et le bloque en utilisant Ettercap et Sslstrip ce qui lui permettra de forcer la victime à utiliser http et par conséquent, il pourra capturer les noms d'utilisateurs et les mots de passe que la victime saisit. Une fois Ettercap et Sslstrip termine la manipulation et le blocage de trafic internet des victimes, l'attaquant redirigera la victime vers le routeur qui à son tour le redirigera vers le site web demandé.

En gros, l'attaquant se place entre la victime et le site web, ce qui lui permet d'intercepter les interactions entre ces derniers.

4.8. Attaque homme du milieu

Dans ce type d'attaque, le pirate (la machine malveillante) se place au milieu d'une communication pour intercepter ou modifier les informations.

Les points sensibles permettant cette technique sont :

DHCP : ce protocole n'est pas sécurisé.

Un pirate peut fournir à une machine victime des paramètres réseaux qu'ils contrôlent.

ARP : si le pirate est dans le même sous réseau que la victime, il peut envoyer régulièrement des paquets ARP signalent un changement d'adresse MAC aux extrémités.

5. Les méthodes de sécurité

5.1. La sécurité élémentaire :

Elles permettent uniquement de résoudre le problème du contrôle d'accès. Il s'agit de trois techniques qui peuvent éventuellement être utilisées de façon complémentaire

5.1.1. L'identificateur de réseau :

Il s'agit de l'ESSID (Extended Service Set Identifier), souvent appelé SSID que l'utilisateur doit connaître pour se connecter au réseau. Cette protection est en fait très sommaire, vus que les points d'accès envoient périodiquement et en clair le SSID dans les trames balises. Il suffit d'une simple écoute du réseau pour obtenir le SSID.

5.1.2. Le mot de passe

Pour se connecter au réseau, l'utilisateur doit donner le mot de passe. Cette protection est également très simpliste. Il est facile pour un intrus de capturer le mot de passe et de l'utiliser par la suite pour se connecter au réseau.

5.1.3. La protection par adresse MAC

Chaque adaptateur réseau possède une adresse physique unique appelée adresse MAC, représentée par douze chiffres hexadécimaux.

Les points d'accès permettent généralement dans leur interface de configuration, de gérer une liste de droits d'accès basée sur les adresses MAC des équipements autorisés à se connecter

au réseau. Le filtrage MAC peut aussi être contourné. Une écoute passive du réseau permet de récupérer les adresses MAC reconnues par le réseau.

5.1.4. Réglage de la puissance d'émission

Il est recommandé de pouvoir adapter la puissance d'émission de chaque point d'accès afin qu'il puisse diffuser une fréquence radio sans perturber son environnement et éventuellement les autres points d'accès.

5.2. Sécurité renforcé

5.2.1. Mise en place d'un pare-feu

Un pare-feu(en anglais firewall), est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.

Il a pour principale tâche de contrôler le trafic entre différentes zones en filtrant les flux de données entrant et sortant son but est de fournir une connectivité contrôlée et maîtrisée entre des zones différents.

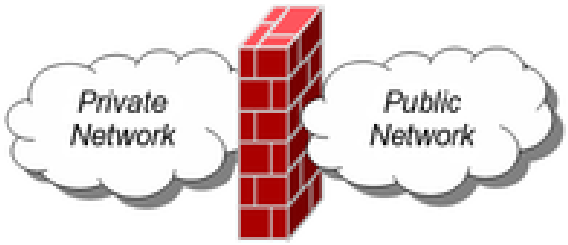

Figure 18: un pare-feu représenté par un mur de brique séparant le réseau privé du réseau public.

5.2.2. Utilisation des IDS/IPS :

Systèmes de détection d'intrusion et systèmes de détection et de prévention de l'intrusion, fournissent un complément technologique aux firewalls en leur permettant une analyse plus intelligente du trafic

5.2.3. Mise en place d'un VPN (Virtual Private Network)

Le VPN permet de simuler un réseau privé via internet en cryptant les paquets entre deux points distant une fois que le tunnel est crée à travers le réseau public (internet), entre deux machines (réseaux), ces derniers peuvent s'échanger des données de manière sécurisé, comme s'ils se trouvaient sur le même réseau local.

Le VPN permet aux entreprises de bénéficier d'une liaison sécurisée à moindre coût. Ils peuvent aussi utiliser les lignes spécialisées pour créer le VPN.

5.2.4. Le cryptage

La cryptographie est une méthode permettant de rendre illisible les informations, afin de garantir l'accès au distributeur authentifié uniquement. On distingue deux types de cryptage :

- **Cryptage symétrique :** appelé aussi cryptage à clé secrète. Ce type de cryptage utilise la même clé pour crypter et décrypter le message.

Le principal problème de cette technique est la distribution de la clé dans un réseau.

- **Cryptage asymétrique :** ce type de cryptage utilise deux clés différentes, une privée et n'est connue que de son propriétaire et une autre public et accessible par tout le monde.

Les deux clés (privé et public) sont liées par l'algorithme de cryptage utilisé.

Un message crypté par une clé publique ne peut être décrypté qu'avec la clé privé correspondante.

Le principal avantage de cette technique est de résoudre le problème de l'envoi de clé privé sur le réseau.

5.2.5. Portail captif

Un portail captif est un pare-feu dont le but est d'intercepter les usagers d'un réseau de consultation afin de leur présenter une page web spéciale avant de les laisser accéder à Internet.

Le portail captif assure le contrôle d'accès et l'authentification des utilisateurs grâces aux adresses IP et MAC.

La configuration utilisateur d'un portail captif est simple : l'utilisateur n'a qua ouvrir son navigateur et à se laisser guider **[12].**

❖ **Fonctionnement général d'un portail captif**

Un portail captif est composé :

✓ d'un firewall avec mise à jour dynamique des règles de filtrage.

✓ d'une base de données servant à l'authentification des utilisateurs.

✓ d'un serveur web.

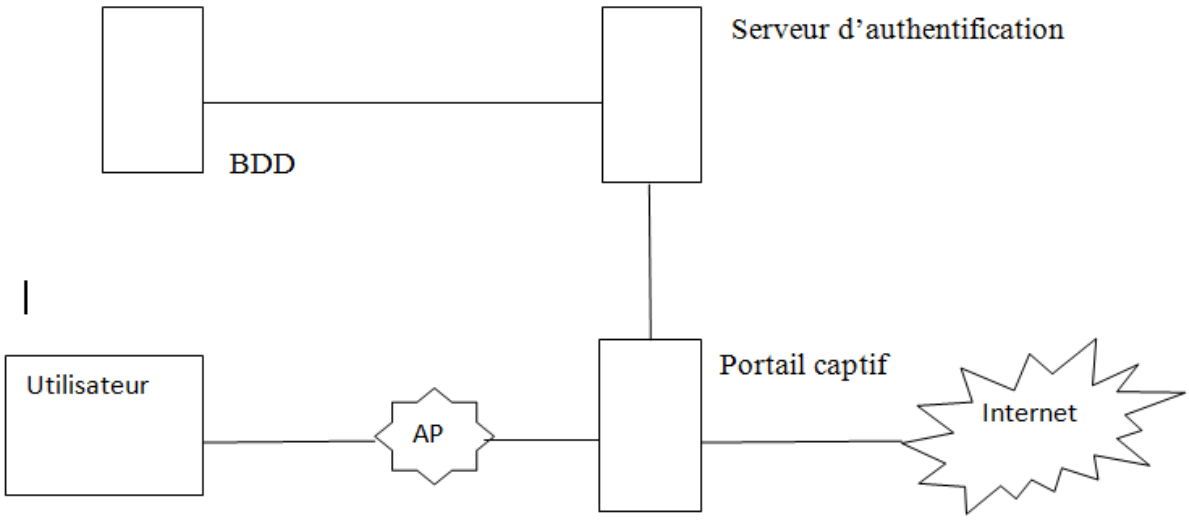

Figure 19 : portail captif

Voici comment fonctionne un portail captif :

1- redirection : lorsqu'un utilisateur s'associe au point d'accès wi-fi (AP), il est immédiatement attaché à un serveur DHCP qui lui attribue une adresse IP. Tout autre accès est bloqué par le portail. Quand l'utilisateur lance son navigateur, celui-ci est réorienté vers le service du portail captif qui le dirige, via http, sur la page du système d'authentification.

2- autorisation : une fois que l'utilisateur s'est correctement authentifié, le système d'authentification envoie un message au portail captif pour lui signaler que cet utilisateur est autorisé à accéder au service. Suite à ce message, le portail captif met à jour les règles du firewall afin d'autoriser les requêtes issues du couples adresse IP/adresse MAC de l'utilisateur authentifié.

3-connexion : l'utilisateur peut désormais accéder à internet.

4-fin de connexion : l'utilisateur peut prévenir le portail captif par l'intermédiaire d'une page de déconnexion **[12].**

6. Discussion

Malgré les problèmes de sécurité, les réseaux sans fil continueront de se développer. Il est donc important de bien connaître les problèmes liés à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes. Il est également important de déterminer le niveau de sécurité souhaité afin de mettre en place une solution en adéquation avec ce choix.

Chapitre III

Installation et configuration d'un réseau Wici

1. Préambule

Le Wici est le nom du Wifi Outdoor commercialisé par Algérie Télécom. Ce standard utilise la bande de fréquences 2.4 GHz et nécessite un espace dépourvu d'obstacle entre l'émetteur et le récepteur. Sa capacité de transmission est de 100 Mbit/s pour un rayon de 1.5 km théoriquement. Mais, dans la pratique, le point d'accès utilisé a une bande passante de 54 Mbit/s et une portée maximale de 400 m.

Dans cette partie nous allons présenter la méthodologie d'installation et de configuration du réseau sans fil Outdoor (Wici), pour couvrir la placette public Mbarek Ait Menguellet qui se trouve à la ville de Tizi-Ouzou.

2. L'étude du site

Le choix d'un bon endroit où placer les AP repose sur les points suivants :

- La planification : sert à déterminer le meilleur emplacement de l'antenne pour être placée à l'extérieur, il faut éviter les couloirs et les portes qui réduisent la portée et créent des interférences en opposition de phase (plusieurs répliques du même signal). Et les obstacles (murs en bétons armés) pour assurer une meilleure diffusion du champ radio afin d'obtenir une bonne couverture du site.
- Avoir une autorisation du ministère de la défense pour installer les différents équipements. Le but étant de ne pas brouiller ou induire en erreur certains radars de l'armée.
- Avoir une visibilité directe en positionnant l'antenne vers un lieu fréquenté par les personnes (la placette).
- Il est préférable de choisir un endroit équipé de fibre optique afin d'éviter de perdre du temps dans les grands travaux d'aménagement.
- Le nombre d'utilisateurs prévus.

2. Présentation de site

En tenant compte de tous les paramètres précédents, le choix s'est porté sur la couverture de la placette Mbarek Ait Menguellet (ex gare routière). Ainsi, l'endroit le plus indiqué pour installer le AP est le toit de la D.G de l'ENIEM. L'image suivante montre la zone couverte et le positionnement des AP.

Figure 20: la zone couverte par le wici.

1. L'installation physique du réseau wifi outdoor

L'architecture globale de ce réseau est représentée par la figure ci-dessous.

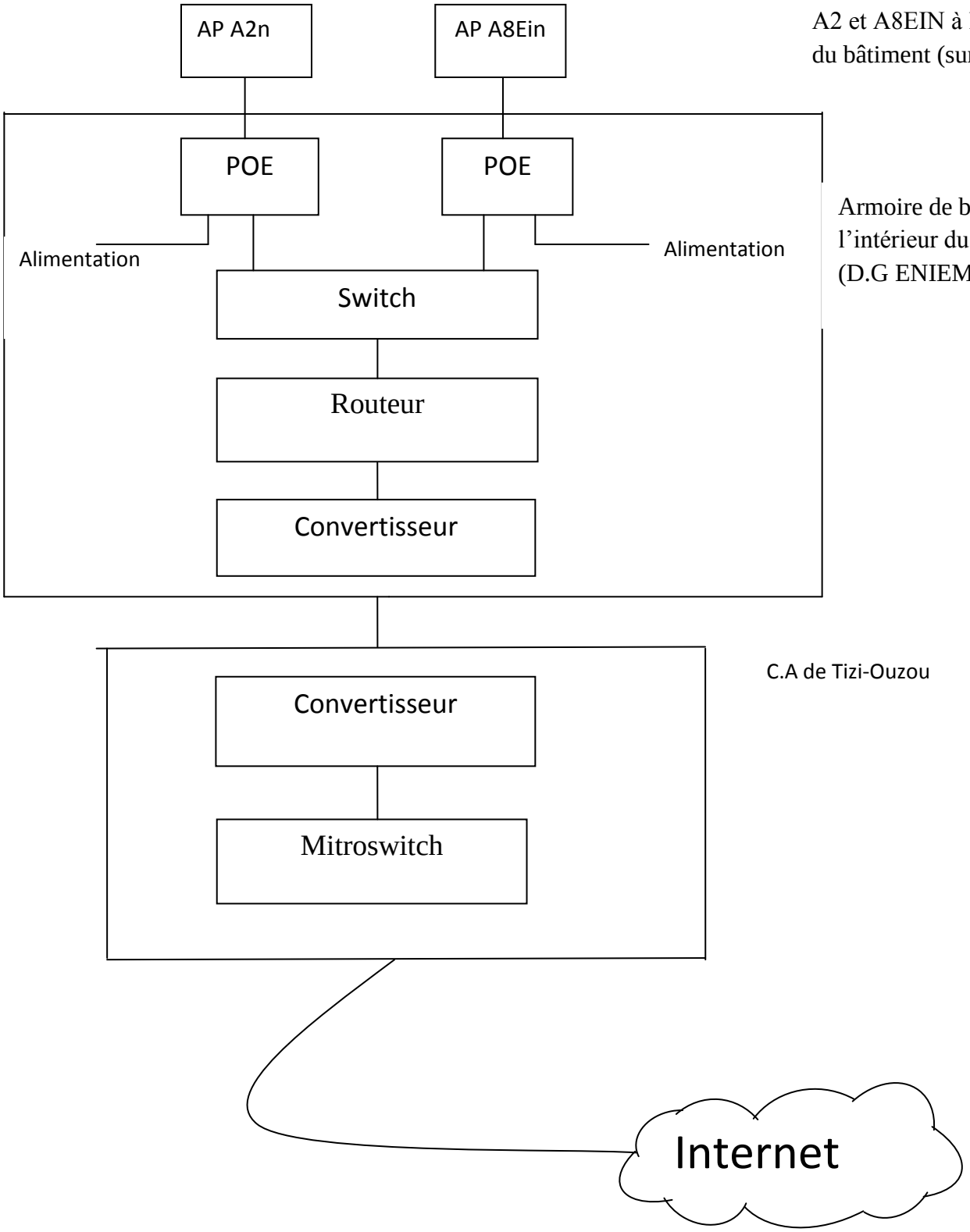

Figure 21 : Architecture globale du wifi outdoor de Tizi-Ouzou

5. Le matériel utilisé pour l'installation

Afin de pouvoir couvrir toute la zone désirée, on a choisi le matériel nécessaire pour notre projet, le tableau suivant contient les équipements et la quantité nécessaire.

Equipements	**Quantité**
Borne WIFI A8-Ein	1
Borne wifi A2n	1
Routeur	1
Injecteur avec adaptateur 48v	2
Switch 24 ports TP-Link	1
Convertisseur FO/FE	2
Armoire de brasage telesystème 9	1
Plateau fixe	1
Bande d'alimentation 08p	1
Cordon de brassage	3
Câble FTP CAT6	100 mètres
Gaine à ressort	60 mètres
Onduleur 1kva	1
Mat d'antenne 3m	1

Tableau 2 : les équipements d'AP wifi outdoor

5.1. Les points d'accès

On a utilisée deux points d'accès, A8-Ein d'une couverture wifi avec un angle de 70° et A2n d'un angle de couverture de 360°.

5.1.1. Point d'accès ALTAI A8-Ein

Le A8-Ein est une station de base multi-radio. Il fournit la meilleure couverture sectorielle par station de base, en particulier dans les environnements non-Line-of-Sight (NLOS). Le réseau d'antennes multifaisceaux de l'A8-Ein est conçu pour fournir une couverture de 5 à 10 fois que celle d'un point d'accès Outdoor standard **[15].**

Le A8-Ein permet d'avoir une couverture plus large et une bande passante plus grande par point d'accès, avec un coût de déploiement plus faible.

La portée de notre antenne dépasse les 400m. Nous nous sommes limités à cette distance car au delà, des pertes de débit apparaissent.

Figure 22: borne wifi ALTAI A8-Ein

- **Caractéristiques de l'antenne de A8-Ein**

A8-Ein	Caractéristiques
LOS/CPE	4000 m
LOS Laptops/Smartphones	1700 m
NLOS Laptops/Smartphones	800 m
LOS Backhaul	10 km

Tableau 3 : caractéristique de point d'accès A8-EIN

5.1.2. Point d'accès ALTAI A2n

Le point d'accès Wifi A2 d'ALTAI est conçu pour être utilisé dans les systèmes Wifi pour les zones de grande densité et pour couvrir les zones où le signal est faible ou inexistant à cause des obstacles. En effet, le A2 ne peut pas être seulement utilisé pour la couverture Wifi mais aussi pour assurer l'interconnexion point-a-point entre deux sites distants.

Figure 23 : point d'accès ALTAI A2n

❖ **Caractéristique de l'antenne de A2n**

A2n	Caractéristiques
LOS Backhaul	12Km
NLOS	450m
Débit	300Mbps

Tableau 4 : caractéristique de point d'accès A2n.

5.1.3. Caractéristiques générales et modes de fonctionnement des points d'accès A2n et A8-Ein.

a. Caractéristiques générales

- équipement robuste qui supporte les intempéries (placé à l'extérieur).
- tout équipement informatique muni d'une carte réseau sans fil peut s'y connecter (pc portable, tablette, téléphone portable,…).

- permet le contrôle à distance (exemple : coupure en cas d'interférence).
- supporte jusqu'à 256 clients.
- réglage de débit de 1 Mbps- 54 Mbps et de la portée.
- sécurisé selon plusieurs possibilités (mot de passe, filtrage adresse mac, WEP, WPA2/PSK, DHCP,…).

b. Mode de fonctionnement

Ils peuvent fonctionner selon 3 modes différents :

- mode AP : utilise la fréquence 2.4 GHZ pour diffuser le signal vers les utilisateurs.
- mode bridge : utilise la fréquence 5 GHZ pour diffuser le signal vers un autre point d'accès.
- Mode répéteur : régénère le signal issu d'un point d'accès afin d'étendre la distance du réseau.

5.2. Le câblage

Nous avons utilisé deux types de câbles qui sont présentés ci-dessous, dans le but d'interconnecter les différents équipements.

5.2.1. Câble paire torsadé FTP (Foiled Twisted Pair)

Le câble FTP est utilisé pour l'interconnexion des points d'accès avec le Switch. Ce câble appartient à la catégorie 6 (blinder). Il permet la transmission de données à des fréquences jusqu'à 500 MHz et à des débits théoriques de 1 Gb/s.

Il est caractérisé par une longueur maximale de 100 m et un débit maximal de 100 Mb/s.

5.2.2. Câble fibre optique

Ce câble à fibre optique est utilisé pour l'interconnexion du point d'accès wifi Outdoor de la placette au centre d'amplification de Tizi-Ouzou.

5.3. Le Switch TP-LINK

C'est un dispositif qui possède 24 ports d'interfaces 10/100/100Base-T type RJ-45, il est utilisé pour interconnecter les 2 bornes wifi (A8Ein etA2) avec le routeur

5.4. Routeur

C'est un équipement qui permet de relier plusieurs réseaux entre eux, il est utilisé dont notre projet pour relier le Switch avec le métro-switch qui se trouve au niveau de centre d'Amplification d'Algérie Telecom.

Figure 24: switch 24 port TP-LINK

5.5. Convertisseur FO/FE TP- Link

On a utilisé deux convertisseurs optiques, le 1^{ér} est placé au niveau du C.A et le 2^{éme} dans l'armoire de brassage dans le but de convertir le lien optique entre le site (ex gare) et le centre d'Amplification d'Algérie Telecom en faste Ethernet, pour que notre lien de transmission soit adapté avec le routeur utilisé.

TP-LINK est un convertisseur d'interface Ethernet pour fibre optique 62,5/125 µm ou 50/125 µm, qui a :

- 1 connecteur RJ45 UTP Ethernet10/100 jusqu'à 200 Mbps.
- 1 connecteur optique (double avec 1 transmission + 1 réception) de type SC.

Figure 25 : convertisseur TP-Link

5.6. Injecteur POE

C'est un dispositif avec une alimentation interne afin de réduire des lignes électriques encombrantes et la gestion de prises électriques. Le produit s'intègre au réseau d'origine pour distribuer du courant et des données au dispositif à distance à travers d'un câble Ethernet standard existant.

Figure 26 :injecteur TP-Link

5.7. Onduleur

L'onduleur est de conception Line Interactive, incluant la technologie de régulation automatique de tension. Il protège des variations de tension du réseau électrique en augmentant ou diminuant la tension au niveau requis par les équipements connectés. Ainsi l'onduleur augmente la durée de vie de ses batteries en restant connecté un maximum de temps au secteur avant de passer en mode secours.

Ce type d'onduleurs sont conçus pour :

- Les serveurs
- Les armoires réseau
- Les matériels réseaux critiques

Figure 27 : onduleur

5.8. Armoire de brassages

On a utilisé une armoire de brassage de marque TELESYSTEM 9U qu'on a fixé au mur à l'intérieur de bâtiment de l'entreprise ENIEM.

.

Figure 28 : l'armoire de brassage.

6. Installation des points d'accès A8Ein et A2n

6.1.Préparation des équipements

Avant la connexion des différents équipements, nous avons préparés la base de données de leurs configurations. Puis nous avons vérifié leur bon fonctionnement.

Nous avons aussi préparé les différents câbles à utiliser et les outils nécessaires à l'installation.

6.2. La position des points d'accès

Les points d'accès doivent être montées sur le bord du toit, alors nous avons choisi d'installer le point d'accès sur le bord du toit de la direction générale de l'ENIEM qui est un endroit mieux protégé (loin de la portée du public).

Figure 29 : Le AP est placé sur le toit de D.G.ENIEM

Il faut monter la barre au point de la zone de couverture plus élevé, et installez le 1m de pôle dessus de tout obstacle devant.

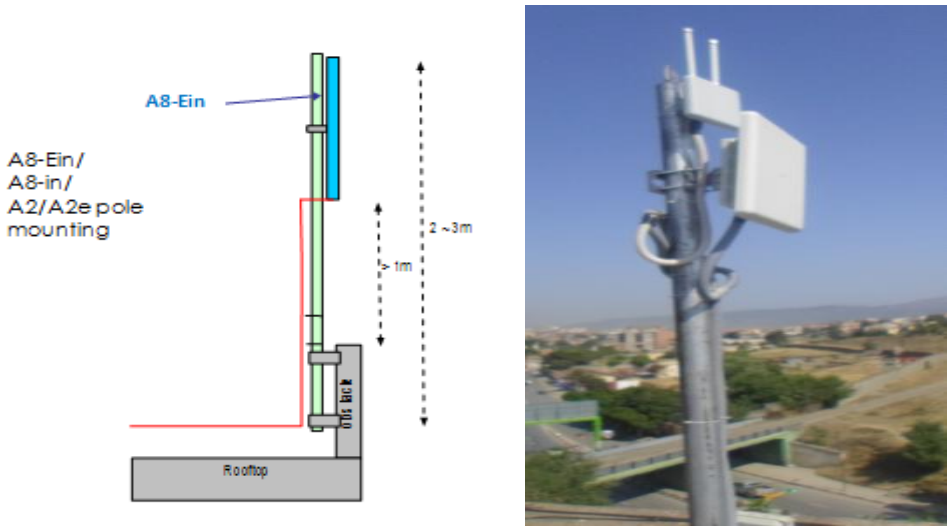

Figure 30 : A8Ein et A2 installés sur le mat.

Il faut éviter d'installer A8-Ein près d'autres systèmes radio**,** mais si ce n'est pas possible on va respecter les différentes distances comme indiqué par la figure 31.

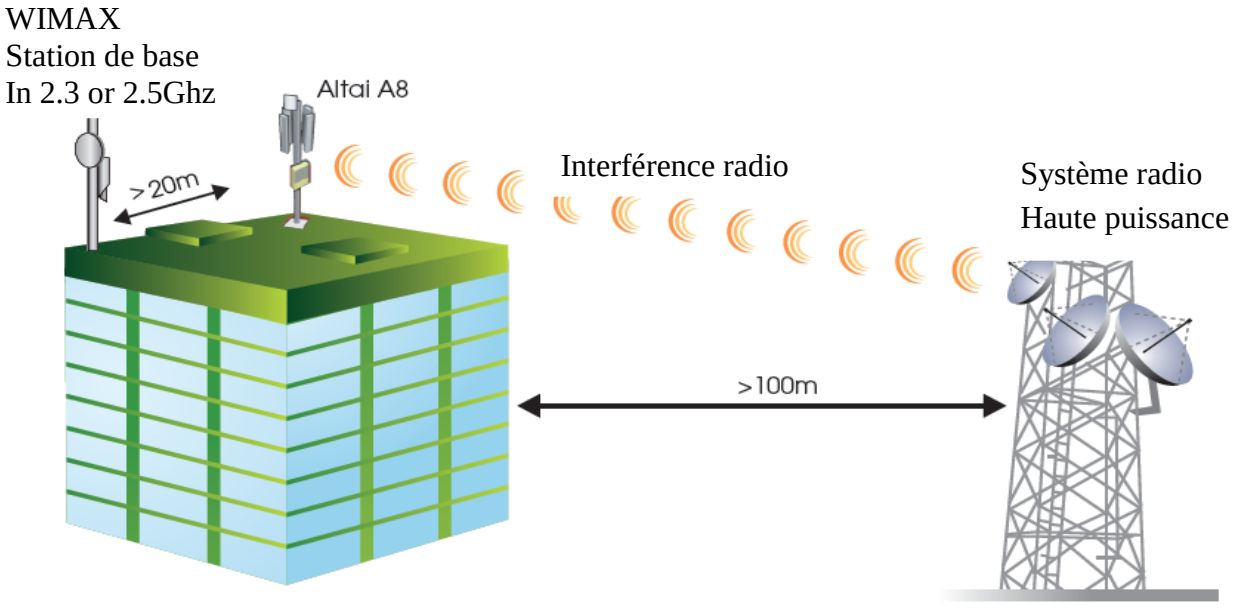

Figure 31 : distance entre le AP A8Ein et d'autres systèmes radio.

6.3. Procédure d'installation du point d'accès A8-Ein

Nous avons commencé par fixer le kit de montage, ensuite nous avons installé le point d'accès A8Ein et appliqué l'étanchéité sur les ports externes.

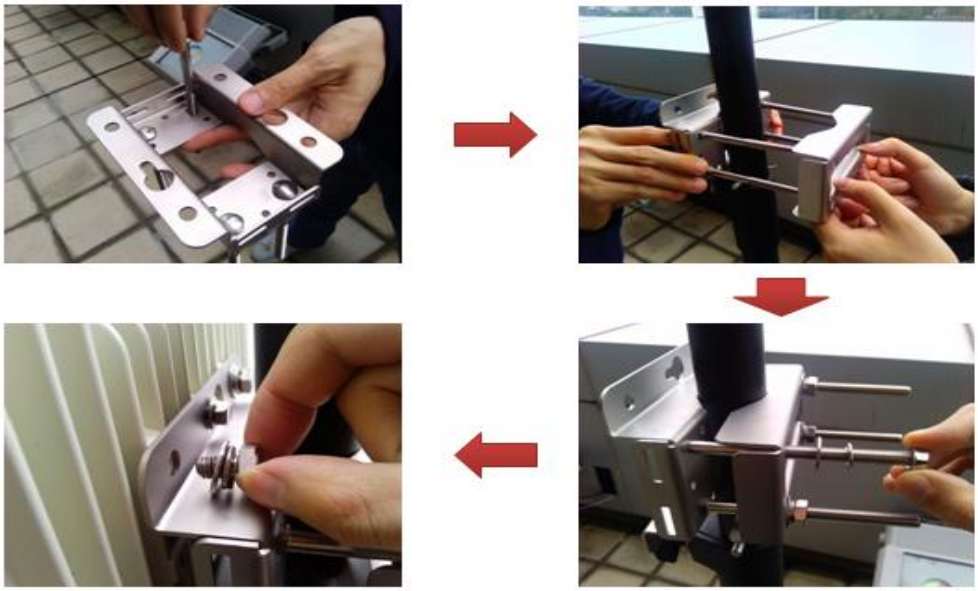

Figure 32 : montage du A8

Une fois le montage est fait on suit les étapes suivantes :

- On relie le câble Ethernet entre A8-Ein et l'injecteur PoE, Puis on l'enroule avec étanchéité,
- On ajuste l'angle de tilt pour A8-Ein, enfin on allume ce AP.

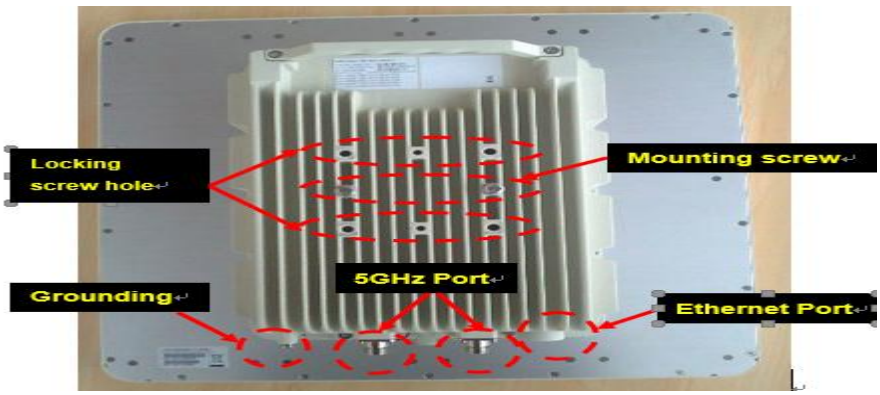

Figure 33: Face arrière de A8-Ein

6.4. Procédures d'Installation de point d'accèsA2

Les procédures d'installation se font comme suit :

- On installe l'antenne externe pour A2, et on applique les intempéries sur les ports externes..
- On branche le câble Ethernet entre la borne A2 et l'injecteur PoE.
- On va ajuster l'angle de tilt pour A2.
- On allume le A2.

Figure 34 : montage de A2

7. La configuration des équipements

La mise en service du wifi Outdoor « Wici », nécessite une configuration du point d'accès A2n et A8Ein et du routeur afin d'établir une liaison. Celle-ci permettra la diffusion de l'Internet vers les clients.

7.1. La configuration globale du réseau

Notre réseau Wici fonctionne grâce à l'architecture réseau ci-dessous, il permet de faire une connectivité entre les différents équipements utilisés

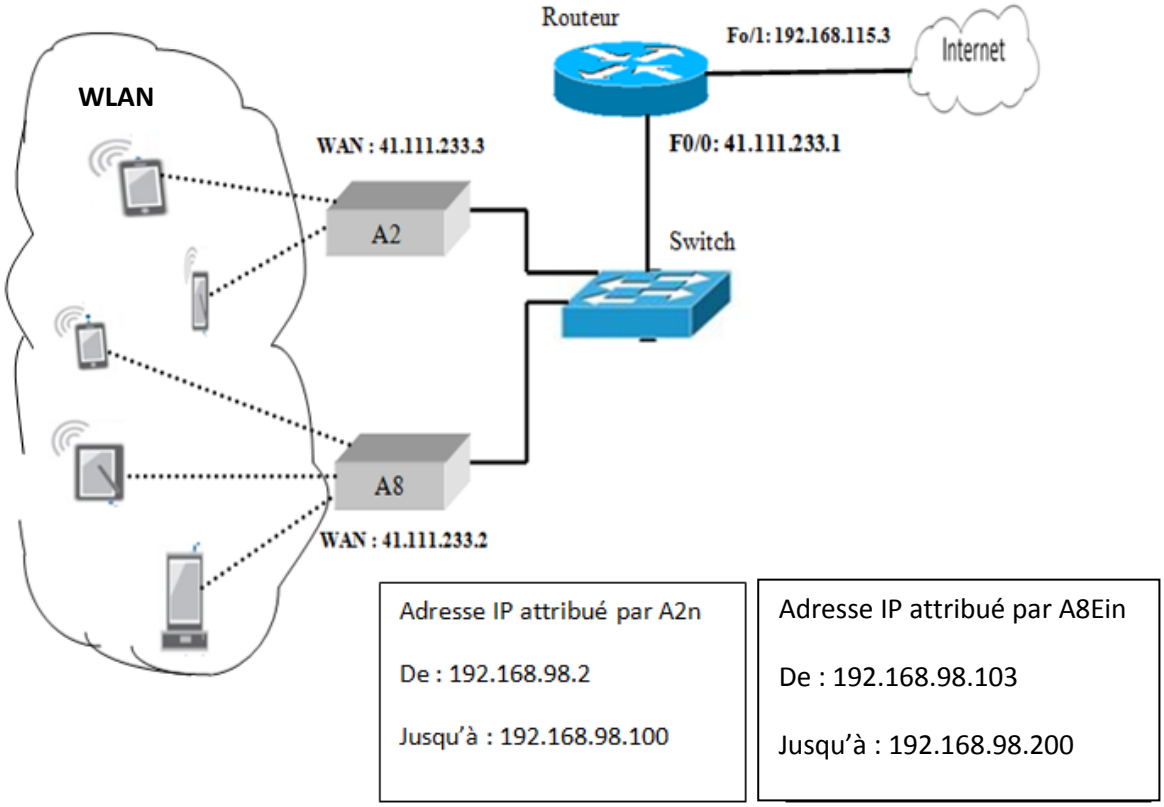

Figure 35 : Schéma global de configuration

7. 2. Configuration du point d'accès A2

7. 2.1. Branchement

On commence par brancher un câble réseau entre l'injecteur POE sur le port « Data in » et le port Ethernet de l'ordinateur. Puis on relie le point d'accès A2 à l'injecteur POE sur le port « Data out » avec un autre câble Ethernet. Enfin, on alimente A2 par une source d'alimentation 220V.

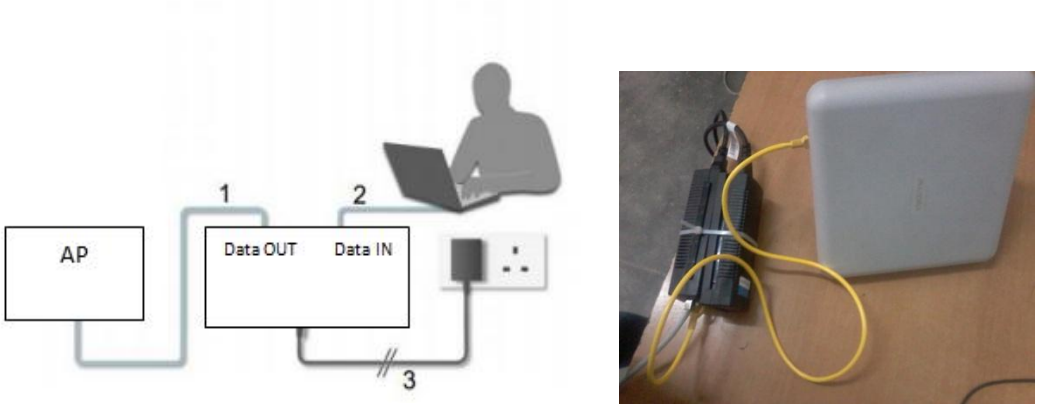

Figure 36 : le branchement

Afin de configurer le point d'accès A2, nous avons utilisé un ordinateur. Ce dernier doit avoir des paramètres IP statiques d'une manière à avoir la même classe d'adresses que celle de A2 :

- Adresse IP : 192.168.1.223
- Masque de sous réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.222 (adresse IP par défaut de A2).

7.2.2. Configuration du AP

On saisi l'adresse du AP (192.168.1.222) dans la barre d'adresses du navigateur Web. Puis, on accède à la page d'accueil de la figure 37 pour saisir le nom utilisateur et le mot de passe :

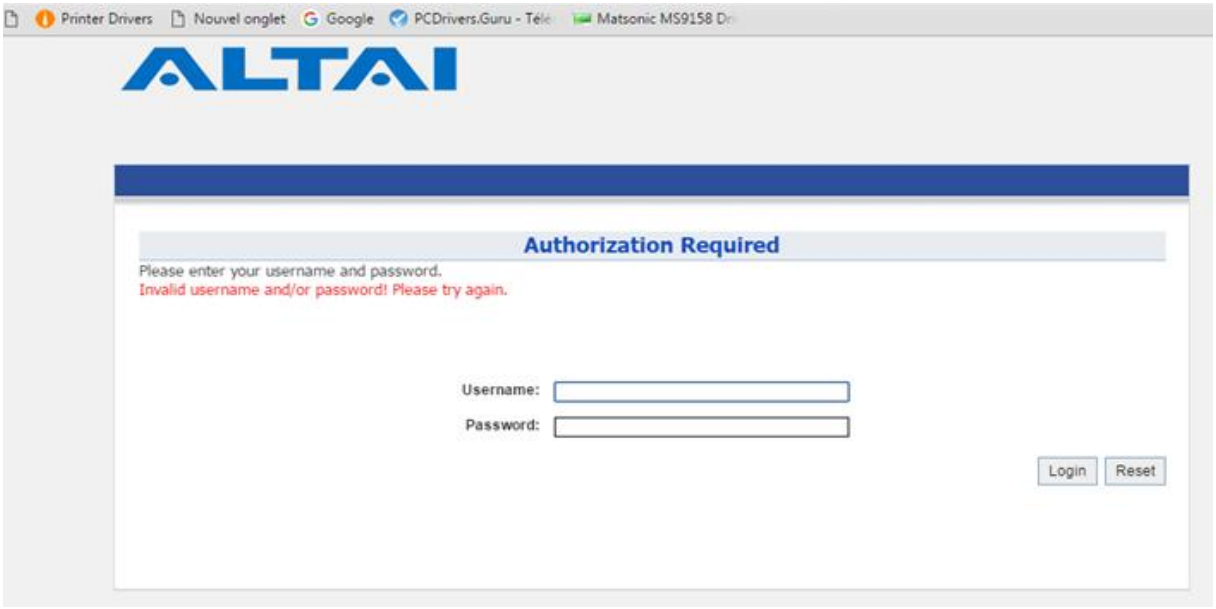

Figure 37 : la page d'accueil du AP.

- **Configuration des interfaces pour le réseau WAN et le réseau LAN**

Dans cette partie on choisit le mode Gateway (passerelle) qui permet de relier le réseau LAN (réseau des utilisateurs ou bien le réseau interne) au réseau WAN (réseau externe). Puis, on active le Nat mode (ensemble d'adresse LAN passe par une seule adresse public celle du WAN) et on saisie les nouveaux paramètres IP pour le WAN qui sont

- Adresse IP (Statique) :41.111.233.3
- Masque de sous réseau : 255.255.255.248
- La passerelle : 41.111.233.1 (Adresse IP du routeur)

Et pour le LAN on saisie l'adresse IP suivante : 192.168.98.1 et le masque de sous réseau : 255.255.255.0

Enfin, on sauvegarde ces paramètres.

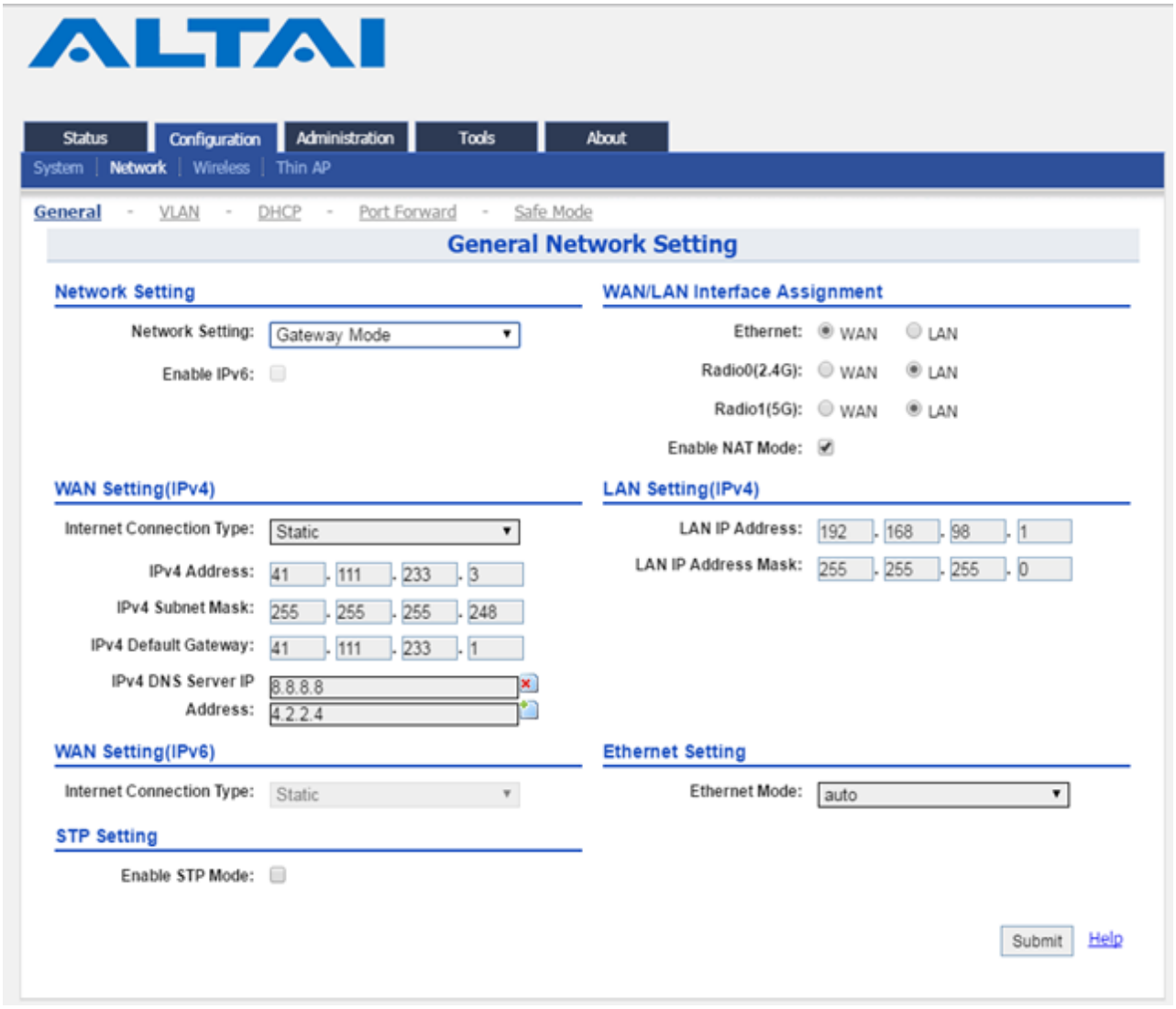

Figure 38 : page pour la configuration du WAN et LAN

- **Activer le serveur DHCP**

Dans notre cas on active le serveur DHCP pour définir une plage d'adresse pour les utilisateurs. La plage d'adresses que nous avons définie pour les clients de A2 est de 192.168.98.2 jusqu'à 192.168.98.100.

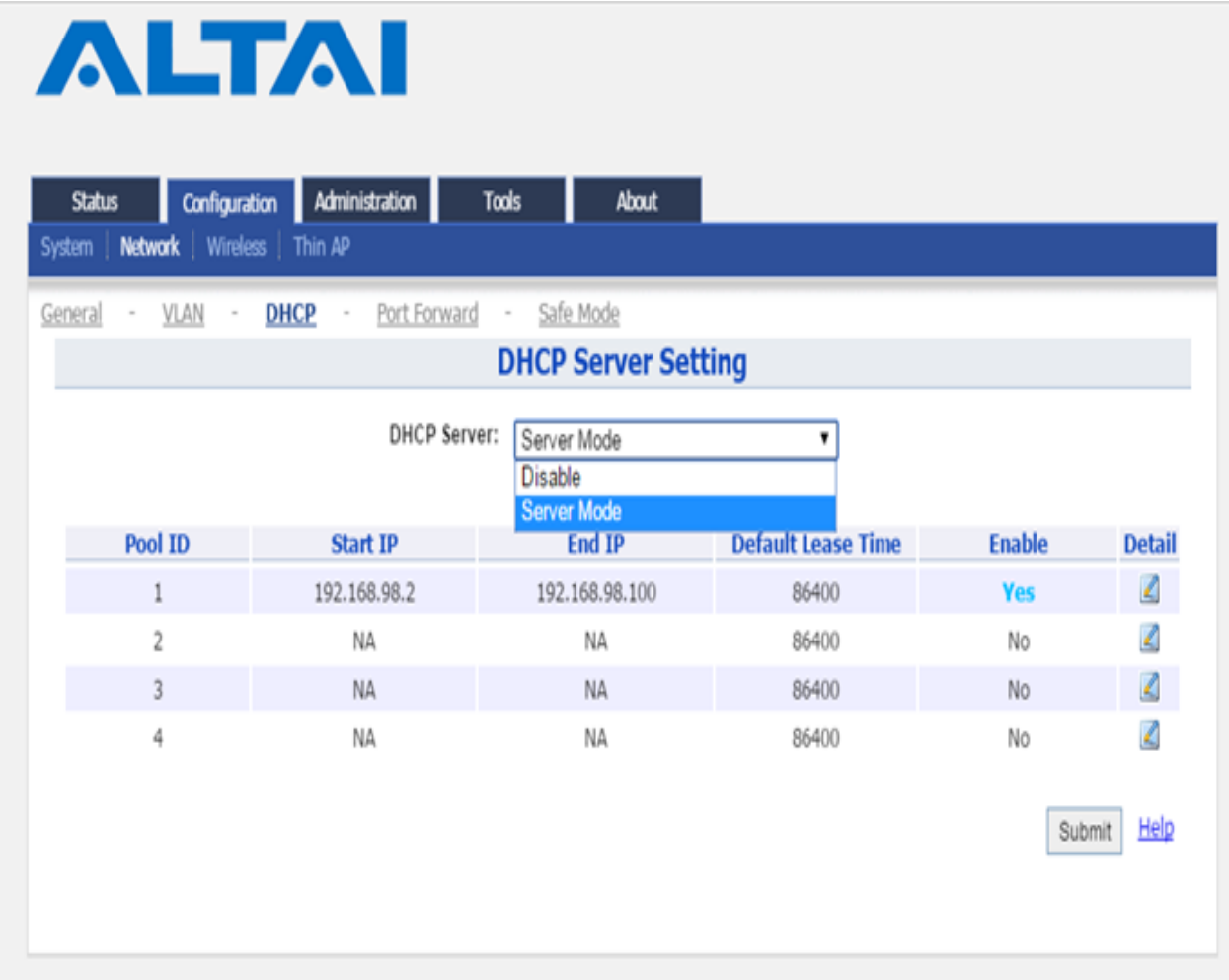

Figure 39 : l'activation du DHCP.

- **Définir la portée du signal du point d'accès A2n**
  - ✓ On clique sur configuration puis Wireless ensuite général.
  - ✓ On choisi la fréquence 2.4 GHz (fréquence de transmission du champ wifi vers les utilisateurs), ensuite on active le champ radio.
  - ✓ On sélectionne AP dans radio mode (diffuser le signal pour les utilisateurs), et Algérie dans contries mode.
  - ✓ Enfin on choisi 23 db puis on sauvegarde.

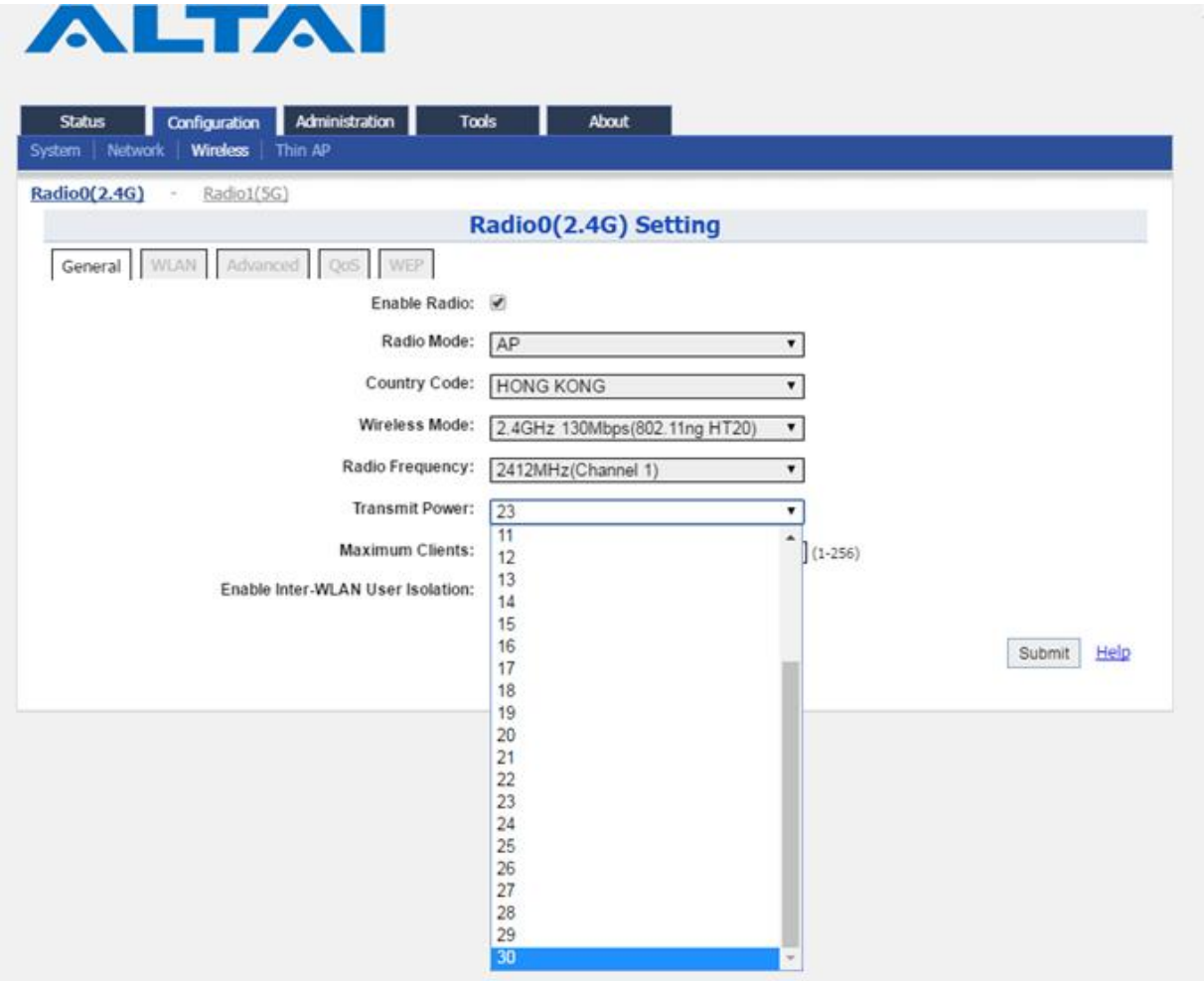

Figure 40 : la porté du AP.

- **Changer le nom de réseau WLAN (SSID)**
  - Pour nommer notre réseau wifi on clique sur configuration puis Wireless ensuite WLAN et on activer le WLAN.
  - Après on clique sur more pour accéder à la fenêtre WLAN général.
  - Ensuite on coche WLAN et on saisi le nouveau nom du WLAN, puis on sauvegarde.

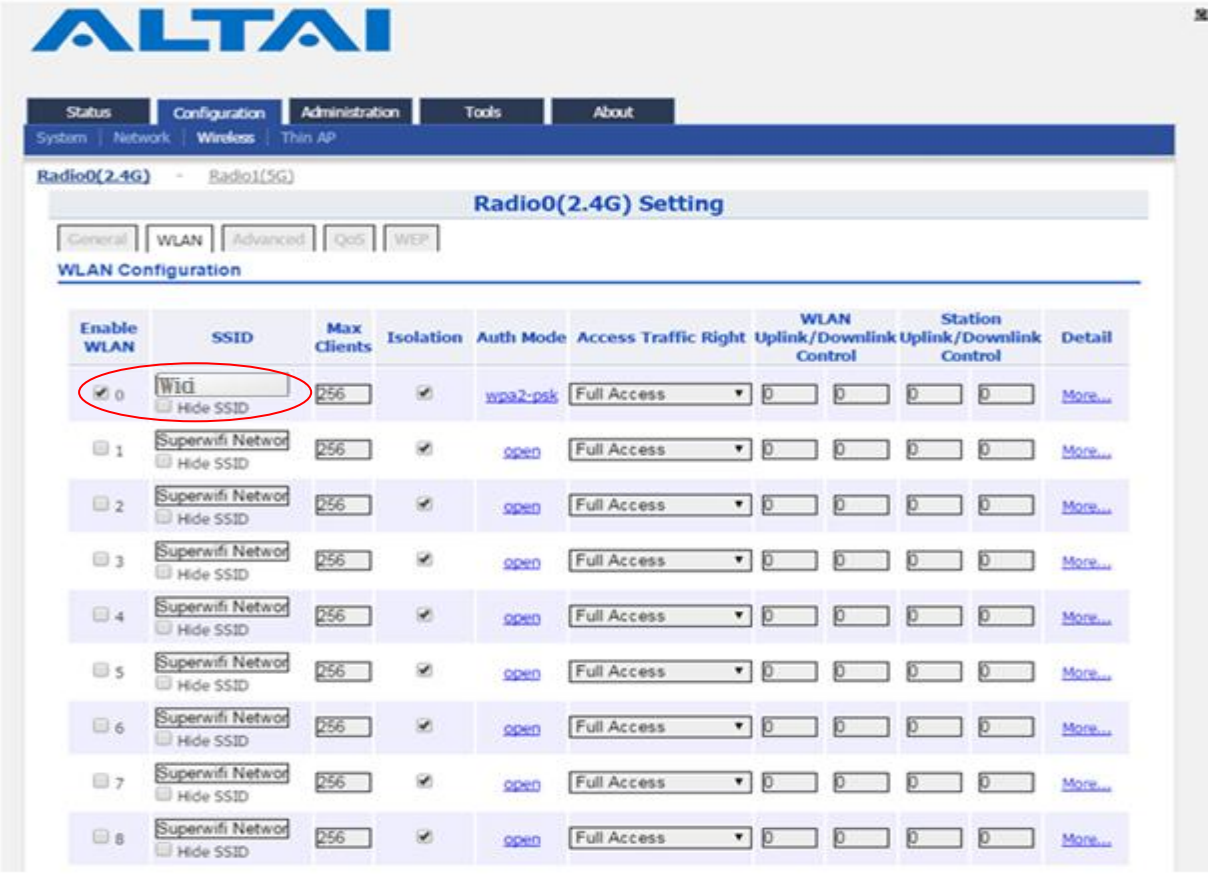

Figure 41 : nommer un réseau WLAN

- **Sécurisé le point d'accès A2**

On peut sécuriser ce point d'accès par un mot de passe Pour limiter le nombre d'utilisateurs.

- On clique sur WLAN Security.
- Choisir WPA2-PSK dans le mode d'authentification.
- Et on sauvegarde.

Dans ce cas seul les personnes ayant le mot de passe peuvent accéder au point d'accès.

Puisque le cas de ce point d'accès est public, donc on laisse le paramètre par défaut « ouvert ».

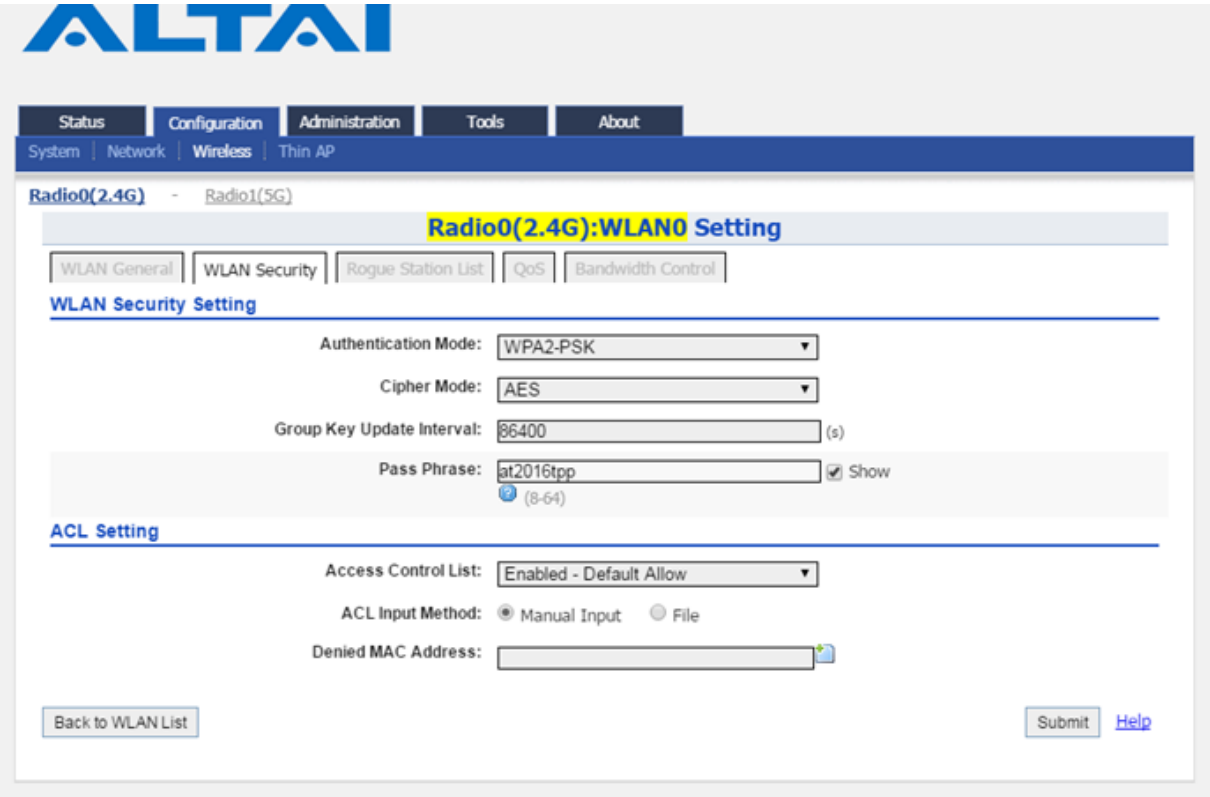

Figure 42: activation de la sécurité

- **Régler le débit**

Dans configuration on clique sur Wireless et on choisi Advanced. Puis, on sélectionne 54 Mbps (débit maximum) et on sauvegarde.

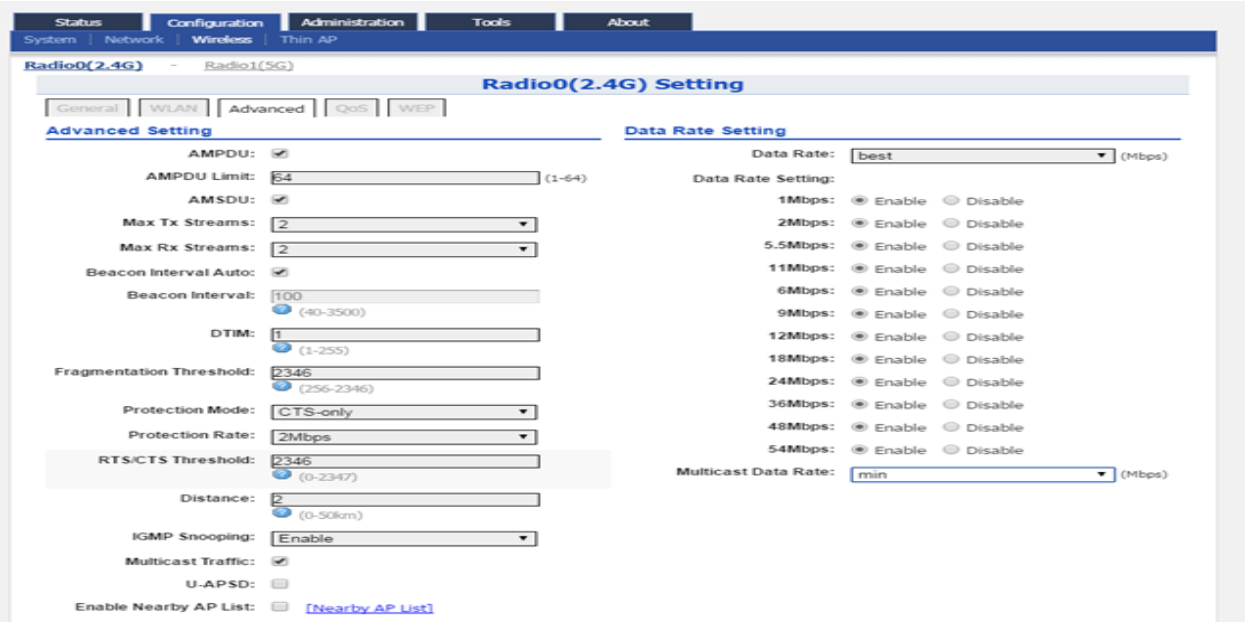

Figure 43: réglage de débit

- **Changer le nom d'utilisateur et le mot de passe**

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. A ce stade, toute personne pouvant accéder au réseau, peut faire les changements ou modifier d'autres paramètres du point d'accès.

Afin d'éviter ces modifications, on a changé le mot de passe et le nom d'utilisateur par défaut

- On Clique sur administration puis sur user admin.
- Saisir un nouveau nom d'utilisateur et un nouveau mot de passe.
- On confirme le mot de passe.

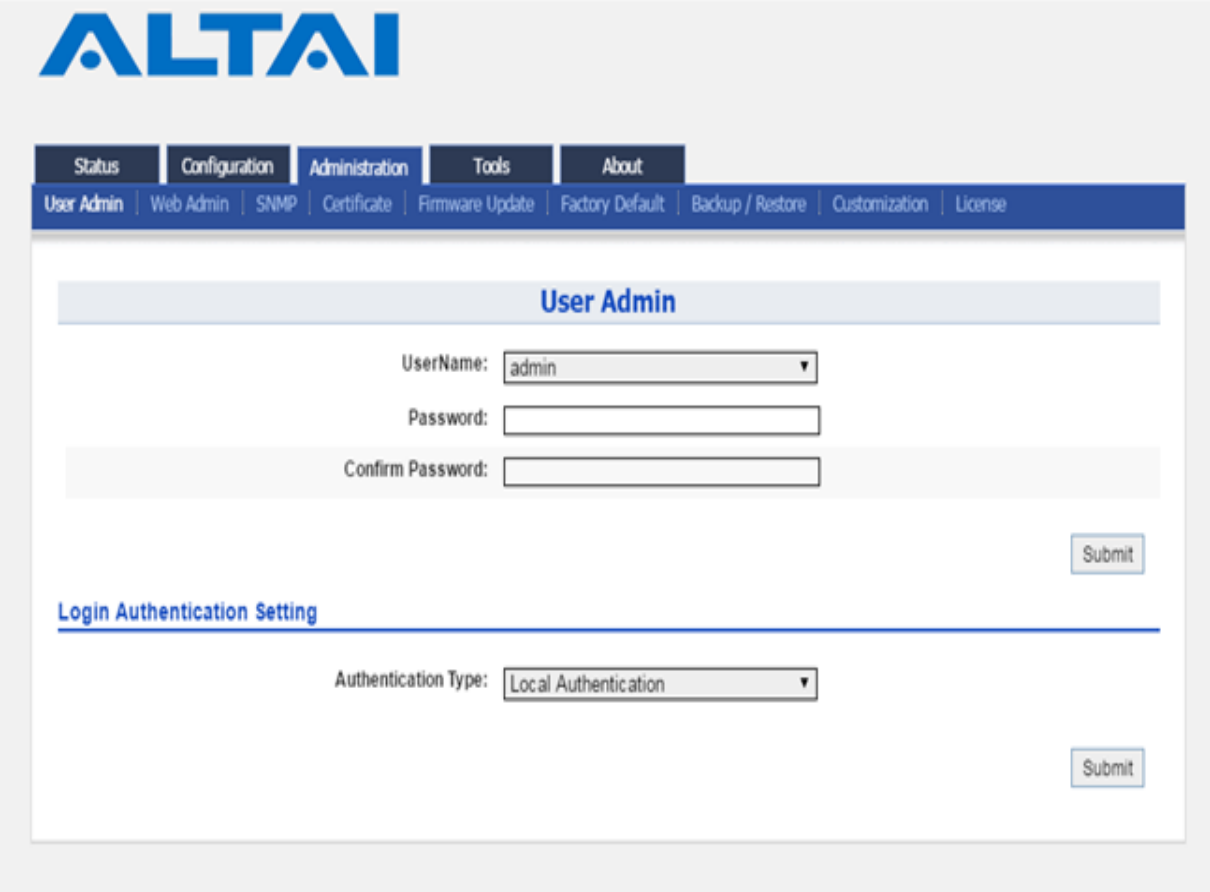

Figure 44 : changement de mot de passe et le nom d'utilisateur

Et on confirme toutes les configurations apporté au point d'accès. Toutefois, si on veut revenir à l'état par défaut du point d'accès on le réinitialise. Pour cela dans administration, on clique sur restaurer les données par défauts.

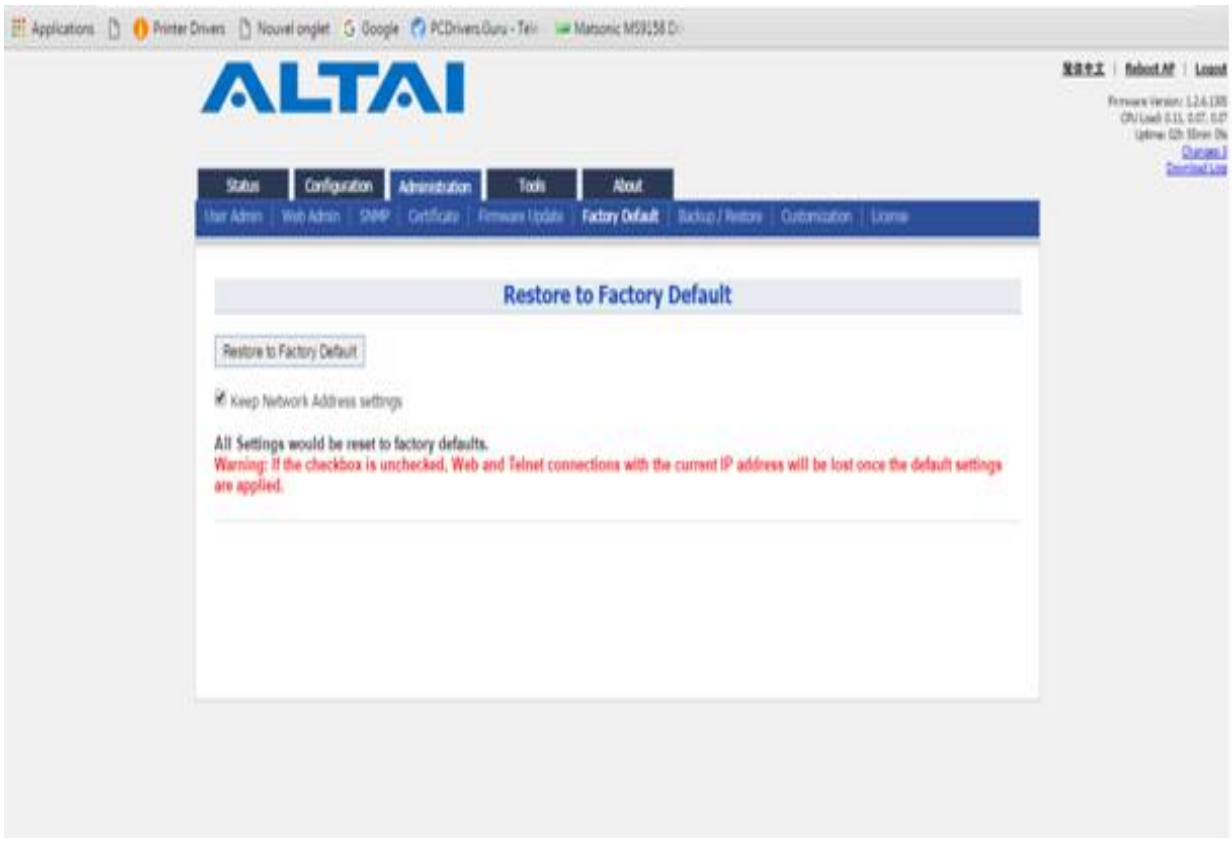

Figure 45 : réinitialisation du point d'accès

7.3. Configuration du point d'accès A8Ein

Les procédures de configuration de A8Ein se font de la même manière que celle de A2, sauf qu'il faut changer les plages d'adresses attribuées par le DHCP pour ne pas avoir un conflit d'adresse.

7.4. Configuration du routeur

7.4.1. Branchement

On branche le câble Console (câble bleu) entre le port console de routeur et le port série (DB 9) de l'ordinateur, à utiliser pour la configuration.

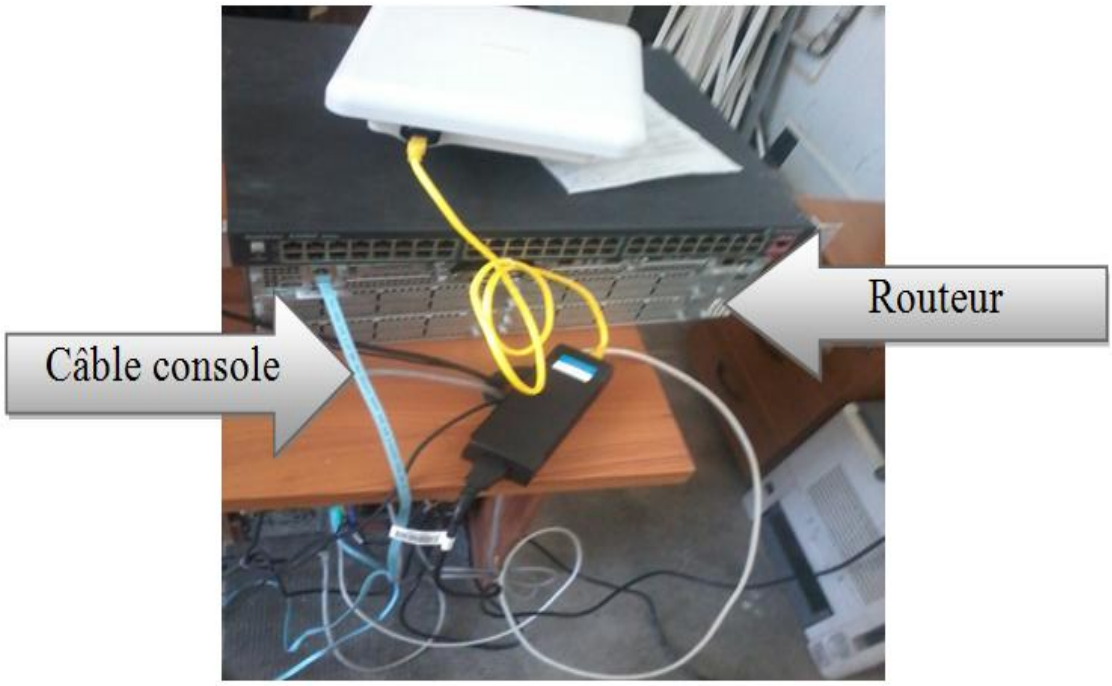

Figure 46 : branchement de routeur

7.4.2. Configuration

Une fois que notre ordinateur est physiquement connecté au routeur par le câble console, on exécute le logiciel Putty pour afficher la console de l'équipement. En effet, le logiciel Putty est un client SSH et Telnet pour Windows 32 bits. Il permet de se connecter à un serveur distant à partir d'un ordinateur connecté à internet. Dans notre cas il permet l'accès à distance du routeur par un ensemble de commandes.

Après avoir lancez Putty, une fenêtre s'ouvre.

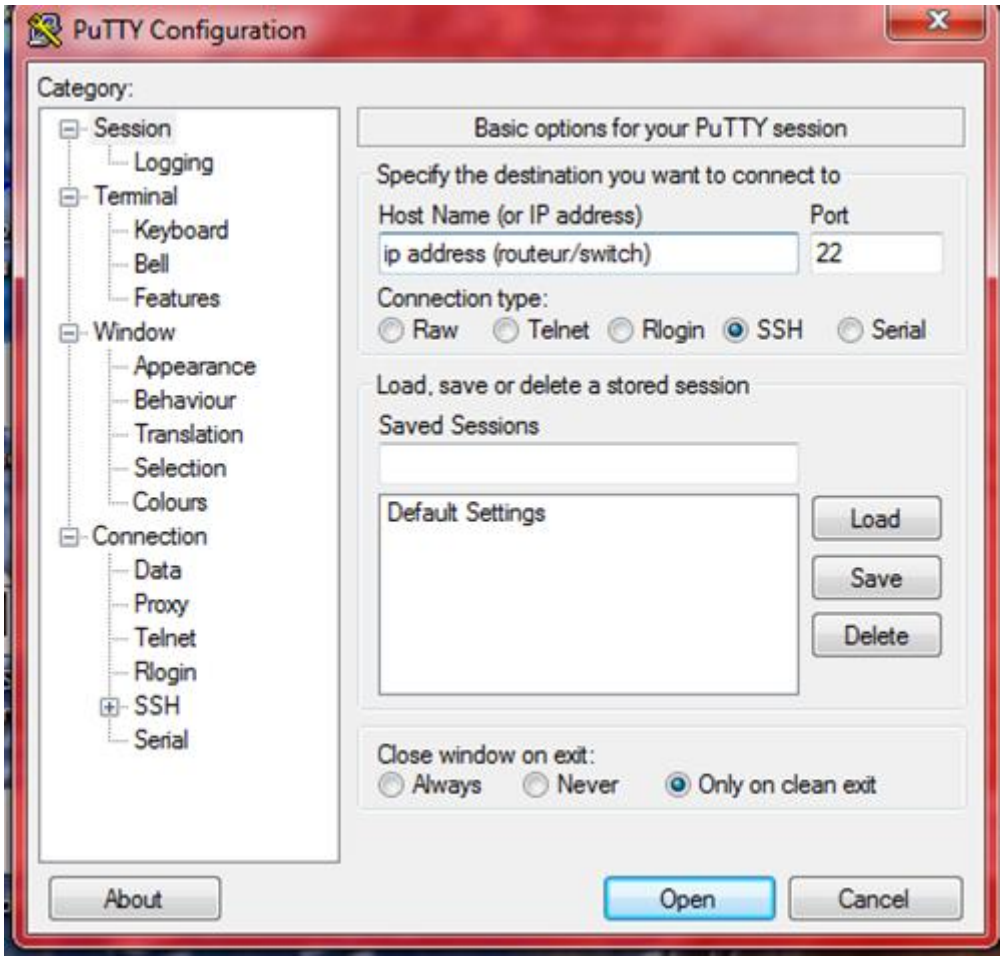

Figure 47 : lacement de Putty.

- ✓ On sélectionne le bouton "SSH" en haut à droite.
- ✓ On choisi le port COM1.
- ✓ On Clique sur open.

7.4.2.1. Configuration des interfaces

- ➢ **Interface gigabitEthernet 0/0 pour le port LAN**

Pour accéder à l'interface gigabitEthernet 0/0, on a utilisé la commande suivante :

- ✓ Router (config) # interface gigabitEthernet 0/0

Ensuite on donne l'adresse IP 41.111.233.1 et le masque sous réseau 255.255.255.248 par la commande

- ✓ Router (config-if) # ip address 41.111.233.1 255.255.255.248

Et on valide la configuration comme suit

- ✓ Router (config-if) # no shutdown

Apres avoir terminé la configuration de cette interface, on sort de la configuration par la commande « Router (config-if) exit ».

- **Interface gigabitEthernet 0/1 pour le port WAN**

Maintenant on va configurer l'interface gigabitEthernet 0/1 et pour accéder à cette interface gigabitEthernet 0/1, on utilise la commande suivante :

- ✓ Router (config) # interface gigabitEthernet 0/1

Ensuite on donne l'adresse IP 192.168.115.2 et le masque sous réseau 255.255.255.252 par la commande

- ✓ Router (config-if) # ip address 192.168.115.2 255.255.255.252

On valide la configuration comme suit

- ✓ Router (config-if) # no shutdown

Définir le chemin par la commande route 0.0.0.0 0.0.0.0 192.168.115.1

Et on quitte la configuration de l'interface par la commande « Router (config-if) exit »

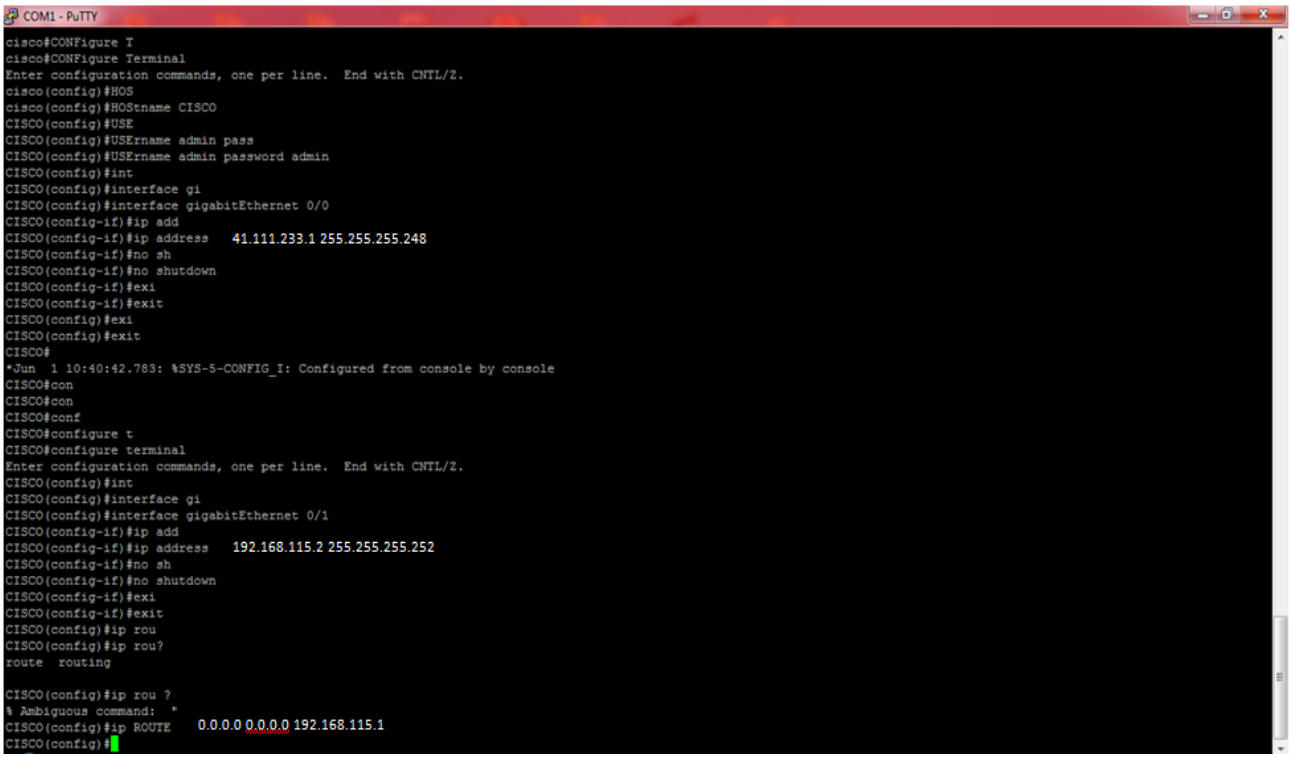

Figure 48 : la configuration des interfaces

La fenêtre suivante montre la configuration des interfaces

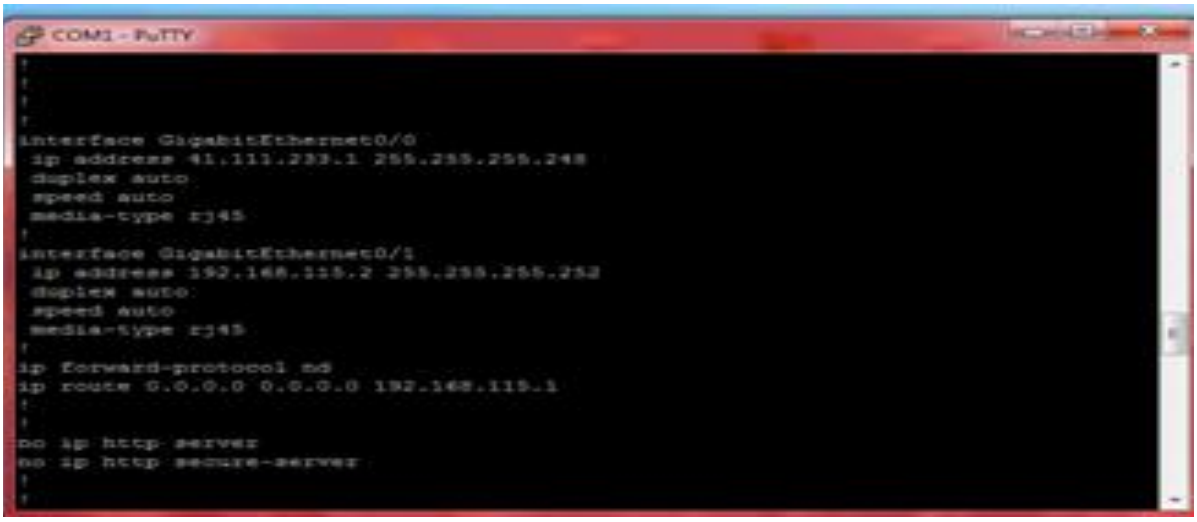

Figure 49 : les interfaces après configuration

8. Les tests effectués

8.1. Test de mot de passe

Il suffit de saisir le mot de passe et le nom d'utilisateur par défaut, comme le montre la figure suivante :

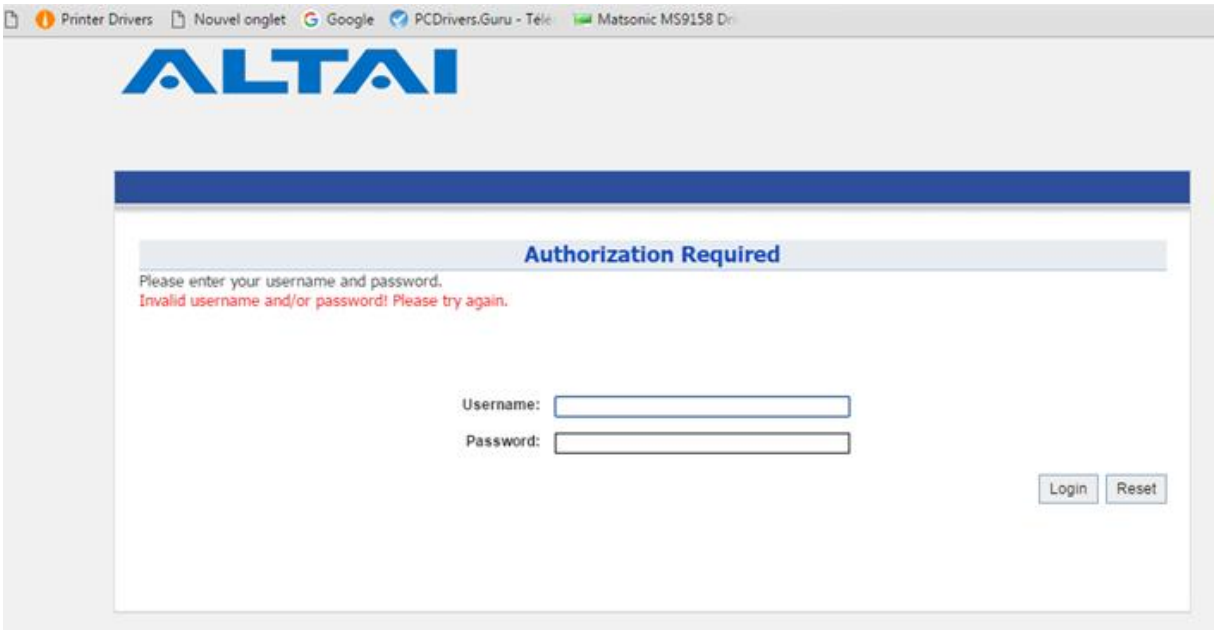

Figure 50 : tester le mot de passe

Si on saisie le mot de passe et nom d'utilisateur erroné, on n'aura pas accès à ce point d'accès.

8.2. Test d'authentification

Pour bénéficiera du réseau wifi outdoor dans les endroits couverts par le WICI, le client doit d'abord activer le wifi sur son terminal (portable, pc, tablette) dans paramètre wifi pour détecter le signal.

Ensuite il choisit le réseau wici.

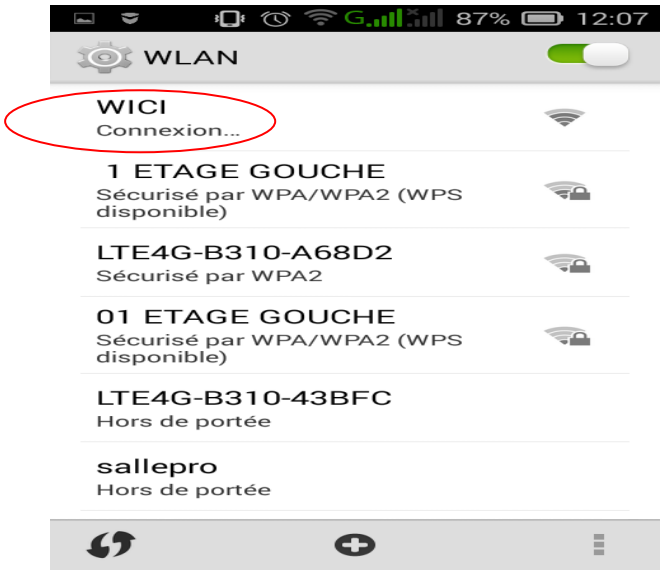

Figure 51 : détection du champ Wici

Ainsi le point d'accès lui attribue une adresse IP.

En ouvrant une page web, il est automatiquement redirigé par le portail captif vers le site d'authentification WICI, sur lequel il doit introduire son identifiant et son mot de passe qui lui seront attribué lors de son inscription chez une agence commercial d'Algérie télécom.

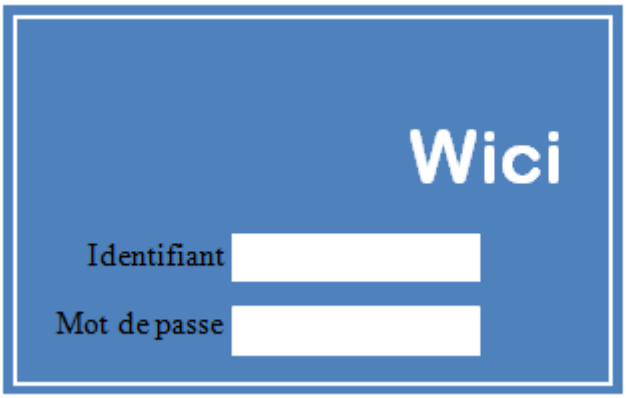

Figure 52 : page d'accueil Wici

❖ **Etapes d'authentifications**

Le client qui se connecte au réseau envoie sa demande au point d'accès. Il envoie son identifiant et son mot de passe sur le réseau qui est relié au serveur Radius.

Le serveur RADIUS joue un rôle dans la gestion de l'authentification des utilisateurs du point d'accès Wici. Le client doit ensuite saisir le code de recharge de sa carte de connexion dans la page suivante.

Figure 53 : Saisir le code de recharge

En effet, un client pourra recharger son compte avec l'une des 3 cartes de recharge suivantes :

- Une carte à 100 DA valables 1 jours.
- Une carte à 500 DA valables 7 jours.
- Une carte à 1000 DA valables 30 jours.

Figure 54 : cartes de recharge wici

Une fois le code introduit, le serveur Radius vérifie s'il est enregistré dans la base de données. Si c'est le cas, il va l'activer et l'effacer afin qu'il ne puisse pas être réutilisé à nouveau.
Et comme il s'agit d'un point d'accès payant un compteur commence a compté le temps jusqu'a son épuisement. Enfin le client pourra accéder au réseau internet et bénéficier de ces différents services.

9. Discussion

Dans ce chapitre nous avons présenté les étapes de mise en service du point d'accès wifi Outdoor. Nous avons commencé par l'étude du site pour choisir l'endroit le mieux adapté ou placé le AP. C'est l'étape la plus déterminante pour avoir une la couverture voulue du réseau Wifi. Ensuite nous avons procédé à l'interconnexion et la configuration des différents équipements. Enfin, les tests effectués démontrent la bonne installation du service Wici.

Conclusion

Conclusion

Le travail qu'on a élaboré consiste en la mise en service d'un réseau wifi outdoor pour couvrir la placette public Mbarek Ait Menguellet (ex gare routière) de Tizi-Ouzou, sous la direction des ingénieurs d'Algérie télécom de Tizi-Ouzou.

Pour donner un accès à l'internet dans les lieux public, Algérie télécom a opté pour la mise en place d'un point d'accès externe. Pour pouvoir réaliser cet objectif nous avons procédé suivant plusieurs étapes. Tout d'abord, Nous avons fait une étude permettant de bien choisir le site où placer le point d'accès. Ceci nous a permis d'avoir une bonne diffusion du signal. Ensuite, nous avons installé l'ensemble des équipements nécessaire. Enfin nous avons configuré les AP de manière à gérer les adresses IP pour l'ensemble des utilisateurs.

D'après l'étude de cette technologie, nous avons constaté qu'un point d'accès externe mis à la disposition du grand public peut être sécurisé afin d'assurer une authentification et une bonne complexité des informations partagées. D'une part par la diffusion d'un identifiant et d'un mot de passe pour chaque utilisateur. D'autre part par la mise en place du serveur Radius et le cryptage WPA2-PSk. De cette façon un utilisateur malveillant ne pourra pas intercepter les communications pour ainsi récupérer des informations personnelles transitant par ce canal.

Pour finir nous pensons que la généralisation du réseau Wici à travers le territoire national est nécessaire, afin de garantir l'accès à internet à tout moment et à n'importe quel lieu. Donc on doit faciliter l'accès à ce réseau afin d'en faire profiter le maximum de client sans avoir à passer par une agence d'Algérie télécom. Dans ce cadre nous proposons comme perspectives que l'inscription d'un nouvel utilisateur à ce service se fasse par internet. Pour cela, nous devons développer l'interface de connexion au réseau Wici.

Bibliographie

Bibliographie

[1] : Davor Males, Guy Pujolle et Olivier Salvatori, Wifi par la pratique, Ed Eyrolles, 2002.

[2] : André Pérez, Architecture des réseaux mobiles, Ed Lavoisier, Paris, 2011.

[3] : Aurélien GERON, Wifi professionnel La norme 802.11, le déploiement, la sécurité, Ed DUNOD, 3ème édition, 2009.

[4] : José Dorgoigne, réseaux informatiques : notions fondamentales, Ed ENI, 4ème édition, 2011.

[5] : G.pujolle, O.Salvatori et J.nozick, les réseaux et télécommunication, Ed Eyrolles, paris, 2004.

[6] : Jean-Michel Mur, les fibres optiques : notions fondamentales, Ed ENI, 2ème édition, juillet 2015.

[7] : Philippe ATELIN, Réseaux informatiques Notion fondamentales, Ed ENI, 3ème édition, 2009

[8] : Laurance Soyer, Mise en place du wifi, Ed ENI, 2005.

[9] : Aurélien Géron, Wifi : deploiement et sécurité, Ed Dunod, 2006.

[10] : Guy Pujolle, Les réseaux sans fil, Ed Eyrolles, 5ème édition, 2006.

[11] : Mohamed N. Salam : 2004, le piratage informatique : définition et problèmes juridiques, mémoire pour l'obtention du diplôme d'Etude Approfondies Interne et International des Affaires, université Libanaise, 2004.

[12] : Hakima Chaouchi, Maryline, Laurent-maknavicius, la sécurité dans les réseaux sans fil et mobiles : concepts fondamentaux, Ed Lavoisier, 2007.

[13] : Khaled DRIDI. Spécification du Protocole MAC pour les Réseaux IEEE 802.11e à Différentiation de Services sous Contrainte de Mobilité, thèse pour l'obtention du diplôme de Doctorat en Réseaux & Télécoms, université Paris Est, 2011.

[14] : https://technet.microsoft.com/fr-fr/library/cc753373%28v=ws.10%29.aspx, consulté le 28/05/2016.

[15] :http://www.altaitechnologies.com/wp-content/uploads/2015/04/Altai-A8-Ein-bgn-Catalog-Eng-150428.pdf, consulté le 01/06/2016.

[16] :http://www.securinets.com/sites/default/files/fichiers_pdf/securilight14/Securilight14_Fake%20access%20point.pdf, consulté le 05/06/2016.