MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II en Electronique

Option : Réseaux et télécommunication

Thème :
Etude et implantation d'un réseau WIFI sécurise au sein de l'INPED

Proposé et dirigé par :
Mr. Y .AIT BACHIR
Mr. N .BOUAOUNE

Présenté par :
Mr. HADIOUCHE Karim
Mr. GUIDOUM Said

Promotion 2010-2011

SOMMAIRE

INTRODUCTION GENERALE

Les entreprises étaient confrontées autrefois à de nombreux problèmes dus à la non interconnexion des ordinateurs. La mise en réseau des ordinateurs et périphériques a permis de résoudre ces problèmes en offrant des avantages tels que la possibilité de communiquer avec plusieurs utilisateurs, le partage des ressources, la facilité d'administration des différents équipements.

Le besoin de plus en plus important de mobilité, ainsi que la diversification des réseaux a poussé les organismes à normaliser les réseaux sans fil pour assurer une compatibilité entre les différents fabricants.

Le présent projet qui entre dans le cadre de la préparation d'un diplôme de master télécommunication et réseau a pour objectif l'étude de la technologie des réseaux sans fil en vue de la mise en place à un réseau sans fil de type IEEE 802.11g. Le choix de ce type de réseau est dicté par une facilité ainsi qu'une rapidité de déploiement.

Pour mener à bien notre projet nous avons d'abord procédé, dans notre premier chapitre à une brève présentation des différents types de réseaux sans fil, puis les équipements utilises dans un réseau sans fil et les modes de fonctionnement.

Le deuxième chapitre concerne l'étude de la sécurité des réseaux sans fil.

Le troisième chapitre, il est consacré à la configuration des points d'accès.

Quant au dernier chapitre est consacré à la mise en place de la plate-forme du réseau WIFI INPED.

CHAPITRE I: PRESENTATION DES RESEAUX SANS FIL

INTRODUCTION

Un réseau sans fils (en anglais wireless network) est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fils un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

Les réseaux sans fils sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

Les réseaux sans fils permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires. En contrepartie se pose le problème de la réglementation relative aux transmissions radioélectriques.

De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour un pirate d'écouter le réseau si les informations circulent en clair. Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil.

1. Présentation de l'organisme d'accueil:

1.1. Présentation de l'INPED

L'institut national de la productivité et du développement industriel (INPED), crée par ordonnance n°67/172 du 31 août 1967, a été érigé en établissement public à caractère industriel et commercial (EPIC) par le décret exécutif n°98-163 du 19 mai 1998.

Placé sous tutelle du ministère de l'industrie et de la restructuration.

Il a pour missions générales de :

Former les cadres d'entreprises et les perfectionner dans les différentes fonctions de gestion qu'il assure.

* Assister les entreprises pour apporter des solutions à leurs problèmes d'organisation et gestion.

* Réaliser des études technico-économiques ou à caractère économique et social pour le compte des institutions et organismes publics et privés

* L'INPED organise des formations de moyenne et longues durées dans les domaines de la gestion des langues d'affaires, de la finance – comptabilité, des techniques documentaires et de techniques de secrétariat. Parallèlement à ces formations documentaires et de techniques de secrétariat. l'INPED organise à l'intention et à la demande des employeurs des stages spécifiques sur le site ou en résidence à l'institut.

- Dirigé par un directeur général, l'institut est organisé en cinq (05) directions :
- Direction administration et finances (D.A.F)
- Direction des études et du perfectionnement (D.E.P)
- Direction des études du conseil et de l'assistance aux entreprises (D.E.C.A)
- Direction des ressources didactiques et de l'information (D.R.D.I)
- Direction des résidences des stagiaires (D.R.S)

1.2 -ORGANIGRAMME GENERALE DE L'I.N.P.E.D

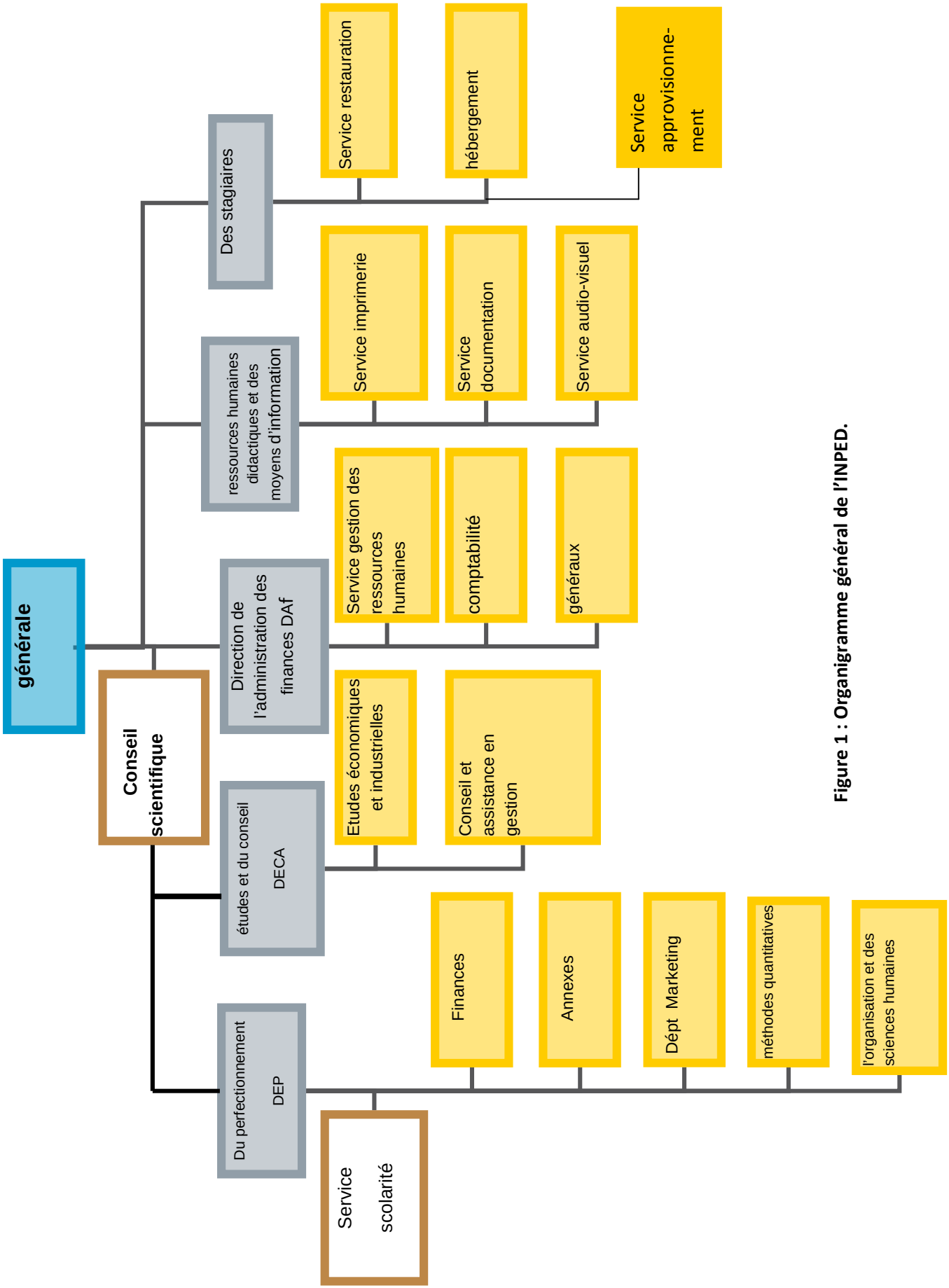


Figure 1 : Organigramme général de l'INPED.

2. Définition d'un réseau sans fil :

Un réseau sans fil ou wireless network est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire en utilisant des ondes radio-électriques.

Un réseau sans fil est un réseau informatique qui connecte différents postes (Ordinateur, laptop, PDA, Caméra wifi, etc.) entre eux par ondes radio.

Un réseau sans fil est constitué d'une station de base (BTS) avec une couverture de type Point à Point ou Point – Multipoint dit cellulaire. Ce dernier type utilisé dans la plus part des réseaux locaux permet de desservir un ensemble d'abonnés d'une zone prédéfinie. Les liaisons hertziennes de la BTS vers les abonnées sont dites voies descendantes (downstream) tandis que les voies montantes (upstream) désignent les liaisons des abonnés vers la BTS.

Afin de ravir les utilisateurs nomades, les connections sans fil ont connu un essor considérable ces trois dernières années. Destine à raccorder les périphériques mobiles aux réseaux informatiques sans passer par une connection filaire comme l'Ethernet et donc du coup priver l'utilisateur de sa mobilité, la connection sans fil est devenu le réseau incontournable pour les entreprises ; mais également le grand public. L'avantage réside dans la zone de couverture de ces réseaux. Elle peut aller a dix mètres a plusieurs kilomètres (bientôt plus de 40km pour le très controverse Wi-Max) et par l'interopérabilité des différentes normes (802.11a, 802.11b, 802.11g pour le Wi-Fi)

Commençons tout d'abord avec Wi-Fi (la norme ISO 802.11). Ce Wireless Fidelity se propage par les ondes radio sur une fréquence de 2.4Ghz. Afin de pouvoir disposer de plusieurs réseaux sur la même surface. Le Wifi permet, grâce à un routeur ou un point d'accès, de desservir une zone de couverture d'un rayon de cent metres théorique. Ceci étant, comme pour les réseaux filaires, l'atténuation du signal se détériore très vite en fonction de la distance du point d'accès, mais également en fonction du nombre et du type d'obstacles rencontrés entre le routeur et le poste client. Toutefois, il est possible d'associer plusieurs points d'accès Wifi sur le même réseau pour étendre de manière significative le signal et la qualité de la ligne radio pour le confort de l'utilisateur final.

Du cote des débits, le Wifi permet d'assurer une bande passante allant jusqu'à 54Mbps pour la norme G (le Super G de Dlink) et 11Mbps pour la norme B.

Pour les appareils légers comme les PDA ou bien encore les téléphones portables, de nombreuses applications sont venues faciliter la tache de tout le monde comme par exemple la synchronisation des contacts avec une station de travail ou bien encore le transfert d'images.

Des lors, la technologie Bluetooth est la plus souvent utilisée pour sa très faible consommation d'énergie

Figure I. 1:Composition d'un réseau wifi

3. Fonctionnement d'un réseau sans fil :

Un réseau sans fil fonctionne de manière analogue au tandem téléphone sans fil - socle que vous utilisez peut-être chez vous. Le téléphone sans fil communique avec un correspondant par l'intermédiaire du socle qui fait office de point d'accès vers le réseau téléphonique.

De même, chaque ordinateur du réseau sans fil muni d'une carte réseau adéquate peut émettre (et recevoir) des données vers (et depuis) un point d'accès réseau. Ce dernier peut être physiquement connecté au réseau câblé et fait alors office de point d'accès vers le réseau câblé.

Il existe plusieurs solutions de réseau sans fil commercialisées, chacune offrant plus ou moins de fonctionnalités suivant le constructeur (elles ont en commun - pour la plupart - le respect de la norme 802.11a, 802.11b et 802.11g qui détaille les spécifications des réseaux sans fil offrant des débits atteignant les 11Mbps ou 55Mbps).

4. Les types du réseau sans fil :

Une première distinction entre les réseaux sans fils dépend de leur champ d'action. Suivant leur portée, selon le périmètre géographique offrant une connectivité (appelé zone de couverture)

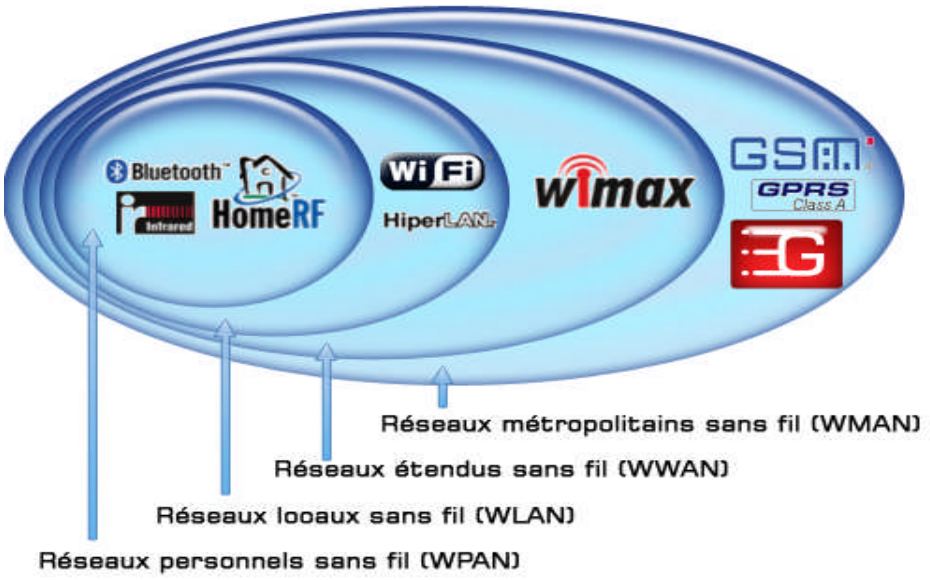


Figure I.2 : classification des réseaux sans fil

4.1. Réseaux personnels sans fil (WPAN) :

Les réseaux personnels sans fil (WPAN pour Wireless Personal Area Networks) sont de 3 types : Bluetooth, Infrarouges, ZigBee

Les réseaux personnels servent à relier différents appareils dans un rayon réduit. Aujourd'hui, le réseau personnel sans fil le plus connu est Bluetooth. Deux nouvelles technologies apparaissent l'une permettant le haut débit UWB et l'autre la connexion d'équipements très peu chers Zigbee.

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fil d'une faible portée de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, caméra sans fil...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. La principale technologie WPAN est la technologie Bluetooth, lancée par Ericsson en 1994, proposant un débit théorique de 1Mbps pour une portée maximale d'une trentaine de mètres. Bluetooth, connue aussi sous le nom IEEE 802.15.1, possède l'avantage d'être très peu gourmande en énergie, ce qui la rend particulièrement adaptée à une utilisation au sein de petits périphériques.

HomeRF (pour Home Radio Frequency), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel, a été abandonnée en Janvier 2003, notamment car les fondeurs de processeurs misent désormais sur les technologies Wi-Fi embarquée (via la technologie Centrino, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi).

La technologie ZigBee (aussi connue sous le nom IEEE 802.15.4) permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). La technologie Zigbee, opérant sur la bande de fréquences des 2,4 GHz et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ.

Enfin les liaisons infrarouges permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses. L'association IRDA (infrared data association) formée en 1995 regroupe plus de 150 membres.

4.2. Réseaux locaux sans fil (WLAN) :

Les réseaux locaux sans fil (WLAN pour Wireless Local Area Networks): Technologies WiFi, Hyperlan . La percée de Wi-Fi ces dernières années a fait connaître les réseaux sans fil. La famille Wi-Fi s'agrandit peu à peu. Dans le domaine des réseaux locaux sans fil, seul l'Hiperlan II tente de le concurrencer. Cependant la montée en puissance des réseaux personnels jusqu'à présent limités à quelques mètres, montre des velléités de briser les barrières (ce fut le cas avec les annonces de Bluetooth 2.0 ou plus récemment avec les évolutions d'UWB). A l'inverse, Wi-

Fi a été utilisé au niveau métropolitain du fait du manque jusqu'à présent de réseaux sans fil plus appropriés.

Le réseau local sans fil (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :
Le Wifi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

hiperLAN2 (HIgh Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.

4.3. Réseaux métropolitains sans fil (WMAN) :

Les réseaux métropolitains sans fil (WMAN pour Wireless Metropolitain Area Networks) sont adaptés à la couverture de villes et de villages arrivent quelques années après les réseaux locaux sans fils de type Wi-Fi. Nous pouvons distinguer trois grandes familles :

- WiMAX, bien adapté aux réseaux métropolitains fixes sans fil à très haut débit (ou par la suite faiblement mobiles).
- Les réseaux mobiles (GSM , GPRS) et la 3e génération (UMTS), bien que constituant un réseau national (pour chaque opérateur de téléphonie mobile), permettent de couvrir les villes et les village.
- MBWA qui dans quelques années pourrait permettre des réseaux mobiles à très haut débit.

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16.

La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.
La norme de réseau métropolitain sans fil la plus connue est le WiMAX permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de plusieurs kilomètres.

4.4. Réseaux sans fil à longue distance (WWAN) :

Les réseaux étendus sans fil (WWAN pour Wireless Wide Area Networks) ce sont des reseaux qui donne à l'utilisateur la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".
Le satellite permet des cellules de la taille de plusieurs pays et facilite l'accès à l'internet dans les zones rurales non accessibles avec les méthodes traditionnelles filaires et sans fil.

5. Architecture réseau WIFI:

Il existe deux modes de fonctionnement

5.1. Le mode Infrastructure :

Le mode infrastructure se base sur une station spéciale appelée Point d'Accès (PA). Ce mode permet à des stations wifi de se connecter à un réseau (généralement Ethernet) via un point d'accès. Elle permet à une station wifi de se connecter à une autre station wifi via leur PA commun. Une station wifi associée à un autre PA peut aussi s'interconnecter.

L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set). Chaque BBS est identifié par un BSSID (BSS Identifier) de 6 octets qui correspond à l'adresse MAC du PA.

Chaque ordinateur se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé ensemble de services de base BSS (basic service set).

Il est possible de relier plusieurs BSS (basic service set) par une liaison appelée système de distribution (DS,Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Le système de distribution (DS) peut être un réseau filaire, ou un câble entre deux points d'accès. Un ESS (Extended Service Set) est repéré par un ESSID (Extended Service Set Identifier), qui est un nom du réseau.

Lorsqu'un utilisateur nomade passe d'un BSS (basic service set) à un autre en se déplaçant l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux,

Cette caractéristique permet aux stations de passer de façon transparente d'un point d'accès à un autre (roaming)

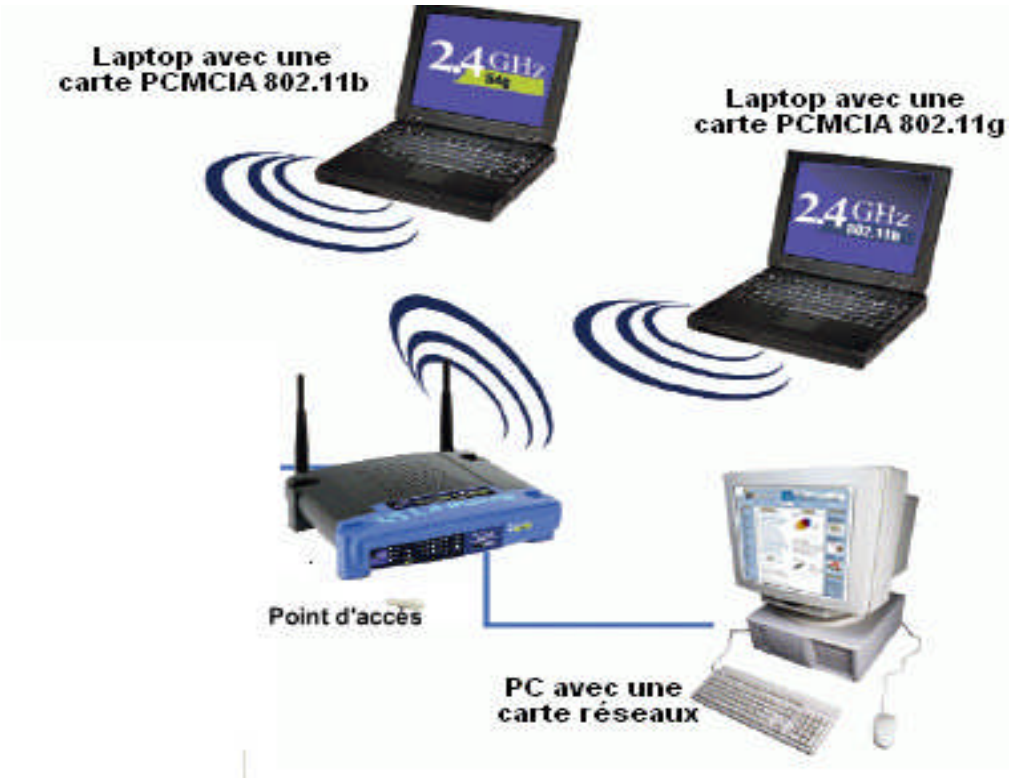


Figure I.3 : mode infrastructure

5.2.Le mode Ad-Hoc :

Le fonctionnement de ce mode est totalement distribué, il n'y a pas d'élément structurant hiérarchiquement la cellule ou permettant de transmettre les trames d'une station à une autre. Ce mode permet la communication entre deux machines sans l'aide d'une infrastructure. Les stations se trouvant à portée de radio forment un IBSS (Independant Basic Service Set).En mode ad hoc les ordinateurs sans fil clients se connectent les uns aux autres pour constituer un réseau point à point (peer to peer), c'est un réseau dans lequel chaque ordinateur est un client et un point d'accès. Cet ensemble est appelé, IBSS (indépendant basic service set).

Dans un réseau ad hoc, la portée du IBSS est déterminée par la portée de chaque station. Contrairement au mode infrastructure, le mode ad hoc ne propose pas de diffuser régulièrement une trame balise d'une station à une autre. Ainsi un IBSS est par définition comme un réseau sans fil restreint.

Figure I.4: mode Ad-Hoc

6. La norme (802.11) :

Le **WIFI** (**W**ireless **F**idelity), la norme **IEE802.11** est un standard décrivant le réseau local sans fils (**WLAN**). Avec le wifi, il est possible de mettre en place des réseaux locaux sans fils à haut débit sous réserve d'être a proximité d'un point d'accès. Le wifi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) et tous les périphériques de liaison à haut débit sur un rayon de plusieurs dizaines de mètres.

La norme **802.11** définit les couches basses du modèle **OSI** pour une liaison sans fil utilisant des ondes électromagnétiques :

La couche physique (**DSSS, FHSS, Infrarouge**), proposant trois types de codage de l'information.

La couche liaison de données, constituée de deux sous-couches, le contrôle de liaison logique (**Logical Link Control**, ou **LLC**) et le contrôle d'accès au support (**Media Access Control**, ou **MAC**).

7. Différents débits et portées :

Les normes 802.11a, 802.11b et 802.11g, appelées «normes physiques» correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents débits en fonction de la portée.

Standard	Bande de fréquence (GHZ)	Débit (Mbit/s)	Portée (m)
802.11a	5	54	10
802.11b	2.4	11	100
802.11g	2.4	54	100

- **802.11a**

La norme **802.11a** permet d'obtenir un débit théorique de **54 Mbit/s**, soit **cinq fois** plus que le **802.11b**, pour une portée d'environ une **trentaine de mètres** seulement. La norme **802.11a** s'appuie sur un **codage** du type (**O**rthogonal **F**requency **D**ivision **M**ultiplexing ; **OFDM**) sur la bande de fréquence **5 GHz** et utilisent **8 canaux** qui ne se recouvrent pas.

Débit théorique (en intérieur)	Portée (mètre)
54 Mbits/s	10 m
48 Mbits/s	17 m
36 Mbits/s	25 m
24 Mbits/s	30 m
12 Mbits/s	50 m
6 Mbits/s	70 m

- **802.11b**

La norme **802.11b** permet d'obtenir un débit théorique de **11 Mbit/s**, pour une portée d'environ une **cinquantaine** de mètres en **intérieur** et jusqu'à **200 mètres en** extérieur (et même au-delà avec des antennes directionnelles).

Débit théorique (Mbits/s)	Portée intérieure	Portée extérieure
11	50 m	200 m
5,5	75 m	300 m
2	100 m	400 m
1	150 m	500 m

Remarque: les équipements **802.11a** ne sont donc pas compatibles avec les équipements **802.11b**. Il existe toutefois des matériels intégrant des puces **802.11a** et **802.11b**, on parle alors de matériels «dual band».

- **802.11g**

La norme **802.11g** permet d'obtenir un débit théorique de **54 Mbit/s** pour des portées équivalentes à celles de la norme **802.11b**. D'autre part, dans la mesure où la norme **802.11g** utilise la bande de fréquence **2,4GHZ** avec un codage **OFDM**, cette norme est compatible avec les **matériels 802.11b**, à l'exception de certains anciens matériels.

Débit théorique (Mbits/s)	Portée intérieure	Portée (à l'extérieur)
54	27 m	75 m
48	29 m	100 m
36	30 m	120 m
24	42 m	140 m
18	55 m	180 m
12	64 m	250 m
9	75 m	350 m
6	90 m	400 m

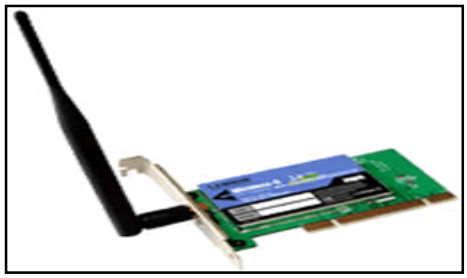
8. Les équipements de transmission :

Il existe différents types d'équipements pour la mise en place d'un réseau sans fil **WiFi** :

Les Adaptateurs Sans Fil Ou Cartes d'accès :

En anglais (Wireless Adapters) ou network interface contrôler, noté **NIC**. Il s'agit d'une carte réseau à la norme **802.11** permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs **WiF**i sont disponibles dans de nombreux formats (carte **PCI**, carte **PCMCIA**, adaptateur **USB**, carte **compact flash**,...). On appelle station tout équipement possédant une telle carte. A noter que les composants **WiFi** deviennent des standards sur les portables (**label**, **Centrino**, **d'Intel**).

La carte réseau sans fil PCI :



Dans un ordinateur de bureau, la carte est habituellement installée à l'intérieur de l'ordinateur, le plus généralement dans un des emplacements de PCI qui sont communs dans la tour ou les configurations de bureau de PC. Sur une carte sans fil, une antenne courte, environ 10cm (4 pouces) dépasse en dehors de l'ordinateur et peut être pivotée environ pour recevoir le meilleur signal.

La Carte PCMCIA :

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

Une carte sans fil connecte à un port USB :

Une troisième possibilité est de connecter la carte par l'intermédiaire d'un câble d'**USB** à l'ordinateur. Dans ce cas-ci, l'antenne sera sur la carte, qui peut être placée n'importe où que le

câble d'**USB** lui permettra, qui pourrait être jusqu'à 5 mètres partir de l'ordinateur. La carte est actionnée bien que le câble d'USB, ainsi aucune alimentation d'énergie supplémentaire ne soit exigée.

Les Points d'accès :

Notés AP pour (Access point), parfois appelés bornes sans fil, fait office de relais entre les ordinateurs portables et le réseau câblé (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes WiFi.

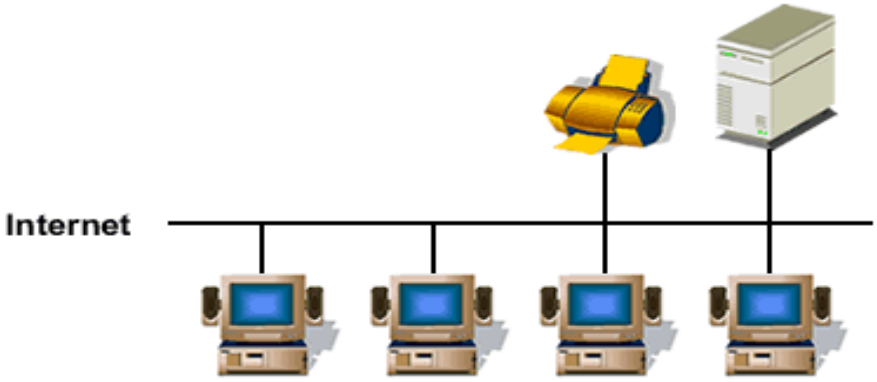


Figure I.5 : Un réseau câblé "traditionnel"

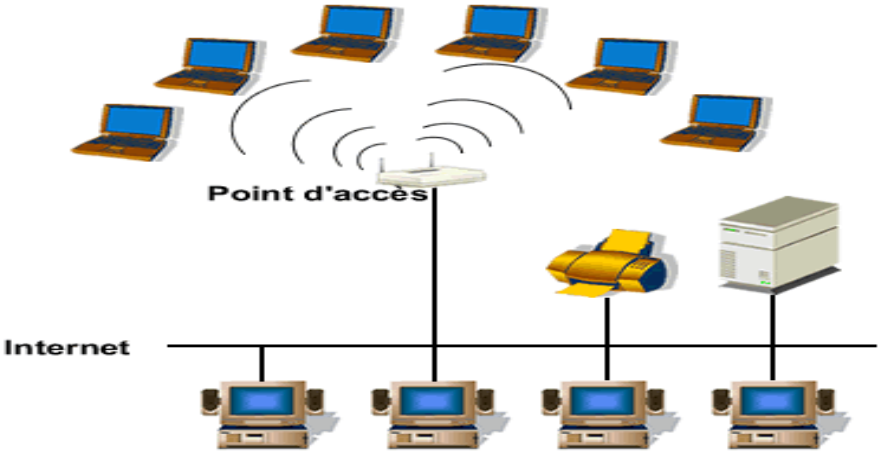


Figure I.6 : Un réseau câblé "traditionnel"
associé à un réseau sans fil (réseau hybride)

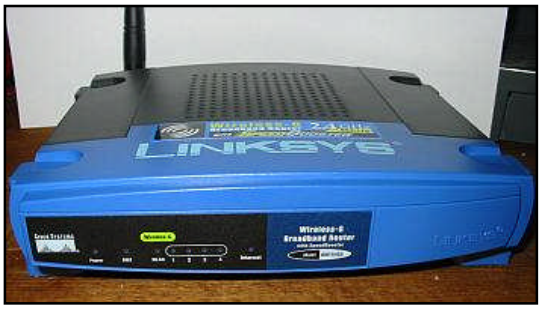


Figure I.7a : point d'accès (vue avant)

Figure I.7b : point d'accès (vue arrière)

9. Les modes d'interconnexion

Access Point (AP) : ce mode permet de créer un réseau à part entière en interconnectant les diverses connexions sans fil.

Wireless Bridge : ce mode permet d'interconnecter deux réseaux entre eux par un "pont sans fil". Ainsi, le réseau A disposant de 2 ordinateurs reliés à un routeur pourra être interconnecté avec le réseau B disposant de 2 ordinateurs reliés entre eux avec un hub ou un switch puis à l'AP.

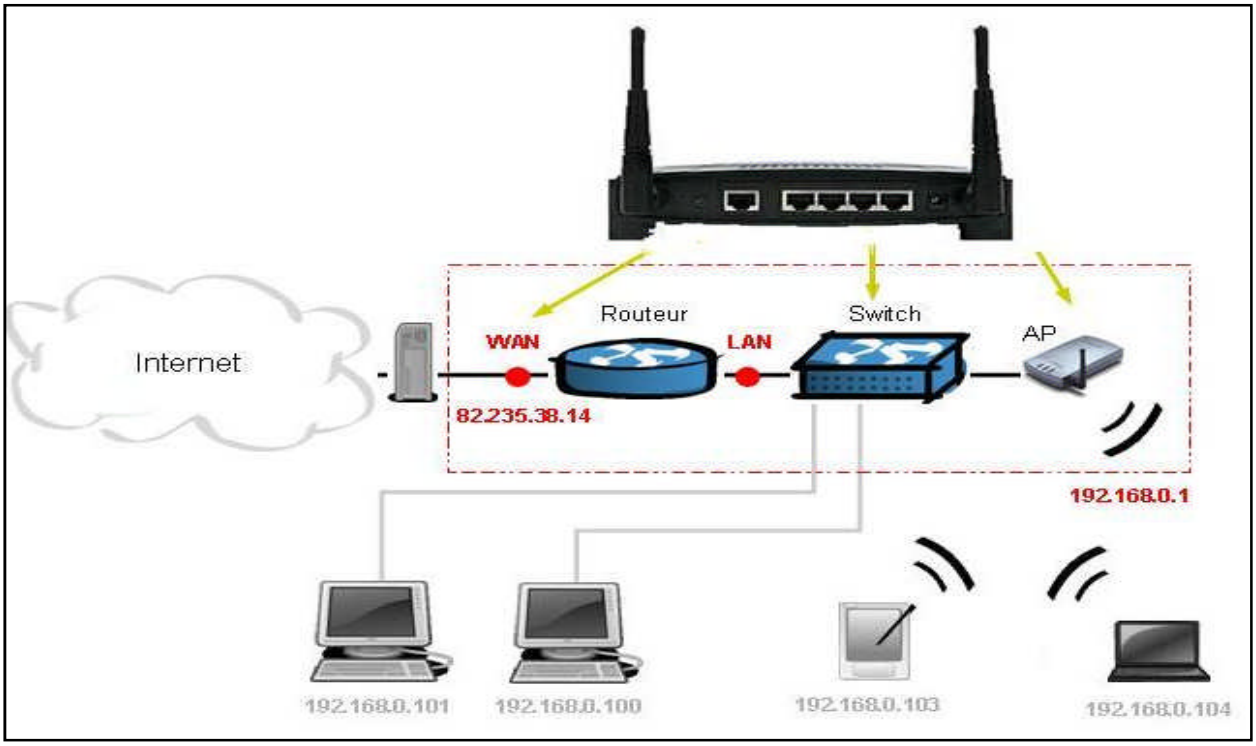


Figure I.8 : point d'accès en mode pont sans fil

Multi point Bridge : similaire au précédant si ce n'est que l'on peux relier plusieurs "points d'accès" entre eux et disposer ainsi du roaming.

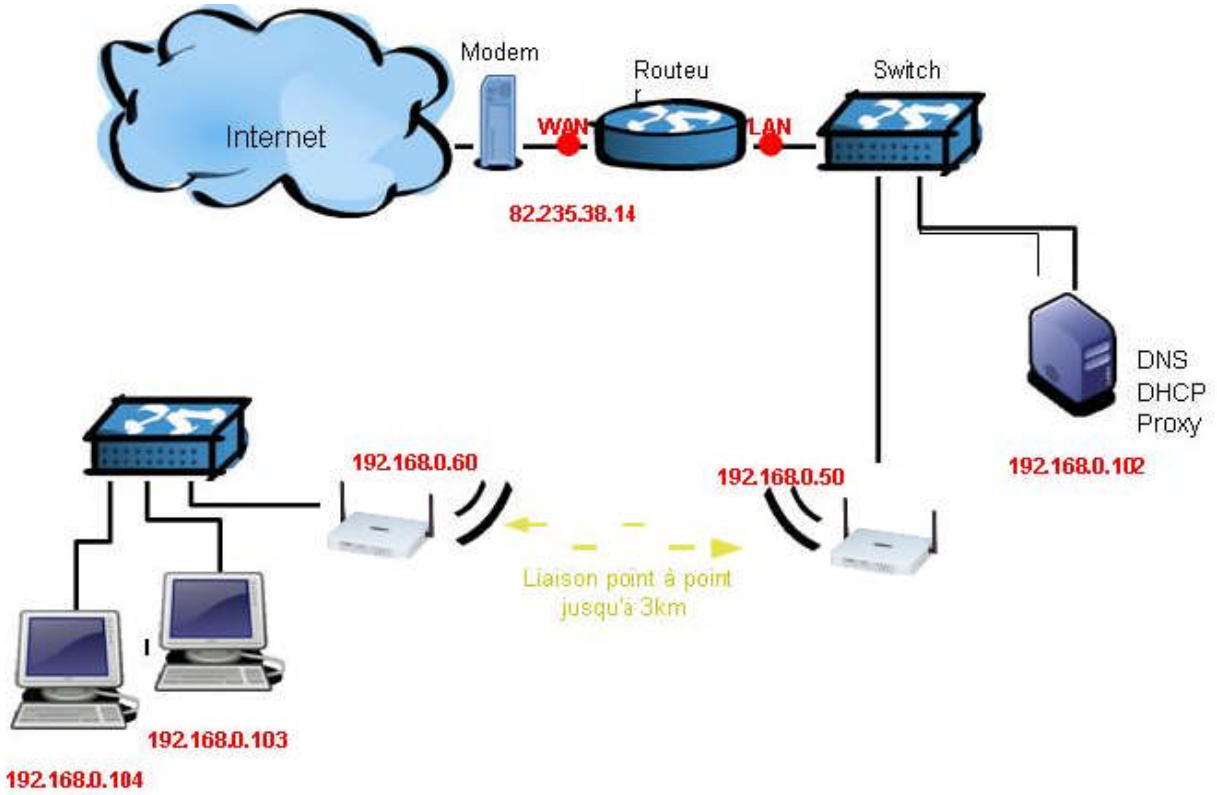


Figure I.9 : point d'accès en mode multi ponts sans fil

Wireless Client: permet de transformer toute carte réseau classique avec fil, une fois connecté à l'AP, en carte réseau Wireless en mode client.

Repeater (Répéteur): permet d'augmenter la distance de fonctionnement du réseau Wireless en renvoyant bit à bit le signal vers son destinataire.

Routeur Wi-Fi

Le modem routeur WiFi

Conclusions

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)

Dans le chapitre qui suit nous allons procéder à la configuration d'un point d'accès.

Nom de la norme	Nom	Description
802.11a	Wifi 5	La norme 802.11a (baptisé Wifi 5) permet d'obtenir un haut débit (54Mbps théoriques, 30Mbps réels). la norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHZ
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11Mbps (6Mbps réel) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHZ, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.11d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.11 (niveau liaison de données).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière a permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole inter-Access point roaming Protocol permettant a un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais)
802.11g		La norme 802.11g offre un haut débit (54Mbps théoriques, 30Mbps réels) sur la bande de fréquence des 2.4 GHZ. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (Hiper LAN 2, dou le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11r		La norme 802.11r a été elaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme 802.11J est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

CHAPITRE II:
ETUDE
DE LA SECURITE
DES
RESEAUX SANS FIL

Introduction

Durant ces dernières années, le développement des nouvelles technologies de l'information et des communications associé à la complexité croissante des échanges d'informations inter et intra entreprises a engendré un engouement certain pour l'informatisation et le développement de réseaux informatiques. De tels réseaux devraient être capables de gérer tous les flux de données qui transitent à travers l'entreprise, tout en assurant un degré de sécurité et de confidentialité essentiel au bon fonctionnement de cette entreprise. Les réseaux locaux sans fil ou *Wireless Local Area Network* (WLAN) sont l'une des catégories de réseaux qui ont connu un très grand essor de par les nombreux avantages qu'ils offrent. Bon nombre de ces réseaux se sont même multipliés dans des endroits publics comme les cafés, les hôtels et les aéroports, plus communément connus sous le nom de *HotSpot*. Les WLAN ont résolu beaucoup de problèmes comparativement aux réseaux locaux filaires classiques. Cependant, ils en ont introduit d'autres aussi, et notamment ceux relatifs à la sécurité des communications.

Dans cet article, nous allons, tout d'abord, donner un bref aperçu des différentes technologies utilisées dans les WLAN. Ensuite, nous exposerons succinctement les problèmes de sécurité relatifs aux WLAN. Enfin, nous présenterons un ensemble de solutions techniques, architecturales et managériales permettant de résoudre sinon de limiter l'impact de ces problèmes.

1. Aperçu sur les WLAN

Les WLAN sont basés sur des liaisons utilisant des ondes électromagnétiques en lieu et place des câbles habituels. Ils permettent de relier très facilement des équipements distants d'une centaine de mètres. De plus, l'installation de tels réseaux ne demande pas de gros investissements, ni de lourds aménagements des infrastructures existantes, comme c'est le cas avec les réseaux filaires, ce qui a valu un développement rapide de ce type de technologies. En contrepartie se pose le problème de la réglementation relative aux transmissions radio. En effet, les transmissions radio servent à un grand nombre d'applications (militaires, scientifiques, amateurs, etc.) et sont sensibles aux interférences. C'est la raison pour laquelle une

réglementation est nécessaire dans chaque pays afin de définir les plages de fréquences et les puissances auxquelles il est possible d'émettre pour chaque catégorie d'utilisation.

Les standards IEEE 802.11 [1] régissent les communications dans les réseaux locaux sans fil. Ces standards se distinguent d'une part par la fréquence d'émission utilisée et d'autre part par le débit des transmissions et la technologie de modulation :

- **IEEE 802.11a** utilise la modulation OFDM (Orthogonal Frequency Division Multiplexing) pour la transmission sur la bande de fréquences UNII (Unlicensed National Information Infrastructure) de 5.150 à 5.725 GHz et offre un débit maximal de 54 Mbps.
- **IEEE 802.11b** utilise la modulation DSSS (Direct Sequence Spread Spectrum) pour la transmission sur la bande de fréquences ISM (Industrial, Scientific and Medical) de 2.4 à 2.5 GHz, possède 3 canaux non interférants et offre un débit maximal de 11 Mbps. Par contre, les réseaux 802.11b ne sont pas compatibles avec les réseaux 802.11a.
- **IEEE 802.11g** combine les avantages de 802.11a et 802.11b. Il offre un débit maximal de 54 Mbps et utilise la modulation OFDM (Orthogonal Frequency Division Multiplexing) pour la transmission mais sur la bande de fréquence ISM (Industrial, Scientific and Medical) de 2.4 à 2.5 GHz. De plus, il est compatible avec 802.11b, ce qui permet d'augmenter le débit tout en évitant une mise à jour matérielle complète, trop coûteuse, des réseaux WLAN déjà existants.

2. Les problèmes de sécurité dans les WLAN

De par leur nature même, les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour une personne malveillante d'intercepter le trafic du réseau si les informations circulent en clair. Par conséquent, il est fondamental de mettre en place des dispositifs adéquats de manière à assurer la confidentialité et l'intégrité des données circulant dans les WLAN.

La sécurité des communications dans les WLAN est basée sur un mécanisme appelé **WEP** pour *Wired Equivalent Privacy*. WEP requiert une clé secrète devant être déployée aux différents points d'accès et dans les appareils sans fil des usagers mobiles (Laptop, PDA,…).

Clé WEP	Vecteur	Graine
40 bits	24 bits	64 bits
104 bits	24 bits	128 bits
232 bits	24 bits	256 bits
488 bits	24 bits	512 bits

Tableau II.1 : constitution des graines binaires

Cette clé sera utilisée d'une part pour le cryptage des données avant leur transmission et d'autre part pour la vérification de l'intégrité des données. Or plusieurs études ont révélé et largement documenté des failles dans ce mécanisme, failles qui ont rendu les WLAN susceptibles à un ensemble d'attaques permettant notamment de retrouver la clé de chiffrement ou d'usurper l'identité d'un utilisateur honnête.

La graine binaire est soumise à l'algorithme RC4 qui à son tour va générer la séquence pseudo aléatoire. Le chiffrement s'opère par application bit à bit d'un OU Exclusif (XOR) entre la séquence pseudo aléatoire obtenue et les données utilisateurs en clair sous forme de

PDU (Protocol Data Unit), comme illustré sur la figure suivante :

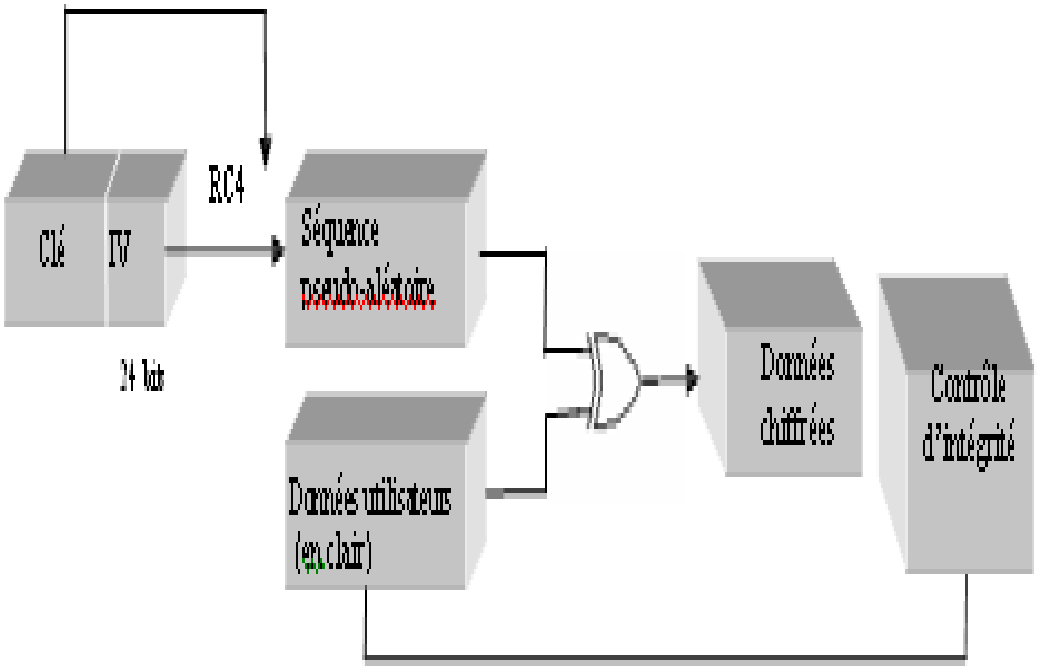


Figure II.1: Mécanisme de chiffrement

Le vecteur d'initialisation change avec chaque paquet (PDU) envoyé. Par ailleurs, un champ de contrôle d'intégrité est obtenu par un CRC 32 calculé sur la trame à encoder (données utilisateurs en clair).

La trame envoyée contient le vecteur d'initialisation, un identificateur de la clé de chiffrement, les données chiffrées (cryptées) et le champ contrôle d'intégrité.

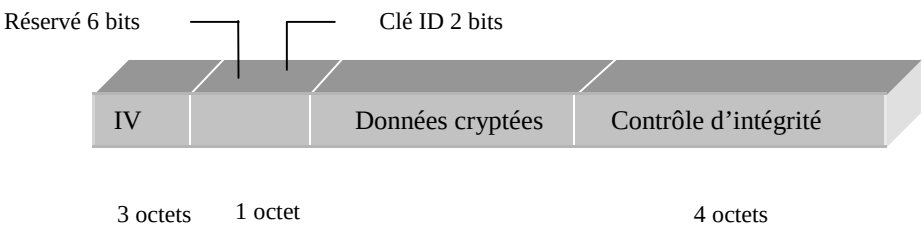


Figure II.2: Encapsulation d'une trame cryptée

L'ID de clé de chiffrement et le vecteur d'initialisation permettent de reconstruire la séquence pseudo aléatoire de chiffrement et de déchiffrer ainsi la trame. L'application bit à bit d'un OU Exclusif entre la séquence pseudo- aléatoire et les données chiffrées permettent de retrouver la trame initiale. Sur cette dernière, l'algorithme de calcul du contrôle d'intégrité est appliquée et le résultat, comparé à la valeur envoyée dans la trame. En cas de correspondance, la trame est acceptée, sinon, elle est rejetée.

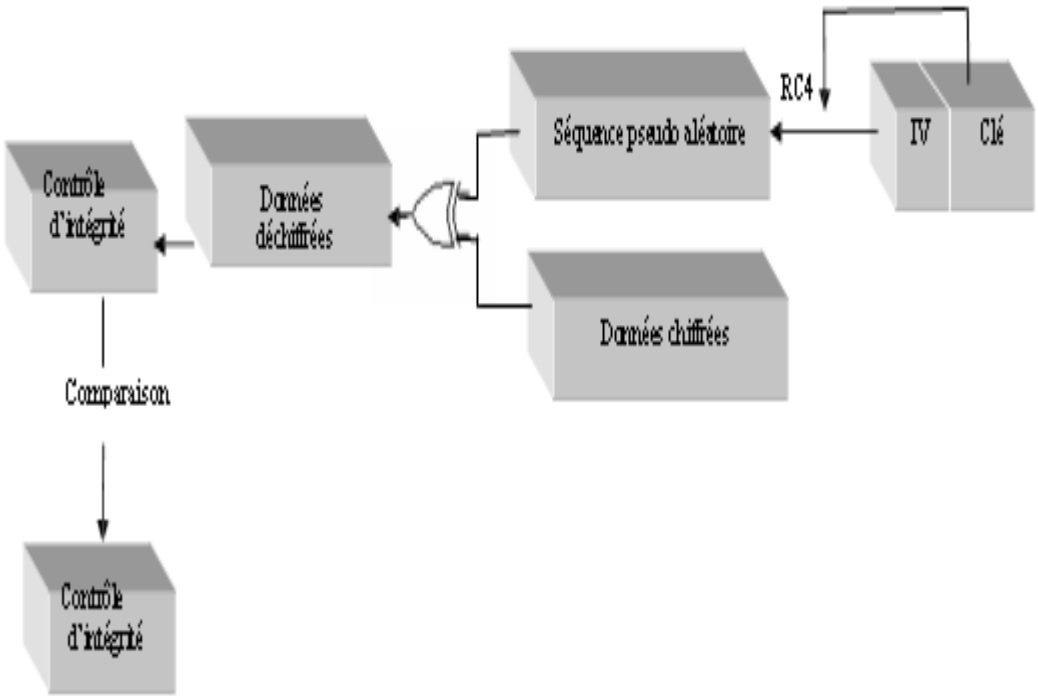


Figure II.3: Mécanisme de déchiffrement

Deux techniques d'authentification sont associées au WEP :

- *Open System Authentification :* C'est la technique d'authentification par

défaut, l'authentification ne produit aucune vérification, un terminal peut donc s'associer avec n'importe quel point d'accès et écouter tout le trafic écoulé au sein du BSS.

- *Shared Key Authentification :* Cette technique est dite de la clé secrète partagée. Elle permet de s'assurer que la station qui souhaite s'authentifier possède bien la clé partagée.

Cette vérification ne nécessite pas de transmettre la clé en clair mais s'appuie sur l'algorithme de chiffrement WEP. Le mécanisme d'authentification se déroule en quatre étapes :

- *Etape 1* : La station désirant s'associer avec le point d'accès envoie une trame d'authentification.
- *Etape 2* : Après avoir reçu la trame, le point d'accès envoie à la station une trame de 128 bits qui correspond à un texte aléatoire généré par l'algorithme de chiffrement.
- *Etape 3* : Après réception de la trame, la station copie le texte dans une trame d'authentification et le chiffre avec la clé secrète partagée avant d'envoyer le tout au point d'accès.
- *Etape 4* : le point d'accès déchiffre le texte avec la même clé et la compare avec celui qu'il avait envoyé plus tôt. S'ils sont identiques, le point d'accès confirme l'authentification, sinon, il envoie une trame d'authentification négative.

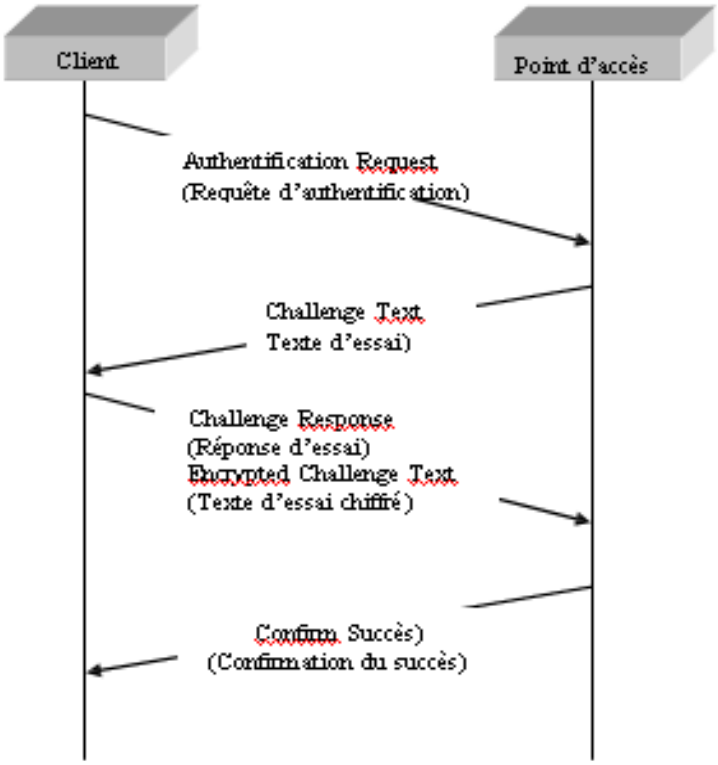


Figure II.4 : Fonctionnement du mécanisme Shared Key Authentification

2.1 Les inconvénients du WEP

Le WEP présente cependant des failles qui peuvent être classées en deux grandes catégories : les failles cryptographiques et les failles architecturales.

Les **failles cryptographiques** sont dues, tout d'abord, à une mauvaise utilisation dans WEP de l'algorithme de chiffrement RC4 (*Rivest's Cipher 4*) qui est un algorithme utilisant le cryptage du flux de données (*stream cipher algorithm*), en ayant recours à un générateur de nombres pseudo aléatoires (PRNG, *Pseudo Random Number Generator*). Ces failles sont également dues à une mauvaise gestion des clés de cryptage et à une trop faible authentification des usagers mobiles. Les **failles architecturales** correspondent à une mauvaise conception du WLAN, notamment le choix de l'emplacement des points d'accès, de l'étendue de leur signal et de leur configuration intrinsèque.

3. Les solutions de sécurité dans les WLAN

Vu l'intérêt croissant et le développement exponentiel de l'utilisation des réseaux locaux sans fil et afin de minimiser l'impact des failles de sécurité découvertes plusieurs solutions techniques architecturales et managériales ont été proposées parmi lesquelles on peut mentionner le filtrage par adresse MAC, les réseaux privés virtuels, le Wi-Fi Protected Access (WPA), le nouveau standard IEEE 802.11i et une bonne gestion stratégique du WLAN.
De plus, on peut citer encore d'autres solutions de sécurité tel que cacher le réseau (le rendre invisible pour les autres utilisateurs) et régler la puissance de l'antenne.

3.1 Le filtrage par adresses MAC

Cette technique est utilisée afin d'empêcher les accès non autorisés aux réseaux locaux sans fil et est basée sur les adresses MAC (*Media Access Control*) des usagers mobiles. Habituellement, chaque carte réseau possède une adresse MAC unique qui permet de la distinguer des autres. D'autre part, un point d'accès peut sauvegarder une liste de contrôle d'accès contenant les adresses MAC des utilisateurs mobiles pouvant se connecter à travers le point d'accès au WLAN, comme l'illustre la Figure 1. Par la suite, chaque usager mobile ayant une adresse MAC ne faisant pas partie de la liste de contrôle se verra automatiquement refuser l'accès. Cette technique demande un grand travail à l'administrateur réseau vu qu'il doit programmer tous les points d'accès avec les bonnes adresses et les maintenir à jour. De plus, cela limite la mobilité des utilisateurs aux points d'accès qui contiennent préalablement leurs adresses. Finalement, dans certains cas il est possible pour des usurpateurs de changer l'adresse MAC des cartes réseaux sans-fil à l'aide d'outils de modification du firmware.

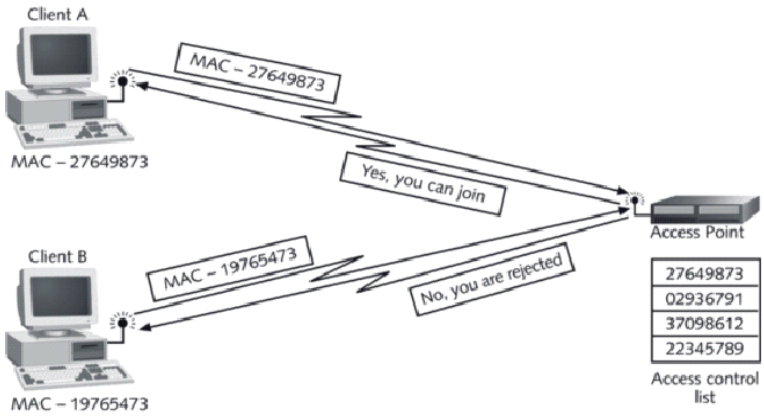


Figure II.5. Sécurisation par adresses MAC

3.2 Les réseaux privés virtuels

Un réseau privé virtuel ou *Virtual Private Network* (*VPN*) est une extension d'un réseau privé comportant des liens sur des réseaux publics comme Internet. Il sécurise une connexion en cryptant tout le trafic du réseau avant de l'envoyer sur Internet, puis en le décryptant lorsqu'il arrive à l'autre extrémité du réseau privé virtuel. Comme le réseau public transporte tout le trafic du réseau privé virtuel sous forme encapsulée, une connexion VPN est également appelée *tunnelling*. Le VPN peut avoir recours aux protocoles PPTP (*Point-to-Point Tunneling Protocol*) ou le mode tunnel du protocole IPSec (*Internet Protocol Security*) pour gérer les tunnels et encapsuler les données privées. Dans le cas d'un WLAN, comme l'illustre la Figure 2, des utilisateurs mobiles distants ayant accès à Internet, dans un *HotSpot* par exemple, pourront alors se connecter au réseau local de l'entreprise d'une manière totalement sécuritaire via un tunnel crypté. L'inconvénient est qu'un VPN requiert une configuration minutieuse tenant compte des problèmes d'interopérabilité et de compatibilité inter plate-forme.

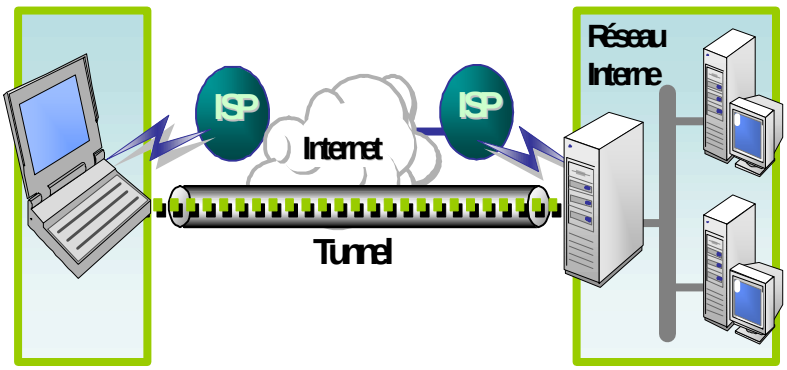


Figure II. 6 : Sécurisation par VPN

3.3 Le Wi-Fi Protected Access

Le Wi-Fi Protected Access (*WPA*) est prôné par la Wi-Fi Alliance, une organisation à but non lucratif composée des leaders industriels constructeurs de matériel pour systèmes sans fil et des entreprises fournissant des services relatifs aux réseaux locaux sans fil. Elle s'occupe

principalement de certifier l'interopérabilité et la compatibilité des produits répondant aux standards IEEE 802.11 et de faire la promotion de cette technologie de réseaux locaux sans fil auprès des industriels et des clients.

WPA peut être utilisé dans un environnement personnel ou professionnel. Il ne nécessite pas de mise à jour matérielle de l'infrastructure existante mais uniquement une mise à jour logicielle. WPA permet d'améliorer deux aspects importants de la sécurité sans fil, en l'occurrence le chiffrement des données et l'authentification.

Pour améliorer le chiffrement, WPA utilise le *Temporal Key Integrity Protocol* (TKIP) qui est basé sur une fonction de mixage de clés par paquet et un *Message Integrity Check* (MIC). Pour améliorer l'authentification, WPA introduit une méthode basée sur des mots de passe, comme l'illustre la Figure II. 7.

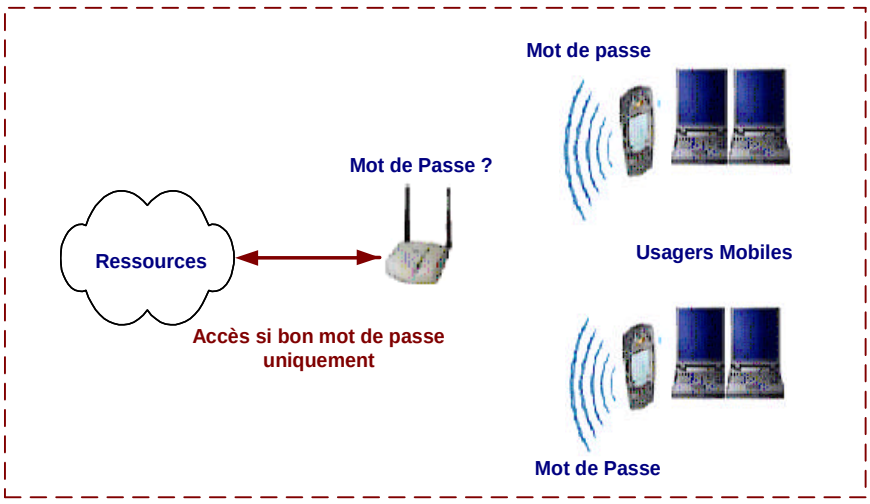


Figure II.7 Authentification sécurisée avec WPA

3.4 Le nouveau standard IEEE 802.11i

Le standard IEEE 802.11i [9] présente une combinaison complexe de plusieurs protocoles et mécanismes visant à sécuriser les WLAN. En effet, pour améliorer la sécurité du chiffrement, deux protocoles cryptographiques sont ajoutés à WEP : *Counter-Mode Cipher Block Chaining Message Authentication Code Protocol* (CCMP) et *Temporal Key Integrity Protocol* (TKIP).

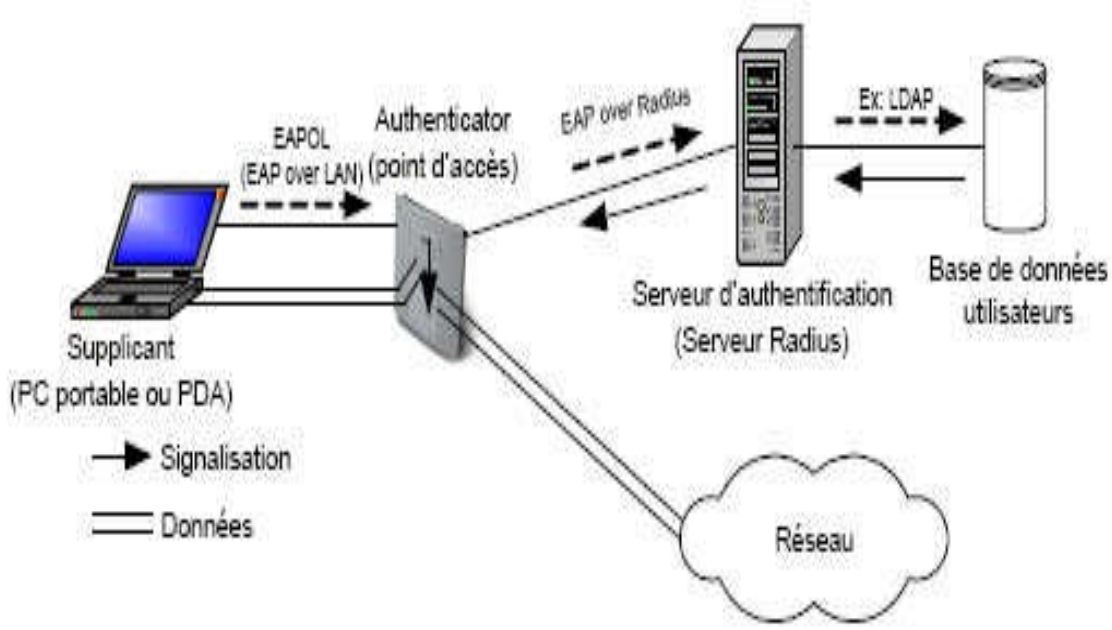


Figure II.8 ARCHITECTURE 802.1X

CCMP est basé sur l'algorithme de cryptage *Advanced Encryption Standard* (AES), alors que TKIP utilise l'algorithme de cryptage RC4. CCMP requiert une mise à jour matérielle des points d'accès tandis que TKIP nécessite seulement une mise à jour logicielle. TKIP est principalement destiné à assurer l'interopérabilité entre anciens et nouveaux réseaux WLAN. Par conséquent, les nouveaux WLAN pourront supporter l'utilisation simultanée de trois protocoles de chiffrement : WEP, TKIP et CCMP. L'unité mobile et le point d'accès concerné utiliseront le plus haut degré de sécurité que les deux peuvent supporter mutuellement. Concernant la gestion des clés, deux nouveaux modes sont introduits : une gestion de clés manuelle et une gestion de clés automatique. La première nécessite un administrateur réseau afin de déployer manuellement les clés de chiffrement, alors que la deuxième se base sur des mécanismes nommés *4-Way Handshake* et *Groupe Key Handshake* afin de gérer convenablement la distribution des clés.

3.5 Une bonne gestion stratégique du WLAN

Une contribution importante à l'efficacité de la sécurité peut être assurée grâce à une bonne gestion stratégique du réseau. En effet, un monitoring assidu et régulier de ce qui se passe sur le réseau sans fil est primordial. Il permettra aux administrateurs de mieux évaluer le degré de sécurité atteint par leur installation et par conséquent l'améliorer s'il ne répond pas

aux objectifs fixés. D'autre part, la mise à jour logicielle régulière des points d'accès représente une opération critique pour maintenir un bon degré de sécurité. Beaucoup d'administrateurs prennent trop de temps avant d'installer des correctifs (*patch*) suite à la découverte d'une faille, ce dont profitent les hackers. Enfin, un audit régulier de l'environnement du WLAN est fortement recommandé. Il permettra de savoir exactement l'étendue du signal du réseau sans fil, comment le réseau est utilisé, par quels utilisateurs et à quelles fins. Il permettra aussi de vérifier les configurations de chaque point d'accès et de leur conformité à la politique de sécurité de l'entreprise.

Conclusions

Nous nous sommes intéressés à l'une des catégories de réseaux qui a connu l'un des plus grands développements ces dernières années : les réseaux locaux sans fil ou WLAN. La raison pour laquelle ce type de réseau a connu une si grande expansion est qu'il offre de nombreux avantages comme par exemple la facilité de déploiement, une meilleure mobilité des usagers ou encore des coûts de mise en place assez faibles. Par contre, l'inconvénient majeur qu'il introduit est la sécurité des communications. Comme nous l'avons illustré, les problèmes de sécurité dans les WLAN sont nombreux, diversifiés et complexes. Prétendre éliminer complètement tous ces problèmes serait utopique mais, en ayant recours à une combinaison des solutions présentées dans cet article, la sécurité des communications dans les WLAN peut être considérablement améliorée. Par ailleurs, les plus sceptiques en matière de sécurité informatique opteront pour une stratégie complètement distincte de ce que nous avons présenté jusqu'à présent, en l'occurrence le *Wait and See* qui consiste à éviter tout déploiement de WLAN jusqu'à ce que les aspects de sécurité soient mieux résolus. C'est d'ailleurs la stratégie adoptée par diverses unités du gouvernement fédéral américain, dont le Pentagone et la plupart des services militaires. De plus un rapport intitulé *The National Strategy to Secure Cyberspace* recommande à toutes les agences gouvernementales américaines une précaution extrême envers les technologies sans fil.

CHAPITRE III:
PROCEDURES DE CONFIGURATION DES POINTS D'ACCES

INTRODUCTION

Le Wifi est une technologie réseau de plus en plus utilisée que ce soit en entreprise ou chez les particuliers. De nombreux constructeurs de matériel informatique produisent des équipements Wifi ayant un plus ou moins grand nombre de fonctions intégrées selon le type d'utilisateur visé. Quelques types de ces points d'accès tels que le TP-LINK TL-WR641G , Cisco Aironet Série 1230 et le cisco 1131 ou encore le DWL-2100APde d-link qui s'adressent avant tout aux entreprises ayant besoin de fonctions avancées de sécurité et de configuration réseau

Les étapes de configuration de base de ces points d'accès seront abordées dans ce chapitre.

1-Installation Logique (Configuration du Point d'Accès) :

Une fois le point d'accès installé, il doit être configuré pour l'utilisation.

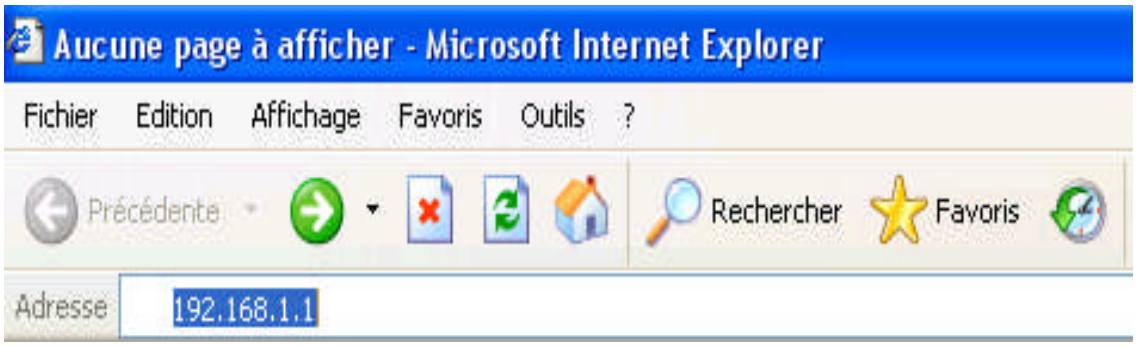
Il existe deux manières de paramétrer le point d'accès :

- Via un utilitaire : en utilisant un CD-ROM fournit dans le package
- Via un configurateur Web : en utilisant une adresse http:/ fournit dans le manuel d'utilisation de l'équipement.

La plus facile à utiliser est la méthode de configuration via un utilitaire, en utilisant un CD - ROM fournit dans le package.

En double cliquant sur un navigateur Web (Internet explorer), on saisi l'adresse par défaut, fournit avec le point d'accès WI-FI qui est : http:/ 192.168.1.1 par laquelle on va accéder au software du point d'accès.

I -1 LE TP-LINK TL-WR641G

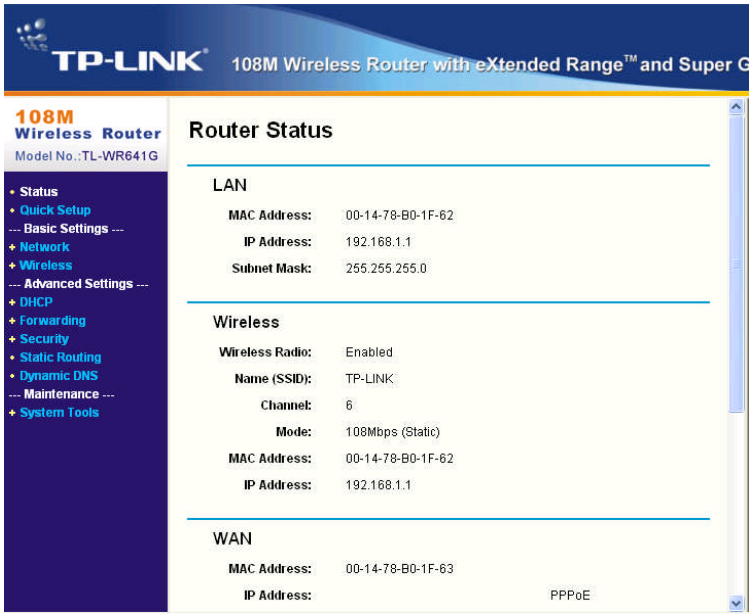


On aura la fenêtre suivante qui comporte une boite de dialogue qui va nous demander d'insérer un nom d'utilisateur et un mot de passe.

Le nom d'utilisateur par défaut est « Admin. » et le mot de passe est aussi par défaut « Admin. » et ils sont changeables par mesure de sécurité.

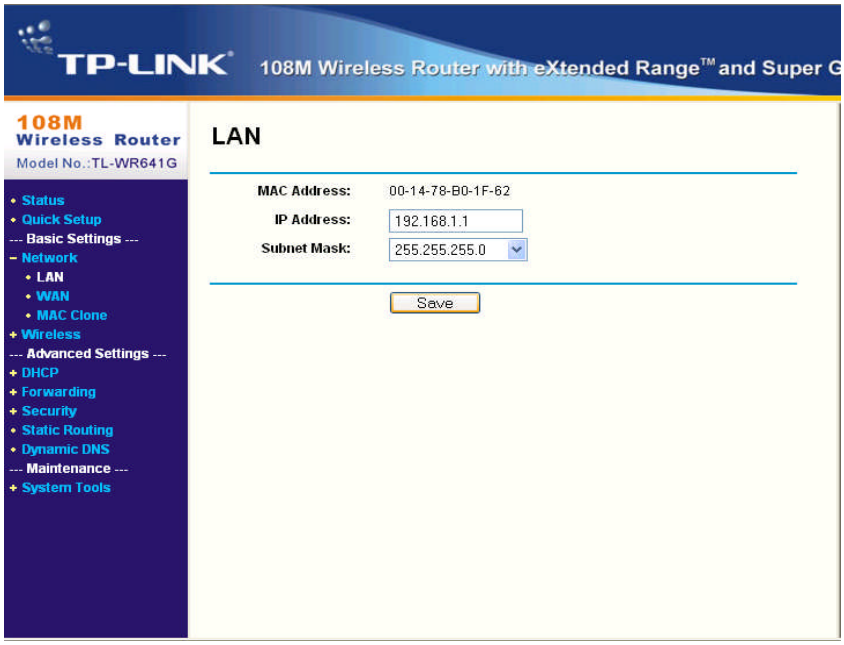
On cliquant sur **ok** on aura le software du point d'accès qui s'affiche comme une page Web sur laquelle il y'a ses paramètres de configuration.

Cette page comporte plusieurs rubriques comme S**tatut , Basic setting , Advenced setting , Maintenance,** qui contiennent des informations sur le paramétrage du point d'accès.

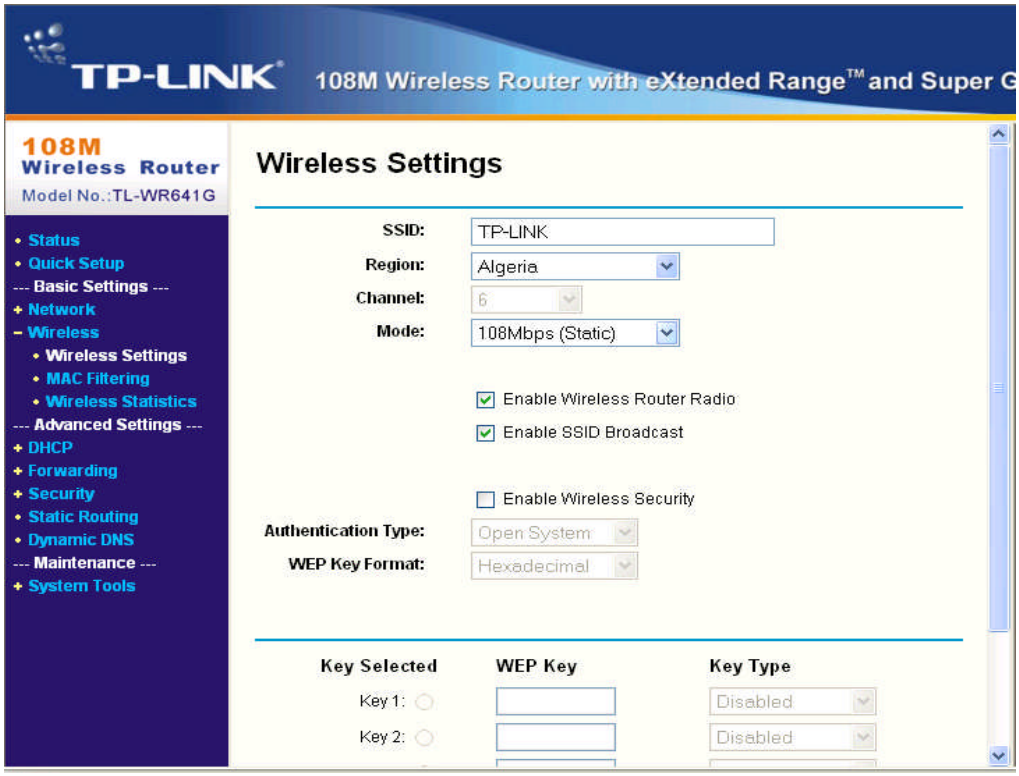


Ces rubriques nous aident à configurer le point d'accès .

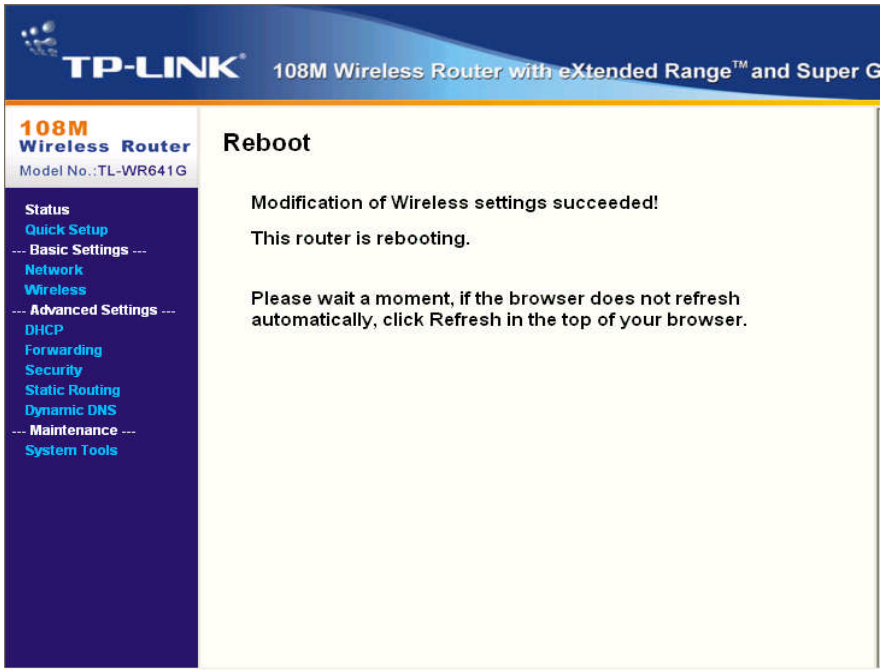
Donc pour rendre le point d'accès compatible avec le réseau qu'on appartient, il faut changer le numéro de réseau dans son adresse **IP,** c'est-à-dire qu'on met une autre adresse IP au lieu de 192.168.1.1.on clique sur save en bas de la page.



Après on passe au changement du SSID qui est le nom du réseau et le canal de transmission sur le quel on travaille comme l'indique la figure suivante, En cliquant sur **save.**

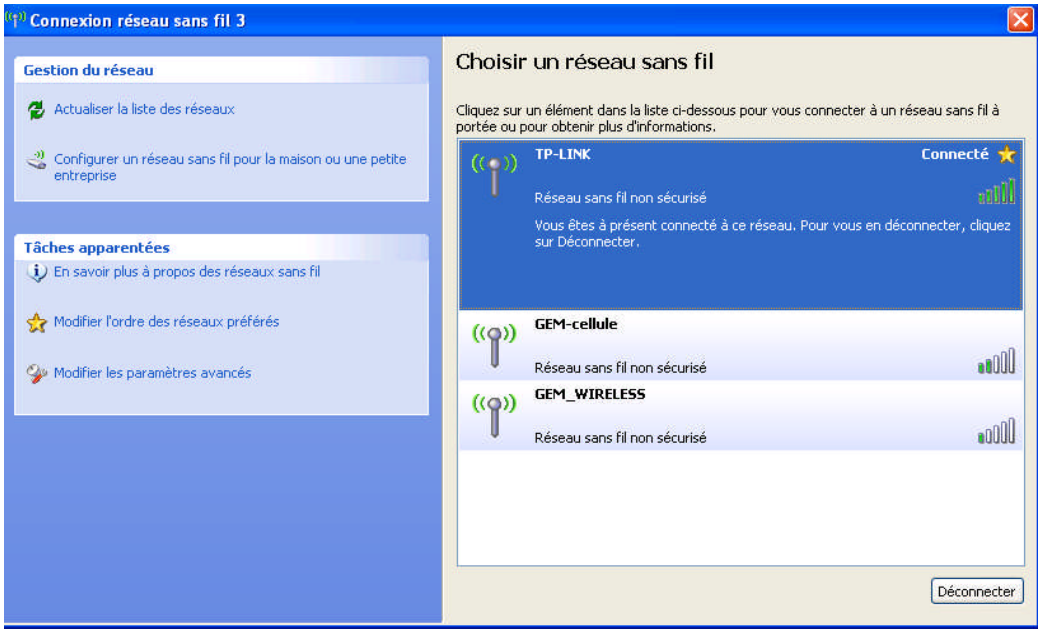


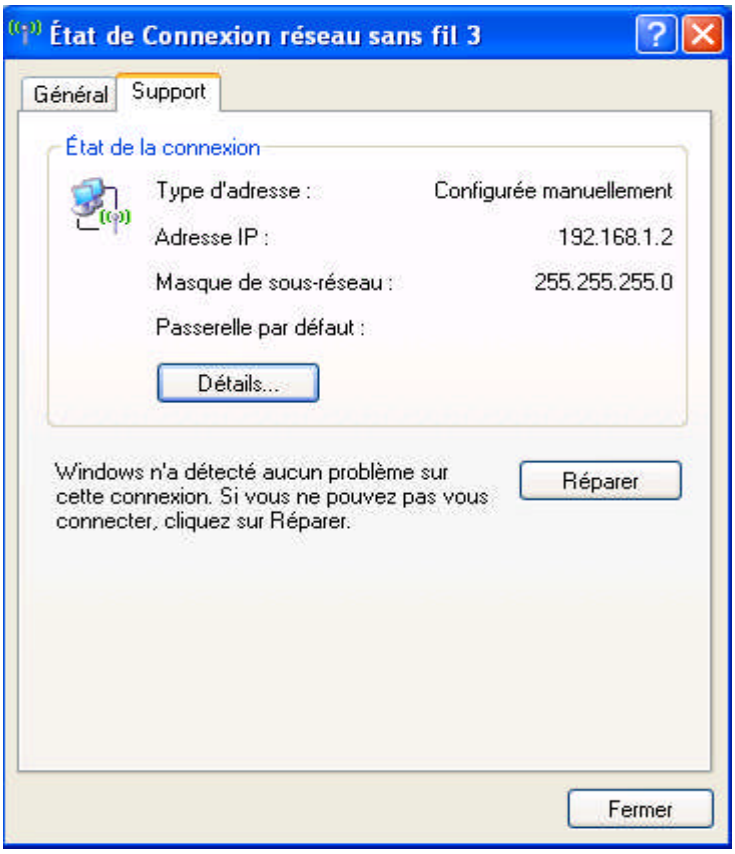
Cette fenêtre représente la fin de la configuration il y'a un reboot pour confirmer la fin de l'installation.



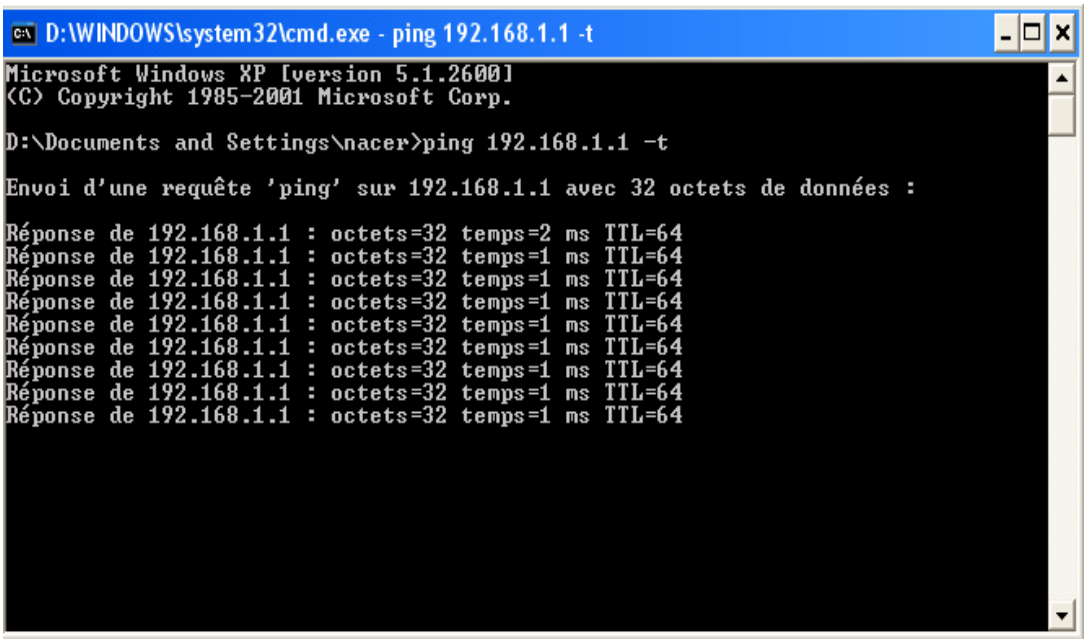
Après on va configurer toutes les cartes réseaux de tous les postes en leur attribuant des adresses IP comportant le même nom de réseau « TP-LINK »

Confirmation de la connexion au réseau sans fil « TP-LINK » sur un poste client.





Après avoir mis en place les postes de travail et le point d'accès WIFI physiquement, une vérification de la connexion en utilisant la commande PING est très indispensable, on va pinguer le point d'accès à partir de chaque poste pour vérifier s'il communique bien, la commande PING est indiquée par la figure suivante :



1.2. Le DWL-2100AP

Pour configurer le DWL-2100AP, il vaut mieux utiliser un ordinateur (équipé d'un adaptateur Ethernet) qui est relié à un commutateur. L'adresse IP par défaut du DWL-2100AP est

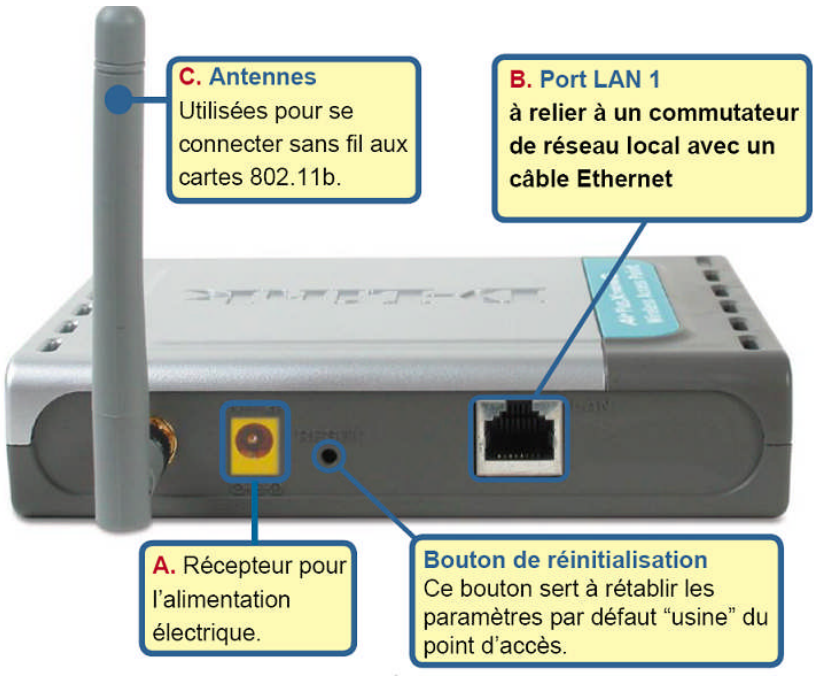
192.168.0.50; le masque de sous-réseau est 255.255.255.0. Il vous faudra attribuer une adresse IP statique appartenant à la même tranche que l'adresse IP du DWL-2100AP.

1.3 Connexion du point d'accès sans fil DWL-2100AP

A.Connectez le câble de l'adaptateur secteur à la **prise** située à l'arrière du DWL-2100AP et branchez l'adaptateur secteur sur une prise murale ou sur un bloc multiprise. Le voyant d'alimentation doit **s'allumer**.

B. Branchez un câble entre le **port Ethernet** situé à l'arrière du DWL-2100AP et un **routeur à large bande Ethernet** (comme le DI-604 D-Link) ou un commutateur à large bande Ethernet (comme le DSS-5+ D-Link). **Nota** : vous pouvez également relier directement le DWL-2100AP à l'ordinateur qui servira à le configurer. Le voyant Link s'allume si le branchement est correct. (Note : les ports LAN du DWL-2100AP sont auto-MDI/MDIX, ce qui signifie que vous pouvez utiliser aussi bien un câble droit qu'un câble croisé sur les ports LAN).

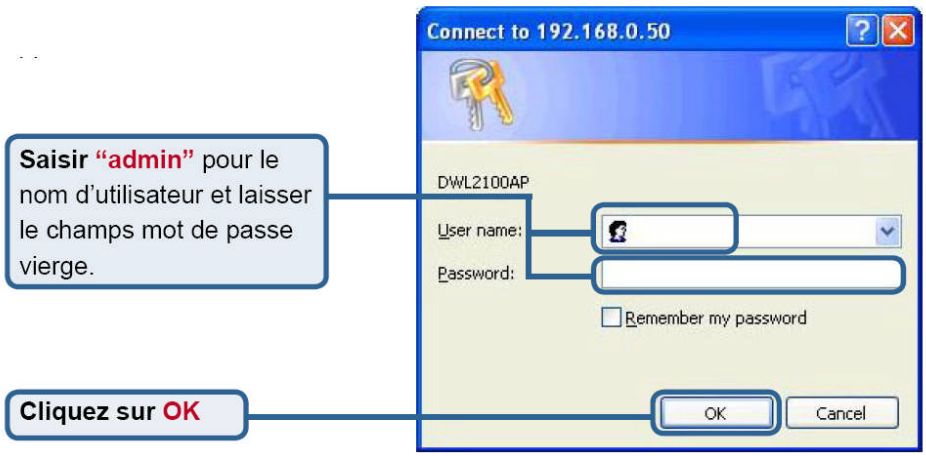
C. L'adaptateur Cardbus sans fil Xtreme G AirPlus DWL-G520 et l'adaptateur Cardbus sans fil Xtrem G AirPlus DLW-G650 sont compatibles d'emblée avec le DWL-2100AP. Les ordinateurs équipés d'adaptateurs sans fil 802.11b peuvent, eux aussi, être reliés au DWL-2100AP.



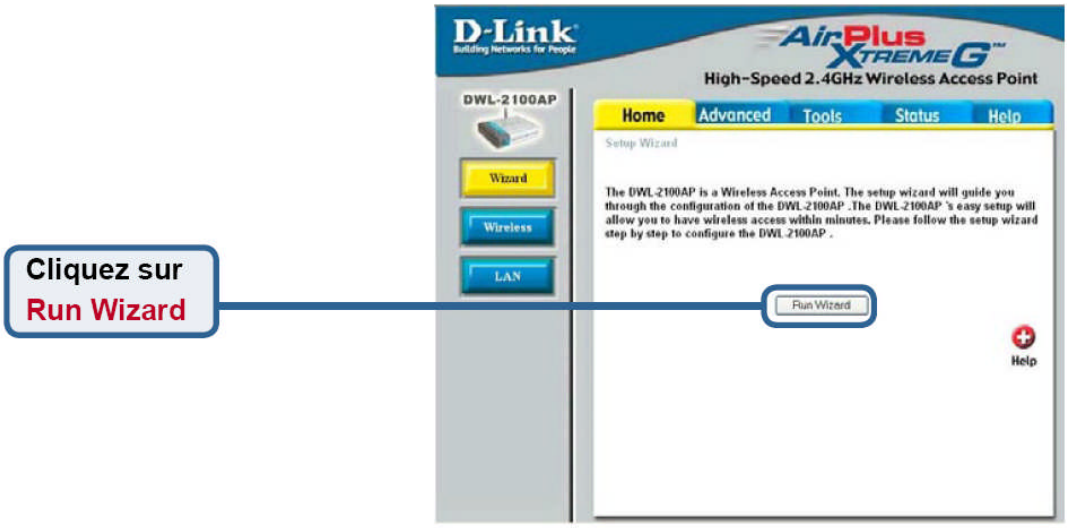
Une fois les opérations ci-dessus effectuées, votre réseau doit se présenter comme illustré ci-dessous

Utilisation le Wizard d'installation

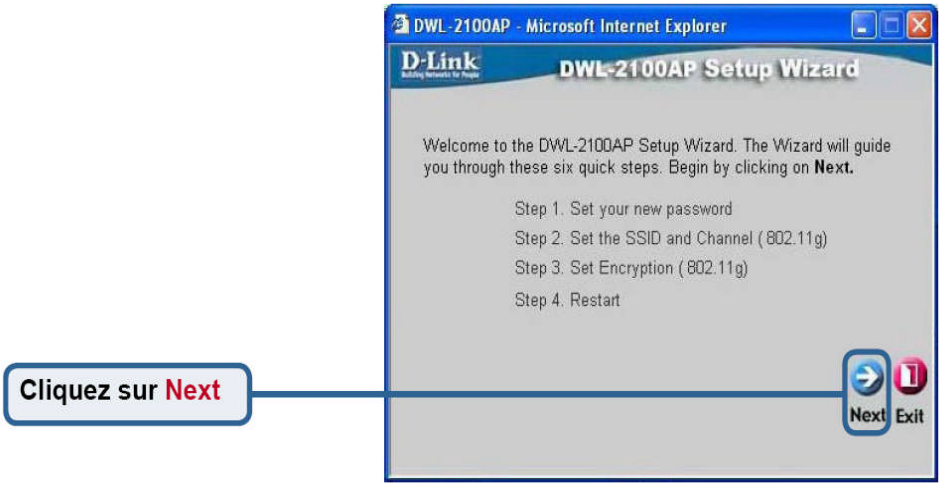
L'écran de connexion apparaîtra



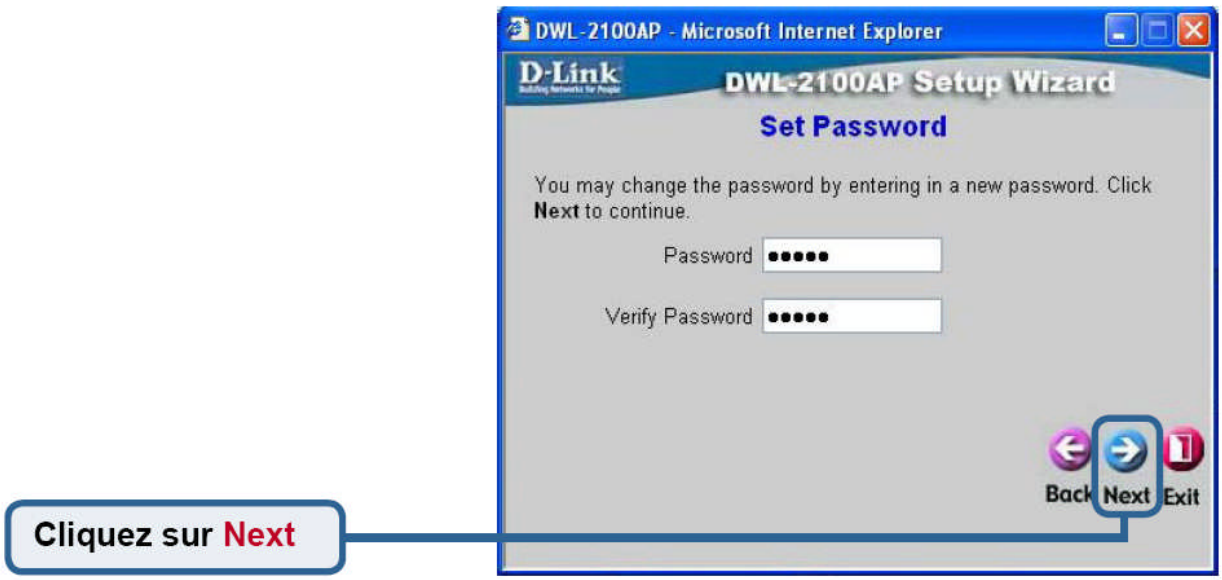
Une fois la connexion établie, l'écran d'accueil **(Home)** apparaît**)**



Les écrans suivants se succèdent.



Étape 1 - Choisissez votre nouveau mot de passe. Vous avez la possibilité de définir un mot de passe. **Étape 1 - Choisissez votre nouveau mot de passe**. Vous avez la possibilité de définir un mot de passe.



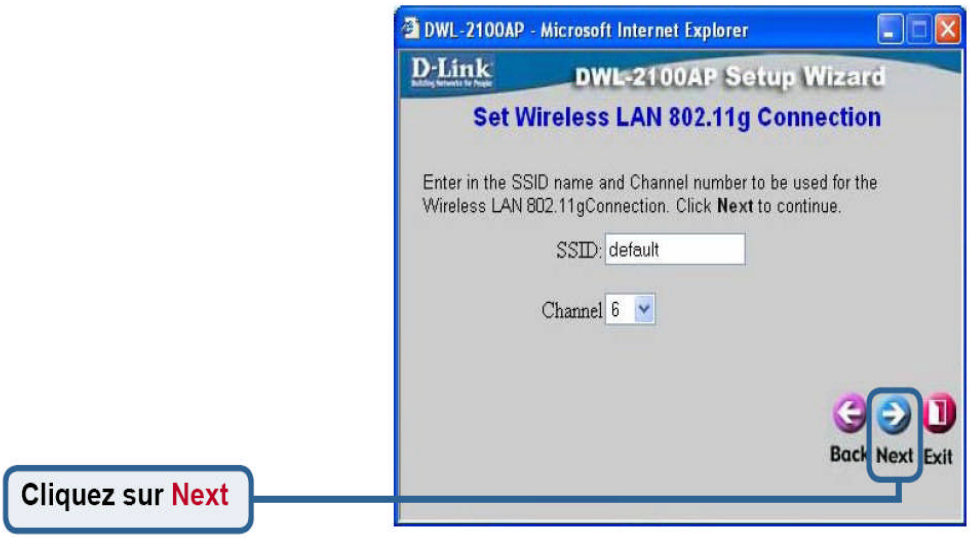
Étape 2 – Paramétrage de la connexion sans fil

Les paramètres de connexion sans fil par défaut sont :

SSID = **default**

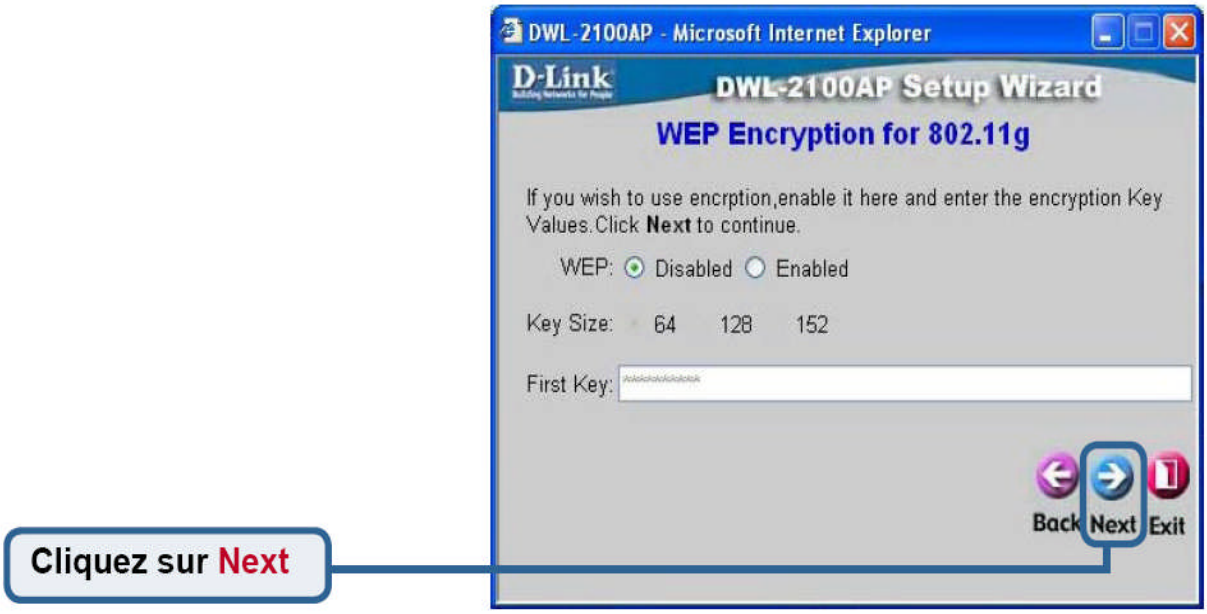
Channel = **6**

Vous pouvez modifier ces paramètres pour les adapter à un réseau sans fil existant

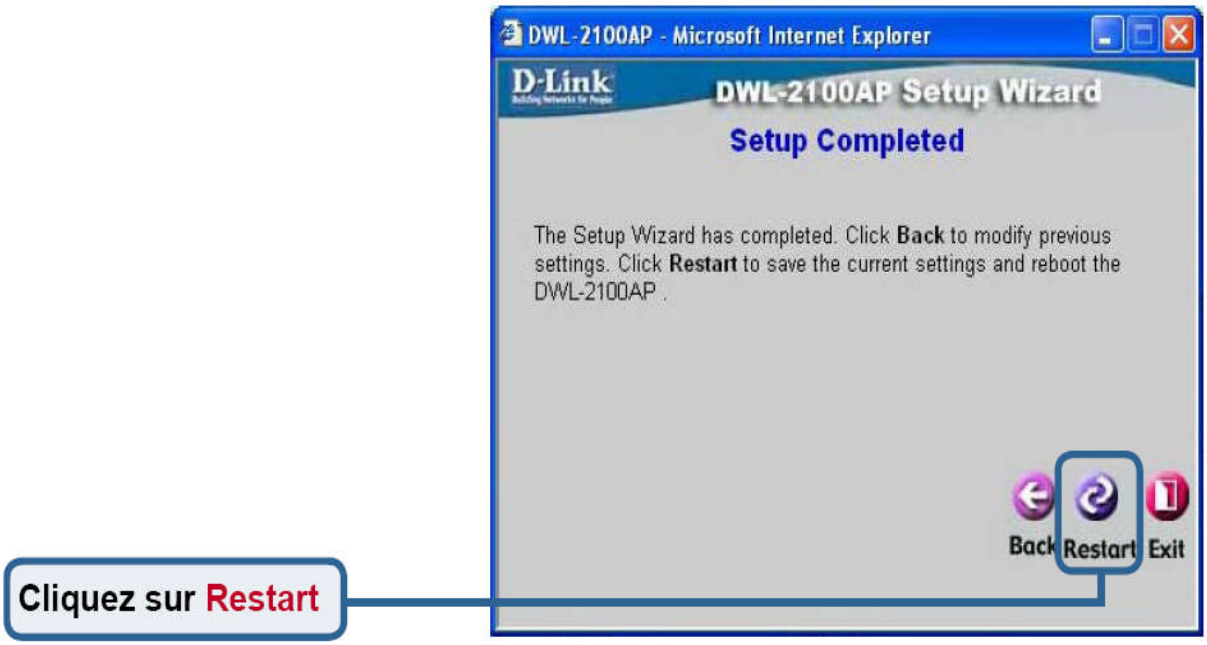


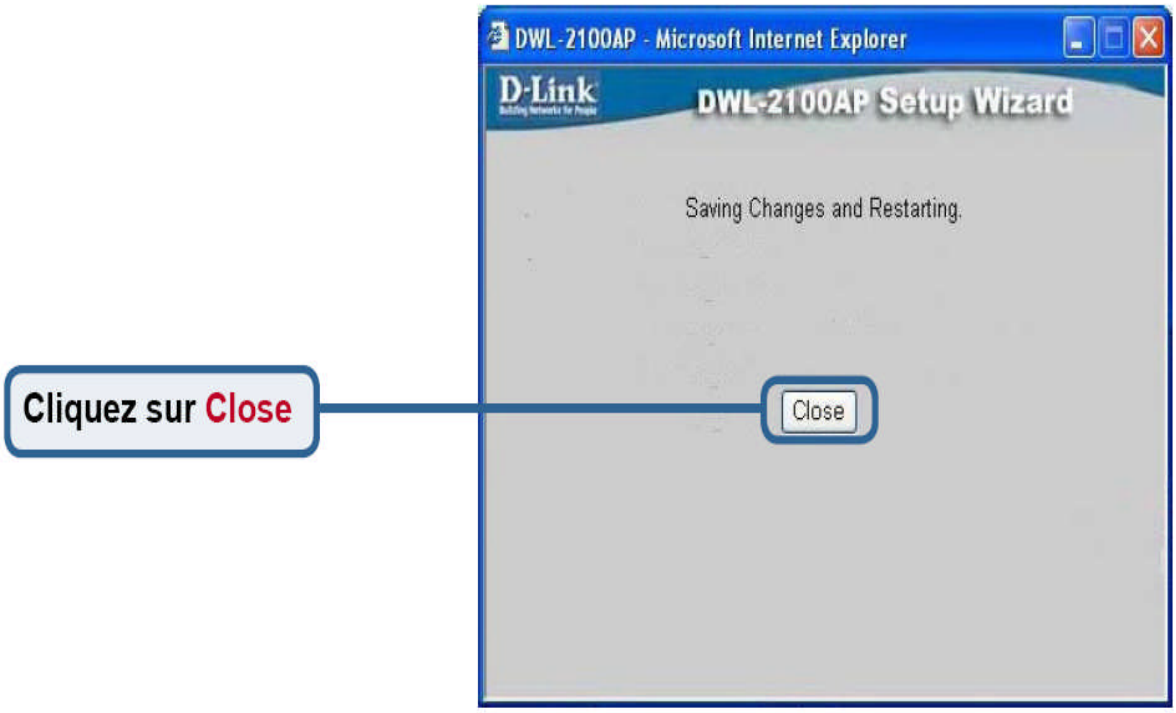
Étape 3 - Cryptage

Le DWL-2100AP autorise deux niveaux de cryptage radio –64 bits et 128 bits. **Par défaut, le cryptage est désactivé**. Vous pouvez modifier les paramètres de cryptage pour sécuriser les communications radio.

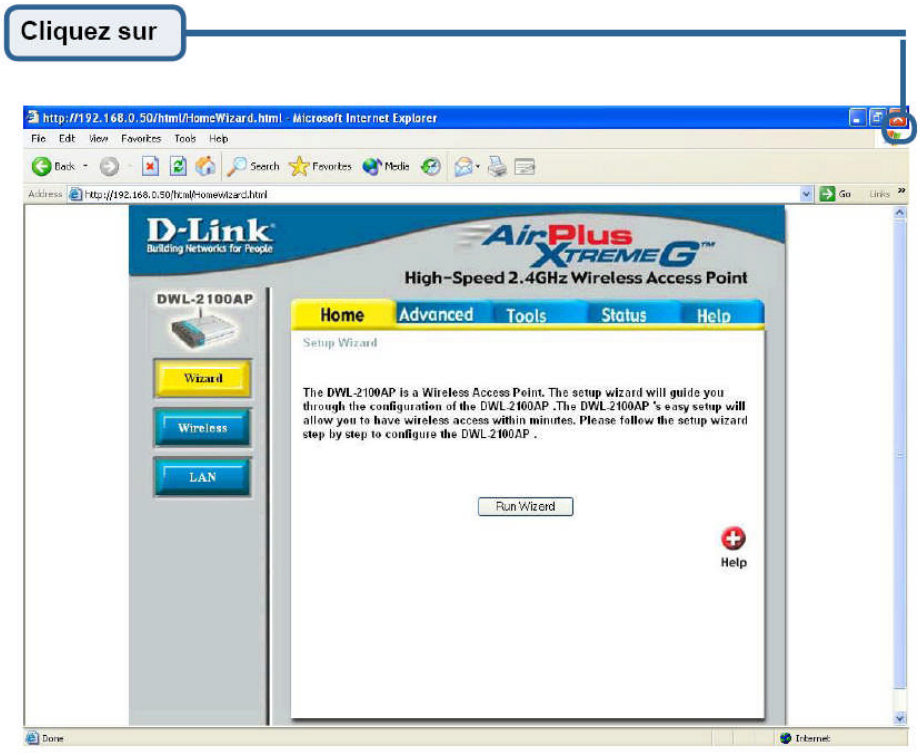


La configuration est terminée





Vous revenez à l'écran **d'accueil.**



Pour la définition d'autres paramètres ou pour des informations supplémentaires, utilisez les onglets **Advanced, Tools,** ou **Status**, ou bien reportez vous au manuel qui se trouve sur le CD ROM.

2. Configuration de la sécurité du réseau à travers le point d'accès (DWL-700AP) :

Configuration de la sécurité de réseau WIFILET a travers le point d'accès DWL-700AP

Après l'installation et la configuration de point d'accès, en opte à activer les options de sécurité

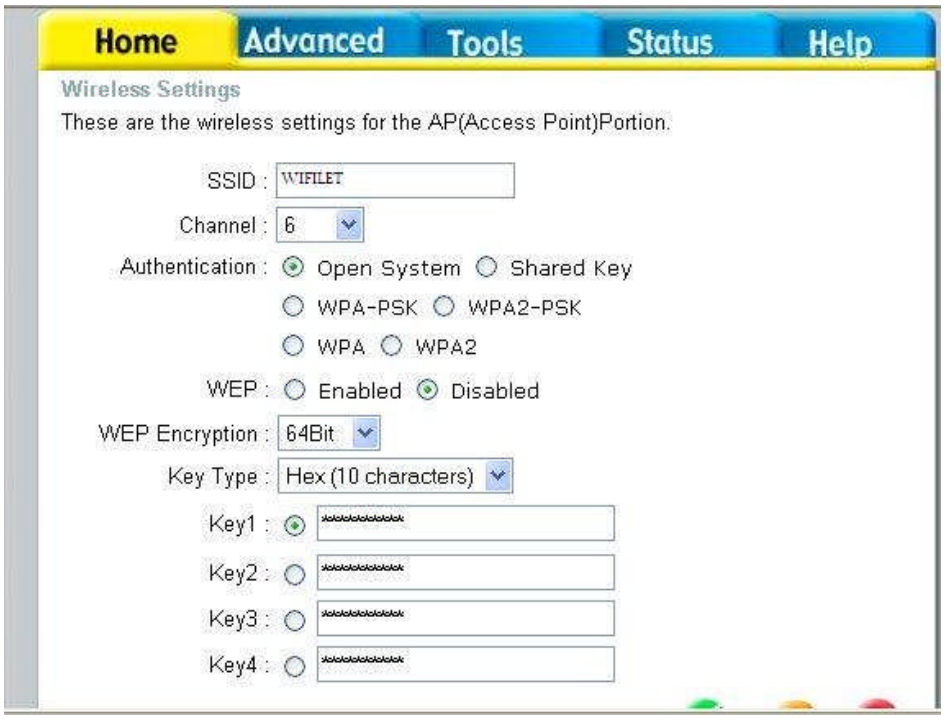
Les points d'accès ont une configuration de base non sécurisée est connue par défaut, pour cela, le premier moyen de sécurité qu'on établit est de changer le nom du point d'accès et le mot de passe

Changer l'adresse IP du point d'accès, en le saisi manuellement

Il est préférable de cacher le nom du réseau sans fil en désactivant SSID, en cliquant sur **Disabled** et pour les clients, ils doivent le saisir manuellement chacun sur sa machine.

La configuration se fait sur la carte réseau en cliquant sur

Propriété>configuration>SSID>ajouter>WIFILET>appliquer>affiché

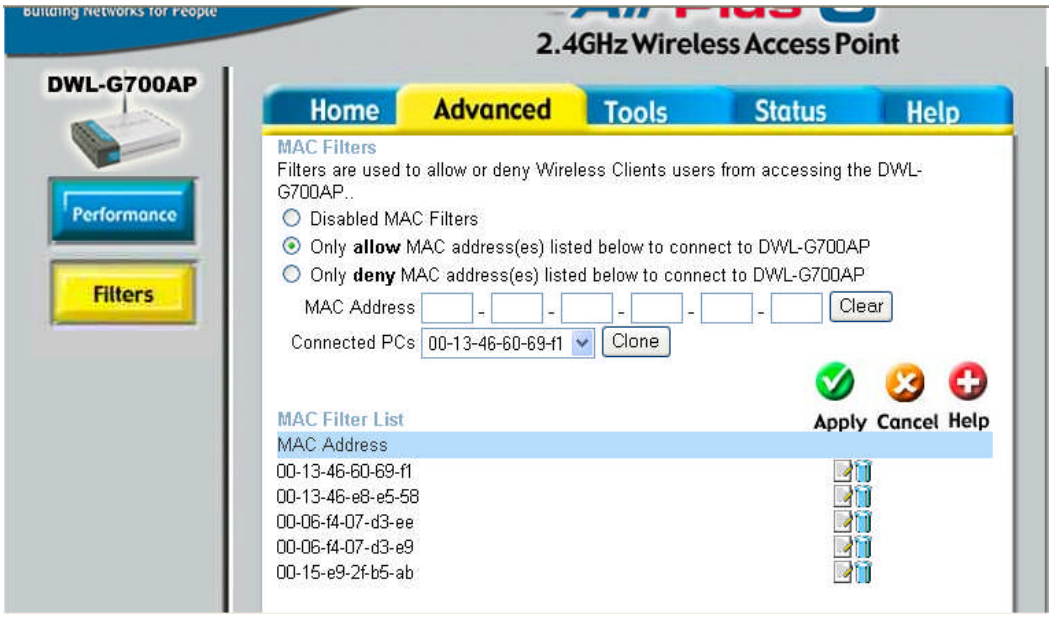


Ensuite on passe au filtrage des adresses MAC, après le recensement des postes de chaque PA

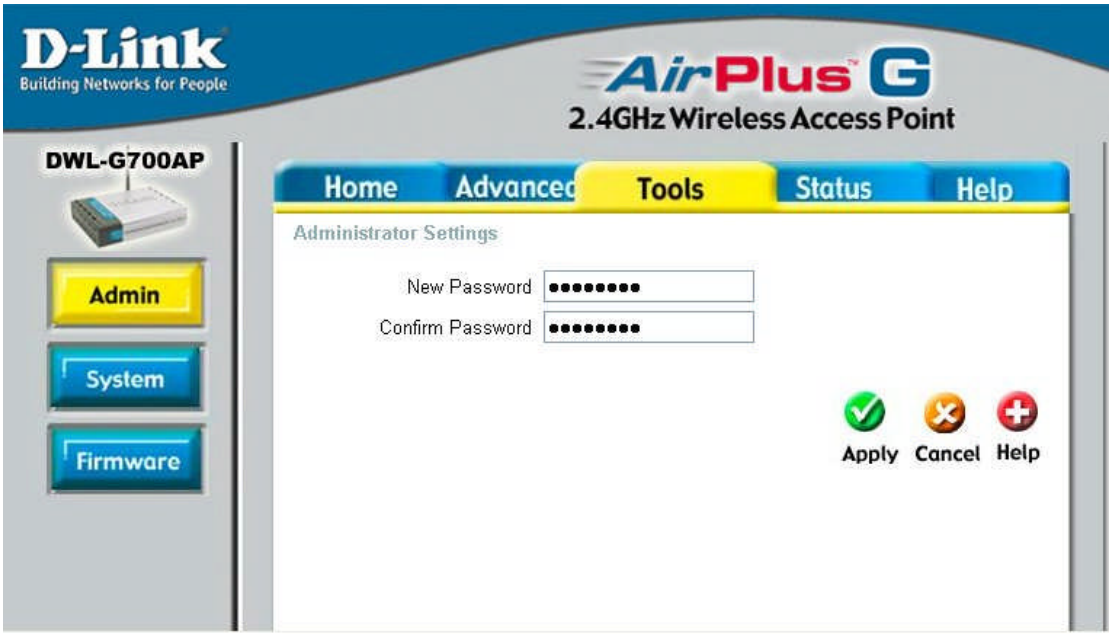
Comment filtrer les adresses MAC :

Cliquer sur **HOME >Advenced>Filtre option**

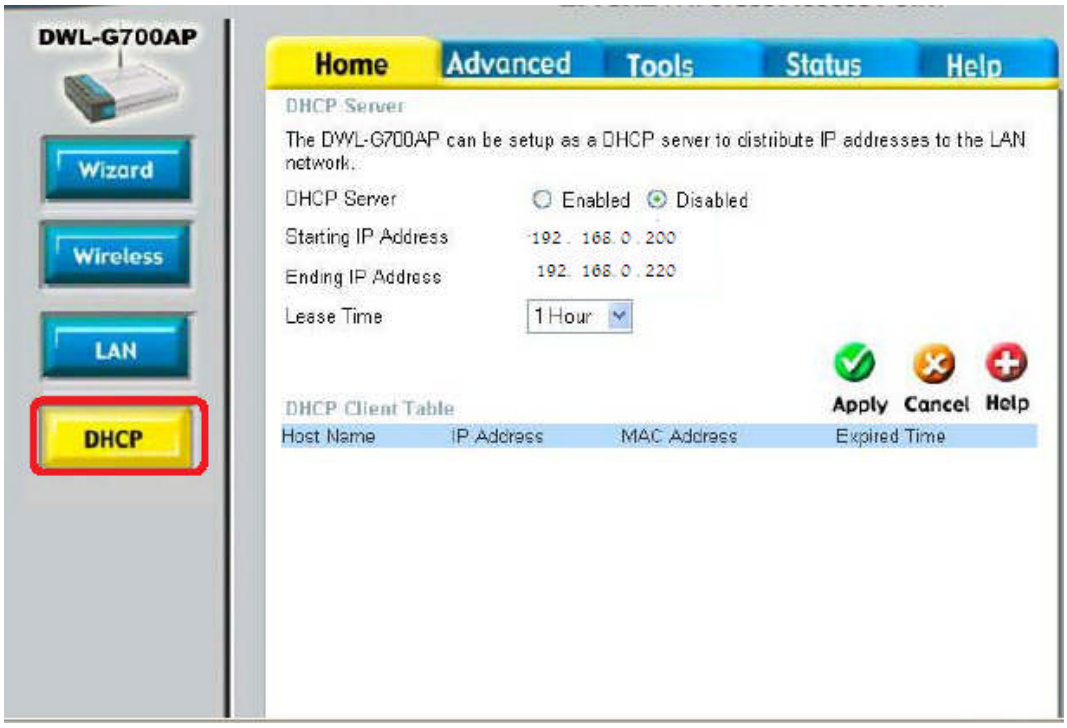
Only affiche les adresses MAC qui sont connectés au PA, on choisi les adresses **MAC** qu'on veut filtrer puis **clone>apply>continuer**



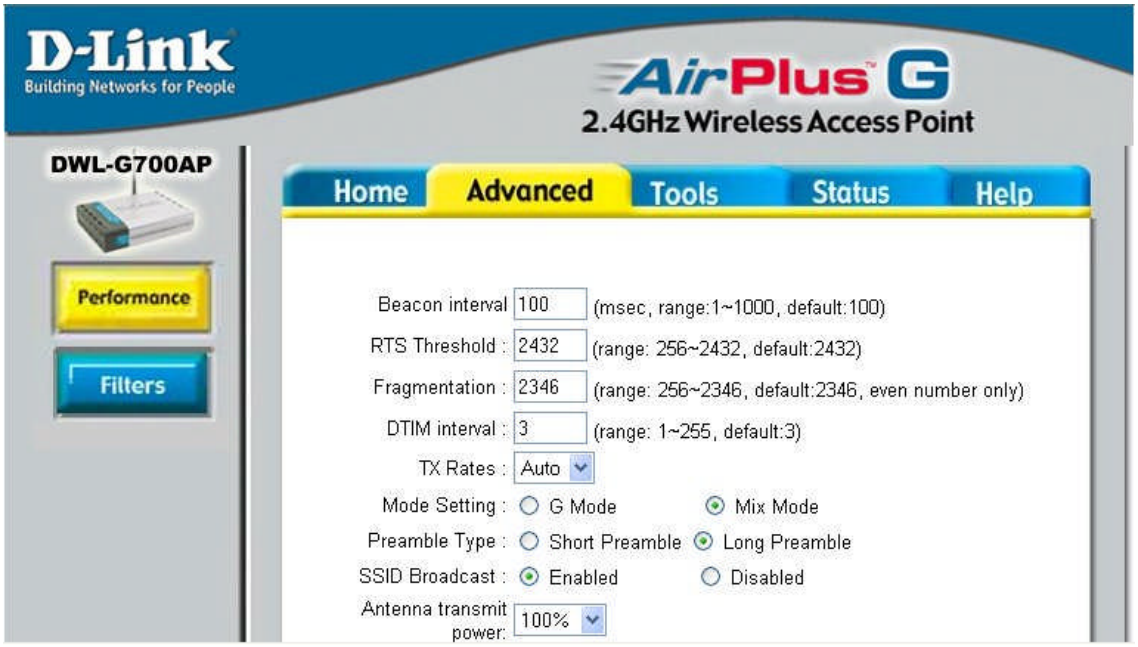
Dans cette fenêtre on clique surTools>Admin pour changer et confirmer le nom de la passerelle



Il est préférable dans les réseaux sans fil de désactiver le **DHCP**

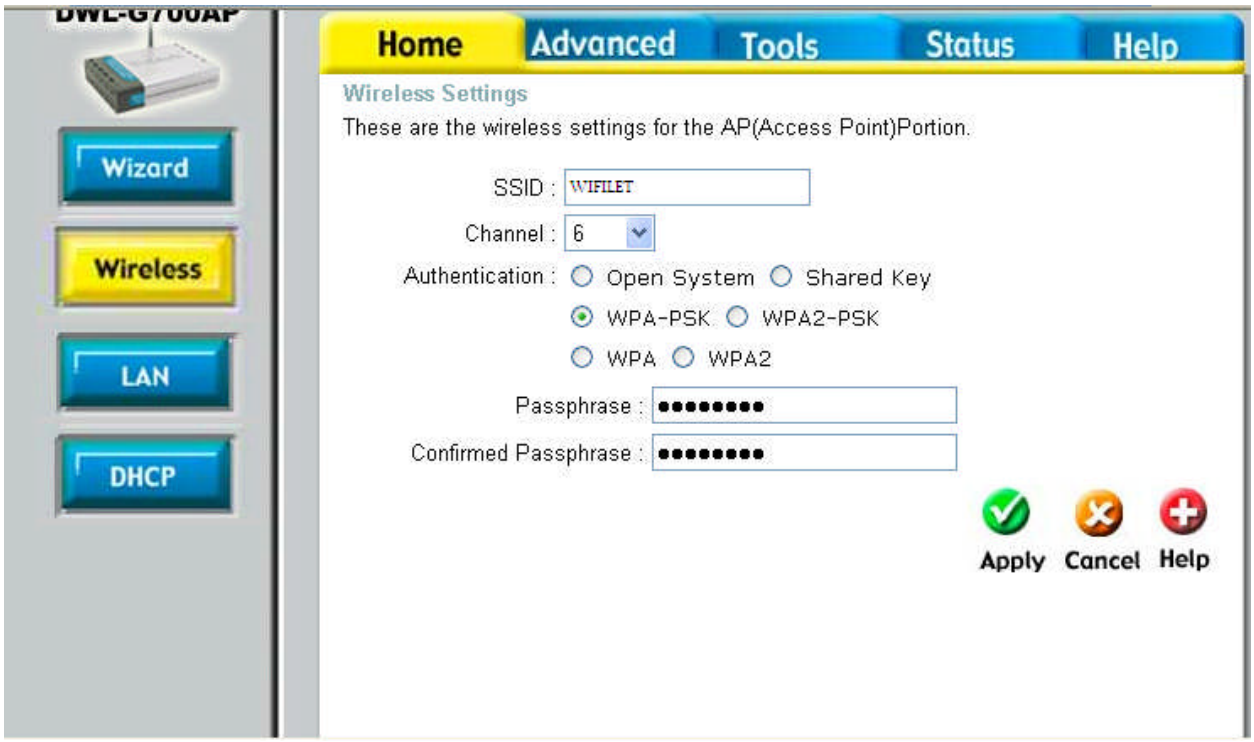


Pour diminuer les fréquences du PA, il est préférable de diminuer l'intensité de transmission des ondes de no PA pour assurer que la connexion de notre réseau (limité les liens de Baliage)



Activation de la clé WAP-PSK comme suit :

Home>Wireless>WAP- PSK>Enable>WAP encryption puis saisi le mot de passe



Conclusion

Ce chapitre a fait preuve de montrer et d'expliquer la configuration et les différents types des points d'accès et étapes à suivre pour leur connexion ainsi que la configuration de la sécurité d'un réseau à travers le point d'accès (DWL-700AP).

CHAPITRE IV: MISE EN PLACE DE LA PLATE FORME DU RESEAU WIFI INPED

INTRODUCTION :

Comme il a été déjà cité en introduction générale l'objectif de notre mémoire est de mettre en place une plate-forme basée sur le concept wifi afin d'exploiter au maximum les avantages de ce dernier.

Vu l'inexistence d'un réseau filaire au niveau du nouveau bloc de l'INPED d'une part et le faible débit de la connexion actuelle (512 KO/s) au niveau du bloc pédagogique d' autre part nous avons propose de mettre en place une plate-forme WIFI. Cette dernière pouvant être reliée au réseau du bloc pédagogique auquel on rajouté un point d'accès.

Notre plate-forme assure le partage de la connexion Internet haut débit 2Mbits/s entre deux blocs de l'INPED.

Dans ce qui suit nous allons présenter les différentes étapes pour la réalisation de cette plate-forme

1. Plate-forme de la réalisation pratique :

1.1- Equipements utilisés :

Le réseau sans fil installé comporte vingt postes qui sont définis comme suit :

1. douze micro-ordinateurs .

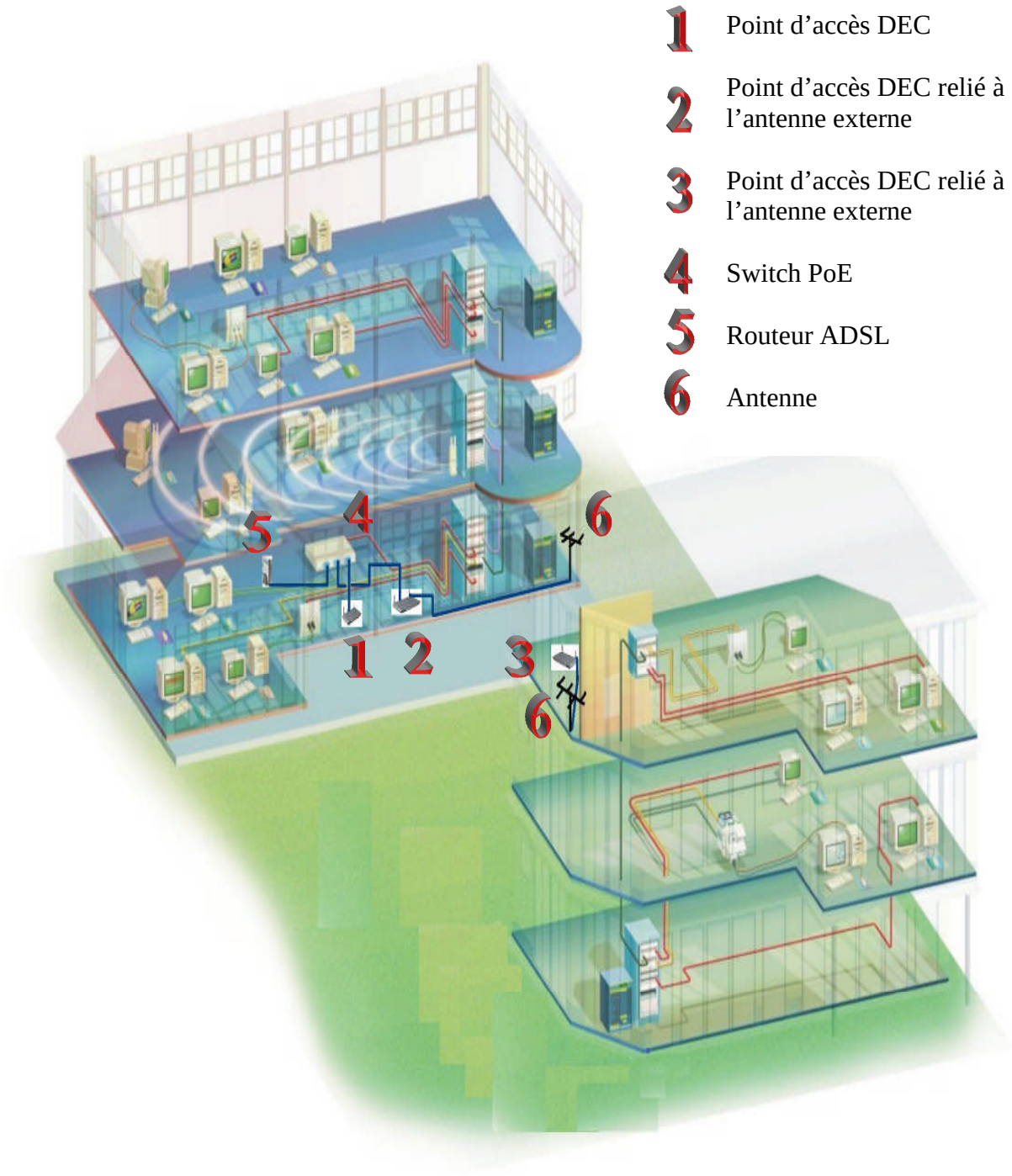
Les postes clients équipés de :

- Microprocesseur Pentium IV 3.00 GHZ.
- 992 Mo de mémoire RAM.
- Disque dur Western Digital de capacité 80 Go.
- Cartes réseaux wirlless (sans fil) de marque D-LINK- DWA –120 USB.

2. 08 Micro portable.
3. Trois point d'accès DWL 3200 AP.
4. Un switch 24 ports Power over Ethernet (PoE) CISCO 296024PCL .
5. Un modem (pour se connecter a Internet) de marque CISCO.
6. Deux imprimantes.
7. Routeur.

1.2- Installation physique du Réseau sans fils :

La structure ci-dessous nous montre l'architecture de la plate forme WIFI réalisé à l' INPED



l'opération de l'installation du réseau WIFI à suivi deux phases distinctes, la première à été définie au sein de le direction des études et du conseil ou une étude préalable des lieux nous à permis de dégager le type,qualité et nombre d'accessoires à installer pour la mise en exploitation.

Le besoin d'information au sein de la DEC nécessite une connexion Internet haut débit qu'il fallait partager entre les différents utilisateurs à travers un réseau WIFI sécurise.

Cette première configuration de base gravite au tour d'un routeur ADSL qui nous permet d'avoir une connexion internet.

La dite configuration est composée de deux points d'accès D-LINK DWA 3200 AP.

A. Pour quoi ce choix ?

Parmi les caractéristiques de ce type de point d'accès est que son alimentation est réalisé par le câble réseau RJ45 par l'intermédiaire d'un switch PoE d'une part, d'autre part nous trouvons un ensemble de caractéristiques tel que :

- il accepte le réseau VPN
- le rapport qualité prix
- il est dote de l'aspect d'authentification WPA2 .

L'alimentation électrique des différents points d'accès est réalisée grâce au switch PoE (Power over Ethernet) installé au niveau de la DEC.

Nous constatons que le switch est doté de 8 sorties RJ45 dont 4 PoE.

La deuxième phase consiste à réaliser une extension du réseau WIFI DEC vers le bâtiment de le DEP. En d'autre terme, émettre le signal radio électrique d'un des points d'accès de la DEC vers le point d'accès récepteur émetteur de la DEP.

B. Quelle est l'approche pratique ?

Entre les deux bâtiments nous constatons une distance de 30 mètres qui a nécessite l'installation de deux antennes pour réaliser la liaison radio électrique entre les deux points d'accès, les deux antennes sont des metteurs récepteurs de signal.

Après ces deux phase des la mise en place de ces équipements, l'aboutissement logique et la mise en exploitation réelle du réseau WIFI. Ceci est réalisé à travers une configuration software qu'il faut opérer au niveau des différents points d'accès.

Tout routeur ou point d'accès dispose d'un logiciel intégré de la configuration, même les petits routeurs domestiques fournis par ALGERIE TELECOM.

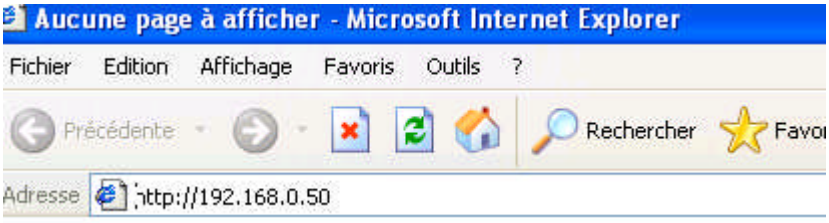
1.3- Installation Logique (Configuration du Point d'Accès) :

Une fois le point d'accès installé, il doit être configuré pour l'exploitation.

Il existe deux manières de paramétrer le point d'accès :

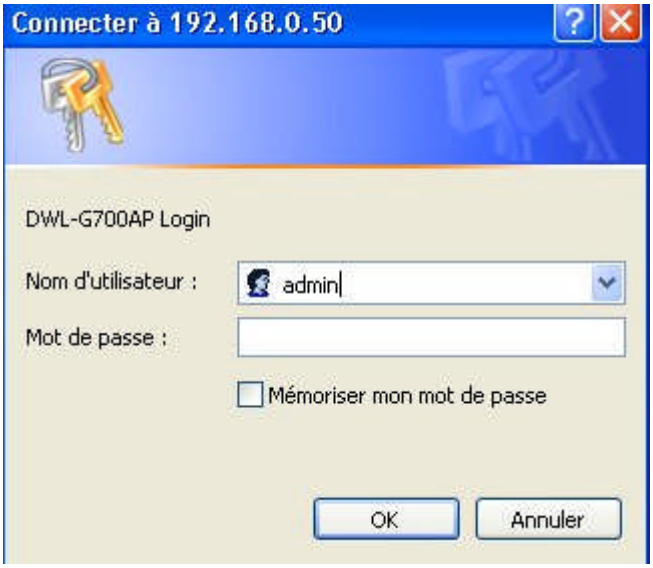
- Via un utilitaire : en utilisant un CD-ROM fournit dans le package
- Via un configurateur Web : en utilisant une adresse http:/ fournit dans le manuel d'utilisation de l'équipement.

En double cliquant sur un navigateur Web (Internet explorer), on saisi l'adresse par défaut, fournit avec le point d'accès WI-FI qui est : http:/ 192.168.0.50 par laquelle on va accéder au software du point d'accès.



On aura la fenêtre suivante qui comporte une boite de dialogue qui va nous demander d'insérer un nom d'utilisateur et un mot de passe.

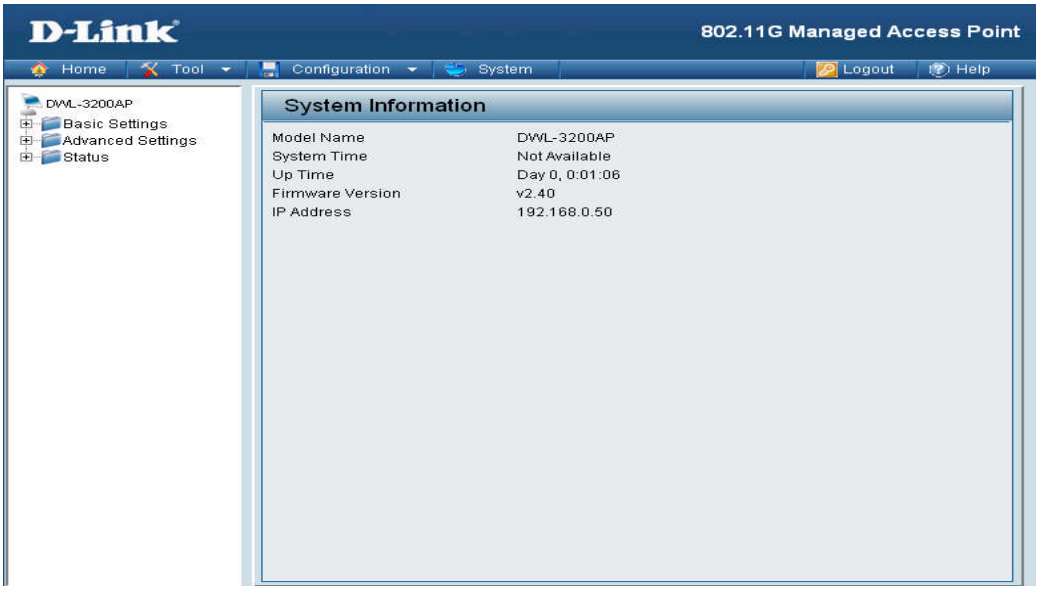
Le nom d'utilisateur par défaut est « Admin. » et le mot de passe est aussi par défaut « Admin. » et ils sont changeables par mesure de sécurité.



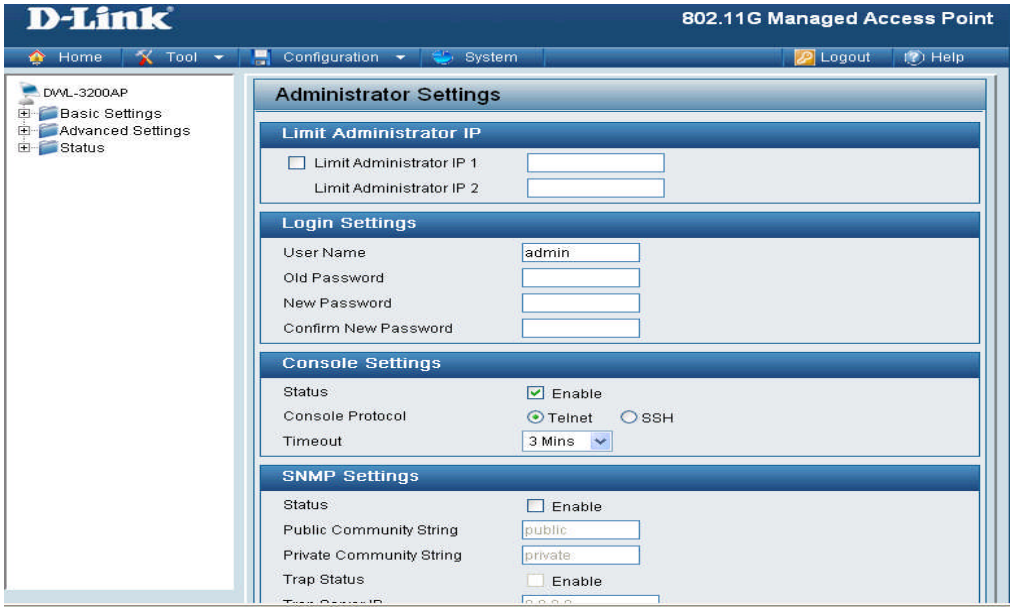
On cliquant sur **ok** on aura le software du point d'accès qui s'affiche comme une page Web sur laquelle il y'a ses paramètres de configuration.

Cette page comporte plusieurs rubriques comme **Home, Tool , Configuration, System** qui contiennent des informations sur le paramétrage du point d'accès.

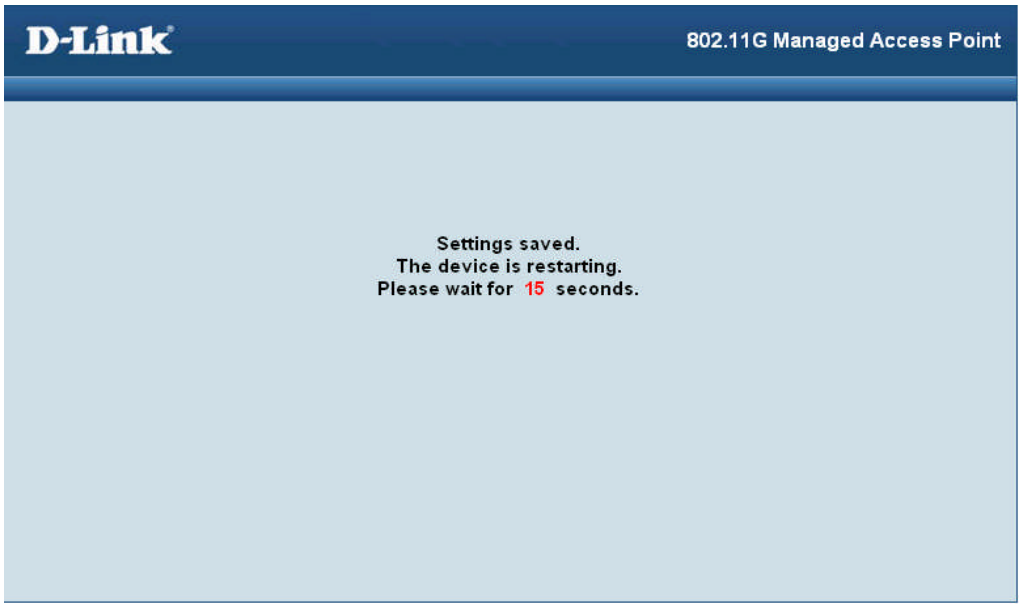
Dans Home en trouve les renseignements sur le point d'accès tel que le nom , la version du programme , l'adresse IP par défaut.



Dans le menu tool en trouve administrator settings la ou en peut changer le nom et le mot de passe du point d'accès.

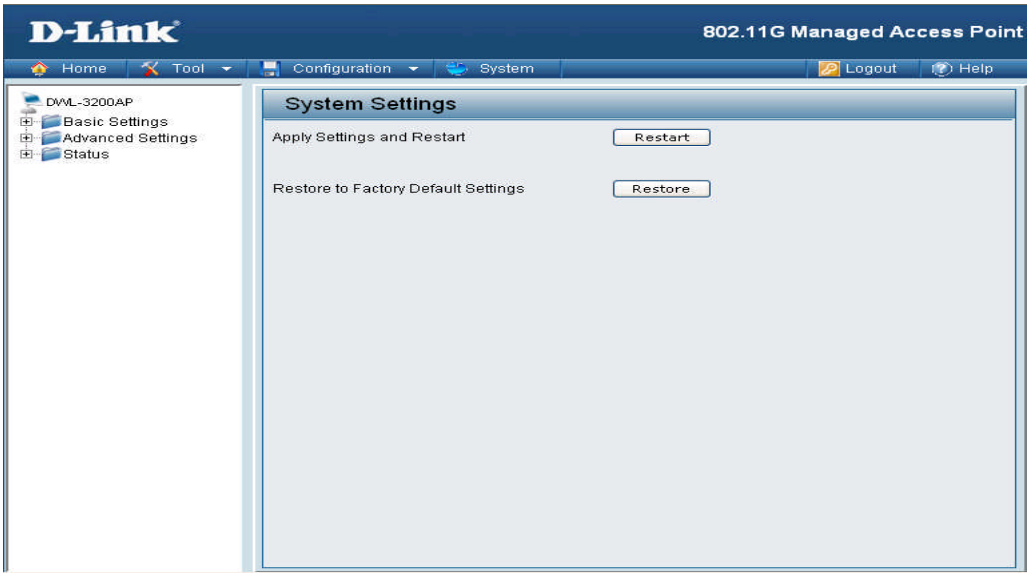


Dans le menu configuration on sauvegarde et active les changements qui en été faits.



Dans le menu system en trouve restart pour rebouter le point d'accès tout en sauvegardant les changements.

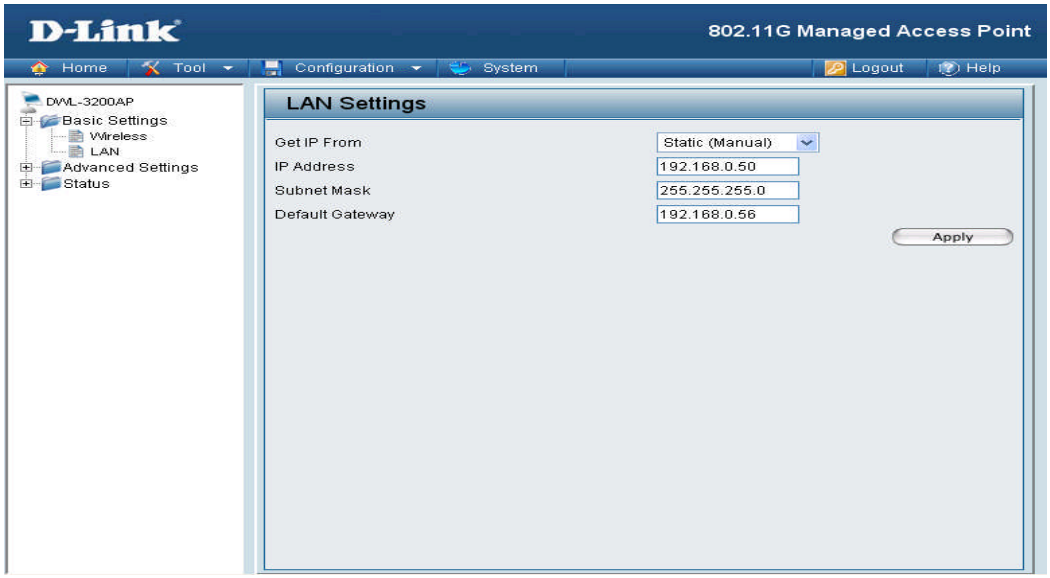
Restore c'est pour restaurer les paramètres par défaut (usine) du point d'accès.



En trouve dans le menu vertical Basic settings, Advenced settings et statut.

Dans basic settings en trouve :

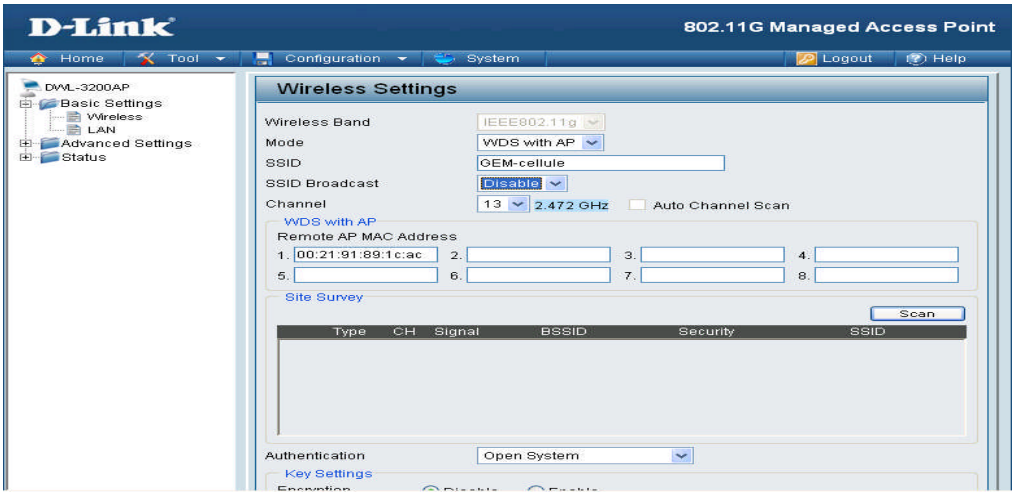
- Wireless : on peut changer le nom du point d'accès, le mode de fonctionnement et le canal de transmission.
- LAN : pour changer l'adresse IP du point d'accès.



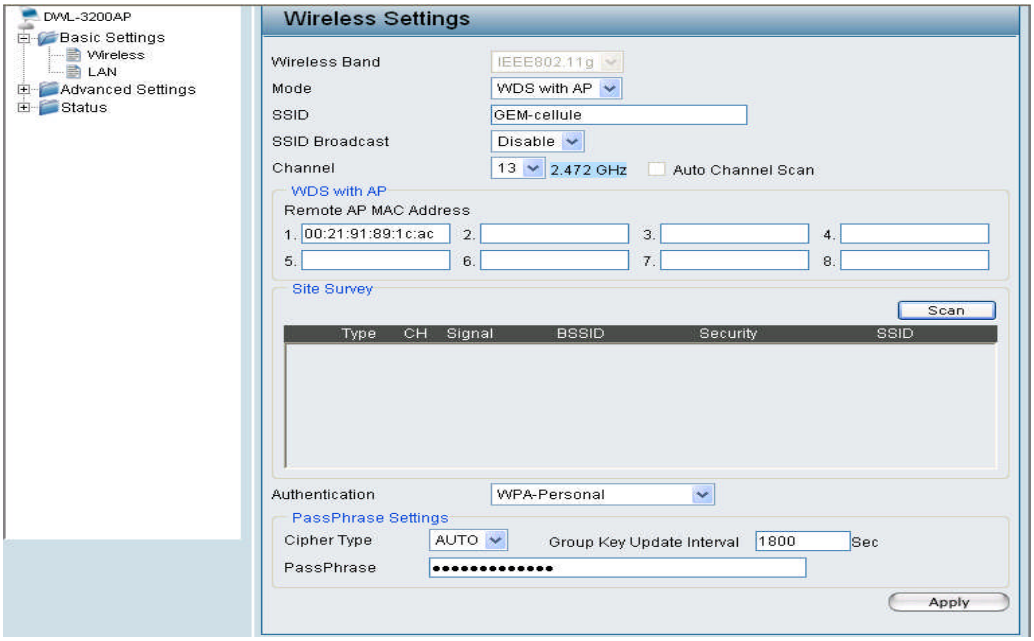
Parmi les étapes utilisées pour sécuriser le réseau c'est :

- Eviter les paramètres par défaut.
- Cacher le réseau sans fil.
- Filtrage par adresse Mac.
- Utiliser l'authentification WPA ,WPA2

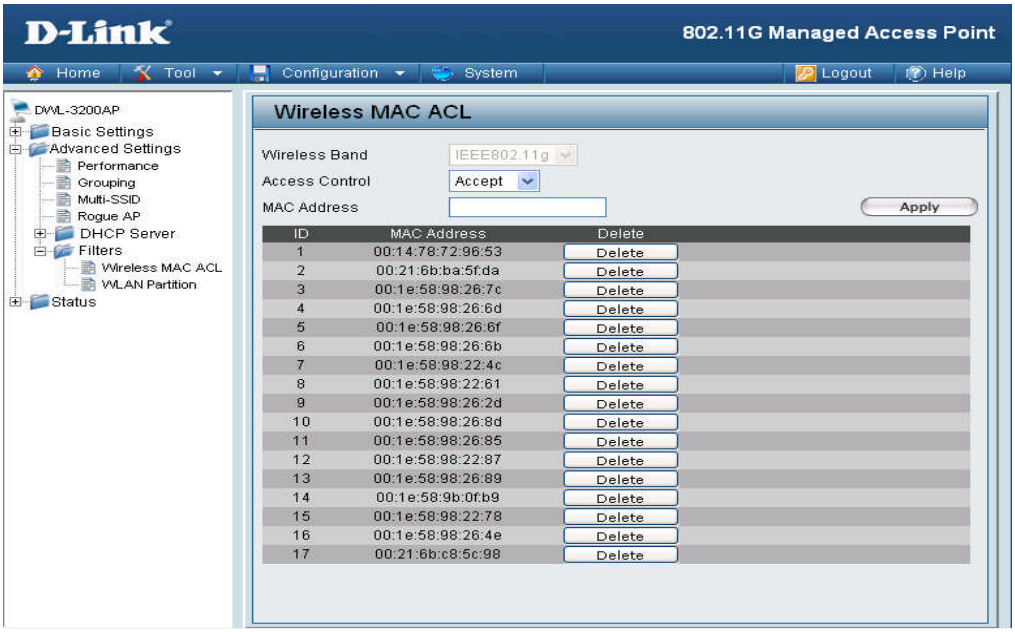
Dans notre cas en remarque q'on a changé SSID D-LINK qui est par défaut par GEM-cellule. On a aussi caché le réseau en mettant le SSID en Disable comme le montre la figure suivante.



Il y'a aussi l'authentification WPA OU WPA2 comme le montre la figure suivante.



Et en fin le filtrage par adresse MAC .

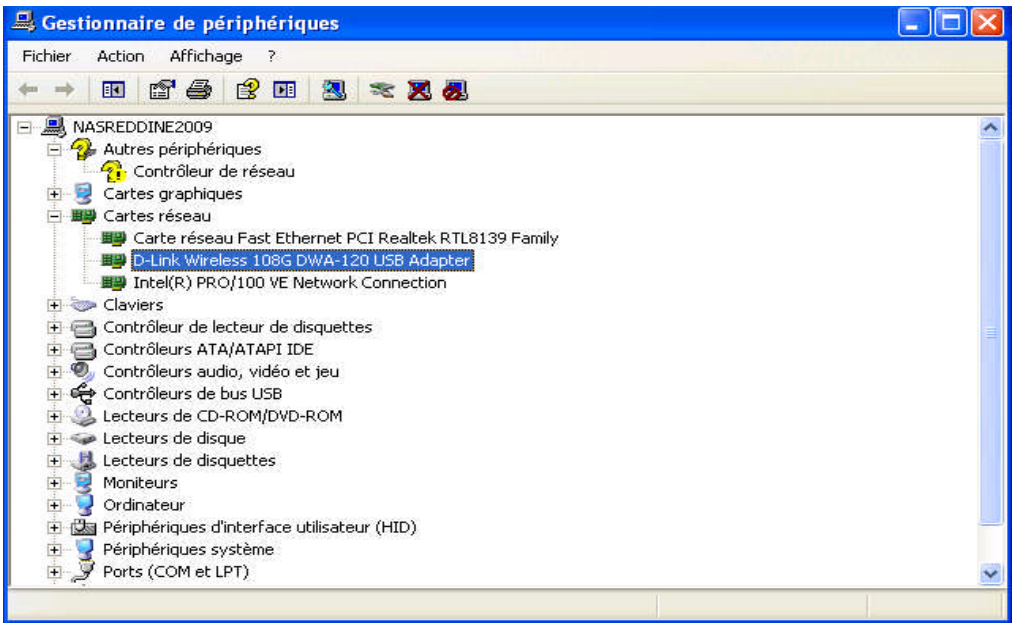


1-4 Connexion d'un poste

1.4.1- Installation de la Carte Réseau sans fil :

Tout d'abord, on installe la carte réseau sans fil physiquement en l'insérant dans son emplacement pour notre cas c'est une carte réseau WIFI USB.

Comme tous périphériques, la carte réseau sans fil est détectée par le système d'exploitation puis on installe son pilote. Pour qu'elle soit opérationnelle.



1.4.2- l'attribution des a dresses IP des postes de Travail :

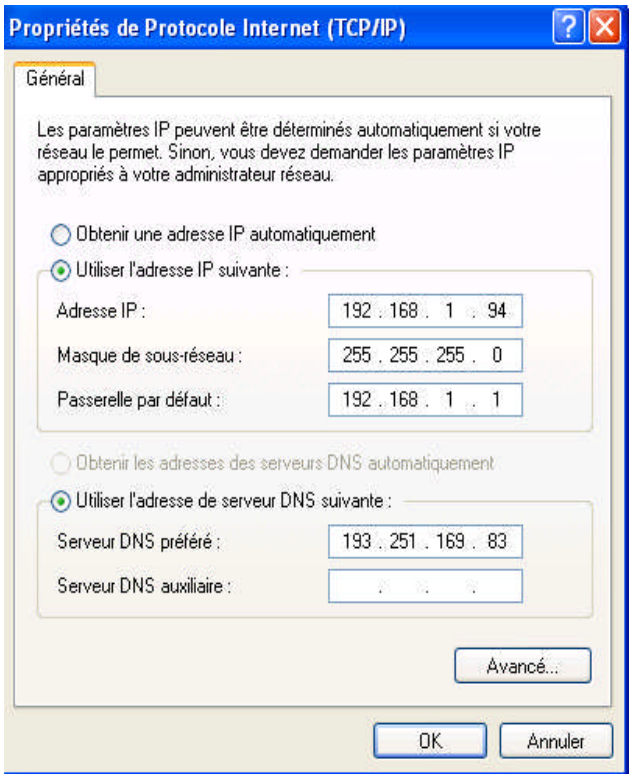
On attribue d'une manière statistique les différentes adresses IP des postes de travail, qui se fait de la même manière que pour une carte réseau câblé.

En cliquant avec le bouton droit de la souris sur l'icône de favoris réseau située sur le bureau, son menu s'affiche et on clique sur **propriétés** sur la prochaine fenêtre on clique sur l'icône de connexion réseau local on aura la fenêtre suivante.

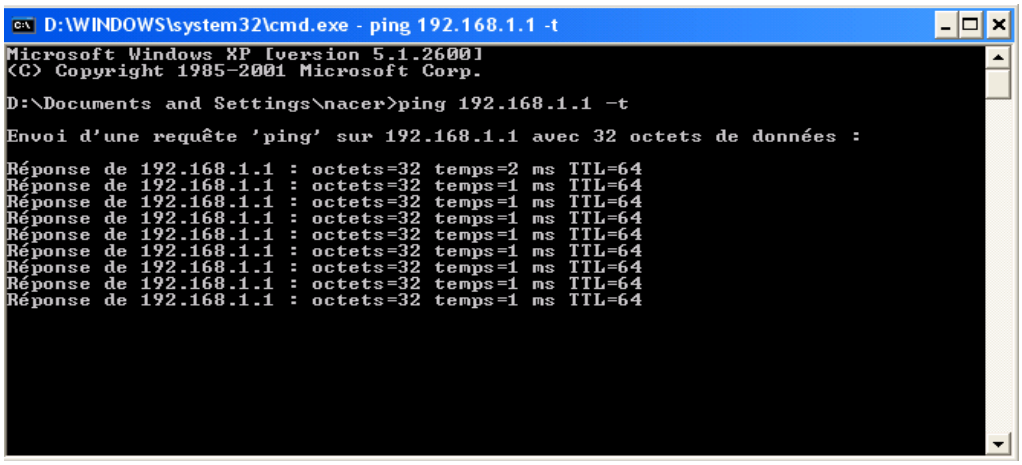
En cliquant sur **protocoles Internet TCP/IP** on aura la boite de dialogue suivante

On saisi l'adresse IP statique du poste avec un masque de sous réseau, la passerelle par défaut qui est l'adresse IP du routeur ADSL et en fin le DNS.

Après on clique sur **OK** pour confirmer la configuration de la carte réseau.

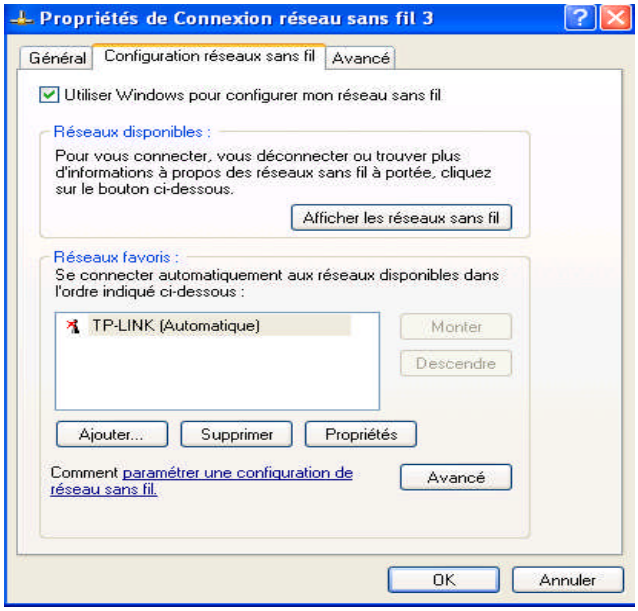


Un ping est indispensable pour vérifier la connexion entre se poste et le routeur

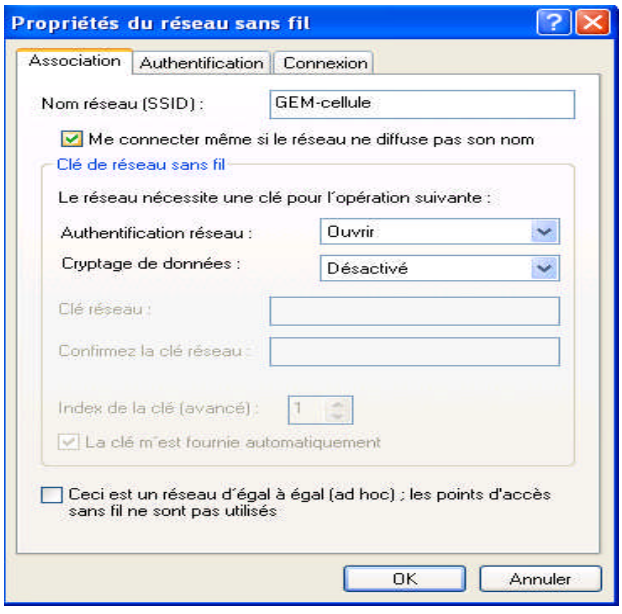


Si le réseau est cache et si un nouveau client veut accéder a ce réseau il faut qu'il connaisse le SSID du réseau, puis il crée le réseau comme suit.

Dans propriétés de connexion configuration réseau sans fil



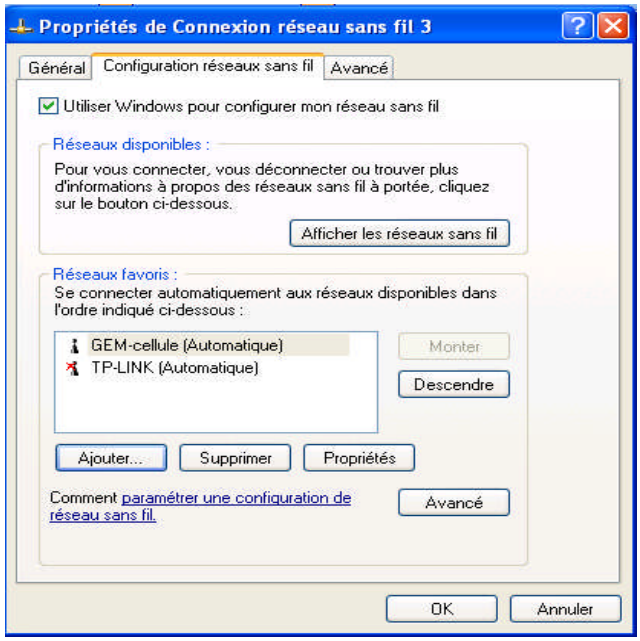
En clique sur ajouter et en introduit le SSID du réseau, cocher la case me connecter même si le réseau ne diffuse pas son nom, en spécifie l'authentification réseau et en fin le cryptage de données



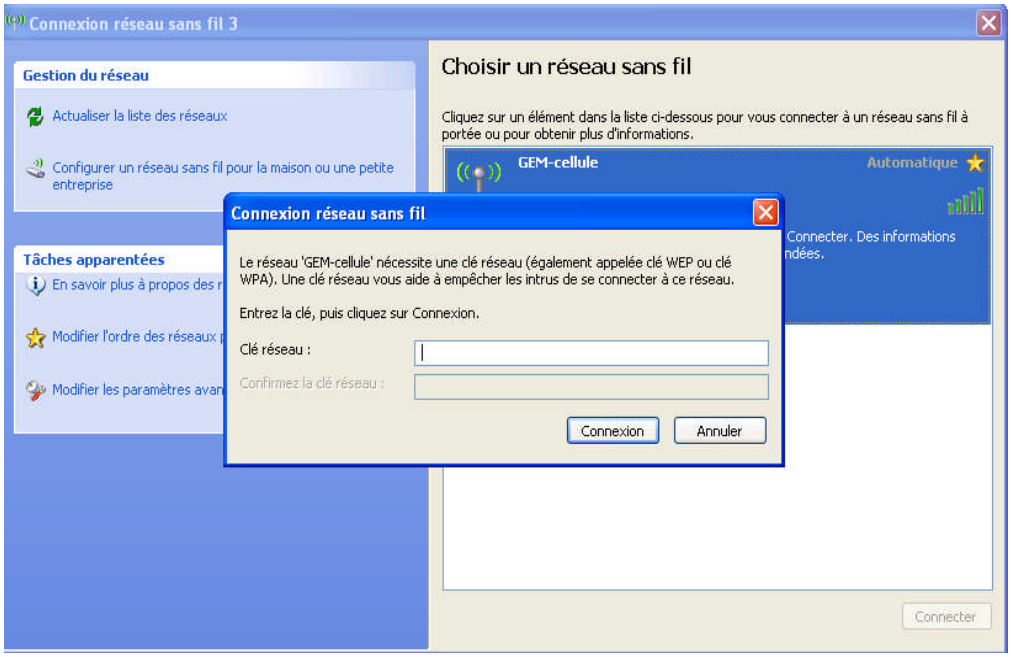
On clique sur ok et on a la fenêtre suivante

On remarque que le nom GEM-cellule a été ajouté aux réseaux favoris.

A partir de là le réseau sera affiché dans la liste des réseaux sans fil.



Dans le cas ou le réseau est sécurisé avec WPA ou WPA2 le client doit entrer la clé réseau pour se connecter comme le montre la figure suivante.



2. Configuration d'un routeur

```
RTR-INPED#show running-config
Building configuration...

Current configuration : 6083 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RTR-INPED          ---NOM du routeur -----
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
aaa new-model
!
!
aaa authentication login default local
!
aaa session-id common
!
resource policy
!
clock timezone GMT+1 1
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
!
```

```
username bmbadmin privilege 15 password 7 0822455D0A16  --- acces du routeur --------
!
!
ip dhcp pool INPED                                  ---------------- DHCP SERVER ---
  network 192.168.110.0 255.255.255.0                 ------ le reseau de INPAD -------
  default-router 192.168.110.250                      ---- la passerell par default
  dns-server 192.168.0.7 193.251.169.165 80.249.75.23  ------ le DNS ----
!
!
!
!
interface FastEthernet0/0                   ------ Configuration de l'interface connecté avec huawi----
 description CONNECTED TO ADSL CONNECTION               ----Description--------
 no ip address                                  ----------pas d'adress ip ---
 duplex half
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
!
interface FastEthernet0/1                   ------ Configuration de l'interface connecté avec le Switch----
 ip address 192.168.110.250 255.255.255.0               ------ Ip du lan la passerell du lan -----
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!

interface Dialer1    -- interface virtuel connexion PPPOE -- point to point protocol over ethernet -
 ip address negotiated                          -------- ip nogociale ------------
 ip mtu 1492                                    ----------- parametre de Djaweb
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
```

```
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname 565487
 ppp chap password 0 oucherif
 ppp pap sent-username 565487 password 0 oucherif
!
ip classless
!
ip http server
ip http authentication local
ip http secure-server

ip nat inside source list 130 interface Dialer1 overl    --- commande du nat avec acces list 130 ----
!
access-list 130 permit ip any any                    ---- le trafic permi du nat ------

!
!
!
control-plane
!
!
banner exec ^CC
You are logged into line $(line) of $(hostname)

^C
banner login ^CC




^C
banner motd ^CC                    -------- ecran qui s'affiche a la connection du routeur ----------
-
```

```
==================================================
| The equipment now being accessed and information available through |
| this equipment is confidential and proprietary. It may be accessed |
| or used only as specifically authorized. All other access or use |
| is prohibited and is subject to legal action! |
==================================================
^C
!
end
```

3. Configuration de Switch

```
switch-INPED#sho run
Building configuration...

Current configuration : 2764 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch-INPED
!
boot-start-marker
boot-end-marker
!
!
username bmbadmin privilege 15 password 0 cisco
!
!
aaa new-model
!
```

```
!
aaa authentication login default local
!
!
!
aaa session-id common
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
ip routing
ip domain-name airalgerie.dz
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2
 spanning-tree portfast
!
```

```
interface FastEthernet0/3
 spanning-tree portfast
!
interface FastEthernet0/4
 spanning-tree portfast
!
interface FastEthernet0/5
 spanning-tree portfast
!
interface FastEthernet0/6
 spanning-tree portfast
!
interface FastEthernet0/7
 spanning-tree portfast
!
interface FastEthernet0/8
 spanning-tree portfast
!
interface FastEthernet0/9
 spanning-tree portfast
!
interface FastEthernet0/10
 spanning-tree portfast
!
interface FastEthernet0/11
 spanning-tree portfast
!
interface FastEthernet0/12
 spanning-tree portfast
!
interface FastEthernet0/13
 spanning-tree portfast
!
interface FastEthernet0/14
```

```
 spanning-tree portfast
!
interface FastEthernet0/15
 spanning-tree portfast
!
interface FastEthernet0/16
 spanning-tree portfast
!
interface FastEthernet0/17
 spanning-tree portfast
!
interface FastEthernet0/18
 spanning-tree portfast
!
interface FastEthernet0/19
 spanning-tree portfast
!
interface FastEthernet0/20
 spanning-tree portfast
!
interface FastEthernet0/21
 spanning-tree portfast
!
interface FastEthernet0/22
 spanning-tree portfast
!
interface FastEthernet0/23
 spanning-tree portfast
!
interface FastEthernet0/24
 spanning-tree portfast
!
!
ip classless
```

```
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 0 4
 exec-timeout 60 0
 privilege level 15
 logging synchronous
line vty 5 15
!
end
```

CONCLUSION :

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

L'implémentation d'un réseau Wi-Fi se heurte souvent aux exigences imposées par les réglementations établies pour l'utilisation des bandes de fréquence. A ces contraintes, viennent s'ajouter la nécessité d'une très bonne planification cellulaire basée sur un choix judicieux de l'emplacement des différents points d'accès avec une bonne répartition des canaux utilisés. Ceci permet de réduire au maximum les possibilités d'interférences et garantit, en conséquence, de meilleures performances du réseau.

CONCLUSION GENERALE

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

La non interopérabilité entre les différentes normes Wi-Fi pose un grand problème de compatibilité entre les équipements. Ainsi une bonne connaissance des différentes normes et des fonctionnalités offertes. Et c'est justement l'analyse de ces différents paramètres qui justifient notre choix porté sur la norme IEEE 802.11g avec un point d'accès de type D-LINK DWA 3200 AP.

L'implémentation d'un réseau WI-FI se heurte souvent aux exigences imposées par les réglementations établies pour l'utilisation des bandes de fréquence. A ces contraintes, viennent s'ajouter la nécessité d'une très bonne planification cellulaire basée sur un choix judicieux de l'emplacement des différents points d'accès avec une bonne répartition des canaux utilisés. Ceci permet de réduire au maximum les possibilités d'interférences et garantit, en conséquence, de meilleures performances du réseau.

Nous tenons également à dire que l'implémentation que nous avons proposé peut être améliorée. Un suivi de ce projet permettra de vérifier le rayonnement tout autour de l'institut grâce à des équipements. Il serait aussi intéressant, une fois la puissance ajoutée, de déterminer les débits disponibles à la limite des différentes cellules afin de procéder à un plus grand recouvrement de ces cellules ou à la mise en place des nouveaux points d'accès si le débit s'avère faible.

Home
Basic Settings
Wireless Settings
Allow you to change the wireless settings to fit an existing wireless network or to customize your wireless network.

Wireless Band
IEEE 802.11g is supported and is backward compatible with IEEE 802.11b. This is for information only.

Mode
Select a function mode to configure your wireless network. Function modes include AP, WDS with AP and WDS. Function modes are designed to support various wireless network topology and applications. Select AP mode to create a wireless LAN. Select WDS with AP mode to wirelessly connect multi networks while still functioning as a wireless AP. Select WDS mode to wirelessly connect multi networks.

SSID
Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The factory default setting is "dlink". The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Broadcast
Indicate whether or not the SSID of your wireless network will be broadcasted. The default value of SSID Broadcast is set to "Enable", which allow wireless clients to detect the wireless network. By changing this setting to "Disable", wireless clients can no longer detect the wireless network and can only connect if they have the correct SSID entered.

Channel
Indicates the channel setting for the DWL-3200AP. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Auto Channel Scan
If you check Auto Channel Scan, the AP will automatically find the best channel to use. This is enabled by default.

Authentication
For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected. The default value for Authentication is set to "Open System".

- Open System:
For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

- Shared Key:
For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

- Open System/Shared Key:
With this setting both shared and open system are employed. Stations have the option of using either but must still have the correct key to decrypt data.

- WPA-Enterprise/ WPA2-Enterprise/ WPA-Auto-Enterprise:
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

- WPA-Personal/WPA2-Personal/WPA-Auto-Personal:
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. It uses TKIP encryption to protect the network through the use of a pre-shared key. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

LAN Settings
Also referred as Private settings. LAN settings allow you to configure LAN interface of DWL-3200AP. LAN IP address is private to your internal network and is not visible to Internet. The default IP address is 192.168.0.50 with subnet mask as 255.255.255.0 for DWL-3200AP.

Get IP From
The factory default setting is "Static (Manual)" which allows the IP address of the DWL-3200AP to be manually configured in accordance to the applied local area network. Enable Dynamic (DHCP) to allow the DHCP host to automatically assign the Access Point an IP address that conforms to the applied local area network.

IP address
The default IP address is 192.168.0.50 for DWL-3200AP. It can be modified to conform to an existing local area network. Please note that the IP address of each device in the wireless local area network must be within the same IP address range and subnet mask. Take default DWL-3200AP's IP address as an example, each station associated to the AP must be configured with a unique IP address falling in the range of 192.168.0.*. "*" ranges from 0 to 255 but 50 in this case.

Subnet Mask
A mask used to determine what subnet an IP address belongs to. The default subnet setting is 255.255.255.0 for DWL-3200AP.

Gateway
Specify the gateway IP address of the local network.

BIBLIOGRAPHIE

Ouvrages :

W802.11 et les réseaux sans fil

Paul Muhlethaler, édition Eyrolles, 2002

W Les réseaux

Guy Pujolle, édition Eyrolles,2003

W L es réseaux

Guy Pujolle, édition Eyrolles,2005

W Réseaux de mobile et réseau sans fil

Al Agha-Pujolle-Vivier,édition Eyrolles,2001

Sites Web :

Httt://www.commentcamarche.net

http://rubb.free.fr

http:/www.isi.edu/nsnam

http://www.cisco.com