# Réseaux sans fil

## 1. Introduction

La grande particularité des réseaux sans fil est d'être un système rapide à déployer, pour un cout raisonnable. En effet, il suffit pour construire un tel réseau d'équiper les postes informatiques d'un adaptateur 802.11 et si nécessaire d'installer un point d'accès. Ce type de réseau utilise donc des ondes radio pour véhiculer des données entre les postes.

L'objectif de ce chapitre est de donner un aperçu technique du standard 802.11 de façon à comprendre les concepts de base. Exposer quelques normes du Wi-Fi puis nous allons passer en revue une présentation globale du fonctionnement.

## 2. Historique

Les réseaux sans fil sont fondés sur une technologie à spectre étalé, initialement développée pour les communications militaires de l'armée américaine pendant la seconde guerre mondiale. Les techniciens militaires pensaient que les spectres étalés étaient plus intéressants car plus résistants au brouillage. Les autres avancées ont permis d'augmenter les débits. Après 1945, les entreprises commerciales ont commencé à exploiter cette technologie, ayant compris l'intérêt qu'elle représentait pour leurs clients.

La technologie des réseaux sans fil a évolué en 1971 avec un projet de l'université de Hawaii appelé **AlohNet**. Ce projet a permis à sept ordinateurs de communiquer depuis les différentes iles en utilisant un concentrateur central sur Oahu.

La recherche universitaire sur **AlohNet** a posé les bases de la première génération de réseaux sans fil, qui opérait sur la plage de fréquence 901-928 MHz, utilisé principalement par les militaires, cette phase du développement des réseaux sans fil n'a connu que peu d'utilisateurs à cause des problèmes de fréquence et de son faible débit.

A partir de ce moment, la fréquence 2.4 GHz a été définie pour une utilisation sans licence. La technologie a donc commencé à émerger et la spécification 802.11 est née. Celle-ci a évolué pour devenir le standard 802.11b et continue son chemin vers des implémentations plus rapides et plus sures**. [1]**

## 3. Définition

Un réseau sans fil (en anglais Wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux

réseaux sans fil, un utilisateur à 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 fil 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 fil 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 facile pour un pirate d'écouter le réseau si les informations circulent en clair. Donc il est nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil. **[2]**

- **L'onde radio**

Les ondes radioélectriques (dites **ondes radio**) sont des ondes électromagnétiques dont la fréquence d'onde est par convention comprise entre 9 KHz et 3000 GHz, ce qui correspond à des longueurs d'onde de 33 km à 0,1 mm. Les ondes hertziennes, utilisées non seulement pour la radio proprement dite (la TSF, comme on l'appelait en 1930) mais aussi pour la télévision, le téléphone portable voire le four à micro-ondes, appartiennent comme la lumière ou les rayons X à la grande famille des ondes électromagnétiques.

Elles sont produites en injectant dans une antenne un courant électrique variable à haute-fréquence. On peut comparer l'antenne à une ampoule électrique nue qui rayonnerait l'énergie que lui communique le courant électrique qui la traverse**. [3]**

## 4. Technologies sans fil

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

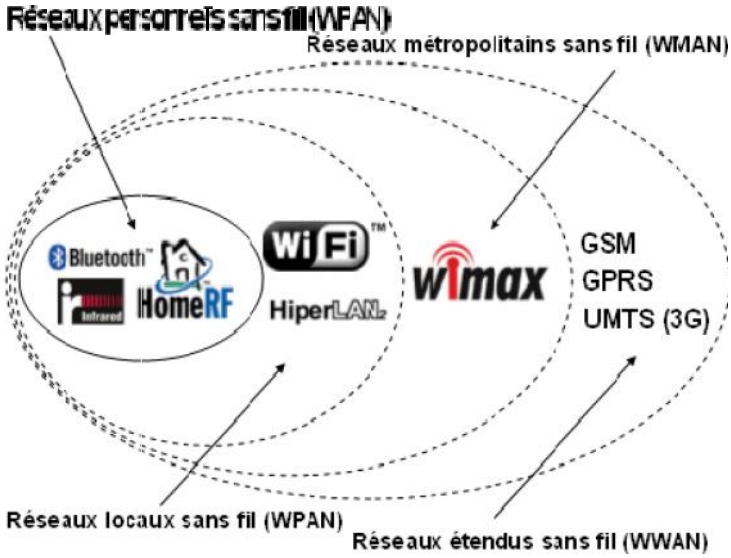


**Figure I.1 :** Catégories des réseaux sans fil

## 4.1. Réseaux WPAN

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN pour **W**ireless **P**ersonal **A**rea **N**etwork) concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) 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. Il existe plusieurs technologies utilisées pour les WPAN : **Bluetooth, Home RF, La technologie ZigBee.**

## 4.2. Réseaux WMAN

La BLR (**B**oucle **L**ocale **R**adio) fait partie des réseaux sans fil de type WMAN. La BLR est une technologie sans fil capable de relier les opérateurs à leurs clients grâce aux ondes radio sur des distances de plusieurs kilomètres.

Les réseaux sans fil de type WMAN (**W**ireless **M**étropolitain **A**rea **N**etwork) sont en train de se développer. Ce phénomène risque de s'amplifier dans les années à venir. La norme IEEE 802.16, est plus connue sous son nom commercial Wi-Max. La dernière version de la norme est IEEE 802.16-2004, ratifiée en juin 2004. Comme dans le cas de la dénomination Wi-Fi ; Wi-Max désigne en fait un ensemble de normes regroupées sous une appellation commune. La norme de réseau métropolitain sans fil la plus connue est le Wi-Max.

Techniquement, le Wi-Max permet des débits de l'ordre de 70 Mbit/s avec une portée de l'ordre de 50 km. Actuellement, le Wi-Max peut exploiter les bandes de fréquence 2,4 GHz,

3,5 GHz et 5,8 GHz. Aujourd'hui, en France, la bande de fréquence 2,4 GHz est libre, la bande de fréquence 5,8 GHz est interdite en utilisation extérieure et la bande des 3,5 GHz est licenciée à un unique opérateur. La norme 802.16e ajoutera de la mobilité à la norme actuelle IEEE 802.16**. [4]**

## 4.3. Réseaux WWAN

Le réseau étendu sans fil (WWAN pour **W**ireless **W**ide **A**rea **N**etwork) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes : **GSM, GPRS**, **UMTS.**

## 4.4. Les réseaux WLAN

Le réseau local sans fil (WLAN pour **W**ireless **L**ocal **A**rea **N**etwork) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres**. [5]**

les WLAN ont été conçus pour offrir un accès large bande radio avec des débits de plusieurs Mbit/s pour relier des équipements de type PC et autres équipements électroniques ou informatiques dans des environnements professionnels, immeubles de bureaux, bâtiments industriels ou grand public et se connecter à un réseau cœur, tel qu'un réseau Ethernet. Ils sont déployés dans des lieux privés mais aussi dans des lieux publics gares, aéroports, campus (hot spots). Ils sont complémentaires des réseaux cellulaires 2G et 3G qui offrent une plus grande mobilité mais des débits plus faibles.

Deux grandes familles se partagent le domaine des WLAN résultant des travaux menés aux Etats-Unis et en Europe. La première famille est celle du Wi-Fi nom donné à la norme IEEE 802.11b qui est actuellement la plus populaire pour offrir des débits jusqu'à 11 Mbit/s pour des distances de 10 à 100 m. La seconde famille est celle de l'HIPERLAN2 et de IEEE 802.11a basée sur l'OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) plus robuste aux distorsions sélectives en fréquence du canal, offrant des débits jusqu'à 54 Mbit/s mais au prix d'une complexité plus grande**. [6]** Il existe plusieurs technologies concurrentes : **hiperLAN2, DECT, Wi-Fi.**

## 4.5. Réseaux WRAN

L'organisation de certification, l'Institute of Electrical and Electronics Engineers ou IEEE, vient d'approuver une nouvelle norme la 802.22 WRAN (**W**ireless **R**egional **A**rea **N**etworks ou système de réseau régional sans fil). Celle-ci va permettre de fournir le haut débit sans fils

dans les zones mal desservies, en se servant des fréquences VHF et UHF des canaux de télévision vacants. Cette norme offrira également un débit de l'ordre de 22Mbps par canal, jusqu'à une distance de 100 kilomètres du transmetteur. La 802.22 vise donc à fournir un accès à large bande dans les zones rurales, mais également dans les pays en voie de développement. **[7]**

# Wi-Fi : Définition

Le nom **Wi-Fi** (contraction de **W**ireless **F**idelity, parfois notée à tort Wi-Fi) correspond initialement au nom donnée à la certification délivrée par la Wi-Fi Alliance, anciennement WECA, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing), le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wi-Fi est en réalité un réseau répondant à la norme 802.11. La norme **IEEE 802.11** (ISO/IEC 802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN).

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit pour peu que l'ordinateur à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert**. [6]**

## 1. Avantages de Wi-Fi

- **Mobilité**

Les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.

- **Facilité et souplesse**

Un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.

- **Coût**

Si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.

- **Évolutivité**

Les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins **[8].**

## 2. Inconvénients de Wi-Fi

- **Complexité**

Le premier problème auquel l'administrateur réseau est confronté est la diversité des compétences nécessaires à la mise en œuvre d'un réseau Wi-Fi. Il faut prendre en considération les problèmes de transmission radio, un éventuel audit du site, l'intégration de l'existant (réseau câblés, mais peut être aussi les quelques ilots Wi-Fi déjà en place), le respect de régulation, le support effectif des standards actuels et à venir, l'administration de ce futur réseau, le monitoring du trafic, etc.

- **Qualité et continuité du signal**

Ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.

- **Sécurité**

La sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice**. [9]** Elle est une préoccupation critique d'un administrateur réseau confronté au Wi-Fi, d'une part parce que les faiblesses des technologies ont été largement traitées sur Internet, d'autre part parce qu'il s'agit d'une approche effectivement nouvelle du sujet, et qui présente une grande diversité.

## 3. Différentes normes Wi-Fi

Les standards régissant les réseaux sans fil pour les PC sont établis par l'IEEE (**I**nstitue of **E**lecrical and **E**lectronics **E**ngineers). La technologie LAN/MAN a reçu le numéro 802, lui même subdivisé en groupes de travail. Les groupes les plus actifs incluent le 802.15, pour les réseaux personnels (Bluetooth), 802.16 pour les réseaux sans fil à large bande Wi-Max et enfin 802.11 pour les LAN sans fil. Dans le groupe 802.11, des définitions plus précises existent, identifiées par les différentes lettres**. [1]**

La norme IEEE 802.11 est en réalité la norme initial offrant des débits de 1 ou 2 Mbit/s. des révisions ont été apportés à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11g, appelés normes 802.11 physiques) ou bien préciser des éléments

afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. On trouvera ci-après une brève description des différentes révisions de la norme 802.11 ainsi que leur signification :

- **802.11a**

La norme 802.11a (baptisé **Wi-Fi 5**) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Elle spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.

Un des avantages de cette norme consiste à remédier aux problèmes rencontrés avec 802.11b, en utilisant une bande de fréquence moins utilisée pour d'autres applications. Rappelons que les bandes de fréquences 5Ghz et 2Ghz sont libres, c'est-à-dire que leur utilisation ne nécessite aucune licence en Europe. De plus, la vitesse théorique de 54Mbps s'avère être plus confortable pour l'échange de gros fichiers comparé à celle du 802.11b qui vaut 11Mbps.

Le 802.11a possède également des inconvénients comme sa portée réduite (15m) et son incompatibilité avec le 802.11b (le passage à cette norme exige donc l'acquisition d'un tout nouveau matériel)**. [8]**

- **802.11b**

Elle est la première norme à généraliser l'utilisation des transmissions sans fil, tout en ayant connu un vif succès commercial. Elle permet d'obtenir des débits théoriques de 11 Mbit/s (6 Mbit/s réels) sur la bande de fréquence de 2.4 GHz. La portée maximale du signal est de 100 mètres en intérieur, et de 300 mètres en extérieur ; sa portée est bien moindre dans les faits (30 et 100 mètres réels). Elle utilise la modulation radio DSSS (**D**irect **S**equence **S**pred **S**pectrum) et HR-DSSS.

Impatients, car la norme 802.11g a tardé à arriver, des constructeurs ont créé une évolution de cette norme, la 802.11b+ qui permet d'augmenter les débits à 22 et 44 Mbit/s (11 à 20 Mbit/s réels). Ces matériels étaient compatibles avec la 802.11b, mais en bridant leur vitesse à 11 Mbit/s. **[10]**

Le principal inconvénient de 802.11b consiste à présenter des interférences possibles avec les appareils fonctionnant sur les mêmes fréquences tels que les fours à micro ondes, les caméras analogiques sans fil et toutes les formes de surveillance ou d'observation professionnelles ou domestiques à distance comme les transmetteurs de salon, la télé-mesure, la télé-médecine, les radio-amateurs ATV, les claviers et souris sans fil**. [8]**

- **802.11c**

La norme 802.11c est une extension de 802.11b concernant la gestion de la couche MAC. Elle améliore les procédures de connexion en pont entre les points d'accès. Les travaux ont été suspendus et la norme restituée au Groupe de Travail 802.11d**. [8]**

- **802.11d**

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**

La norme 802.11e offre des possibilités de qualité de service (**QoS**) au niveau de la couche liaison de données. Elle définit ainsi les besoins des différents paquets en termes de bande passante et de délai de transmission de telle manière à permettre des flux prioritaires. Nous pouvons alors espérer, par exemple, une transmission de la voix et de la vidéo de meilleure qualité (fluidité et débit important). Actuellement, ces applications font l'objet d'un marché en pleine expansion. Par exemple, les téléphones Wi-Fi (F1000 de **UTStarcom**), télévision Wi-Fi…

- **802.11f**

La norme 802.11f est une recommandation à l'intention des vendeurs d'équipement 802.11 visant une meilleure interopérabilité des produits. 802.11f permet à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, indépendamment des marques des points d'accès. En effet, les fabricants d'équipement 802.11 utilisaient des normes propriétaires parfois incompatibles.

- **802.11g**

La norme 802.11g est la plus répandue, elle offre un haut débit (54 Mbps) sur la bande de fréquence des 2.4 GHz. De plus, les matériels conformes à la norme 802.11g fonctionnent en 802.11b (à 11 Mbps), ce qui garantit une compatibilité avec les points d'accès 802.11b. La modulation de 802.11g est l'OFDM comme pour la norme 802.11a.

Malheureusement, ce standard est aussi sensible aux interférences avec d'autres appareils utilisant les mêmes fréquences dans la bande des 2.4 GHz. Parallèlement à l'émergence de ce standard sur le marché, nous notons la naissance d'un besoin de la part des utilisateurs de qualité de service. La sécurité n'est pas toujours garantie et le cryptage proposé, lorsqu'il est utilisé, s'est avéré faillible (WEP). Il manque un aspect de sécurité de transmission au standard 802.11g. Ce problème est éloigné avec l'utilisation de WPA à la place de WEP. Mais le standard 802.11i consacré à la sécurité des transmissions, propose des solutions complètes, avec l'utilisation de l'algorithme WPA2 (**W**i-Fi **P**rotected **A**ccess version **2**), une version nettement améliorée du WPA. **[11]**

- **802.11h**

La norme 802.11h adapte la couche MAC visant à rendre compatible les équipements 802.11 avec les infrastructures utilisant HiperLAN2. En effet, bien qu'aucune des deux ne soit standardisée, ces normes ne sont jusqu'ici pas compatibles.

802.11h permet la détection automatique de fréquence de l'AP (Access Point) et le contrôle automatique de la puissance d'émission dans le but d'éliminer les interférences entre AP. La conformité est ainsi garantie avec la réglementation européenne en matière de fréquence et d'économie d'énergie (**D**ynamic **F**requency **S**olution & **T**ransmit **P**ower **C**ontrol). Cette norme, pas encore standardisée, est développée par l'IEEE et l'ETSI.

- **802.1x**

Il s'agit d'une sous-section du groupe de travail 802.11i, visant à l'intégration du protocole EAP. 802.1x se charge de la sécurisation de transmission de l'information dans les réseaux filaires et sans fil au moyen d'authentification sûre.

802.1x supporte diverses méthodes d'authentification comme les cartes à jeton, Kerberos, les mots de passe à utilisation unique, les certificats et les clefs publiques. Un exemple d'application est l'emploi d'un serveur d'authentification Radius combiné à une distribution dynamique de clefs, qui garantit un niveau de sécurité élevé.

- **802.11i**

Le but de la norme 802.11i est d'améliorer la sécurité des transmissions (gestion et distribution dynamique des clés, chiffrement des informations et authentification des utilisateurs). **[11]**

802.11b et 802.11g utilisent WEP pour sécuriser la transmission au moyen de clefs de cryptage. Le chiffrement utilisé est RC4, qui s'est avéré faible. 802.11i utilise WPA2. Elle utilise l'authentification EAP définie dans 802.1x et s'appuie sur le chiffrement AES (**A**dvanced **E**ncryption **S**tandard). De plus, elle assure la confidentialité au moyen d'un chiffrement à clés temporaires TKIP, plus performant que l'algorithme utilisé avec 802.11g et 802.11b.

- **802.11j**

Le but de la norme 802.11j est de rendre compatible 802.11a avec la réglementation japonaise.

- **802.11k**

La norme 802.11k permet aux appareils compatibles de faire des mesures de signaux complètes pour améliorer l'efficacité des communications. Les avantages sont multiples tels

que l'administration à distance de la couverture réseau, ou une amélioration du roaming automatique via des « site report ».

- **802.11 IR**

La norme 802.11IR a été élaborée afin d'utiliser des signaux infrarouges. Les applications sont rares et nous pouvons affirmer que cette norme n'est plus d'actualité étant donné les faibles débits proposés (2Mbits/s).

- **802.11n**

Cette norme est très prometteuse car elle doit permettre d'atteindre les débits du filaire, avec un débit de 540 Mbits (100 Mb/s réels) et une portée de 100 mètres réels. Elle intégrera la technologie MIMO et devrait être compatible avec les anciennes normes avec un fonctionnement en mode mixte qui permettra d'avoir des transmissions à débit hétérogène fonctionnant en 802.11a, b ou g avec l'ancien matériel et en 802.11n avec le nouveau. Utilise la modulation radio MIMO-OFDM.

Le 802.11n utilise des fréquences de 2.4 et 5 GHz et ne fonctionne qu'en mode infrastructure avec un point d'accès centrale sur le quel tous les clients se connectent.

## 4. Equipements Wi-Fi

- **Eléments actifs Wi-Fi**

Les points d'accès ou des cartes clientes possèdent le même type d'éléments actifs Wi-Fi : leur fonction principale est de convertir les données numériques provenant d'un réseau Ethernet en signaux analogiques destinés à l'antenne. C'est à son niveau que les protocoles de modulation/démodulation des signaux interviennent. En réception, il effectue le processus inverse consistant à décoder les signaux transmis par l'antenne en données IP pour le réseau. Les caractéristiques principales d'un élément actif sont sa puissance d'émission et sa sensibilité en réception (puissance minimale admissible pour interpréter les données et assurer la liaison), toutes deux exprimées en mW ou dBm. Sont réglables sur ce matériel Wi-Fi le débit de liaison souhaité, parfois le niveau de puissance de sortie, ainsi que plusieurs protocoles liés à la sécurité et à l'identification des autres AP connectées.

- **Points d'accès (AP)**

Le rôle des points d'accès est similaire à celui que tiennent les hubs dans les réseaux traditionnels. Il permet aux stations équipées de cartes Wi-Fi d'obtenir une connexion au réseau. On parle alors d'association entre l'AP et chaque station connectée. Les trames d'information envoyées par un client sont ré émises par l'AP, ce qui permet à la station de

joindre un autre client qu'elle ne peut pas forcément voir directement (éloignement, obstacle). Le support physique étant les ondes radio, on ne peut pas empêcher les stations non destinataires de recevoir les trames émises, d'où l'analogie avec le hub. Les APs sont nécessaires lorsque le réseau sans fil fonctionne en mode infrastructure. Ce sont en fait des boîtes qui contiennent une carte Wi-Fi comme on en trouve sur les stations, une ou plusieurs antennes et du logiciel embarqué dans une puce pour gérer tout cela. Le logiciel présent permet de fournir des services supplémentaires liés à la sécurité et l'identification des autres AP connectés. Il est possible de transformer un ordinateur équipé d'une carte Wi-Fi en point d'accès, par simple adjonction de programmes.


**Figure I.2 :** Exemple de point d'accès

- **Routeurs**

Centre névralgique de votre installation, connectés à votre modem haut débit, le routeur « transforme » votre connexion Internet filaire en connexion sans fil.

La plupart des routeurs font office de borne sans fil offrant l'accès Internet à tous vos ordinateurs. Ils disposent également de ports Ethernet (en générale quatre) pour raccorder physiquement les postes les plus proches et certains offrent une sécurité pour le réseau en étant dotés de firewall et de limitations d'accès.

- **Les modems/routeurs**

Les modems/routeurs offrent une solution deux-en-un en regroupant dans un même appareil un modem (pour accédera la ligne Internet) et un routeur pour repartir cette connexion sur vos différents ordinateurs.

- **Cartes Wi-Fi**

Ce terme désigne les périphériques actifs Wi-Fi/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**

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.

**Figure I.3 :** Carte PCMCIA

- **PCI**

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.

**Figure I.4 :** Carte PCI

- **USB**

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.

**Figure I.5 :** Carte USB

- **Antennes**

L'antenne intégrée à l'AP ou à la carte Wi-Fi peut être remplacée par une 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 :

- Les omnidirectionnelles
- Les directionnelles
- Les patchs ou antennes sectorielles


**Figure I.6 :** Schéma général du réseau Wi-Fi

## 5. Architecture Wi-Fi (802.11)

La norme IEEE 802.11 définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Cette dernière est elle-même subdivisée en deux sous-couches, la sous-couche LLC et la couche MAC.

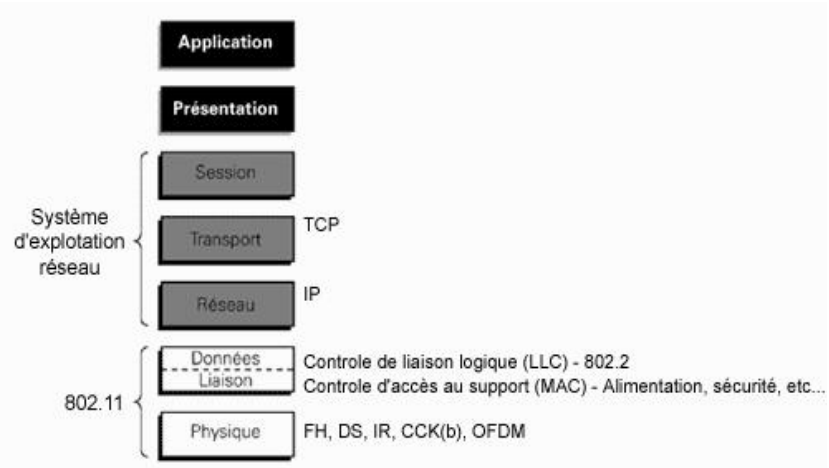


**Figure I.7 :** Couches du modèle OSI

## 5.1. Couche physique

(Notée parfois couche PHY) elle définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. La norme 802.11 propose en réalité trois couches physiques, définissant des modes de transmission alternatifs: DSSS, FHSS, Infrarouges.

### a. FHSS (Frequency Hopping Spread Spectrum)

La technique de FHSS consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission est ainsi réalisée en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée. L'émetteur et le récepteur s'accordent sur un schéma de saut, et les données sont envoyées sur une séquence de sous-canaux. Chaque conversation sur le réseau 802.11 s'effectue suivant un schéma de saut différent, et ces schémas sont définis de manière à minimiser le risque que deux expéditeurs utilisent simultanément le même sous-canal. La séquence de fréquences utilisée est publique. FHSS est utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

Les techniques FHSS simplifient relativement la conception des liaisons radio, mais elles sont limitées à un débit de 2 Mbps, cette limitation résultant essentiellement des réglementations de l'ETSI qui restreignent la bande passante des sous-canaux à 1 MHz. Ces contraintes forcent les systèmes FHSS à s'étaler sur l'ensemble de la bande des 2,4 GHz, ce qui signifie que les sauts doivent être fréquents et représentent en fin de compte une charge importante.

### b. DSSS (Direct-Sequence Spread Spectrum)

En revanche, la technique divise la bande de 2,4 GHz en 14 canaux de 22 MHz. Les canaux adjacents se recouvrent partiellement, seuls trois canaux sur les 14 étant presque entièrement isolés. DSSS augmente la fréquence du signal numérique en le combinant avec un autre signal d'une fréquence plus élevée. Les données sont transmises intégralement sur l'un de ces canaux

de 22 MHz, sans saut. La technique du « chipping » aide à compenser le bruit généré par un canal donné, c'est-à-dire moduler chaque bit avec la séquence Barker. **[12]**

Dans ce but, le standard 802.11 DSSS original spécifie un chipping sur 11 bits (baptisé séquence Barker) pour le codage des données. La longueur du « chipping code » détermine combien de données seront transmises au-dessus d'une unité de temps (c'est-à-dire la bande passante). Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

### c. Infrarouges (IR)

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. Cette technologie a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon unidirectionnelle, soit en vue direct soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé. Il est possible grâce a la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelés PPM (**P**ulse **P**osition **M**odulation).

La modulation PPM consiste à transmettre des impulsions à amplitude constante, et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de 16-PPM, tandis que le débit de 2Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles.

## 5.2. Couche liaison de données

Constitué de deux sous-couches : le contrôle de la liaison logique (**L**ogic **L**ink **C**ontrol, ou LLC) et le contrôle d'accès au support (**M**edia **A**ccess **C**ontrol, ou MAC).

- Couche LLC : utilise les mêmes propriétés que la couche LLC 802.2.
- Couche MAC : son rôle est similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente. Cependant la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

Les fonctionnalités nécessaires pour réaliser un accès sur une interface radio sont les suivantes :

- Procédure d'allocation du support
- Adressage des paquets
- Formatage des trames
- Contrôle d'erreur CRC

- Fragmentation et réassemblage

### a. Couche MAC

Le but principale de la couche MAC est de fournir un couplage efficace entre les services de la couche RLC 2 et la couche physique. De cette perspective, la couche MAC supporte quatre fonctions principales :

- Le mappage entre les canaux logiques et de transport. En effet, quand le standard offre différents options pour le transport de données pour un canal logique donné, la couche MAC s'occupe de choisir le canal de transport selon la configuration choisi par l'opérateur.
- La sélection du format de transport qui fait référence par exemple, au choix la taille du' Transport Block' et le schéma de modulation.
- Gestion de propriété entre les connais logique d'une terminale ou entre plusieurs terminaux.
- Correction d'erreur à travers le mécanisme HARQ.

### b. Couche LLC

Couche dépourvue du codage analogique: on récupère les bits. Réalisé à la limite du hardware et du software (firmware EEPROM). Les services rendus par la couche LLC aux couches supérieures sont spécifié par 3 classes :

- **LLC1 :** service sans connexion et sans acquittement. Le travail est fait dans les couches supérieures ou on accepte de perdre des données (ex : Visio confi et temps réel) les couches supérieures assurent la reprise en cas d'erreur).
- **LLC2 :** service avec connexion ex : porteuse (pour les transmissions longues de fichiers,).
- **LLC3 :** service sans connexion et avec acquittement. Cela évite de maintenir une table active : datagramme. En fait, on écoute en permanence car il y a des diffusions d'écoute (on arrose tout le monde).

## 5.3. Modes de fonctionnement

De manière générale, la machine cliente demande des informations via le réseau et la machine serveur offre des services. Deux types d'architectures sont généralement distinguées pour les réseaux sans fil à savoir le mode Ad hoc et le mode Infrastructure.

### 5.3.1. Mode infrastructure

C'est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte réseau Wifi entre eux via un ou plusieurs points d'accès qui agissent comme des concentrateurs.

L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé Cellule de base BSS (**B**asic **S**ervice **S**et). Chaque BSS est identifié par un BSSID (un identifiant de 6 octets). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.

Lorsque le réseau est relié à plusieurs BSS, chacun d'eux est relié à un système de distribution DS (**D**istribution **S**ystem) par l'intermédiaire de leur point d'accès. Le système de distribution (DS) peut être aussi bien un réseau filaire (Ethernet), qu'un câble entre deux points d'accès ou bien même un réseau sans fil.

Un groupe de BSS interconnectés par un système de distribution forme un ensemble de services étendu ESS (**E**xtended **S**ervice **S**et). **[13]**

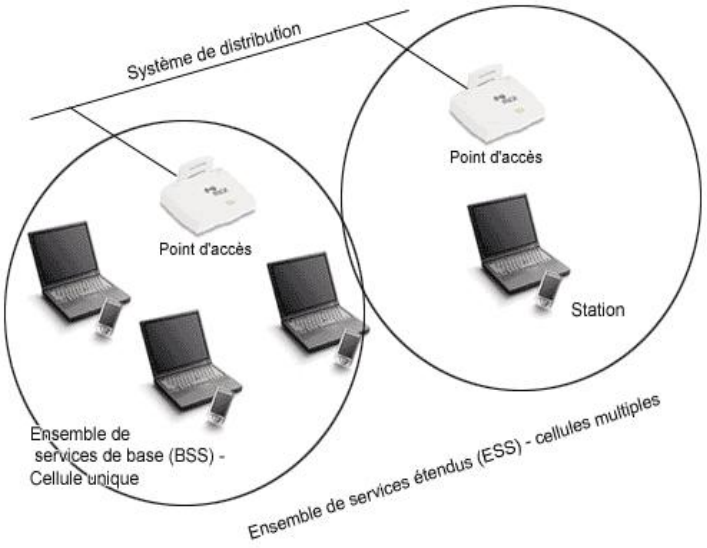


**Figure I.8 :** Mode infrastructure

Lorsqu'une station entre dans un BSS ou ESS, elle doit s'associer à un point d'accès. L'association comporte les différentes étapes suivantes :

- **La station écoute le canal afin de découvrir le point d'accès disponible**

Cette écoute peut se faire de deux manières différentes :

- Ecoute passive : la station écoute sur tous les canaux de transmissions et attend de recevoir une trame balise du point d'accès.
- Ecoute active : sur chaque canal de transmission, la station envoi une trame de requête (**P**robe **R**equest **F**rame) et attend la réponse. Une fois l'écoute est terminée, la station choisi le point d'accès le plus approprié.

- **Authentification**

Une fois que le point d'accès est choisi, la station doit s'authentifier auprès lui. Il y a deux méthodes d'authentification:

- Open System Authentification : Authentification par défaut, le terminal peut s'associer à n'importe quel point d'accès et écoute toutes les données qui transitent au sein du BSS.
- Shared Key Authentification : Meilleur que la précédente utilisé dans le cas d'une sécurité WEP.

- **Association**

Dés qu'une station est authentifiée, elle peut s'associer avec le point d'accès, elle envoie pour cela une trame de requête d'association et attend que le point d'accès lui réponde. **[13]**

### 5.3.2. Mode Ad-Hoc

Un groupe de terminaux forme un ensemble de services de base indépendants IBSS (**I**ndependent **B**asic **S**ervice **S**et). Chaque station peut établir une communication avec n'importe quelle station dans l'IBSS, sans être obligée de passer par un point d'accès. **[13]**

Ce mode permet de déployer, rapidement et n'importe où, un réseau sans fil. Le fait de ne pas avoir besoin d'infrastructure, autre que les stations et leurs interfaces, permet d'avoir des nœuds mobiles. D'un point de vue militaire, c'est très intéressant. Sur le champ de batailles, même si une partie des équipements est détruite, il est toujours possible de communiquer. On imagine aussi, l'intérêt lors de catastrophes naturelles, tel que les tremblements de terre. Les réseaux ad-hoc permettent d'établir très rapidement un système de communication efficace. **[14]**

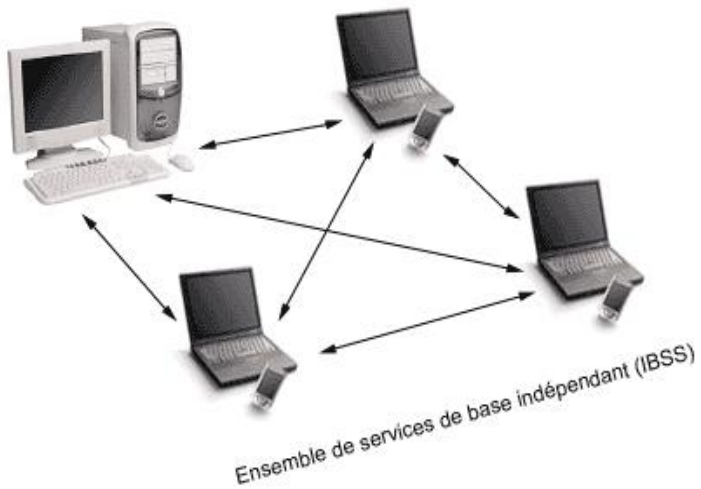


**Figure I.9 :** Mode Ad-Hoc

## Conclusion

Dans ce chapitre on a bien vu que 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. 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. Contrairement le Wi-Fi a beaucoup de problèmes de sécurité, dans le chapitre qui suit, on va détailler les mécanismes utilisé pour mettre au point une stratégie de sécurité.