République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de Fin d'Etude
pour l'obtention du Diplôme de Master Académique

Domaine : **Sciences et Techniques**
Filière : **Télécommunications**
Spécialité : **Systèmes de Télécommunications**

Etude et Mise en place d'un HotSpot Wi-Fi au niveau du Département d'Electronique et Télécommunications

Présenté par :
Amrane Mohamed Lamine
Djebala Hanane

Sous la direction de :
M. Khalfallaoui Abderrezak

MAI 2013

REMECIEMENT

A travers ce modeste travail, nous tenons à remercier vivement notre encadreur M. Khalfallaoui Abderrezak Pour l'intéressante documentation qui'il a mise a notre disposition, pour ses conseils précieux et pour toutes les commodités et aisances qu'il nous a apportées durant notre étude et réalisation de ce projet.

Nos remerciements les plus vifs s'adressent aussi aux 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 professeurs et enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de notre cycle universitaire. Sans omettre bien sûr de remercier profondément tous ceux qui ont contribué de près ou de loin à la réalisation du présent travail.

Et enfin, que nos chers parents et familles, et bien avant tout, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleures conditions.

Amrane Mohamed Lamine

Djebala Hanane

Sommaire

Liste des Figures

Chapitre I : Introduction aux communications sans fil

Chapitre II : Etude de la Technologie HotSpot

Chapitre III : Planification et Optimisation Du HotSpot Wi-Fi Dép ELN & TLC

Chapitre IV : Mise en place Expérimentale du HotSpot Dép ELN & TLC

Liste des Tableaux

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Le projet de fin d'étude du Master Systèmes des Télécommunications met l'accent sur une réalisation concrète pour laquelle l'étudiant met en place un protocole de travail déterminé. Les sujets proposés par l'équipe pédagogique impliquent une étude approfondie dans les domaines balayés par la formation Systèmes des Télécommunications. En l'occurrence, nous avons choisi un sujet dans le domaine des réseaux mais qui nécessite cependant des connaissances en télécommunications. D'une part, pour expliquer l'échange des données et d'autre part pour expliquer le comportement des ondes.

Depuis quelque temps des bornes sans fil placées dans des endroits publics donnent un accès gratuit ou non à Internet. Ces bornes sans fil ''Wi-Fi'', ou HotSpot, dont le but commercial est d'attirer une nouvelle clientèle « nomade » doivent être à la fois simple d'accès, et surtout par le fait qu'elles soient dans un endroit public, très sécurisées.

Les HotSpot se sont rapidement développés à l'échelle mondiale mais ce n'est pas le cas de l'Algérie. Ces HotSpot permettant ainsi à des utilisateurs nomades disposant d'équipements adaptés (ordinateurs ou téléphones portables compatibles, PDA et autres) de se connecter à Internet de partout avec beaucoup de simplicité. Si ces connexions Internet sont ouvertes au grand public, cela ne veut pas dire qu'il n'existe aucune protection à l'accès et pour les utilisateurs. Nous savons bien qu'une fois connectés sur un même réseau, les utilisateurs deviennent potentiellement vulnérables. La première des protections qui a été mise en place au sein des HotSpot est le portail captif avec une authentification par fichier local ou bien un serveur à distance.
Le Département d'Electronique et Télécommunications désire aujourd'hui mettre en place un HotSpot Wi-Fi qui permettre un accès Wi-Fi gratuit à Internet pour ses étudiants, conférenciers, professeurs, etc… tout en réglementant ce même accès.

C'est dans ce but qu'il nous a été demandé de mettre en œuvre un portail qui capte n'importe quel service demandé (HTTP, FTP, …) et n'autorise le passage de ces services que si la personne répond aux critères de sécurité demandé. Ces besoins dépassent aujourd'hui la logique d'un pare feu classique.

Pour nous guider vers une solution technique nous analyserons donc dans un premier temps les attentes du Département d'Electronique et Télécommunications afin de bien cibler les besoins.

Pour mener à bien notre projet nous avons d'abord procédé, dans notre premier chapitre à une brève présentation des différents types de réseaux sans fil, puis à l'étude d'interface radio. Ce chapitre est consacré aussi à la norme IEEE 802.11 (Wi-Fi). Nous y avons décri également les privilèges de cette norme ainsi que le mécanisme de communication entre équipements et le modèle en couches puis on a présenté rigoureusement l'aspect théorique de Wi-Fi, en proposant une étude approfondie de l'ensemble des fonctionnalités apportées par le standard 802.11 et ses différentes améliorations : l'évolution, la structure de la trame, techniques d'accès…, etc.

Le deuxième chapitre est une étude sur la technologie HotSpot il se divise en deux partie la première partie est une généralité sur les HotSpot pour les règlementations et les différentes lois de l'ARPT, qui décrit la responsabilité du FAI vers ces accès ainsi qu'une étude du marché mondial et l'évolution de ces HotSpot dans le monde. La deuxième partie contient le principe de fonctionnement des HotSpot où nous présenterons les principales solutions libres de portails captifs et des serveurs d'authentification ainsi qu'une orientation de choix de la solution la plus approprié au Cahier des Charges du Département d'Electronique et Télécommunications.

Le troisième chapitre présente le bilan de liaison pour faire fonctionner notre système et les processus de planification et d'optimisation de l'emplacement des points d'accès. Pour ce faire, nous avons opté pour une approche par mesure utilisant l'outil Wolf Wi-Fi Pro. Nous commençons à savoir la problématique du sujet, par suite la conception du logiciel. La dernière partie de ce chapitre est consacrée à la présentation et à l'interprétation des résultats de mesure obtenus avec ce modèle.

Enfin, dans le quatrième chapitre nous détaillerons la mise en place expérimentale du HotSpot Dép ELN & TLC. Commençant par l'identification des composants matériels et la topographie utilisée, ensuite les différentes étapes de configuration des matériels à savoir la configuration du portail captif et le serveur d'authentification. Dans la dernière partie nous montrons les résultats du test de fonctionnement de notre HotSpot Dép ELN & TLC.

CHAPITRE I

[Introduction aux communications sans-fil]

2-2- Réseaux locaux sans fils (WLAN)

Le réseau local sans fils (WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

• Le WiFi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

• HiperLAN2 (High Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute), permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5150 et 5300 MHz.

• DECT (Digital Enhanced Cordless Telecommunication), norme des téléphones sans fils domestiques. Alcatel et Ascom développent pour les environnements industriels, telles les centrales nucléaires, une solution basée sur cette norme qui limite les interférences. Les points d'accès résistent à la poussière et à l'eau. Ils peuvent surveiller les systèmes de sécurité 24/24h et se connecter directement au réseau téléphonique pour avertir le responsable en cas de problème [2].

Technologie	Norme	Débit (Mbits/s)	Portée (mètres)	Bande de Fréquence (GHz)	Observation
WiFi	IEEE 802.11	2 - 54	35 -50 (indoor) des centaines (outdoor)	2,4 – 2,4835 5	Elle comporte plusieurs déclinaisons IEEE 802.11 a/b/g/n…etc
HiperLAN 1	ETSI	19 - 20	50	5	- La vitesse de déplacement de l'utilisateur ne peut excéder 10 m/s - Permet d'accéder aux réseaux ATM
HiperLAN 2		25	200		
HiperLink		155	150 - 200	17,2 – 17,3	Permet des liaisons fixes entre 2 points
DECT		2	300	1880 – 1900 MHz	Technique d'accès TDMA

Tableau 1.2: Technologie des réseaux WLAN

2-3- Réseaux métropolitains sans fils (WMAN)

Le réseau métropolitain sans fils (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication. Et ce sont des réseaux qui couvrent partiellement ou totalement la superficie d'une ville [2].

Technologie	Norme	Débit (Mbits/s)	Portée (km)	Bande de fréquence (GHz)	Observation
WiMax	IEEE 802.16	70	50	1 – 66	- Permet le raccordement des hots spots WiFi pour l'accès à Internet - Techniques d'accès TDMA comporte plusieurs déclinaisons
HiperAccess	ETSI	25	5	5	- Permet d'accéder aux réseaux ATM

Tableau 1.3: Technologie des réseaux WMAN

Le Wimax (standard de réseau sans fils poussé par Intel avec Nokia, Fujitsu et Prowim) basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit maximum de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est d'avantage destiné aux utilisateurs itinérants [2].

2-4- Réseaux étendus sans fils (WWAN)

Le réseau étendu sans fils (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. Les principales technologies sont les suivantes :

- GSM (Global System for Mobile Communication ou Groupe Spécial Mobile)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System)

hnologie	Norme	Débit (Mbits/s)	Portée (km)	Bande de fréquence (GHz)	Observation
GSM	Européenne	9.6 Kbits/s	0.3 – 30	[890-915] MHz [935-960] MHz [1710-1785] MHz [1805-1880] MHz	- Utilise une commutation de circuits Système très sécurisé
GPRS	Européenne	≤ 120 kbits/s	0.3 – 30	[890-915] MHz [935-960] MHz [1710-1785]MHz [1805 :1880]MHz	- Utilise une commutation de paquets - Prise en charge des applications de données à moyens débits - Utilise le protocole IP pour le formatage des données
UMTS	Européenne (ETSI)	≤ 2 Mbits/s	0.3 – 30	2 GHz	- Offre un accès à Internet et à ses serveurs web - Supporte des applications audio et vidéo basse définition - Fonctionne en mode paquet et mode circuit
DMA 2000	Américaine (TIA)	≤ 2 Mbits/s		2 GHz	- Utilise la technique d'étalement de bande
EDGE	Européenne	59.2 kbits/s	0.3 – 30	2 GHz	-Utilise la commutation de circuit
S 95	Américaine	1,2288 Mchips/s		800-900 MHz 1800-1900 MHz	- Utilise la technologie CDMA

Tableau 1.4: Technologie des réseaux WWAN

3- Standard IEEE 802.11

L'IEEE a développé la norme 802.11 sous plusieurs versions regroupant ainsi les normes physiques suivies des normes d'amélioration. Elles offrent chacune des caractéristiques différentes en termes de fréquence, de débit ou de portée du signal [3].

3-1- Les normes physiques

La première version normalisée par l'IEEE fût la 802.11. Elle utilisait la modulation DSSS sur la bande 2.4 GHz. Cette norme n'était pas compatible entre constructeurs. De plus, elle offrait un débit très faible (2 Mbps), comparés aux débits que proposait la norme Ethernet filaire. L'IEEE développa de nouvelles générations de réseaux sans fil : la 802.11b, la 802.11a et la 802.11g.

a. La 802.11b ou Wi-Fi 2 : C'est la première norme Wi-Fi interopérable. Avec un débit de 11 Mbps, elle permet une portée de 300 mètres dans un environnement dégagé. Elle utilise la bande des 2.4GHz avec 3 canaux radios disponibles. Cette norme Wi-Fi a connu beaucoup d'extensions et chacune d'entre elles, visant à apporter une amélioration soit au niveau du débit, soit au niveau de la bande passante ou même de la sécurité, de la qualité de service ou de la capacité du canal etc.

b. La 802.11 a : Encore appelé Wi-Fi 5, cette norme permet d'obtenir du haut débit (54 Mbit/s) tout en spécifiant 8 canaux. Mais elle n'est pas compatible avec la 802.11b. Elle utilise la technique de modulation OFDM.

c. La 802.11g : La 802.11a offre un débit assez élevé mais la portée est plus faible et son usage en extérieur est souvent interdit. Pour répondre à ces problèmes, l'IEEE développe la nouvelle norme 802.11g, offrant le même débit que le Wi-Fi 5, tout en restant compatible avec le Wi-Fi 2 (bande de fréquences de 2.4 GHz) .Cette norme vise aussi à remplacer Wi-Fi 2 sur la bande 2.4 GHz mais avec un débit plus élevé pouvant atteindre les 54 Mbits/s. Elle utilise la technique de modulation OFDM.

3-2- Les normes d'amélioration

Les normes suivantes ont apporté des améliorations sur la sécurité, l'interopérabilité, la qualité de service, la gestion du spectre etc [3].

a- La 802.11i : Amélioration au niveau MAC destinée à renforcer la sécurité des transmissions, et se substituant au protocole de cryptage WEP. Elle vise à renforcer la sécurité des transmissions

b- La 802.11d : En permettant aux différents équipements d'échanger des informations sur les plages de fréquences et les puissance autorisées dans le pays d'origine du matériel, cette norme permet l'adaptation des couches physiques afin de fournir une conformité aux exigences de certains pays particulièrement strictes, exemple France, Japon.

c- La 802.11e : Elle vise à améliorer la qualité de service (bande passante, délai de transmission pour les paquets…) et les fonctionnalités d'authentification et de sécurité.

d- La 802.11f : Elle assure l'interopérabilité entre les différents points d'accès des différents constructeurs.

e- La 802.11h : Elle gère le spectre de la norme 802.11a et vise à améliorer la sous couche MAC, afin de rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2. Enfin, elle s'occupe de l'assignation automatique de fréquences du point d'accès et du contrôle automatique de la puissance d'émission, afin d'éliminer les interférences entre points d'accès.

Norme	Normalisation	Bande Ghz	Débit Théorique (Mbits/s)	Débit Réel (Mbits/s)	Portée Théorique	Observations
802.11	1997	2.4	2	<1	100 m	Utilisateurs particuliers
802.11a	1999	5	54	2-24	20 m	Usage extérieur interdit en France
802.11b	1999	2.4	11	4-6	60 m	Compatible 802.11
802.11g	2003	2.4	54	20-28	20 m	Compatible 802.11b
802.11n	2009	2.4 / 5	450	200	50/125 m	Compatible 802.11a/b/g

Tableau 1.5 : Comparaison des principales normes 802.11

4- Etude de l'interface radio

4-1- Support de transmission (les ondes radio)

Les ondes radio, également appelées ondes hertziennes car elles furent découvertes par le physicien allemand Heinrich Hertz en 1888, sont des ondes électromagnétique, c'est-à-dire des oscillations combinées d'un champ magnétique et d'un champ électrique. Les ondes radio, les infrarouges, la lumière visible, les ultraviolets, les rayons X ou encore les rayons gamma sont tous des exemples d'onde électromagnétique. Ces ondes transportent de l'énergie sans avoir besoin d'un quelque support matériel : autrement dit, elles peuvent se propager dans le vide [4].
La théorie des ondes électromagnétique est trop vaste et complexe pour le traiter ici en détail, voici donc les principaux qu'il faut retenir :

- La portée du signal ;
- Le bruit, interférences et multipath ;
- Le débit ;

4-2- Les bandes de fréquences utilisées dans la norme IEEE 802.11

Les technologies utilisées pour les réseaux WPAN et les WLAN, fonctionnent sur deux bandes :

- La bande ISM (Industrial, Scientific and Medical) (de 2400 à 2500 Mhz).
- La bande U-NII (Unlicenced-National Information Infrastructure) (de 5150 à 5720 Mhz).

4-2-1- La bande ISM

La bande ISM correspond à trois sous bandes (902-928 Mhz, 2.400-2.4835 Ghz, 5.725-5.850 Ghz) seule la bande de 2.400-2.4835 Ghz, avec une bande passante de 83.5 Mhz, est utilisée par la norme 802.11.

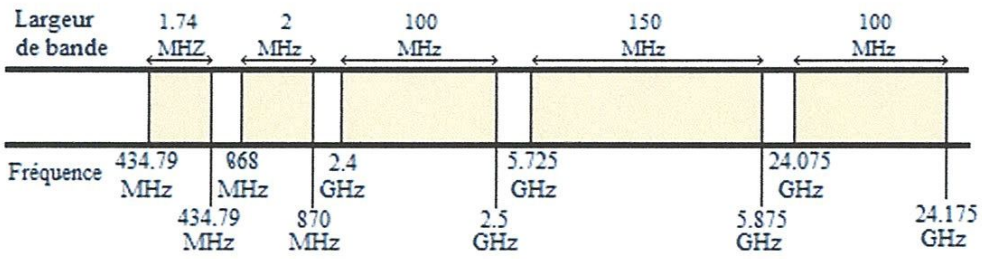


Figure 1.2 : Répartition des Bandes ISM en France et en Europe

Cette bande ISM est reconnue par les principaux organismes de la réglementation, tels que la FCC aux Etats-Unis, l'ETSI en Europe, l'ART en France, l'ARPT en Algérie. La largeur de bande

libérée pour les RLAN varie cependant suivant les pays (voir tableau suivant). En plus une utilisation sans licence.

Pays	Bande de fréquences
Etats-Unis (FCC)	2.400-2.485 Ghz
Europe (ETSI)	2.400-2.4835 Ghz
Japon (MKK)	2.471-2.497 Ghz
France (ART)	2.4465-2.4835 Ghz
Algérie (ARPT)	2.4465-2.4835 Ghz

Tableau 1.6: Allocation des bandes de fréquences ISM selon les pays [4].

4-2-2- La bande U-NII

La bande sans licence U-NII est située autour de 5Ghz. Elle offre une largeur de bande de 300Mhz (plus importante que celle de la bande ISM qui est égale à 83.5 Mhz). Cette bande n'est pas continue mais elle est divisée en trois sous-bandes distinctes de 100 Mhz. Dans chaque sous bande la puissance d'émission autorisée est différente. La première et la deuxième sous bande concernent des transmissions en intérieur. La troisième sous-bande concerne des transmissions en extérieur. Comme pour la bande ISM, la disponibilité de ces trois bandes dépend de la zone géographique. Les Etats-Unis utilisent la totalité des sous-bandes, l'Europe n'utilise que les deux premières et le Japon la première. Cette bande est reconnue par les mêmes principaux organismes de règlementation [4].

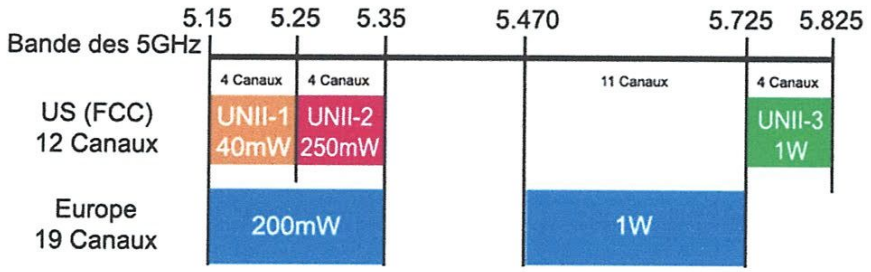


Figure1.3 : Répartition de la bande U-NII

4-3- Les canaux

Comme nous l'avons vu, toutes les variantes du WiFi découpe la bande de fréquence sur laquelle reposent (2.4 Ghz ou 5 Ghz) en canaux ils sont différents selon les variantes utilisées.
Le 802.11 FHSS utilise la bande de 2.4 Ghz et la découpe en canaux de 1 Mhz numérotés à partir de 2400 Mhz. Les canaux utilisables changent en fonction de la législation du pays où se trouve, mais en deux mots on a droit aux canaux 2 à 83 en Europe et aux canaux 2 à 80 aux Etats-Unis. Du coup, la plupart de matériel se limite aux canaux 2 à 80. Le 802.11 FHSS n'étant presque plus utilisé nous ne détaillerons pas davantage ses canaux.

Pour toute les autres variantes du WiFi sur la bande de 2.4 Ghz c'est-à-dire le 802.11 DSSS le 802.11b et le 802.11g. Quatorze canaux de 22 Mhz largeur sont définis également numérotés à partir de 2400 Mhz. Leurs centres ne sont espacés que de 5 Mhz de sorte qu'ils se superposent en partie. Ceci permet de choisir avec une certaine souplesse la bande de la fréquence que l'on préfère utiliser, mais si l'on a deux réseaux au même endroit et qu'ils utilisent des canaux voisins on aura beaucoup d'interférences. Pour éviter les interférences on recommande un espace de cinq canaux au moins donc on ne peut pas utiliser que trois canaux simultanément au même endroit.

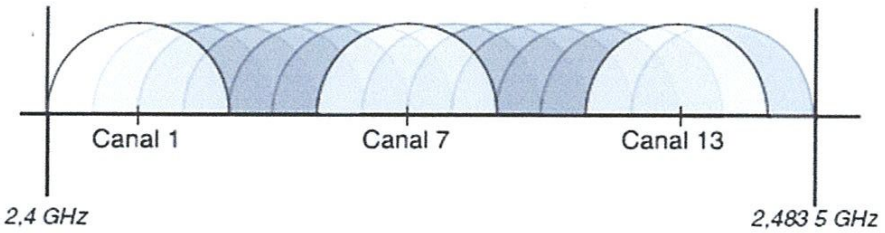


Figure 1.4 : Recouvrement des canaux dans la bande ISM

4-4- Technique de transmission

La couche physique définit plusieurs techniques de transmission permettant de limiter les problèmes d'interférences :

4-4-1- Etalement de la bande spectrale

L'étalement de bande a pour but d'utiliser plus de bande que nécessaire par le bais d'un facteur d'étalement. L'IEEE a initialement défini trois couches physiques initiales :

- **Le FHSS :**

La modulation FHSS (Frequency Hopping Spread Spectrum) a été inventée et brevetée en 1942 par l'actrice hedy lamar et le pianiste george antheil, qui étaient assez polyvalents ! Le principe du FHSS est assez simple : une large bande de fréquence est divisée en de multiples canaux et les communications se font en sautant (hopping) successivement d'un canal à un autre, selon une séquence et un rythme convenus à l'avance entre l'émetteur et le récepteur.

Il est difficile d'intercepter les communications si l'on ne connaît pas la séquence choisie, c'est pourquoi elle fut très appréciée par les militaires américains qui l'utilisèrent pour radioguider les torpilles sans que l'ennemi puisse intercepter ou brouiller le signal. Dans le cas du 802.11, cette fonction n'est (malheureusement) pas exploitée car les séquences de canaux utilisées ne sont pas secrètes.

Le FHSS offre également une résistance importante aux interférences voire même aux brouillages volontaires car les canaux pour lesquels le bruit est trop important peuvent être simplement évites. Toutefois, le 802.11 FHSS n'exploite pas cette capacité, contrairement au Bluetooth et au HomeRF qui sont deux technologies sans fil utilisant la modulation FHSS.

Un dernier avantage du FHSS est que plusieurs communications peuvent avoir lieu en même temps sur la même bande de fréquences pourvu qu'elles utilisent des séquences de canaux ne rentrant pas en collision les unes avec les autres. Par exemple, une communication pourrait utiliser la séquence triviale : 1,2,3, 1,2,3, 1,2,3, tandis qu'une autre communication aurait la séquence suivante 2,3,1,2,3,1,... de sorte qu'à aucun moment les deux communications n'utilisent le même canal.

Dans la première version du 802.11, la bande de fréquence allant 2400 Mhz à 2483.5 Mhz a été découpée pour le FHSS en canaux de 1 Mhz de largeur chacun.

Dans la plupart des pays, les canaux 2 à 80 sont autorisés. Au sein de chaque canal, la modulation gaussienne FSK (Frequency Shift Keying) à deux états 2GFSK (2Gaussian FSK) est utilisée et permet un débit de 1 Mb/s. En utilisant la modulation 4GFSK on peut atteindre un débit de 2 Mb/s. En utilisant la modulation GFSK (Gaussian FSK) comme modulation sous-jacent, le FHSS permet d'éviter les interférences entre canaux voisins, ce qui permet à plusieurs utilisateurs de communiquer en FHSS en même temps sans gêner.

Le standard 802.11a défini un mécanisme d'adaptation dynamique du débit en fonction du rapport signal/bruit : lorsqu'il élever, la modulation utilisée est la 4GFSK à 2 Mb/s, sinon le 802.111 s'adapte automatiquement et descend au 2GFSK à 1 Mb/s [3].

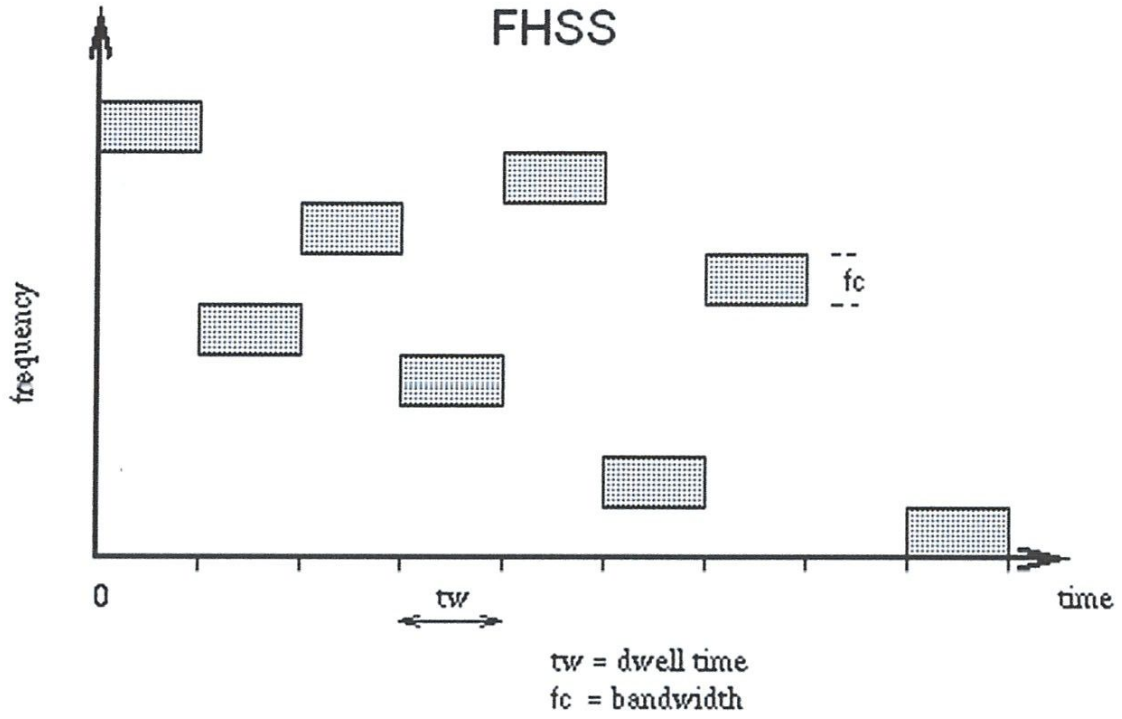


Figure 1.5: Etalement de spectre à saut de fréquence FHSS

- **Le DSSS (**chipping)

La modulation DSSS (Direct Séquence Spread Spectrum) est également une technique d'étalement de spectre, mais contrairement au FHSS, aucun saut de fréquence n'a lieu : le DSSS provoque des transitions d'état très rapides (Chipping) qui tendent à étaler le spectre du signal. Pour ce faire, l'émetteur envoie une séquence de plusieurs bits, appelés des chips, pour chaque bit d'information à transmettre. Par exemple, en peut choisir d'envoyer 11101 au lieu de 0 et son inverse (00010) au lieu de 1 : dans le cas, si l'on veut transmettre l'information 010, alors on émettra les chips suivant : 11101 00010 11101. Dans cet exemple ; la séquence 11101 est ce qu'on appelle le (code d'étalement). Plus le code est long, plus le débit artificiellement démultiplié, donc plus le spectre est étalé. Par exemple, si le débit envoyé est égale à 1 Mb/s, mais avec DSSS sera bien sûr égal 11Mb/s si le code d'étalement de 11 chips : du coup, la bande de fréquence occupée par le signal est égale au double du débit de la source. Sans ce chipping, la bande occupée n'aurait qu'une largeur de 2 Mhz (deux fois 1 Mb/s).

Le DSSS présente deux intérêts importants :

- Tout d'abord, comme nous l'avons dit, le spectre de fréquences du signal est étalé, avec tous les avantages (et les inconvénients) que cela apporte, en particulier une meilleur résistance au bruit ;
- Le fait que l'on émettre plusieurs chips pour chaque bit information signifie que l'on peut avoir une redondance important, qui permet de corriger des erreurs de transmission. En résulte que la modulation DSSS étale le spectre du signal par une technique de chipping. Ceci permet avant tout de mieux résister au bruit.
  Pour communiquer, l'émetteur et le récepteur doivent se mettre d'accord sur un canal fixe à utiliser. Pour un débit de 1 Mb/s le 802.11 DSSS repose sur la modulation 2DPSK (2 Differential PSK) mais, pour un débit 2 mb/s utilisent simplement 4DPSK (4 Differential PSK). Dans les daux cas, le code d'étalement a une longueur de 11 bits et il est toujours égal

à 10110111000. Ce code fait partie d'une famille de codes aux propriétés mathématiques similaires, définie en 1953 par le mathématicien Barker.

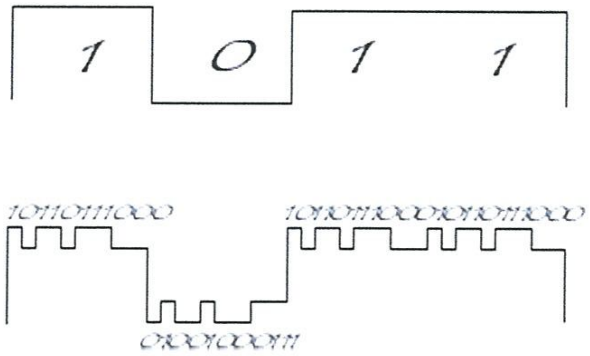


Figure 1.6 : Etalement de spectre à séquence directe (DSSS)

Pour atteindre des débits de 5.5 Mb/s ou 11 Mb/s, le 802.11b amélioré encore ce procédé en utilisant la modulation CCK (Complementary Code Keying) pour atteindre ce qu'on appelle le DSSS à haut vitesse ou HR-DSSS (High-Rate-DSSS). Celle-ci repose toujours sur le même principe de base d'étalement par chipping avec la modulation 4DPSK. Toutfois, au lieu d'utiliser toujours le même code de BARKER pour étaler le signal, elle utilise jusqu'à 64 codes différent, ce qui permet de transporter 6 bits information (car 2^6=64) en plus deux bits autorisés par la modulation 4DPSK. Ces codes, de 8 bits de longueur chacun, sont des codes complémentaires c'est-à-dire que leur propriétés mathématique permettent aux récepteur de ne pas le confondre, même s'il y a quelques erreurs de transmission, voire même un décalage dans le récepteur dû au multipath, puisqu'il y a nettement moins de redondance, on obtient un débit plus importante, en tout cas tant que la réception est bonne (donc faible distance). Puisque le résistance au multipath est meilleur, le HR-DSSS est mieux adapté en intérieur et à courtes distance que le DSSS sur BARKER.

Malheureusement, alors que le FHSS peut sauter les canaux encombrés par du bruit ou des interférences, le DSSS ne le peut pas.

Comme pour le FHSS, le standard définit pour le DSSS un mécanisme d'adaptation automatique du débit en fonction de la distance. Ainsi, à courte distance la modulation sera le HR-DSSS à 11 Mb/s (8 bits information pour 8 chips émis). Plus, loin en passe automatiquement à 5.5Mb/s (4 bits information pour 7 chips émis). Ensuite, on descend à 2 Mb/s en utilisent le DSSS/BARKER et 4DPSK, puis à 1 Mb/s en DSSS/BARKER et 2DPSK [3].

4-4-2- La modulation OFDM

La modulation OFDM (Orthogonal Frequency Division Multiplexing), parfois appelée DMT (Discrete Multitone Modulation), est sans doute la plus puissance des trois modulations du WiFi car elle permet à la fois les débits les plus importants (54 Mb/s), la meilleur résistance au multipath, mais aussi la plus grande capacité de partage du spectre.

L'OFDM repose sur le principe de multiplexage : permettre la transmission simultanée de plusieurs communications sur une même bande de fréquence. Il existe le multiplexage par division des communications au cours du temps, qu'on appelle le TDM (Time Division Mutliplexing) : chaque communication dispose de sa tranche de temps pour émettre des données et peut utiliser l'ensemble du spectre. Le multiplexage peut également se faire en partageant les différentes communications par fréquences : c'est FDM (Frequency Division Multiplexing).

Un spectre assez large est divisé en de multiple sous-porteuse (Sub-Carriers) et les données sont émises simultanément sur chaque sous-porteuse. Malheureusement, il est alors possible d'avoir des interférences entre les sous-porteuses, ce qu'on appelle ICI (Inter-Carrier-Interference). Pour résoudre ce problème, l'OFDM utilise une fonction mathématique assez complexe pour rendre les sous-porteuses (Orthogonales), c'est-à-dire pour qu'elles n'interfèrent pas les unes avec les autres. Dans le cas du 802.11, il s'agit d'une transformation de Fourier inverse rapide IFFT (Inverse Fast Fourier Transform). Grâce à cette fonction, les porteuses sont placées dans le spectre de fréquences de telle sorte que les pics de puissance d'une porteuse donnée correspondent aux zéros des autres porteuses.

Les deux premières sous-bandes (Low et Middle) de la bande U-NII sont divisées en 8 canaux de 80 Mhz. Chaque canal est ensuite divisé en 52 sous-canaux de 300 Khz, 48 pour la transmission de données et 4 pour la correction d'erreur appelé FEC (Forward Correction Error). Le WiFi en utilise quatre comme (pilotes) qui servent à synchroniser les fréquences et à mesurer en permanance les interférences et les décalages de phase, afin de s'y adapter au mieux [3].

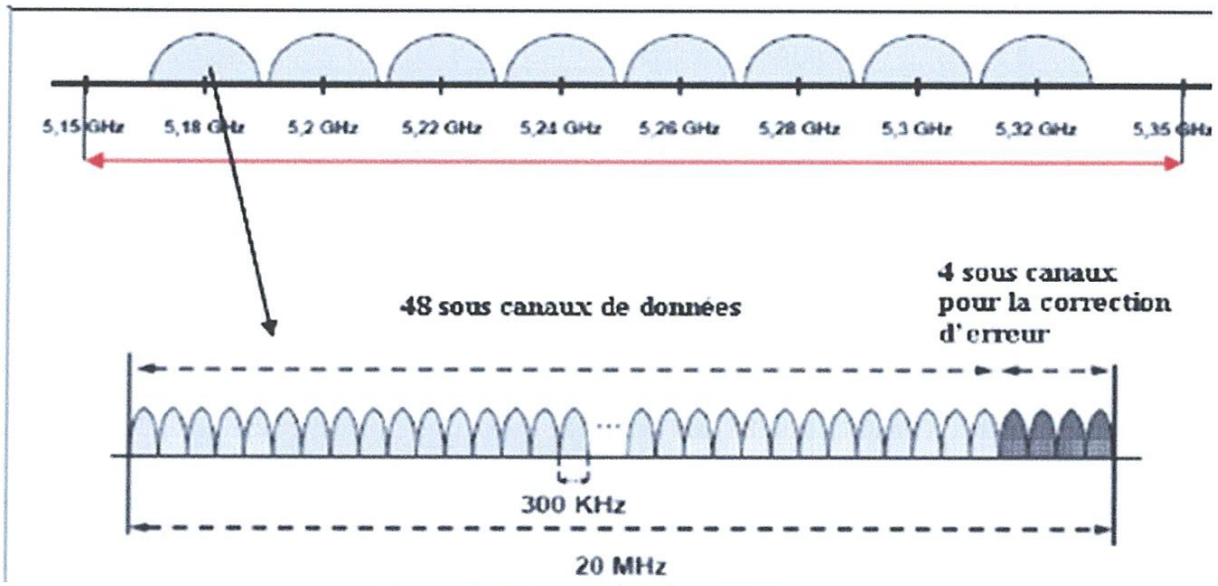


Figure 1.7 : La modulation OFDM

5- Communication entre equipements

L'architecture d'un réseau Wi-Fi est basée sur un système cellulaire. Il existe deux principaux modes de fonctionnement [1].

5-1- Le mode ad hoc

En mode ad hoc, il n'y a aucune administration centralisée. Il n'existe pas de point d'accès. Les stations terminales communiquent directement entre elles selon des liaisons point à point ou point multi point. Ces stations forment une cellule appelée *IBSS* (Idependant Basic Service Set).

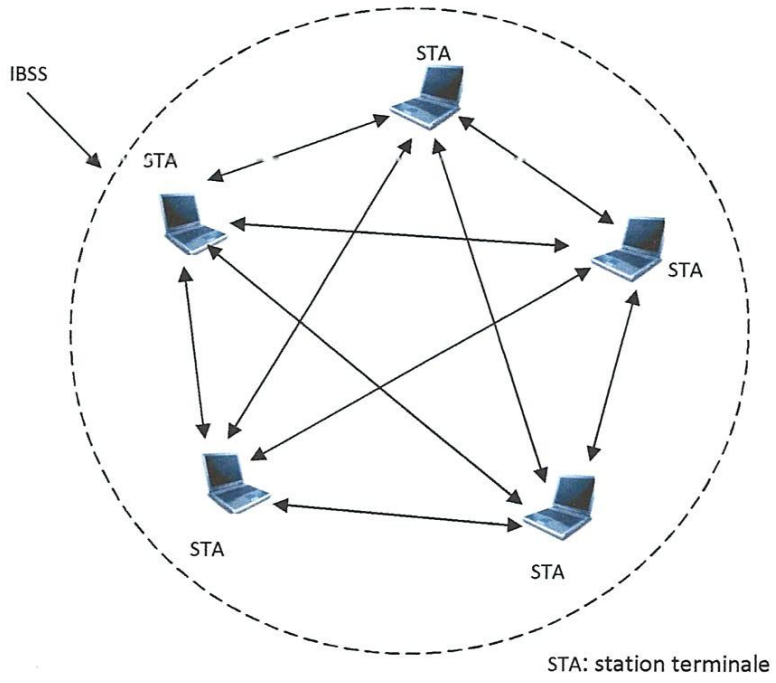


Figure 1.8 : Mode ad hoc

5-2- Le mode infrastructure

Dans ce mode, une station de base appelée Access Point (point d'accès) gère toutes les stations terminales à portée radio. Il permet aux stations terminales de communiquer entre elles et avec des stations d'un réseau filaire existant. L'ensemble constitué par le point d'accès et les stations sous son contrôle forme un BSS (Basic Service Set/Ensemble de services de base) ; la zone ainsi couverte est appelée BSA (Base Set Area).

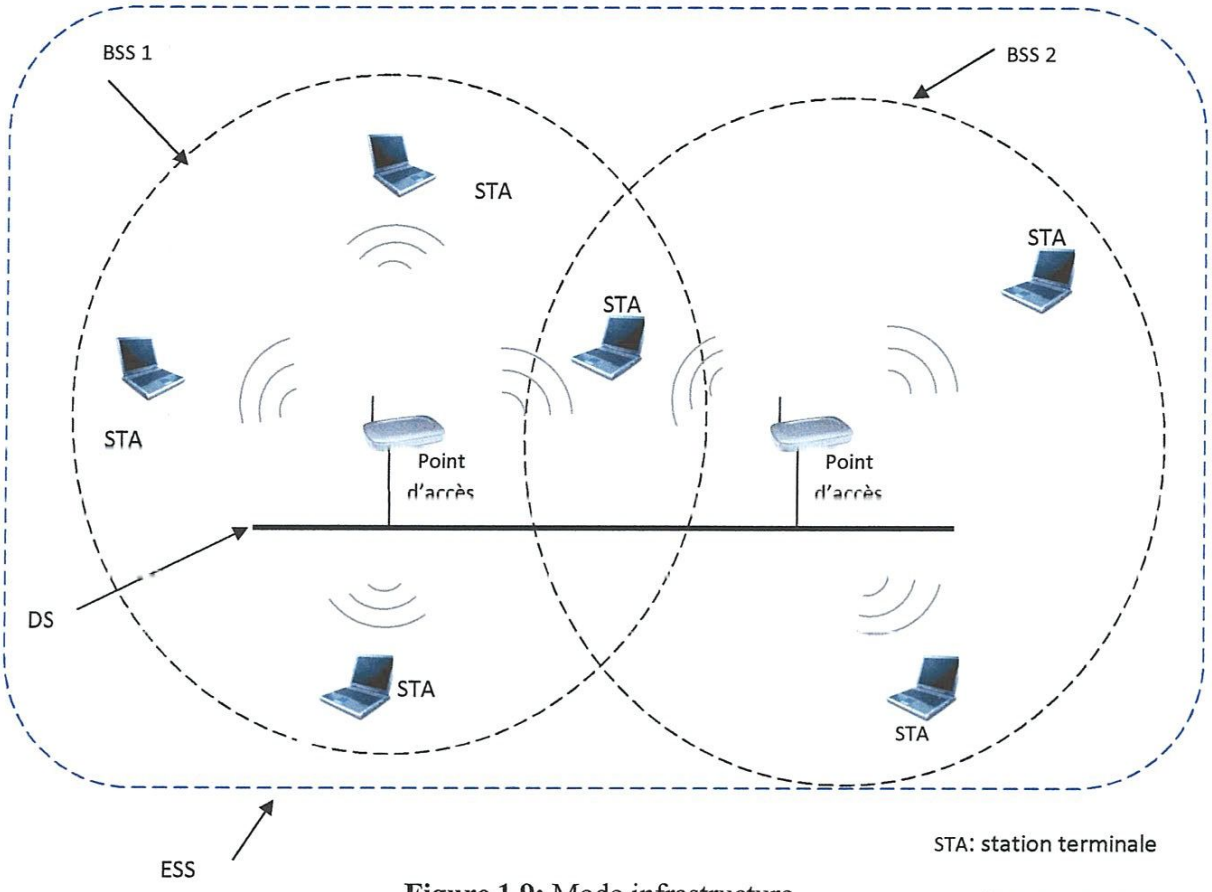


Figure 1.9: Mode infrastructure

Le BSS est identifié par un BSSID qui est généralement l'adresse MAC du point d'accès. Un ensemble de BSS forme un ESS (Extended Service Set). Les BSS (plus précisément leurs points d'accès) sont interconnectés via un DS (distribution system/système de distribution). Le système de distribution ou backbone est implémenté indépendamment de la partie sans fil, c'est généralement un réseau Ethernet, mais il peut aussi être un réseau Token Ring, FDDI ou un autre réseau local sans fil. Cette architecture permet aussi d'offrir aux usagers mobiles l'accès à d'autres ressources (serveurs de fichier, imprimante, etc.) ou d'autres réseaux (Internet).L'ESS est identifié par un ESSID communément appelé SSID est qui constitue le nom du réseau. Le SSID est un premier niveau de sécurité, vu que la station doit connaître ce SSID pour pouvoir se connecter au réseau.

Dans le mode infrastructure, Il existe plusieurs topologies qui dépendent des caractéristiques de la zone à couvrir, du nombre d'utilisateurs, des besoins de mobilité, du choix des canaux et du trafic. En fonction de ces critères, on opte pour l'une des topologies suivantes [5]:

– ***Topologie à cellules disjointes***

Cette topologie, illustrée à la figure 1.10 se justifie en cas de faible nombre de canaux disponibles ou si l'on souhaite éviter toute interférence. Il est toutefois difficile de discerner si les cellules sont réellement disjointes, sauf lorsqu'elles sont relativement éloignées. Dans ce type d'architecture, la mobilité n'est pas possible.

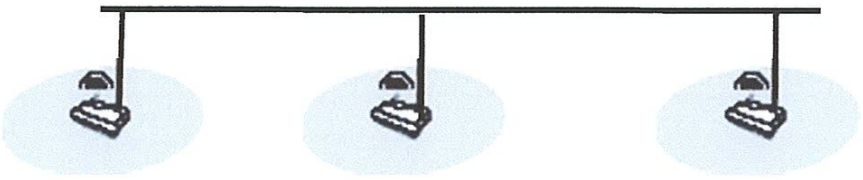


Figure 1.10 : Topologie à cellules disjointes

– ***Topologie à cellules partiellement recouvertes***

Cette topologie, illustrée à la figure 1.11 est caractéristique des réseaux sans fil. Elle permet d'offrir un service de mobilité continue aux utilisateurs du réseau, tout en exploitant au maximum l'espace disponible. Cependant, elle exige en contrepartie une bonne affectation des canaux afin d'éviter les interférences dans les zones de recouvrement. Cette topologie est à privilégier en cas de déploiement d'une solution de téléphonie IP WiFi.

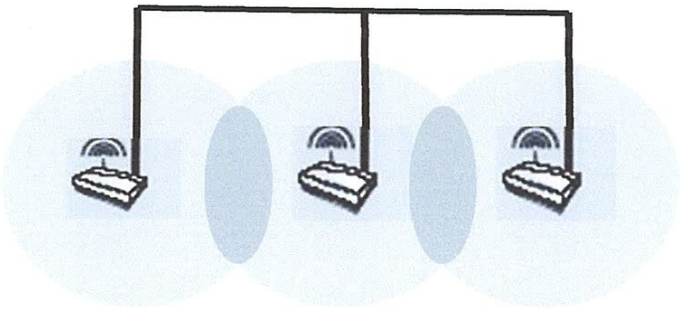


Figure 1.11 : Topologie à cellules partiellement recouvertes

– ***Topologie à cellules recouvertes***

Dans cette topologie, illustrée à la figure 1.12, une bonne configuration des canaux est également nécessaire afin d'éviter les interférences. Elle permet, dans un espace restreint pratiquement à une cellule, de fournir la connectivité sans fil à un nombre important d'utilisateurs. C'est pourquoi elle est utilisée dans les salles de réunion ou lors des grandes conférences dans le but de fournir un accès sans fil fiable à tous les participants.

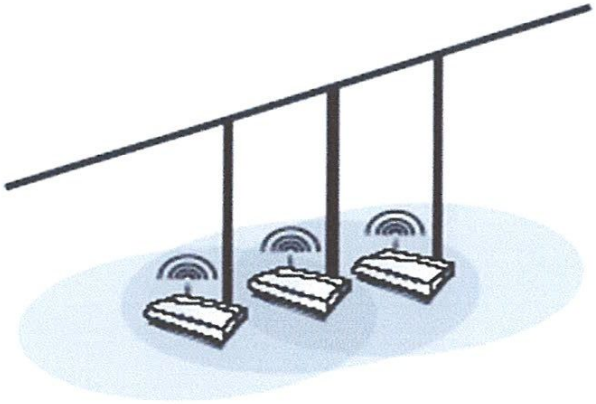


Figure 1.12 : Topologie à cellules recouvertes

6- Communication entre équipements en mode infrastructure

Dans le mode infrastructure les stations se trouvant dans la même cellule sont fédérées autour du point d'accès avec lequel ils rentrent en communication. Cette communication est basée sur un système distribué pour l'accès au canal de communication. Le système d'accès multiple n'existe pas en WiFi, ce sont alors les techniques d'accès citées précédemment, qui permettent de résoudre le problème de partage du canal de communication [5].

6-1- Communication entre une station et un point d'accès

Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal une requête de sondage (Probe Request), contenant l'ESSID pour lequel il est configuré, ainsi que les débits que son adaptateur sans fil supporte. Si aucun ESSID n'est configuré, la station écoute le réseau à la recherche d'un ESSID.

En effet, chaque point d'accès diffuse régulièrement (0.1 seconde) une trame balise contenant les informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé, mais il est possible (même recommandé) de désactiver cette option. A chaque requête de sondage reçue, le point d'accès vérifie l'ESSID et la demande de débit présent dans la trame balise. Si l'ESSID correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle elle se trouve. Le débit est d'autant meilleur que le point d'accès est proche.

6-2- Communication entre deux stations à travers un point d'accès

Pour entrer en communication avec une station destinatrice B, la station émettrice A doit d'abord passé par le point d'accès pour son authentification et son association. Pour cela, la station A envoie une trame de demande d'authentification au point d'accès qui lui répond avec une trame réponse d'authentification.

Après l'échange de trames d'authentification, la station A envoie au point d'accès une trame de requête d'association, ce dernier envoie à son tour une trame de réponse à la requête d'association permettant ainsi à la station A d'avoir accès à la station B.

Avant de transmettre ses données à la station B, la station A lui envoie d'abord un paquet d'appel sous forme d'une trame RTS. Si cette trame est correctement reçue par la station B, alors cette dernière l'acquitte avec une trame CTS. La station A vérifié si la trame CTS est reçue sans erreur, auquel cas elle peut envoyer ses données. Au cas échéant la procédure sera reprise.

6-3- Le Handover

Les stations qui se déplacent d'une cellule à une autre doivent rester synchronisées pour maintenir la communication. Le point d'accès envoie périodiquement des trames de gestion, plus précisément des trames balises (Beacon frame) qui contiennent la valeur de son horloge, aux stations qui peuvent ainsi se synchroniser. La station terminale choisit son point d'accès en fonction de la puissance du signal du point d'accès, du taux d'erreurs par paquet et de la charge du réseau. La station demande à accéder à une BSS dans deux cas :

- Terminal qui était éteint et qui par la suite est mis sous tension
- Terminal en déplacement

L'adaptateur réseau est capable de changer de point d'accès selon la qualité des signaux reçus et provenant des différents points d'accès. Les points d'accès peuvent aussi communiquer entre eux et échanger des informations concernant les stations grâce au système de distribution (DS).

Pour pouvoir s'associer à un point d'accès, c'est-à-dire établir un canal de communication avec le point d'accès, la station procède à une écoute de l'environnement.

- *Ecoute passive* : la station attend la réception d'une trame balise appelée Beacon Frame venant du point d'accès.

- *Ecoute active* : la station, après avoir trouvé le point d'accès le plus approprié, lui envoie une demande d'association via une trame appelée Probe Request Frame.

La station peut envoyer une requête d'association à un ou plusieurs points d'accès. Le point d'accès envoie une réponse à la requête. Si c'est un échec, la station prolonge son écoute. En cas de succès, la station accepte l'association. Le point d'accès signale la nouvelle association au DS, qui met à jour sa base de données puis informe l'ancien point d'accès afin qu'il puisse libérer ses ressources [5].

7- Le modèle en couche IEEE

La norme IEEE 802.11 repose sur une architecture en couche définie par le standard IEEE et couvre les deux premières couches du modèle OSI, c'est à dire la couche physique et la couche liaison de données [6]:

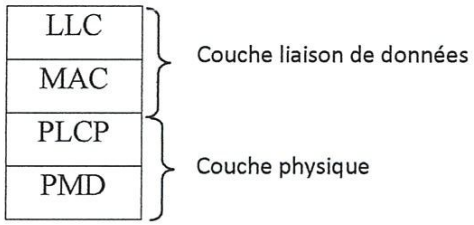


Figure 1.13 : Modèle IEEE

7-1- La couche liaison de données

Elle est aussi composée de deux sous couches.

7-1-1- La sous couche LLC

La sous couche LLC de la norme IEEE 802.11 utilise les mêmes propriétés que la sous couche LLC de la norme IEEE 802.3, ce qui correspond à un mode avec connexion et avec acquittement des données.

7-1-2- La sous couche MAC

La sous couche MAC 802.11 intègre les mêmes fonctionnalités que la sous couche MAC 802.3, à savoir :

- la procédure d'allocation du support
- l'adressage des paquets
- le formatage des trames
- le contrôle d'erreurs CRC.

Dans la norme 802.11, la sous couche MAC réalise également la fragmentation et le réassemblage des trames.

7-2- La couche physique

Elle assure la transmission des données sur le support, elle est constituée de deux sous couches : PMD et PLCP

7-2-1- La sous couche PMD

Elle spécifie le type de support de transmission, le type d'émetteur-récepteur, le type de connecteur et la technique de modulation et de démodulation.

7-2-2- La sous couche PLCP

Elle s'occupe de la détection du support et fournit un signal appelé CCA (Clear Channel Assessment) à la sous couche MAC pour lui indiquer si le support est occupé ou non. L'IEEE a

défini quatre types de couches physiques différentes caractérisées chacune par une technique de modulation précise. Il s'agit des techniques suivantes :

- *FHSS*
- *DSSS*
- *OFDM*
- *Infrarouge*

7-3- Format de la trame MAC

La trame MAC est la trame encapsulée au niveau de la sous couche MAC, son format est le suivant :

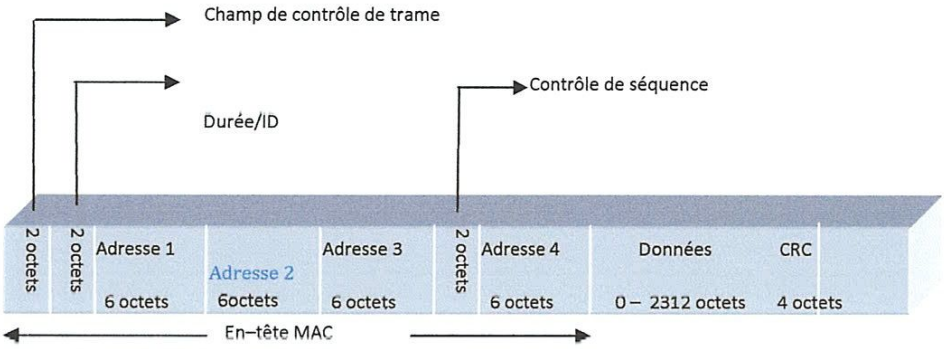


Figure 1.14 : Format de la trame MAC

7-3-1- ***Le champ de contrôle***

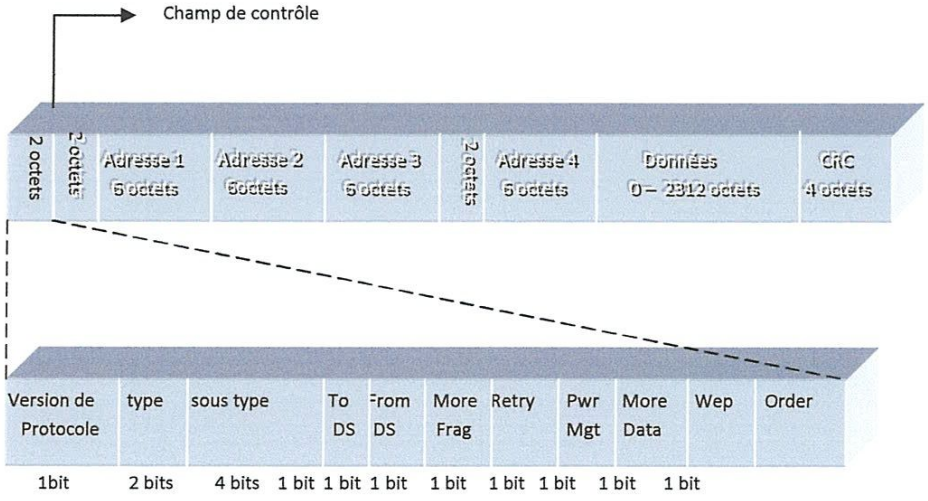


Figure 1.15 : Champ de contrôle

- Le champ *version de protocole*
  Il contient deux bits qui peuvent être utilisés pour reconnaître des versions futures possibles du standard 802.11. Dans la version courante, la valeur est fixée à 0.
- Le champ *type* indique le type de trame à transmettre sur le réseau. Il existe trois types de trames : les trames de gestion, les trames de contrôle et les trames de données.

Type	00	01	10	11
Nature	Gestion	Contrôle	Données	Réservé

Tableau 1.7 : Types de trames

- Pour chaque type de trame (valeur du champ type), le champ *sous type* nous donne la fonction à réaliser.

Les trames de gestion : Elles sont utilisées lors des procédures d'association et de désassociation d'une station avec le point d'accès, de la synchronisation et de l'authentification.

Sous type	Nature du sous type
0000	Requête d'association
0001	Réponse à une requête d'association
0010	Requête de réassociation
0011	Réponse une requête de réassociation
0100	Interrogation (probe) requête
0101	Interrogation (probe) réponse
1010	Désassociation
1011	Authentification
1100	Désauthentification

Tableau 1.8 : Trames de gestion

Les trames de contrôle : Il en existe plusieurs parmi lesquelles on peut citer :

- La trame RTS : paquet spécial d'appel envoyé par la station source avant le paquet de données.
- La trame CTS : envoyée par la station destination après avoir reçu le paquet spécial d'appel.
- La trame d'accusé de réception
- La trame PS-Poll
- La trame CF-End
- La trame CF-End + CF –ACK

Sous type	Nature du sous type
1010	PS-Poll
1011	RTS (Request To Send)
1100	CTS (Clear To Send)
1101	ACK (Acknowlegment)/Acquittement

Tableau 1.9 : Trames de contrôle

Les trames de données : Elles contiennent les données utilisateurs, notamment les adresses source, destination et BSSID, ce qui permet aux points d'accès d'acheminer correctement les trames vers leurs destinations.

Sous type	Nature du sous type
0000	Données
0001	Données+CF-ACK
0010	Données+CF-Poll
0011	Données+CF-ACK+CF-Poll
0101	CF-ACK (pas de données)
0110	CF-Poll (pas de données)
0111	CF-ACK+CF-Poll (pas de données)

Tableau 1.10 : Trames de données

- *To DS* (pour le système de distribution) : Le bit est à 1 lorsque la trame est adressée au point d'accès pour qu'il l'a fasse suivre au DS, sinon ce bit est à 0.

- *From DS* (Venant du système de distribution) : Ce bit est mis à 1 si la trame vient du DS, dans le cas contraire il est à 0.
- *More Frag* (d'autres fragments) : Ce bit est mis à 1 quand il y a d'autres fragments qui suivent le fragment en cours. Il est à 0 s'il ne reste plus de fragments à transmettre. Un ensemble de fragments forme un paquet.
- *Retry* (Retransmission) : Ce champ renseigne si la trame est transmise pour la première fois ou si elle est retransmise.
- *Pwr Mgt* (gestion d'énergie) : Ce champ indique l'état de la station après la transmission. Si le bit est à 0, la station terminale est en mode normal. Si le bit est à 1, la station terminale est en état d'économie d'énergie.
- *More Data* (d'autres données) : Le point d'accès utilise ce champ pour indiquer à une station terminale en état d'économie d'énergie, s'il a ou non des trames en attente qui lui sont destinées.
- *WEP* (sécurité) : Ce champ permet de déterminer si la station utilise le cryptage.
- *Order* (ordre) : Ce champ permet de vérifier si l'ordre de réception des fragments est le bon.

7-3-2- Le champ de Durée / ID

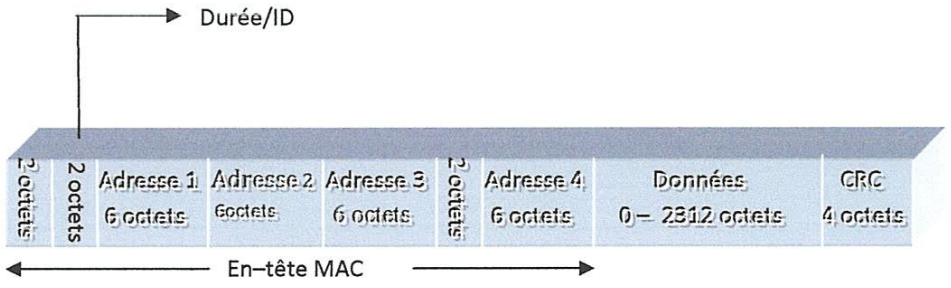


Figure 1.16 : Format de la trame

Ce champ a deux sens qui dépendent du type de trame :

- Pour les trames de Polling en mode d'économie d'énergie, c'est l'ID de la station.
- Dans les autres trames c'est la valeur de durée utilisée pour le calcul du vecteur d'allocation (NAV).

Les champs adresse 1, 2, 3 et 4

Ces champs correspondent à des adresses MAC de stations sources, de stations de destination ou de BSSID (Base services Set Identifier). Les adresses MAC de ces différents champs spécifient des types de transmissions bien précis.

To DS	From DS	Adresse 1	Adresse 2	Adresse3	Adresse 4	Cas considéré
0	0	Destination	Source	BSSID	Non utilisé	Cas 1
1	0	BSSID	Source	Destination	Non utilisé	Cas 2
0	1	Destination	BSSID	Source	Non utilisé	Cas 3
1	1	BSSID (destination)	BSSID (source)	Destination	Source	Cas 4

Tableau 1.11 : Signification des adresses dans la trame des données

- *L'adresse 1* est toujours l'adresse du récepteur. Si le bit To DS est à 1, c'est l'adresse du point d'accès qui est généralement le BSSID. Par contre si le bit est à 0, il s'agit de l'adresse de la station de destination (Transmission entre deux stations terminales d'un même IBSS).
- *L'adresse 2* est toujours l'adresse de l'émetteur. Si le bit From DS est à un, c'est l'adresse

du point d'accès (BSSID). S'il est à 0, c'est l'adresse de la station terminale source (Transmission entre deux stations terminales d'un même BSS).

- *L'adresse 3* correspond à l'adresse de l'émetteur lorsque le bit From DS est à 1.Sinon et si le bit To DS vaut 1, elle correspond à l'adresse de la station de destination (Transmission entre point d'accès et une station terminale sous son contrôle).
- *L'adresse 4* est spécialement utilisée dans le cas d'une communication entre 2 points d'accès faisant intervenir le système de distribution (DS). Les bits To DS et From DS seront donc tous les deux à 1 (Transmission entre deux stations terminales d'un même ESS mais n'appartenant pas au même BSS).

Le contrôle de séquence

C'est un champ sur 12 bits utilisé pour attribuer à chaque trame un numéro de séquence entre 0 et 4095. Le numéro de séquence est incrémenté de 1 à chaque fois qu'une trame est envoyée. Au cours de la transmission d'une trame, quatre bits sont utilisés pour coder le numéro du fragment dans l'ordre d'envoi des fragments.

Le CRC

Il s'étend sur 32 bits. Le CRC sert au contrôle d'erreur à partir d'un polynôme générateur standard :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x + x^4 + x^2 + x + 1$$

7-4- Le format de la trame Wi-Fi

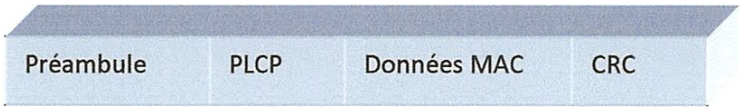


Figure 1.17 : Trame WiFi

a. *Le préambule* est dépendant de la couche physique et contient deux champs : un champ de synchronisation Synch et un champ SFD. Le champ Synch est utilisé par le circuit physique pour sélectionner l'antenne à laquelle se raccorder. Quant au champ SFD, il est utilisé pour délimiter le début de la trame.

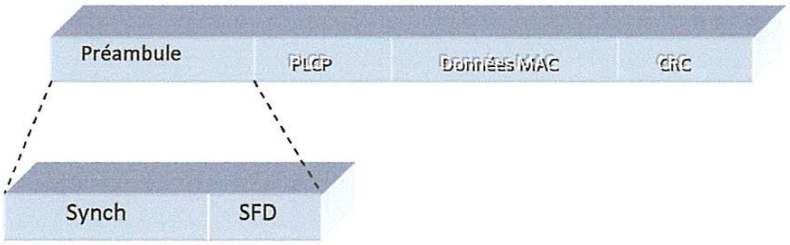


Figure 1.18 : Préambule

La longueur du champ préambule varie selon la technique de modulation utilisée au niveau de la couche physique.

Pour la technique de modulation FHSS, le champ Synch s'étend sur 80 bits et le champ SFD sur 16

bits. Dans la technique DSSS, il existe deux formats possibles du champ Préambule : un format par défaut avec un champ Synch long de 128 bits, et un format avec un champ Synch court de 56 bits. Le deuxième format est utilisé pour améliorer les performances du réseau dans les cas de données critiques telles que la voix, la VoIP (Voice over IP). Le préambule court est également intéressant lorsque les trames doivent être fragmentées (on transmet moins de bits non utiles).

b. *L'en-tête PLCP* contient les informations logiques utilisées par la couche physique pour décoder la trame. Dans la modulation FHSS l'en-tête PLCP se présente comme suit :

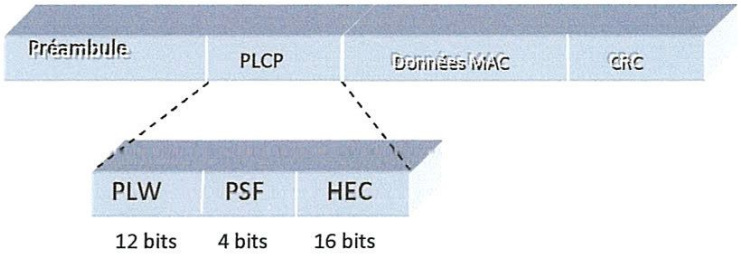


Figure 1.19 : En-tête PLCP-FHSS

- Le champ *PLW* sur 12 bits indique le nombre d'octets que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.
- Le *fanion de signalisation PSF* s'étend sur 4 bits et indique le débit de transmission des données MAC.
- Le champ *HEC* utilise un CRC sur 16 bits pour la vérification de l'intégrité de l'en-tête PLCP.

Dans la modulation DSSS, l'en-tête PLCP se présente sous une autre forme.

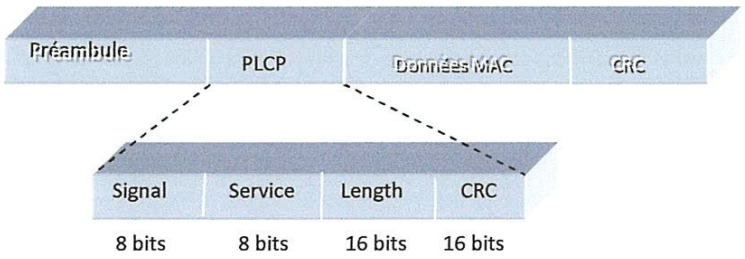


Figure 1.20 : En-tête PLCP-DSSS

Elle est composée de quatre champs.

- Le champ *Signal* s'étend sur 8 bits et indique la modulation à utiliser pour l'émission et la réception des données.
- Le champ *Service* sur 8 bits est réservé pour une utilisation future.
- Le champ *Length* de 16 bits indique le nombre de microsecondes nécessaires pour transmettre les données.
- Le champ de *contrôle d'erreurs* CRC sur 16 bits.

c. Le champ de *données MAC* a été détaillé précédemment.

d. Le champ de *contrôle d'erreur* CRC sur 16 bits qui permet de vérifier l'intégralité des données.

8- Les techniques d'accès

La norme 802.11 ne prévoit pas un système d'accès multiple, il se pose alors un problème de partage du canal de communication entre les différentes stations. C'est ainsi que l'IEEE définit au niveau de la sous couche MAC, deux techniques d'accès que sont la DCF (Distribution Coordination Function) et la PCF (Point Coordination Function) [5].

8-1- DCF (Distribution Coordination Function)

La DCF est conçue pour prendre en charge le transport des données asynchrones dans lequel tous les utilisateurs désirant transmettre des données ont une chance égale d'accéder au support de transmission. Ce mode d'accès à compétition repose sur la technique CSMA/CA. Le CSMA/CA évite les collisions en utilisant des trames d'acquittement, ACK (Acknowledgment) : un acquittement est envoyé par la station de destination pour confirmer que les données ont été reçues de manière intacte.

L'accès au support est contrôlé par l'utilisation d'espaces inter-trames ou IFS (Inter-Frame Spacing), qui correspondent aux intervalles de temps entre la transmission de deux trames. Ces espaces inter-trames correspondent à des périodes d'inactivité sur le support de transmission. L'IEEE 802.11 définit trois types d'espaces inter-trames :

- SIFS (Short Initial Inter-Frame Spacing) : c'est le plus court des espaces inter-trames. Il permet de séparer les trames au sein d'un même dialogue. Il dure 28 µs.
- PIFS (PCF-IFS) : utilisé par le point d'accès pour bénéficier d'une priorité supérieure dans le cas d'un accès au support contrôlé. Le PIFS correspond à la valeur du SIFS auquel on ajoute un timeslot de 78 µs, défini dans l'algorithme de Backoff.
- DIFS (DCF-IFS) : inter-trame pour l'accès distribué, utilisé lorsqu'une station veut commencer une nouvelle transmission. Il correspond à la valeur du PIFS auquel on ajoute un temps de128 µs.

Les terminaux d'un même BSS peuvent écouter l'activité de toutes les stations qui s'y trouvent. Ainsi, lorsqu'une station envoie une trame, les autres stations l'entendent et pour éviter une collision, ils mettent à jour un timer appelé NAV (Network Allocation Vector). Le NAV permet de retarder les transmissions. Lors d'un dialogue entre deux stations, le NAV est calculé par rapport au champ de Durée/ID des différentes trames qui sont envoyées (données, ACK, SIFS etc.). Les autres stations ne pourront transmettre que lorsque le NAV atteint la valeur zéro.

Une station, avant de transmettre écoute d'abord le support. Si aucune activité n'est détectée pendant une durée correspondant à un DIFS, elle peut alors transmettre. Par contre si le support est occupé, elle prolonge son écoute. Lorsque le support devient libre, la station retarde encore sa transmission en utilisant l'algorithme de Backoff.

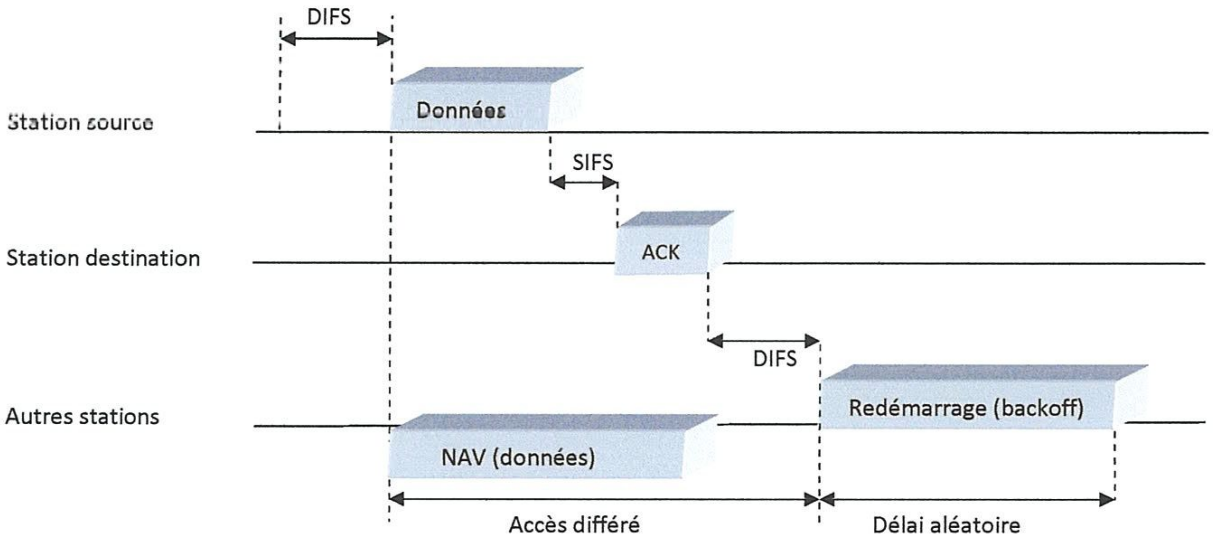
Si les données envoyées ont été reçues de manière intacte, la station destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer la bonne réception des données.

L'algorithme de Backoff permet de résoudre le problème d'accès simultané au support. Initialement, une station calcule la valeur d'un temporisateur appelé timer Backoff compris entre zéro et sept et correspondant à un certain nombre de timeslots. Lorsque le support est libre, les stations décrémentent le timer et pourront transmettre lorsque celui-ci atteint la valeur zéro. Si le support est de nouveau occupé avant que le temporisateur n'atteigne la valeur zéro, la station bloque le temporisateur. Lorsque plusieurs stations atteignent la valeur zéro au même instant, une collision se produit et chaque station doit régénérer un nouveau timer, compris cette fois-ci entre zéro et quinze.

Pour chaque tentative de retransmission, le timer croît de la façon suivante :

$$[2^{2+i} * ranf(\ )] * timeslot$$

i correspond au nombre de tentatives consécutives d'une station pour l'envoie d'une trame et ***ranf( )***, à une variable aléatoire uniforme comprise entre 0 et 1.



ACK: acknowledgement/ acquittement

DIFS: distributed coordination function

Figure 1.21 : Procédé de transmission dans le CSMA/CA

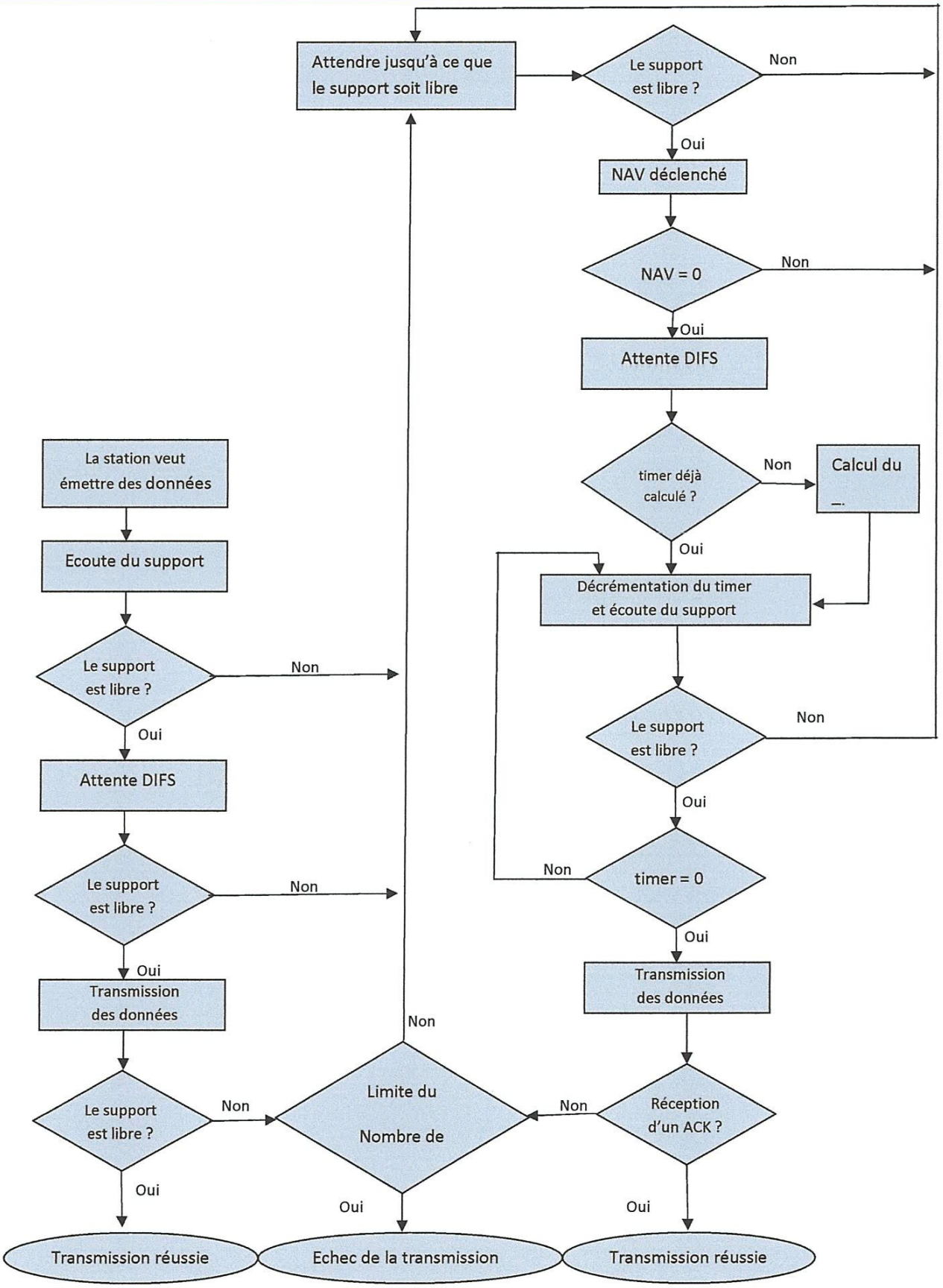


Figure 1.22 : Mécanisme du CSMA/CA

8-2- PCF (Point Coordination Function)

La PCF est un mode d'accès sans contention. Elle est basée sur l'interrogation successive des stations (polling) contrôlées par le point d'accès de façon à organiser les transmissions suivant un multiplexage temporel dynamique du canal de communication. Pour cela, les stations envoient des trames spéciales appelées PR (Polling Request) auxquelles le point d'accès répond en envoyant les données demandées. Pour contrôler l'accès au support, le point d'accès dispose d'une priorité supérieure en utilisant des inter trames PIFS qui sont plus courtes que les inter trames DIFS utilisées par les stations. Toutefois, le point d'accès doit s'assurer que les stations puissent accéder au support au moyen de la technique DCF, c'est pourquoi les deux modes sont alternés : il existe une période dite CFP (Contention Free Period) pour la PCF et une période dite CP (Contention Period) pour la DCF alternées par une trame balise permettant de synchroniser les stations.

9- Avantage des réseaux sans fil

On peut distinguer deux grandes catégories : les avantages métier principaux et les avantages opérationnels. Les avantages métier principaux regroupent les éléments contribuant à améliorer la productivité des utilisateurs, à rationaliser les processus commerciaux existants ou à permettre la mise en place de nouveaux processus commerciaux. Les avantages opérationnels concernent des points tels que la réduction des coûts de gestion ou la diminution des dépenses d'investissement [2].

9-1- Principaux avantages métier

Le principal avantage que les réseaux locaux sans fil est probablement le gain de souplesse et de mobilité. Le personnel est affranchi de son poste de travail et peut se déplacer librement dans les locaux, sans être déconnecté du réseau. Voici quelques exemples illustrant ces propos.

• Les employés amenés à se déplacer entre différents bureaux, ou bien les télétravailleurs de passage au siège de l'entreprise, évitent perte de temps et ennuis grâce à la connexion transparente au réseau local de l'entreprise. La connexion est quasi-instantanée et accessible depuis tout endroit couvert par le réseau local sans fil : inutile donc de rechercher une prise réseau, un câble voire une personne du service informatique pour vous connecter.

• Les employés chargés de la gestion des informations restent joignables où qu'ils se trouvent dans le bâtiment. Grâce au courrier électronique, aux agendas informatisés et aux technologies de messagerie instantanée, le personnel peut rester en ligne, même durant une réunion ou lorsqu'il est amené à s'éloigner de son poste de travail.

• Les informations en ligne sont disponibles en permanence. Les réunions ne doivent plus être interrompues pendant que quelqu'un part à la recherche du rapport des chiffres du mois précédent ou de la mise à jour d'une présentation. Ceci peut considérablement améliorer la qualité et la productivité des réunions.

• L'organisation jouit d'une souplesse accrue. Le personnel n'étant plus lié à un poste de travail donné, des déplacements simples et rapides de postes de travail ou même de bureaux entiers sont désormais possibles, afin de s'adapter aux structures des équipes et des projets. Ceci facilite le travail d'équipe et permet une collaboration plus productive au sein-même des équipes.

• L'intégration de nouveaux périphériques et applications dans l'environnement informatique de l'entreprise évolue de façon très sensible.

9-2- Avantages opérationnels

Les avantages opérationnels de la technologie réseau local sans fil, c'est-à-dire les caractéristiques permettant de réduire les investissements et les coûts opérationnels, peuvent se résumer comme suit:

• Les coûts d'équipement réseau des bâtiments sont considérablement réduits. Bien que la plupart des bureaux soient pré câblés, certains espaces de travail ne le sont pas.

• Le réseau peut facilement être adapté aux niveaux de besoin changeants en fonction de l'évolution de l'organisation, ou même d'un jour à l'autre ; il est infiniment plus simple de déployer une concentration supérieure de points d'accès sans fil sur un site donné que d'augmenter le nombre de ports réseau câblés.

• Les investissements ne sont plus liés aux bâtiments : les infrastructures de réseau sans fil peuvent être déplacées facilement vers un nouveau site, tandis que le câblage physique demeure dans les bâtiments.

10- Problèmes spécifiques aux réseaux sans fils de type IEEE 802.11

10-1- Support de transmission

Malgré leurs nombreux avantages, les réseaux sans fil posent d'énormes problèmes liés au support de transmission. Les ondes radio *se propagent* dans l'air, *en ligne droite*, à la vitesse de la lumière et peuvent être déviées par réflexion, réfraction ou diffraction à cause des obstacles rencontrés sur leur trajectoire. Les ondes radio peuvent même être totalement absorbées.

L'existence d'interférences, principalement dues aux réflexions multiples, a des conséquences néfastes sur les paramètres de la liaison c'est-à-dire sur le taux d'erreur, la portée ainsi que le débit, qui sont des grandeurs étroitement liées.

Parallèlement aux problèmes dus au support de propagation, la sécurité, la mobilité ainsi que la qualité de service (fonction de l'application utilisée) restent les maillons faibles des réseaux sans fil [6].

10-2- Sécurité

10-2-1- Présentation

Bien que les réseaux sans fil offrent la mobilité ainsi que la rapidité et la facilité de déploiement, la sécurité demeure un réel problème. La propagation dans l'espace fait que n'importe quel individu ayant des équipements d'écoute appropriés (adaptateur radio, antenne directive, scanner) peut écouter le trafic sur le réseau (écoute passive).

D'autres attaques menacent l'intégrité d'un réseau comme l'intrusion ou la dissimulation d'identité. Avec l'intrusion, un étranger pénètre un système de communication puis accède au système d'information de l'entreprise. Dans la dissimulation d'identité, un destinataire reçoit un message en provenance d'une personne qu'il croit connaître mais dont l'identité a été usurpée.

Type d'Attaque	Solution préconisée
Intrusion	Contrôle d'accès
Dissimulation	Identification

Tableau 1.12 : Types d'attaques et solutions préconisées

10-2-2- Principales attaques

L'attaque d'un réseau nécessite l'utilisation d'une station espionne située dans la zone de couverture ou en dehors de celle-ci à condition qu'elle soit munie d'une antenne directive.

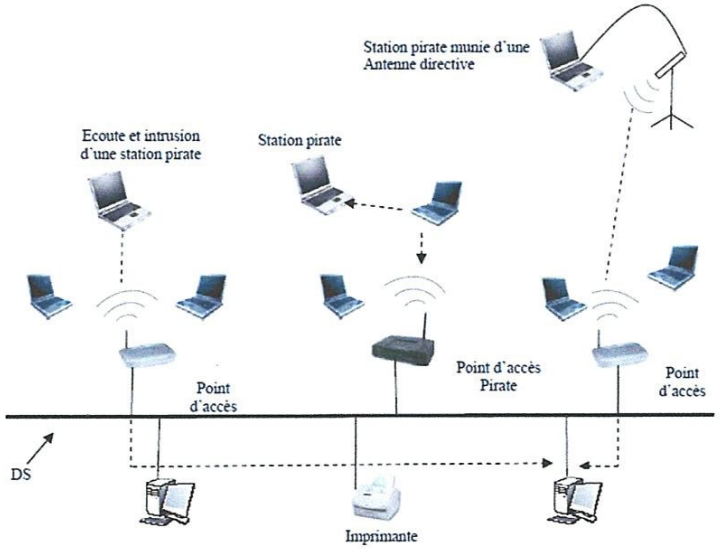


Figure 1.23 : Différents cas d'attaque

- **L'interception des données**: En absence de système de cryptage efficace, il est facile de récupérer le contenu des données qui circulent sur le médium.
- **L'intrusion dans le système** : Elle consiste, pour une station étrangère au réseau, à se connecter au point d'accès puis à intégrer le réseau.
- **Attaque de l'homme au milieu** : Il suffit de mettre en place un point d'accès étranger dans la zone de couverture du réseau WLAN afin d'intégrer le réseau. Les stations cherchent alors à se connecter à ce point d'accès (pirate) en fournissant ainsi les informations concernant le réseau auquel elles sont rattachées. L'exploitation de ces informations permet aux pirates de se connecter au réseau.
- **Attaque par porte dissimulée** : Cette technique est identique à la précédente, la seule différence provient du fait que le point d'accès pirate est directement raccordé au système de distribution du réseau.

10-3- Qualité de service

10-3-1- Présentation

La qualité de service est liée au type d'application, chaque application étant caractérisée par ses propres besoins. Pour la transmission de données (web, FTP), il n'y a pas besoins de temps réel, le flux peut être irrégulier mais les erreurs ne sont pas tolérées. Pour la voix et la vidéo, au contraire, les flux doivent être réguliers (délai constant), mais le système est plus tolérant aux erreurs.
Les principaux paramètres de qualité de service qui sont pris en compte dans les applications temps réels sont :

- *Le délai de transit* : c'est le temps que met le paquet pour transiter de l'émetteur au récepteur. Il dépend du temps de propagation et du délai de congestion (temps passé dans les files d'attente du point d'accès). Sachant que les mémoires tampon des points d'accès sont de taille limitée, tout paquet arrivant dans une file pleine est perdu.
- *Le taux d'erreur* : c'est le pourcentage de paquets erronés par flux.
- *La gigue :* c'est la variation de délai dans les temps d'arrivée des différents paquets.
- *Le débit* : c'est la quantité d'information par unité de temps circulant sur le réseau.

10-3-2- Dégradation gracieuse de service

La mobilité d'un hôte a un impact très important sur ces paramètres de qualité. En effet, lorsqu'une station se déplace d'un BSS à un autre, l'information doit être relayée par le point d'accès auquel la station était associée précédemment, il en résulte alors de courtes périodes durant lesquelles la station terminale ne reçoit plus d'information. Par ailleurs, vue que la mobilité des stations est imprévisible, plusieurs utilisateurs peuvent se retrouver simultanément dans une même cellule, les ressources de la cellule en terme de bande passante seront alors insuffisantes pour satisfaire tous les paramètres de qualité.

10-3-3- Allocation de la bande passante

Pour remédier à la dégradation gracieuse du service, il est nécessaire que la bande passante soit allouée de façon optimale, pour cela deux solutions sont retenues :

- *Solution N°1 : Attribuer une priorité aux connexions déjà ouvertes* Les connexions déjà ouvertes (en handover) doivent être prioritaires sur les connexions qui tentent de s'ouvrir en parallèle, il est souhaitable d'utiliser un système avec des priorités pour pénaliser d'abord les connexions définies comme étant les moins importantes. Mais il n'est pas toujours possible de trouver un ordre total des priorités de toutes les applications. De plus, un utilisateur avec des connexions de faible priorité peut perdre toutes ses connexions, ce qui n'est bien sûr pas souhaitable.
- *Solution N°2 : Spécification des préférences (Profil de perte)* Chaque application a des besoins qui lui sont propres, il est alors possible que chaque utilisateur spécifie, lors de l'établissement de la connexion, ses préférences concernant les pertes d'information acceptables. Ce profil est utilisé en même temps que d'autres paramètres pour allouer la bande passante aux différents utilisateurs mobiles présents dans une cellule.

10-4- Mobilité

L'un des problèmes majeurs des réseaux locaux sans fil est la gestion de la mobilité des utilisateurs. La difficulté réside dans l'adressage IP, le routage des paquets et la localisation des ressources lors du déplacement des utilisateurs. L'environnement mobile pose également un problème de sécurité.

11- Les Applications du Wi-Fi [3]

- **L'extension du réseau d'entreprise :** Si une entreprise désir ajouter une extension du réseau avec des point d'accès pour éviter les problèmes des câbles.
- **Le Wi-Fi à domicile :** le partage de la connexion internet à travers un modem Wi-Fi.
- **Les HOTSPOTS :** Il s'agit d'un lieu où la connexion vers un réseau Internet est possible via une connexion sans fil et grâce à un ensemble de technologies et de protocoles mis en œuvre. On parle également de borne ou de point d'accès Wi-Fi.
- **Le Wi-Fi communautaire :** c'est un type des réseaux Wi-Fi ouvert pour le public comme FON.

12- Conclusion

Dans ce chapitre nous avons commencé par les classifications des réseaux sans fil, l'apparition de standard 802.11 et la création de la technologie Wi-Fi. Ensuite nous avons établi une étude générale sur l'interface radio dans cette partie nous avons su les bandes de fréquences utilisées dans le réseau Wi-Fi, en effet l'intérêt de ces bandes de fréquences est qu'elles sont utilisée sans licence, puis nous avons présenté les modulations utilisé et les différent architecture de déploiement.

CHAPITRE II

[Etude de la Technologie HotSpot]

Partie A

[Généralité sur les HotSpot]

1- INTRODUCTION

L'implémentation d'un HOTSPOT Wi-Fi fait intervenir plusieurs processus aussi importants les uns que les autres. L'utilisation d'un accès internet est sous la responsabilité du fournisseur d'accès on cas d'une utilisation frauduleuse ou abusif le FAI est responsable devant les autorités concerné selon les lois et les décrets de l'**ARPT** (l'**A**utorité de **R**égulation des **P**ostes et **T**élécommunications). Ainsi que la réglementation des bandes de fréquences est plus que nécessaire, vu que des utilisateurs appartenant à des réseaux différents et travaillant dans les mêmes bandes de fréquences peuvent mutuellement se perturber. La configuration des canaux et le choix optimal de l'emplacement des points d'accès sont indispensables afin d'éviter les interférences au sein d'un même réseau ainsi que les baisses de débits. En plus des problèmes posés par les interférences, la sécurité demeure un aspect essentiel et plusieurs solutions de sécurité se sont succédé afin de mieux sécuriser les HOTSPOT WIFI.

2- Législation

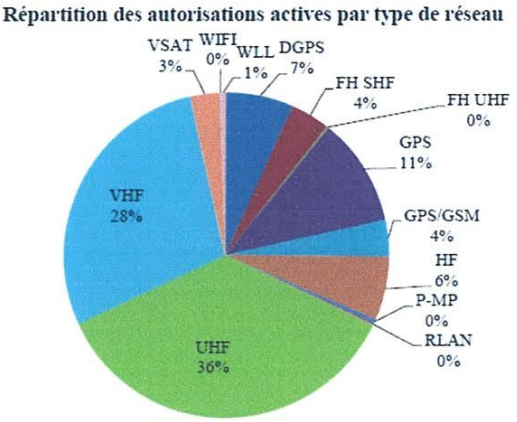
2-1- La législation sur la fourniture d'un accès Wi-Fi – Responsabilités

La fourniture d'un accès Internet sans fil dans un lieu public, nécessite que vous soyez possession des droits d'exploitations des fréquences sans-fil utilisées : 2,4Ghz pour le Wi-Fi. Cette autorisation d'exploitation des ondes Wi-Fi est délivrée sous forme de licence par L'ARPT (l'**A**gence de **R**égulation des **P**ostes et **T**élécommunications)

2-2- Etat des autorisations

La gestion des demandes d'autorisations d'exploitation de réseaux radioélectriques par l'ARPT se traduit au 31 décembre 2011 par 2369 autorisations pour l'exploitation de différents types de réseaux, dont 1349 actives, 14 archivées, 27 expirées et 979 résiliées.
Le détail des autorisations actives par type de réseau est donné comme suit :

- 382 VHF ; 52 FH SHF ; 3 FH UHF ; 85 HF ; 486 UHF ; 145 GPS ; 90 DGPS ; 50 GPS/GSM ; 40 VSAT ; 2 RLAN ; 6 P-MP (Point Multipoint) ; 7 WLL ; 1 Wi-Fi.



Source :ARPT

Figure 2.1 : Répartition des autorisations actives par type de réseau [7]

La figure 2.1 nous montre que le nombre d'utilisation des HOTSPOT Wi-Fi en Algérie quasiment nul; une seule autorisation a été fournie au cours de l'année 2011

2-3- Risques concrets d'usage de la connexion internet en accès Wi-Fi:

L'usage d'une connexion internet en accès Wi-Fi provoque des risques d'utilisation qui peuvent causer des problèmes avec les autorités judicieuse. Parmi ces risques il y a [8]:

- Téléchargements illégaux.
- Activité pédophile.
- Connexion à des sites d'échanges de fichiers.
- Usurpation d'identité sur des forums ou des messageries instantanées....
- Diffusion de propos diffamatoires, xénophobe sur internet.
- Usage de l'accès internet pour des actions de Spam, de piratage, de diffusion de virus.

2-4- Responsabilité du FAI (Fournisseur d'Accès Internet) :

Selon les lois de l'ARPT le Fournisseur d'Accès Internet (ex: Université) doit enregistrer les trafics pour des raisons de sécurité (pédophilie, terrorisme...). En effet, le fournisseur de l'ADSL (Algérie Télécom : DJAWEB, FAWRI, ANIS, ...etc.) se contente d'enregistrer le trafic effectué sur l'accès qu'il fournit (jusqu'à la prise téléphonique). Cela signifie que le trafic effectué sur l'accès Internet sans-fil que l'université fourni n'est pas identifié par ce dernier. Dans cette mesure, en cas de malversation sur l'accès à Internet, le Fournisseur d'Accès Internet « l'Université », ne pouvant pas identifier les différents utilisateurs qui font usage de la connexion Internet, portera directement la responsabilité sur son client, c'est-à-dire l'Université.

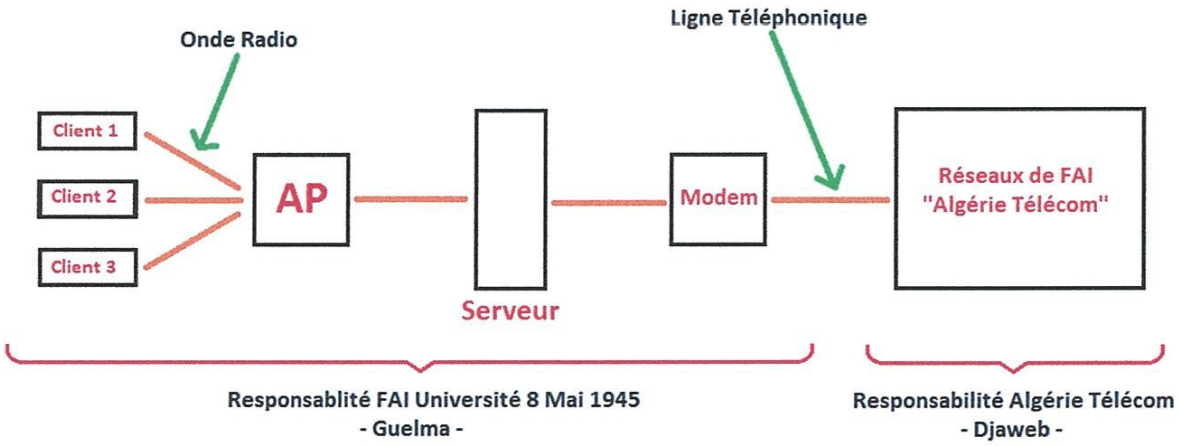


Figure 2.2 : Responsabilité des FAI

Voici donc les responsabilités de l'Université 8 Mai 1945- Guelma envers l'accès à Internet gratuit proposé à ces enseignants, employeurs et étudiants :

- L'Université doit identifier et authentifier tous les utilisateurs qui fréquentent et se connectent sur l'accès Internet.
- L'Université doit enregistrer tout le trafic effectué sur Internet par tous les utilisateurs se connectant à Internet et conserver ces données pendant une période fixé par la loi de l'ARPT (nécessite le déploiement et la configuration d'un serveur de logs).
- L'Université doit être capable de fournir ces informations sur simple commission rogatoire ou réquisition judiciaire.
- L'Université doit veillez à pouvoir interdire le téléchargement illégal.
- L'Université doit maintenir informé et appliquer toutes nouvelles obligations légales appliquées aux opérateurs.

L'Université doit donc mettre en place un système permettant d'authentifier les utilisateurs se connectant au point d'accès. Donc il faut mettre en place un portail captif permettant l'authentification des utilisateurs. Un portail captif est une méthode permettant de gérer

l'authentification d'utilisateurs sur un réseau. Il a pour rôle dans un premier temps de distribuer les adresses IP aux clients qui se connectent, puis dans un second temps de capturer toutes les requêtes à destination du web. Il force ainsi le client à passer par la page de demande d'authentification. Il n'est pas possible de passer outre, seul la page d'authentification du portail captif est autorisé sans être, au préalable, authentifié. Le portail captif permet donc seulement d'adresser les clients (DHCP) et d'afficher l'interface web permettant l'authentification (certains HOTSPOTS prennent en charge d'autres fonctionnalités comme le pare feu…). Il ne gère donc pas l'authentification en elle-même. Il est donc indispensable de mettre en place un serveur d'authentification par exemple de type Radius afin de gérer l'authentification. Il est aussi possible de mettre en place une base de données afin de gérer les utilisateurs.

2-5- Règle pour la mise en place :

La mise en place d'un HOTSPOT conforme à la législation Algérienne implique plusieurs étapes.

- Créer un accès (compte) individuel pour chaque utilisateur, établir le lien entre ce compte et la personne physique, par exemple en demandant une carte d'identité, ou carte d'étudiant et en relevant le numéro de cette dernière,
- Ensuite il est nécessaire d'enregistrer les heures d'accès de ce visiteur, ceci est fait directement par le portail captif,
- Finalement l'Université enregistre l'activité internet des utilisateurs, le contenu n'est ici pas archivé, uniquement les adresses IP visités.

2-6- Réduire les problèmes de responsabilité de l'université envers l'accès Internet.

Nous avons donc vu que l'université 8 mai 1945-Guelma sera dès la mise en place de l'accès à Internet responsable de celle-ci. Afin de réduire au maximum les abus, il sera préférable pour l'université de maximiser la sécurité en terme d'accès à Internet (empêcher l'accès à des sites interdits par la loi…). Comme vu précédemment l'université doit être en règle envers l'état Algérien.

2-7- Conservation des logs :

1- Par la loi n°09-04 du 05-08-2009 [9]:

- Consécration du principe de surveillance des communications électroniques (notamment les cas de surveillance préventive).
- Implication des fournisseurs de services dans le processus de prévention de la cybercriminalité.
  a- Obligations incombant à tous les fournisseurs de services (conservation des données relatives au trafic).
  b- Les obligations spécifiques aux fournisseurs d'accès Internet (mettre en place des dispositifs techniques permettant de limiter l'accessibilité aux distributeurs contenant des informations contraires à l'ordre public ou aux bonnes mœurs et en informer les abonnés).

Les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

- les informations permettant d'identifier l'utilisateur,
- les données relatives aux équipements terminaux de communication utilisés,
- les caractéristiques techniques, ainsi que la date, l'horaire et la durée de chaque communication,
- les données relatives aux services complémentaires demandés ou utilisés et leur fournisseur,
- les données permettant d'identifier le ou les destinataires de la communication.

3- LA REGLEMENTATION

La WiFi utilise les deux bandes de fréquences, U-NII (Unlicensed National Information Infrastructure) et ISM (Industrial, Scientific and Medecinal) tout comme les réseaux HiperLAN 1, HiperLAN 2, Bluetooth, ZigBee, HomeRF, ainsi que certaines applications telles que les fours micro-ondes, les périphériques sans fil (d'ordinateurs, PDA, …etc.).

L'utilisation de ces bandes de fréquences est régie par les lois des organismes chargés de la réglementation pour éviter toute perturbation entre utilisateurs. Cette réglementation fait apparaître trois zones géographiques caractérisées chacune par un organisme de normalisation spécifique qui fixe ses recommandations. Le respect des différents standards est assuré par les différentes autorités de régulation nationales [5].

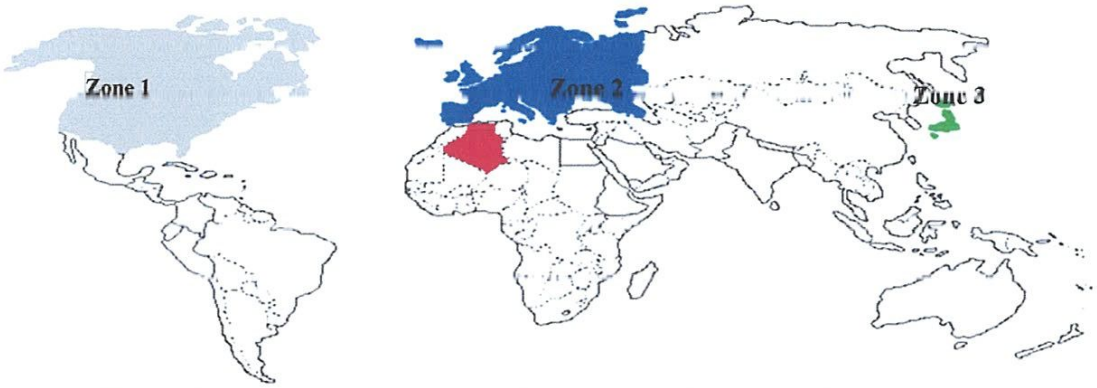


Figure 2.3 : Zones régissant la réglementation des bandes de fréquence

Zone	Organisme de normalisation
Amérique de nord	FCC (Federal Communications Commission)
Europe	CEPT (Conférence Européenne des Postes et Télécommunications)
Japon	RCR (Research and Development Center for Radio Communications)

Tableau 2.1 Organismes de normalisation

3-1- Utilisation des canaux

La norme 802.11g utilise la modulation OFDM avec un débit de 54 Mbits/s. Elle travaille dans la bande ISM (2,4-2.4835 MHz) qui est divisée en 14 canaux de 20 MHz et espacés de 5 MHz.

Canal	Fréquence(Ghz)	Zone 1	Zone 2	Zone 3
1	2.412	Permise	Permise	Permise
2	2.417	Permise	Permise	Permise
3	2.422	Permise	Permise	Permise
4	2.427	Permise	Permise	Permise
5	2.432	Permise	Permise	Permise
6	2.437	Permise	Permise	Permise
7	2.442	Permise	Permise	Permise
8	2.447	Permise	Permise	Permise
9	2.452	Permise	Permise	Permise
10	2.457	Permise	Permise	Permise
11	2.462	Permise	Permise	Permise
12	2.467	Interdite	Permise	Permise
13	2.472	Interdite	Permise	Permise
14	2.484	Interdite	Interdite	Permise

Tableau 2.2 : Utilisation des canaux dans les différentes zones [5]

Actuellement, les normes retenues par l'**A**gence **N**ationale des **F**réquences (**ANF**) sont celles utilisées en Europe (Zone 2).

3-2- La Puissance d'émission

Selon la bande de fréquence et selon que l'on soit en indoor (Intérieur) ou outdoor (extérieur), la puissance d'émission est limitée. Par exemple, les limites en Algérie sont données par le tableau ci-dessous :

Conformément aux décisions n° 11/01 et 11/02 du 22 mars 2011, les conditions d'utilisation des réseaux locaux radioélectriques -RLAN- dans les bandes de fréquences des 2,4 GHz et 5 GHz sont les suivantes [10] *:*

	Puissance maximale utilisable	
Bande de fréquence	**Indoor**	**Outdoor**
2,4 – 2,4835	< 10mW	<28mW
5,150 – 5,250	<200mW	200mW
5,250 – 5,350	<200mW	1000mW
5,470 – 5,670	<200mW	1000mW

Tableau 2. 3 : Règles générales d'utilisation des bande ISM & U-NII

3-3- Wi-Fi Alliance

La Wi-Fi Alliance est une association professionnelle mondiale à but non lucratif regroupant des centaines de grandes sociétés dédiées à une connectivité transparente. La Wi-Fi Alliance se consacre au développement technologique et commercial, ainsi qu'aux programmes de réglementation, pour favoriser une vaste adoption du Wi-Fi dans le monde entier.

Le programme Wi-Fi CERTIFIED a été lancé en mars 2000. Label d'interopérabilité et de qualité largement reconnu, il garantit que les produits Wi-Fi offrent la meilleure expérience utilisateur possible. La Wi-Fi Alliance a homologué plus de 14 000 produits à ce jour et encourage l'utilisation des produits et des services Wi-Fi sur les marchés tant établis que nouveaux.

Wi-Fi, Wi-Fi Alliance, WMM, Wi-Fi Protected Access (WPA), ainsi que les logos Wi-Fi CERTIFIED, Wi-Fi, Wi-Fi ZONE et Wi-Fi Protected Setup sont des marques déposées de la Wi-Fi Alliance. Wi-Fi CERTIFIED, Wi-Fi Direct, Wi-Fi Protected Setup, Wi-Fi Multimedia, WPA2, Passpoint, Miracast et le logo Wi-Fi Alliance sont des marques de la Wi-Fi Alliance [11].

Site : www.wi-fi.org
Chaîne YouTube Wi-Fi Alliance :
www.youtube.com/wifialliance
Contact :
Sandrine Cormary
Edelman pour Wi-Fi Alliance
sandrine.cormary@edelman.com
+33 (0)1 56 69 73 86

3-4- Le label Wi-Fi

La spécification Wi-Fi est établie par la WECA (Wireless Ethernet Compatibility Alliance), dont la mission est d'assurer l'interopérabilité des produits IEEE 802.11 et de promouvoir cette technologie. La WECA offre pour cela un service de test d'interopérabilité aux constructeurs, si l'équipement passe ce test avec succès, il obtient alors la certification Wi-Fi et peut utiliser le label Wi-Fi suivant [11]:

Figure 2.4 : Label Wi-Fi

4- Etude de Marché des HOTSPOT

Pour tenter de dégager les usages qui pourraient se développer sur les HOTSPOTS Wi-Fi et voir quelle part de la population est susceptible d'être touchée, il est intéressant de faire le point sur les taux d'équipement des entreprises et des ménages en ordinateurs portables et assistants (PDA), les principaux terminaux d'accès au Wi-Fi. Prévoir le nombre de HOTSPOTS qui pourraient voir le jour dans le monde est très empirique alors que le marché commence à peine à émerger. Les estimations des cabinets d'études sont d'ailleurs très diverses.

4-1- Les HOTSPOT dans le monde

En termes d'usage, les HotSpot Wi-Fi représentent une grande révolution dans le monde : des nombreux opérateurs Internet proposent des accès Internet via des Hospot dans le monde mais ce n'est pas le cas de l'Algérie. Voici une carte mondiale nous montre la répartition des Hotspot dans le monde.

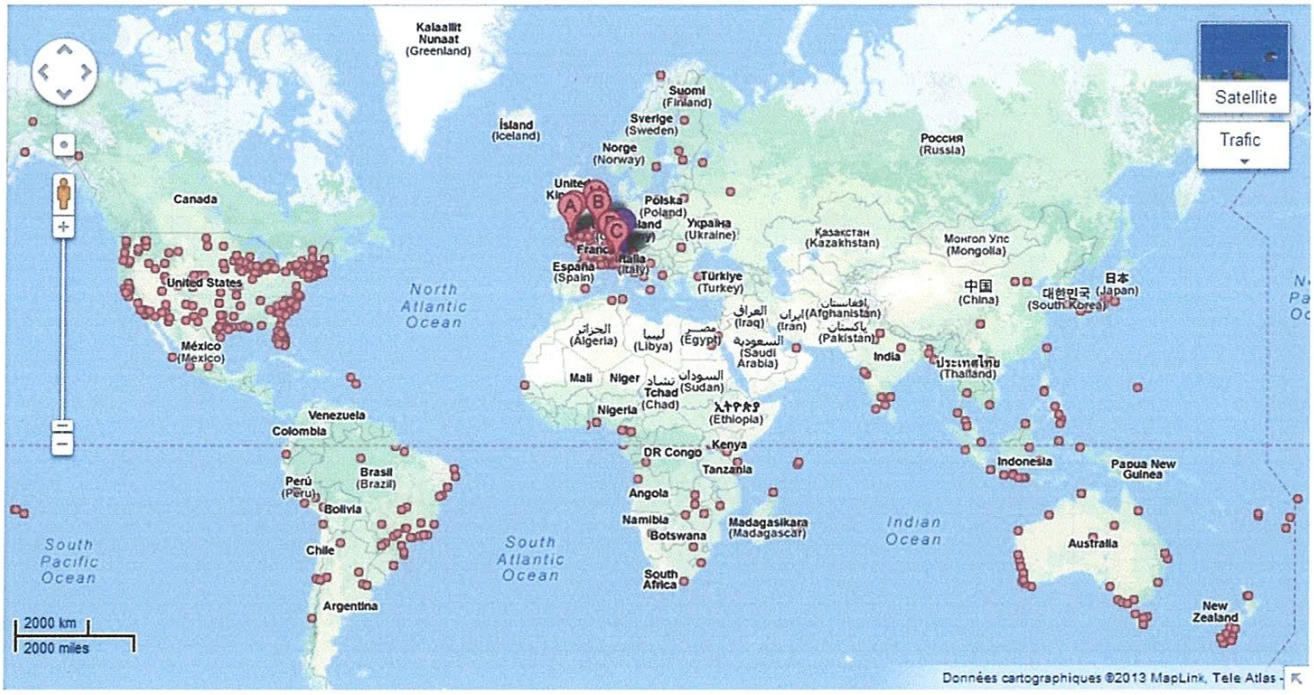


Figure 2.5 : les HOTSPOT Wi-Fi dans le Monde [12]

Jour après jour, la vitesse d'évolution des nombres des équipements certifiés Wi-Fi augmente. Ce qui nécessite le déploiement des réseaux de communication entre ces équipements.

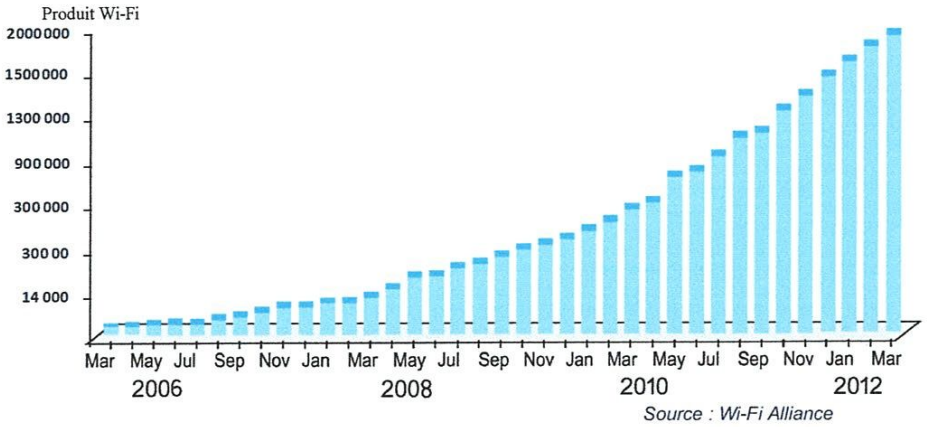


Figure 2.6 : Evolution du nombre de produits certifiés Wi-Fi

4-2- Les Revenue Annuelle

Analisys[R] estime que 40 millions d'Européens utiliseront des HOTSPOTS Wi-Fi en 2010 (générant un marché de 6 milliards d'Euros '600 milliards DZD'). Donc on peut dire que c'est un marché qui pourrait remplacer le marché du pétrole avec succès [13].

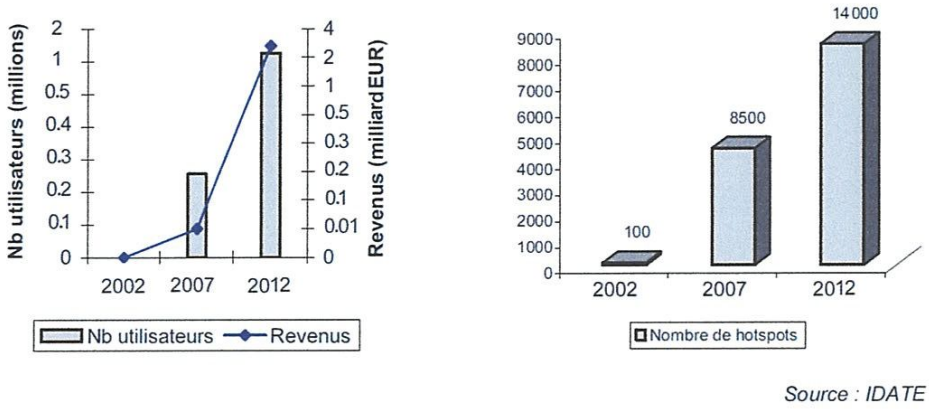


Figure 2.7 : Evolution des Revenue et Nbre des utilisateurs Wi-Fi & Développement de Nbre des HOTSPOTS WIFI en France

4-3- Les prévisions des HOTSPOTS Wi-Fi

Les prévisions concernant les HOTSPOTS sont particulièrement variable. Le Gartner Group prévoit 2 Millions HOTSPOTS dans le monde d'ici à 2017. Avec un marché de 100 Milliard d'euro '100 000 Milliard DZD'. Par contre selon les prévisions de la société new-yorkaise ABI Research, il devrait y avoir plus de 4 Millions HOTSPOTS dans le monde pour la même période. Cela présente une grande croissance du nombre de points d'accès par rapport à 2010 [14].

Les trois quarts des sites (74%) sont situés en Amérique du Nord et en Europe, mais la région Asie-Pacifique rattrape son retard. *D'ici 2017, l'Asie-Pacifique les dépassera en nombre de HOTSPOT Wi-Fi,* anticipe ABI Research [14].

Actuellement, l'Europe reste le marché dominant avec plus de 100.000 sites en services. L'hôtellerie est le premier secteur industriel à déployer ce type de réseaux sans fil, avec quelque 60.000 points d'accès dans le monde. Ils devraient être 218.000 d'ici 2017, notamment grâce à l'utilisation des réseaux Wi-Fi pour proposer des services de téléphonie à bas prix grâce à la VoIP.

La société Jiwire référence quant à elle actuellement 129.228 hotspots dans le monde, au sein de son annuaire Wi-Fi consultable sur ZDNet.fr [14].

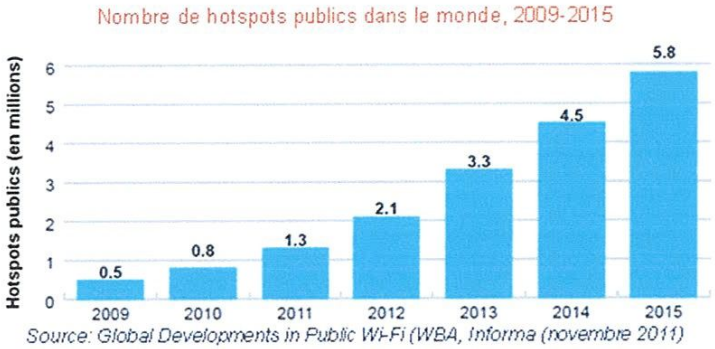


Figure 2.8 : prévisions des HOTSPOTS Wi-Fi

5- Conclusion

Le marché des HOTSPOTS Wi-Fi n'est pas une mode, mais un véritable marché émergeant. Wi-Fi est soutenu par une croissance accélérée du nombre de HOTSPOTS déployés. Par ailleurs un nombre croissant d'acteurs investissent aujourd'hui dans les HOTSPOTS Wi-Fi ; parmi eux figurent des start-up mais également des opérateurs fixes ou mobiles et des ISP qui possèdent la dimension financière pour assurer un déploiement de HOTSPOT Wi-Fi à grande échelle.

Partie B

[Principe de fonctionnement du HotSpot]

1- Introduction

La dénomination exacte d'un HotSpot est Wireless Internet HotSpot. Il s'agit d'un lieu où la connexion vers un réseau Internet est possible via une connexion sans fil et grâce à un ensemble de technologies et de protocoles mis en œuvre. On parle également de borne ou de point d'accès Wi-Fi. Les HotSpots se sont rapidement développés à l'échelle mondiale permettant ainsi à des utilisateurs nomades disposant d'équipements adaptés (ordinateurs ou téléphones portables compatibles, PDA et autres) de se connecter à Internet de partout avec beaucoup de simplicité. Si ces connexions Internet sont ouvertes au grand public, cela ne veut pas dire qu'il n'existe aucune protection à l'accès et pour les utilisateurs. Nous savons bien qu'une fois connectés sur un même réseau, les utilisateurs deviennent potentiellement vulnérables. La première des protections qui a été mise en place au sein des HotSpot est le portail captif avec une authentification par fichier local ou bien un serveur à distance.

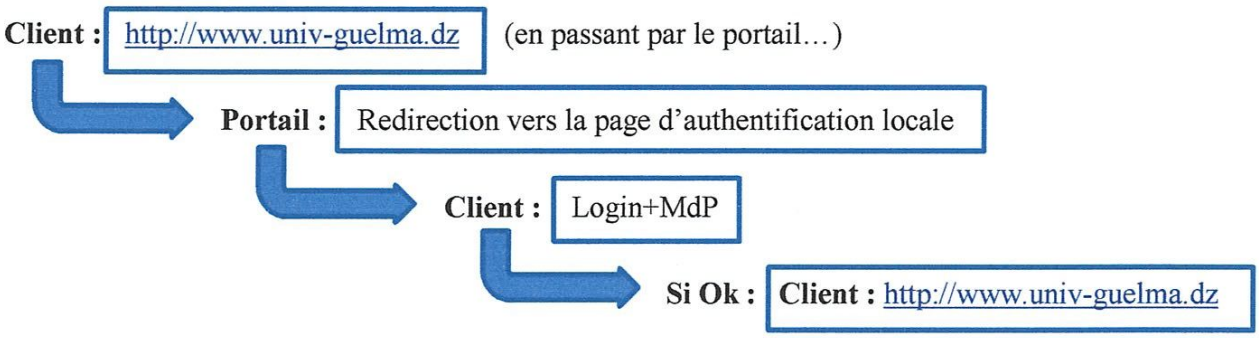
2- Portail Captif :

Le portail captif est un logiciel qui s'installe sur un HotSpot et qui permet de gérer l'authentification des utilisateurs qui souhaitent se connecter à Internet. Il faut noter que tous les HotSpot ne fonctionnent pas sur le principe d'un portail captif, mais pour des raisons de sécurité de plus en plus de HotSpots souhaitent aujourd'hui disposer d'un portail captif.

Le portail captif a réussi à s'imposer comme la solution pour les réseaux sans fil publics qu'ils soient gratuits ou payants. Mais il faut noter que le portail captif peut également fonctionner sur des réseaux filières. Il n'y pas d'exception entre réseau sans fil ou réseau filière, le but est de forcer l'utilisateur à s'identifier avant d'accéder au réseau Internet. L'identification se fait généralement via une page Internet et pour les HotSpots payants elle peut nécessiter le paiement par carte bancaire.

Un portail captif est une structure permettant un accès rapide à Internet. Lorsqu'un utilisateur cherche à accéder à une page Web pour la première fois, le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page Web stockée localement sur le portail captif grâce à un serveur HTTP. Ceci permet à tout ordinateur équipé d'un navigateur HTML et d'un accès Wi-Fi de se voir proposer un accès à Internet. La connexion au serveur est sécurisée par SSL grâce au protocole HTTPS, ce qui garantit l'inviolabilité de la transaction. Les identifiants de connexion (identifiant, mot de passe) de chaque utilisateur sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant. Une fois l'utilisateur authentifié, les règles du Firewall le concernant sont modifiées et celui-ci se voit alors autorisé à utiliser son accès pour une durée limitée fixée par l'administrateur. A la fin de la durée définie, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session [17].

2-1- Fonction type d'un portail captif :



Remarque : Il faut que cette redirection fonctionne avec tous les protocoles applicatifs.

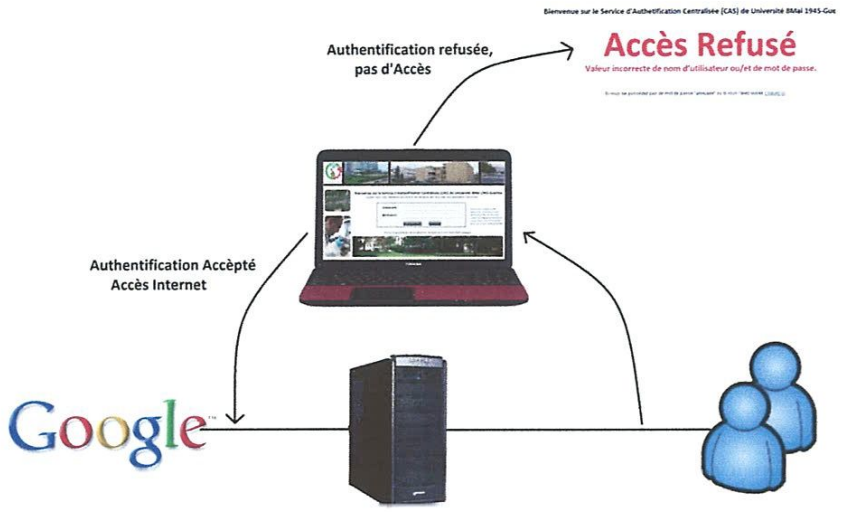


Figure 2.9 : Schéma théorique d'un portail Captif

Interprétation : Quoi que désire faire le client, s'il veut surfer sur le WEB il devra d'abord passer par le portail captif afin de s'authentifier.

La différence entre un simple Firewall et un portail réside dans le fait que le portail captif ne refuse pas une connexion. Il la redirige vers une page d'authentification.

2-2- Etude comparatif entre des différentes solutions :

Installer un portail captif nécessite de faire le choix entre plusieurs solutions possibles. Pour cela on a passé beaucoup du temps dans les recherches sur internet, il s'est avéré qu'il n'existe pas de portail captif reconnu sous Windows, seul FIRSTSPOT a été trouvé mais celui-ci est peu répandu dans le monde du HotSpot (pas de réel suivi des failles de sécurité…). La solution retenue sera donc une solution sous *nix.

2-2-1- Le routage sous Unix

Tout d'abord, qu'est-ce que le routage? C'est la manière dont nous dirigeons l'information sur un réseau depuis sa source vers sa destination. Une information, pour être transmise doit passer par des relais :

C'est eux qui sont chargés du routage. Dans le cadre du portail captif, notre tâche est de router les informations entre Internet et les machines du réseau Wi-Fi.

Cependant, afin de comprendre le fonctionnement du portail captif, il est nécessaire d'également comprendre globalement le fonctionnement d'Unix, que nous présenterons brièvement avant d'en venir plus précisément au routage sous cet OS [15].

2-2-2- Système d'exploitation BSD

FreeBSD est un système d'exploitation UNIX libre. Le nom vient de l'association d'une part de free qui signifie à la fois « libre » et « gratuit » dans l'anglais courant, et d'autre part de Berkeley software distribution (BSD), l'UNIX développé à l'université de Berkeley. Free prend un sens plus connoté dans ce nom : il signifie que le logiciel peut être utilisé gratuitement même pour un usage commercial, que les sources complètes sont disponibles et utilisables avec un minimum de restrictions quant à leur usage, leur distribution et leur incorporation dans un autre projet (commercial ou non), et enfin que n'importe qui est libre de soumettre son code source pour enlever un bug ou améliorer le logiciel, ce code étant incorporé aux sources après accord.

L'objectif du projet FreeBSD est de fournir un système qui peut servir à tout, avec le moins de restrictions possibles.

Historiquement, les développeurs se sont focalisés pendant un temps sur la plate-forme i386 au sens large (x86) et les performances, c'est-à-dire les temps de réponses du système

pour n'importe quelle sollicitation. En 2010, FreeBSD est utilisable et soutenu par la communauté sur un grand nombre de plates-formes : Alpha, AMD64, ARM, i386 (architecture i386 ou x86, incluant les Pentium), ia64 (la famille de processeurs Intel Itanium et Itanium 2), x86-64, MIPS, PC98 (architecture NEC PC-98x1), PowerPC, SPARC (architecture UltraSPARC de Sun Microsystem) et Xbox.

FreeBSD offre des possibilités avancées en termes de réseau, de performance, de sécurité et de compatibilité. Il y a notamment une compatibilité binaire Linux et Windows NT (XP inclus). La première permet l'exécution de programmes compilés Linux, la seconde permet l'utilisation des pilotes Windows NT des cartes réseau sans fil Wi-Fi. Le logiciel est un standard industriel sur le marché des serveurs. De nombreux fournisseurs d'accès, hébergeurs et organismes utilisent FreeBSD, parmi lesquels Walnut Creek CDROM, Yahoo! Inc. Ou Netcraft. Le 24 mai 1999, l'équipe du serveur miroir *ftp.cdrom.com* a annoncé avoir battu leur record de transfert de données pour un serveur : 1,33 tébioctets en 24 heures [18].

2-2-3- Pénétration des marchés :

FreeBSD est considéré comme un standard industriel dans le marché des serveurs. Il n'y a pas de données maintenues sur les utilisateurs du système d'exploitation, mais des organismes d'observation comme Netcraft (qui a tous ses serveurs sous FreeBSD) permettent d'effectuer des évaluations qualitatives. De grandes parties d'internet (Netblock owners) sont sous FreeBSD :

- Yahoo!, qui comprend HotJobs.com Ltd, Altavista ou Geocities ;
- Rackspace.com ;
- Isle, Inc ;
- Bayerischer Rundfunk ;
- Japan Network Information Center ;
- ViaNet Communications ;
- Hopemoon Co, Ltd ;
- Full Internet Provider.

D'anciens utilisateurs (ou actuels mais non confirmés) de FreeBSD sur serveurs sont :

- Microsoft (hotmail)13,14.

L'utilisation de FreeBSD pour un usage domestique, sans être confidentielle, est bien plus modérée auprès du grand public que le système GNU/Linux.

Pourtant, FreeBSD fait fonctionner les logiciels qui ont largement aidé à populariser les systèmes GNU/Linux, parmi lesquels le serveur graphique X associé à l'espace bureautique et de fenêtrage KDE, la suite bureautique OpenOffice.org, le navigateur web Firefox.

D'autres facteurs entrent en jeu. Sans prétention d'exhaustivité, de hiérarchie quant à l'impact, il y a vraisemblablement :

La médiatisation, à laquelle ont participé de grandes entreprises comme IBM, Microsoft, Novell ou RedHat, des organismes d'état et les différents médias qui relayent les sujets sélectionnés ;

Une synergie entre des mouvements : logiciel-libre, un contre-courant par rapport à Microsoft et aux solutions propriétaires ;

La licence : parfois jugée trop libre, elle permet à des entreprises comme Apple ou Microsoft d'intégrer du code FreeBSD à leur système d'exploitation.

Sans être décisif, un logo ou un slogan est un porte-parole qui par la répétition et la force de l'image aident à marquer les esprits [19].

2-2-4- Comparaison entre GNU/Linux et FreeBSD :

FreeBSD et GNU/Linux sont deux systèmes de type Unix. Alors que FreeBSD tend à être entièrement conçu par une seule équipe, chaque composant de GNU/Linux est développé par une équipe différente. De cette manière la cohésion de ces composants est assurée d'office dans le cas de FreeBSD tandis que sous GNU/Linux elle se révèle très complexe, c'est pourquoi il existe

des distributions GNU/Linux, qui sont des systèmes préassemblés dans le but d'être plus rapidement fonctionnel pour l'utilisateur.

Entre les deux systèmes, la nomenclature des périphériques diffère, de même que quelques commandes, ou encore l'arborescence du système de fichiers. C'est typiquement le même genre de différences que l'on peut trouver entre deux distributions GNU/Linux très différentes.

L'ensemble des distributions GNU/Linux étant très hétérogène, il est extrêmement difficile de le comparer à une seule entité. Cependant tout comme quelques distributions GNU/Linux, FreeBSD entend fournir un système simple, rapide, stable, sûr, à destination des utilisateurs qui ont déjà une bonne connaissance des systèmes informatiques (par exemple si lors de l'installation l'utilisateur a choisi d'installer un environnement graphique, il ne sera pas configuré automatiquement ni lancé au démarrage par défaut). À ce titre, FreeBSD se rapproche de Gentoo par exemple.

FreeBSD est très loin de l'installation en quelques clic d'Ubuntu, qui est parfaitement fonctionnelle fraichement installée et déjà équipée de tous les logiciels de base pour une utilisation domestique. C'est ce que propose PC-BSD, un système FreeBSD préinstallé pour une utilisation bureautique, à l'image d'une distribution GNU/Linux [20].

2-2-5- Pourquoi choisir Unix (BSD) pour la mise en place du portail captif?

Unix présente de nombreux avantages pour la mise en place d'un portail captif qui nous conduisent à utiliser cet Operating System (Système d'Exploitation) :

- Les systèmes *nix sont réputés pour leur stabilité, ce qui les rend particulièrement adaptés au rôle de routeurs et serveurs qui doivent tourner 24h/24 sans être victimes de défaillances logicielles (aussi appelées *bugs*).
- Il intègre nativement une solution configurable de routage native (ie : intégrée, sans besoin d'installer un logiciel supplémentaire) des paquets réseaux, fonction nécessaire à la mise en place du portail captif.
- Il met à disposition les outils nécessaires tel que serveur HTTP et base de donnée.
- Sa haute configurabilité nous permet de concevoir le système le plus efficient.
- Son fonctionnement ouvert permet une meilleure compréhension des mécanismes qui vont être étudiés, mais aussi un meilleur contrôle.
- Sa gratuité limite les coûts de mise en place aux seuls frais de matériel.

De plus, les solutions *nix sont parmi les mieux supportées au monde étant donné le nombre de personnes impliquées dans le projet. Un tel système possède une réactivité supérieure quand aux résolutions de bugs et de mises à jour de sécurité, et nous avons accès à une documentation très importante sur Internet et généralement de qualité comparables aux ouvrages sortis sur le sujet.

La technique du portail captif est plus ou moins la même quel que soit la solution utilisée, le but est de mettre en jeu plusieurs équipements et protocoles permettant à l'utilisateur de se connecter au serveur [15].

2-2-6- Théoriquement comment ça se présente la connexion d'un client sur un HotSpot ?

L'utilisateur commence par se connecter à un réseau (en filière ou en Wi-fi), cette connexion se fait sans problème grâce à des protocoles spécifiques. Une fois connecté, l'utilisateur est dirigé automatiquement vers un serveur DHCP qui lui attribue une adresse IP. L'adresse IP est une sorte d'identité pour l'utilisateur nécessaire également pour envoyer des informations (protocole TCP/IP). Mais l'utilisateur n'a pas toujours accès à Internet pour le moment mais il est connecté au réseau. Il va donc lancer une page Internet. Cette page va envoyer une requête de type Web grâce au protocole HTTP vers le serveur, cette requête passe obligatoirement par la passerelle qui elle va renvoyer à l'utilisateur une page web d'authentification.

Si l'utilisateur dispose des paramètres nécessaires (Login/password) pour se connecter au réseau. Il va donc les saisir et transmettre ces informations sur le serveur. Il est important de noter

que la page envoyée à l'utilisateur est cryptée grâce au protocole SSL qui permet de protéger les données qui sont transmises par l'utilisateur pour son authentification.

Il va ensuite se produire un ensemble d'opérations au sein de différents serveurs. Dans un premier temps les données cryptées sont envoyées dans le serveur de base de données qui vérifie que cet utilisateur existe bel et bien. Si le serveur de base de données constate que l'utilisateur existe, selon le portail captif en œuvre, il envoie les informations vers le serveur d'authentification. Il s'agit du serveur radius. Les portails captifs cités dans ce dossier sont tous compatibles Radius.

Toutefois, après vérification sur le serveur d'authentification, des informations liées à l'adresse IP et l'adresse physique (adresse MAC) de l'utilisateur sont envoyées vers la passerelle afin d'ouvrir l'accès à l'utilisateur qui pourra par la suite se connecter au réseau Internet.
Ces opérations se font en quelques secondes, elles sont quasiment invisible pour l'utilisateur qui restera ainsi connecté un bon moment mais des requêtes Ping lui seront régulièrement envoyées afin de vérifier qu'il est toujours connecté. Si le serveur constate un moment d'absence, l'utilisateur sera déconnecté et devra par la suite relancer la procédure d'authentification [16].

La figure 2.10 montre les différentes étapes pour pouvoir se connecter

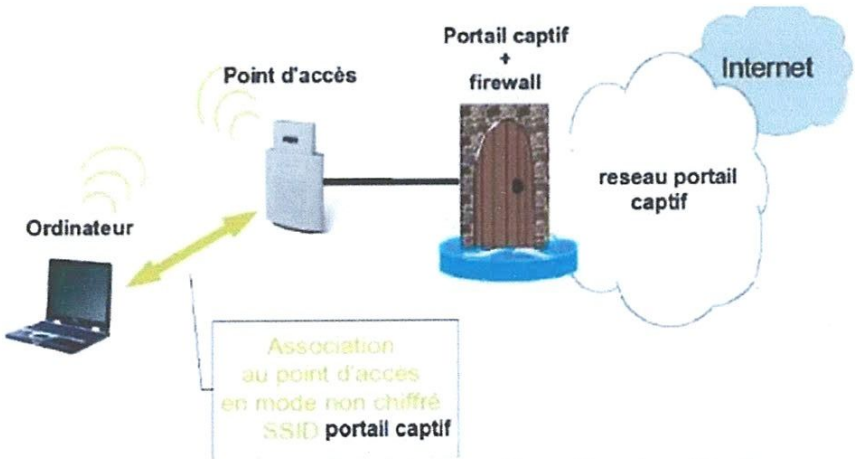


Figure 2.10 : Connexion théorique d'un client à un HotSpot

On a vu un bref détail sur ce système d'exploitation et nous savons qu'il existe sous ce système d'exploitation de nombreux logiciels dont voici les caractéristiques principales. Nous allons détailler les caractéristiques de 6 solutions Open Source. Ils sont installés sur des équipements qui permettent de les faire fonctionner.

Voici une liste non exhaustive des portails captifs open source :

- NoCat
- Talweg
- Wifigod
- Chillispot
- PfSense
- Public IP

a. NoCat [21]

NoCatSplash est un démon public de la passerelle de réseau ouvert. Il se comporte comme un [captive / open / actif] portail. Le démon de la passerelle modifie les règles de pare-feu sur la passerelle pour passer le trafic pour ce client (basé sur l'adresse IP et Adresse MAC).

NoCatSplash est le successeur de NoCatAuth, qui a été écrit en Perl. NoCatSplash est écrit en multithread C ANSI afin d'être plus petit et mieux travailler sur des appareils de type embarqués. Voici quelque spécification :

- Compatible Radius, LDAP, MySQL
- Ecrit en Perl
- Communique avec la passerelle pour informer si l'utilisateur peut passer. Peut régler le débit et spécifier des règles de pare-feu pour un utilisateur.
- Sécurisation du transfert entre le système authentification et la passerelle par clé pgp. La doc conseille de séparer le serveur d'authentification (droits limités) de la passerelle (droit root pour pouvoir modifier les règles iptables).
- Fenêtre de saisie du mot de passe en https.
- Simplicité au niveau utilisateur, performance

Sécurise le partage d'une connexion sans fil redirige les utilisateurs vers une page web: authentification via HTTPS

Se compose de :

- **NoCatSplash** : Portail Captif
- **NoCatAuth**: Application d'Authentification
- **Splash server** : génère des formulaires (Splash pages) Dépendances:

- Linux, FreeBSD, netBSD ou Mac OSX
- L'activation des modules liés à netfilter dans le noyau
- Libghttp pour le remote splash
- Perl et gmake

b. Talweg [22]

Crée par l'université Paul Verlaine de Metz, conçu pour les réseaux sans fil s'exécutant sous Linux, garantie de l'identité des personnes utilisant le réseau.

Dépendances :

- Linux
- Un serveur web Apache + mode perl + mode ssl + mode mono
- Un serveur de DNS
- Un serveur de DHCP
- Iptables

Talweg est une solution de portail captif basé sur le Framework .Net/Mono. Ce proxy/gateway utilise le protocole HTTPS pour les liaisons entre le client et le server.

Voici quelque spécification :

- Compatible Radius
- Récupère les demandes d'accès aux pages web et les retourne dans une connexion https
- Limite l'accès aux ports 80 et 443 de part son fonctionnement

c. Wifidog [23]

Wifidog est une solution complète et portable de portail captif.

Elle permet d'ouvrir un hotspot librement en limitant les abus liés à une ouverture libre et sans restrictions d'une connexion à Internet (téléchargements illégaux, spams...).

Le projet Wifidog a été lancé par Île sans fil et est en cours de développement. Il est utilisé en France à Clermont-Ferrand par l'association Bougnat sans fil

D'autres solutions existent [...] mais sont peu portables (NoCat nécessite perl, GnuPG , OpenSSL) ou sont seulement conçues pour n'afficher que des mises en garde sans aucun contrôle d'accès (juste un splash screen).

Wifidog permet d'avoir un système centralisé de contrôle des accès, un système derépartition de la bande passante et même de diffuser du contenu spécifique à un hotspot donné. Il fonctionne avec n'importe quel navigateur (pas de Javascript, marche aussi avec les PDA). Il est développé en C et spécialement pour le fameux WRT54G, mais il fonctionne aussi ailleurs (sur n'importe quel Linux récent)...

Voici quelque spécification :

- Compatible Radius
- Nécessite Apache, php, Psql, Pear, smtp pour envoie des identifiants
- Faible consommation en ressource réseau
- Contrôle iptable pour définir les règles de passage du firewall
- Adapté à une communauté et à une gestion d'un parc conséquent de PDA avec un monitoring poussé.
- Vérifie l'activité grâce à un ping. Evite d'avoir un pop-up comme dans noCat.
- Fonctionne sur des plateformes embarquées ou autres.

d. ChilliSpot [24]

ChilliSpot est un portail captif open source ou un contrôleur de point d'accès LAN sans fil. Il est utilisé pour authentifier les utilisateurs d'un réseau local sans fil. Il prend en charge connexion basée sur le Web, ce qui est aujourd'hui la norme pour les HotSpots publics, WISP authentification "client intelligent", et il prend en charge Wi-Fi Protected Access (WPA et WPA2). Authentification, d'autorisation et de comptabilité (AAA protocole) est gérée via RADIUS (à bord ou à distance).
Développement sur le projet initial se poursuit, mais lentement pour certains. Le Coova-Chilli est un projet actif et a depuis ajouté de nombreuses nouvelles fonctionnalités et est une partie intégrante du firmware CoovaAP.

À la mi-2008, ChilliSpot semble être très mort. Le développeur Jens Jacobsen a disparu, et le domaine de chillispot.org a expiré.

Voici quelque spécification :

- Compatible Radius
- Nécessite Apache, Mysql, php
- Perte au niveau de la bp et consommation de ressources système
- Authentification WPA possible

e. PfSense [25]

PfSense est le descendant de m0n0wall. C'est donc un système d'exploitation pare-feu basé sur le noyau FreeBSD et sur le module de filtrage "ipfw". La configuration de PfSense est stockée dans un seul fichier XML à l'instar de m0n0wall. La séquence de démarrage est aussi fondée sur des fichiers php.

Néanmoins, PfSense n'est pas vraiment orienté à l'embarqué. Ceci explique la panoplie de fonctionnalités offertes par cette distribution. Par rapport à m0n0wall (son ancêtre), PfSense offre en plus les possibilités suivantes :

- Common Address Redundency Protocol (CARP) et PfSync (synchronisation entre machines PfSense)
- Possibilités d'alias étendue (alias pour interfaces réseau, utilisateurs…).
- Configuration XML de synchronisation entre maître et hôte de backup permettant de faire un point unique d'administration pour un cluster pare-feu. La synchronisation est assurée via XML-RPC.
- Equilibrage de charge (load balancing) pour les trafics entrant et sortant.
- Graphes montrant les statuts des files d'attentes.

- Support du protocole SSH pour l'accès distant.
- Support de multiples interfaces réseaux WAN.
- Serveur PPPoE.
- …

f. Public IP

Public IP consiste a obtenu une adresse IPv4 d'après le FAI et faire partager une connexion. Tout est centralisée chez l'opérateur afin de pouvoir la gestion des utilisateurs… etc.

Le tableau 3.1 présente une comparaison entre les différentes solutions citées précédemment :

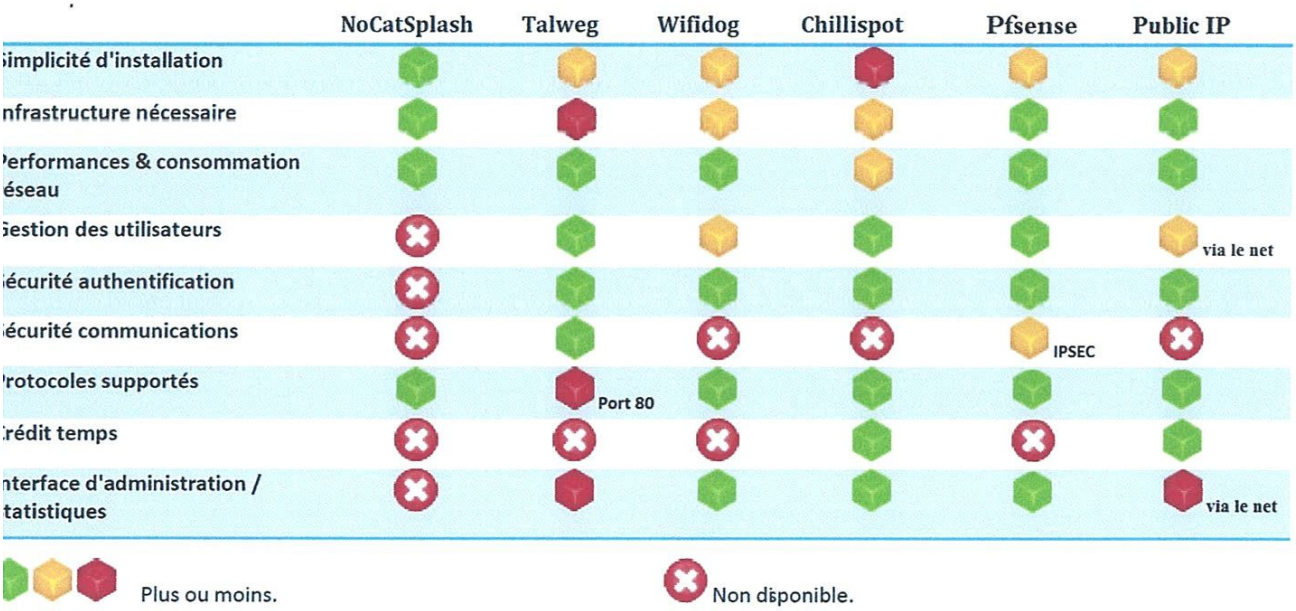


Tableau 2.4 : Comparaison entre les différentes solutions libres [26]

Le tableau 2.5 montre les avantages et les inconvénients de chaque solution :

	Avantages	Inconvénients
NoCatSplasH	-S'intègre bien comme solution rapide	Les utilisateurs s'enregistrent eux-mêmes
Talweg	Simple, efficace	Seul le port 80 passe
Wifidog	Supporte tous les protocoles, sécurité des authentifications	Difficile à mettre en place, trafic non sécurisé
Chillispot	Spécialement conçu pour le WiFi	Trafic non sécurisé
Public IP	Accepte tout type de LAN (WiFi/filaire)	Administration en ligne, trafic non sécurisé
Monowall / Pfsense	Administration autonome en local, multi fonctionnalités, toujours en évolution	Pour l'instant PfSense est en version Bêta, même si déjà très stable !

Tableau 2.5 : Avantages et Inconvénients des différentes solutions libres

2-2-7- Orientation du choix :

Au vu de ce comparatif, et d'après notre besoin, la solution d'un firewall et portail de type PfSense ou (**P**acket **F**ilter **S**ense) semble être la plus performante et évolutive puisqu'il permet de réponde aux critères de sécurité et d'authentification dont nous avons besoin (sécurité de l'authentification et de la communication). Ainsi que cette solution répond le mieux aux critères de :

- Disponibilité (Base FreeBSD, load balancing, etc…)
- Confidentialité (HTTPS Web GUI, HTTPS authentification, IPSEC, PPTP, etc...)
- Auditabilité (Statistique très nombreuses avec Ntop, etc…)
- Mise à jour (système Upgradable sans réinstallation, packages téléchargeables directement depuis le Web GUI, etc…).
- Simplicité d'administration, d'installation.
- Autonomie complète.

Cette solution est proposée en Live CD d'environ 50Mo. Il est basé sur un système d'exploitation BSD (gratuit et open source).

Figure 2.11 : Logo PfSense

3- Serveur d'Authentification :

Afin de réaliser notre HotSpot Dép ELN & TLC, il a été choisi de réaliser une authentification par serveur. En effet ce type d'authentification est le plus sécurisé et permet une gestion plus simple des accès. L'authentification par serveur se fait par différents protocoles dont voici les principaux :

- Kerberos
- CAS
- Radius

3-1- Kerberos [27]

Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Créé au Massachusetts Institute of Technology, il porte le nom grec de Cerbère, gardien des Enfers (Κέρβερος). Kerberos a d'abord été mis en œuvre sur des systèmes Unix.

Dans un réseau simple utilisant Kerberos, on distingue plusieurs entités :

- Le client ©, a sa propre clé secrète $\mathbf{K_C}$
- Le serveur (S), dispose aussi d'une clé secrète $\mathbf{K_S}$
- Le service d'émission de tickets (TGS pour Ticket-Granting Service), a une clé secrète $\mathbf{K_{TGS}}$ et connaît la clé secrète $\mathbf{K_S}$ du serveur
- Le centre de distribution de clés (KDC pour Key Distribution Center), connaît les clés secrètes $\mathbf{K_C}$ et $\mathbf{K_{TGS}}$

Le client C veut accéder à un service proposé par le serveur S.

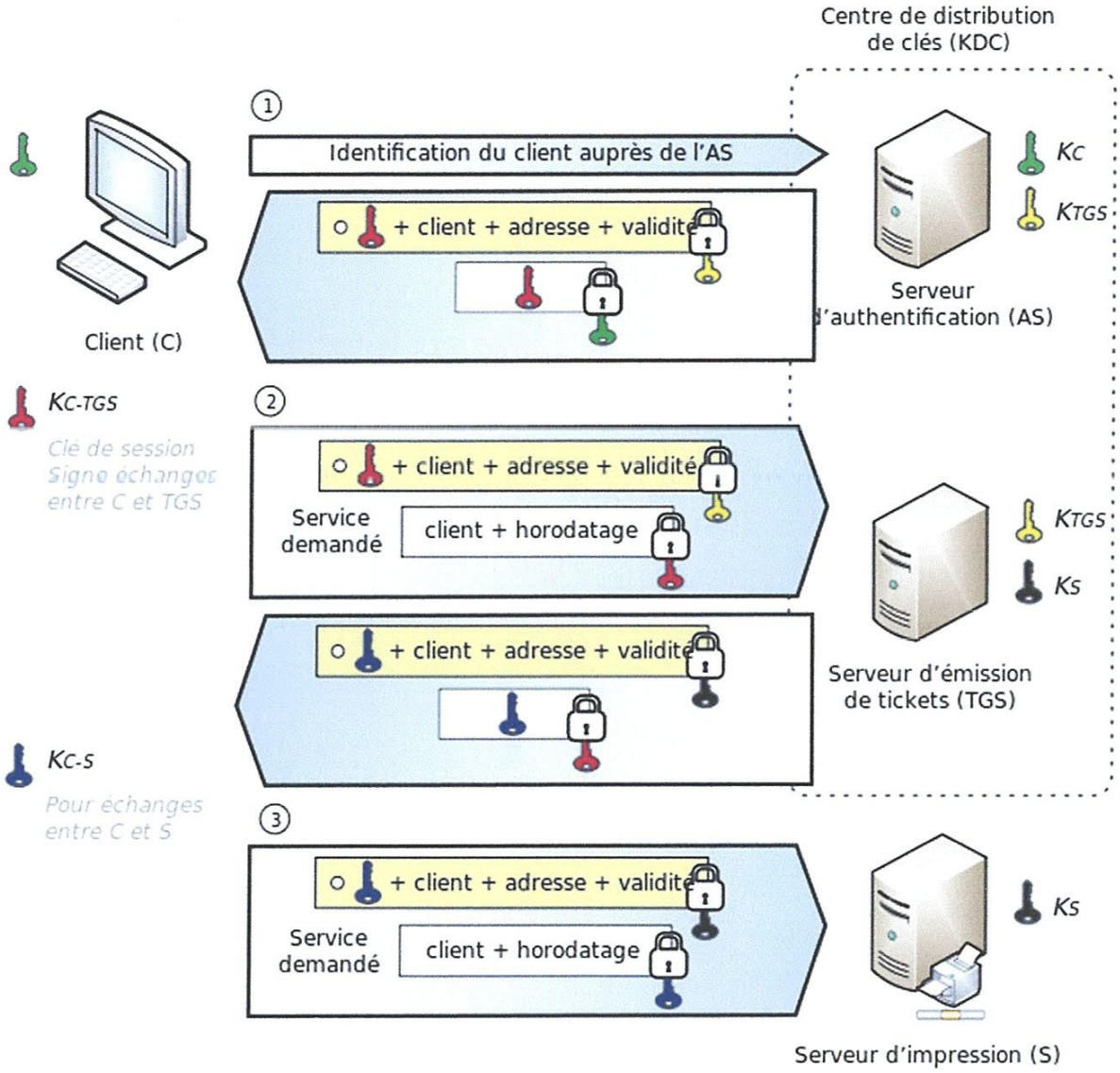


Figure 2.12 : Fonctionnement du protocole Karberos

La première étape pour le client consiste à s'identifier auprès du serveur de clés (KDC). Le client a une clé secrète K_C, celle-ci est également connue par le serveur de clés. Le client envoie son nom au serveur de clés et lui indique le TGS qui l'intéresse. Après vérification sur l'identité du client (cette partie dépend des implémentations, certains serveurs utilisent des mots de passe à usage unique), le serveur de clés lui envoie alors un ticket T_{TGS}. Ce ticket autorise le client à faire des requêtes auprès du TGS.

Ce ticket T_{TGS} est chiffré par le serveur de clés avec la clé du TGS (K_{TGS}). Il contient notamment des informations sur le client mais également la clé utilisée pour établir la communication entre le client et le TGS. Cette clé de session, nous la noterons $K_{C,TGS}$. Le client reçoit également cette clé de session $K_{C,TGS}$, elle a toutefois été chiffrée avec la clé secrète K_C du client.

À ce stade, le client possède un ticket T_{TGS} (qu'il ne peut pas déchiffrer) et une clé $K_{C,TGS}$.
La deuxième étape est l'envoi par le client d'une demande de ticket auprès du TGS. Cette requête contient un identifiant (des informations sur le client ainsi que la date d'émission) chiffré avec la clé de session $K_{C,TGS}$ (qui est trouvée par le client en déchiffrant les informations reçues depuis le

serveur de clés avec sa clé secrète). Le client envoie aussi le ticket qui lui avait été transmis par le serveur de clés.

Le TGS reçoit alors son ticket et il peut le déchiffrer avec sa clé secrète K_{TGS}. Il récupère le contenu du ticket (la clé de session) et peut ainsi déchiffrer l'identifiant que lui a envoyé le client et vérifier l'authenticité des requêtes. Le TGS peut alors émettre un ticket d'accès au serveur. Ce ticket est chiffré grâce à la clé secrète du serveur K_S. Le TGS envoie aussi ce ticket chiffré avec la clé secrète du serveur K_S et la clé de session $K_{C,S}$ chiffrée à l'aide de la clé $K_{C,TGS}$ au client pour les communications entre le serveur final et le client.

La troisième étape est le dialogue entre le client et le serveur. Le client reçoit le ticket pour accéder au serveur ainsi que l'information chiffrée contenant la clé de session entre lui et le serveur. Il déchiffre cette dernière grâce à la clé $K_{C,TGS}$. Il génère un nouvel identifiant qu'il chiffre avec $K_{C,S}$ et qu'il envoie au serveur accompagné du ticket.

Le serveur vérifie que le ticket est valide (il le déchiffre avec sa clé secrète K_S) et autorise l'accès au service si tout est correct.

3-2- CAS (Central Authentification Service) [28]

Le Central Authentication Service (CAS) est un système d'authentification unique (SSO) pour le web développé par l'Université Yale, partenaire majeur dans le développement de uPortal. Ce logiciel est implanté dans plusieurs universités et organismes dans le monde.

3-2-1- Intérêt

CAS est un système d'authentification unique : on s'authentifie sur un site Web, et on est alors authentifié sur tous les sites Web qui utilisent le même serveur CAS. Il évite de s'authentifier à chaque fois qu'on accède à une application en mettant en place un système de ticket.

3-2-2- Principe de fonctionnement

CAS est essentiellement un protocole basé sur des requêtes HTTP pures. Certains messages sont cependant formatés en XML.

Ce protocole est basé sur une notion d'échange de tickets, un peu à la manière de Kerberos. Ces tickets sont des « opaque handles » : ils ne transportent aucune information.
Il y a 2 tickets nécessaires au fonctionnement de base, plus 2 autres tickets dans le cas d'utilisation de proxy CAS :

- **Ticket-Granting Cookie (TGC)**
  C'est un cookie de session qui est transmis par le serveur CAS au navigateur du client lors de la phase de login. Ce cookie ne peut être lu / écrit que par le serveur CAS, sur canal sécurisé (HTTPS).
  Si le navigateur web n'accepte pas les cookies, l'utilisateur devra se ré-authentifier à chaque appel au serveur CAS.

- **Service Ticket (ST)**
  Ce ticket va servir à authentifier une personne pour une application web donnée. Il est envoyé par le serveur CAS après que l'utilisateur se soit authentifié, et est transporté dans l'URL.
  Ce ticket ne peut être utilisé qu'une seule fois. Il y a ensuite dialogue direct entre l'application web et le CAS via un GET HTTP, avec le ST en paramètre. En réponse, le serveur CAS retourne l'identifiant de la personne, et donc l'authentifie. Il invalide également le ticket (libération des ressources associées).
  En fait, ce ticket concerne une personne, pour un service, et utilisable une seule fois.

- **Proxy-Granting-Ticket (PGT)**
  Il est envoyé par le serveur CAS à une application web proxy CAS disposant d'un ST valide. Ce ticket confère au proxy CAS la possibilité de demander au serveur CAS de générer un Proxy Ticket (PT) pour une application tierce et une personne donnée.
- **Proxy-Ticket (PT)**
  Il est généré par le serveur CAS à la demande d'un proxy CAS. Il permet d'authentifier l'utilisateur pour un service distant, avec lequel le client web n'a pas d'accès direct. Le service distant l'utilisera comme le ST.Il est possible d'utiliser des proxies CAS en cascade.
  Dans le fonctionnement de CAS, le service ayant besoin de l'authentification est en relation directe avec le serveur CAS lors de la validation du ticket. Ceci rend possible l'utilisation de ce mécanisme pour transporter des informations complémentaires (autorisations, attributs, ...).
  Le paquet fourni propose le nécessaire pour mettre en œuvre le protocole CAS ; à charge de l'implémenteur de développer le module d'authentification interne. Un module d'authentification LDAP a été récupéré pour les essais ; il est à améliorer.
  Le portage de CAS vers uPortal se fait facilement (les bibliothèques sont fournies). Dans ce cas, uPortal devient proxy CAS ; il obtient donc un PGT du serveur CAS. Il est donc possible à un canal qui utiliserait un service tiers sachant authentifier CAS de demander un PT pour ce service; des essais fructueux ont été faits dans ce sens.

3-3- RADIUS (Remote Authentification Dial-In User Service) [29]

RADIUS est un acronyme pour (Remote Authentication Dial-In User Service)
Gérer des lignes séries et des accès modems pour un grand nombre d'utilisateurs peut amener une nécessité forte pour une administration de qualité. Puisque les accès modem sont par définition un lien vers le monde extérieur, ils exigent une attention particulière à la sécurité, à l'autorisation et à la comptabilité.

Ceci peut mieux être realisé en contrôlant une (base de données) simple des utilisateurs, qui tient compte de l'authentification (vérifiant le nom et le mot de passe d'utilisateur) aussi bien que l'information de configuration détaillant le type de service à délivrer à l'utilisateur (par exemple, Slip, PPP, telnet, rlogin...).

Radius permet le respect des trois A : ''Authentification, Authorization and Accounting'' (AAA) ou Authentification, Autorisation et Comptabilisation.

- Authentification : Processus permettant de garantir que la personne qui tente d'accéder à Internet dispose d'un compte valide. Le mot de passe de l'utilisateur est comparé avec les entrées figurant dans une base de données centrale.
- Autorisation : Permet à l'exploitant du réseau de définir les services réseau dont les utilisateurs finaux peuvent bénéficier. Par exemple, une entreprise peut autoriser ses employés à utiliser les possibilités Internet à distance à partir de leur domicile, mais n'autoriser qu'un accès financé par l'entreprise au réseau de cette dernière.
- Comptabilisation : Permettent à l'exploitant du réseau d'effectuer un suivi détaillé de l'utilisation qui est faite a partir de ce réseau.

Le protocole Radius a été développé à l'origine par Livingston Entreprise pour leur série de serveur d'accès réseau (Network Access Server) PortMaster (Serveurs de modems). Radius est aujourd'hui une norme de l'IETF (Internet Engineering Task Force) qui est suivie par les principaux fournisseurs d'équipements réseau comme Cisco ou Lucent.

3-3-1- Fonctionnement de RADIUS

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
- Le NAS achemine la demande au serveur RADIUS ;

- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur : soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
  - **ACCEPT :** l'identification a réussi ;
  - **REJECT :** l'identification a échoué ;
  - **CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » ;

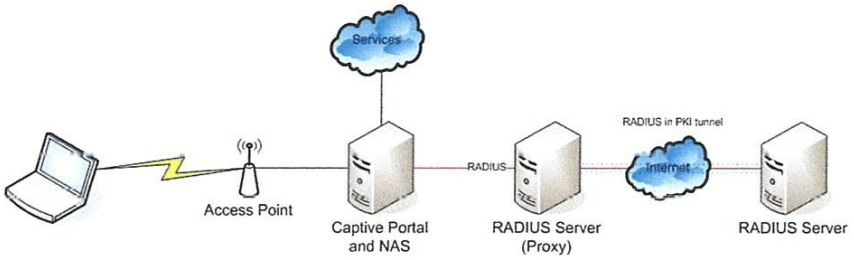


Figure 2.13 : Schéma Général Authentification par Radius

3-4- Comparaison entre les différentes solutions étudiées :

	Avantages	Inconvénients
Kerberos	-Kerberos propose un système d'authentification mutuelle permettant au client et au serveur de s'identifier réciproquement. -L'authentification proposée par le serveur Kerberos a une durée limitée dans le temps, ce qui permet d'éviter à un pirate de continuer d'avoir accès aux ressources : on parle ainsi d'anti re-jeu. -Kerberos partage avec chaque client du réseau une clé secrète faisant office de preuve d'identité.	Le système d'authentification Kerberos est victime de trois vulnérabilités importantes. La première permet à un utilisateur non authentifié de se connecter à distance sous n'importe quel compte. Les deux autres autorisent un utilisateur déjà authentifié à exécuter du code, notamment sur le serveur de clé.
Radius	-De multiples possibilités d'authentification. -Traitement individuel d'un utilisateur ou d'une machine (on peut mixer les méthodes d'authentification) -Gestion centralisée. Trace de toutes les connexions ou tentatives dans un log.	RADIUS est strictement client-serveur, d'où des discussions et bagarres de protocoles propriétaires quand un serveur doit légitimement tuer une session pirate sur un client.
Cas	-S'adapte à presque n'importe quelle solution d'authentification de campus. -Propose deux modes de fonctionnement de base (avec et sans proxy) -Fonctionne par « tickets » et ces tickets ne transportent aucune information.	Il ne permet pas dans sa version actuelle de récupérer des informations de droits d'accès ou des attributs liés à la personne.

Tableau 2.6 : Avantages et Inconvénients des différents protocoles d'authentifications

3-5- Orientation du choix :

Au vu de ce comparatif, et d'après notre besoin, la solution la mieux adaptée à notre projet a donc été « RADIUS », c'est le protocole qui est le plus approprié. Radius répond à tous les critères de choix précisés auparavant.

Méthodes d'authentification	OpenRadius	GNU-Radius	ICRadius	Freeradius	IAS
EAP	✗	✗	✗	✓	✓
EAP/TLS	✗	✗	✗	✓	✓
EAP/TTLS	✗	✗	✗	✓	✓
EAP/MD5	✗	✗	✗	✓	✗
CHAP	✗	✓	✗	✓	✓
PEAP	✗	✗	✗	✓	✓
Couple login/mot de passe	✓	✓	✓	✓	✓
PEAP MSCHAPv2	✗	✗	✗	✗	✓

Tableau 2.7 : Comparaison de différentes méthodes d'authentification

On s'aperçoit que seul IAS sous Windows possède l'implémentation de PEAP MSCHAPv2. De plus le changement de type d'authentification est plus facile sous Server 2003. Le serveur d'authentification choisi sera donc RADIUS sous Windows Server 2003 avec une authentification PEAP MSCHAPv2 (La partie serveur est nativement présente). MSCHAPv2 est sensible aux attaques de dictionnaire. Mais avec le protocole PEAP ce n'est pas un problème car les informations circulent dans un canal sécurisé.

PEAPv0 comporte une autre faiblesse. Il transmet le logon en dehors du tunnel TLS. L'utilisation d'un sniffer peut permettre de récupérer un nom d'utilisateur valide. Grâce à cette information un individu mal intentionné peut provoquer un DOS en verrouillant les utilisateurs valides. Ce problème est résolu dans PEAPv2. La gestion des utilisateurs se fera avec Active Directory. Ceci permettra de gérer les droits d'accès sur le réseau…

Figure 2.14 : Logo RADIUS

4- Exemples de HotSpot existant en Algérie

De nombreux opérateurs Internet proposent des accès Internet via des HotSpot dans le monde mais ce n'est pas le cas de l'Algérie. Ces accès sont quasiment tous gérés par des portails captifs, Prenons un exemple de portail captif que nous avons eu l'occasion d'utiliser :

4-1- Le HotSpot 01WiFi Aéroport Houari Boumediene(Alger):

C'est l'un des HotSpot de la société Française 01WiFi qui est installé au niveau de l'Aéroport international Houari Boumediene (Alger). Il est gérer et administrer par la même société. Pour se connecter, il faut dans un premier temps se connecter physiquement au réseau, on est ensuite dirigé vers une page d'authentification. Pour un premier accès, il faut renseigner l'un des distributeurs automatique qu'ils ont placé dans des plusieurs coins du hall de l'aéroport cette entreprise a été utilisée des distributeurs automatique pour faciliter les vente des tickets. On reçoit automatiquement un ticket qui contient des paramètres de connexions avec lesquels on peut s'authentifier afin de pouvoir accéder au réseau public Internet pour une durée bien déterminé.

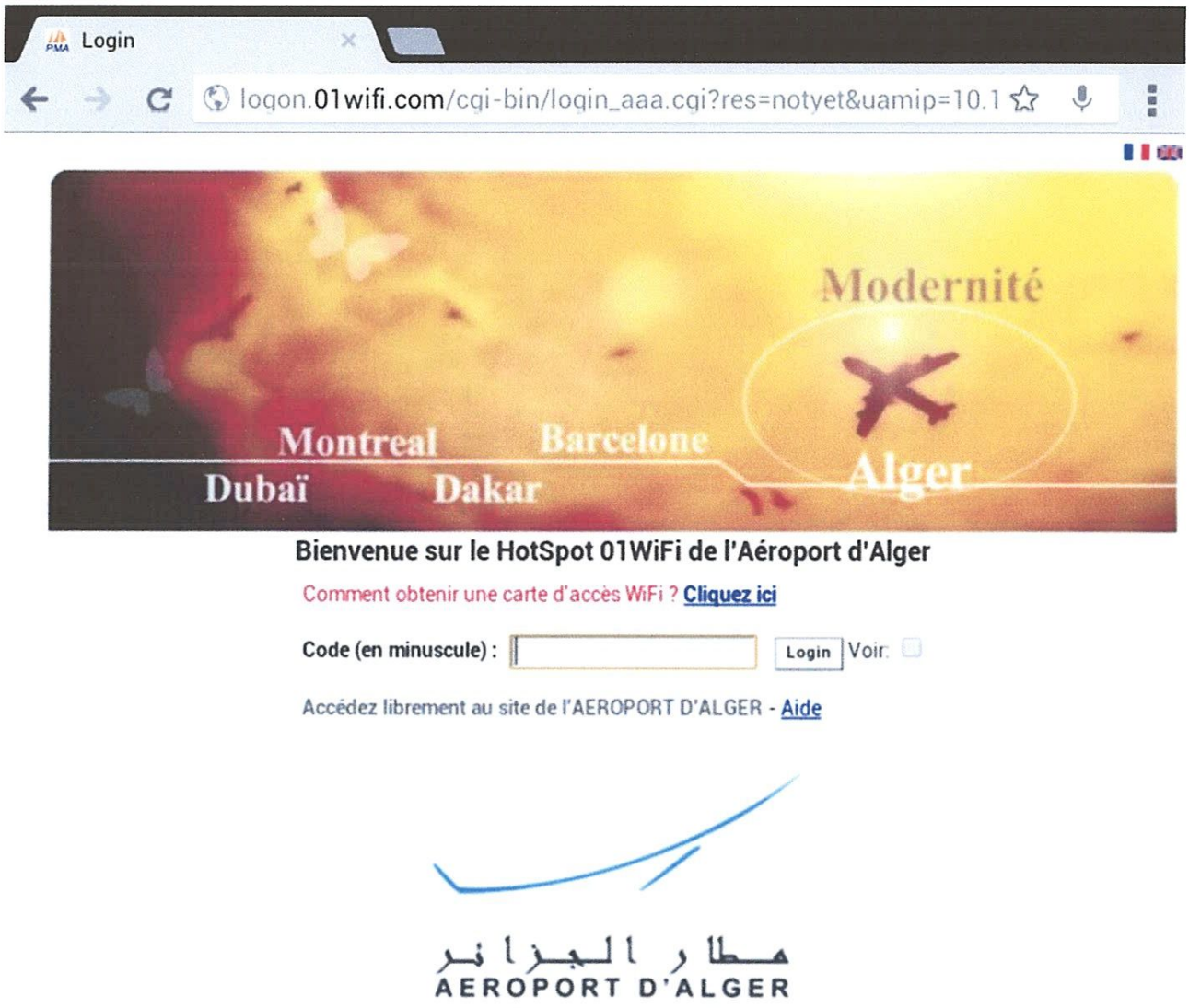


Figure 2.15 : Page d'accueil HotSpot 01Wifi Aéroport Houari Boumediene

Par la suite une page elle nous montre comment obtenir un ticket pour se connecter à internet :

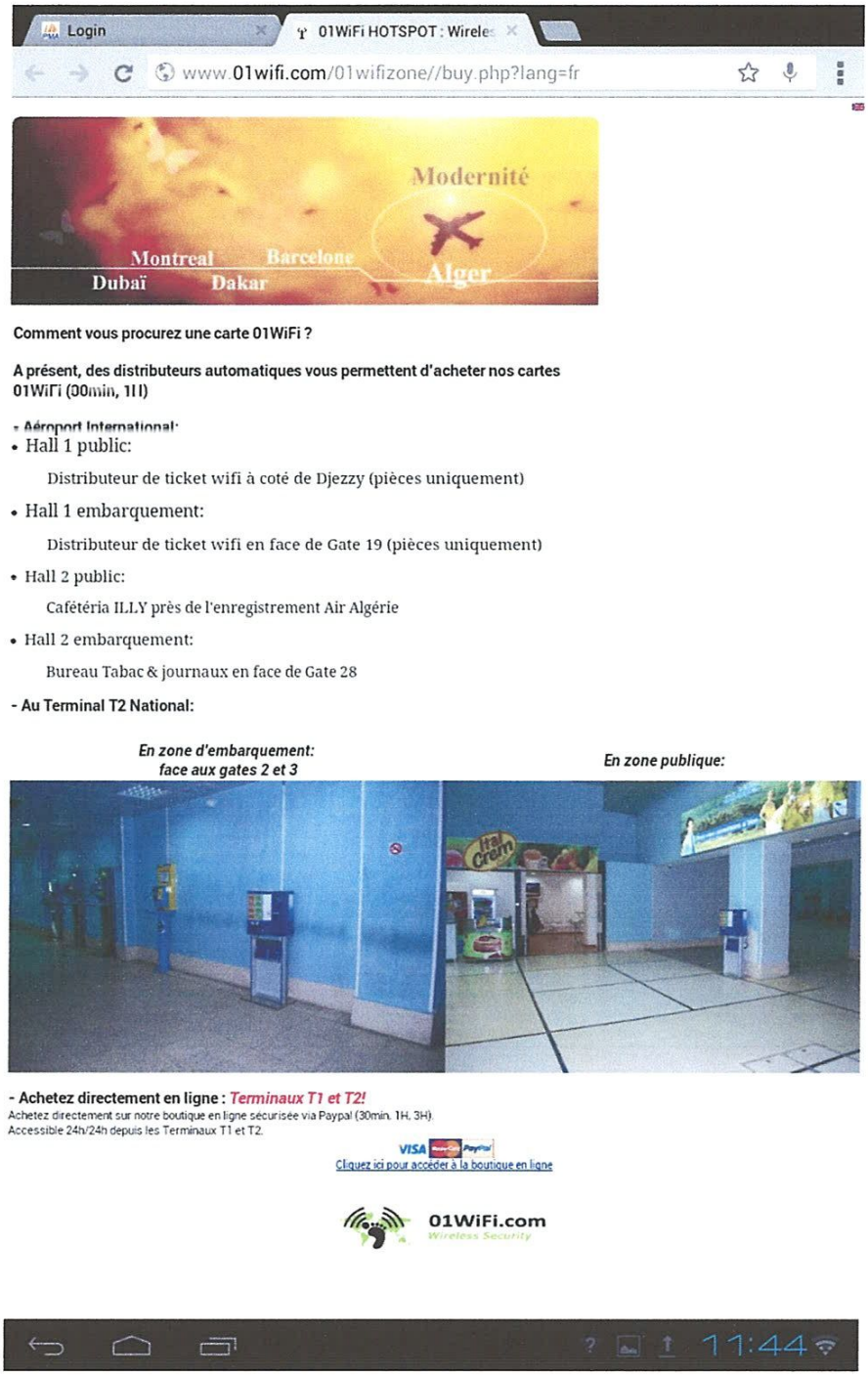


Figure 2.16 : Distributeur automatique des Tickets

5- Conclusion

Après avoir détaillé le principe de fonctionnement des HotSpot Wi-Fi où nous avons présenté sa structure globale qu'est composé d'un Portail Captif, et un serveur d'Authentification ces deux serveurs ont pour rôles d'assurer la propre fonctionnalité de notre HotSpot.

On a donné le fonctionnement général de notre HotSpot maintenant il nous reste de faire une étude de planification et optimisation pour faire fonctionner ce HotSpot dans les meilleures conditions. Et c'est le cas du chapitre suivant.

CHAPITRE III

Planification et Optimisation

u HotSpot Dép ELN & TLC]

1- Introduction

Le design d'un système de communication sans fil doit aboutir à un positionnement optimal des antennes d'Emission/Réception, dont l'objectif de planification est de pouvoir satisfaire une Qualité de Service (QoS) avec un nombre minimal de ces antennes. Ce qui nécessite de calculer la zone de couverture de chacune d'entre elles et conclure sur la QoS assurée dans tout l'environnement considéré.

Avant de commencer la description des résultats des mesures obtenues pour ce travail, nous pensons nécessaire de décrire les paramètres, les contraintes ainsi que les modèles de l'outil de planification pris pour mener à bien les expériences de ce travail.

2- Paramètres et contraintes de planification :

Les paramètres et les contraintes de planification que nous jugeons nécessaires pour aborder notre processus de planification sont décrits dans les tableaux suivants [2]:

Paramètre de planification	
Radio	• Puissances maximales (des points d'accès et des stations mobiles), • Bande de fréquences déployées, • Gain des antennes, • Type de récepteur (avec/sans diversité) : ceci pourra influer sur le seuil de couverture et les valeurs des puissances d'émission, • Estimation des valeurs de C/I selon la technologie utilisée (DSSS, FHSS, etc.), • Type de modulation utilisée, sachant que plus une modulation est compliquée, plus est le débit offert mais, la surface couverte sera réduite et elle sera de plus en plus susceptible à l'interférence.
Utilisateurs et Service	• Estimation du nombre d'abonnés voulant établir une connexion (estimation de la densité des abonnées.), • Distribution des mobiles, • Données statistiques sur le trafic spécifique à chaque application, • Débit propre à chaque pièce de l'environnement indoor suivant l'application, • Données statistiques sur la mobilité des abonnées (déplacement entre couloirs, halles et bureaux),
Base de données Géographiques	• Aménagement de l'intérieur et données statistiques sur les affaiblissements des obstacles,

Tableau 3.1 paramètres de planification

Contraintes	
Taux d'erreur	• Ne dépassant pas 10^{-6}
Répartition des débits	• Garantie du débit demandé par chaque pièce
Taux de couverture	• Supérieur ou égale à 90%

Tableau 3.2 Contraintes de planification

3- APERÇU DU RESEAU EXISTANT

Le Département d'Electronique et Télécommunications est un bâtiment qui comprend deux étages avec un rez de chaussée, tous les laboratoires et les bureaux enseignants du côté gauche (rez de chaussée, 1er et 2eme étage) sont câblées en filaire à partir de baie de brassage (Switch1) qui est placée au rez de chaussée dans le bureau N° 0.2 et Tout les laboratoires et les bureaux administratifs, enseignants du côté droite (rez de chaussée, 1er et 2eme étage) sont câblées en filaire à partir de baie de brassage (Switch2) qui est placée au 1er étage dans le bureau N°1.2. Ils ont interconnectés via deux (02) liaisons câblées au répartiteur général dans l'immeuble de la faculté des sciences et technologies.

Les salles de cours ne sont pas encore reliée au réseau de l'établissement ce qui empêche les étudiants, de se connecter à Internet.

Pour les laboratoires et les bureaux actuellement connectées au réseau local, aucune politique de contrôle d'accès n'a été mise en place. Le partage des données et des ressources matérielles s'effectuent via le groupe de travail de la faculté. Un serveur Windows 2003 Server est installé et qui joue le rôle d'une passerelle. L'adressage des postes est manuel.

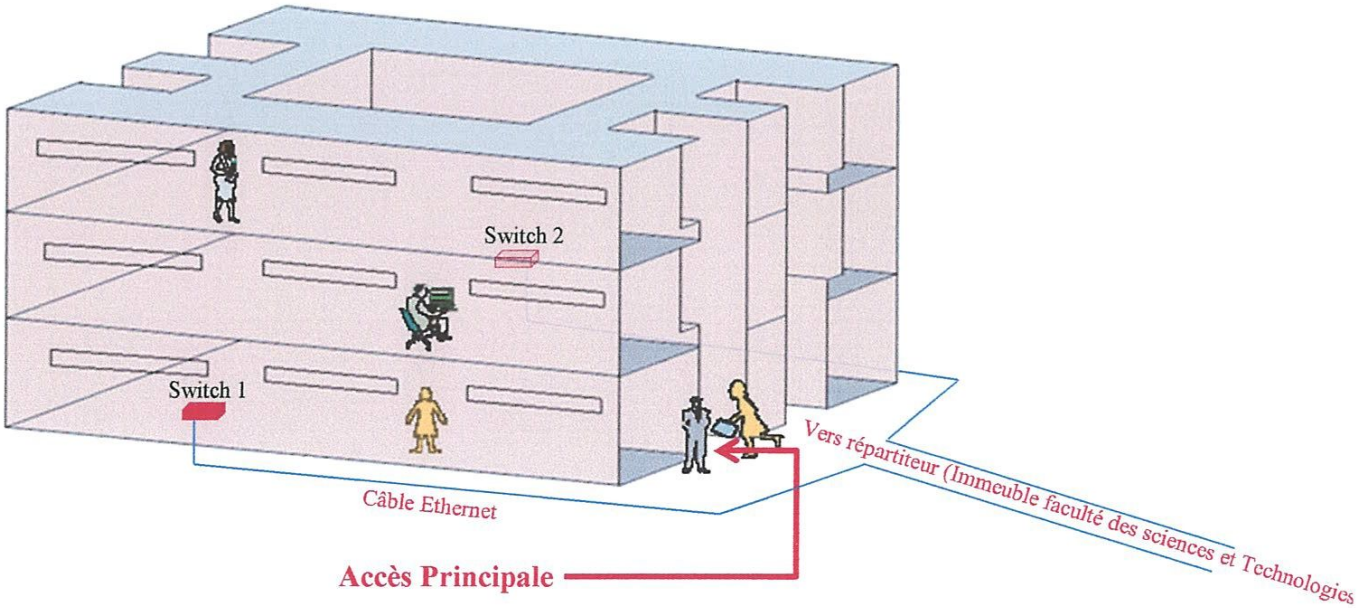


Figure 3.1 : Plan 3D du Département d'Electronique et Télécommunications (infrastructure réseau)

4- Choix de l'architecture :

Il existe deux (02) topologies de connexion entre les équipements mobiles AD-HOC et Infrastructure. Pour le déploiement de notre HotSpot on va utiliser la topologie Infrastructure.

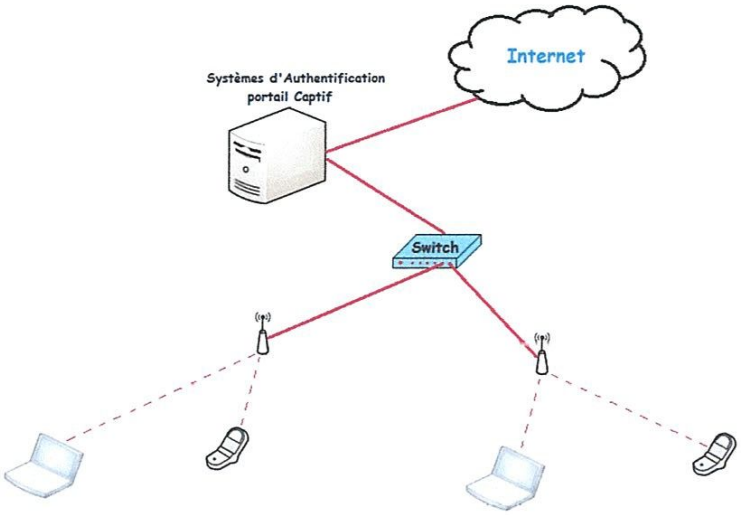


Figure 3.2 : Topologie du HotSpot

5- Choix de la norme Wi-Fi :

Les normes de Wi-Fi sont nombreuses et diverses. De toutes ces normes, les plus connues sont 802.11a, 802.11b et 802.11g, qui sont les principales du standard 802.11 ceci grâce à leur large intégration dans les matériels et logiciels.

Notre orientation a été fixée sur la norme 802.11g qui est compatible avec 802.11b, évoluent tous deux dans la bande des 2,4 Ghz, avec des vitesses de transmission comprises entre 1 et 11Mbit/s pour la norme 802.11b et 1 et 54 Mbit/s pour la norme 802.11g.

6- Calcule de la portée d'une antenne :

Délimiter la zone géographique (surface) que peut desservir un point d'accès avec une puissance donnée (nous devons fixer un seuil de couverture qui sera proportionnel à une QoS cible).

6-1- Cas du Parking

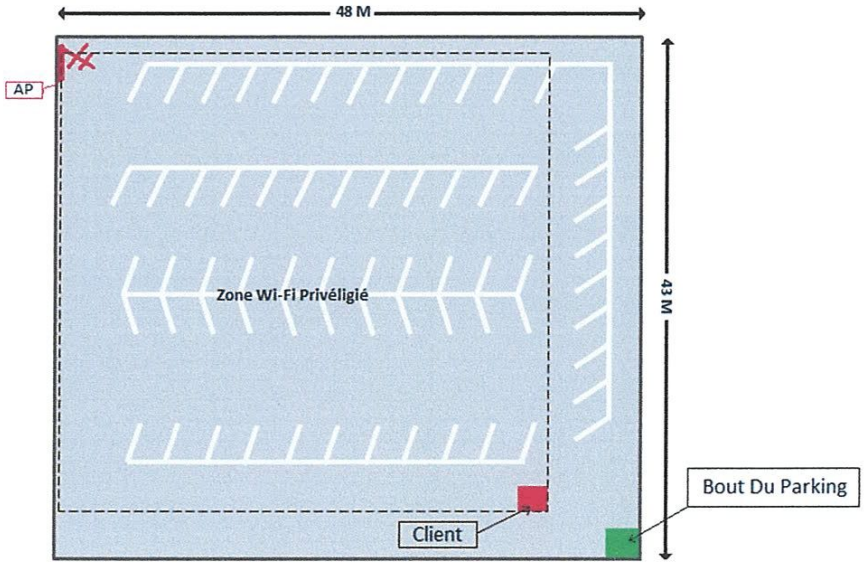


Figure 3.3 : Plan du Parking

1 - Calcul de la distance entre le point d'accès et l'extrémité de la pièce. Puisque la zone Wi-Fi privilégié se termine avant cette extrémité nous obtiendrons une marge d'erreur.

Utilisation de Pythagore :

$$D^2 = 48^2 + 43^2$$

La distance du point d'accès au bout de la pièce est d'environ **65 M**.

2 – Calcul des pertes dues à la propagation pour la distance D = 65 M.

Longueur d'onde $\lambda = (3 * 10\text{^}8) / 2.4\text{Ghz}$

$\lambda = 0.12248$ M

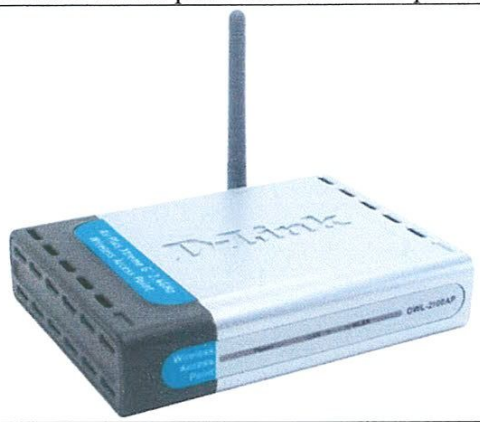
Perte de propagation = $20 * \log ((4 * \pi * 65)/0.12248)$

Perte de propagation = 76 dB.

6-1-1- Matériel d'Emission :

a- AP D-link DWL-2100AP

Le choix a été fait pour des raisons de performance d'un côté et de son faible cout d'un autre côté.

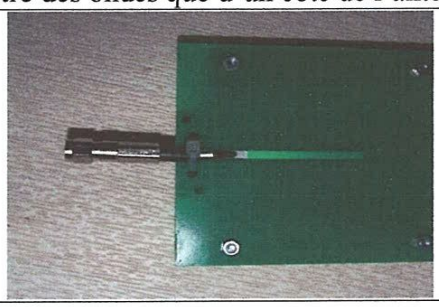


- compatible IEEE 802.11g, (2.4 GHz)
- alimentation par Ethernet (PoE) norme IEEE 802.3af
- Le support WPA et 802.1x autorise une authentification mutuelle sûre, permettant de garantir que seuls les clients légitimes se connectent aux serveurs d'entreprise RADIUS.
- Manageable par protocole SNMP MIB I, MIB II, et 802.11 MIB
- Supporte les protocoles d'authentification de port 802.1x les plus répandus, y compris EAP, TLS, PEAP et TTLS.

- sensibilité en réception classique -75 dBm (Rx) à 54 Mbps
- puissance d'émission (Tx) de 19 dBm

b- Antenne Patch

Choisi puisque le point d'accès se trouvera dans un coin de mur, il vaut mieux donc emmètre des ondes que d'un côté de l'antenne, d'où le choix d'une antenne directive type Patch.



- Fréquence : 2.4 ~ 2.5 GHz
- Gain: 22dBi à 2.45GHz
- Câble : Coaxial de X m
- Polarisation : Linéaire et verticale
- Connecteur : RP SMA

- **Gain d'émission (point d'accès):**

Addition du gain de l'émetteur 19dB + gain de l'antenne 22dB – perte dans le câble 1dB – perte dans le connecteur 1dB.

(La perte dans le câble et dans le connecteur n'étant pas renseigné nous avons pris le pire des cas pour chacun (1dB), donc une marge supplémentaire).

Total = 39dB

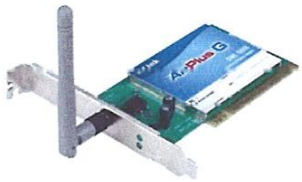
- **Gain de réception (point d'accès):**

Addition du gain du récepteur -75dB + gain de l'antenne 22dB - perte dans le câble 1dB – perte dans le connecteur 1dB.

Total = -55dB

6-1-2- Matériel de réception :

Nous sommes en train de faire une étude pour le déploiement d'un HotSpot Wi-Fi, donc chaque utilisateur va connecter avec leur propre terminal pour cela les caractéristiques des carte réseaux Wi-Fi de ces terminaux sont différents. Mais la plupart des cartes réseaux possèdent les caractéristiques suivantes :

	- Gain d'émission à 54mbps 18 à 22 dBm - Sensibilité de réception a 54mbps -80 à -72 dBm

- **Tableau récapitulatif et bilan radio :**

	Puissance	Perte de propagation	Totale	Respect tolérances
Point d'Accès, émission	39 dB	76 dB à 65 M	-37 dB	54 Mbps **Ok**
Point d'Accès, réception	-55 dB		21 dB	54 Mbps **Ok**
Client réception	-75 dB		1 dB	54 Mbps **Ok**
Client émission	20 dB		-56 dB	54 Mbps **Ok**

Tableau 3.3 : Bilan radio

D'après l'emplacement choisi ainsi que l'équipement, la liaison Wi-Fi sera de bonne qualité puisque nous restons dans la tolérance des 76 dB théorique pour avoir un système opérationnel.
Nous avons pris des marges de tolérance sur :

- La distance
- La qualité médiocre du câble et des connecteurs

Cependant nous n'avons pas pris en compte :

- Les obstacles potentiels aux ondes (personnes, véhicule dans la pièce).
- Le bruit dans l'environnement. (condition météorologique)

Mais si l'on considère que les marges que l'on a accordés sont supérieures ou égale aux paramètres non pris en compte le réseau wifi sera opérationnel à 54mbps, sinon moins mais toujours possible.

6-2- Cas intérieure de l'immeuble

Notre immeuble est un milieu fermé donc l'affaiblissement de la puissance du signal est en grande partie du aux propriétés des milieux traversés par l'onde.
Quelques exemples d'atténuations (en dB)

- Fenêtre (verre), air humide, plastique: 3dB
- Cloison mobile: 6 dB
- Eau, végétation, animaux: 9 dB
- Mur de faible épaisseur (type plâtre): 3 dB
- Mur porteur (béton), verre blindé, dalle métal conducteur: 20 dB

Ces valeurs donnent des ordres de grandeur et ne font bien sûr pas référence [2].

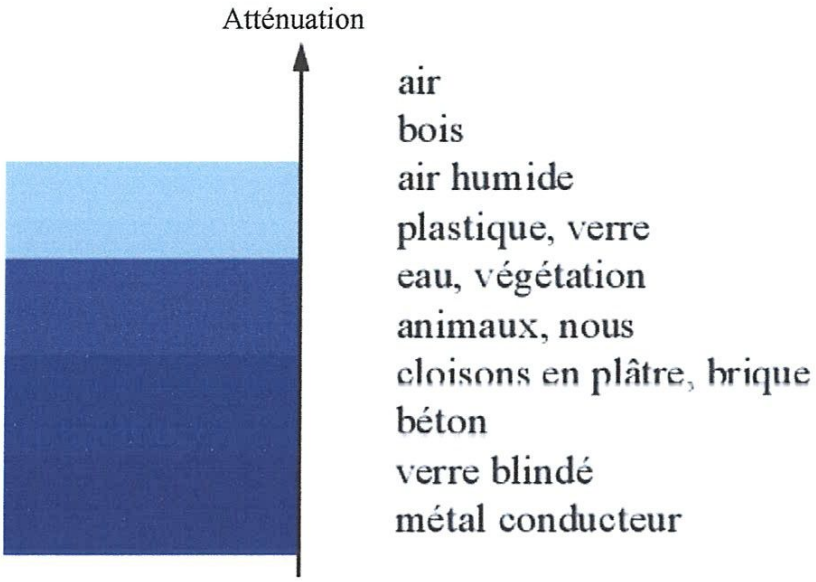


Figure 3.4 : Affaiblissement de signal par rapport aux propriétés des milieux [2]

Voici un tableau donnant les niveaux d'atténuation pour différents matériaux :

Matériaux	Affaiblissement	Exemples
Air	Aucun	Espace ouvert, court intérieur
Bois	Faible	Porte, plancher, cloison
Plastique	Faible	Cloison
Verre	Faible	Vitres non teintées
Verre teinté	Moyen	Vitres teintées
Eau	Moyen	Aquarium, fontaine
Etres vivants	Moyen	Foule, animaux, humains, végétation
Briques	Moyen	Murs
Plâtre	Moyen	Cloisons
Céramique	Elevé	Carrelage
Papier	Elevé	Rouleaux de papier
Béton	Elevé	Murs porteurs, étages, piliers
Verre blindé	Elevé	Vitres pare-balles
Métal	Très élevé	Béton armé, miroirs, armoire métallique

Tableau 3.4 : Affaiblissement par rapport aux propriétés des milieux

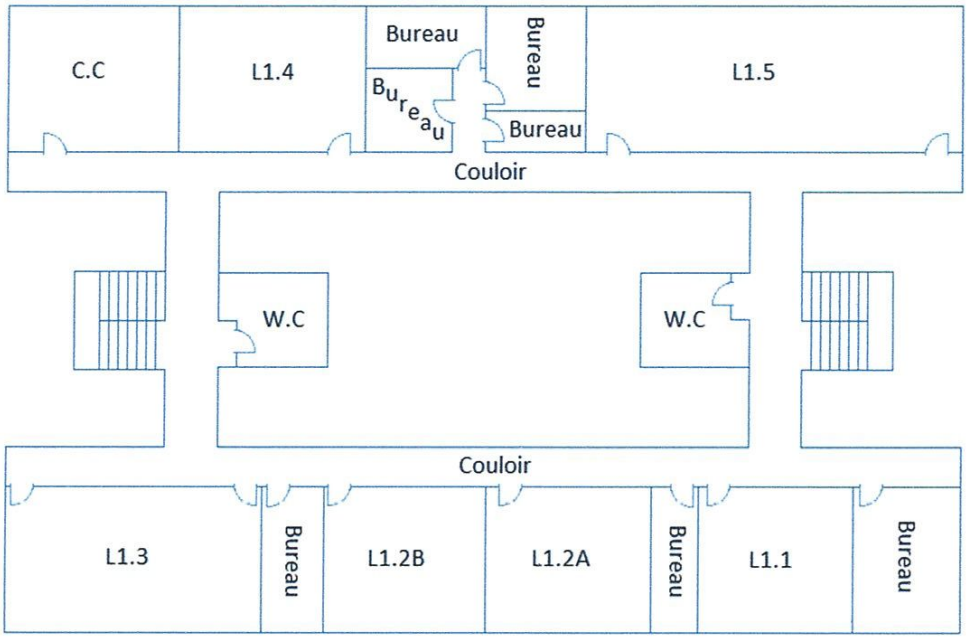


Figure 3.5 : Plan 1er Etage du département d'Electronique et Télécommunications

Pour la couverture intérieure on va garder les mêmes antennes des points d'accès. Car nous avons vu que le gain des antennes qui sont fournis avec les points d'accès est 2.2 dB. Il suffit pour une couverture d'un rayon de 15 M dans un milieu fermé.

7- Estimations de Nombre des utilisateurs :

Il est important d'évaluer le nombre de stations mobiles pouvant être gérées par un seul point d'accès afin de déterminer le nombre de points d'accès pour une même zone à couvrir. Les stations mobiles doivent à portée radio du point d'accès et peuvent évaluer la distance les sépare du point d'accès grâce au niveau de signal reçue.

Le type d'application (données, voix, vidéo) détermine la nature du trafic que le réseau doit écouler. Ainsi, on s'assure que les performances du réseau répondent aux besoins des utilisateurs. Par exemple, on peut être amené à ajouter un nouveau point d'accès ou un autre adaptateur IEEE 802.11 au point d'accès déjà existant de façon à offrir davantage de bande passante et à assurer de meilleurs délais d'accès aux utilisateurs sur le point d'accès concerné.

Pour éviter les cas de saturation de notre systèmes et pour que tous les utilisateurs de notre HotSpot peuvent connecter sans problèmes de chute de débit ou de distribution des adresses IP.il faut faire une étude sur la charge de trafic.

Le département d'Electronique et Télécommunications et le département d'Electrotechnique possèdent :

Département ELN & TLC		**Département Electrotechnique**	
Etudiant	136	**Etudiant**	112
Enseignant	28	**Enseignant**	24
Employée	4	**Employée**	5
Total	168	**Total**	141
Total		**309**	

Source : Dép ELN & TLC & Dép ELE

Tableau 3.5: le nombre des enseignants, étudiant et employé pour chaque département