N° d'ordre :
N° de série :

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE D'EL-OUED
FACULTE DES SCIENCES ET TECHNOLOGIE
Département D'électronique

Mémoire de fin d'étude présenté
Pour l'obtention du diplôme de

Licence ACADEMIQUE

Domaine : **Sciences et techniques**
Filière : **Electronique**
Spécialité : **Télécommunications**

Présenté par : **HATROUBI Hadjer**
MEKKAOUI Belkis

Les technologies sans fil : le Wi-Fi et la sécurité

Déposé le 03-06- 2014

Au niveau du jury composé de :

M.	**KHELIL Abdellatif**	MA	Président
M.	**KHELIL Abdellatif**	MA	Examinateur
M.	**BOULILA Mohamed**	MA	Directeur du mémoire

2013-2014

Remerciements

La louange est à Allah, qui nous a facilité l'accomplissement de ce travail de recherche chose ne peut étre qu'avec la volonté de Dieu à lui la tout puissance et la Majesté et que la louange initiale et finale appartient à allah, Seigneur des mondes.

Je tiens à exprimer ma vive reconnaissance et mes sincères remerciements à Monsieur BOULILA Mohamed , pour avoir accepté de diriger mes recherches. Je le remercie également pour sa bienveillance, ses conseils judicieux et l'encadrement de qualité dont il m'a fait bénéficier aimablement. Je lui adresse, en signe de reconnaissance, toute ma gratitude et tout mon respect pour ses qualités humaines et scientifiques.

Je tiens à remercier mes parents pour les nombreuses relectures de ce mémoire et leur soutien sans faille, depuis toujours.

Enfin, j'adresse un remerciement chaleureux à l'ensemble du personnel de Université d'El Oued pour avoir accompagné mon évolution pendant ces trois belles années.

A vous tous, MERCI !

HATROUBI Hadjer
MEKKAOUI Belkis

Dédicaces

À nos parents,

Recevez de moi l'agrume de notre labeur, de nos nuits blanches, de notre exil. Pour votre soutien inconditionnel, votre patience et votre générosité, pour tous les efforts que vous avez consentis en nos faveur, je vous dédie ce travail en témoignage de notre grande reconnaissance.

À nos frères et soeurs,

Je vous dédie ce mémoire en guise de remerciements pour vos encouragements et votre soutien. Je vous souhaite le plus radieux des avenirs.

À tous nos amis pour leurs encouragements et leur soutien, et à tous ceux qui n'ont aidé et soutenu le long de la réalisation de ce projet.

Nos pensées vont également à tous ceux qui n'ont aidé de près ou de loin à mener à bien ce travail.

HATROUBI Hadjer

MEKKAOUI Belkis

Table des matières

Table des matières i
Liste des figures..... ii
Liste des tableaux.....iii
Abréviations.....iv
Introduction générale v
Chapitre 1 : La norme 802.11 (Wi-Fi)
1.1 Introduction 1
1.2 Présentation de la norme Wi-Fi (802.11)..... . 1
1.3 Description des couches de Wi-Fi.....1
1.3.1 La couche physique..... 2
1.3. 1.1 Etalement de spectre en séquence directe (DSSS) 2
1.3. 1.2 Etalement de spectre par saut de fréquence(FHSS) 2
1.3.1.3 Infrarouge 3
1.3.1.4 Modulation multiporteuse (OFDM).....3
1.3.2 La couche liaison de données.....6
1.3.2.1 La couche LLC (Logical Link Control) 6
1.3.2.2 La couche MAC (Media Access Control) 6
1.3.2.2.1 La Fonction de coordination DCF 7
1.3.2.2.2 La Fonction de coordination PCF 9

1.4 Format des trames 9
1.4.1 Préambule (Trame 802.11) 10
1.4.2 En-tête PLCP (Trame 802.11)..... 10
1.4.3 Données MAC (Trame 802.11)..... 10
1.4.3.1 Contrôle de trame (en-tête MAC)..... 11
1.4.3.2 Durée / ID (en-tête MAC).....12
1.4.3.3 Les champs adresses (en-tête MAC).....12
1.4.3.4 Contrôle de séquence (en-tête MAC) 13
1.4.4 Contrôle de redondance cyclique (Trame 802.11).....13
1.4.5 Format des trames les plus courantes.....13
1.4.5.1 Format des trames RTS.....13
1.4.5.2 Format de la trame CTS 14
1.4.5.3 Format de la trame ACK 14
1.5 Les différentes extensions Wi-Fi 14
1.5.1 La norme 802.11a 15
1.5.2 La norme 802.11b..... .16
1.5.3 La norme 802.11g..... 16
1.5.4 La norme 802.11e..... 16
1.5.5 La norme 802.1 1h 17
1.5.6 La norme 802.11i..... 17
1.5.7 La norme 802.11n 17
1.6 Conclusion 18

Chapitre 2 : La sécurité Wi-Fi

2.1 Introduction.....19
2.2 Les caractéristiques des réseaux sans fil et leur impact sur la sécurité.....19
2.2.1 La transmission par ondes électromagnétique 19
2.2.2 Caractéristiques des implémentations 20
2.2.3 Le brouillage radio..... 20
2.2.4 L'utilisation de batteries 20
2.3 Les attaques contre les réseaux sans fil 20
2.3.1 Le déni de service.....20
2.3.2 Le reniflement 21
2.3.3 Le guerre conduite 21

2.3.4 Le farinage guerre 22
2.3.5 L'usurpation 22
2.4 Sécuriser le Wi-Fi..... 22
2.4.1 Les protocoles de sécurité..... 25
2.4.1.1 Le chiffrement WEP 25
2.4.1.2 Le WPA 28
2.4.2 Les extensions de sécurité 29
2.4.2.1 La 802.1x 29
2.4.2.2 La norme 802.11i 32
2.5 Conclusion 33

Chapitre 3 : Configuration d'un réseau Wi-Fi

3.1 Introduction..... 34
3.2 Configuration d'un réseau sans fil ..... .34
3.2.1 Configuration d'un réseau avec infrastructure 34
3.2.1.1 Présentation du mode d'implémentation "Infrastructure" 34
3.2.1.2 Schéma du réseau 35
3.2.1.3 Processus d'installation.....35
3.2.1.3.1. Configuration du point d'accès.....35
3.2.1.3.2. Connexion au réseau sans fil.....36
3.2.2 Configuration d'un réseau sans infrastructure (ad hoc) 39
3.2.2.1 Présentation du mode d'implémentation "Ad Hoc".....39
3.2.2.2 Configuration d'un réseau Ad Hoc sous Windows XP SP2 39
3.2.2.2.1 Schéma du réseau.....39
3.2.2.2.2 Processus d'installation.....40
3.3 Conclusion 43
Conclusion Générale.....vi
Annexes.....vii
Rapport de stage.....viii
Bibliographie.....ix

Liste des figures

Chapitre 1 : La norme 802.11 (Wi-Fi)

Fig 1.1 - Répartition des 14 canaux des technologie DSSS..... 2

Fig 1.2 - La transmission OFDM..... 4

Fig 1.3 - Spectre de la modulation multiporteuse OFDM 4

Fig 1.4 - L'organisation de la couche Liaison..... 6

Fig 1.5 - Mécanisme de vérification du canal.....7

Fig 1.6 - Algorithme de la méthode d'accès DCF.....8

Fig 1.7 - Les composants des trames 802.11.....9

Fig 1.8 - Format de trame utilisée dans le Wi –Fi..... 10

Fig 1.9 - La description des champs de contrôle..... 11

Fig 1.10 - Les format des trames RTS..... 13

Fig 1.11 - Format de la trame CTS..... 14

Fig 1.12 - Format de la trame ACK..... 14

Fig 1.13 - Fréquence centrale de la norme 802.11a..... 16

Chapitre 2: La sécurité Wi-Fi

Fig 2.1 - Architecture de sécurisation..... 25
Fig 2.2 - Le chiffrement WEP..... 26
Fig 2.3 - Echanges pour l'authentification dans WEP..... 27
Fig 2.4 - Architecture la norme 802.1x..... 29
Fig 2.5 - Principe de fonctionnement de 802.1x..... 30
Fig 2.6 - Le mécanisme d'authentification de 802.1x..... 31
Fig 2.7 - Les phases opérationnelles du 802.11i..... 32

Chapitre 3: Configuration d'un réseau Wi-Fi

Fig 3.1 - Réseau sans fil avec infrastructure 33
Fig 3.2 - Schéma du réseau en mode infrastructure.....34
Fig 3.3 - Page d'accueil du point d'accès 35
Fig 3.4- Icône de connexion réseau sans fil 35
Fig 3.5 - Sélectionner réseaux avec point d'accès uniquement.....36
Fig 3.6 - Connexion au réseau `rectorat-academie'.....36
Fig 3.7 - Authentification auprès du serveur 37
Fig 3.8 - Machine connectée 37
Fig 3.9 - Réseau «rectorat-academie »....37
Fig 3.10 - La topologie ad hoc 38
Fig 3.11 - Propriétés de connexion réseau sans fil 39
Fig 3.12 - Propriété du réseau sans fil..... 40
Fig 3.13 - Connexion réseau sans fil 41
Fig 3.14 - Connexion au réseau NUMERICABLE-XXX 41
Fig 3.15 - La connexion de la machine créatrice du réseau 41
Fig 3.16 - Connexion d'autres machines 42

Liste des tableaux

Tableau 1.1 - Nombre de sous canaux utilisés pour le FHSS…… 3
Tableau 1.2 - Tableau comparatif entre les différentes technologies de transmission du 802.11 …… 5
Tableau 1.3 - L'utilisation des différentes adresses selon les bits From DS et To DS… 13
Tableau 1.4 - Paramètres dimensionnant de la couche physique IEEE 802.11a…… 16
Tableau 1.5 - Les différentes normes 802.11…… 18

Abréviations

A

AA : Authentification Agent

ACL : Access Control List

ACK : ACKnowledgement

AES : Advanced Encryption Standard ou Audio Engineering Society

AP : Access Point

B

BSS : Basic Service Set

BSSID : Basic Service Set Identifier

BEB : Binary Exponentiel Bachoff

C

CCK : Complementary Code Keying

CRC : Cyclic Redondance Control

CSMA/CA : Carrier Sense Multiple Access with Collision Avoidance

CTS : Clear To Send

D

DBPSK : Differential Binary Phase Shift Keying

DCF : Distributed Coordination Function

DHCP : Dynamic Host Configuration Protocol

DIFS : Distributed Inter-Frame Space

DOS : Denial Of Services

DQPSK : Differential Quadrature Phase Shift Keying

DS : Distribution System

DSSS : Direct Sequence Spread Spectrum

E

EAP : Extensible Authentification Protocol

ESS : Extended Service Set

F

FCS : Frame Check Sequence

FEC : Forward Error Connection

FHSS : Frequency Hope Spread Spectrum

G

GFSK : Gaussian Frequency Shift Keying

GPS : Global Positioning System

H

HR/DSSS : High Rate DSSS

http : HyperText Transfer Protocol

I

IBSS : Independant Basic Setvice Set

ICV : Integrity Check Value

ID : IDentifier

IEEE : Institute of Electrical and Electronics Engineers

IP : Internet Protocol

IR : InfraRed

ISM : Industrial , Scientific and Medical

IV : Initializator Vector

L

LAN : Local Aera Netxork

LLC : Logical Link Control

LSAP : Logical Service Access Point

M

MAC : Medium Access Control

MIC : Message Integrity Protocol

MK : Master Key

N

NAV : Network Allocation Vector

o

OFDM : Orthogonal Frequency Division Multiplexing

OSI : Open System Interconnection

P

PAE : Port Access Entity

PBCC : Paquet Binary Convolutional Codeing

PDA : Personnal Data Assistant

PLCP : Physical Layer Convergeance Protocol

PPM : Pulse Position Modulation

Q

QAM : Quadrature Amplitude Modulation

QoS : Quality of Services

R

RADIUS : Remote Authentication Dial In User Server

RC4 : Ron's Cipher 4

RSN : : Robust Security Network

RSNA : Robust Security Network Association

RTS : Request To Send

S

SFD : Start Frame Delimiter

SSID : Service Set Identifier

STA : station terminale

SIFS : Short Inter Frame Space

T

TF : Transformée de Fourier

TKIP : Temporal Key Integrity Protocol

U

U-NII : Unlicenced –National Information Infrastructure

UM : Unité Mobile

W

WECA : Wireless Ethernet Compatibility Alliance

WEP : Wired Equivalent Privacy

Wi-Fi : Wireless Fidelity

WLAN : Wireless Local Area Network

WPA : WiFi Protocol Access ; Wireless Protected Access;

Introduction Générale

Les réseaux sans fil ont été crées pour permettre aux utilisateurs d'effectuer des communications de tel sorte à garder la connectivité des équipements, tout en ayant gain de mobilité et sans avoir recours aux " fils " utilisés dans les réseaux traditionnels et qui encombrent ces derniers.

Ces dernières années, les technologies sans fil ont connues un essor considérable que se soit au niveau commercial ou dans le domaine des recherches, ceci revient aux multiples avantages qu'elles offrent (mobilité, faible coûts, etc.). Mais, comparer aux interfaces filaires, peu nombreuses sont les interfaces sans fil qui offrent un débit rapide (ondes hertziennes, l'infrarouge) [1].

Il existe plusieurs technologies pour les réseaux sans fil se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions (Bluetooth , Zigbee , Hiperlan , Wi-Fi qui est l'objet de ce mémoire), leur arrivée à soulevée un engouement nouveau pour les réseaux radio qui étaient jusqu'alors le domaine exclusif des militaires.

les réseaux sans fil sont classés en quatre catégories selon leur étendue géographique et normalisés par uncertain nombre d'organismes parmi les quels nous citerons l'ISO (International Standardization Organization), l'IEEE (Institute of Electrical and Electronics Engineers) et l'ETSI (European Télécommunications Standards Institute).

Wi-Fi est le nom courant pour Wireless Fidelity, et correspond à la norme IEEE 802.11. Cette norme de réseau informatique sans fil a été définie par le consortium IEEE en 1999. Le nom ' Wi-Fi ' est une marque déposée par le Wireless Ethernet Compatibility Alliance (WECA) [2].

Afin d'effectuer une étude détaillée sur la norme Wi-Fi, notre mémoire est organisé comme suit :

Dans le premier chapitre, nous nous consacrons à l'étude des technologies employées au niveau de la couche physique et la couche liaison de données.

Dans le second chapitre, nous focalisons sur les chiffrements et les standards de sécurité de la norme IEEE 802.11.

Dans le troisième chapitre, nous présentons les différents modes de configuration d'un réseau Wi-Fi avec et sans infrastructure.

Dans le conclusion , nous avons basé sur donner les avantages de réseau Wi-Fi; les problèmes et les inconvénients et leurs solutions .

Finalement, ce mémoire se termine par un rapport de stage qui fait la synthèse de ce qui a été vu tout au long de cette étude et donne un aperçu sur le matériel de travaux pratique de recherche futurs.

Chapitre 1

La norme 802.11 (Wi-Fi)

Sommaire :

1.1 Introduction;
1.2 Présentation de la norme Wi-Fi (802.11);
1.3 Description des couches de Wi-Fi;
1.4 Format des trames;
1.5 Les différentes extensions Wi-Fi;
1.6 conclusion ;

1.1 Introduction :

La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom **Wi-Fi** (contraction de Wireless Fidelity) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance)[1].

Dans ce chapitre, nous allons commencer par une présentation de la norme Wi-Fi ainsi que ses couches physique et liaison, ensuite nous décrivons le format des trames utilisé dans cette norme, enfin nous allons citer quelque unes de ses extensions[1].

1.2 Présentation de la norme Wi-Fi (802.11) :

La norme Wi-Fi est une technologie de réseau informatique qui décrit les couches physiques et MAC d'interfaces réseau radio et infrarouge .Elle offre des débits allant jusqu'à 54 Mbps (tout dépond du milieu) sur une distance de plusieurs centaines de mètres suivant les techniques et les éventuelles extensions de la norme employée. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs fixes, des assistants personnels PDA (Personnel Data Assistant) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur)[2].

Le Wi-Fi cible deux contextes d'utilisation distincts pour un réseau Wi-Fi ayant chacun des caractéristiques propres. Il s'agit du mode infrastructure et du mode ad hoc (sans infrastructure). Ces deux modes de fonctionnement permettent de définir la topologie du réseau sans fil[2].

1.3 Description des couches de Wi-Fi :

La norme Wi -Fi définit les deux couches basses du modèle OSI d'un réseau sans fil de type WLAN (Wireless LAN), à savoir une couche liaison de données et une couche physique[2].

1.3.1 La couche physique :

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, elle propose plusieurs types de codage de l'information : DSSS, FHSS, IR, OFDM, toutes ces technologies permettent des débits de 1Mbps et 2Mbps[3].

1.3.1.1 Etalement de spectre en séquence directe (DSSS) :

DSSS (Direct Sequence Spread Spectrum) est une deuxième couche physique définie dans la norme 802.11 de 1997. Elle sera également présente dans la norme 802.11b ratifiée en 1999. Il s'agit d'une couche physique divisant la bande de 2,4GHz à 2,483GHz en 3 canaux de 22MHz. Il est donc possible d'utiliser 3 réseaux WLAN différents sur un même site, sans risquer de perturbations . Les modulations utilisées sont des DBPSK (Differential Binary Phase Shift Keying) et DQPSK (Differential Quadrature Phase Shift Keying), respectivement pour les normes à 1et 2Mbits/s. Il s'agit de modulations de phase ,la première associant 1 bit à 1 symbole et la seconde associant 2 bits à chaque symbole . La norme 802.11b utilise quant à elle une modulation CCK (Complementary Code Keying) ou PBCC (Packet Binary Code Keying). La modulation CCK est en fait une méthode de codage qui ici, utilise la modulation DQPSK. Elle permet d'associer 4 ou 8 bits à chaque symbole. De même, la PBCC est le codage associé à une modulation DBPSK, pour un débit de 5,5Mbit/s, ou DQPSK, pour une modulation de 11 Mbits/s sur une couche PHY DSSS[3,5].

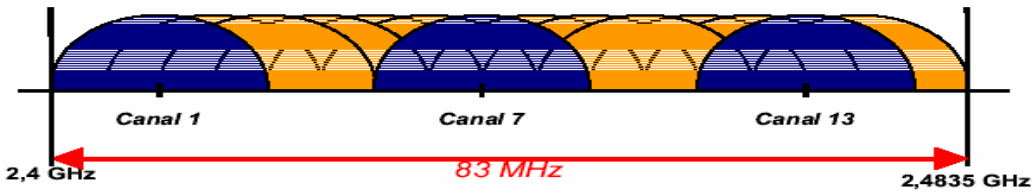


Fig 1.1 - Répartition des 14 canaux des technologie DSSS

1.3.1.2 Etalement de spectre par saut de fréquence(FHSS) :

La FHSS (Frequency Hopping Spread Spectrum) est utilisée par la première norme 802.11 et permet d'atteindre des débits de 1 ou 2 Mbit/s. La plage de 2,4 à 2,483GHz est divisée en 79 canaux distincts, chacun d'une largeur de 1MHz. La particularité de la FHSS est que la transmission ne se fait pas sur un canal unique,

mais en sautant de canal en canal selon une séquence pseudo aléatoire connue. A l'origine, cette technique est issue des systèmes de transmission militaires afin que les messages transmis ne puissent pas être interprétés, la porteuse changeant de fréquence de manière très rapide. En effet ,une FHSS change de canal toutes les 400 ms. Ceux- ci sont régis par 3 jeux de canaux ayant chacun 26 séquences (26 sauts de fréquences par jeux). La modulation utilisée avec la FHSS est une GFSK (Gaussian Frequency Shift Keying). Il s'agit d'une modulation de fréquence filtrée par un filtre gaussien (permettant d'éliminer les résidus de composantes continues engendrées par la modulation)[3,4].

Pays	Etats-Unis	Europe	Japon
Nombre de canaux utilisés	79	79	23

Tableau 1.1- Nombre de sous canaux utilisés pour le FHSS

1.3.1.3 Infrarouge (IR) :

Une liaison infrarouge permet de créer des liaisons sans fil de quelques mètres avec un débit qui peut atteindre quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dûes aux interférences lumineuses [6] .

Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelée PPM (pulse position modulation). Cette dernière consiste à transmettre des impulsions à amplitudes constantes, et à coder l'information suivant la position de l'impulsion[6] .

1.3.1.4 Modulation multiporteuse (OFDM):

Le OFDM (Orthogonal Frequency Division Multiplexing) est une modulation multiporteuse, utilisée par les normes 802.11a, 802.11n . Le canal est ici subdivisé en 52 sous-porteuses . Chaque sous-porteuse n'a donc qu'une faible bande passante et par conséquent, un faible débit. Cependant, toutes ces sous-porteuses vont être utilisées pour transmettre les données en parallèle. La particularité de l'OFDM tient notamment dans la manière dont sont agencées ces sous-porteuses afin de maximiser leur nombre sur une bande passante donnée. En effet, chaque porteuse est

orthogonale aux porteuses qui l'entourent. Ceci signifie que les spectres de chaque porteuse se recouvrent partiellement, mais que, lorsque le spectre d'une sous porteuse atteint un maximum de puissance, alors le spectre des sous porteuses adjacentes devient nul[4].

L'un des grands avantages de l'OFDM est que toutes les opérations sont réalisées dans le domaine fréquentiel , ce qui simplifie grandement les calculs et l'implémentation des circuits radio. Une transformée inverse de Fourier est utilisée en bout de la chaîne radio afin de passer le signal dans le domaine temporel[5].

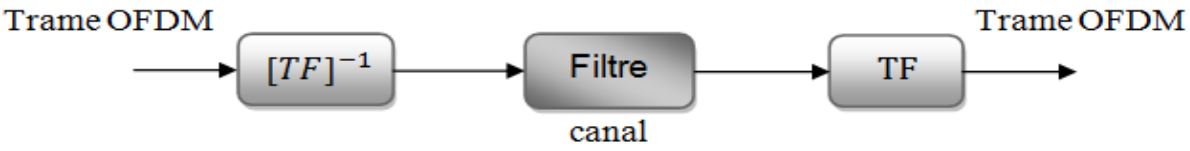


Fig 1.2 - La transmission OFDM

La modulation utilisée pour moduler chacune des sous-porteuses est la DBPSK, la DQPSK(aussi appelée 4-QAM) ou encore la m-QAM selon le débit escompté. La m-QAM est la modulation permettant d'obtenir les meilleurs débits. QAM signifie "Quadrature Amplitude Modulation". Il s'agit d'une combinaison d'une modulation d'amplitude et d'une modulation de phase. Pour mieux comprendre, l'étude de quelques formules mathématiques s'impose[5].

Le signal de la porteuse peut être écrit ainsi :

$$P(t)= A(t).\ e^{j2\pi fpt} \qquad (1.1)$$

$$P(t)= I(t).\cos(2\pi fpt)+Q(t).\sin(2\pi fpt) \qquad (1.2)$$

Avec :

I(t) : amplitude de la composante réelle

Q(t) : amplitude de la composante en quadrature.

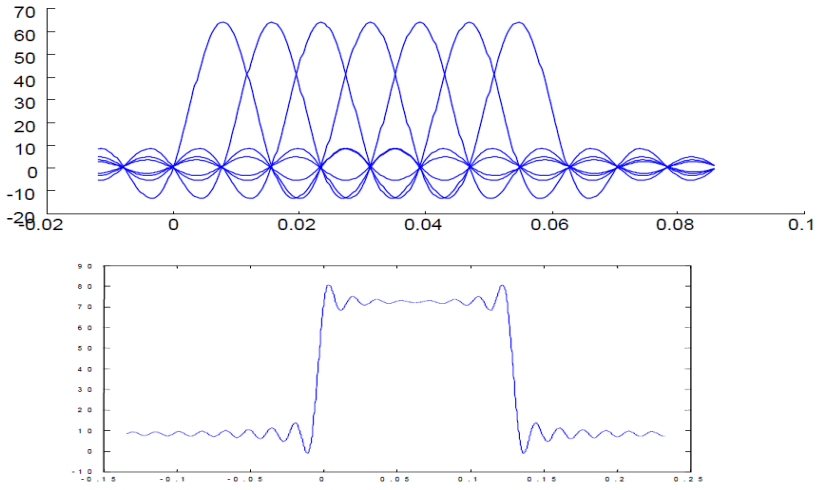


Fig 1.3 - Spectre de la modulation multiporteuse OFDM

L'ensemble des symboles présents dans le repère Oiq est appelé constellation. Cette constellation, et en conséquence le nombre de bits pouvant être transmis en une fois, peut être augmentée pour un meilleur débit binaire. Au plus récepteur de différencier un symbole d'un autre et au plus cette détection sera une constellation contient de symboles , au plus il est difficile pour le vulnérable au bruit. En effet, si on augmente le nombre de symboles dans une constellation ,la distance inter symboles s'en retrouve réduite . La m-QAM comportant le plus grand nombre de symboles dans les modulations utilisés par les normes 802.11 est la 64-QAM. Chaque symbole code donc 6 bits[5].

- Comparaison entre ces techniques **:**

Technique de transmission	***Avantages***	***Inconvénients***
DSSS	**-** Elle propose des vitesses de transmissions plus importantes	**-** L'utilisation d'un seul canal pour la transmission, rend le système DSSS plus sensibles aux interférences.
FHSS	**-** Elle empêche une perte totale du signal, grâce à la technique de transmission par saut. **-** Elle constitue une solution efficace dans un environnement où il y a beaucoup de multitrajets.	**-** faible largeur de bande par canal ne lui permettant pas d'atteindre des vitesses de transmissions élevées. - Utilisation de toute la largeur de bande, ce qui implique une charge supplémentaire sur le réseau.
Infrarouge		**-** La transmission se fait avec une longueur d'onde très faible. **-** Une traversée des obstacles (murs, plafonds, cloisons...) n'est pas possible.
OFDM	**-** Permet d'atteindre des vitesses de transmission jusqu'à 54 Mbps pour la 802.11a et la 802.11g. - Elle offre un mécanisme de correction d'erreurs sur l'interface physique.	

Tableau 1.2-Tableau comparatif entre les différentes technologies de transmission du 802.11

1.3.2 La couche liaison de données :

La couche liaison de données a pour objectif de réaliser le transport des données et elle est constituée de deux sous-couches :

1.3.2.1 La couche LLC (Logical Link Control) :

La couche *LLC* a été définie par le standard IEEE 802.2 .elle permet d'établir un lien logique entre la couche MAC et la couche réseau du modèle OSI (transition vers le haut jusqu'à la couche réseau). Ce lien se fait par l'intermédiaire du Logical Service Access Point (LSAP) [7].

La trame LLC contient une adresse en en-tête ainsi qu'une zone de détection d'erreur en fin de trame : le **f**orward **e**rror **c**orrection (FEC) comme le montre la figure 1.4 :

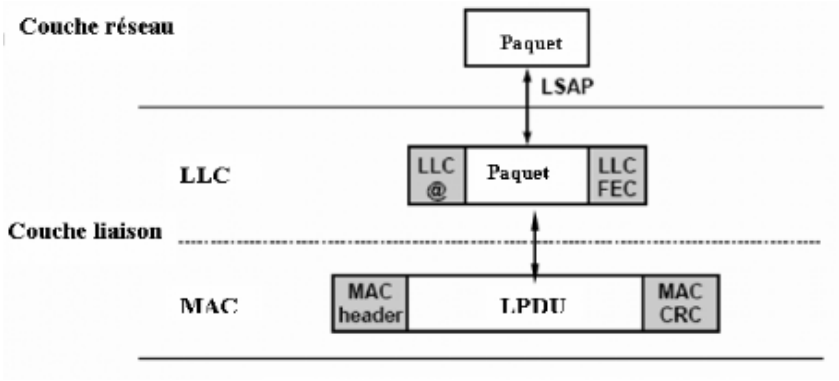


Fig 1.4 - L'organisation de la couche Liaison

Son rôle principal réside dans son système d'adressage logique, qui permet de masquer aux couches hautes les informations provenant des couches basses. Cela permet de rendre interopérables des réseaux complètements différents dans la conception de la couche physique ou la couche MAC possédant la couche LLC[7].

1.3.2.2 La couche MAC (Media Access Control) :

La sous-couche MAC est spécifique à la norme Wi-Fi et définit deux nouveaux mécanismes qui assurent la gestion d'accès de plusieurs stations à un support partagé dans lequel chaque station écoute le support avant d'émettre, elle assure aussi le

contrôle d'erreur permettent de contrôler l'intégrité de la trame à partir d'un CRC (voir format de trame). Elle peut utilisée deux modes de fonctionnement[8] :

1.3.2.2.1 La Fonction de coordination DCF :

Le DCF (**D**istributed **C**oordination **F**onction) est un mode qui peut être utilisé par tous les mobiles, et qui permet un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès (mode totalement distribué). Il met en oeuvre un certain nombre de mécanismes qui visent à éviter les collisions et non pas à les détecter. Dans ce mode tous les nœuds sont égaux et choisissent quand ils veulent parler. Ce mode peut aussi bien être lorsqu'il n'y a pas de station de base (mode ad hoc) que lorsqu'il y en a (mode infrastructure) . Ce mode s'appuie sur le protocole CSMA/CA[8].

- **La méthode d'accès de base CSMA/CA :**

Un protocole CSMA/CA (Carier Sense Multiple Access with Collision Avoidance) utilise un mécanisme d'esquive de collision en imposant un accusé de réception systématique des paquets (ACK), ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception[9].

Ce protocole fonctionne de la manière suivante : Une station voulant émettre, doit d'abord écouter le support de transmission, s'il est occupé (i.e. une autre station est en train d'émettre), alors, la station remet sa transmission à plus tard. Dans le cas contraire, la station est autorisée à transmettre[9] .

La procédure de vérification se fait en utilisant deux types de messages, le premier est appelé **RTS** (Ready To Send) qui est envoyé par la station et contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond par un deuxième message qui est le **CTS** (Clear To Send), puis la station commence l'émission des données (voir Figure 1.5) .

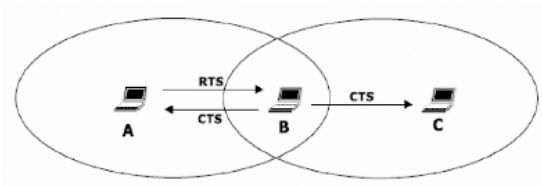


Fig 1.5 - Mécanisme de vérification du canal

A chaque paquet envoyé, l'émetteur doit recevoir un accusé de réception ACK (**ACK**nowledgement), qui indiquera qu'aucune collision n'a eu lieu. Si l'émetteur ne reçoit pas de l'accusé de réception, alors il retransmet la trame après un ACK_TIMEOUT jusqu'à ce qu'il obtienne ou abandonne au bout d'un certain nombre de transmission [7].

Ce type de protocole est très efficace quand le support n'est pas surchargé, mais il y a toujours une chance que des stations émettent en même temps (collision). Cela est dû au fait que les stations écoutent le support, repèrent qu'il est libre, et finalement décident de transmettre, parfois en même temps qu'un autre exécutant, cette même suite d'opération[10].

Ces collisions doivent être détectées pour que la couche MAC puisse retransmettre le paquet sans avoir à repasser par les couches supérieures, ce qui engendrerait des délais significatifs[10].

- **Algorithme de backoff exponentiel BEB (Binary Exponentiel Backoff) :**

Le backoff est une méthode bien connue pour résoudre les différents entre plusieurs stations voulant avoir accès au support. Cette méthode demande que chaque station choisisse un délai d'attente aléatoire compris entre 0 et la taille d'une fenêtre de contention de valeur CW qui est égale à un certain nombre de slots, et d'attendre ce nombre de slots avant de transmettre, toujours en vérifiant qu'une autre station n'a pas accédé au support avant elle[10].

Le backoff exponentiel signifie qu'à chaque fois qu'une station choisit un slot et provoque une collision, la durée d'attente aléatoire est augmentée exponentiellement (doublée à la tentative de transmission suivante). La figure suivante montre l'algorithme de la méthode d'accès DCF[7] :

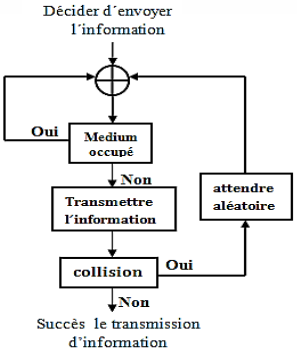


Fig 1.6 - Algorithme de la méthode d'accès DCF

1.3.2.2.2 La Fonction de coordination PCF:

Le PCF (**P**oint **C**oordination **F**onction) appelée mode d'accès contrôlé, est fondé sur l'interrogation à tour de rôle des stations, contrôlées par le point d'accès qui indiquera a chacun des mobiles qui lui sont rattachés quand ils doivent émettre leurs paquets. Durant la phase où le point d'accès impose l'ordre des transmissions, il n'y a pas de contention pour l'accès au canal[7].

Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données. Cette méthode est optionnelle et ne fonctionne qu'en mode infrastructure[7].

1.4 Format des trames :

Le taux d'erreur de transmission sur les réseaux sans fils augmente généralement avec des paquets de taille importante, c'est la raison pour laquelle le Wi-Fi offre un mécanisme de fragmentation, permettant de découper une trame en plusieurs morceaux (fragments) [10].

La norme Wi-Fi définit le format des trames échangées .Chaque trame est constituée d'un en-tête (appelé MAC header, d'une longueur de 30 octets), d'un corps et d'un FCS (Frame Sequence Check) permettant la correction d'erreur[10].

Il y a trois principaux types de trames :

- Les trames de **données**, utilisées pour la transmission des données.
- Les trames de **contrôle**, utilisées pour contrôler l'accès au support (eg : RTS, CTS, ACK).
- Les trames de **gestion**, transmises de la même façon que les trames de données pour l'échange d'informations de gestion, mais qui ne sont pas transmises aux couches supérieures.

Chacun de ces trois types est subdivisé en différents sous-types, selon leurs fonctions spécifiques. Toutes les trames 802.11 sont composées des composants suivants [11]:

Préambule	En-tête PLCP	Données MAC	CRC

Fig 1.7- Les composants des trames 802.11

1.4.1 Préambule (Trame 802.11) :

Il est dépendant de la couche physique et comprend :

Synch : c'est une séquence de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne appropriée (si plusieurs sont utilisées), et pour corriger l'offset de fréquence et de synchronisation.

SFD : Le Start Frame De limiter consiste en la suite de 16 bits 0000 1100 1011 1101, utilisée pour définir le début de la trame[11].

1.4.2 En-tête PLCP (Trame 802.11) :

L'en-tête PLCP est toujours transmis à 1 Mbps et contient des informations logiques utilisées par la couche physique pour décoder la trame :

- Longueur de mot du PLCP_PDU : il représente le nombre d'octets que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.

- Fanion de signalisation PLCP : il contient seulement l'information de taux, encodé à 0,5 Mbps, incrémenté de 1 Mbps à 4,5 Mbps.

- Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC 16 bits[11].

1.4.3 Données MAC (Trame 802.11) :

La figure suivante montre le format général de la trame MAC, certains champs sont seulement présents dans une partie des trames, comme décrit ultérieurement.

Contrôle *de trame* (2octets)	Durée/ID (2octets)	Adresse1 (6octets)	Adresse2 (6octets)	Adresse3 (6octets)	Contrôle de séquence (2octets)	Adresse4 (6octets)	Corps de la trame 0-2312 octets	CRC 4octets

En-tête MAC

Fig 1.8 - Format de trame utilisée dans le Wi–Fi

1.4.3.1 Contrôle de trame (en-tête MAC) :

Le champ de contrôle de trame contient les informations suivantes :

Version de protocole	type	Sous - type	To DS	From DS	More Frag	Retry	Pwr Mgl	More Data	WEP	Order

octet 1 (2.2 et 4 bits) **octet 2** (0 fois 1bit)

Fig 1.9 - La description des champs de contrôle

- **Version de protocole** : ce champ contient 2 bits qui pourront être utilisés pour reconnaître des versions futures possibles du standard 802.11. Dans la version courante, la valeur est fixée à 0.
- **Type et sous-type** : Ces champs respectivement, de 2 et 4 bits, définissent le type et le sous- type des trames. Il existe trois types de trames : des trames de données (pour la transmission des données), les trames de contrôle utilisées pour l'accès au support (RTC, CTS…) et les trames de gestion utilisées pour l'association à un point d'accès ou pour la synchronisation et l'authentification.
- **To DS** (pour le système de distribution) : ce bit est mis à 1 lorsque la trame est adressée au Point d'Accès pour qu'il l'a fasse suivre au DS (Distribution System). Ceci inclut le cas où le destinataire est dans la même cellule et que le Point d'Accès doit relayer la trame. Le bit est à0 dans toutes les autres trames.
- **From DS** (venant du système de distribution) : ce bit est mis à 1 quand la trame vient du DS.
- **More Fragments** (d'autres fragments) : ce bit est mis à 1 quand il y a d'autres fragments qui suivent le fragment en cours.
- **Retry** (retransmission) : ce bit indique que le fragment est une retransmission d'un fragment précédemment transmis. Ceci sera utilisé par la station réceptrice pour reconnaître des transmissions doublées de trames, ce qui peut arriver si un paquet d'accusé de réception se perd.
- **Power Management** (gestion d'énergie) : ce bit indique que la station sera en mode de gestion d'énergie après la transmission de cette trame. Ceci est utilisé par les stations changeant d'état, passant du mode d'économie d'énergie au mode active ou le contraire.

- **More Data** (d'autres données) : ce bit est également utilisé pour la gestion de l'énergie. Il est utilisé par le Point d'Accès pour indiquer que d'autres trames sont stockées pour cette station. La station peut alors décider d'utiliser cette information pour demander les autres trames ou pour passer en mode actif.
- **WEP** (sécurité) : ce bit indique que le corps de la trame est chiffré suivant l'algorithme WEP.
- **Order** (ordre) : ce bit indique que cette trame est envoyée en utilisant la classe de service strictement ordonné (Strictly-Ordered service class). Cette classe est définit pour les utilisateurs qui ne peuvent pas accepter de changement d'ordre entre les trames unicast et multicast [11].

1.4.3.2 Durée / ID (en-tête MAC) :

Ce champ à deux sens, dépendant 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 NAV.

1.4.3.3 Les champs adresses (en-tête MAC) :

Une trame peu contenir jusqu'à 4 adresses, selon le bit **To DS** et **From DS** définit dans le champ de contrôle, comme suit :

- **Adresse 1** : est toujours l'adresse du récepteur (i.e. la station de la cellule qui est le récepteur imsupport du paquet). Si To DS est à 1, c'est l'adresse du Point d'Accès. sinon , c'est l'adresse de la station.
- **Adresse 2 :** est toujours l'adresse de l'émetteur (i.e. celui qui, physiquement, transmet le paquet). Si From DS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice .
- **Adresse 3** :est l'adresse de l'émetteur original quand le champ From DS est à 1. Sinon, et si To DS est à 1, Adresse 3 est l'adresse destination.
- **Adresse 4** :est utilisé dans un cas spécial, quand le système de distribution sans fil (Wireless Distribution System) est utilisé et qu'une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, To DS et From DS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire[11].

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

Tableau 1.3 - L'utilisation des différentes adresses selon les bits From DS et To DS

1.4.3.4 Contrôle de séquence (en-tête MAC) :

Le champ de contrôle de séquence est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame, et pour reconnaître les paquets dupliqués. Il consiste en deux sous-champs, le numéro de fragment et le numéro de séquence qui définissent le numéro de trame et le numéro du fragment dans la trame[11].

1.4.4 Contrôle de redondance cyclique (Trame 802.11) :

C'est un champ de 32 bits, qui est un résumé de message correspondant au reste de la division de ce message par le polynôme définit pour le CRC32. On pourra avoir le même CRC32 pour plusieurs messages différents alors qu'un message donné aura toujours le même CRC32[2].

Ce résumé de message, qui est calculé avant l'envoi permet de certifier que le message n'a pas subi de modification (bien que cela soit possible si le nouveau message à été choisi pour que son CRC32 soit identique à celui de l'original) ce qui permet de garantir l'intégrité de la trame[11].

1.4.5 Format des trames les plus courantes :

1.4.5.1 Format des trames RTS :

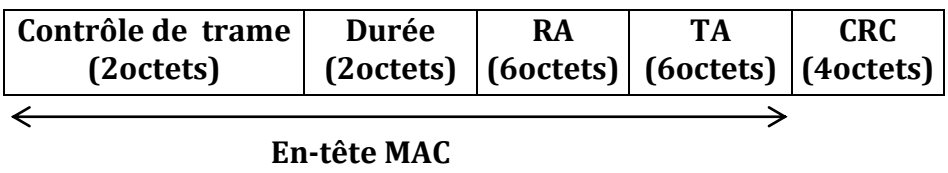


Fig 1.10 - Les format des trames RTS

RA : est l'adresse du récepteur de la prochaine trame de données ou de gestion.

TA : est l'adresse de la station qui transmet la trame RTS.

La valeur de la durée est le temps, en microsecondes, nécessaire à la transmission de la trame de gestion ou de données suivante, plus une trame CTS, plus une trame ACK, plus 3 intervalles SIFS [10].

1.4.5.2 Format de la trame CTS :

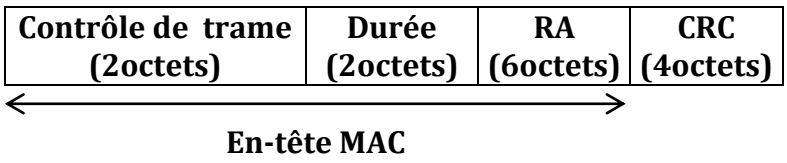


Fig 1.11 - Format de la trame CTS

RA : est l'adresse du récepteur de la trame CTS, directement copiée du champ TA de la trame RTS.

La valeur de la durée est la valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame CTS et d'un intervalle SIFS[10].

1.4.5.3 Format de la trame ACK :

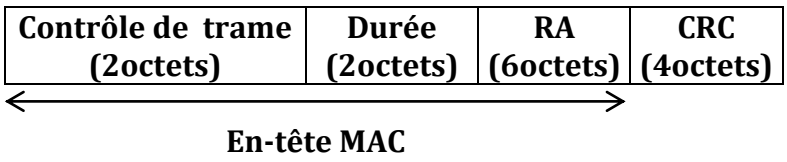


Fig 1.12 - Format de la trame ACK

RA est le champ directement copié du champ Adresse 2 de la trame précédent cette trame ACK.

Si le bit More Fragment était à 0 dans le champ de contrôle de trame de la trame précédente, la valeur de la durée est mise à 0. Sinon, c'est la valeur du champ durée précédent, moins le temps, en microsecondes, demandé pour transmettre la trame ACK et l'intervalle SIFS[10].

1.5 Les différentes extensions Wi-Fi :

Le Wi-Fi est un regroupement de plusieurs normes IEEE 802.11 (802.1 1a, b, g, e, h,...), définissant la transmission de données via le medium «hertzien», elles se

différencient principalement selon la bande passante, la distance d'émission, ainsi que le débit qu'elles offrent[2]. Les principales extensions sont les suivantes :

1.5.1 La norme 802.11 a (WiFi 5) :

Wi-Fi 5 utilise la bande U-NII située autour de 5 GHz. Cette bande offre une largeur égale à 300 MHz (au lieu des 83.5 MHz de la bande ISM).Utilisant une approche OFDM, cette couche physique représente une avancée importante par rapport aux formes d'ondes précédemment décrites dans ce document [7].

La norme 802.11a permet d'obtenir un haut débit (54 Mbit/s théoriques). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.

- *Canaux :*

La relation entre la fréquence centrale le numéro de canal est donnée par l'équation suivante :

F centrale du canal = 5000 + 5× nch (MHz) avec nch= 0, 1, …..200.

Cette définition offre un système de numérotation unique pour tous les canaux espacés de 5 MHz entre 5 GHz et 6 GHz.

Les bandes basse et centrale contiennent 8 canaux sur une bande passante totale de 200 MHz tandis que la bande haute contient 4 canaux sur une bande totale de 100 MHz. Les fréquences centrales des canaux situés aux extrémités des bandes basse et centrale doivent être espacées de 30 MHz des fréquences limites des bandes basse et centrale et de 20 MHz des fréquences limites de la bande haute[7].

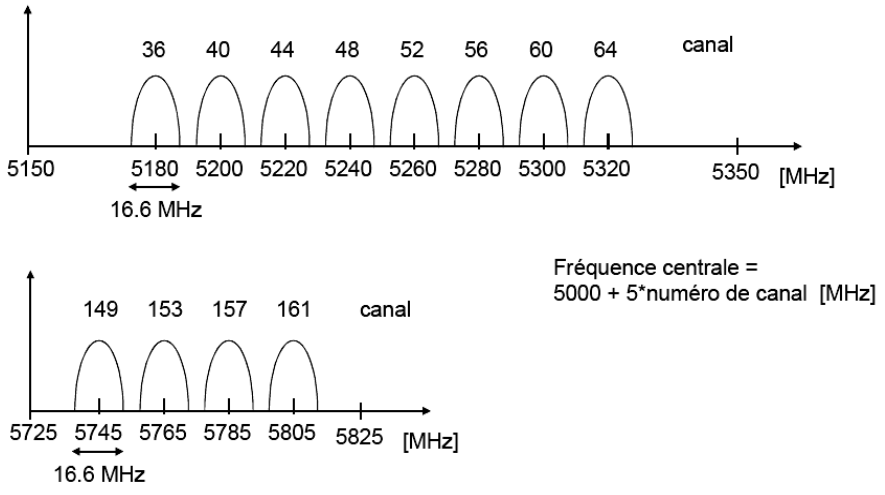


Fig 1.13- Fréquence centrale de la norme 802.11 a

- Quelques paramètres dimensionnant de la couche physique IEEE 802.11a :

Paramètres	Valeurs
NSD : nombre de sous- porteuses de données	48
NSP : nombre de sous- porteuses pilote	4
NST: nombre de sous- porteuses au total	52 (NSD+NSP)
ΔF: espacement en fréquence des sous -porteuses	0.3125 MHz (=20/64 MHz)
TFFT : Période IFFT/FET	3.2 µs(1/ΔF)
T signale : Durée de symbole OFDM	4 µs (TGI+TFFT)
TGI : Durée de l'intervalle de garde	0.8µs (TFFT/4)
Bande passante occupée	16;6 MHz
Largeur des canaux	20 MHz

Tableau 1.4- Paramètres dimensionnant de la couche physique IEEE 802.11a

1.5.2 La norme 802.11b (Wi-Fi) :

En 1999, une nouvelle couche physique 802.11b, plus communément appelée Wi-Fi, a été ajoutée au standard 802.11. Fonctionnant toujours dans la bande ISM, cette couche physique utilise une extension du DSSS, appelée HR/DSSS (High Rate DSSS) [7].

Le HR/DSSS utilise le même système de canaux que le DSSS. Le problème du choix d'un canal permettant la colocalisation de différents réseaux reste donc entier. Comme ils s'appuient sur le DSSS, les réseaux Wi-Fi et 802.11 DSSS sont compatibles et peuvent communiquer entre eux, mais aux débits de 802.11 DSSS, compris entre 1 à 2 Mbit/s[7].

Le HR/DSSS possède une meilleure efficacité spectrale que le DSSS et il permet d'offrir deux débits : 5.5 Mbit/s ou 11 Mbit/s[7].

1.5.3 La norme 802.11g :

Cette norme a été développée en 2003 .Elle étend la norme 802.11b, en augmentant le débit jusqu'à 54Mbps théorique (30 Mbps réels). Elle fonctionne aussi à 2,4GHz, ce qui rend les deux normes parfaitement compatibles[12].

Grâce à cela, les équipements 802.11b sont utilisables avec les points d'accès 802.11g et vice- versa. Cependant, 802.11g utilise la technique de modulation OFDM[13] .

1.5.4 La norme 802.11e :

Disponible depuis 2005. Elle vise à donner des possibilités en matière de qualité de service (QoS) au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo[1].

1.5.5 La norme 802.11h :

Elle cherche à mieux gérer la puissance d'émission et la sélection des canaux dans la bande de 5 GHz. Elle vise aussi à rapprocher la norme 802.11 du standard Européen (Hiper LAN 2) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie [10].

1.5.6 La norme 802.11i :

Ratifié en juin 2004 ,cette norme décrit des mécanismes de sécurité des transmissions. Elle propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11 a, 802.11b et 802.11g. La 802.11i agit en interaction avec les normes 802.11b et 802.11g. Le débit théorique est donc inchangé, à savoir 11 Mbps pour la 802.11b et 45 Mbps pour la 802.11g[1].

1.5.7 La norme 802.11n :

La norme "n" est une amélioration des normes "g" et "a" existant auparavant. Cette nouvelle norme permet d'atteindre des débits théoriques allant jusqu'à 495 Mbit/s alors que les précédentes normes ne permettaient qu'un débit maximum de 54 Mbit/s[10].

Protocole	Date de la norme	Fréquence	Taux de transfert		Portée	
			Type	Max	Intérieur	Extérieur
Legacy	1997	2.4 -2.5 GHz	1 Mbit/ s	2 Mbit/ s	?	**?**
802.11a	1999	5.15-5.35/5.47-5.725/ 5.725-5.875 GHz	25 Mbit/ s	54 Mbit/ s	25m~	**~75m**
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/ s	11 Mbit/ s	~ 35m	**~100m**
802.11g	2003	2.4-2.5 GHz	25 Mbit/ s	54 Mbit/ s	25m~	**~75m**
802.11n	2009	2.4 GHz ou 5GHz	200Mbit/ s	540 Mbit/ s	~ 50m	**~125m**

Tableau 1.5- Les différentes normes 802.11

1.6 conclusion :

Les réseaux sans fil en général, et le Wi-Fi en particulier sont des technologies intéressantes et très utilisées dans de divers domaines comme l'industrie , la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation (absence de câblage), la disponibilité (aussi bien commerciale que dans les expériences). Mais la sécurité dans ce domaine reste un sujet très délicat, car depuis l'utilisation de ce type de réseaux plusieurs failles ont été détectées.

Chapitre 2

La sécurité Wi-Fi

Sommaire :

2.1 Introduction ;
2.2 Les caractéristiques des réseaux sans fil et leur impact sur la sécurité ;
2.3 Les attaques contre les réseaux sans fil ;
2.4 Sécuriser le Wi-Fi ;
2.5 Conclusion ;

2.1 Introduction :

La sécurité informatique est considérée comme l'un des critères les plus importants dans le jugement de la fiabilité d'un système informatique. Cependant, les réseaux sans fil ne satisfaits pas cette contrainte, ce qui fait d'eux une cible intéressante pour les pirates. Les organisations déploient aujourd'hui la technologie sans fil à un rythme soutenu, souvent sans tenir compte de la fiabilité et leur niveau de sécurité[6].

Dans ce chapitre nous allons évoquer les différentes attaques contre les réseaux sans fil et présenter les solutions qui permettent d'augmenter la sécurité pour ce mode de connexion.

2.2 Les caractéristiques des réseaux sans fil et leur impact sur la sécurité :

Les principales caractéristiques des réseaux sans fil sont :

2.2.1 *La transmission par ondes électromagnétique :*

Les réseaux sans fil ont la particularité d'utiliser les ondes électromagnétiques pour les transmissions des données. Ce type de transmission à la propriété de se propager dans toutes les directions et sur une grande superficie. Il est donc très difficile d'envisager une limite absolue au réseau, et sa frontière n'est pas observable.

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé[6].

Cette technologie (sans fil) est donc, une porte ouverte à l'écoute et permet à un malveillant de profiter de la connexion (si le réseau de l'entreprise est connecté à un réseau Internet), et sera même possible d'insérer du trafic illégal et de s'introduire dans le réseau pour produire des actions malintentionnées.

2.2.2 *Caractéristiques des implémentations :*

Les identificateurs de réseau et les clés de chiffrement sont généralement stockés dans un fichier sur le disque de la machine ou sur Windows dans la base de registre comme avec **Agere**, ou, plus rarement, sur la carte elle-même comme **Cisco**. Le vol de l'ordinateur ou de la carte sans fil, entraîne alors le risque du vol de la clé[14] .

2.2.3 *Le brouillage radio :*

Toujours, à cause de l'utilisation des ondes radio comme support de communication qui sont très sensibles aux interférences, un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes, par exemple, peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

2.2.4 *L'utilisation de batteries :*

L'un des grands problèmes de la norme Wi-Fi est la sur consommation d'énergie, voir plus que celle de l'usage du téléphone, sachant que la batterie est leur seul moyen d'alimentation énergétique puisque les machines sont mobiles. En conséquence, la principale attaque est le déni de service sur la batterie de l'équipement, en effet, un pirate peut envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surchargée.

2.3 Les attaques contre les réseaux sans fil :

Les principales attaques contre les réseaux sans fil sont :

2.3.1 *Le déni de service :*

(denial of services (DoS)), apparaissent comme les attaques les plus faciles à réaliser par un attaquant. La criticité de telles attaques dépend fortement du contexte d'utilisation mais n'est jamais complètement négligeable .Les modèles de dénis de services qui suivent se dégagent plus particulièrement dans le cas de réseau sans fil ad hoc :

- Brouillage du canal radio pour empêcher toute communication.

- Tentative de débordement des tables de routages des nœuds servant de relais.
- Non-coopération d'un nœud au bon fonctionnement du réseau dans le but de préserver son énergie. L'égoïsme d'un nœud est une notion propre aux réseaux ad hoc. Un réseau ad hoc s'appuie sur la collaboration sans condition de ses éléments. Un nœud refusant de jouer le jeu peut mettre en péril l'ensemble.
- Tentative de gaspillage de l'énergie de nœuds ayant une autonomie de batterie faible ou cherchant à rester autonome (sans recharge) le plus longtemps possible. Ces nœuds se caractérisent par leur propension à passer en mode veille le plus souvent possible. L'attaque consiste à faire en sorte que le nœud soit obligé de rester en état d'activité et ainsi de lui faire consommer toute son énergie. Cette attaque est référencée par Ross Anderson et Franck Stajano sous l'appellation **" sleep deprivation torture attack"**, un scénario de torture par privation du sommeil.
- Dispersion et suppression du trafic en jouant sur les mécanismes de routage [15].

2.3.2 *Le reniflement:*

C'est l'attaque la plus classique. Par définition, un réseau sans fil est ouvert, c'est-à dire non sécurisé. Cette attaque consiste à écouter les transmissions des différents utilisateurs du réseau sans fil, et de récupérer n'importe qu'elles données transitant sur le réseau si celles-ci ne sont pas cryptées. Il s'agit d'une attaque sur la confidentialité[15].

Pour un particulier la menace est faible car les données sont rarement confidentielles. En revanche, dans le cas d'un réseau d'entreprise, l'enjeu stratégique peut être très important.

2.3.3 *Le guerre conduit (Utilisation non autorisée):*

Elle consiste à circuler dans des zones urbaines avec un équipement d'analyse Wi-Fi à la recherche des réseaux sans fils « ouverts ». Il existe des logiciels spécialisés permettant de détecter des réseaux Wi-Fi et de les localiser géographiquement en exploitant un GPS **(**Global Positioning System**)**. L'ensemble des informations, relative au réseau découvert, est mis en commun sur des sites Internet dédiés au recensement. On y trouve généralement une cartographie des réseaux à laquelle sont

associées les informations techniques nécessaires à la connexion, y compris le nom du réseau SSID et éventuellement la clé WEP de cryptage [15].

2.3.4 Le farinage guerre:

Le farinage de guerre est fondé sur le même principe que celui décrit ci-avant. La différence est que, plutôt que de recenser les informations sur des sites Internet, ses dernières sont simplement mises en palace sur les lieux mêmes. Son but est de rendre visible les réseaux sans fils en dessinant à même sur le trottoir ou sur les murs de bâtiments des symboles à la craie indiquant la présence d'un réseau sans fil [15].

2.3.5 L' usurpation:

L'usurpation consiste à usurper soit l'adresse IP, soit l'adresse MAC d'une autre machine. En modifiant l'adresse IP source dans l'entête du paquet, le récepteur croira avoir reçu un paquet de cette machine. Si le serveur considérait cette machine comme une machine de confiance, beaucoup de données sensibles pourront être consultées, modifiées, voir même supprimées [15].

2.4 Sécuriser le Wi-Fi :

La sécurité est le point crucial dans les réseaux sans fil, et cela à cause de leurs caractéristiques décrites précédemment. Néanmoins, il est possible de sécuriser un réseau de façon plus ou moins forte, selon les objectifs de sécurité.

La sécurité informatique totale n'existe pas, il faut plus modestement parler de niveau de sécurité. Avec la technologie Wi-Fi, le niveau de sécurité par défaut est en général très bas .Il est donc nécessaire de l'augmenter dès l'installation[15].

La sécurité dans les réseaux sans fil repose sur trois éléments essentiels :

- ***Confidentialité :***

Pour permettre la confidentialité, il faut évidemment crypter les données échangées dans le réseau et cela doit respecter deux propriétés essentielles :

- Etre facile et rapide à utiliser.
- Etre difficile a cassé.

➢ *Authentification :*

L'authentification est un élément important dans la sécurité d'un système d'information. Elle permet d'authentifier toute station voulant s'associer à un réseau. C'est donc une étape nécessaire et très sensible. Si l'authentification n'est pas assurée, l'accès aux données sera plus facile pour les attaquants, ainsi que leurs modifications éventuelles [15].

➢ *L'intégrité :*

Le standard IEEE 802.11 définit un mécanisme sommaire d'intégrité des trames basé sur le CRC. Cette valeur est appelée ICV (Integrity Check Value) et est de longueur 4 octets. Les propriétés du CRC sont telles que le niveau de sécurité atteint est très faible. Il est ainsi possible pour un utilisateur mal intentionné de modifier une trame tout en mettant à jour le CRC afin de créer une trame modifiée valide.

Elle permet de savoir si les données envoyées n'ont pas été altérées pendant la transmission [15].

Avant de sécuriser un réseau sans fil, il faut d'abord prendre en considération quelques services de base :

- **Une infrastructure adaptée :**

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir et de configurer leur puissance de manière à limiter la propagation du signal dans des zones publiques. Le contrôle du réseau dans sa globalité permettra également de détecter les déploiements pirates [15].

- **Eviter les valeurs par défaut :**

Les configurations par défaut des équipements Wi -Fi sont d'une manière générale très peu sécurisées et dont les pirates peuvent avoir accès plus facile- ment. Le changement de cette configuration est l'une des étapes essentielles dans la sécurisation d'un réseau sans fil. Pour cela il est nécessaire de :

- Changer les mots de passe administrateurs : Les mots de passe par défaut des points d'accès sont connus de tous, souvent, il n'y en a même pas. Il faut le

modifier dès que le point d'accès est sous tension par un mot de passe plus fort. Bien entendu, le choix du mot de passe doit respecter les règles élémentaires de sécurité, c'est-à-dire au moins huit caractères de type alphanumérique et il ne doit pas être issu d'un dictionnaire (car c'est plus facile à deviner) [15].

- Changer le nom du réseau (SSID) : Tout réseau Wi-Fi a un nom (le SSID), changer et cacher ce dernier à la vue des utilisateurs malintentionnés est une bonne pratique, et cela se fait comme suit :

  - Eviter l'utilisation d'un SSID trop simple.
  - Désactiver la diffusion automatique «broadcast» du nom SSID du réseau sans fil en cochant la case du type «disable SSID», pour qu'il n'apparaisse pas dans la liste des connexions possibles [16].

- **Le filtrage des adresses MAC :**

Chaque équipement informatique possède une adresse physique qui lui est propre, appelée adresse MAC (Media Access Control). C'est un identifiant matériel unique inscrit dans chaque carte réseau. Contrairement à une adresse IP qui peut changer, l'adresse MAC est définie une fois pour toute en usine par le fabricant de la carte. Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. (Ex: 44-6F-D5-00-A1) [16].

Le filtrage par adresse MAC est une fonctionnalité de sécurité que l'on trouve dans certains points d'accès, elle est basée sur la technique **ACL** (Access Control List), elle consiste à utiliser des listes d'accès. En effet, chaque point d'accès dispose d'une liste où sont inscrites toutes les adresses MAC des stations mobiles autorisées à l'accès. Le point d'accès procède alors à un filtrage sur la base des adresses MAC répertoriées. Chaque liste doit être continuellement mise à jour, manuellement ou par un logiciel spécialisé, afin d'ajouter ou de supprimer des utilisateurs [16].

Cette précaution, un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines, mais il ne faut pas compter dessus pour arrêter un pirate déterminer. Il existe, bien évidemment, des techniques permettant d'usurper une adresse MAC et ainsi de pouvoir se connecter au point d'accès. Elle est aussi, assis difficile à mettre en oeuvre pour les réseaux d'une grandes tailles où

l'administrateur doit au minimum saisir toutes les adresses MAC autorisées dans un fichier de référence [16].

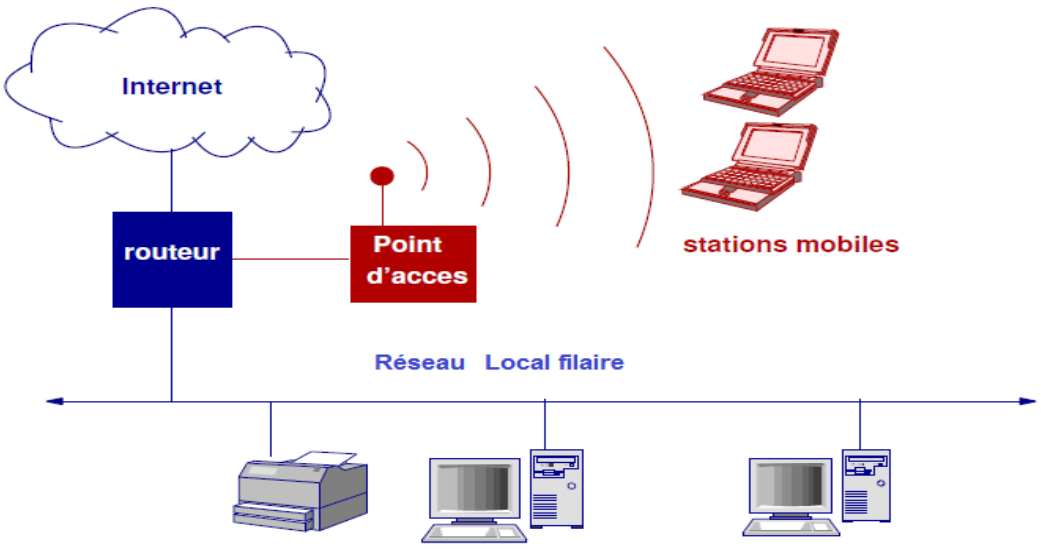


Fig 2.1- Architecture de Sécurisation

2.4.1 Les protocoles de sécurité :

Tous les services de sécurité cités ci-avant n'empêchent pas un utilisateur mal intentionné muni d'un matériel d'écoute performant de capter les émissions, mais elles rendent la tache plus difficile. Donc pour mieux sécuriser la 802.11, voici quelques moyens et techniques de sécurisations :

2.4.1.1 Le chiffrement WEP (Wired Equivalent Privacy) :

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fil, la norme Wi-Fi intègre un mécanisme simple de chiffrement de données (cryptage). Cette technique a pour but de sécuriser les données circulant sur le réseau en fournissant un niveau de sécurité identique au réseau filaire [16].

Le protocole **WEP** est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme RC4 (Ron's Cipher 4 développer en 1984 par Ron Rivest pour RSA Data Security), il permet de générer à partir d'une clé **k** et d'un vecteur d'initialisation **IV** une séquence pseudo-aléatoire **S** (qui a toujours la même taille que la clé dérivée), cette séquence est la clé effective du cryptage. L'opération de cryptage par un ou-exclusif (XOR) du texte en clair couplé à son CRC32 (somme de contrôle servant à vérifier l'intégrité des données) et de S [16].

Les clés utilisées dans ce protocole sont d'une longueur de 64 bits ou 128 bits (des implémentations récentes vont même jusqu'à pousser cette longueur à 232 bits). Les 24 bits de la clé servent pour le Vecteur d'Initialisation, ce qui signifie que seul 40bits ou 104 bits sont réservés pour la clé [16].

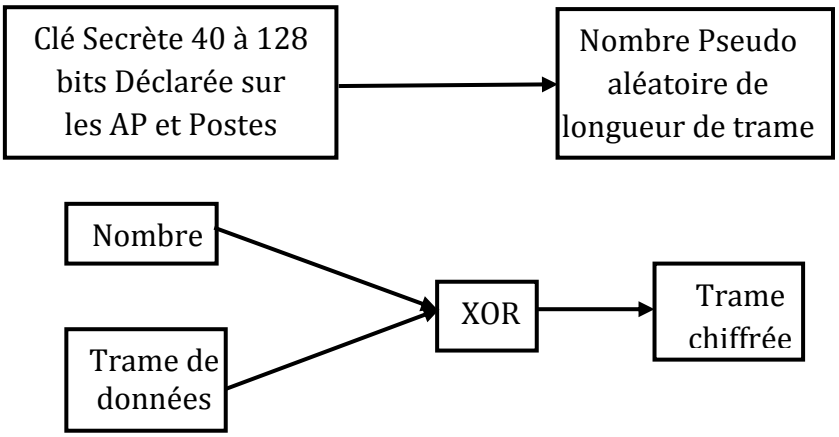


Fig 2.2- Le chiffrement WEP

Le message chiffré est alors déterminé en utilisant la formule suivante :

$$C = [\, M \,||\, \mathrm{ICV}(M) \,] \oplus [\, \mathrm{RC4}(K \,||\, \mathrm{IV}) \,] \qquad (2.1)$$

Avec:

M: le message

ICV: vérification d'integrité la valeur

RC4 : un algorithme de chiffrement

IV : un vecteur d'initialisation

K : clé secrète

- **L'authentification avec WEP :**

Après avoir identifié un AP, l'Initiateur (la station) commence par émettre une requête d'authentification (Authentication Request). Lorsque le Répondeur (le point d'accès ou la station en mode ad hoc) intercepte cette requête, il génère un texte aléatoirement par dérivation de la clé WEP qu'il connaît [16].

Ce texte qui est appelé «Challenge» est envoyé à l'Initiateur qui se charge de le crypter avec sa propre clé WEP. Il renvoie le challenge crypté au Répondeur ainsi qu'un nouveau IV.

Lorsque le Répondeur reçoit le challenge crypté, il le décrypte à l'aide de sa clé WEP et de l'IV reçu et compare le résultat obtenu au challenge d'origine. Si la comparaison aboutit à une similarité totale, l'Initiateur est authentifié, sinon il ne l'est pas.

Quand une station cliente tente de communiquer avec un réseau qui utiliserait une autre clé, la communication est ignorée. Il est donc indispensable d'avoir une homogénéité parfaite des paramètres WEP sur l'ensemble du réseau. C'est-à-dire que la même clé WEP doit être configurée à la fois sur l'ensemble des points d'accès et l'ensemble des stations mobiles qui souhaitent se connecter au réseau. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications. Ce mécanisme est montré sur la figure suivante[16] :

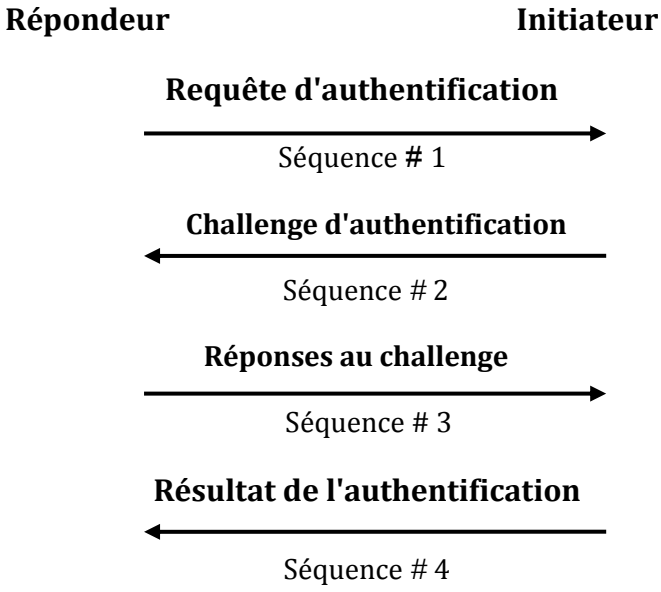


Fig 2.3 -Echanges pour l'authentification dans WEP

- **Les limites et faiblesses du WEP :**

Comme on vient de le voir, le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données, et cela à cause de :

a) La clé du cryptage est statique :

À force d'être utilisée, elle finit donc par être détectée à partir des données échangées. Si elle était modifiée au cours des échanges, le pirate aurait beaucoup plus de mal à forcer le système, car il faudrait qu'il soit en mesure de décrypter toutes les clés [16].

b) La clé est sur cinq caractères (40 bits) :

Le choix des combinaisons est donc très limité (du RC4 40 bits a été cassé en 3 heures avec un réseau de calcul distribué en 1997). C'est pourquoi il est conseillé d'utiliser une clé de 128 bits[16].

- L'algorithme de chiffrement RC4 présente des clés faibles et l'espace disponible pour les IV est trop petit (24 bits).

- Selon les équipements 802.11, la clé WEP est rentrée soit en binaire, hexadécimal ou en ASCII, cela pose bien évidemment des problèmes sur un réseau 802.11 hétérogène [17].

- **Failles :**

Des failles ont été signalées dans le WEP, en juillet 2001, Fluhrer , Mantin et Shamir ont publié une attaque pragmatique contre le vecteur d'initialisation de RC4 tel que spécifié dans WEP : " Weaknesses in the Key Scheduling Algorithm of RC4".

En juillet 2001, d'autres analystes cryptographiques de l'université du Maryland et de Cisco Systems, ont signalé des faiblesses et des failles dans les dispositifs d'authentification et de cryptage WEP de la norme WLAN IEEE 802.11, vous trouverez l'article de l'université du Maryland à l'adresse[17] .

2.4.1.2 Le WPA (Wireless Protected Access):

Le WPA est une amélioration de l'algorithme WEP et de l'authentification des réseaux 802.11. Développé par l'IEEE pour combler les faiblesses du WEP, le WPA offre une sécurité nettement supérieure par rapport au WEP grâce à :

- **Des techniques de cryptage plus aléatoires :** Dans WPA, contrairement au WEP, le caractère aléatoire du cryptage est nettement renforcé, ce qui a pour effet de nettement compliquer la tache du pirate [18].

- **Une grande facilité d'utilisation :** Avec le WPA, l'utilisateur n'aura pas de problème concernant la représentation de la clé qui doit être une fois en hexadécimal, une autre en ASCII. Ici, il ne faut utiliser qu'un simple mot de passe[18].

2.4.2 Les extensions de sécurité :

Face aux attaques et défaillances totales des mécanismes de sécurité dans les réseaux 802.11 décrites ci-avant, la recherche de solutions immédiates a été nécessaire. Pour répondre à ce manque de sécurité, deux groupes de travail se sont formés au sein de l'IEEE, le premier est le 802.1x qui est destiné assurer la sécurisation des accès au réseau, tandis que le second qui est le 802.11 i se base sur un protocole de chiffrement de données et la gestion des clés [16].

2.4.2.1 La 802.1x :

Le standard 802.1x normalisé par l'IEEE pour sécuriser des transmissions à base de Wi-Fi se décline en deux sous parties importantes. La première concerne la gestion et la création dynamique des clés, quant à la seconde elle permet de mettre en place des procédures d'authentification des clients[16].

Au-dessus de la couche MAC IEEE se trouvent la couche 802.1x et la couche AA (Authentification Agent). C'est cette couche qui contient le mécanisme véritable du protocole d'authentification [16].

Une architecture incorporant la norme 802.1x à la norme 802.11 est illustrée sur la figure 2.4:

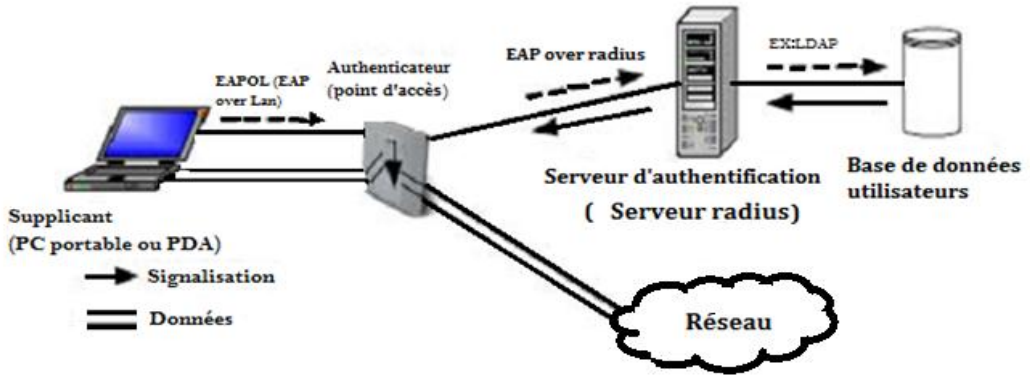


Fig 2.4- Architecture la norme 802.1x

Plusieurs éléments sont concernés dans l'architecture de l'authentification :

- Supplicant (Client) :

Elément s'insérant sur le réseau et demandant l'accès au réseau.

- Authentificator (Contrôleur qui correspond au point d'accès):

Elément permettant le relais des informations spécifiques à l'authentification vers le contrôleur. Son rôle est d'effectuer le contrôle des trames transitant sur un port particulier [16].

- Authentification server (Serveur d'authentification):

C'est la partie qui valide le supplicant au réseau, elle utilise le protocole **EAP** (Extensibl Authentification Protocol) qui gère le transport des informations relatives à l'authentification [16].

- **Principe de fonctionnement de 802.1x :**

Lors de la détection d'un nouveau client (suppliquant), le port sur le commutateur (authentificator) sera permis et placer à l'état **«non autorisé»**. Dans cet état, on permettra seulement le trafic 802.1x ; l'autre trafic, tel que DHCP et http (Hyper Text Transfer Protocol), sera bloqué à la couche liaison de données.

L'authentificator enverra EAP-Demander l'identité au suppliquant, se dernier envoie alors le paquet EAP-Réponse que l'authentificator expédiera au serveur de l'authentification (Authentificator Server) qui peut, accepter ou rejeter EAP-Demander ; dans le premier cas, l'authentificator placera le port au mode **«autorisé»** et le trafic normal sera permis, sinon le port sera toujours dans l'état **«non autorisé»** [16]**.**

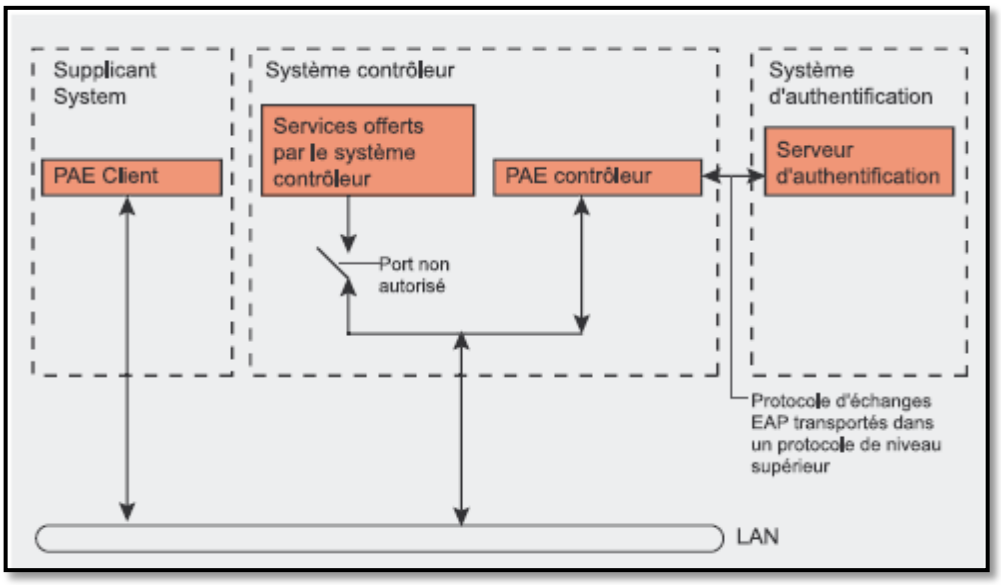


Fig 2.5-Principe de fonctionnement de 802.1x

Quand le suppliquant veut se déconnecter, il enverra un message EAP-Fermeture de session à l'authentificator qui placera ainsi le port à l'état **«non autorisé»**, bloquant de nouveau tout le trafic **non-EAP**. Ce fonctionnement est illustré sur la figure:

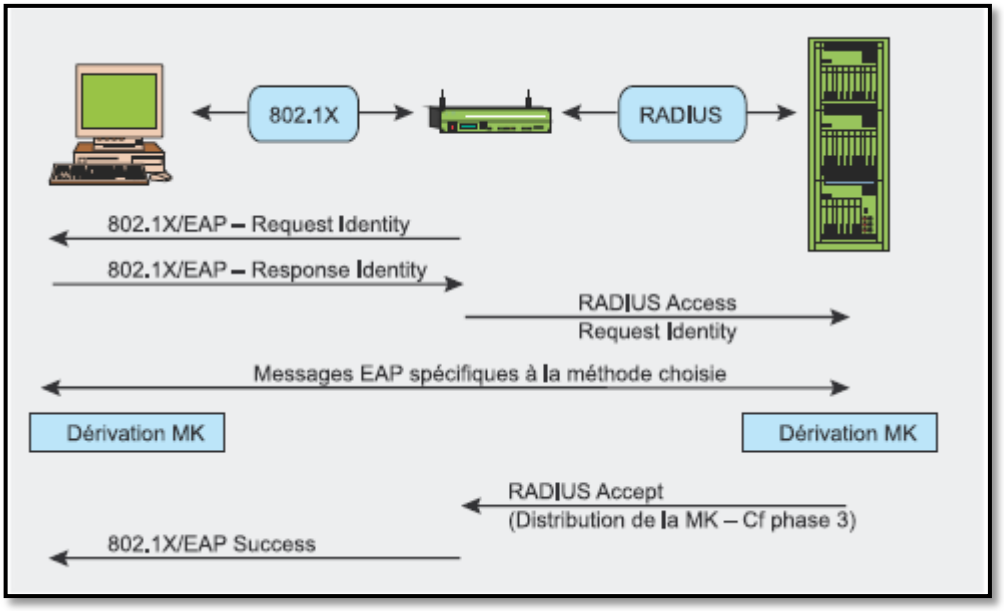


Fig 2.6- Le mécanisme d'authentification de 802.1x

La mise en place de l'IEEE 802.1x dans une architecture réseau n'est pas très simple, mais cela constitue une alternative intéressante à la faiblesse du cryptage WEP. Sur un réseau local, la mise en oeuvre de 802.1x doit s'effectuer sur tous les équipements actifs du réseau.

En effet, bien que la norme prévoie l'utilisation en mode multipoint (plusieurs suppliquant pour un seul authentificator) ce mode est à éviter, il est sujet des attaques de type «Déni de service» [16].

- **Faille :**

A l'université de Californie à Berkeley, deux chercheurs ont démontrés, que l'authentification de l'utilisation à l'aide du 802. 1x présentait deux gros problèmes (`man in the middle' et `session hijacking') et n'est donc pas quelques choses de sûr[16].

2.4.2.2 La norme 802.11i (WPA2) :

Le **WECA** a annoncé l'inclusion d'IEEE 802.11i dans sa certification Wi-Fi dès 2003 .Les débits théoriques atteignent toujours 11 Mbps pour la 802.11b et 54 Mbps pour la 802.11g.

Le rôle de ce groupe est de définir des mécanismes supplémentaires pour améliorer la sécurité d'un système 802.11[18].

Le groupe IEEE 802.11i travaille dans les directions suivantes :

- Intégration du standard IEEE 802.1x , permettant de gérer l'authentification et l'échange de clé dans un réseau 802.11.
- Utilisation d'un nouveau protocole de gestion des clés, le **TKIP** (Temporel Key Integrity Protocol) destiné a amélioré l'authentification paquet par paquet. Ce protocole génère et distribue des clés WEP dynamiques, qui utilisent un vecteur d'initialisation de 48 bits au lieu de 24 bits du WEP.
- Utilisation dans la norme IEEE 802.11 d'un nouvel algorithme de cryptage AES (Advanced Encryption Standard) pour lutter contre les faiblesses de RC4. c'est un algorithme de chiffrement de type symétrique. L'inconvénient de cette approche est le manque de compatibilité avec les équipements existants.

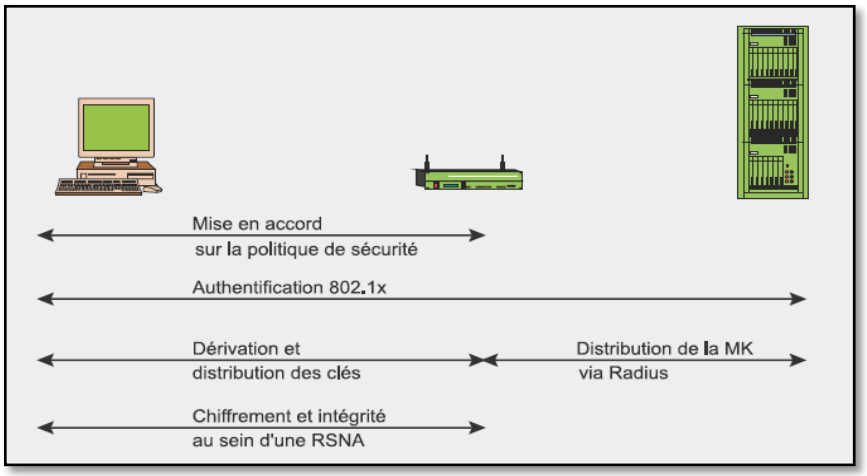


Fig 2.7- Les phases opérationnelles du 802.11i

L'extension IEEE 802.11i permet d'utiliser des clés dynamiques par station ou même par session. Le WPA est un sous-ensemble de la norme 802.11i qui vise à pallier les failles de sécurité du WEP. Son fonctionnement repose sur un système d'échange de clés dynamiques, renouvelées tous les 10 kilo-octets de données. Ce

procédé, appelé TKIP génère des clés WEP dynamiques via des réauthentifications 802.1x périodiques. Le WPA a l'avantage de pouvoir être introduit dans le firmware des cartes 802.11 construites avant 2004. Cette compatibilité s'explique par le fait que le protocole TKIP utilise le même algorithme de chiffrement que le WEP [16].

2.5 Conclusion :

Malgré des problèmes de sécurité intrinsèques, les réseaux sans fil continuent à se développer. Il est donc important de bien connaître les problèmes liés à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes.

Il est également important de déterminer le niveau de sécurité souhaité afin de mettre en place une solution en adéquation avec ce choix. Nous avons vu, comment lutter contre l'écoute passive, par le chiffrement au niveau 802.11 (WEP, WPA,..) et le contrôle d'accès par l'authentification d'un nœud 802.11 (filtrage des adresses MAC, 802.1x,...).

Chapitre 3

Configuration d'un réseau Wi-Fi

Sommaire:

3.1 Introduction;

3.2 Configuration d'un réseau sans fil (avec infrastructure, sans infrastructure);

3.3 Conclusion;

3.1 Introduction :

La mise en place d'un réseau sans fil (Wireless LAN) permet de connecter les ordinateurs entre eux, sans qu'ils soient reliés par des câbles réseaux, et cela se fait par la propagation des ondes radio. Cette mise en place peut être réalisée de deux modes :en passant par un point d'accès (Access point) équipé d'une antenne Wi-Fi : mode « avec infrastructure »,en connectant directement plusieurs ordinateurs équipés en Wi-Fi entre eux : en mode « ad hoc » [20].

Dans ce qui suit, nous allons donner les différentes étapes nécessaires pour mettre en place un réseau sans fil qu'il soit en mode avec et sans infrastructure (ad hoc).

3.2 Configuration d'un réseau sans fil:

Avant de parler de la configuration, il est nécessaire de décrire le type de cartes utilisées. Chaque carte Wi-Fi est fournie à l'achat avec un pilote d'installation et un logiciel de gestion. Pour installer la carte, il faut que celle-ci soit connectée à l'ordinateur. Dans notre cas, les équipements fournis sont des cartes PCI, donc il faut que chacune soit connectée à la carte mère. Ensuite insérer le CD d'installation et suivre les instructions. Enfin, il faut redémarrer le système et voilà la carte installée [20].

3.2.1 Configuration d'un réseau avec infrastructure :

3.2.1.1 Présentation du mode d'implémentation "Infrastructure" :

Implémenter un réseau sans fil avec le mode d'implémentation "infrastructure" implique la présence d'un point d'accès. C'est sur ce dernier que chaque ordinateur client se connectera via une liaison sans fil voir la figure 3.1 [21].

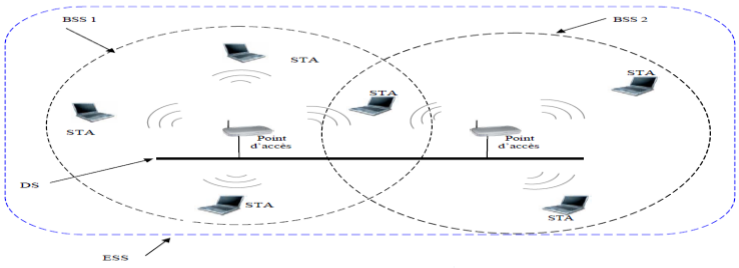


Fig 3.1 -Réseau sans fil avec infrastructure

3.2.1.2 Schéma du réseau :

Parmi notre ensemble de matériel on a choisi les équipements suivants :

- 7 ordinateurs fixes de marque HP. Leurs systèmes d'exploitation est le Windows XP SP2 2002.
- 1 ordinateur portable de marque TOSHIBA avec Windows Vista Version Intégrale.
- 1 point d'accès relié au réseau Ethernet.

La disposition de nos équipements est représentée dans la figure (Fig 3.2) [22].

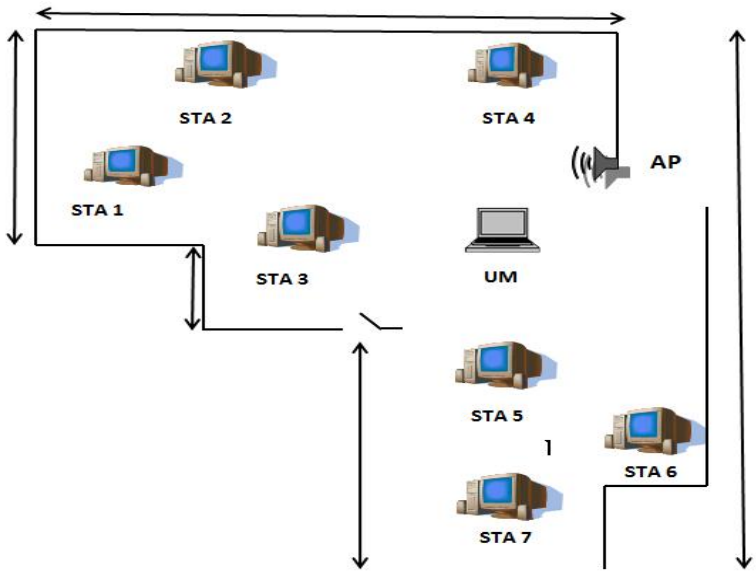


Fig 3.2- Schéma du réseau en mode infrastructure

3.2.1.3 Processus d'installation :

Avant de pouvoir mettre en réseau plusieurs machines équipées d'adaptateurs sans fil, le point d'accès doit être configuré:

3.2.1.3.1 Configuration du point d'accès :

Pour accéder à la page de configuration d'un point d'accès relié au réseau Ethernet, il faut se référer au manuel de configuration de celui-ci qui fourni l'adresse IP par défaut. (En générale, l'adresse IP fournie est 192.168.0.1) [15].

Après authentification, on accède à la page principale de configuration du point d'accès. A l'aide de celle-ci nous pouvons :

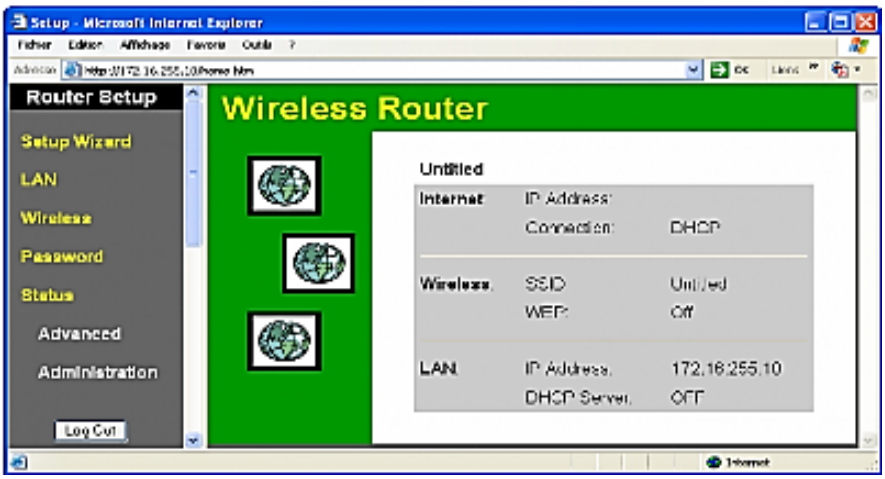


Fig 3.3 - Page d'accueil du point d'accès

- Définir le type d'adressage des machines du réseau :

Adressage dynamique : Le réseau wifi va être fonctionnel si on choisir les paramètres par défauts du point d'accès, mais il est préférable d'effectuer quelques modifications afin d'assurer une meilleure sécurité.

Adressage IP statique : On aura besoin de le sélectionner parmi les choix de la liste défilante de l'onglet « *LAN* », et de noter les données qui apparaissent(IP et DNS du serveur) pour les introduire lors de l'adressage statique des machines.

- Choisir un SSID (sec.2.4), différent de celui par défaut. Dans notre cas le SSID est «rectorat-academie » qui est fournit par défaut.
- Désactiver la diffusion par inondation du SSID. La désactivation de la diffusion par inondation du SSID se fait dans le cas d'un réseau fermer c'est-à-dire tous les utilisateurs du réseau sont défini. Mais dans le cas d'une offre de services, on opterait pour le contraire.
- Activer le service WEP de l'onglet « Wireless ».

3.2.1.3.2 Connexion au réseau sans fil :

➢ Une fois la configuration faite sur chaque ordinateur client, le réseau "infrastructure" peut être utilisé. En effet l'icône, présente dans la barre des tâches, désignée pour représenter une connexion sans fil, indique Fig 3.4.

Fig 3.4 -Icône de connexion réseau sans fil

- Effectuer un clique-droit sur l'icône de la figure (Fig 3.4) et choisir «Ouvrir les connexions réseau» et faite un clique-droit sur «Connexion réseau sans fil» et sélectionner «Propriétés».
- Puis cliquer sur l'onglet « Configuration réseau sans fil », et cliquer sur le bouton «Avancé». On voit alors apparaître la fenêtre de la figure (Fig 3.5).

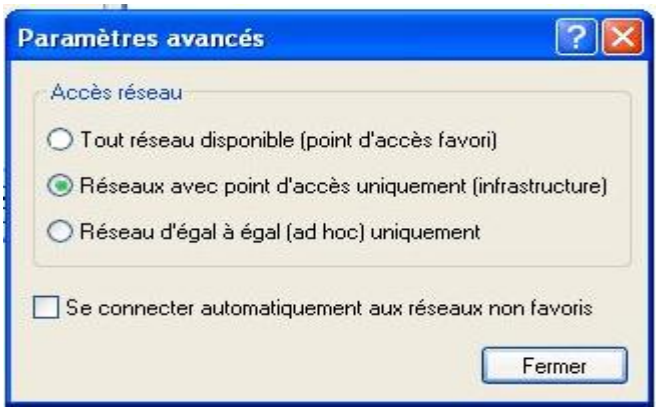


Fig 3.5- Sélectionner réseaux avec point d'accès uniquement

- Sélectionner «réseaux avec point d'accès uniquement(infrastructure) » dans les choix proposés.
- Effectuer un clique-droit sur l'icône de la figure (Fig 3.4) et choisir «*Afficher les réseaux sans fil disponibles* » pour voir apparaître la fenêtre de la figure

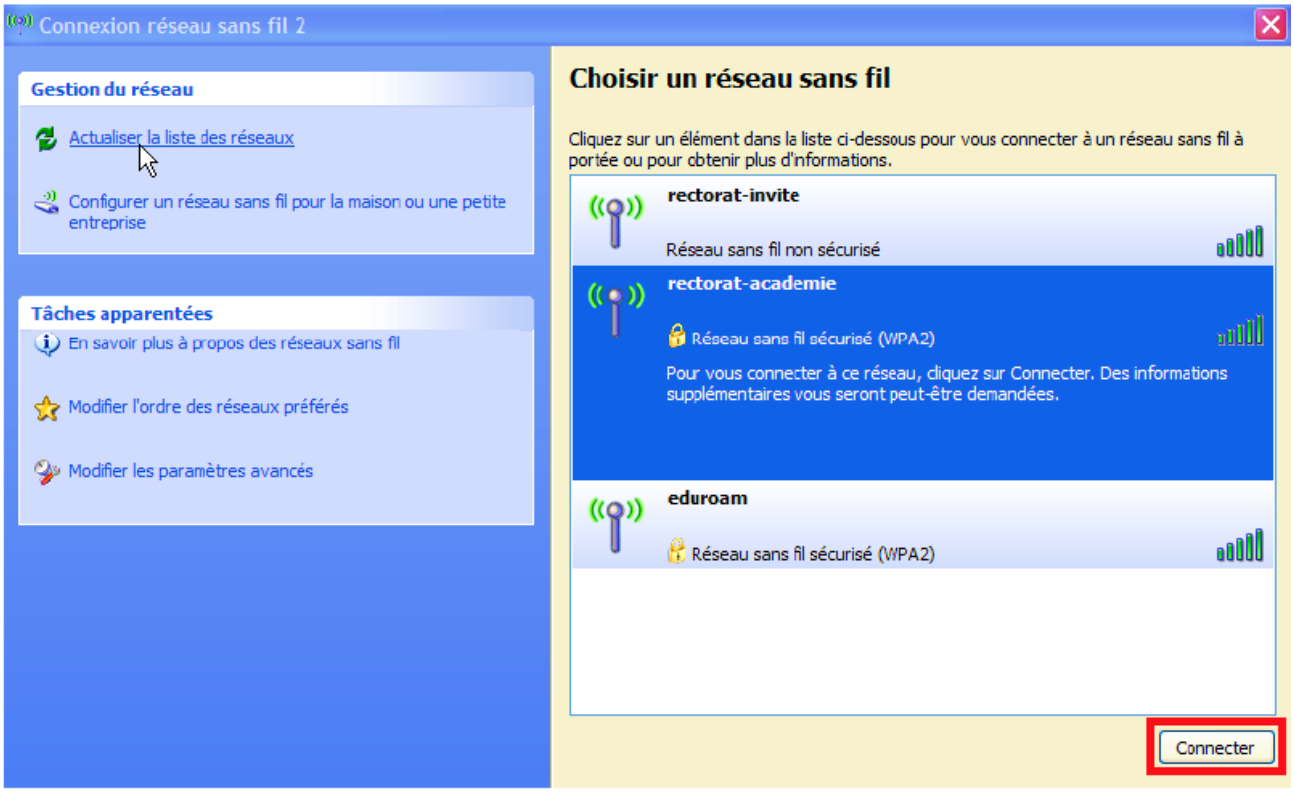


Fig 3.6 - Connexion au réseau ' rectorat-academie'

➢ Choisir dans la liste qui apparaît le réseau «rectoral-academie » et cliquer sur connecter [23].

L'icône de la figure (Fig 3.7) change de forme indiquant que la machine effectue une authentification auprès de serveur.

Fig 3.7 -Authentification auprès du serveur

Si la connexion est réussie, L'icône change de forme une deuxième fois indiquant que la machine est connectée au point d'accès (Fig 3.8).

Fig 3.8- Machine connectée

Après configuration du point d'accès et de chaque machine (Fig 3.9), on remarque que la puissance du signal au niveau de chaque machine du réseau est à « Très bonne ».

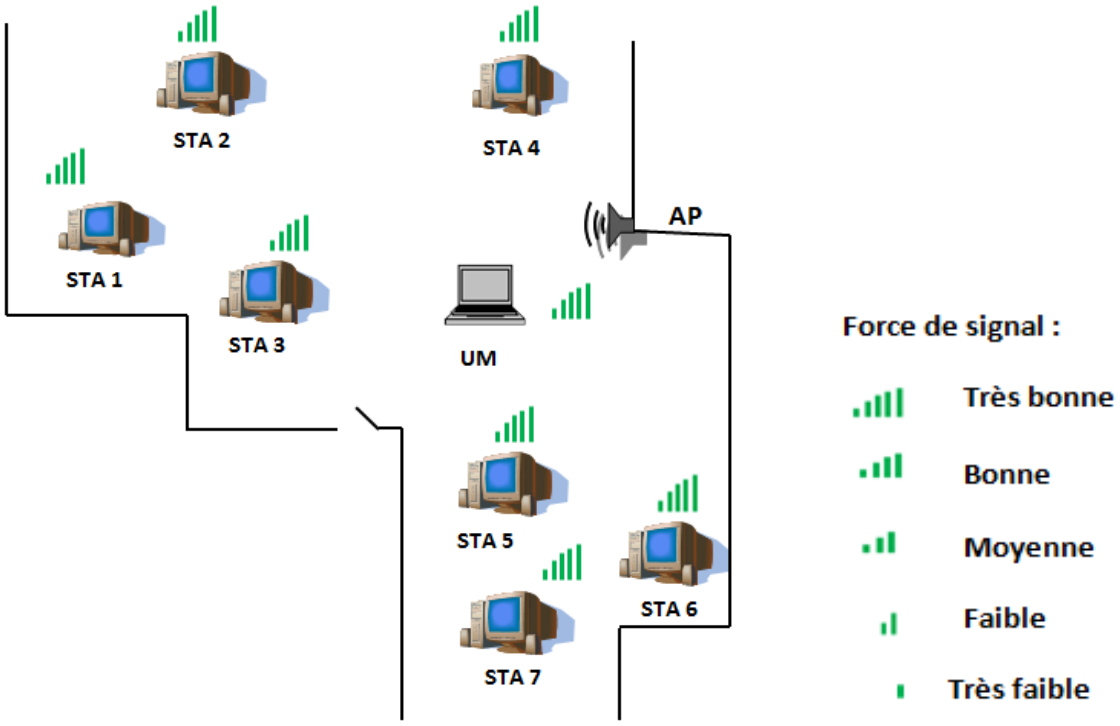


Fig 3.9- Réseau ' rectorat-academie'

3.2.2 Configuration d'un réseau sans infrastructure (ad hoc) :

3.2.2.1 Présentation du mode "Ad Hoc" :

Le mode "ad hoc" diffère du mode "infrastructure". En effet les ordinateurs ne se connectent pas à une borne d'accès, mais simplement entre eux afin d'échanger des données. Ce type d'implémentation nécessite au moins deux ordinateurs équipées en Wi -Fi. Le mode "ad hoc" permet de construire un réseau où chaque ordinateur est à la fois client et point d'accès : c'est donc un réseau point à point (peer to peer), appelé aussi d'égal à égal [21] (voir figure 3.10) :

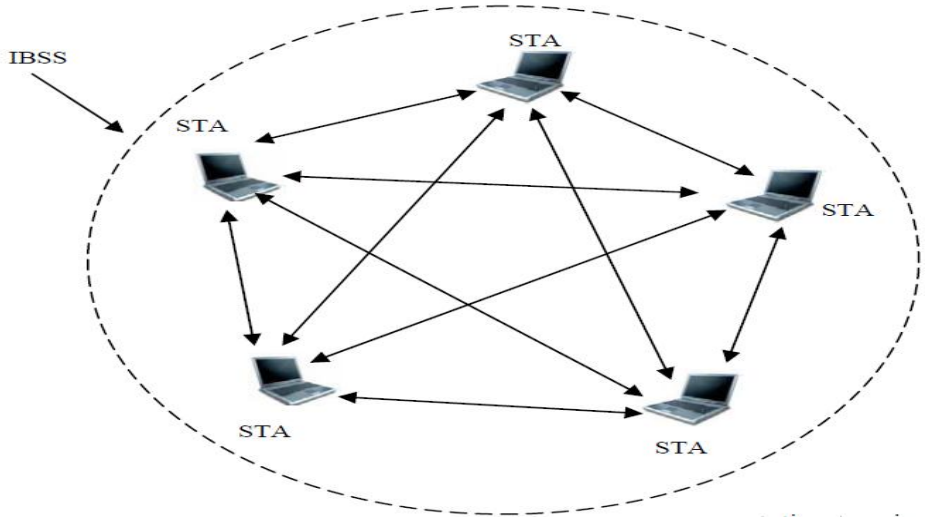


Fig 3.10 - La topologie ad hoc

Tout comme un réseau sans fil en mode "infrastructure", le réseau sans fil "ad hoc" est identifié par un nom unique : le SSID.

3.2.2.2 Configuration d'un réseau Ad Hoc sous Windows XP SP2 :

3.2.2.2.1 Schéma du réseau:

Pour créer un réseau en mode sans Ad hoc, on a choisi initialement le matériel suivant :

- 5 ordinateurs fixes. Leurs systèmes d'exploitation est le Windows XP 2.
- 1 ordinateur portable de marque TOSHIBA avec Windows Vista Version Intégrale [22].

3.2.2.2.2 Processus d'installation :

On suit les mêmes étapes que l'installation d'un réseau avec infrastructure jusqu'à l'apparition de la figure Fig 3.5 :

➢ Sélectionner « *Réseaux disponibles*» dans les choix proposés et valider le choix.

➢ Après la sélection, cliquer sur le bouton « *Ajouter* » dans la figure (Fig 3.12)

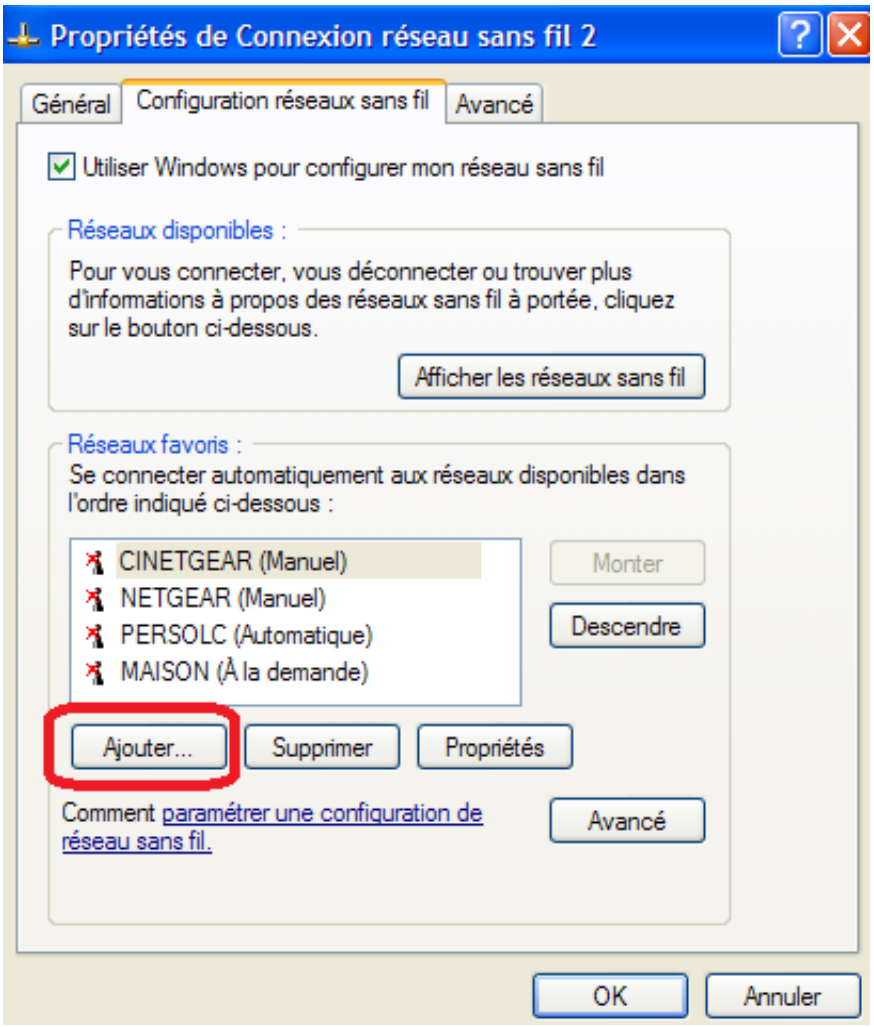


Fig 3.11- Propriétés de connexion réseau sans fil

- Dans la fenêtre qui apparaît (Fig 3.13), on effectue les modifications suivantes :

- Donner le nom « SSID » du réseau Ad hoc a créé, dans notre cas on a choisit : «NUMERICABLE-XXXX».
- Afin de sécuriser notre réseau, un mot de passe est indispensable. Pour l'associer au réseau il faut décocher la case « *La clé m'est fourni automatiquement*» en remplissant les champs «*Clé réseau*» et «*confirmez la Clé réseau* ».

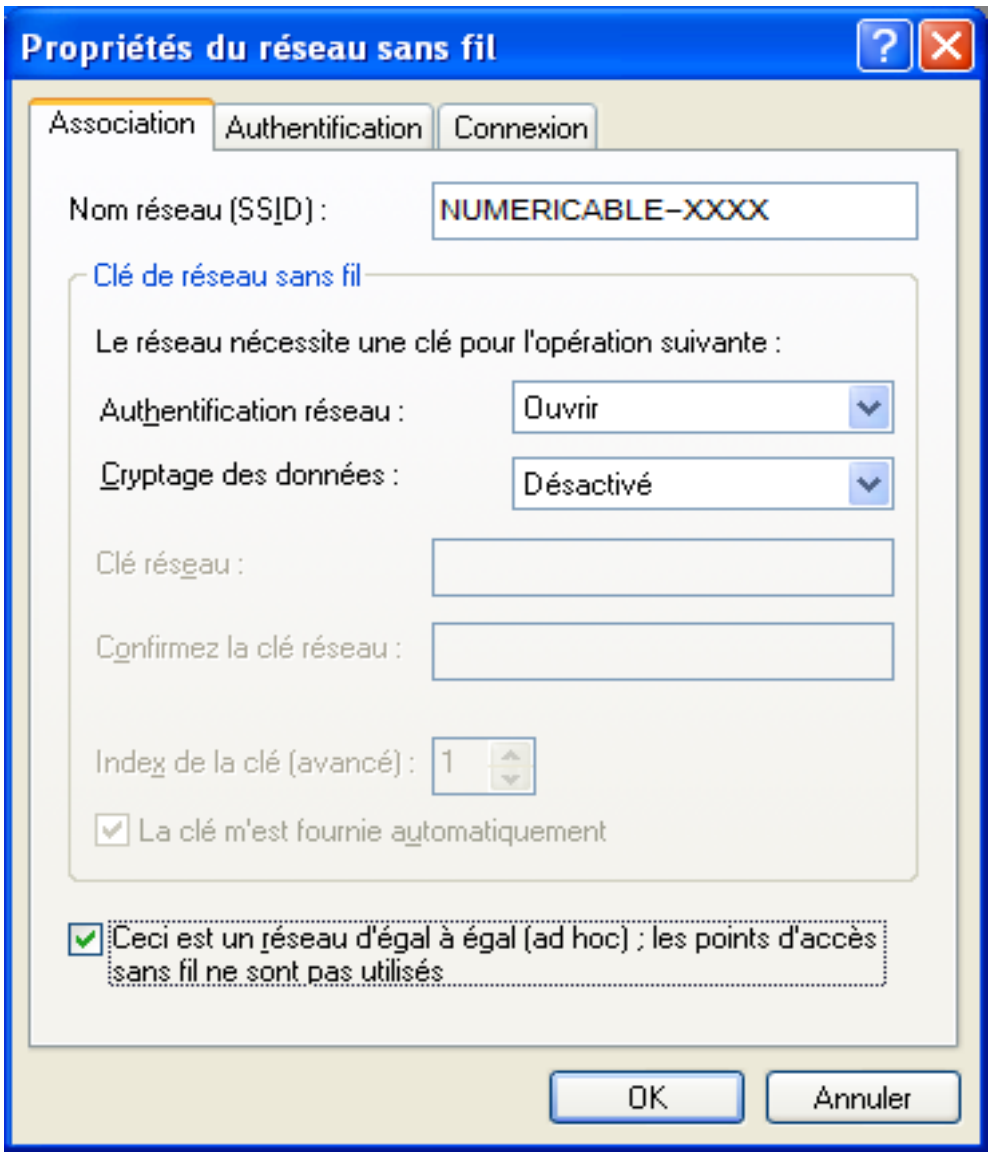


Fig 3.12- Propriété du réseau sans fil

- Il faut bien cocher la case « *Ceci est un réseau d'égale à égale (ad hoc) ; les points d'accès sans fil ne sont pas utilisés* », pour indiquer que le type de notre réseau est bien de type *Ad Hoc* [23].

A se stade, le nom « NUMERICABLE-XXXX» doit être affiché dans « *Réseaux favoris* » et notre réseau est prêt à être utilisé. Pour le mètre en œuvre, il faut au moins qu'une autre machine se connecte au réseau.

- Pour connecter une machine au réseau « NUMERICABLE-XXXX», on procède comme suit :
- Afficher les connexions réseau disponible en cliquant sur « *connexion réseau* » dans *l'explorer*, ou clique-droit sur l'icône « *Connexion au réseau sans fil* » de la zone des notifications.

- Une fois arriver à la page correspondante, on choisit « *Afficher les réseaux sans fil disponibles* » dans le menu contextuel de la « *Connexion réseau sans fil* »
- Dans la fenêtre qui apparaît on voit bien que le réseau « NUMERICABLE-XXXX» est détecté par la carte Wi-Fi de la machine, On va donc cliquer sur «*Connecter* ».

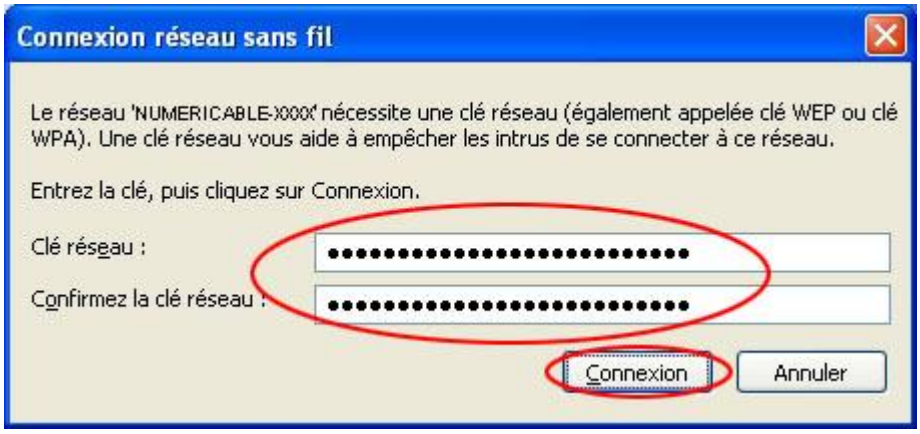


Fig 3.13- Connexion réseau sans fil

* Dans la fenêtre de dialogue qui apparaît (Fig 3.14**)**, on saisit le mot de passe attribué à ce réseau, et on clique sur « *Connexion* ».

* Le système essai alors de se connecter à «NUMERICABLE-XXXX » (Fig3.12)

Fig 3.14 -Connexion au réseau ' NUMERICABLE-XXXX '

* Une fois connectée, une page apparaît dans la barre des taches indiquant que la machine est bien connectée au réseau « NUMERICABLE-XXXX» :

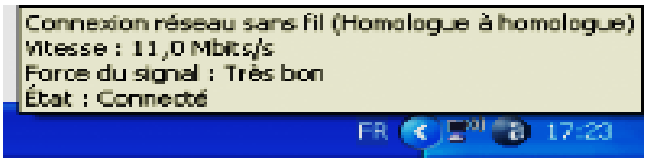


Fig 3.15- La connexion de la machine créatrice du réseau

* Au moment où la deuxième machine essai de se connecter, la première machine (créatrice du réseau) automatiquement va essayer de s'authentifier, on voit donc l'authentification à gauche de la barre des taches.

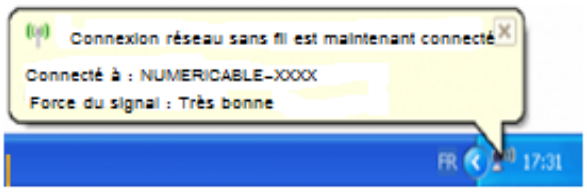


Fig 3.16 - Connexion d'autres machines

* Une fois connecté, on voit l'apparaissions d'une affiche confirmant la connexion. Maintenant, le réseau « NUMERICABLE-XXXX» est opérationnel, il suffit juste de partager sur le réseau des données, des ressources et des applications pour permettre aux autres machines connectées de les exploiter [23].

3.3 Conclusion :

Ce chapitre a fait preuve de montrer et d'expliquer la mise en place d'un réseau sans fil en deux modes existants, à savoir avec et sans infrastructure. Cette configuration nous a permet d'échanger des données entre les différentes machines connectées au réseau ('rectorat-academie' en mode infrastructure , ou 'NUMERICABLE-XXXX ' en mode ad hoc).

Conclusion Générale

Bien que les réseaux sans fil offrent beaucoup d'avantages, nous avons pu noter à travers ce présent projet qu'ils présentent aussi de sérieux inconvénients et causent souvent d'énormes difficultés de mise en œuvre.

Lors du déploiement d'un réseau sans fil, le Wi-Fi (802.11) semble être la solution répondant au mieux aux besoins des réseaux locaux sans fil grâce à l'avantage qu'elle procure, qui est son interopérabilité avec les réseaux de type Ethernet. En effet, seule les deux premières couches du modèle OSI sont définies par le Wi-Fi. Cette technologie, est fréquemment utilisée dans les entreprises désirant accueillir des utilisateurs mobiles ou souhaitant une alternative au réseau filaire tout en conservant des performances quasi identiques.

On a vu que le Wi-Fi soufrait de beaucoup de problèmes de sécurité, mais cette faiblesse a été comblée par l'intégration du WPA et de la 802.11i.

Outre l'aspect qualité de service, les réseaux Wi-Fi se doivent de remporter le défi de la mobilité sécurisée, en assurant un transfert entre cellules Wi-Fi le plus sécuritaire et le plus rapide possible .

Une fois, tous ces défis relevés, la technologie Wi-Fi sera certainement un pilier majeur pour l'établissement de l'Internet ambiant de demain, offrant sécurité, mobilité ،qualité de service et haut débit.

L'installation d'un réseau sans fil permet aussi de régler les nombreux problèmes techniques que connaissent les réseaux filaires, comme les problèmes de câblages, d'insuffisances de locaux pouvant accueillir beaucoup de machines.

Annexes

- **Couche Réseau:**

Cette couche est chargée de réaliser l'aiguillage des paquets vers les bonnes machines. C'est elle qui prend notamment en charge l'IP afin d 'assurer cette transmission. L'échelle d'action de cette couche est le paquet.

- **L'IEEE (Institute of Electrical and Electronics Engineers) :**

Organisation à but non lucrative de droit Américain, elle publie de nombreuses normes concernant les réseaux. Elle possède de nombreux groupes de travail autour des normes 802. Les normes 802 concernent les 2 couches les plus basses du modèle OSI . Les normes 802.11 définissent, elles, le fonctionnement des liaisons Wi-Fi.

- **La station** :

Il s'agit d'un élément connecté au réseau pouvant recevoir et/ou transmettre des informations sur celui-ci.

- **Le routeur (router)** :

Le routeur peut-être considéré comme un commutateur encore plus élaboré. Il réalise les fonctions du commutateur tout en ayant plus de mémoire que ce dernier et en permettant la création de sous-réseaux entre les machines y étant connectées. Il assure également un rôle de pare-feu, afin de protéger les stations se trouvant en aval dans le réseau. Il permet aussi d'exécuter des règles de redirections d'adresse au niveau IP ou de ports réseau et permet, de surcroît, une gestion des priorités dans les données transmises. C'est donc un appareil agissant au niveau 3 du modèle OSI.

- **EAP (Extensible Authentification Protocol):**

Est le protocole d'authentification conçu pour PPP (point to point protocol), le protocole d'échange utilisé dans le réseau téléphonique afin de pouvoir acheminer un trafic de trames sur des circuits commutés. EAPoL (EAP over Lan) est la variante implémentée pour l'authentification sur un réseau local comme le 802.11.

- **RSN (Robust Security Network) :**

Une nouvelle architecture de sécurité robuste passant à l'échelle et convenant parfaitement tant aux entreprises qu'aux particuliers pour les réseaux sans fil .

- **Le protocole TKIP (Temporary Key Integrity Protocol) :**

Est une amélioration apportée au protocole WEP dans la nouvelle norme 802.11i afin d'assurer une compatibilité avec les réseaux de premières génération déjà déployés de manière importante. L'objectif de TKIP est de pallier un certain nombre de failles de sécurité découvertes dans le WEP comme les attaques par rejeu et la linéarité du CRC.

- **La bande ISM(Industrial , Scientific and Medical):**

La bande ISM utilisée dans 802.11/b/g correspond à une bande de fréquence située autour de 2.4 GHz, avec une largeur de bande de 83.5 MHz (2.4 MHz – 2.4835 MHz). Cette bande ISM est reconnue par les principaux organismes de réglementation.

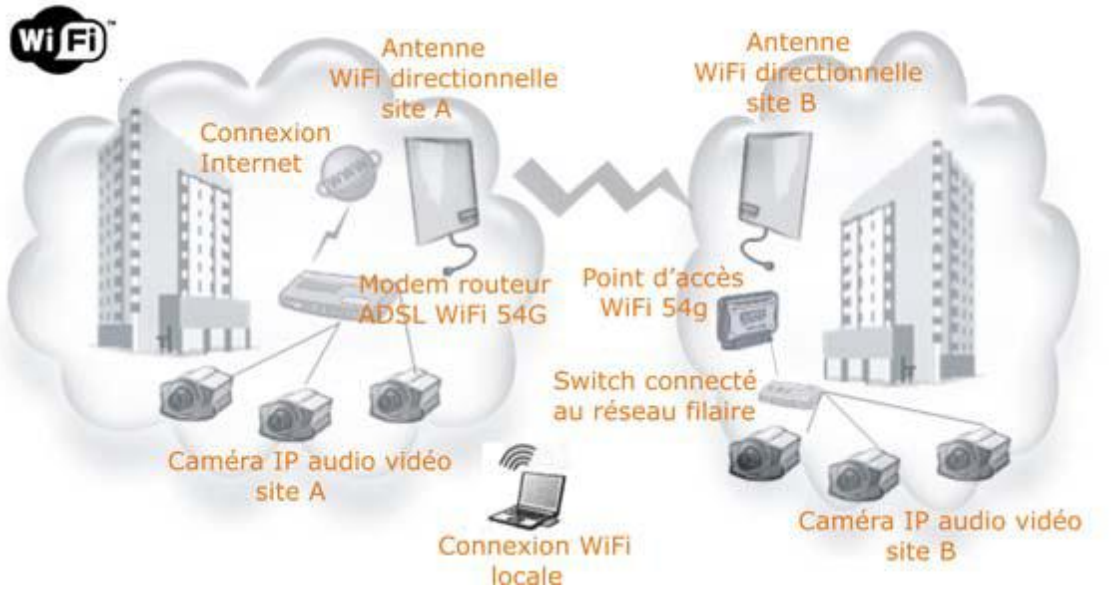
- **La bande U-NII (Unlicenced –National Information Infrastructure):**

La bande sans licence U-NII est située autour de 5 GHz. Elle offre une largeur de bande de 300 MHz (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.

- **PAE (Port Access Entity):**

Dans les réseaux sans fil, le point d'accès joue le rôle de contrôleur. Chaque port physique (port virtuel dans le cas des réseaux sans fil) est divisé en deux ports logiques c'est un PAE .

Rapport de stage



Sommaire :

1. Introduction ;
2. Rappel théorique ;
3. La pratique ;
4. Conclusion ;

1. Introduction :

Les technologies dites « sans fil », la norme 802.11 en particulier, facilitent et réduisent le coût de connexion pour les réseaux de grande taille. Avec peu de matériel et un peu d'organisation, de grandes quantités d'informations peuvent maintenant circuler sur plusieurs centaines de mètres, sans avoir recours à une compagnie de téléphone ou de câblage

De but de comprendre le câblage de materiel WiFi et leur composont ; nous faissons d'un stage dans le branche d'Algérie Télécom à DEBILA .

2. Rappel théorique :

2.1 Architectures :

Le déploiement d'un réseau Wi-Fi permet de reproduire l'ensemble des applications liées à l'utilisation d'un réseau Ethernet classique mais sans fil. Il existe deux types d'applications principales liées aux technologies radio: l'extension d'un réseau existant et le partage de ressources.

2.1.1 Étendre un réseau existant :

Des liaisons point à point de plusieurs kilomètres permettent de prolonger un réseau local ou éventuellement d'amener l'Internet haut débit là où personne ne le propose Prenons l'exemple de deux écoles distantes ,à vue ,possédant chacune un réseau informatique et désirant mettre en commun leurs réseaux.

Le Wi-Fi par le biais d'une liaison directionnelle (point à point) permet de relier les deux infrastructures .en réduisant les coûts de 10 à 100 fois par rapport à un raccordement câblé.

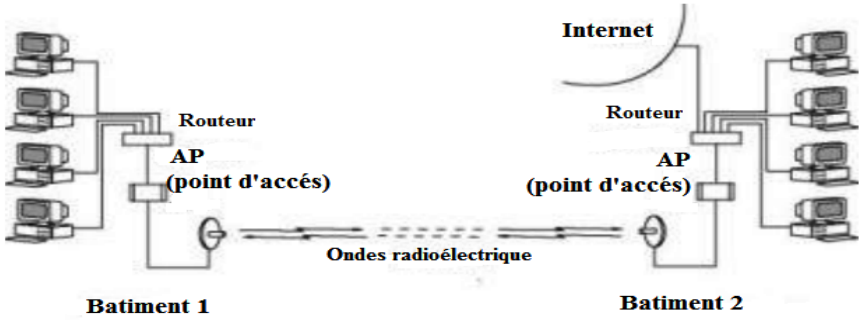


Fig 1- Liaison directionnelle entre deux réseaux locaux

2.1.2 Partager une ressource réseau :

La seconde consiste à mutualiser des éléments réseaux) fichiers , images ,films , applications ,matériel, Connexion Internet) entre plusieurs usagers.

Cinq voisins désirent par exemple de partager un accès Internet haut débit ,en toute légalité selon le contrat passé avec leur fournisseur d'accès :une liaison omnidirectionnelle Wi-Fi va permettre de Mutualiser facilement l'accès à cette ressource .Dans ce cas ,le débit de la connexion sera partagé entre les utilisateurs simultanés.

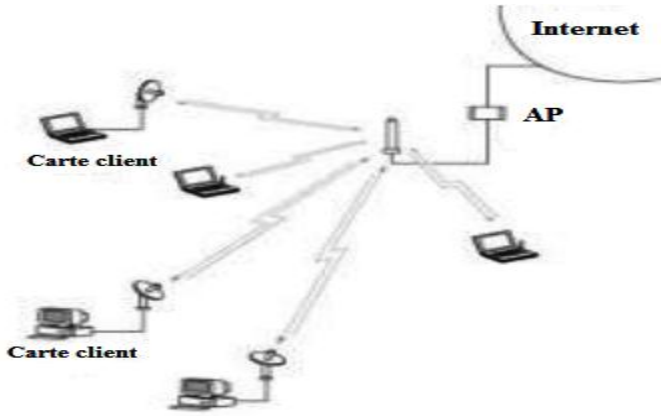


Fig 2 - Partage de ressources

N'importe quelle ressource peut être partagée de la sorte: imprimante ,scanner, serveur de données‹ permettant par exemple la mise en place d'un site contributif de données à l'échelle d'un village ou d'un quartier.

L'utilisation du Wi-Fi a permis de s'affranchir de la contrainte de câblage et de la mise en place d'un switch ou d'un hub mais aussi de réduire considérablement les délais de déploiement.

2.2 Matériel :

Une connexion Wi-Fi se présente sous la forme d'une antenne ,reliée à un périphérique actif Wi-Fi, lui-même connecté au réseau existant ou à un ordinateur. Cet élément actif assure la conversion des données (ondes radio<->données numériques) entre l'antenne et le matériel ou réseau informatique .Il peut s'agir d'un concentrateur ,nommé point d'accès ou AP ,ou de cartes clientes PCI ou PCMCIA directement insérées dans les ordinateurs.

Il n 'y pas de site d'émission et de réception en Wi-Fi: tous les éléments échangent des données de manière bidirectionnelle (en half-duplex).

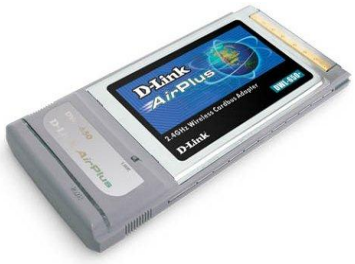
3. La pratique :

A - Les cartes Wi-Fi :

Ce terme désigne les périphériques actifs wifi/antenne directement branchés à un ordinateur client. Ils jouent exactement le même rôle que les cartes réseaux traditionnelles à la différence près qu'on ne branche pas de câble dessus, puisque la liaison est assurée par radio.

Elles existent en trois formats.

- **PCMCIA (Personal Computer Memory Card International Association) :**



Il s'agit du format le plus répandu puisque ce format est spécifique aux portables dont les propriétaires étaient les premiers intéressés par la technologie sans fil.

- **PCI (Peripheral Component Interconnect):**

C'est le format standard pour les ordinateurs de bureau mais les cartes restent au format PCMCIA. Il y a donc un adaptateur PCMCIA-PCI sur lequel est logée une carte PCMCIA ; le prix d'achat est donc légèrement supérieur aux modèles précédents.

- **USB(Universal Serial Bus):**

Ce format s'est rapidement popularisé pour sa simplicité d'utilisation et les constructeurs n'ont pas tardé à proposer également des cartes Wi-Fi à ce format.

B - Les antennes :

L'antenne intégrée à l'AP ou à la carte Wi-Fi peut être remplacée par un antenne externe plus puissante reliée par un câble d'antenne, la plupart du temps avec un parafoudre pour protéger l'appareil.

Le choix d'une antenne est important et doit être déterminé par le rôle qu'elle devra assurer, c'est à dire les interactions souhaitées avec les autres éléments Wi-Fi

distants. En fonction des caractéristiques du terrain et des zones à couvrir, il pourra par exemple être décidé de réaliser des liaisons point à point via deux antennes directionnelles ou utiliser un élément omnidirectionnel en cas de clients plus dispersés et rapprochés.

Il y a 3 grandes familles d'antennes :

B.1 Les omnidirectionnelles :

Ce type d'antenne rayonne dans toute les directions à la fois. Ce sont les modèles les plus chers car les plus complexes à réaliser. On doit les employer lorsque les stations peuvent être n'importe où par rapport à l'AP. En revanche, la distance maximale depuis l'AP reste limité en comparaison des autres antennes.

B.2 Les directionnelles :

Ces antennes ont un fort gain, c'est-à-dire qu'elles peuvent capter un signal à plus grande distance qu'une antenne omnidirectionnelle, mais dans une zone très restreinte. En général, plus le gain est fort, plus la zone couverte est rétrécie mais on peut capter le même signal depuis un point encore plus éloigné.

type parabolique **type yagi**

Fig 3 - Les antenne directionnelles

Typiquement, les antennes directionnelles sont employées pour créer des liaisons point à point, où seulement deux appareils Wi-Fi sont associés l'un à l'autre. Ce type de lien est nécessaire pour parcourir de longues distances (environ >500 m).

Pour évaluer les performances d'une antenne, on se base sur des abaques qui indique le gain en fonction de la direction.

C - Les points d'accès (AP):

Il existe ce que l'on appelle des points d'accès (composés en général d'une carte Wi-Fi et d'une antenne) qui permettent de donner un accès au réseau filaire - auquel il est raccordé - aux différentes stations avoisinantes équipées de cartes Wi-Fi. Cette sorte de concentrateur est l'élément nécessaire pour déployer un réseau centralisé (mode infrastructure).

Il y a deux types de points d'accès :

• Le point d'accès simple qui n'a qu'une fonction de lien entre le réseau filaire et le réseau sans fil .

• Le point d'accès routeur qui permet de connecter un modem ADSL Ethernet afin de partager une connexion Internet sur un réseau sans fil. Ils peuvent intégrer un concentrateur offrant de connecter d'autres appareils sur un réseau sans fil.

4. Conclusion :

La mise en place d'un réseau Wifi à l'extérieur des bâtiments et sur le domaine public n'est pas totalement interdite, mais soumise à des restrictions drastiques et à une procédure d'autorisation préalable. En revanche, à l'intérieur des bâtiments et à l'extérieur tant qu'il s'agit d'une propriété privée et tant que les émetteurs respectent des limites de puissance, vous pouvez faire ce que bon vous semble.

Bibliographie

[1] K.Al Agha. *Réseaux sans fil et mobiles*. 2004.

[2] BOUREDJI Zouhir. Le WiFi : réseau local sans fil. CERIG/EFPG. 2003

[3] D. Dominique. *Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc de la simulation à l'expérimentation*. Institut National des Sciences Appliquées de Lyon. 2003.

[4] Aurélien Géron . *WiFi professionnel : La norme 802.11, le déploiement, la sécurité*, Dunod,2009. AESTD1003v1 2009-06-04

[5] Matthew Gast. *802.11 Réseaux sans fil*. O'Reilly, 2005.

[6] Pejman Roshan, Jonathan Leary. *Réseaux WiFi : notions fondamentales*. Cysco Systems,2004.

[7] F.DI GALLO. *WiFi l'essentiel qu'il faut savoir*... 2003.

[8] H. Labiod et H. Afifi*. De Bluetooth à Wi-Fi Sécurité, qualité de service et aspects pratique*.

[9] M. Dawoud. *Analyse du protocole AODV*. Université Paul sabatier, 2006.

[10] P. Mühlethaler. *802.11 et les réseaux sans fil*. Août 2002.

[11] Davor MALES, Guy PUJOLLE .Wi-Fi par la pratique. Ed EYROLLES.

[12] Paul Muhlethaler. 802.11 et les réseaux locaux sans fil. Ed EYROLLES.

[13] J-P HAUET. *Aperçu sur les nouvelles communications sans fil et leurs applications dans l'industrie*. Novembre 2004.

[14] S. Djahel. *LE ROUTAGE OLSR ET L'ATTAQUE DE TROU NOIR : ANALYSE ET DETECTION*. Thèse de magistère, Université A/M ira de Bejaia. 2006.

[15] H. Schauer. *SECURITE DES RESEA UX SANS FIL ET 802.11B*. 8 Juillet 2002

[16] B.GUARET -DUPORT. *Les réseaux sans fil (Wi-Fi)*. Septembre 2004.

[17] L .Toinel and al l. *802.11 Les réseaux sans fil*. Nantes-wireless et Angers wireless. Mars 2003.

[18] Sean Convery, Darrin Miller et Sri Sundaralingam. *Description détaillée de la sécurité pour les réseaux locaux sans fil*. Cisco SAFE 2003

[19] P-O BOURGEOIS - Alexis MARCOU. *La sécurité dans IEEE 802.11*. Université de Nantes. 26 juillet 2004.

[20] E.CONCHON. *DÉFINITION ET MISE EN OEUVRE D'UNE SOLUTION D'EMULATION DE RESEAUX SANS FIL*. 27 Octobre 2006.

[21] J.Van der Meerschen. *Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi*. Université Libre de Bruxelles. 2006.

[22] P. AIMON, N. DUMAS, L. FALLET et S. FOUILLEUX . Wi-Fi Etude théorique &projet ROBI. Janvier 2004.

[23] H.Davis. Absolute Beginner's Guide to Wi-Fi: ® wireless Networking. 27/Avril/2004.

Résumé

La croissance continue du développement des technologies sans fil et des ordinateurs ainsi la nécessité de satisfaire les utilisateurs en leurs offrant une liberté de se déplacer tout en gardant la connectivité, promet un avenir florissant pour les systèmes WLAN en particulier les systèmes le Wi-Fi.

Ce mémoire présente la norme Wi-Fi qui est une technologie sans fil, utilisant les ondes radio qui éliminent les câbles. Pour ce faire une description de cette norme était nécessaire en citant quelques caractéristiques et notions de base.

La sécurité est aussi un objet qu'il ne faut pas négliger dans, puisqu'elle joue un rôle important dans un réseau sans fil ou le support de transmission est difficile voir impossible de contrôler. Pour cela on essayer de donner les différentes attaques contre le Wi -Fi et quelques solutions pour y remédier.

On a mis en place un réseau Wi-Fi en deux modes différents : en mode infrastructure et en mode ad hoc.

Mots clés: WLAN ,Wi-Fi, la sécurité , attaques, Infrastructure ,Ad hoc

Abstract

Continued growth in the development of wireless technology and computers and the need to satisfy the users by offering them freedom to move while maintaining connectivity promises a bright future for WLAN systems in particular Wi-Fi systems

This paper presents the Wi-Fi standard is a wireless technology, using radio waves that eliminate cables. To do this a description of this standard was necessary, citing some features and basics.

Safety is also an object that should not be overlooked in, since it plays an important role in a wireless network or the transmission medium is difficult or impossible to control. For this we try to give the various attacks against Wi-Fi and some solutions to address them.

It has set up a Wi-Fi network in two different modes: infrastructure mode and ad hoc mode.

Key words : WLAN ,Wi-Fi , the security ,attacks, Infrastructure , Ad hoc

ملخص

إنّ التقدم المستمر في تطوير التقنيات اللاسلكية وأجهزة الكمبيوتر كذلك الحاجة لإرضاء المستخدمين بمنحهم حرية التنقل مع الحفاظ على الاتصال، تبّشر بمستقبل مشرق لأنظمة الشبكات اللاسلكية WLAN و خاصة أنظمة ال Wi-Fi.

تعرض هذه المذكرة نموذج ال Wi-Fi الذي هو تقنية لاسلكية تستخدم موجات الراديو التي تستغني عن الكابلات . للقيام بوصف هذا النموذج من الضروري ان نضع له عدة خصائص ومبادئ أساسية.

الحفاظ على المعلومة هو أيضا موضوع لا ينبغي تجاهله ، لأنه يلعب دورا هاما في الشبكة اللاسلكية أو دعامة النقل التي من الصعب أو من المستحيل السيطرة عليها .لهذا نحاول أن نقدم الاستهلاكات المتعددة ضد ال Wi-Fi وبعض الحلول للتصدي لها.

تكون شبكة الWi-Fi على شكل وضعيتين مختلفين :وضعية البنية الأساسية و وضعية الأقران (بلا بنية أساسية).

الكلمات المفتاحية :الشبكات اللاسلكية ،ال Wi-Fi ، الحفاظ على المعلومة ، الإستهلاكات ، وضعية البنية الأساسية ، وضعية الأقران