



Les supports physiques de transmission: Les infrastructures sans fil



A. Introduction au réseau sans fil

Un réseau sans fils (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 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 radio-électriques (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

En contrepartie se pose deux problèmes:

- La réglementation relative aux transmissions radio-électriques.
- 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 (c'est le cas par défaut).



B. Les catégories de réseaux sans fils

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

1. Réseaux personnels sans fils (WPAN)

Le réseau personnel sans fils (appelé également réseau individuel sans fils ou réseau domestique sans fils et noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fils 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 fils entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN.

a. La technologie Bluetooth (norme IEEE 802.15.1)



C'est la principale technologie WPAN est, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres via une liaison hertzienne. Elle possède l'avantage d'être très peu gourmande en énergie, ce qui la rend particulièrement adaptée à une utilisation au sein de petits périphériques, elle n'est pas spécialisé réseaux

Au sein d'un réseau bluetooth, un appareil sert de maître et jusque 7 périphériques esclaves qui se partagent la bande passante. Il est possible en théorie de faire communiquer jusque 10 groupes d'appareils, soit 80 appareils. Sécurisée, cette connexion est transparente uniquement si les deux appareils se connaissent. .

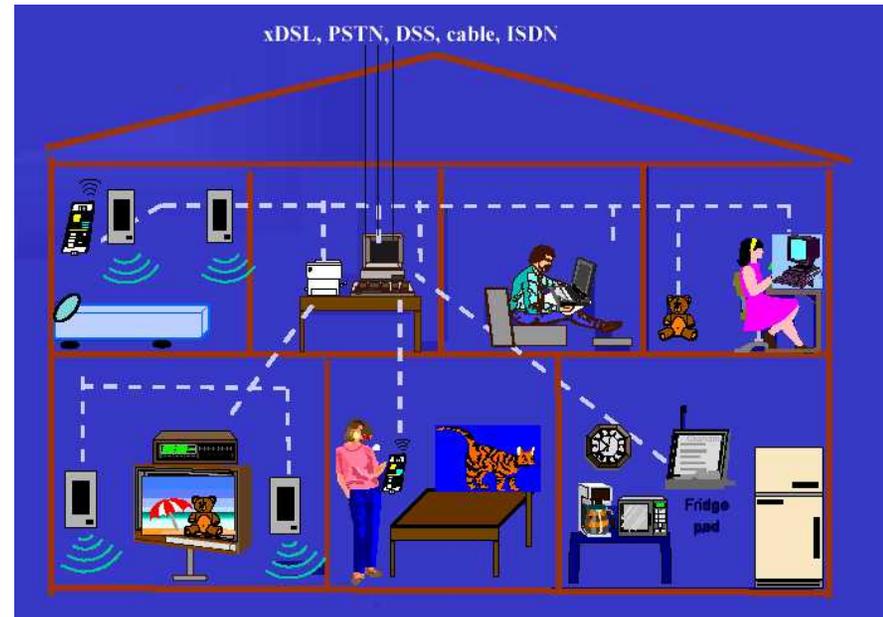




b. La technologie HomeRF (pour Home Radio Frequency)



Elle est 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 fondateurs 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).

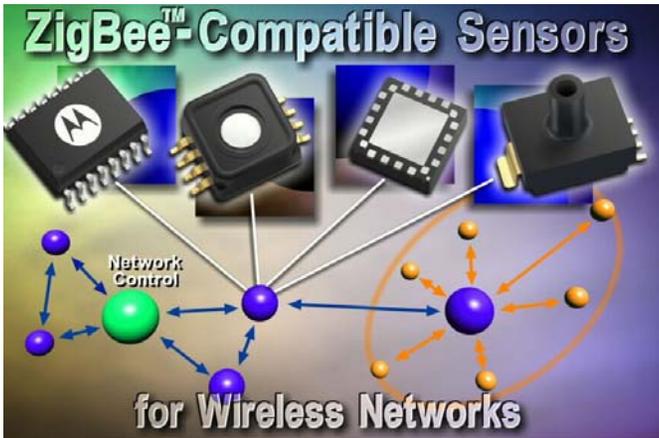




c. La technologie ZigBee (Norme IEEE 802.15.4)



Elle 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, ...).





d. La technologie infrarouge



Enfin les liaisons infrarouges permettent de créer des liaisons sans fils 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.



Diagramme illustrant une liaison basée sur la technologie irDA (Infrared Data Association) pour connecter divers appareils.



2. Réseaux locaux sans fils (WLAN)

Le réseau local sans fils (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.

a. La technologie Wifi (norme IEEE 802.11)



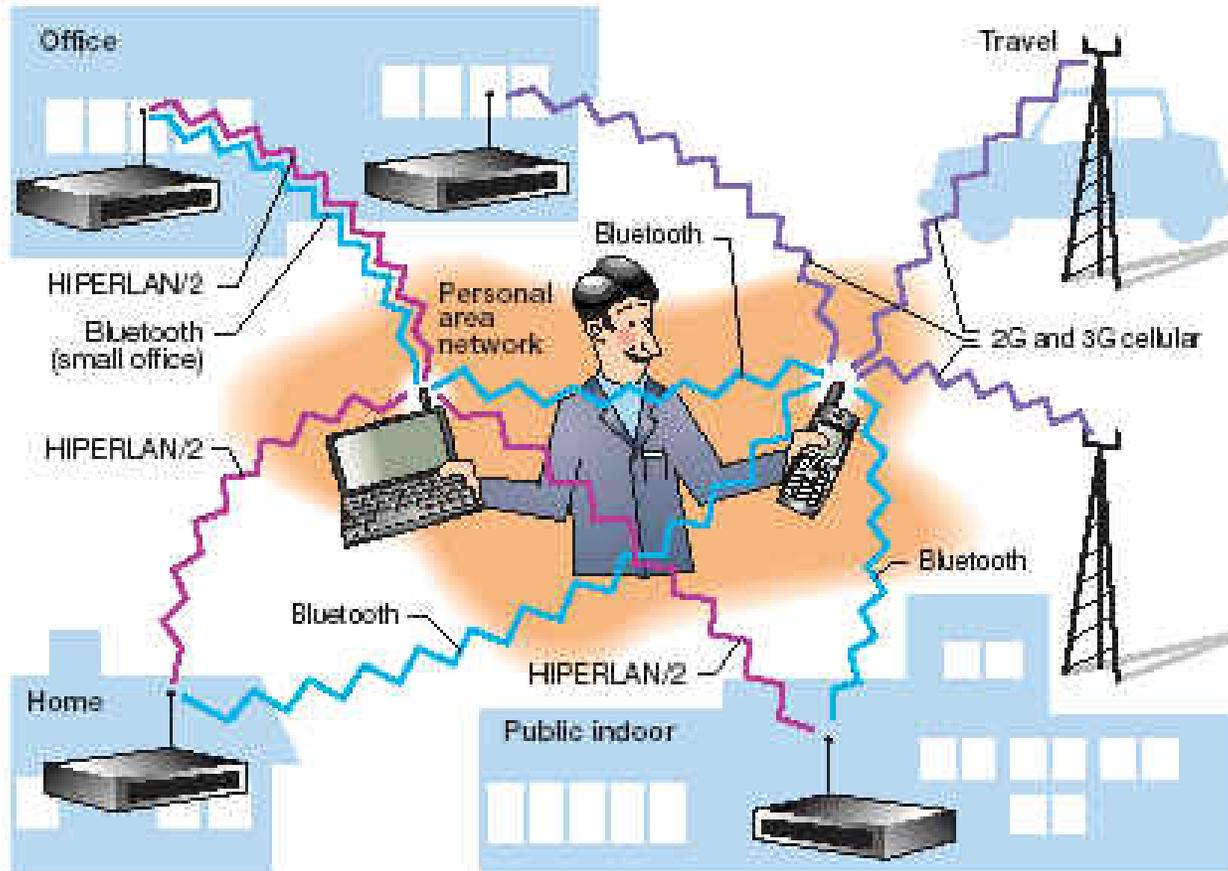
Elle est soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

Elle est composé de plusieurs normes qui opèrent sur des fréquences radios différentes. Elle permet de monter un réseau sans fil entre les différents équipements informatiques (PC, Consoles de jeu, PDA...). Grâce au WIFI vous pourrez partager vos fichiers et votre connexion ADSL avec vos proches sans l'encombrement des fils. Vous bénéficierez ainsi de tous les avantages du haut débit à n'importe quel endroit et n'importe quel moment. (Cette technologie sera développer dans la suit de ce document)

b. La technologie hiperLAN2 (High Performance Radio LAN 2.0)

HiperLAN2

C'est une 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. L'Hiperlan2 à une nette supériorité technique par rapport au Wifi, notamment en matière de qualité de service.



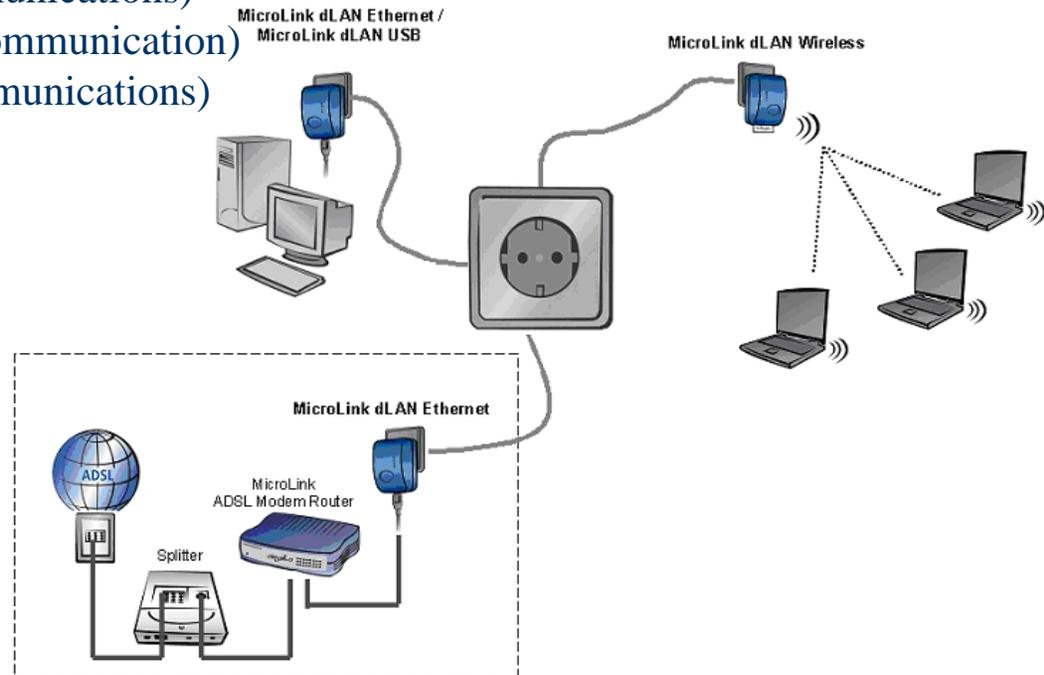
c. Introduction aux CPL (Courants porteurs en ligne)



On retient sous l'appellation CPL (Courants Porteurs en Ligne) toute technologie qui vise à faire passer de l'information à bas débit ou haut débit sur les lignes électriques en utilisant des techniques de modulation avancées.

Selon les pays, les institutions, les sociétés, les courants porteurs en ligne se retrouvent sous plusieurs mots-clés différents :

- CPL (Courants porteurs en ligne)
- PLC (Powerline Communications)
- PLT (Powerline Telecommunication)
- PPC (Power Plus Communications)



3. Réseaux métropolitains sans fils (WMAN)

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

4. Réseaux étendus sans fils (WWAN)

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

- GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile) dont le débit est de 9 kbits/s



- GPRS (General Packet Radio Service) dont le débit est de 20-30 kbits/s



- UMTS (Universal Mobile Telecommunication System) dont le débit est de 1 Mbits/s





C. Propagation des ondes radio

1. Introduction

Il est nécessaire d'avoir une culture minimum sur la propagation des ondes hertziennes afin de pouvoir mettre en place une architecture réseau sans fil, et notamment de disposer les bornes d'accès (point d'accès) de telle façon à obtenir une portée optimale.

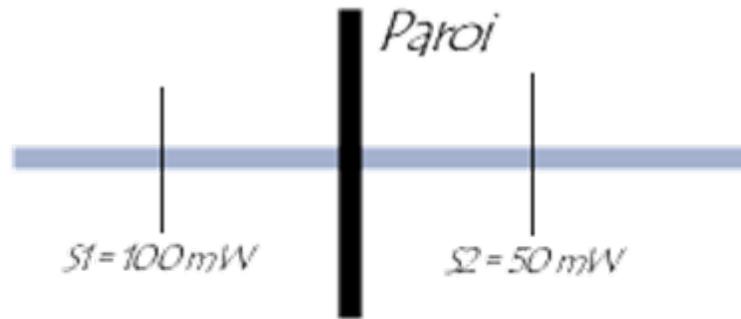
Les ondes radio (notées RF pour Radio Frequency) se propagent en ligne droite dans plusieurs directions. La vitesse de propagation des ondes dans le vide est de 3.10^8 m/s.

Dans tout autre milieu, le signal subit un affaiblissement dû à

- La réflexion
- La réfraction
- La diffraction
- L'absorption

2. Absorption des ondes radio

Lorsqu'une onde radio rencontre un obstacle, une partie de son énergie est absorbée et transformée en énergie, une partie continue à se propager de façon atténuée et une partie peut éventuellement être réfléchiée (réflexion).



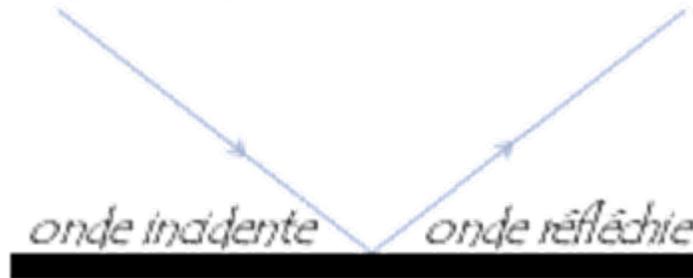
$$R \text{ (dB)} = 10 \log \left(\frac{S_2}{S_1} \right) = -3 \text{ dB}$$

L'atténuation augmente avec l'augmentation de la fréquence ou de la distance. De plus lors de la collision avec un obstacle, la valeur de l'atténuation dépend fortement du matériau composant l'obstacle. Généralement les obstacles métalliques provoquent une forte réflexion, tandis que l'eau absorbe le signal.

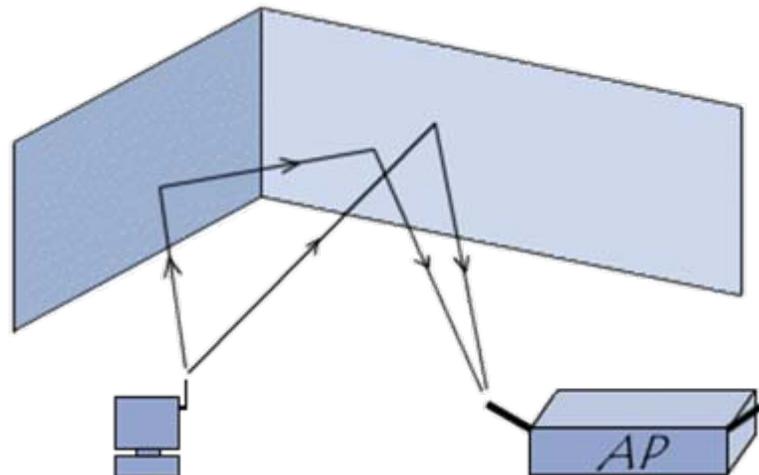


3. Réflexion des ondes radio

Lorsqu'une onde radio rencontre un obstacle, tout ou partie de l'onde est réfléchi, avec une perte de puissance. La réflexion est telle que l'angle d'incidence est égal à l'angle de réflexion.



Par définition une onde radio est susceptible de se propager dans plusieurs directions. Par réflexions successives un signal source peut être amené à atteindre une station ou un point d'accès en empruntant des chemins multiples (on parle de *multipath* ou en français *cheminements multiples*).





La différence de temps de propagation (appelées délai de propagation) entre deux signaux ayant emprunté des chemins différents peut provoquer des interférences au niveau du récepteur car les données reçues se chevauchent.

Ces interférences deviennent de plus en plus importantes lorsque la vitesse de transmission augmente car les intervalles de temps entre les données sont de plus en plus courts. Les chemins de propagations multiples limitent ainsi la vitesse de transmission dans les réseaux sans fil.

Pour remédier à ce problème les cartes Wi-Fi et points d'accès embarquent deux antennes par émetteur. Ainsi, grâce à l'action de l'AGC (Aquisition Gain Controller), qui commute immédiatement d'une antenne à l'autre suivant la puissance des signaux, le point d'accès est capable de distinguer deux signaux provenant de la même station. Les signaux reçus par ces deux antennes sont dit décorrélés (indépendants) si ils sont séparés de $\Lambda/2$ (6,25 cm à 2.4GHz).

4. Autres phénomènes physiques

- La réfraction

C'est la déviation de l'onde lors d'un changement de milieu

- La diffraction

Lorsqu'une onde arrive sur un obstacle elle se retrouve divisée (éparpillée) en plusieurs ondes.



5. Propriétés des milieux

L'affaiblissement de la puissance du signal est en grande partie du aux propriétés des milieux traversés par l'onde. Voici un tableau donnant les niveaux d'atténuation pour différents matériaux :

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



D. Présentation du WIFI (norme 802.11)

1. Introduction au WIFI

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom WiFi (contraction de Wireless Fidelity, parfois notée Wi-Fi) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), 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 Wifi est en réalité un réseau répondant à la norme 802.11.

Grâce au Wi-Fi il est possible de créer des réseaux locaux sans fil à haut débit pour peu que la station 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 machines 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.



2. Les différentes normes WiFi

Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Nom de la norme	Nom	Description
802.11a	Wifi5	La norme 802.11a (baptisé <i>WiFi 5</i>) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps 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 11 Mbps (6 Mbps réels) 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 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau <i>liaison de données</i>).
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 <i>liaison de données</i> . 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 à 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 <i>Inter-Access point roaming protocol</i> permettant à 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 <i>itinérance</i> (ou <i>roaming en anglais</i>)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps 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



Les supports physiques de transmission: Les infrastructures sans fil

Nom de la norme	Nom	Description
802.11g+ 802.11 Turbo g		Ce réseau sans fil est la première à assurer un débit théorique de 100 Mbits. Le 802.11g+ ou Turbo g n'est qu'une modification de la norme IEEE 802.11g et non ratifié par le consortium Wi-Fi Alliance.
802.11h		La norme <i>802.11h</i> vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le <i>h</i> de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme <i>802.11i</i> a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l' <i>AES (Advanced Encryption Standard)</i> et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11r		La norme <i>802.11r</i> a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme <i>802.11j</i> est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.
802.11n		La Wi-Fi Alliance a annoncé que la nouvelle norme IEEE 802.11n sera disponible avant la fin de l'année 2005. Cette nouvelle norme de réseau sans fil est la première à assurer un débit théorique "officiel" de 108 Mbits. Le 802.11n fonctionnera en interopérabilité avec les produits réseaux en 802.11b et 802.11g.



E. Les modes de fonctionnement du Wifi

1. Les éléments d'un réseau Wifi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wifi :

a. Les adaptateurs

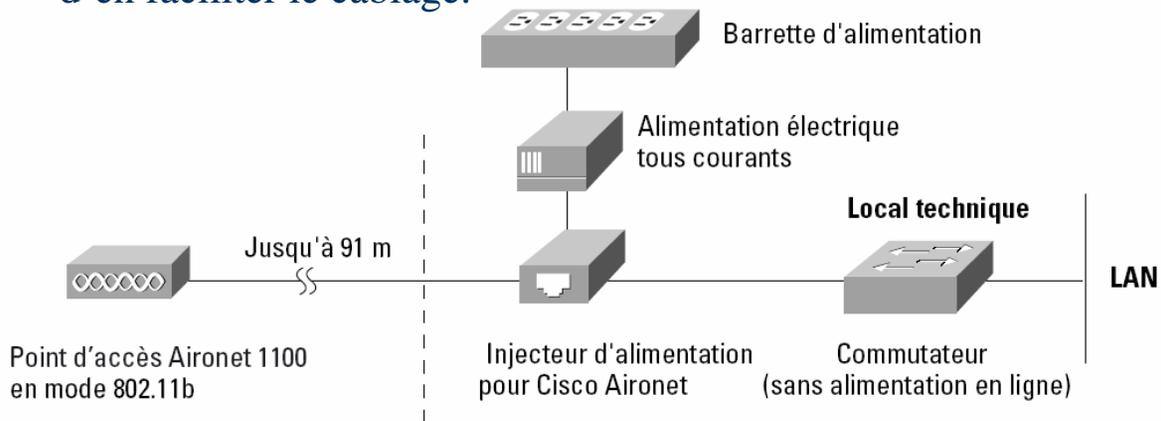
Les adaptateurs sans fil ou cartes d'accès (en anglais wireless adapters ou network interface controller, noté NIC) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs WiFi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte CompactFlash, ...). On appelle station tout équipement possédant une telle carte.





b. Les points d'accès

Les points d'accès (notés AP pour Access point, parfois appelés bornes sans fil) permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes wifi. Certains points d'accès peuvent être alimentés en ligne (via le câble réseau). Ceci permet d'en faciliter le câblage.

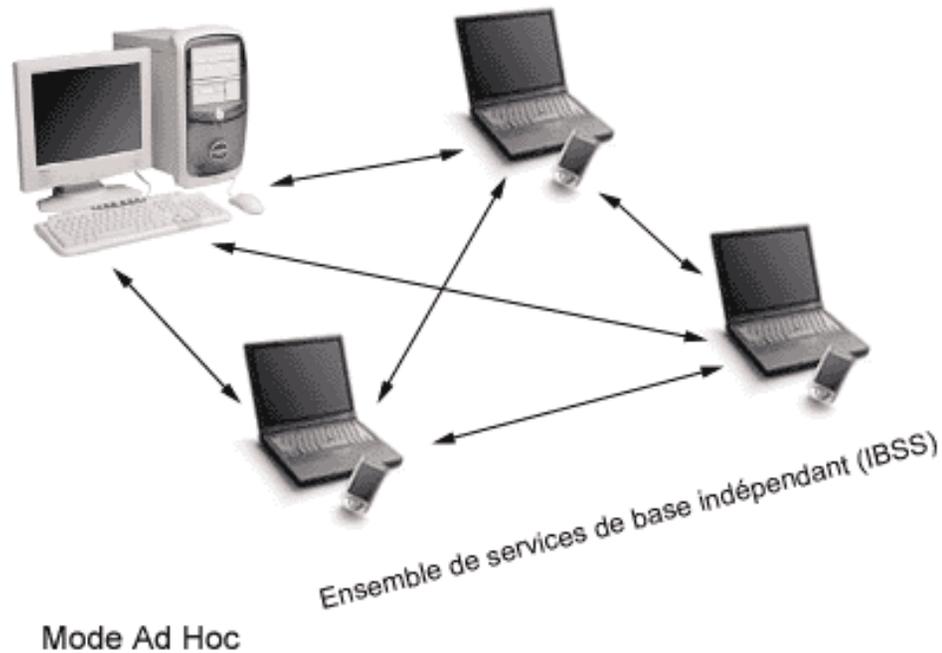




2. Les modes opératoires

a. Le mode ad hoc

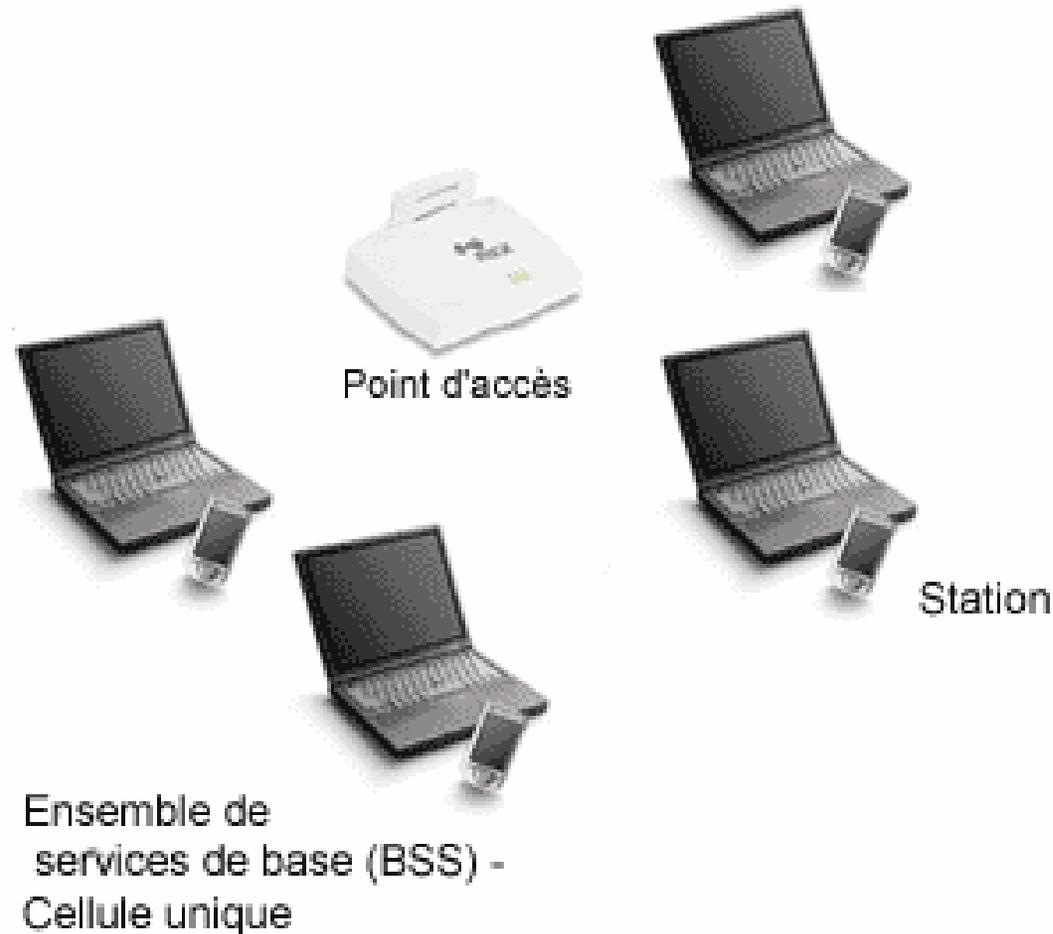
Ce mode est également baptisé point à point, ou ensemble de services de base indépendants - soit IBSS, de l'anglais Independent Basic Service Set, représente simplement un ensemble de stations sans fil 802.11 qui communiquent directement entre elles sans point d'accès ni connexion à un réseau filaire. Ce mode permet de créer rapidement et simplement un réseau sans fil là où il n'existe pas d'infrastructure filaire ou encore là où une telle infrastructure n'est pas nécessaire pour les services attendus, chambre d'hôtel, centre de conférence ou aéroport par exemple, ou enfin lorsque l'accès au réseau filaire est interdit (cas du consultant sur le site du client).





b. En mode infrastructure BBS

le réseau sans fil consiste au minimum en un point d'accès connecté à l'infrastructure du réseau filaire et un ensemble de postes réseaux sans fil. Cette configuration est baptisée Basic Service Set (BSS, ou ensemble de services de base). Il s'agit généralement du mode par défaut des cartes 802.11b.

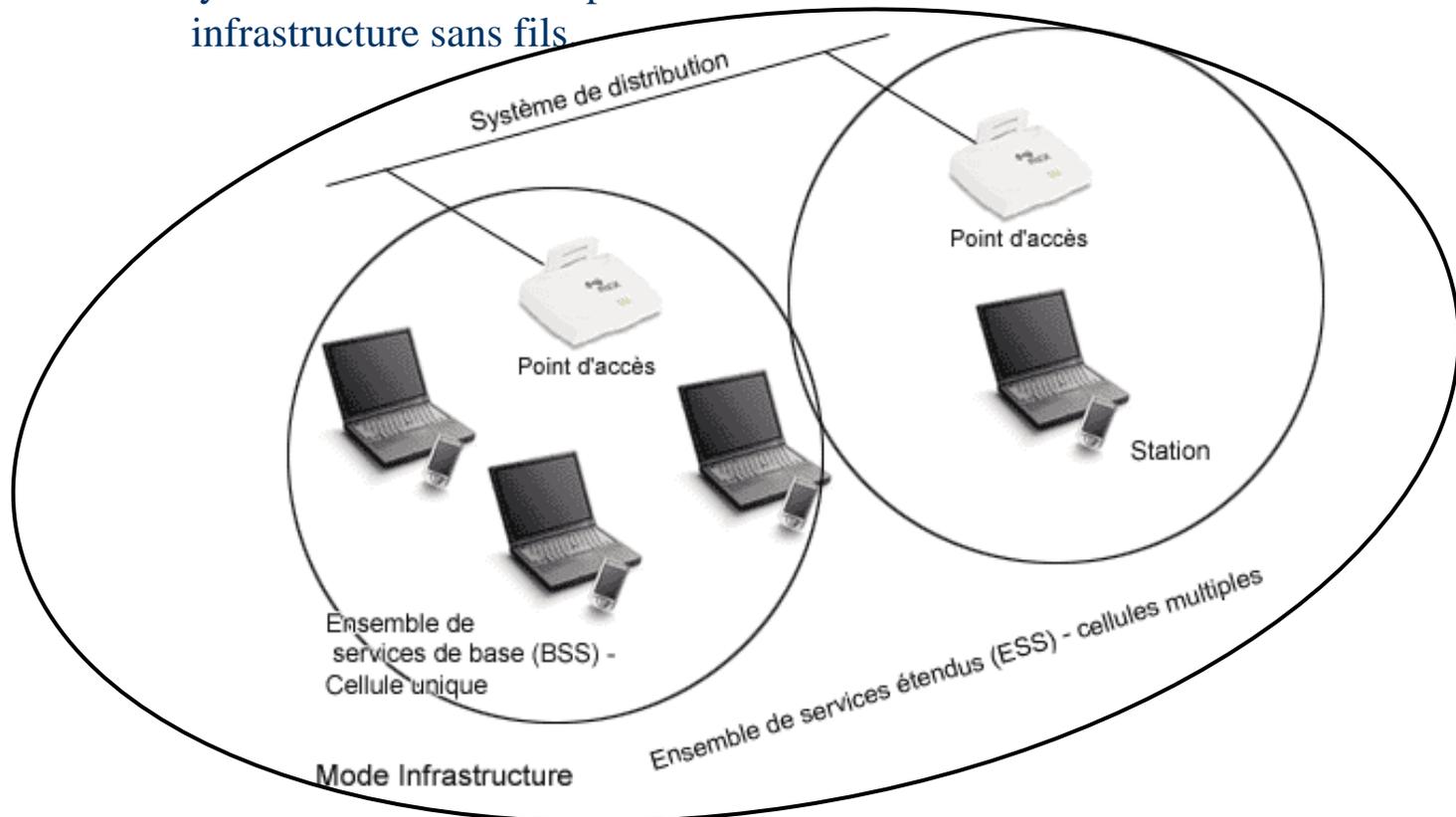




c. En mode infrastructure ESS

Un Extended Service Set (ESS, ou ensemble de services étendu) est un ensemble d'au moins deux BSS formant un seul sous-réseau. Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau. Il est nécessaire pour qu'une station se connecte au réseau étendu.

Le système de distribution peut être soit une infrastructure filaire ou une autre infrastructure sans fils

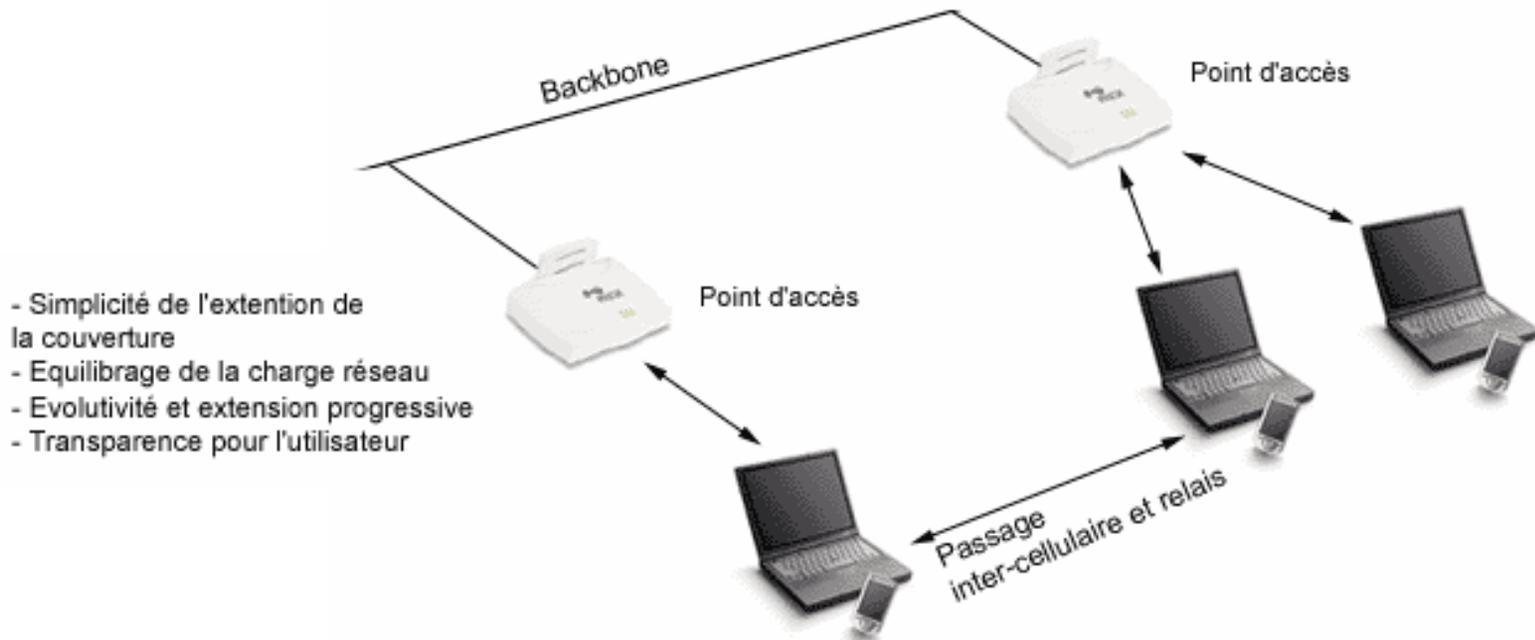




d. Associations, architectures cellulaires et itinérance

L'interface réseau est responsable de la manière dont un client s'associe à un point d'accès. Lorsqu'un client 802.11 entre dans le rayon d'action d'un ou plusieurs points d'accès, il choisit l'un de ces points pour s'y associer (on dit aussi qu'elle se joint à un BSS) en fonction de la puissance du signal, des taux d'erreurs observés dans la transmission des paquets, et de la charge. Une fois accepté par le point d'accès, le client règle son canal radio sur celui du point d'accès. Périodiquement, il explore tous les canaux 802.11 pour déterminer si un autre point d'accès est susceptible de lui offrir de performances supérieures. S'il détermine que c'est le cas, il s'associe au nouveau point d'accès, se réglant sur le canal radio de ce point d'accès.

Itinérance entre les points d'accès

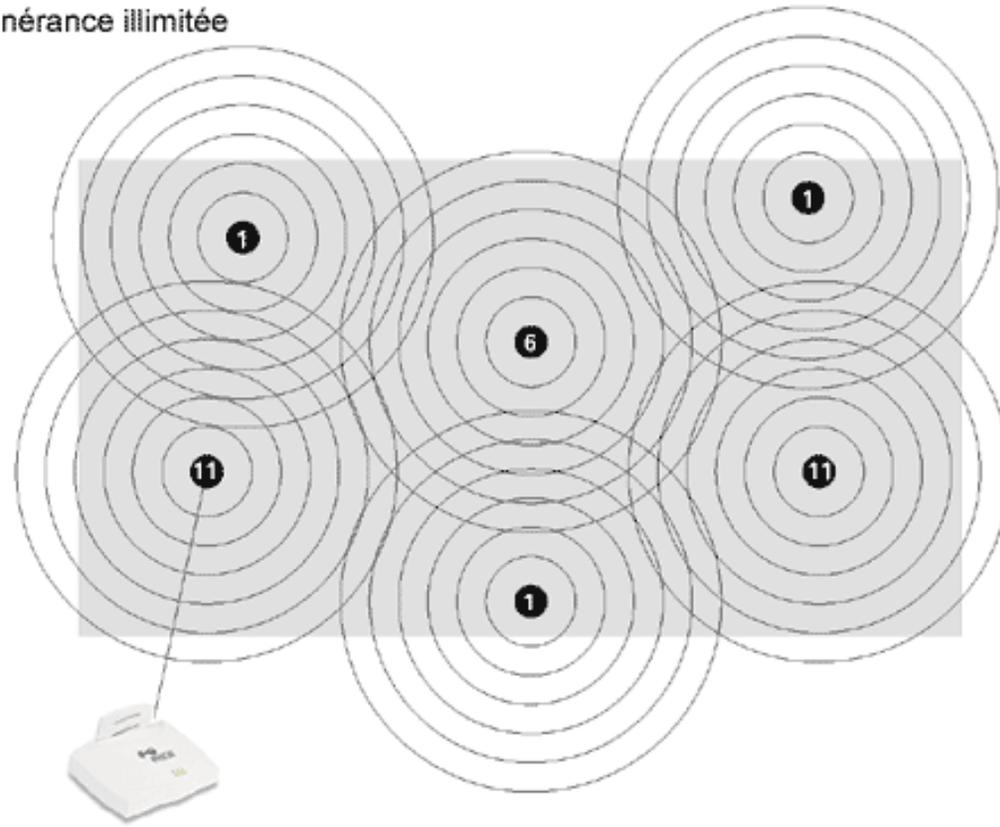




e. Chevauchement des zones d'émission

Lors de la réalisation d'une infrastructure ESS certaines zones d'émission se recouvrent. Ainsi, si deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distorsions du signal risquent de perturber la transmission. Ainsi pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle manière à ne pas avoir deux points d'accès utilisant les mêmes canaux proches l'un de l'autre.

Itinérance illimitée





2. Programmation des canaux

a. Les canaux disponibles

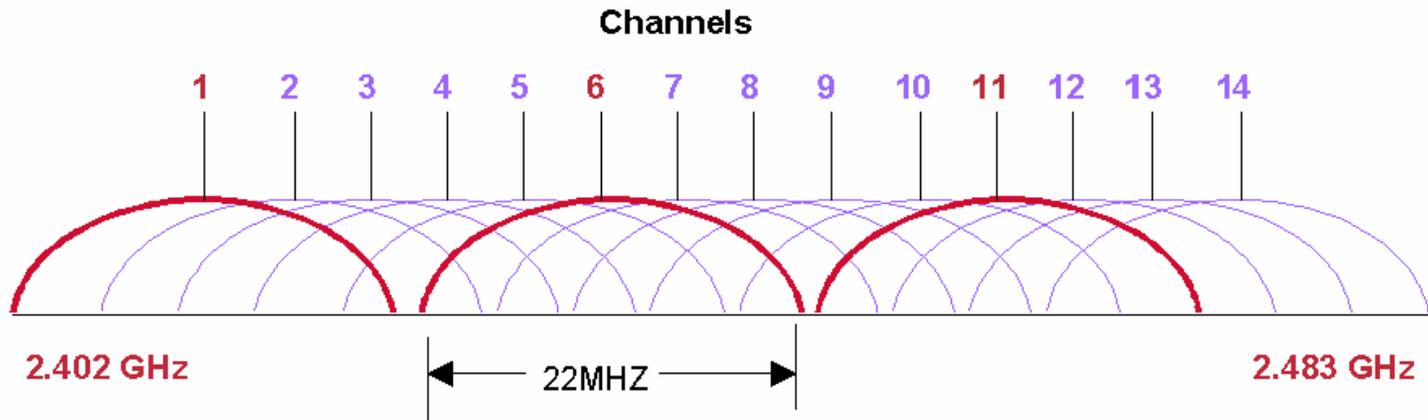
AFFECTATION DES CANAUX DANS LA BANDE 2400 MHz SELON LA NORME 802.11b		
Channel	Freq. Centrale MHz	Commentaires
1	2412	Les canaux 1 à 6 sont situés dans la bande amateur 2400-2450 MHz
2	2417	
3	2422	
4	2427	
5	2432	
6	2437	
7	2442	Les canaux 7 à 11 sont autorisés dans différents pays pour les dispositifs selon 802.11b mais ne peuvent être utilisés pour le Service Amateur
8	2447	
9	2452	
10	2457	
11	2462	
12	2467	Attribué en Europe seulement
13	2472	Attribué en Europe seulement
14	2477	Attribué au Japon seulement

Notons enfin qu'en France, l'utilisation de WiFi est libre en intérieur (limitation de puissance à 10 mW pour la bande fréquence 2400-2446,5 MHz, et à 100mW pour la bande de 2446,5 à 2483,5 GHz), mais régulée en extérieur. Cette régulation devrait toutefois s'assouplir au fur et à mesure de la libération des fréquences par l'armée qui devrait s'achever en 2004.

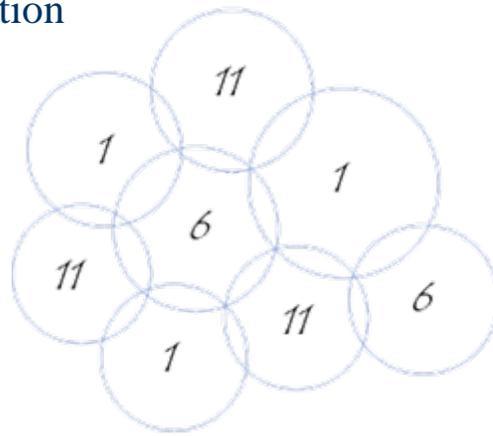


b. Choix des canaux

Pour une transmission de 11 Mbps correcte il est nécessaire de transmettre sur une bande de 22 MHz car, d'après le théorème de Shannon, la fréquence d'échantillonnage doit être au minimum égale au double du signal à numériser. Ainsi certains canaux recouvrent partiellement les canaux adjacents, c'est la raison pour laquelle des canaux isolés (les canaux 1, 6 et 11) distants les uns des autres de 25MHz sont généralement utilisés.



Exemple de configuration





F. La portée et les débits

1. Présentation

L'IEEE 802.11b définit un débit de transmission allant jusqu'à 11Mbit/s. Ils communiquent donc par les ondes radio parce que ces ondes ne sont pas affectées par les structures d'un bâtiment et qu'elles peuvent se réfléchir pour contourner les obstacles. Le débit du WLAN dépend de plusieurs facteurs, dont :

- le nombre d'utilisateurs,
- la portée des micro-cellules,
- les interférences,
- la propagation sur de multiples chemins ,
- le support des standards,
- le type de matériel
- les protocoles supplémentaires, les règles d'accès.

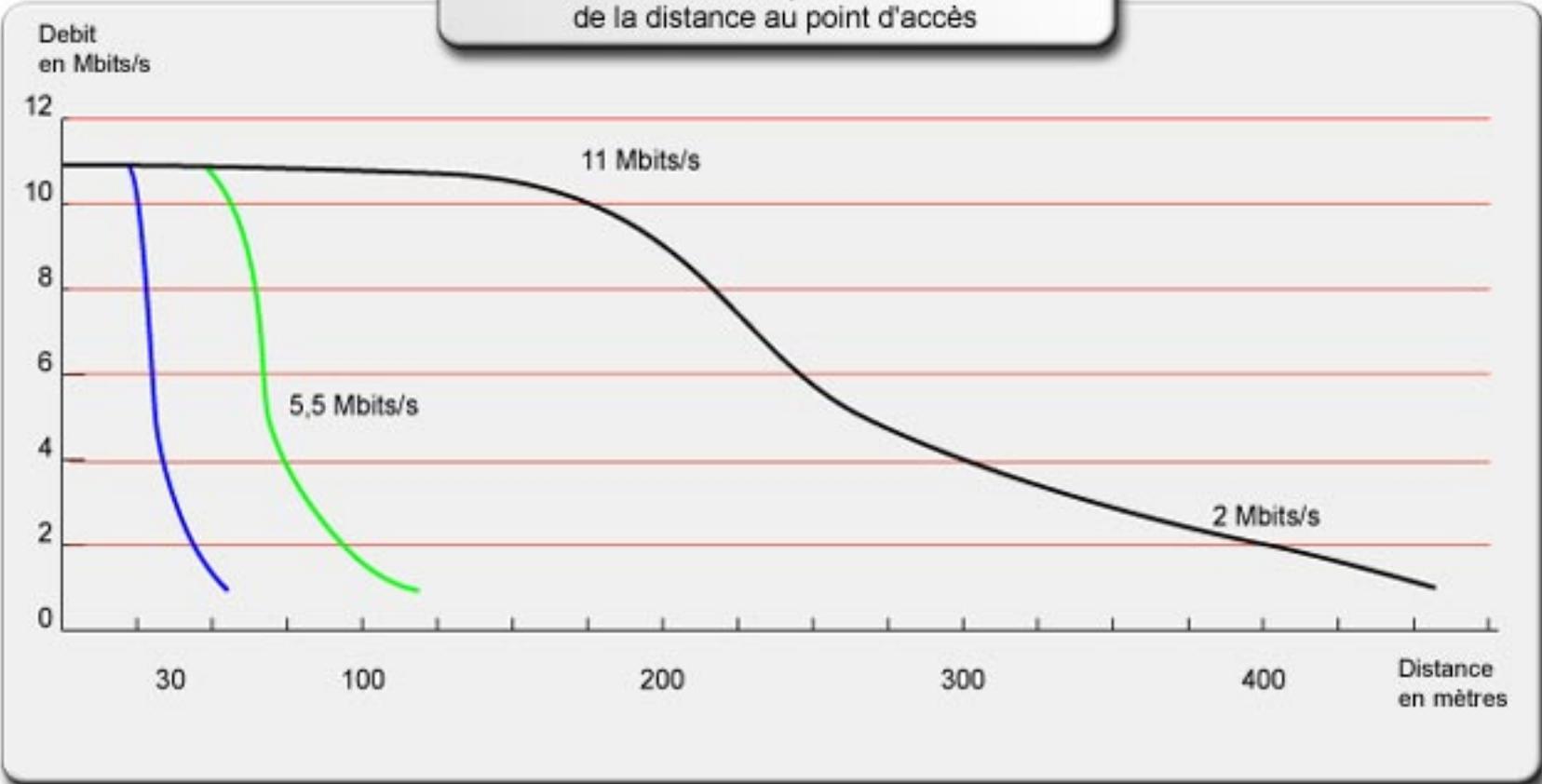
Ils réduisent en pratique la bande passante de 4 à 5 Mbps. Bien entendu, tout ceci affecte le trafic des données sur les portions filaires du réseau,

Débit	11 Mbits/s	5,5 Mbits/s	2 Mbits/s	1 Mbits/s
Portée en extérieur @ 100mW	65 m	90 m	125 m	180 m
Portée en intérieur @ 100mW	30 m	35 m	45 m	55 m



2. Mesure de débit

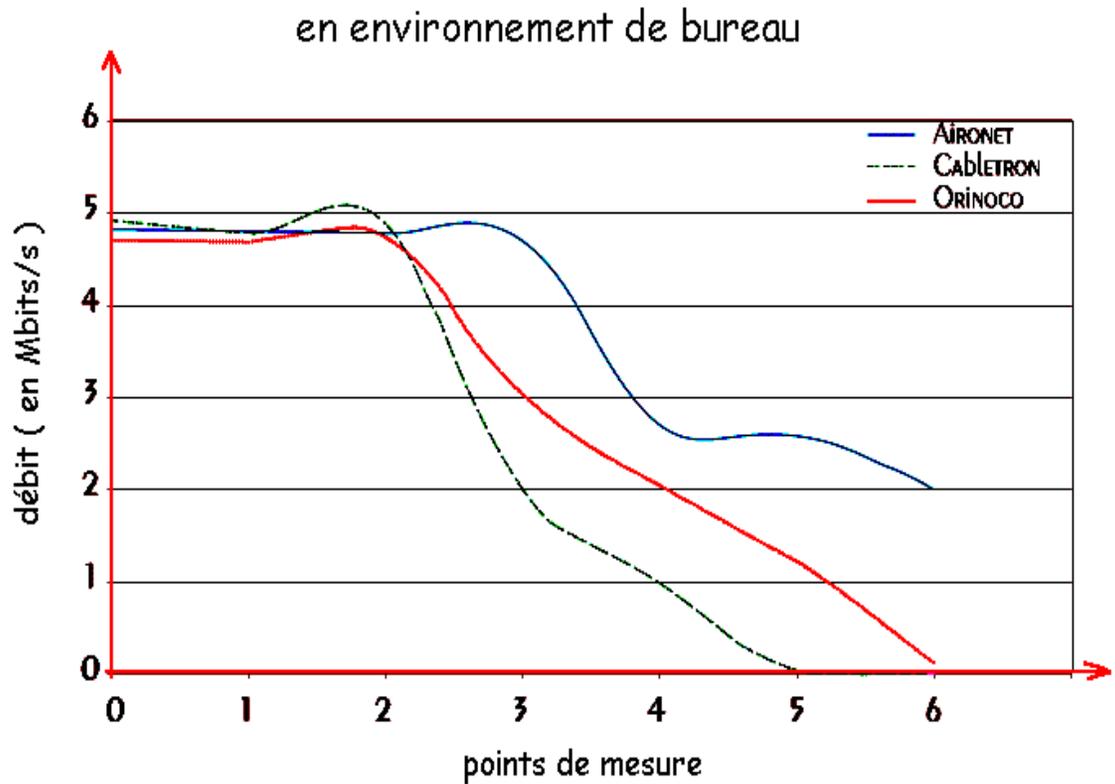
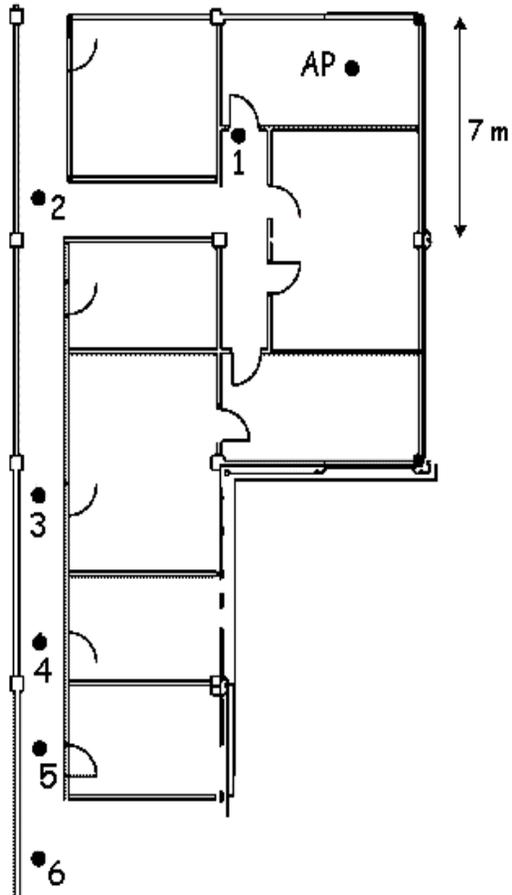
Variations de la bande passante en fonction de la distance au point d'accès



- Environnement ouvert
- Environnement semi-clos (de bureaux)
- Environnement clos (bureau cloisonné)



2. Exemple d'infrastructure réalisée en 802.11 en intérieur





G. La sécurité

La sécurité sur les réseaux WiFi est un sujet à la mode...

Il est possible d'écouter le réseau d'une entreprise dans la rue (WarDriving)

Comment sécuriser ces points d'accès :

- les AP ne doivent pas être liés aux réseaux de câbles, (Intercaler un firewall)
- les utilisateurs des réseaux WLAN doivent être authentifiés (VPN, SSH, 802.1X etc.),

En plus, il faut :

- désactiver la diffusion du SSID dans les AP, et activer le masquage du SSID,
- désactiver la communication client-client dans les AP,
- changer les paramètres par défaut des AP (le SSID, les mots de passe, l'adresse IP etc.),
- mettre à jour en temps réel le firmware des AP et des cartes sans fil,
- activer le contrôle d'accès au niveau MAC et IP (le mieux serait d'activer les deux),
- activer le chiffrement WEP (de 128- ou de 256-bits),
- éviter l'utilisation des clés secrètes WEP faciles à deviner,
- mettre en oeuvre la politique de changement fréquent des clés secrètes WEP,
- utiliser les AP gérant le WPA (TKIP et 802.1X),
- désactiver le protocole DHCP sur les réseaux WLAN, surtout pour les étendues des adresses.