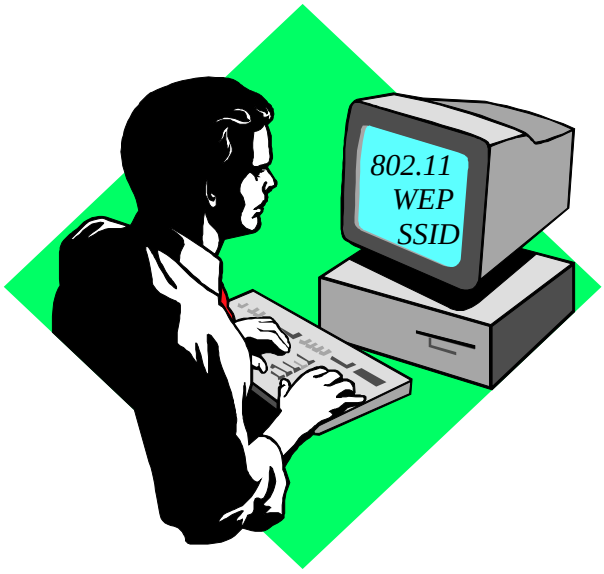
DI GALLO Frédéric

WiFi

L'essentiel qu'il faut savoir…



Extraits de source diverses récoltées en 2003.

AVANT-PROPOS

Exit câbles, fils et cordons! Les données jouent les filles de l'air. L'Internet haut débit s'invite partout dans la ville avant d'arroser les campagnes. Le 802.11 et ses dérivés, c'est la petite techno qui place le PC au cœur du réseau domestique. Et dire que l'armée ne voulait pas partager…

Les sources bibliographiques de cette synthèse sont référencées en annexe.

INTRODUCTION

MISE EN ŒUVRE DU WI-FI

SECURITE: LES PRECAUTIONS

ANNEXES

INTRODUCTION

INTRODUCTION

Le Wi-Fi est un **ensemble de fréquences radio** qui élimine les câbles, partage une connexion Internet et permet l'échange de données entre plusieurs postes.

La technologie est **connue aux Etats-Unis depuis 1997**. Là-bas, on recense 11 millions de points d'accès contre 80 dans l'Hexagone. Mais la France assouplit sa législation sur les ondes radio et s'emballe à son tour pour le Wi-Fi : les grands opérateurs montrent leur intérêt, les périphériques compatibles s'installent en rayon. Le passage aux réseaux sans fil ouvre de nouvelles perspectives d'usage communautaire de l'informatique. **Cap sur le Wi-Fi !**

I. Les réseaux sans fils

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".

NB: Remarque concernant l'orthographe des réseaux sans fils :Malgré l'utilisation de "sans fil", communément admise, les orthographes exactes sont "sans fils" et "sans -fil" On parle ainsi de "réseau sans fils" ou bien "du sans-fil".

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 comme c'est le cas avec les réseaux filaires. En contrepartie se pose le problème de la réglementation relatives 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. 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 fils.

1.1) 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) :

a) Réseaux personnels sans fils (WPAN)

Le réseau personnel sans fils (appelé également réseau individuel sans fils ou réseau domotique 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 :

- La principale technologie WPAN est la technologie **Bluetooth**, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps 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 gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein de petits périphériques. La version 1.2 réduit notamment les interférences avec les réseaux Wi-Fi.

- **HomeRF** (*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 intégré dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...).

- 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 utilisé pour la domotique (télécommandes) mais souffre toutefois des perturbations dûes aux interférences lumineuses. L'association **irDA** (infrared data association) formée en 1995 regroupe plus de 150 membres.

b) Réseaux locaux sans fils (WLAN)

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

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

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

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

c) 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.

d) 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 connecté à un réseau étendu sans fils. Les principales technologies sont les suivantes :

- GSM (*Global System for Mobile Communication* ou Groupe Spécial Mobile)
- GPRS (*General Packet Radio Service*)
- UMTS (*Universal Mobile Telecommunication System*)
- **Wimax** (standard de réseau sans fils poussé par Intel avec Nokia, Fujitsu et Prowim). Basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit maximum de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est davantage destiné aux utilisateurs itinérants.

1.2) Historique

En 1997; alors que l'attention est accaparée par le succès d'Internet et l'euphorie boursière montante, un événement est passé inaperçu sauf pour quelques spécialistes et observateurs: l'adoption du standard IEEE 802.11 ou **Ethernet sans fil**. Exploitant la bande de fréquence de 2,4 GHz, le 802.11 plafonne à un débit de 2 Mbits/s au maximum. Ce précurseur est suivi de plusieurs déclinaisons dont le célèbre Wi-Fi qui connaît un franc succès, aidé par le volontarisme des fabricants, distributeurs et fournisseurs de services... Wi-Fi, est un nom composé à la manière de hi-fi et signifiant ***Wireless Fidelity***. Il désigne les différentes déclinaisons de la norme IEEE 802.11 qui permet à plusieurs ordinateurs de communiquer sans fil en utilisant comme support les ondes radio. **Les câbles disparaissent enfin**. Avantage: le déploiement d'un réseau Wi-Fi est assez simple, le prix plutôt modeste en comparaison d'autres technologies.

Le Wi-Fi est une technologie intéressante pour de nombreuses sociétés liées au monde des télécoms et d'Internet. Les collectivités locales et **surtout les particuliers** profitent de la facilité d'accès à Internet haut débit liée à cette norme. Dans sa déclinaison la plus connue, 802.11 b, le Wi-Fi utilise la bande de fréquence de 2,4 GHz et atteint un débit théorique de 11 Mbits/s (contre 128, 512 Kbits/s ou 1 Mbits/s pour l'ADSL), le 802.11a culmine à 22 Mbits/s et le 802.11 g, enfin, flirte avec les 54 Mbits/s. Le Wi-Fi peut certes servir à surfer sur Internet, mais pas seulement. Il autorise l'organisation de réseaux -pourvus ou pas d'Internet - pour échanger des fichiers, des données, et bien entendu pour jouer:.. Ce ne sont là que quelques exemples de ses usages possibles Les avantages des réseaux sans fil ne sont plus à démontrer surtout à une génération de plus en plus habituée à la mobilité. La multiplication des appareils (PDA, PC portables, terminaux et bientôt les téléphones portables) capables de communiquer entre eux en fait le support idéal des réseaux modernes.

II. Présentation de WiFi (802.11)

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- **La couche physique** (notée parfois couche PHY), proposant trois types de codage de l'information.
- **La couche liaison** de données, constitué de deux sous-couches : le contrôle de la liaison logique (*Logical Link Control*, ou LLC) et le contrôle d'accès au support (*Media Access Control*, ou MAC)

La couche physique 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 :

Couche Liaison de données (MAC)	802.2		
	802.11		
Couche Physique (PHY)	DSSS	FHSS	Infrarouges

Il est possible d'utiliser n'importe quel protocole sur un réseau sans fil WiFi au même titre que sur un réseau ethernet.

3.1) Les différentes normes WiFi

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. La logique aurait voulu un ordre alphabétique. 80211a pour le moins performant 80211 b, c.. mais non. 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 permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Le 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 rééls) 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 (*bridging*)	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 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 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 *Inter-Access point roaming protocol* 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.
802.11g		La norme 802.11g offrira un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. Cette norme vient d'être validée. La norme 802.11g a une compatibilité ascendante avec la norme b.
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréq. 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.
802.11IR		La norme 802.11j a été élaborée 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.

3.2) Les équipements WiFi

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

a) Les adaptateurs sans fil ou cartes d'acc ès

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. A noter que les composants Wi-Fi deviennent des standards sur les portables (label Centrino d'Intel).

b) 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. Cette sorte de hub est l'élément nécessaire pour déployer un réseau centralisé en mode infrastructure. Certains modèles proposent des fonctions de modem ADSL et comprennent plus ou moins de fonctions comme un pare-feu.

c) Les autres

- **Smart Display**: écrans mobiles, soutenus par Microsoft.
- **Chaînes WiFi**: offrant la capacité de lire les MP3 directement sur le disque dur d'un ordinateur grâce à l'interface Ethernet sans fil intégrée. Elle préfigure toute une génération de produits, capables de lire, outre les CD audio, les radios qui émettent en MP3 sur Internet.
- **Assistant personnel**: les PDA intégrant le WiFi est parfois plus avantageux qu'un portable pour lire ses mails, importer des documents voir surfer sur le net.
- **Rétroprojecteurs**: pour des présentations avec portables mobiles.
- **Caméra video**: transmettre des images à distance à l'ordinateur qui les enregistre.

Les composants Wi-Fi ne sont pas plus onéreux que ceux des réseaux filaires, bientôt toutes les plates-formes seront vendues avec des modules Wi-Fi intégrés. C'est déjà le cas dans le monde des PC portables, qui, sous l'impulsion d'Intel, fait sa révolution sans fil grâce au Centrino.

Pour plus de détails sur le fonctionnement de la technologie WiFi, se reporter en annexe.

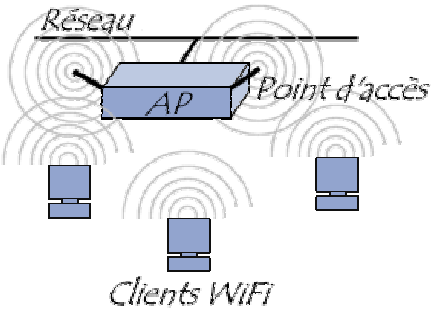
LA MISE EN OEUVRE

MISE EN ŒUVRE DU WI-FI

I. Les modes opératoires

1.1) Le mode infrastructure

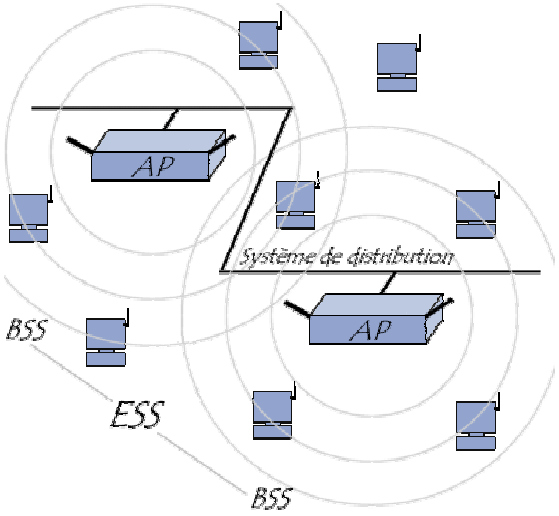
a) Le principe:



En mode infrastructure, chaque **ordinateur station** (notée STA) se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base (en anglais *Basic Service Set*, noté BSS) et constitue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.

Il est possible de **relier plusieurs points d'accès** entre eux (ou plus exactement plusieurs BSS) par une liaison appelée **système de distribution** (notée DS pour *Distribution System*) afin de constituer un **ensemble de services étendu** (*Extended Service Set* ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil !

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 et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.



Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé itinérance (en anglais ***roaming***).

b) La communication avec le point d'accès

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

En effet chaque point d'accès diffuse régulièrement (à raison d'un envoi toutes les 0.1 secondes environ) une trame balise (nommée *beacon* en anglais) donnant des informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option.

A chaque requête de sondage reçue, le point d'accès vérifie l'ESSID et la demande de débit présents dans la trame balise. Si l'ESSID correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe. En effet d'une manière générale, plus un point d'accès est proche, meilleur est le débit.

Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même SSID) pourra ainsi choisir le point d'accès offrant le meilleur compromis de débit et de charge.

***Remarque**: Lorsqu'une station se trouve dans le rayon d'action de plusieurs points d'accès, c'est elle qui choisit auquel se connecter !*

c) Les hotspots:

Un hotspot est une bornes d'accès Wi-Fi installée dans les lieux publics et de passage, donnant accès à un réseau métropolitain privé ou public. Les métiers des services et de la restauration ne s'y sont pas trompés et l'intérêt pour les hotspots va grandissant pour attirer une clientèle de consommateurs technophiles. Il est même question de transformer les antiques taxiphones des bars en hotspots.

Aux États-Unis et en Grande Bretagne, les hot spots se multiplient, notamment dans les aéroports, les gares, les hôtels, les centres de congrès, ainsi que dans les entreprises en France, où l'on recense quelque 80 hotspots publics, de nombreux projets voient le jour depuis quelques mois Une étude de l'institut IDC/Orange menée en décembre 2002 prévoit que d'ici 2005, 20 % des accès aux systèmes d'information des entreprises se feront via des connexions sans fil Cependant, beaucoup de questions restent encore en suspens comme la sécurité, la gestion du roaming (maintien de la connexion d'un point d'accès à un autre, voire d'un opérateur à un autre), la saturation des fréquences, les problèmes de réglementation.

d) Créer un hotspot de quartier

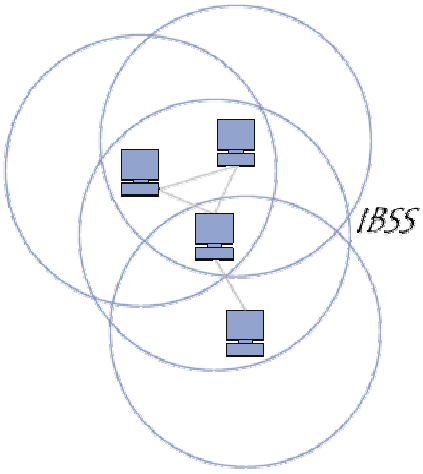
Depuis que le régulateur a autorisé l'usage de la bande de 2,4 GHz pour la création de réseau Ethernet sans fil, il est possible aux particuliers de mettre en place leur propre réseau. Il suffit de respecter les limitations de puissance imposées pour pouvoir diffuser jusqu'à 100 m. Pour créer un hotspot de quartier, la procédure n'est pas plus compliquée que celle en intérieur. Elle requiert toutefois un peu de planification et quelques précautions. La planification sert à déterminer le meilleur emplacement pour l'antenne qui peut être allongée, pour être placée en extérieur sur un toit ou un balcon Il faut éviter les couloirs et les portes qui réduisent la portée et créent des interférences en opposition de phase (plusieurs répliques du même signal). Les obstacles sont à éviter ce qui paraît évident, ce qui l'est moins c'est la prise en compte des obstacles mobiles. Rien n'est plus hermétique aux ondes qu'un camion stationné dans la rue d'à côté. Naturellement les sources d'interférences doivent être identifiées et leur impact sur les transmissions évalué.

Une fois ce travail accompli, l'installation du réseau peut commencer. Selon le choix de l'administrateur, le réseau peut être ouvert ou sécurisé. Dans le premier cas, l'usage d'une vieille machine ne contenant pas de données personnelles est le plus conseillé. Dans le cas où le réseau est sécurisé, les utilisateurs potentiels doivent, recevoir chacun un login, un mot de passe et éventuellement une clé.

e) Que dit la loi ?

Cette possibilité d'atteindre d'autres utilisateurs dans le voisinage -qui de proche en proche créent un maillage de réseaux autonomes- a de tout temps inquiété les États. La France n'est pas le seul pays à se montrer méfiant. La bande de fréquence dévolue au 802.11 (de 2400 à 2483,5 MHz) est restée longtemps **l'otage des militaires**. Jusqu'à aujourd'hui et dans certains départements (voir la liste :www.art-telecom.fr/communiques/communiques/2003/index-c030203-58.htm) l'installation d'un réseau sans fil en extérieur est soumise à autorisation du ministère de la Défense. Il s'agit de ne pas brouiller ou induire en erreur certains radars de l'armée française et de l'Otan qui utilisent les portions hautes (2454 à 2483,5 MHz) de la bande. Ainsi, l'**ART** (Autorité de régulation des télécommunications) a "libéré" l'utilisation de bornes Wi-Fi aux particuliers en intérieur comme en extérieur, mais sous réserve de respecter les valeurs maximales de puissance. En clair; il est possible à tout un chacun d'utiliser librement un réseau à l'intérieur des murs de son habitation à condition que la puissance du rayonnement n'excède pas 100 mW En extérieur, la limite est réduite à 10 mW, soit un débit de données réduit à mesure que l'on s'éloigne du points d'accès. Au-delà d'un rayon de 100 mètres, le débit réel chute considérablement. Le recours à une antenne extérieur de 100 mW (limite maximale infranchissable) est soumis à l'autorisation du ministère de la Défense. Les décisions de l'ART rendent possible le partage entre plusieurs utilisateurs d'un même accès haut débit (ADSL, câble) en installant une borne Wi-Fi. Il faut cependant vérifier que le contrat d'abonné avec le fournisseur d'accès ne s'y oppose pas. En suspens, une question juridique épineuse: qui du fournisseur d'accès Wi-Fi ou du FAI est juridiquement responsable devant la loi ?

1.2) Le mode ad hoc



En mode **ad hoc**, les machines sans fil clientes se connectent les unes aux autres afin de constituer un **réseau point à point** (*peer to peer* en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès.

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais *independant basic service* set, abrégé en IBSS).

Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure.

Dans un réseau ad hoc, la portée du BSS indépendant est déterminé par la portée de chaque station. Cela signifie que si deux des stations du réseaux sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi un IBSS est par définition un réseau sans fil restreint.

II. Mise en place d'un réseau

2.1) Déployer un réseau sans fil

Depuis la décision de l'ART d'autoriser, sous certaines conditions, l'utilisation de réseaux sans fil, les particuliers découvrent les joies de la mobilité domestique. Pour peu de disposer d'une connexion haut débit, le partage familial de celle-ci élimine le traditionnel embouteillage pour consulter l'e-mail. Avec Windows XP, la mise en place d'un réseau domestique est prise en charge par le système qui fournit les informations de configuration de la couche de transport (TCP/IP). Il est même proposé de créer une disquette de configuration des autres postes clients. Le réseau Ethernet 802.11b est fondé sur une architecture cellulaire où chaque alvéole est contrôlé par un AP (ou *Access Point*). Relié à un ordinateur connecté à Internet cet AP sert alors de routeur Internet tandis que le PC hôte devient une passerelle dirigeant le trafic collecté par l'AP vers le Web Cette architecture centralisée grâce à un serveur est appelée Infrastructure. On peut aussi construire un réseau sans fil en Ad-hoc ou *peer-to-peer* où les postes clients communiquent les uns directement avec les autres à égalité. Les machines connectées échangent périodiquement leurs tables de routage et établissent des protocoles de routage en temps réel: les chemins sont établis à la demande. Pour deux ordinateurs, il vous faut alors envisager une solution de type Ad-hoc. Elle consiste à doter chaque PC d'une interface réseau Wi-Fi comme les adaptateurs USB. Une fois configurés, les deux PC peuvent partager une connexion Internet, l'un servant de passerelle à l'autre.

Mais pour déployer un réseau de 3 postes ou plus, une solution plus élaborée est à envisager: Il faut alors opter pour une borne d'accès (AP) et équiper postes clients de cartes d'accès. Les cartes adaptatrices PCI sont déconseillée: prix plus élevé et l'antenne d'une carte PCI est collée à l'arrière de la machine posée au sol ou au mieux sur le bureau. Ce qui n'est l'idéal pour une bonne réception.

2.2) Combattre les interférences

Contrairement aux réseaux filaires, les réseaux sans fil requièrent des précautions supplémentaires pour assurer la meilleure propagation possible des ondes Le Wi-Fi est une technologie basée sur des spécifications qui englobent des protocoles divers spécialisés dans les communications et le transport des données par les airs. Des technologies de transfert comme DSSS (Direct Sequence Spread Spectrum) ou FHSS (frequency Hopping Spread Spectrum) sont là pour corriger certains problèmes d'interférence, mais elles ne vous dispensent pas de prendre quelques précautions Laccès au réseau sans fil se fait par le protocole CSMA (Carrier Sense Multiple Access) Quand une interface du réseau veut émettre, elle écoute le support de transmission et si celui-ci est libre, alors elle émet Les interférences diffusées sur les canaux écoutés provoquent une attente de la part de l'interface qui veut émettre, ce qui ralentit le réseau même si l'indicateur de débit est au maximum Il vous est donc fortement conseillé de réduire, voire d'éliminer, toutes les sources possibles d'interférences En premier lieu les appareils Bluetooth qui opèrent dans la bande de fréquence de 2,4 GHz ainsi que les fours à micro-ondes Assurez-vous que votre téléphone sans fil résidentiel ne squatte pas les fréquences utilisées Les obstacles sont également une source d'interférences et d'affaiblissement du signal Il ne s'agit pas seulement d'obstacles visibles tels que les murs -surtout ceux en béton -et les arbres qui affaiblissent le signal, mais aussi d'obstacles non visibles tout aussi perturbateurs, le champ magnétique d'une télévision par exemple.

SECURITE
Les principales précautions à prendre

SECURITE: LES PRECAUTIONS

Les ondes radio-électriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations).

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

Là où le bât blesse c'est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues "publiques" dans le rayon de couverture du point d'accès !

I. Le chiffrement

1.1) WEP

Tandis que les sirènes du Wi-Fi chantent à qui veut les entendre, les hackers et autres casseurs de code n'ont pas tardé à démontrer la vulnérabilité du **chiffrement WEP** (*Wired Equivalent Privacy*) utilisé dans le Wi-Fi. Le principe du fonctionnement du WEP est basé sur des clés de cryptage partagées interdisant l'accès à toutes les personnes ne connaissant pas ce mot de passe. Chaque périphérique 802.11 b (cartes, points d'accès, etc.) utilise une clé . soit un mot de passe, soit une clé dérivée de ce mot de passe. La faille provient du mode de fonctionnement de **l'algorithme de chiffrement (RC4)** qui permet à tout décodeur de déduire certaines informations menant à la reconstitution de la clé. Les parades sont nombreuses mais ne garantissent pas une efficacité à 100 %. Il est toutefois possible de dissuader les intrus en multipliant les obstacles devant eux. Des protocoles de sécurité tels que **IPSec, SSL ou SSH** ne sont pas à la portée du premier utilisateur venu. Dans tous les cas, le WEP est utile et l'activer c'est déjà éliminer certains risques. Il existe une autre solution qui consiste à considérer le réseau sans fil comme une zone publique.

Le cas d'un partage de connexion Internet entre voisins est le plus typique de cette configuration à condition qu'un routeur sans fil sert de passerelle et non pas un PC qui risque de contenir des informations confidentielles.

1.2) WAP

Pour pallier les insuffisances du WEP, un remplaçant est à l'étude. Appelé **WPA** (*Wi-Fi Protected Access*), son fonctionnement repose sur un système **d'échange de clés dynamiques**, renouvelées tous les 10 ko de données Ce procédé, appelé **TKIP** (*Temporal Key Integrity Protocol*), protége mieux les clés du décryptage et devrait améliorer sensiblement la sécurité des réseaux sans fil même si l'algorithme utilisé reste inchangé

D'après la plupart des constructeurs, il est possible de mettre à jour le firmware de votre matériel 802.11b pour intégrer le WPA.

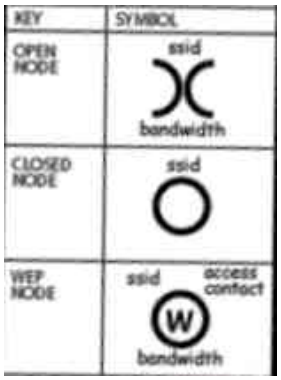
1.3) Verrouillez votre réseau !

Ne vous reposez pas sur le seul protocole WEP pour sécuriser votre réseau. Un bon administrateur doit connaître les possibilités de son matériel sur le bout des doigts pour le configurer au mieux. Pour s'identifier auprès d'un AP, les clients d'un réseau sans fil 80211 b utilisent un **identifiant de réseau** ou **SSID** (*Service Set Identifier*). Sans algorithme de chiffrement, l'identifiant de réseau n'est pas crypté lors de la transmission des trames Un utilisateur mal intentionné, qui écoute le réseau, peut obtenir le SSID lui permettant ainsi d'accéder au réseau. De plus, le décodage du SSID est souvent facilité par le fait qu'il porte un nom explicite. nom du service ou de l'organisme utilisateur du réseau par exemple.

Afin de supprimer la vulnérabilité du SSID, le protocole de chiffrement WEP à été mis en place, mais **il n'est pas suffisant**. Des précautions supplémentaires peuvent être prises pour compliquer la tâche des « grandes oreilles » malveillantes. La première est de **supprimer la configuration par défaut** des AP en modifiant la clef WEP si elle est activée et l'identifiant réseau (SSID) installés par défaut. Il est également impératif de pr**otéger ou de désactiver les services d'administration** fournis avec l'interface. En dernier lieu, il peut s'avérer nécessaire de **réduire la puissance d'émission** de l'AP au minimum nécessaire afin de diminuer le rayonnement des ondes. Cette action n'empêche pas un utilisateur mal intentionné muni d'un matériel d'écoute performant de capter vos émissions, mais c'est plus difficile. Pour augmenter la sécurité de votre réseau, il est également possible sur certains équipements de **filtrer les adresses MAC** ayant le droit de communiquer avec le pont. Cette liste doit être reproduite sur chaque pont du réseau sans fil si vous désirez garder toute la mobilité du réseau. Malgré cela, il est toujours possible à un utilisateur mal intentionné de récupérer le trafic échangé entre deux machines (même si le protocole WEP est actif), voire de simuler une adresse MAC décodée, si celui-ci se trouve dans le périmètre du réseau Alors soyez paranoïaques !

II. Le piratage

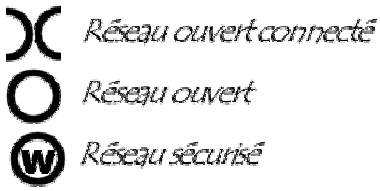
2.1) Une nouvelle génération de hackers



Comme toute nouvelle technologie, Ethernet sans fil a tout de suite intéressé les hackers qui se sont lancés dans de nouvelles activités de piratage dont le ***wardriving*** (ou war-Xing pour "war crossing"). Venue des Etats-Unis, cette pratique consiste à détecter les réseaux sans fil publics ou privés et à tenter de les pénétrer. Les pirates" patrouillent" en voiture dans des quartiers délimités à l'avance. À l'aide d'un ordinateur portable et d'une carte réseau PCMCIA, 802.11b de préférence, les pirates scannent les fréquences à la recherche de réseaux. C'est la technique de base qui peut être améliorée en trafiquant une antenne directionnelle couplée à de puissants logiciels de détection. Des logiciels spécialisés dans ce type d'activité permettent même d'établir une **cartographie très précise** en exploitant un matériel de géolocalisation (GPS, *Global Positionning System*). Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fil déployés non sécurisés, offrant même parfois un accès à Internet ! De nombreux sites capitalisant ces informations ont vu le jour sur Internet, si bien que des

étudiants londoniens ont eu l'idée d'inventer un "**langage des signes**" dont le but est de rendre visible les réseaux sans fil en dessinant à même le trottoir des symboles à la craie indiquant la présence d'un réseau wireless, il s'agit du « **war-chalking** » (francisé en craieFiti ou craie-fiti). Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet, un rond signale la présence d'un réseau sans fil ouvert sans accès à un réseau filaire et enfin un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé.

Cette nouvelle forme de piratage, née avec l'avènement des réseaux sans fil pose de sérieux problèmes de sécurité et de confidentialité pour les entreprises équipées en réseaux sans fil 802.11b. À tel point que la CNIL a tiré la sonnette d'alarme en mettant en garde les utilisateurs contre les risques de piratage des réseaux radio. Certains pratiquent le wardriving comme un jeu, mais il peut être redoutable dans le domaine de l'espionnage industriel.



Grâce à la propagation des ondes, un réseau sans fil est un ensemble ouvert. Il appartient à son administrateur de décider s'il le rend disponible aux autres et quels sont les usages qu'il autorise accès partagé à Internet ou jeux.

2.2) Les risques en matière de sécurité

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

- L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil,
- Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à Internet,
- Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences,
- Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices.

a) L'interception de données

Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

b) L'intrusion réseau

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

c) Le brouillage radio

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisé dans le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

d) Les dénis de service

La méthode d'accès au réseau de la norme 802.11 est basé sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connus, il est simple pour un pirate d'envoyer des paquets demandant la désassociation de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fil est consommatrice d'énergie. Même si les périphériques sans fil sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

III. Les solutions

3.1) Une infrastructure adaptée

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à **positionner intelligemment les points d'accès** selon la zone que l'on souhaite couvrir. Eviter les murs extérieurs mais choisir plutôt un emplacement central. En se promenant autour de l'immeuble, on peut établir le périmètre à l'intérieur duquel la borne est accessible. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de **réduire la puissance de la borne** d'accès afin d'adapter sa portée à la zone à couvrir.

3.2) Eviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le **mot de passe de l'administrateur**. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration (généralement via une interface web sur un port spécifique de la borne d'accès) notamment pour définir un mot de passe d'administration.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître **l'identifiant du réseau** (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de **désactiver la diffusion** (SSID broadcast: diffusion du nom SSID) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur **la marque ou le modèle du point d'accès** utilisé. L'idéal est même de modifiez régulièrement le nom SSID!

Il faudrait même éviter de choisir des mots reprenant l'identité de l'entreprise ou sa localisation, qui sont susceptibles d'être plus facilement devinés.

3.3) Activer le cryptage WEP ou WAP

C'est assez étonnant, mais de nombreuses bornes et interfaces WiFi sont installées sans mise en place du cryptage WEP qui permet de limiter les risques d'interception de données. Il est fortement recommandé de préférer une **clé WEP sur 128 bits** à celle, utilisée souvent par défaut, de 64 bits. Certes l'activation du WEP est un plus mais il faut savoir qu'elle ralentit le débit d'information: temps de cryptage - décryptage. Sans oublier de **modifier les clés de cryptage WEP régulièrement**.

3.4) Le filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC). Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. Les points d'accès permettent généralement dans leur interface de configuration de gérer une **liste de droits d'accès** (appelée ACL) basée sur les **adresses MAC** des équipements autorisés à se connecter au réseau sans fil. En activant ce MAC Address Filtering (Filtrage des adresses MAC), même si cette précaution est un peu contraignante, cela permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résout pas le problème de la confidentialité des échanges.

3.5) Améliorer l'authentification

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (en anglais AAS pour *Authentication*, *Authorization*, and *Accounting*) il est possible de recourir à un **serveur RADIUS** (*Remote Authentication Dial-In User Service*). Le protocole RADIUS (défini par les RFC 2865 et 2866), est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

3.6) Mise en place d'un VPN

Pour connecter les utilisateurs nomades se branchant au réseau par le biais d'une borne publique, et pour toutes les communications nécessitant un haut niveau de sécurisation, il faut mettre en place un **réseau privé virtuel** (VPN) qui offrira un bon niveau de sécurité et empêchera la plupart des intrusions indésirables.

3.7) Définir des adresses IP fixes

Les risques d'intrusion externes sont bien moindres en attribuant des a**dresses IP fixes aux stations de la flotte** bénéficiant d'une connexion sans fil. Il est ainsi possible de gérer une table d'adresses des connexions autorisées. Il faut, dans ce cas, **désactiver la fonction DHCP** au niveau du serveur auquel est connectée la borne WiFi.

3.7) Installer un pare-feu

On peut aussi installez un **firewall** comme si le point d'accès était une connexion internet. Ce firewall peut être le serveur **IPsec** (VPN) des clients sans fils.

Un réseau WiFi "sécurisé" peut se schématiser comme cela. On considère ici que tout le réseau WiFi est étranger au réseau local, au même titre qu'Internet. L'utilisation d'un pare-feu (firewall) comme pour la connexion Internet, permet de filtrer les adresses MAC associé à des adresses IP fixes. Dans le cas du VPN, le firewall ou un serveur derrière ce dernier fait office de terminal VPN. Certains points d'accès proposent des "petits" firewall permettant de faire un filtrage de plus sur les clients de votre réseau.

Chacun est libre de modifier ces règles en ajoutant des couches supplémentaires. Sachez que le futur protocole IP ipv6 contient dans ses paquets la sécurisation ipsec. L'ipv6 peut être utilisé en WiFi si les clients gèrent l'ipv6, actuellement tous les Linux, Unix ont une pile ipv6 fonctionnelle, sur Windows 2000 et XP l'ipv6 est activable et utilisable mais sera proposé par défaut dans les prochaines versions.

IV. En conclusion

La sécurisation d'un réseau qu'il soit filaire ou sans fils est possible par de nombreux moyens matériels et/ou logiciels. Son choix dépend de l'utilisation que vous voulez faire de votre réseau et des moyens dont vous disposez.

ANNEXES

ANNEXES

I. La technologie employée par le Wi-Fi

1.1) Les canaux de transmission

On appelle canal de transmission une bande étroite de fréquence utilisable pour une communication. Dans chaque pays, le gouvernement est en général le régulateur de l'utilisation des bandes de fréquences, car il est souvent le principal consommateur pour des usages militaires.

Toutefois les gouvernements proposent des bandes de fréquence pour une utilisation libre, c'est-à-dire ne nécessitant pas de licence de radiocommunication. Les organismes chargés de réguler l'utilisation des fréquences radio sont :

- l'ETSI (European Telecommunications Standards Institute) en Europe
- la FCC (Federal Communications Commission) aux Etats-Unis
- le MKK (Kensa-kentei Kyokai) au Japon

En 1985 les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine. Ces bandes de fréquence, baptisées ISM (Industrial, Scientific, and Medical), sont les bandes 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz.

En Europe la bande s'étalant de 890 à 915 MHz est utilisée pour les communications mobiles (GSM), ainsi seules les bandes 2.400 à 2.4835 GHz et 5.725 à 5.850 GHz sont disponibles pour une utilisation radio-amateur.

1.2) Les technologies de transmission

Les réseaux locaux radio-électriques utilisent des ondes radio ou infrarouges afin de transmettre des données. La technique utilisée à l'origine pour les transmissions radio est appelé transmission en bande étroite, elle consiste à passer les différentes communications sur des canaux différents. Les transmissions radio sont toutefois soumises à de nombreuses contraintes rendant ce type de transmission non suffisantes. Ces contraintes sont notamment :

- Le partage de la bande passante entre les différentes stations présentes dans une même cellule.
- La propagation par des chemins multiples d'une onde radio. Un onde radio peut en effet se propager dans différentes direction et éventuellement être réfléchie ou réfractés par des objets de l'environnement physique, si bien qu'un récepteur peut être amené recevoir à quelques instants d'intervalles deux mêmes informations ayant emprunté des cheminements différents par réflexions successives.

La couche physique de la norme 802.11 définit ainsi initialement plusieurs techniques de transmission permettant de limiter les problèmes dûs aux interférences :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe,
- La technologie infrarouge.

a) La technique à bande étroite

La technique à bande étroite (*narrow band*) consiste à utiliser une fréquence radio spécifique pour la transmission et la réception de données. La bande de fréquence utilisée doit être aussi petite que possible afin de limiter les interférences sur les bandes adjacentes.

b) Les techniques d'étalement de spectre

La norme IEEE 802.11 propose deux techniques de modulation de fréquence pour la transmission de données issues des technologies militaires. Ces techniques, appelées étalement de spectre (en anglais spread spectrum) consistent à utiliser une bande de fréquence large pour transmettre des données à faible puissance. On distingue deux techniques d'étalement de spectre :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe

c) La technique de saut de fréquence

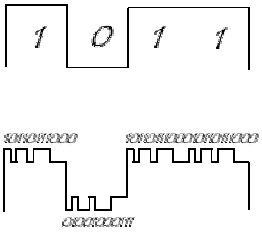
La technique FHSS (*Frequency Hopping Spread Spectrum*, en français étalement de spectre par saut de fréquence ou étalement de spectre par évasion de fréquence) consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant 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 se fait ainsi 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'étalement de spectre par saut de fréquence a originalement été conçue dans un but militaire afin d'empêcher l'écoute des transmissions radio. En effet, une station ne connaissant pas la combinaison de fréquence à utiliser ne pouvait pas écouter la communication car il lui était impossible dans le temps imparti de localiser la fréquence sur laquelle le signal était émis puis de chercher la nouvelle fréquence.

Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, l'étalement de spectre par saut de fréquence n'assure donc plus cette fonction de sécurisation des échanges. En contrepartie, le FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

d) Etalement de spectre à séquence directe

La technique DSSS (*Direct Sequence Spread Spectrum*, étalement de spectre à séquence directe) consiste à transmettre pour chaque bit une séquence Barker (parfois appelée bruit pseudo-aléatoire ou en anglais pseudo-random noise, noté PN) de bits. Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

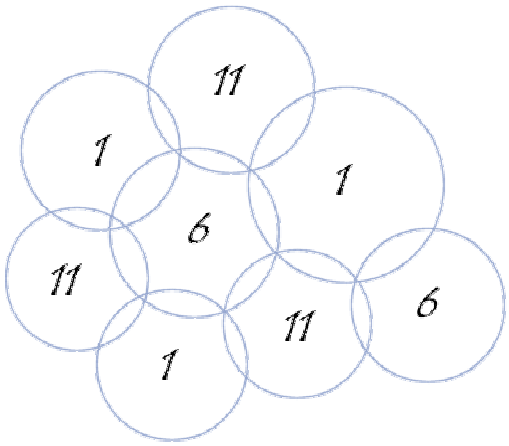


La couche physique de la norme 802.11 définit une séquence de 11 bits (10110111000) pour représenter un 1 et son complément (01001000111) pour coder un 0. On appelle *chip* ou *chipping code* (en français puce) chaque bit encodé à l'aide de la séquence. Cette technique (appelée chipping) revient donc à moduler chaque bit avec la séquence *barker*.

Grâce au chipping de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions, voir de la correction d'erreurs.

Dans le standard 802.11b, la bande de fréquence 2.400-2.4835 GHz (d'une largeur de 83.5 MHz) a été découpée en 14 canaux séparés de 5MHz, dont seuls les 11 premiers sont utilisables aux Etats-Unis. Seuls les canaux 10 à 13 sont utilisables en France.

Toutefois, 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.



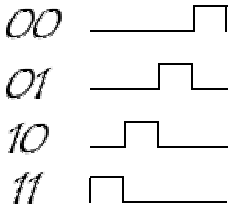
Ainsi, si deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distortions du signal risquent de perturber la transmission. Ainsi pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle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

Le standard 802.11a utilise la bande de fréquence 5.15GHz à 5.35GHz et la bande 5.725 GHz à 5.825 GHz, ce qui permet de définir 8 canaux distincts d'une largeur de 20Mhz chacun, c'est-à-dire une bande suffisamment large pour ne pas avoir de parasitage entre canaux.

e) La technologie infrarouge

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon uni-directionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé.

Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé PPM (pulse position modulation).



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 2 Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles :

1.3) Les techniques de modulation

Tandis que la radio classique utilise une modulation de fréquence (radio FM pour Frequency Modulation) ou bien une modulation d'amplitude (radio AM pour Amplitude Modulation), le standard 802.11b utilise une technique de modulation de phase appelée PSK pour Phase Shift Keying. Ainsi chaque bit produit une rotation de phase. Une rotation de 180° permet de transmettre des débits peu élevés (technique appelé BPSK pour Binary Phase Switch Keying) tandis qu'une série de quatre rotations de 90° (technique appelé QPSK pour Quadrature Phase Switch Keying) permet des débits deux fois plus élevés.

a) Optimisations

La norme 802.11b propose d'autres type d'encodage permettant d'optimiser le débit de la transmission. Les deux séquences Barker ne permettent de définir que deux états (0 ou 1) à l'aide de deux mots de 11 bits (compléments l'un de l'autre).

Une méthode alternative appelée CCK (complementary code keying) permet d'encoder directement plusieurs bits de données en une seule puce (chip) en utilisant 8 séquences de 64 bits. Ainsi en codant simultanéments 4 bits, la méthode CCK permet d'obtenir un débit de 5.5 Mbps et elle permet d'obtenir un débit de 11 Mbps en codant 8 bits de données.

La technologie PBCC (Packet Binary Convolutionnary Code) permet de rendre le signal plus robuste vis-à-vis des distorsions dûes au cheminement multiple des ondes hertziennes. Ainsi la société Texas Instrument a réussi a mettre au point une séquence tirant avantage de cette meilleure résistance aux interférences et offrant un débit de 22Mbit/s. Cette technologie baptisée 802.11b+ est toutefois non conforme à la norme IEEE 802.11b ce qui rend les périphériques la supportant non compatibles avec les équipements 802.11b.

La norme 802.11a opère dans la bande de fréquence des 5 GHz, qui offre 8 canaux distincts, c'est la raison pour laquelle une technique de transmission alternative tirant partie des différents canaux est proposée. L'OFDM (Orthogonal Frequency Division Multiplexing) permet d'obtenir des débits théoriques de 54 Mbps en envoyant les données en parallèle sur les différentes fréquences. De plus la technique OFDM fait une utilisation plus rationnelle du spectre.

Technologie	Codage	Type de modulation	Débit
802.11b	11 bits (Barker sequence)	PSK	1Mbps
802.11b	11 bits (Barker sequence)	QPSK	2Mbps
802.11b	CCK (4 bits)	QPSK	5.5Mbps
802.11b	CCK (8 bits)	QPSK	2Mbps
802.11a	CCK (8 bits)	OFDM	54Mbps
802.11g	CCK (8 bits)	OFDM	54Mbps

1.4) Le WEP

Le WEP est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 ou 128 bits. Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 128 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre le nombre pseudo-aléatoire et la trame.

La clé de session partagé par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.

De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session. De plus une faille décelée par Fluhrer, Mantin et Shamir concernant la génération de la chaîne pseudo-aléatoire rend possible la découverte de la clé de session en stockant 100 Mo à 1 Go de traffic créés intentionnellement.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en oeuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

II. Bibliographie

- **Magazine PC EXPERT - Octobre 2003** – Page 67 – "Mieux gérer sa sécurité" - *Dossier réalisé par Fabrice Neuman, Philippe Roure, Vincent Verhaeghe et Stefan Greiner.*

- **Magazine PCMAX - Juin 2003** – Pages 14 à 23 – "Branchez vous Wi-Fi" *Dossier réalisé par Mourad Krim.*

- **Site Presence-PC.com** - Publié le **24 juin 2003** –"Le guide Wi-Fi" *Dossier réalisé par Pierre-Henry Muller.*

- **Site CommentCaMarche.net** - "Les réseaux sans fils" et "Le Wi-Fi" *Dossier réalisé par Jean-François Pillou.*