Le Wi-Fi

Les réseaux sans fils

Dans la famille des réseaux "Wireless", ceux qui sont construits selon la famille de normes 802.11 connaissent un énorme développement. Leurs champs d'application les plus communs sont :

- en milieu personnel, le déploiement d'un petit réseau, principalement destiné à partager une connexion internet haut débit,
- en entreprise, pour permettre la connexion facile de stations de travail nomades (portables) au réseau ou à une partie du réseau de l'entreprise,
- dans les zones rurales, pour distribuer aux administrés un accès internet obtenu le plus souvent par une solution satellite,
- dans les lieux publics "hi-tech", pour proposer aux clients munis de portables un accès numérique...

Devant la multitude de solutions proposées, il est probablement nécessaire de faire le point sur cette technologie qui dispose certes d'avantages incontestables, mais qui n'est pas exempte d'inconvénients.

Nous allons essayer de faire le point sur le Wi-Fi, sans entrer trop dans les détails du protocole dans les niveaux 1 et 2, (les couches physique et liaison de données, qui sont de l'ordre de la manipulation d'ondes porteuses), ni sur les autres couches d'ailleurs, puisqu'à partir du niveau 3 tout se passe de la même manière que sur un réseau filaire, mais plutôt sur les contraintes de topologie et de sécurité dont il faut absolument tenir compte.

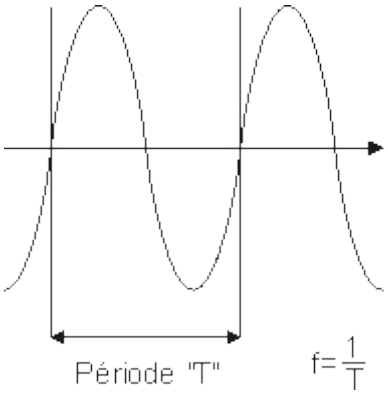
Plan du chapitre

Rappels

Ça va mieux en le disant...

Il n'est probablement pas inutile de commencer par quelques rappels sur les ondes électromagnétiques.

Période, fréquence, longueur d'onde...

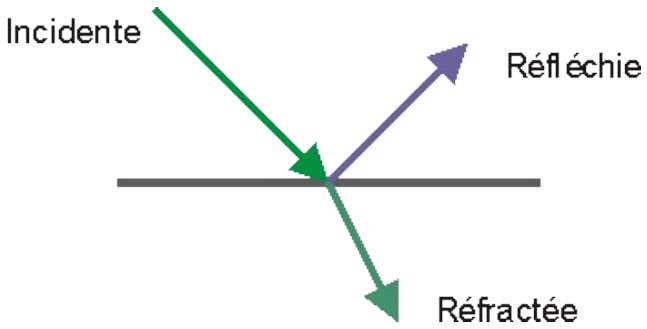


La "longueur d'onde" fait intervenir une dimension spatiale. Les ondes radio (électromagnétiques) se propagent dans le vide (et dans l'air, avec une erreur négligeable) à la vitesse de 300 000 Km/s (3×10^8 m/s). Dans le cas qui nous intéresse, la fréquence est de l'ordre de 2,5 Ghz pour les normes 802.11b et 802.11g, les plus utilisées actuellement, ce qui nous donne une période de 4×10^{-10} s.

La longueur d'onde est la distance parcourue par l'onde pendant une période, elle est donc ici de l'ordre de 12 cm
($3 \times 10^8 \times 4 \times 10^{-10} = 12 \times 10^{-2}$).

On admettra qu'un objet peut constituer un obstacle à la propagation d'une onde lorsque cet obstacle atteint une dimension supérieure ou égale à la longueur de l'onde.

Les ondes et les obstacles



Lorsqu'une onde rencontre un obstacle, sauf si cet obstacle dispose de caractéristiques très particulières, cette onde est en partie réfléchie (renvoyée par l'obstacle dans une autre direction), réfractée (une partie de l'onde traverse l'obstacle) et absorbée (l'obstacle absorbe une partie de l'énergie de l'onde).

Les cas particuliers sont :

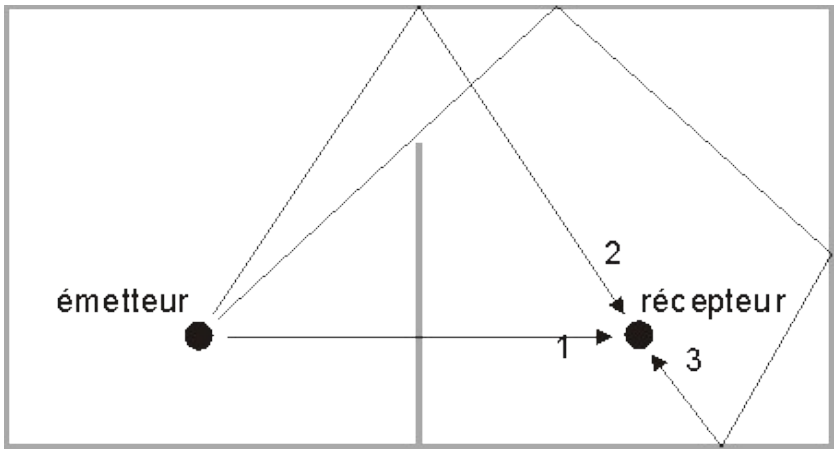
- l'obstacle réfléchissant, qui fait que la quasi totalité de l'onde incidente est réfléchie,
- l'obstacle absorbant, qui fait que la quasi totalité de l'énergie de l'onde est absorbée.

Il est assez facile d'observer ces phénomènes dans le domaine acoustique. Les ondes ne sont plus électromagnétiques, mais subissent tout de même les effets de réfraction, de réflexion et d'absorption. Nous verrons plus loin ce que ça donne dans une enceinte close.

Les "échos"

En atmosphère libre (sans obstacles), il n'y a généralement pas de problèmes encore qu'une atmosphère libre n'est que théorique, sauf éventuellement dans l'espace. En effet, sur terre, nous avons au moins le sol qui constitue un obstacle.

Généralement, le Wi-Fi s'utilise dans des murs et là, il y a plein d'obstacles.



Imaginons un émetteur et un récepteur placés dans des salles contiguës. L'émetteur émet dans toutes les directions, si bien qu'il y aura une multitude d'ondes réfléchies, dont certaines atteindront le récepteur. Dans l'exemple, l'onde 1 atteint directement le récepteur, en traversant la cloison, l'onde 2 l'atteint après une réflexion, l'onde 3 après 3 réflexions...

Clairement, il y en aura beaucoup plus, avec des chemins différents (plus ou moins longs) et avec des atténuations plus ou moins importantes.

Pour une seule source d'émission, le récepteur va recevoir plusieurs fois la même information, plus ou moins atténuée et plus ou moins décalée dans le temps.

En acoustique, le problème est bien connu sous le nom de "réverbération" (beaucoup d'échos, avec des décalages temporels très petits).

De plus, en un point donné, deux ondes peuvent parvenir en opposition de phase. Elles n'auront probablement pas la même amplitude, mais leur somme mathématique aura tendance à donner un résultat nul, ce qui conduira à une perte de la porteuse, en ce point précis.

Le traitement de la réverbération est une chose complexe à étudier, mais empiriquement, l'on sait bien que jusqu'à un certain point, ce n'est guère gênant pour récupérer l'information, voire même, ce peut être bénéfique. En revanche, si le "taux de réverbération" devient trop grand, le signal devient inexploitable (effet "cathédrale").

Pour les ondes électromagnétiques que nous utilisons pour le Wi-Fi, il en va de même. Ceci pour expliquer une faiblesse majeure du système : dans un bâtiment, il est très difficile, voir impossible de prévoir la position optimale du ou des émetteurs en fonction des points d'écoute souhaités. Dans la plupart des cas, il faudra procéder à des tests pour obtenir la couverture désirée.

Et pour que les choses soient tout à fait claires, ayez présent à l'esprit que les réseaux Wi-Fi permettent le passage de données dans les deux sens. Autrement dit, ici, chaque point est à la fois émetteur et récepteur, qu'il s'agisse d'une borne d'accès ou d'un poste du réseau.

Les canaux d'émission

Nous verrons pourquoi plus tard, les normes 802.11xx utilisent des bandes de fréquences divisées

en plusieurs canaux. Chaque canal correspond à une fréquence de porteuse bien définie et chaque canal est éloigné de ses voisins par un écart constant en fréquence.

Par exemple, dans les normes 802.11b et 802.11g, il y a en France 13 canaux possibles, de 2,412 GHz à 2,472 GHz, espacés les uns des autres de 5 MHz.

Chaque canal utilise une certaine bande de fréquence (largeur du canal, due à la modulation de la porteuse). La largeur de chaque canal est de 22 MHz, si bien que les canaux se recouvrent. Nous verrons que ceci aura une grande importance dans la suite.

Canal 802.11b ou g	Fréquence centrale	Plage de fréquence ±11 MHz
1	2.412 GHz	2.401 – 2.423 GHz
2	2.417 GHz	2.406 – 2.428 GHz
3	2.422 GHz	2.411 – 2.433GHz
4	2.427 GHz	2.416 – 2.438 GHz
5	2.432 GHz	2.421 – 2.443 GHz
6	2.437 GHz	2.426 – 2.448 GHz
7	2.442 GHz	2.431 – 2.453 GHz
8	2.447 GHz	2.436 – 2.458 GHz
9	2.452 GHz	2.441 – 2.463 GHz
10	2.457 GHz	2.446 – 2.468 GHz
11	2.462 GHz	2.451 – 2.473 GHz
12	2.467 GHz	2.456 – 2.478 GHz
13	2.472 GHz	2.461 – 2.483 GHz

Et la qualité du matériel ?

Elle a bien entendu son importance. Par exemple, nous savons tous qu'avec deux oreilles, on entend mieux qu'avec une seule. Pas seulement grâce au repérage spatial que l'écoute binaurale permet, mais aussi parce que le cerveau met en oeuvre des techniques de corrélations entre les signaux reçus par chaque oreille, qui permettent d'éliminer, jusqu'à un certain point, les perturbations apportées par la réverbération et le bruit.

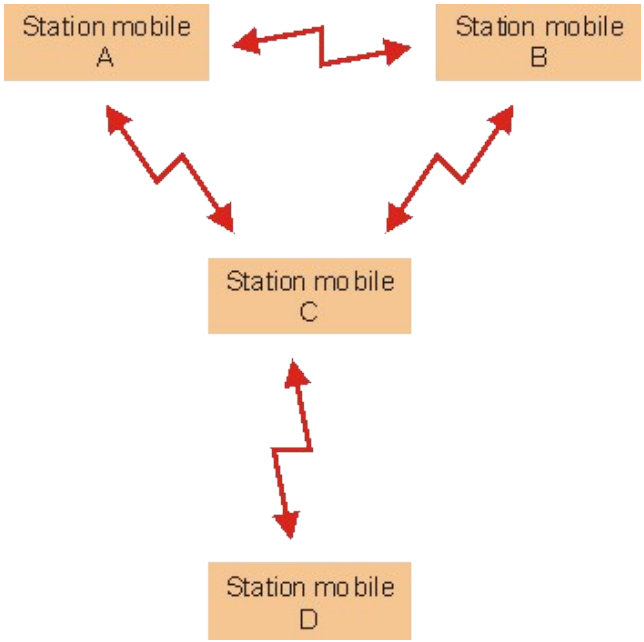
Les systèmes Wi-Fi peuvent être équipés de techniques similaires, qui permettent plus ou moins efficacement de traiter un signal entaché de réverbération.

Nous n'entrerons pas d'avantage dans la définition des normes 802.11xx, de toutes façons, il n'est pas possible d'agir sur le protocole, de même qu'il n'est pas possible d'agir au niveau 1 d'un réseau Ethernet. Ce qu'il est important de comprendre ici, c'est que les problèmes de propagation sont importants et peuvent considérablement influer sur le résultat obtenu.

Architectures : les divers modes de fonctionnement

Il y a fondamentalement deux façons de faire fonctionner un réseau Wi-Fi, suivant ce que l'on souhaite faire.

Le mode "ad hoc"



Il n'y a pas dans le réseau de point émetteur/récepteur ayant un rôle particulier. C'est typiquement le mode que l'on choisira si l'on souhaite juste faire communiquer entre elles deux ou trois machines disposant chacune d'une interface Wi-Fi. C'est un mode de fonctionnement rudimentaire, qui peut rapidement devenir compliqué si le nombre de machines en réseau augmente.

Chaque station ne peut communiquer qu'avec les stations qui sont à portée. Dans l'exemple :

- la station C peut communiquer avec toutes les autres stations,
- les stations A, B et C peuvent communiquer entre elles,
- la station D ne peut communiquer qu'avec la station C.

En aucun cas, la station C ne pourra servir de relais pour que, par exemple, D puisse communiquer avec A.

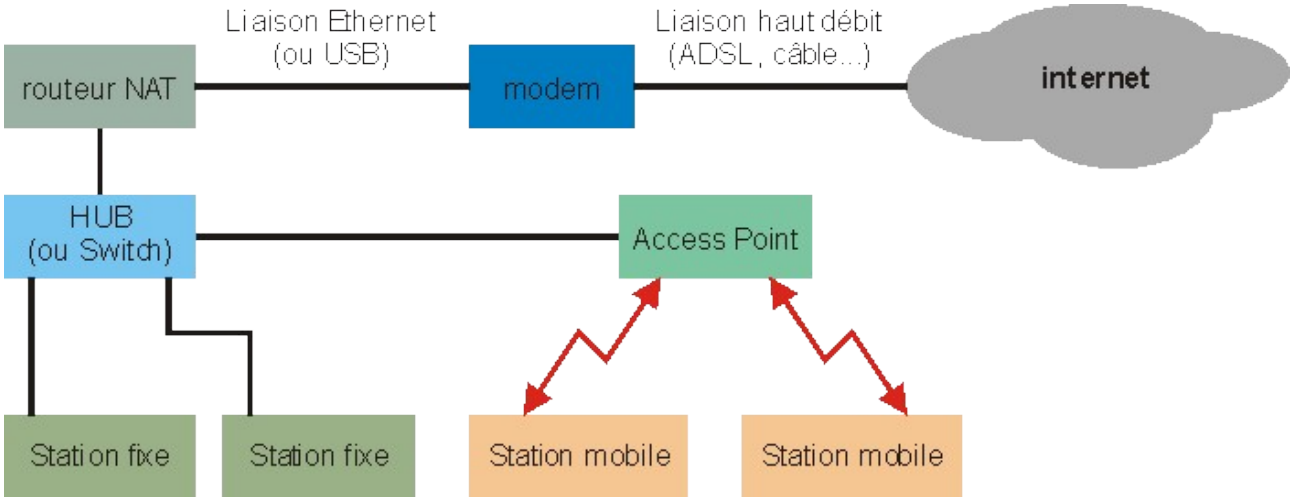
Cet exemple le montre clairement, ce type de réseau n'a d'intérêt que pour permettre à des machines proches (et peu nombreuses) de communiquer entre elles en dehors de toute structure.

Le mode "infrastructure"

Dans ce mode, il y a au moins un émetteur/récepteur Wi-Fi qui joue un rôle particulier, celui de point d'accès (Access Point). C'est typiquement le mode utilisé lorsque l'on souhaite étendre un réseau câblé, genre Ethernet, avec une couverture Wi-Fi pour les portables, ou pour les machines que l'on ne souhaite pas câbler.

Les "modems Wi-Fi", entendez par là les modems ADSL ou câble, qui proposent une connectivité Wi-Fi fonctionnent généralement dans ce mode. C'est ce mode que nous étudierons plus en détail.

En voici une représentation typique :

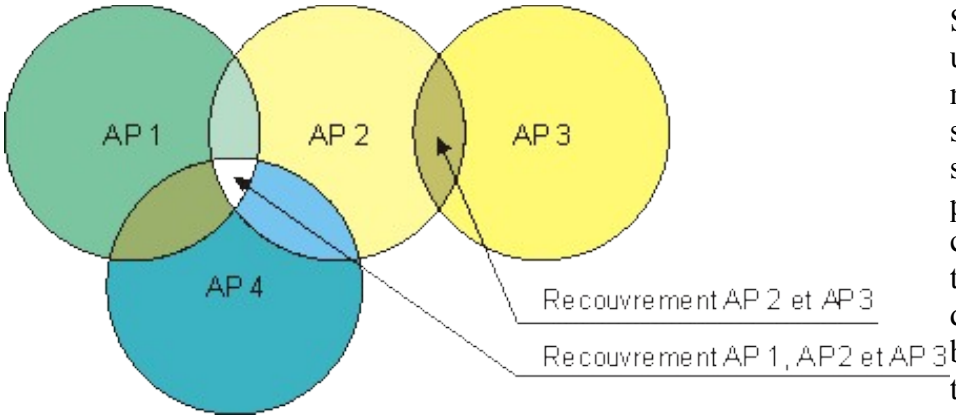


Ici, toutes les fonctions sont distinctes, mais rien n'interdit que les fonctions modem, routeur NAT et Point d'accès soient concentrées dans le même boîtier. Dans un tel cas, les stations fixes et mobiles pourront communiquer entre elles car nous pourrons faire en sorte qu'elles soient sur le même réseau IP (avec tous les risques que ça comporte au niveau de la sécurité).

Le point d'accès agit un peu comme un HUB pour les stations mobiles. Généralement ce point d'accès (que nous appellerons par la suite AP, pour reprendre la terminologie courante) dispose lui-même d'une adresse IP, qui permet de l'administrer à distance par divers moyens (telnet, mini serveur http, application dédiée).

Ici, l'AP sert de relais non seulement entre les stations mobiles, mais aussi entre les stations mobiles et les stations fixes. Pour une station mobile, tout se passe comme si elle était connectée au réseau local par un fil. S'il y a un serveur DHCP sur le LAN, les stations mobiles peuvent même recevoir leur configuration IP de façon automatique.

Vous l'aurez compris, le mode "ad-hoc" n'a d'intérêt qu'occasionnellement, en dehors de toute structure.



Si l'on souhaite obtenir une couverture convenable sur un site donné, il sera probablement nécessaire de placer plusieurs points d'accès. Dans un tel cas, les zones de couverture de plusieurs points d'accès viendront probablement se recouvrir partiellement.

Dans l'exemple donné, AP1, AP2 et AP3 se recouvrent partiellement. AP2 et AP3 également. Si l'on veut éviter des interférences dans ces zones de recouvrement, il faudra prendre quelques précautions. Bien entendu, AP1 AP2 et AP3 ne devront pas utiliser le même canal. Mais rappelez vous aussi que les canaux se recouvrent partiellement. Non seulement il faudra utiliser des canaux différents, mais en plus, il faudra que ces canaux ne se recouvrent pas. Ça laisse finalement très peu de choix, reportez-vous au tableau vu plus haut, et vous constaterez qu'il n'est matériellement pas

possible de placer quatre points d'accès se recouvrant partiellement, avec les canaux autorisés en France.

En revanche, AP3, qui ne recouvre que AP2, pourra utiliser le même canal qu'AP1 ou AP4.

Mais d'abord, savoir où l'on va...

Les risques sanitaires

Nous allons mettre en oeuvre un réseau sans fils, qui va utiliser des ondes radio. Les ondes radio, nous l'avons vu, sont capricieuses et peuvent :

- ne pas passer là ou l'on voudrait qu'elles passent, ce qui peut conduire à multiplier les AP et, accessoirement, la facture (financière) de l'installation,
- passer là où l'on ne voudrait pas qu'elles passent, et c'est sans doute ce cas le plus dangereux.

En effet, pour fixer les esprits, vous êtes chez vous et vous montez votre réseau Wi-Fi, qui va permettre à toutes vos machines de communiquer entre elles et d'accéder à l'Internet par le truchement de votre ADSL2+ super rapide et tout, sans avoir à tirer le moindre câble, ô combien inesthétique.

Oui, mais qu'est-ce qui va empêcher :

- votre (vos) voisin(s) de profiter non seulement de votre accès internet super très haut débit, mais aussi des ressources que vous partagez sur votre réseau local ?
- les "geeks" qui, dans leur voiture, passent leur temps à repérer les AP à portée de rue pour en extraire le maximum ?

Nous verrons qu'il y a des moyens de se protéger, et aussi, hélas, des moyens de passer outre ces protections...

Cependant, il faut bien l'admettre, lorsque l'on utilise un portable, le Wi-Fi, c'est bien pratique.

Le vocabulaire

Pour bien faire du Wi-Fi, il faut déjà maîtriser le vocabulaire qui va avec. Ne vous y trompez pas, monter un réseau Wi-Fi, à moins que vous n'ayez une chance pas possible, ne se fera pas sans mal. La loi de Murphy[1] et ses innombrables corollaires feront que vous devrez vous battre implacablement avec ce système.

Les documentations, souvent en anglais, usent et abusent de surcroît d'une panoplie d'acronymes incompréhensibles par le non initié. Un petit exemple ?

Wireless	Commençons par quelque chose de simple, c'est juste un mot anglais qui signifie : sans fils.
WLAN	Comme Wireless LAN : réseau local sans fils.

1 Loi de Murphy : http://www.courtois.cc/murphy/murphy.html

Wi-Fi	Le nom **Wi-Fi** (contraction de *Wireless Fidelity*, parfois notée à tort *Wi-Fi*) correspond initialement au nom donnée à la certification délivrée par la Wi-Fi Alliance[2], 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 Wi-Fi est en réalité un réseau répondant à la norme 802.11. *(Définition tirée de l'excellent site CCM[3])*
Hot Spot	Zone publique couverte par un réseau sans fils (gares ferroviaires, aéroports, hôtels...).
WA	Comme Wireless Adapter. Comprenez : interface réseau sans fils.
AP	On l'a déjà vu : Access Point. Point d'accès en mode "infrastructure".
BSS	Comme "Basic Service Set". Ensemble de services de base. Ensemble formé d'un point d'accès et des stations qui y sont connectées. Aussi appelé "Cellule".
BSSID	Identifiant d'un BSS. Absolument fondamental, comme nous le verrons plus loin, c'est en réalité l'adresse MAC du point d'accès.
ESS	Comme nous l'avons vu, dans un réseau de type "infrastructure", il se fera souvent qu'un seul AP ne suffise pas à assurer la couverture souhaitée. Dans ce cas, il faudra ajouter d'autres points d'accès, en prenant soin qu'ils puissent travailler en bonne intelligence. Si l'on y arrive, on aura alors créé un ESS : Extended Service Set, qui n'est finalement qu'un ensemble homogène de BSS. Cet ensemble, par extension, si je puis dire, peut se rapporter à un seul point d'accès,
ESSID	Identifiant de l'ESS. Il s'agit d'un nom que l'administrateur va donner au(x) point(s) d'accès qui constitue(nt) l'ESS. Dans le cas particulier où l'ESS est constitué d'un seul BSS, on pourra aussi parler de SSID (voyez comme ça devient vite amusant, de parler le Wi-Fi).
DS	Distribution System. Système de distribution qui est là pour connecter entre eux plusieurs AP afin qu'ils puissent constituer un ESS.
IBSS	Independant BSS. Même chose qu'un BSS, mais sans AP. Autrement dit, c'est un ensemble de stations connectées en mode "ad-hoc". Un IBSS doit disposer d'un SSID unique.

2 Wi-Fi Alliance : http://www.wi-fi.org/
3 CCM : http://www.commentcamarche.net/

WEP	Wired Equivalent Privacy. Système de chiffrement du réseau (au niveau liaison, c'est-à-dire au niveau 2) dont l'ambitieux objectif est de rendre un réseau sans fils aussi sûr qu'un réseau filaire. Vu du côté utilisateur, WEP se résume à une clé de chiffrement qu'il faudra partager entre les partenaires d'un même ESS.
WPA	Wi-Fi Protected Access. Comme WEP n'a pas vraiment convaincu tout le monde, la "Wi-Fi Alliance" (pas besoin de traduire, je pense), a décidé de normaliser un nouveau système de sécurité. Je ne résiste pas au plaisir de citer un fragment d'article paru sur journaldunet.com : *Absente du WEP, l'authentification fait son apparition au sein de WPA. Le protocole prévoit deux modes d'authentification : un mode "entreprise" - qui implique d'installer un serveur central (de type Radius par exemple) pour identifier toute personne souhaitant se connecter - et un mode "personnel". WPA s'appuie sur la famille 802.1x et le protocole EAP (Extensible Authentification Protocol), extension du protocole PPP (Point-to-Point Protocol), qui peut supporter de nombreux mécanismes d'authentification tels que des cartes à jeton, des mots de passe à usage unique et l'authentification par clé publique utilisant des cartes à puce.* Vous le voyez, c'est très facile et à la portée du non initié. Mais nous aurons l'occasion d'en reparler.
MIMO	Multiple-Input Multiple-Output, encore appelé "multipath". C'est une technologie très complexe, utilisant plusieurs antennes pour diffuser les ondes radio. Pratiquement, l'objectif est d'améliorer les performances en corrigeant autant que possible les problèmes d'interférences. Le résultat annoncé est une minimisation des points d'ombre et une augmentation de la portée. Existe pour 802.11b et 802.11g et devrait être normalisé dans 802.11n. Je n'ai pas pu tester cette technologie, mais en fonction de ce qui en est dit ça et là, il semblerait vivement déconseillé de l'utiliser tant qu'elle ne sera pas normalisée.

Ce petit lexique devrait nous permettre, du moins dans un premier temps, d'aller un peu plus loin dans la découverte d'un réseau Wi-Fi.

Le matériel

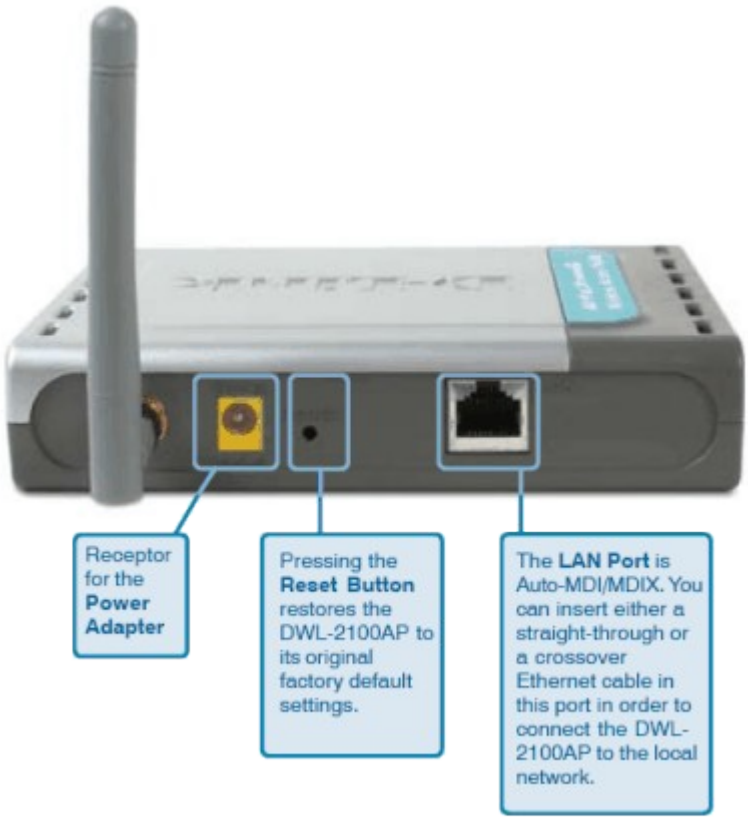
Pour poursuivre cet exposé, nous allons nous appuyer sur un minimum de matériel. En principe, le choix du matériel n'a pas une importance capitale pour la mise en oeuvre des concepts, encore que chaque constructeur peut ajouter ses petits "+" à la norme. Méfiez-vous de ces petits "+" qui, s'ils sont utilisés, risquent de provoquer des incompatibilités entre matériels de marques différentes.

Le réseau filaire

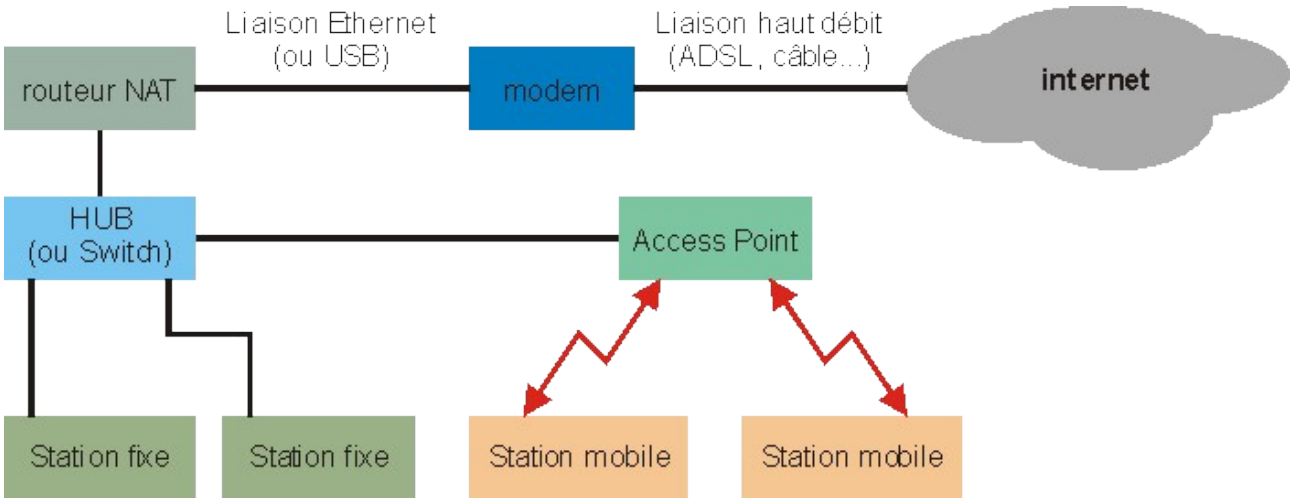
Nous disposons d'un réseau filaire Ethernet, nous utilisons bien entendu TCP/IP, le réseau utilise la plage IP 172.16.0.0/16.

Une passerelle vers l'Internet est présente (machine Linux avec IPtables), il y a sur ce réseau un serveur DHCP qui permet de configurer automatiquement les hôtes du réseau. Tout ceci fonctionne parfaitement, et nous voulons maintenant étendre ce réseau avec un accès Wi-Fi pour que les stations portables puissent accéder simplement à ce réseau.

Nous allons donc ajouter un AP (Point d'accès) qui ne sera la borne DWL-2100AP. Soyons bien clair tout de suite, il n'est absolument pas question de faire de la publicité pour cette marque, ni pour ce modèle (ni de la contre-publicité, d'ailleurs). C'est le matériel dont je dispose, voilà tout.



Il s'agit d'un "simple" point d'accès, au sens où il n'y a ni modem ni routeur intégré dans ce boîtier. Il est typiquement conçu pour être connecté à un réseau filaire existant



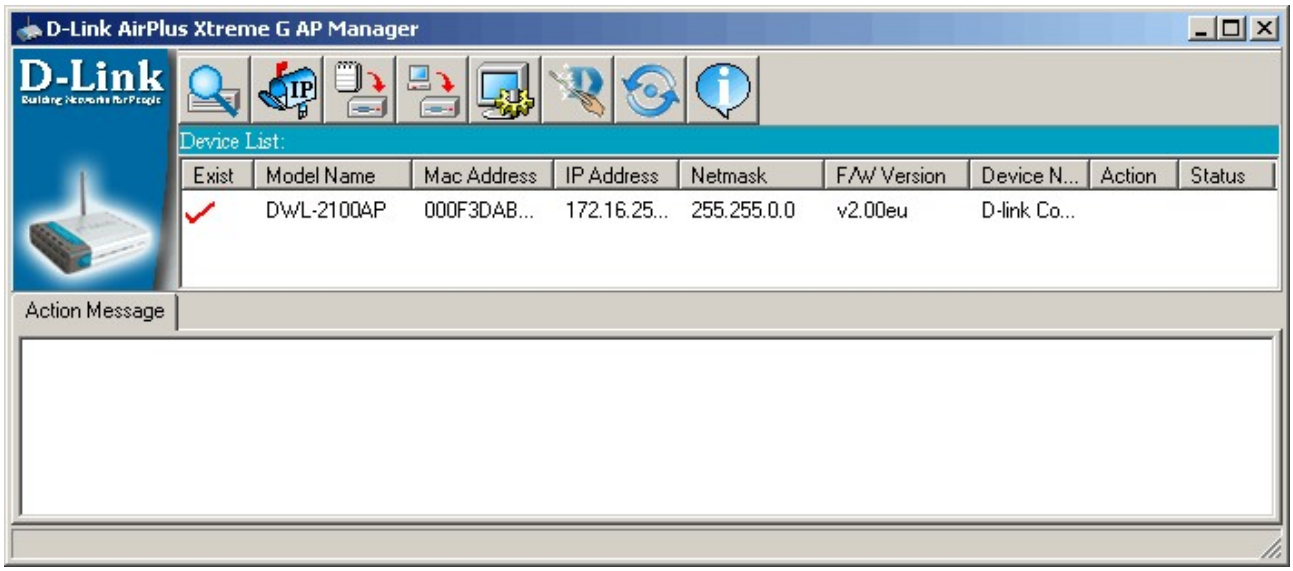
La face arrière nous montre l'extrême simplicité de ce genre d'équipement. De gauche à droite :

- l'antenne,
- la prise d'alimentation,
- le bouton "reset",
- la prise réseau RJ 45.

Il suffit presque de brancher pour que ça marche. Presque, parce que, comme nous allons le voir, cet AP dispose d'une adresse IP par défaut égale à 192.168.0.50.

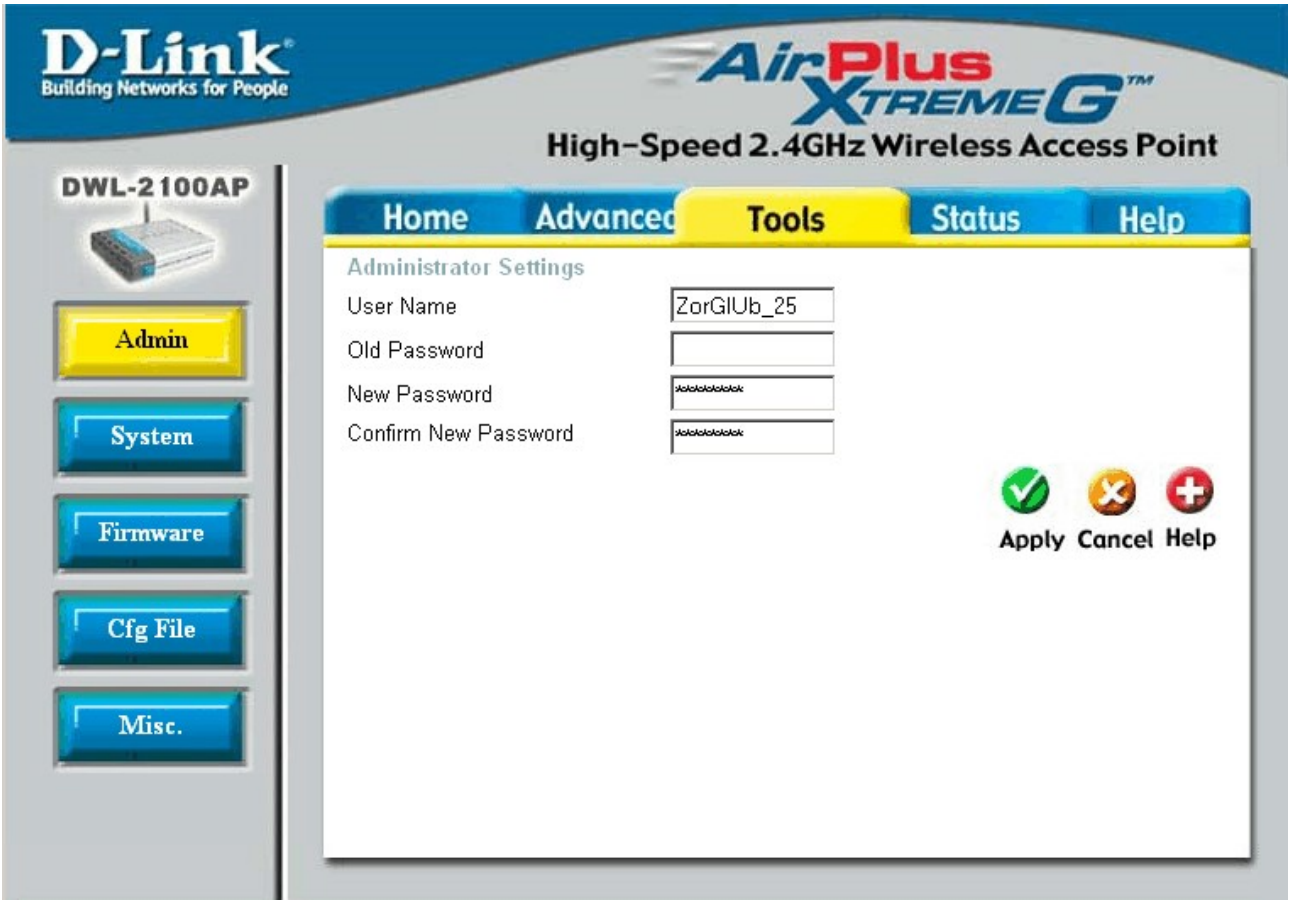
C'est bien, mais ça ne va pas avec le plan d'adressage que nous avons dans l'exemple. Ici, le seul fait de brancher ne constitue que la première étape, mais pour l'instant, la borne demeure inutilisable.

La borne est fournie avec un utilitaire qui doit être capable de résoudre ce problème :



Une fois le problème de l'adresse IP résolu, nous pourrons nous passer de cet utilitaire, le point d'accès embarquant un mini serveur web qui nous permettra de le configurer. Est-ce un avantage ? Ce n'est pas si sûr. Par le fait, toute station connectée au réseau pourra accéder à ce serveur web.

Bien entendu, il y a tout de même une identification nécessaire. Par défaut, l'utilisateur s'appelle "admin" et le mot de passe est vide. La première chose à faire est donc de modifier tout ça :



Utilisez, si votre matériel le permet, un nom d'administrateur qui sorte un peu de l'ordinaire et surtout, mettez un mot de passe **solide** et même, pourquoi pas un nom d'utilisateur non trivial (on peut faire largement moins trivial que dans l'exemple), lettres majuscules et minuscules, chiffres, symboles et malgré tout, pensez que vous êtes en http et que le login sera facilement récupérable avec un sniffeur sur le réseau.

Vous me direz alors, "peut-être qu'il serait plus sûr d'exploiter l'utilitaire vu plus haut ?"

AP Manager utilise le protocole tftp il n'y a pas de nom d'utilisateur et le mot de passe circule là aussi en clair.

La troisième solution, ce serait telnet, mais là encore, les informations sur le login passent en clair...

Vous le voyez, côté réseau local, c'est déjà pas terrible du côté de la sécurité. Lorsque vous êtes sur votre réseau domestique, ça peut encore passer, mais sur un réseau d'entreprise, c'est beaucoup plus délicat.

Du côté des clients, j'ai utilisé quatre cartes Wi-Fi différentes :

- une D-Link DWL-G650 802.11g (PCMCIA), la seule des quatre à supporter le système WPA
- une D-Link DWL-650 802.11b, la seule que j'ai pu faire fonctionner correctement sous Linux avec les drivers Hostap
- une BeWAN PCMCIA 802.11b
- une Marvell 802.11g intégrée à la carte mère Asus P5GD2

Config simple

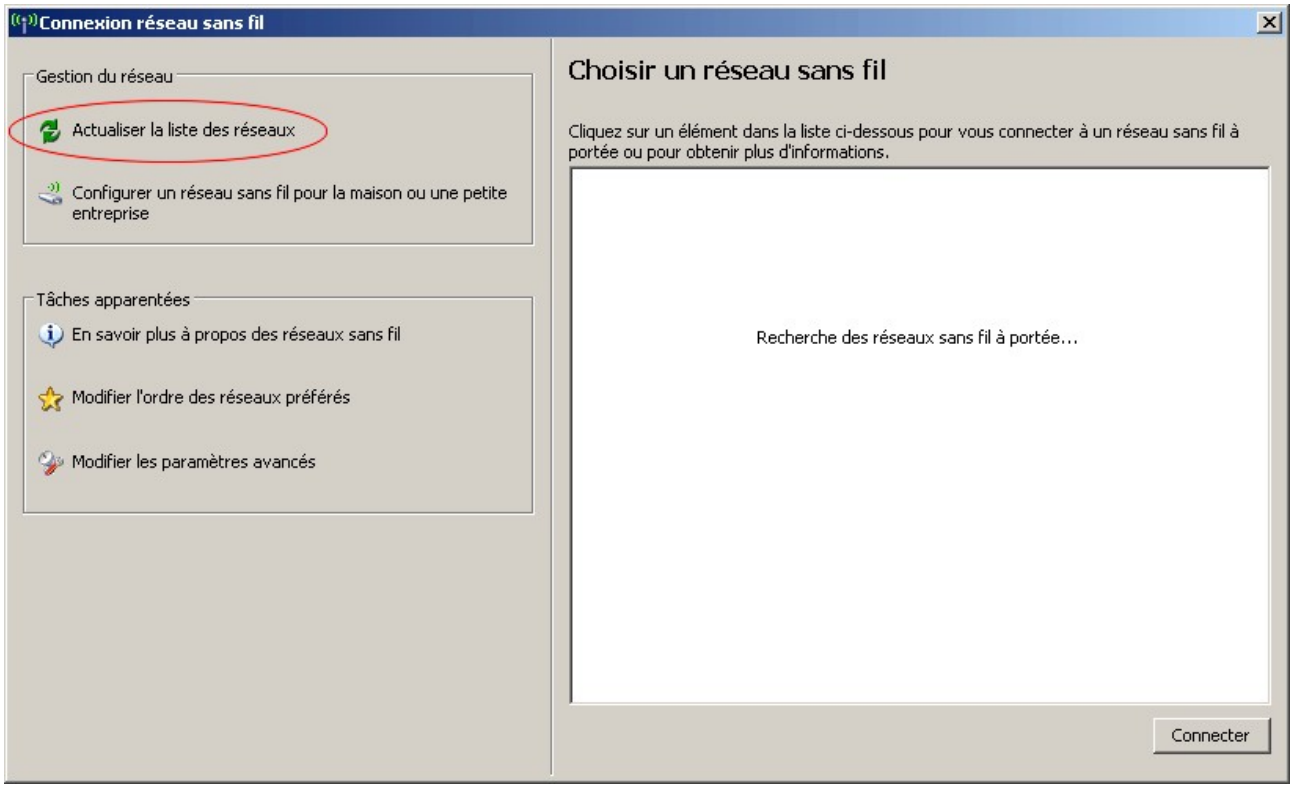
Soyons ingénus

Dans le but de mettre en place une solution qui fonctionne, nous n'allons pas nous poser trop de questions, du moins au début.

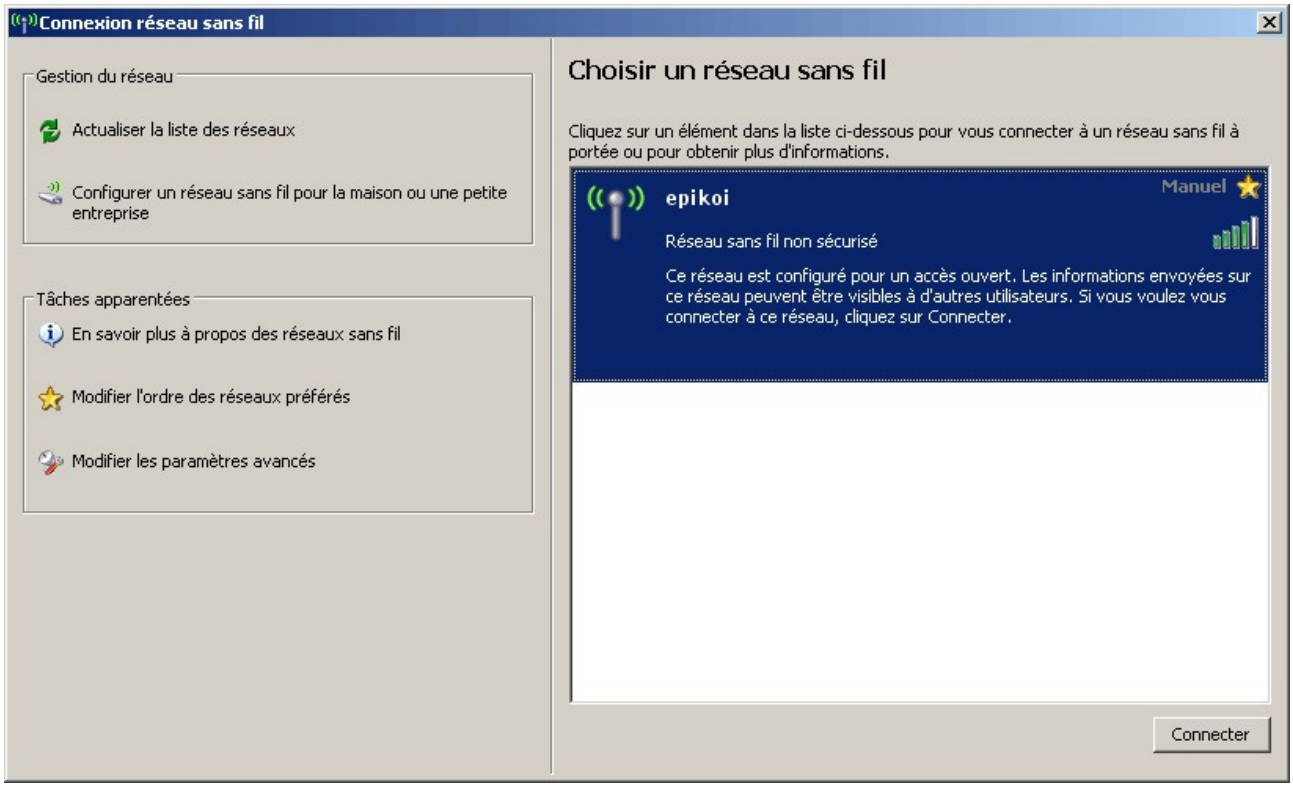
Nous supposons que notre point d'accès est correctement configuré côté réseau local, avec une adresse IP accessible pour l'administration. Il suffit alors de configurer la borne en point d'accès, de lui attribuer un SSID, éventuellement un canal. Si nous avons un serveur DHCP sur le réseau local, il ne sera pas nécessaire de configurer celui qui est présent sur la borne. Sinon, ce sera plus simple pour les clients d'utiliser le serveur DHCP de la borne, qu'il faudra alors configurer.

En l'absence de précautions particulières, ça devrait fonctionner tout seul.

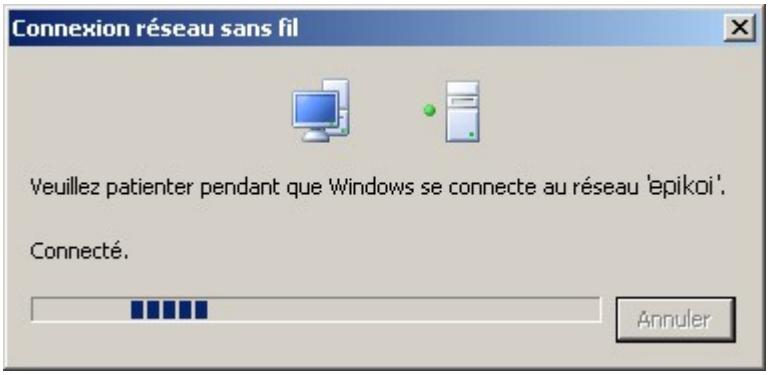
Vous prenez un portable équipé Wi-Fi, vous faites une recherche des réseaux Wi-Fi disponibles :



Normalement, s'il est à portée de votre borne, il doit le trouver facilement et vous indiquer le SSID du réseau :



Il vous reste à vous y connecter :



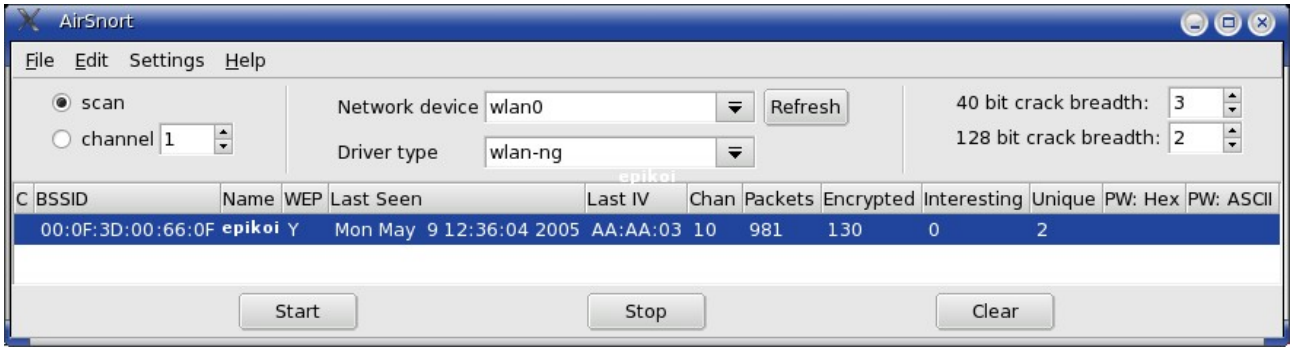
Et ça devrait fonctionner.

Oui mais...

Simple, n'est-ce pas ? Seulement voilà. N'importe qui peut faire ça. Pensez qu'un réseau Wi-Fi passe là où il veut (et pas forcément où vous voulez).

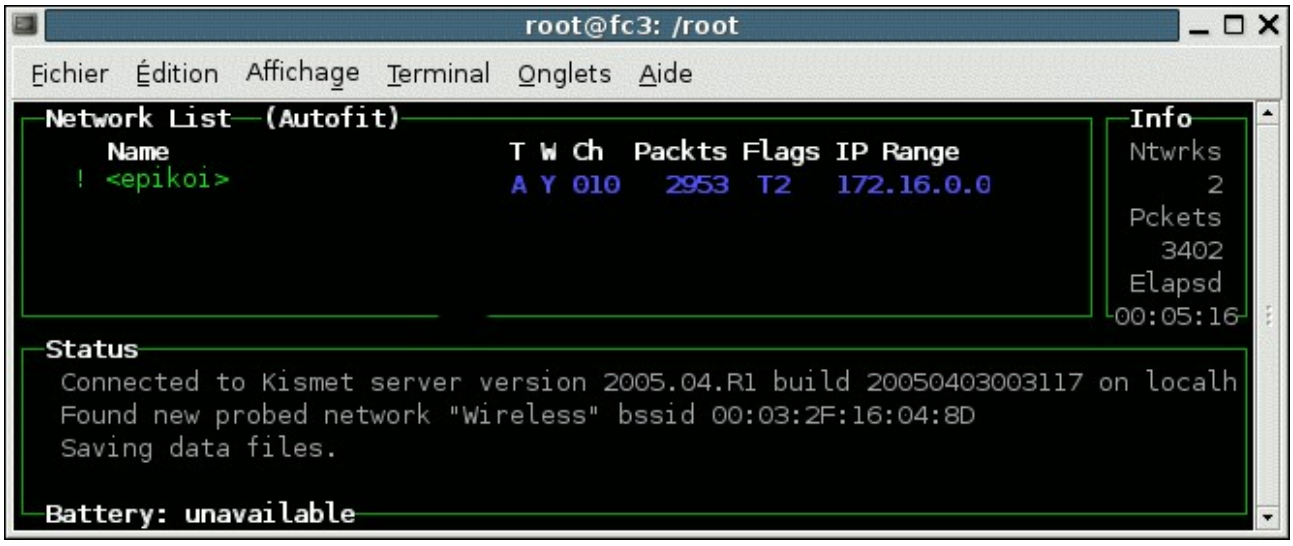
Voici un petit utilitaire graphique, sous Linux, qui fait en gros la même chose :

Et, dans la foulée, un autre utilitaire plus puissant, que nous retrouverons d'ailleurs un peu plus loin :

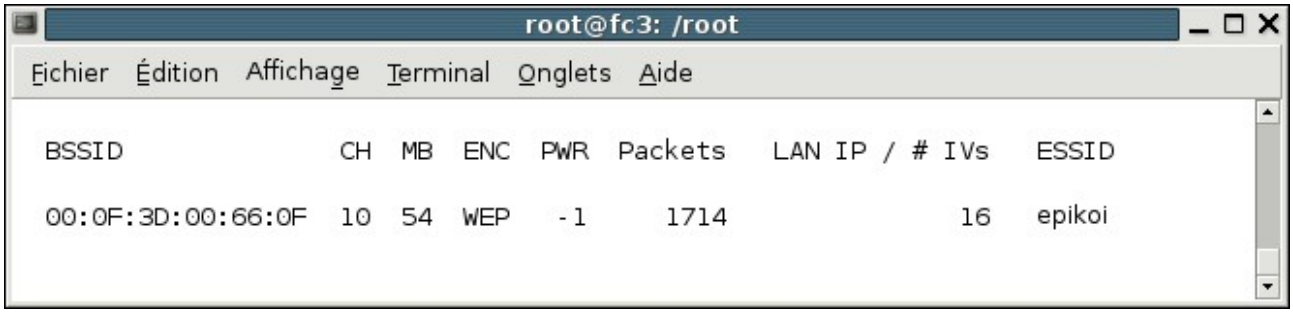


Vous en voulez d'autres ?

Kismet :



Airodump :



Ce dernier est probablement le plus intéressant de tous. Nous anticipons un peu sur la suite, la capture d'écran est faite avec une protection WEP mise en place, que nous verrons plus loin.

Dans un cas comme dans l'autre, vous voyez que l'indiscret dispose de tous les éléments nécessaires pour se connecter à votre réseau Wi-Fi.

Et alors ?

Alors, répétons-le, n'importe qui, à portée de votre borne, peut se connecter à votre réseau Wi-Fi et peut par exemple :

- consommer votre bande passante,
- s'intégrer à votre réseau local et profiter de vos ressources partagées,
- prendre possession de vos machines pour y installer toutes sortes de choses qui pourront lui servir, par la suite, depuis l'Internet,
- utiliser votre connexion internet pour se livrer, sous votre identité, à toutes sortes d'activités répréhensibles.

Cette liste est bien entendu nullement exhaustive.

Donc...

Il n'est clairement pas pensable de rester dans cet état. Il vous faudra verrouiller quelque peu votre installation pour essayer de limiter les risques d'intrusion.

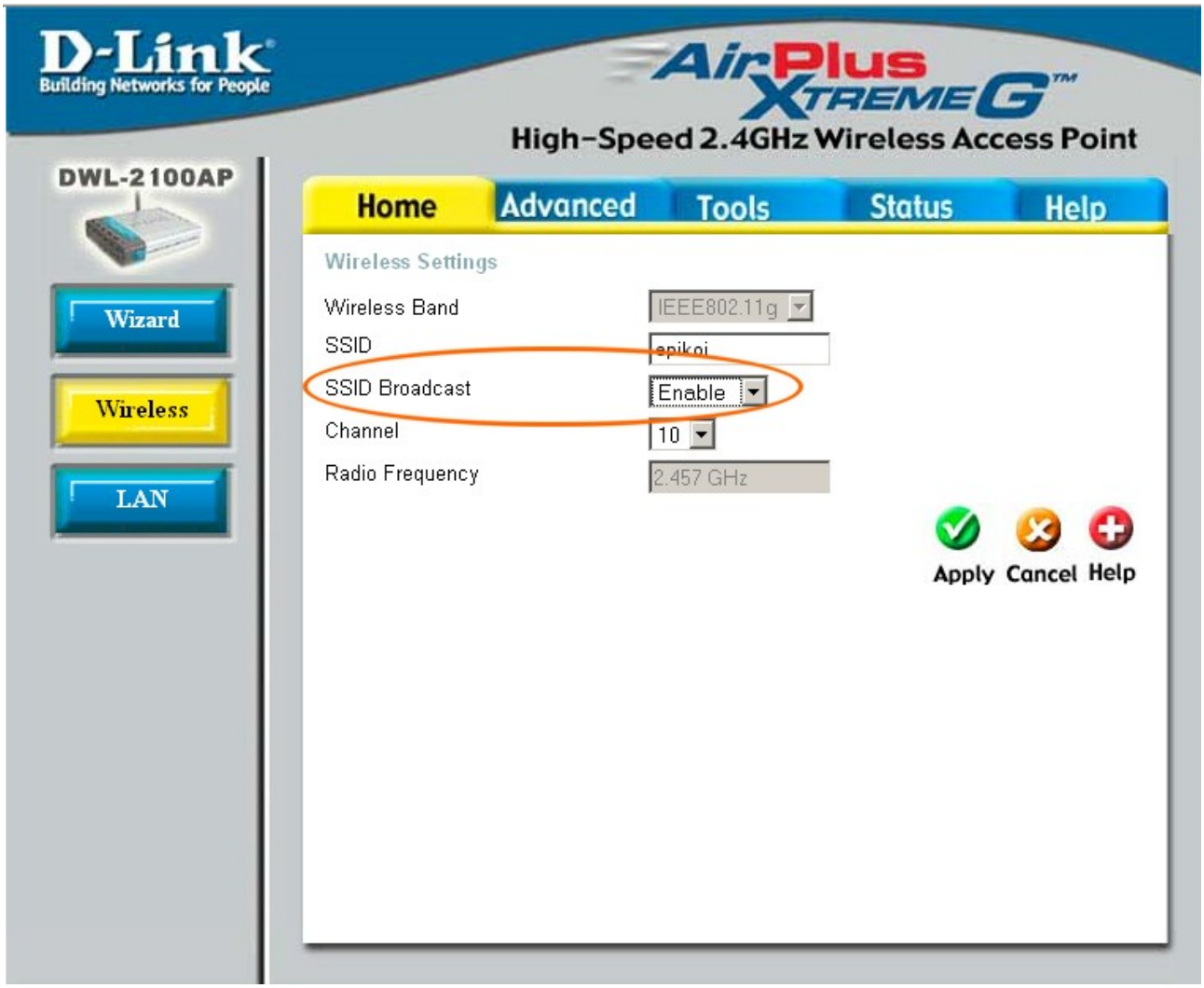
Config avancée

Rendre le SSID "invisible"

Par défaut, un point d'accès Wi-Fi publie son SSID (en Broadcast). C'est nécessaire pour la découverte de réseaux Wi-Fi accessibles. Mais est-ce vraiment nécessaire, justement ?

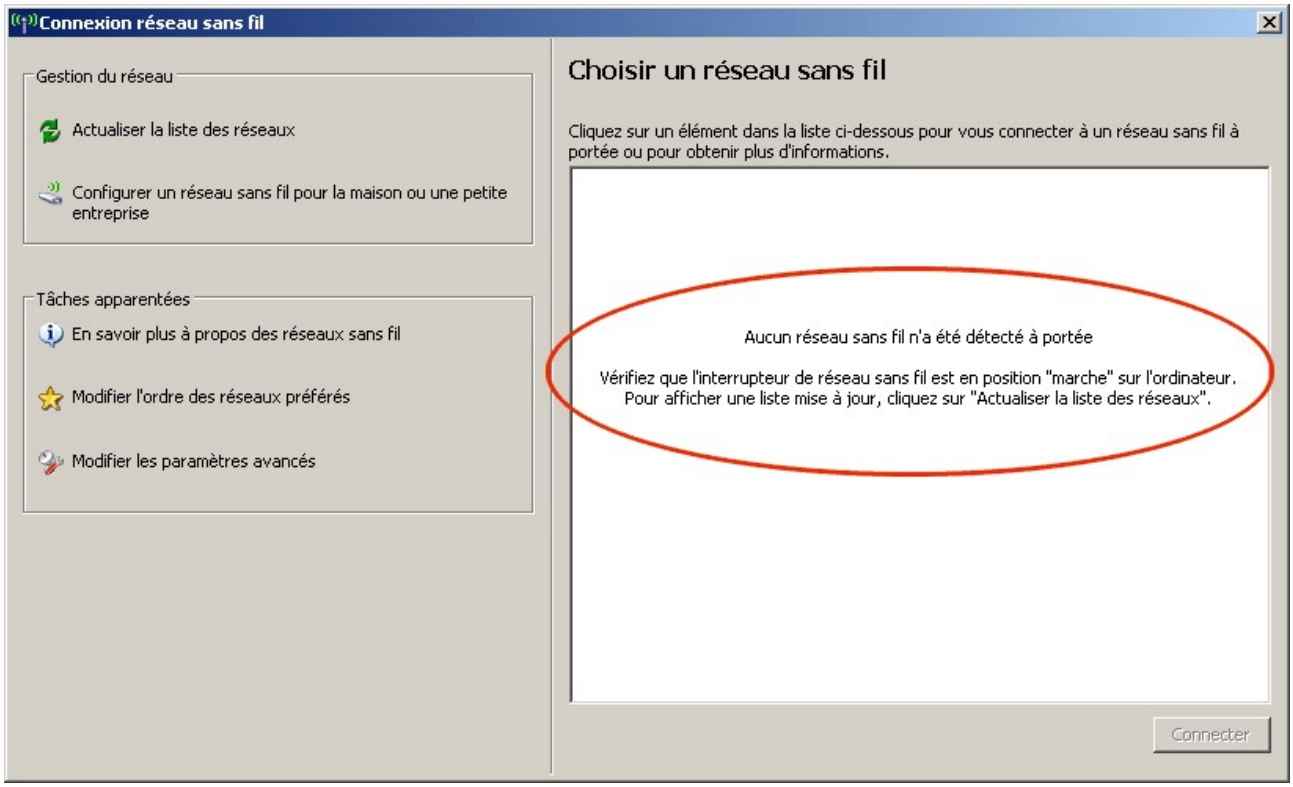
Sur un "hot spot" public (il faudrait dire : zone ASFI), c'est probablement nécessaire, puisque l'accès est volontairement public. Sur votre installation personnelle, c'est complètement inutile, il suffit en effet de l'indiquer à vos utilisateurs.

Tous les points d'accès ne savent pas forcément inhiber cette fonction de publication. C'est cependant le cas sur la borne que nous utilisons pour cet exposé :



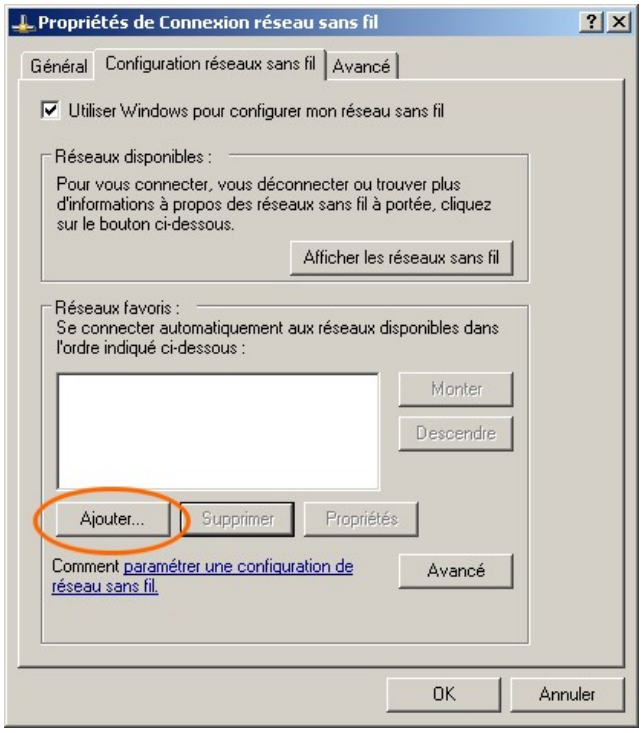
Il suffit de passer ce paramètre à "Disable" (Vous disiez "parlons français" ?)

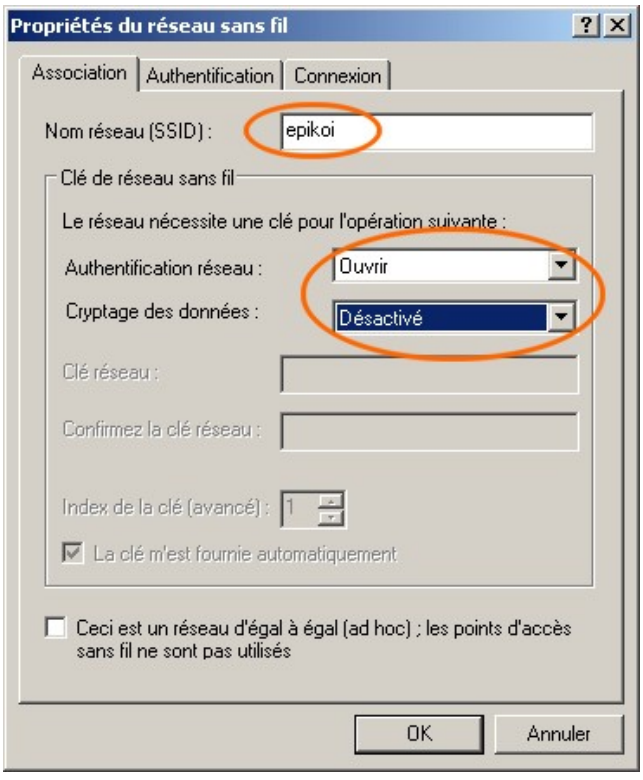
Seulement voilà. Si maintenant, nous essayons d'actualiser la liste des réseaux sans fils, il se produit ceci :



Et là, comment faire ? L'un des moyens les plus simples, consiste :

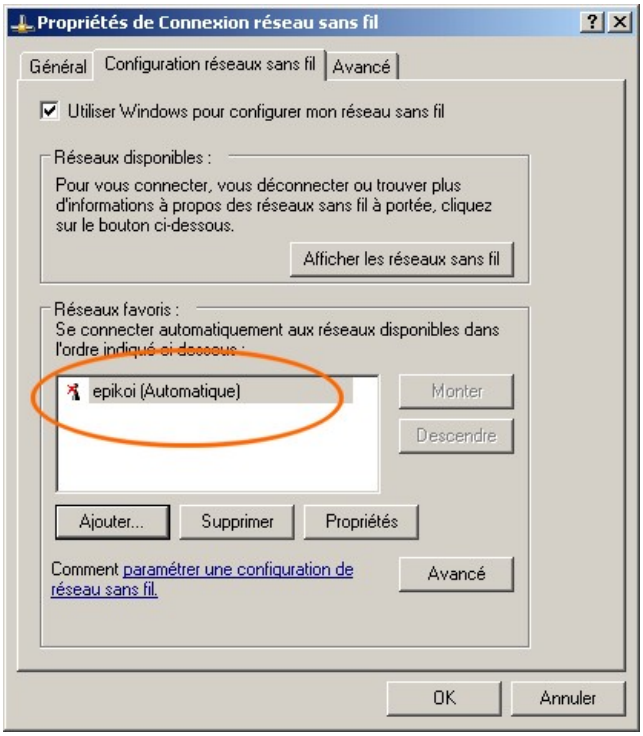
À cliquer sur "Modifier l'ordre des réseaux préfé- Puis de faire " ajouter" :
rés" :





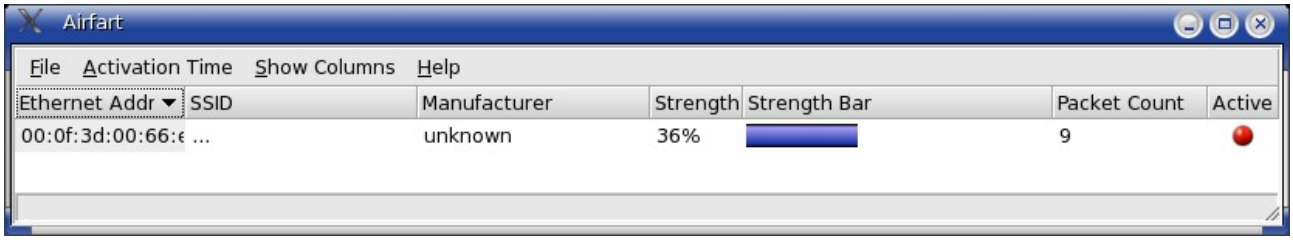
Vous indiquez alors le nom du réseau (SSID), pour l'instant, nous n'avons ni authentification du réseau, ni chiffrement des données.

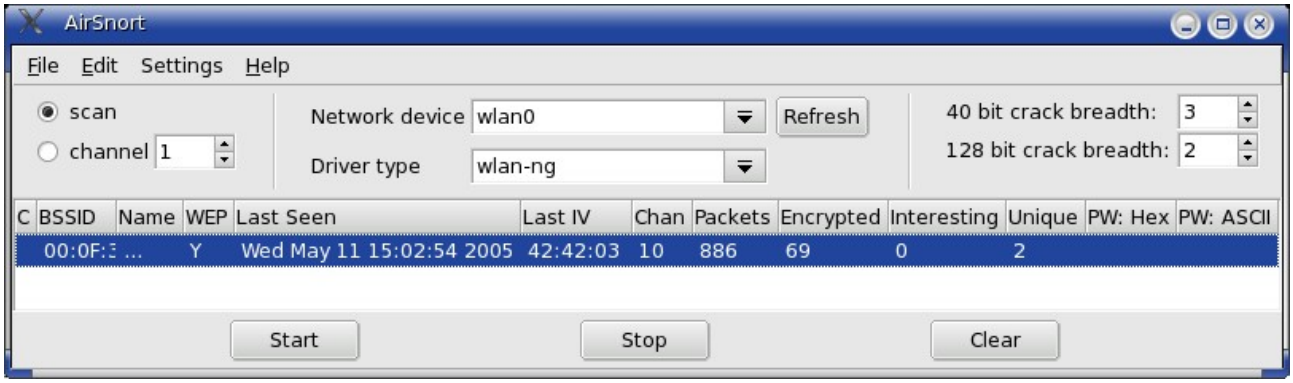
Faites "OK", et vos réseaux favoris seront alors à jour.



Vous devriez maintenant pouvoir vous connecter au réseau sans fils.

Voyons ce que disent Airfart et Airsnort :





Chouette ! le SSID n'apparaît plus. S'il n'apparaît plus, le pirate ne pourra plus se connecter sur le réseau Wi-Fi.

C'est avec ce genre de raisonnement que l'on se retrouve vite à poil (sauf le respect que je vous dois).

Airsnort ou Airodump, savent enregistrer leurs logs au format "pcap" (même format qu'Ethereal, que vous devez commencer à connaître). Nous n'allons pas déballer tout un log, mais juste une ou

deux trames capturées, lorsqu'un client "officiel" se connecte au réseau Wi-Fi :

```
Frame 158 (49 bytes on wire, 49 bytes captured)
...
IEEE 802.11 wireless LAN management frame
...
    Tagged parameters (25 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 3
        Tag interpretation: epikoi
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) [Mbit/sec]
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6,0 9,0 12,0 18,0 24,0 36,0 48,0 54,0 [Mbit/sec]
        Tag Number: 255 (Reserved tag number)
        Tag length: 255
[Malformed Packet: IEEE 802.11]

No.     Time        Source              Destination     Protocol Info
    160 14.124925   D-Link_ab:66:e8     172.16.0.2      IEEE 802.11 Probe Response[Malformed Packet]

Frame 160 (75 bytes on wire, 75 bytes captured)
...
IEEE 802.11 wireless LAN management frame
...
    Tagged parameters (39 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 3
        Tag interpretation: epikoi
        Tag Number: 1 (Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 6,0 12,0 24,0 36,0
[Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 10
        Tag Number: 7 (Country Information)
        Tag length: 6
        Tag interpretation: Country Code: GB, Any Environment, Start Channel: 1, Channels: 13, Max
TX Power: 20 dBm
        Tag Number: 42 (ERP Information)
        Tag length: 1
        Tag interpretation: ERP info: 0x4 (no Non-ERP STAs, do not use protection, short or long
preambles)
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 9,0 18,0 48,0 54,0 [Mbit/sec]
        Tag Number: 255 (Reserved tag number)
        Tag length: 255
...
```

Peu importent les autres paramètres (que j'ai laissé parce qu'ils ne sont pas totalement inintéressants), ce qui compte ici, c'est que l'on peut malgré tout parfaitement capturer le SSID du réseau Wi-Fi.

D'ailleurs, en laissant tourner Airsnort ou Airodump, sitôt qu'un client viendra se connecter au réseau Wi-Fi, le SSID apparaîtra.

Cette précaution n'arrêtera donc que les parfaits profanes qui ne savent pas aller au delà de la découverte d'un SSID dans les trames de broadcast. C'est donc une protection finalement assez illusoire.

N'autoriser que les adresses MAC connues

La plupart des points d'accès permet de n'autoriser la connexion Wi-Fi qu'à une liste d'adresses MAC connues. Une adresse MAC, c'est dépendant du hardware de l'interface. Vous connaissez vos interfaces et vous n'autorisez qu'elles. L'indiscret, qui arrivera avec son portable à portée de votre réseau, même s'il arrive à découvrir votre SSID, ne sera pas accepté parce que son adresse MAC ne figurera pas dans la liste des adresses connues.

Soit, mais :

- cette liste est difficilement gérable lorsqu'elle devient un peu longue,
- la plupart des linuxiens le sait bien, une adresse MAC, ça peut se changer.

Notre pirate sniffe votre réseau. Bien entendu, lorsqu'un client "connu" se connecte, il devient alors très facile de lire son adresse MAC :

```
Frame 158 (49 bytes on wire, 49 bytes captured)
    Arrival Time: May 11, 2005 16:00:27.146581000
...
IEEE 802.11
    Type/Subtype: Probe Request (4)
    Frame Control: 0x0040 (Normal)
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:11:2f:41:cd:a1 (172.16.0.2)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
...
```

Une fois que l'on dispose d'une adresse MAC valide et du SSID, je vous laisse chercher sur les sites spécialisés, quelles sont les multiples façons de s'introduire quand même sur votre réseau "protégé".

Pour l'instant, nous n'avons pas réussi à mettre en place des protections bien efficaces. De plus, les connexions n'étant pas chiffrées, même sans se connecter à votre réseau, des "sniffeurs" Wi-Fi permettront aisément de voir vos mots de passe qui circulent en clair (POP, IMAP, FTP...), et même, suivant le cas, des données que vous aimeriez bien pouvoir garder pour vous.

Une pincée de chiffrement : le WEP

Nous allons avoir recours aux bonnes vieilles techniques de chiffrement des données, pour essayer de sécuriser un peu plus notre réseau sans fils.

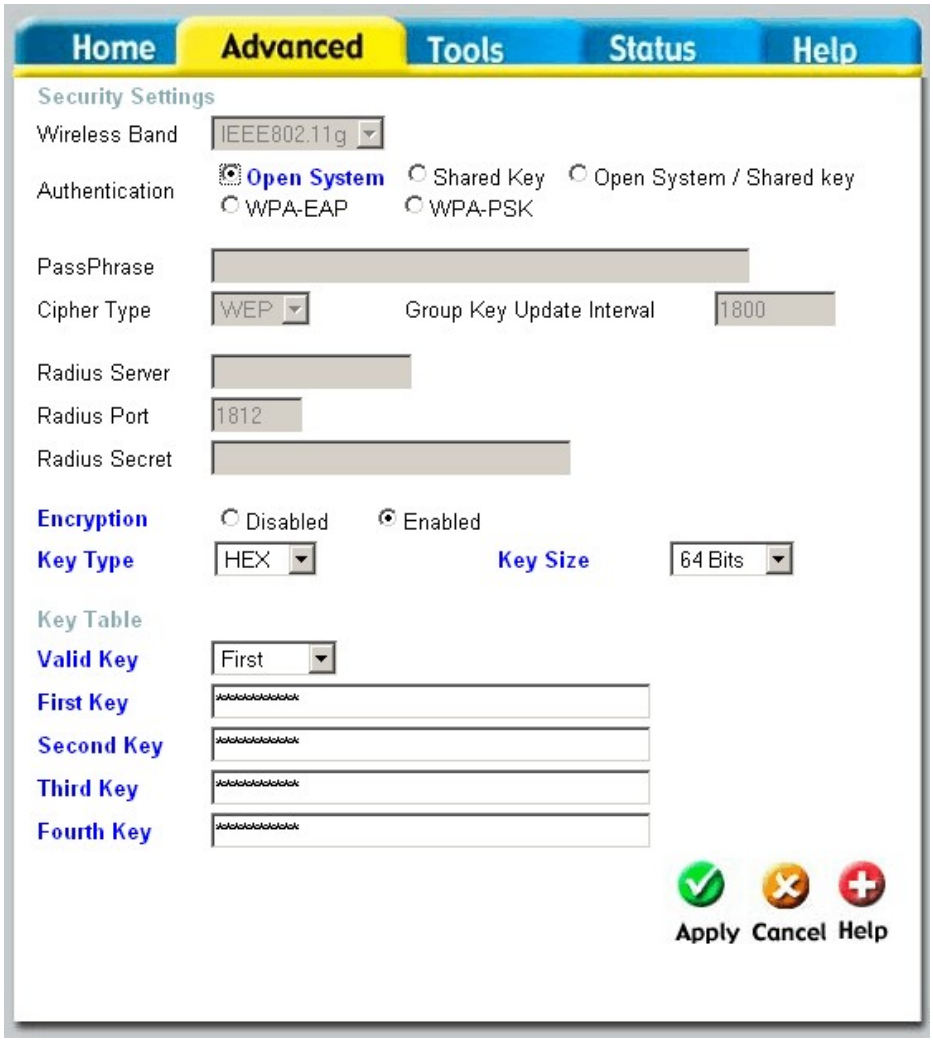
WEP utilise le protocole de chiffrement RC4 et une clé de chiffrement symétrique et statique. Nous n'entrerons pas dans les détails de RC4, ce qui est du ressort des spécialistes de la cryptographie, disons simplement qu'il a été démontré que ce protocole comportait quelques faiblesses graves.

La clé statique, doit être distribuée manuellement sur le ou les points d'accès ainsi que sur tous les clients du réseau sans fils. Nous savons qu'un secret partagé ne reste jamais secret bien longtemps, et plus il est partagé, plus son temps de vie est court.

Nous n'avons pas encore commencé, que déjà, trois grosses faiblesses sont identifiées dans le système WEP :

- le fait que le secret est partagé, ce qui introduit une faiblesse du dit secret,
- le mode de distribution de la clé statique (qui n'est renouvelée que par le bon vouloir de l'administrateur du réseau),
- le protocole de chiffrement lui-même, qui est réputé faible.

Le second point est souvent renforcé par les équipementiers en proposant d'introduire non pas une seule clé, mais plusieurs, en indiquant simplement l'index de la clé actuellement utilisée. Autrement dit, l'administrateur pourra configurer les différents noeuds du réseau avec un ensemble de plusieurs clés (4 dans le cas du point d'accès utilisé ici) en indiquant quelle est actuellement la clé utilisée. C'est un complément de protection que ne vaut que si la clé active est souvent changée, et de façon aléatoire, autant que possible. Mais cette procédure de changement de clé active reste manuelle et doit être exécutée sur tous les noeuds du réseau.



La longueur de la clé peut actuellement être de 64 bits ou de 128 bits, ce qui est à la fois vrai et faux. RC4 nécessite un "vecteur d'initialisation" de 24 bits, qui est généré par RC4 lui-même, si bien que la clé définie par l'administrateur ne fera en réalité que 40 ou 102 bits

La clé partagée peut également servir à faire une pseudo authentification des noeuds sur le réseau. Si l'on choisit l'authentification nommée "shared-key", lorsqu'un client va essayer de se connecter sur un point d'accès, ce dernier lui enverra un texte en clair, que le client chiffrera et renverra au point d'accès.

Ainsi, le point d'accès pourra vérifier que le client dispose bien de la clé et le client, s'il est accepté par le point d'accès en déduira que l'AP dispose de la même clé que lui.

Ainsi également, tout indiscret qui regarde ce qu'il se passe sur votre réseau pourra disposer d'un texte en clair et de son équivalent chiffré, ce qui est une information de premier ordre pour découvrir la fameuse clé. Il faut donc éviter d'utiliser cette méthode d'authentification.

Pour le reste, RC4 va faire son travail et va chiffrer les trames qui circulent sur le réseau sans fil, au niveau 2 (transport).

Pratiquement...

Un intrus, même s'il découvre votre ESSID, même s'il usurpe une de vos adresses MAC autorisées, ne pourra pas se connecter à votre réseau tant qu'il ne disposera pas de la clé partagée.

Donc, nous avons résolu le problème, mais à certaines conditions. En effet, quels sont les moyens dont le pirate dispose, pour s'emparer de la fameuse clé ?

Le "social engineering"

Comme son nom l'indique, cette méthode est purement "sociale". Elle consiste à obtenir l'information par un membre quelconque de l'organisation, qui partage le secret. Un exemple ? Un ami, une relation, un collaborateur occasionnel a eu besoin d'utiliser votre réseau Wi-Fi une fois et vous lui avez communiqué la clé.

La cryptanalyse

Ici, nous entrons dans le domaine informatique. L'indiscret se poste en un point où il peut capturer les trames de votre réseau. Il va alors enregistrer sur sa machine tout ce qu'il capte, pour y découvrir les points faibles du système RC4 appliqué à la norme 802.11. Un outil comme Airodump fait ça très bien, et indiquera en temps réel le nombre de vecteurs d'initialisation (IV) susceptibles d'aider un autre outil (Aircrack) à découvrir votre clé. On estime que pour une clé de 64 bits (40 en réalité), un échantillon de 200 000 trames représentatives permet de déduire la clé en seulement quelques minutes.

Récupérer l'échantillon représentatif peut prendre un "certain temps", qui dépend principalement du trafic généré sur votre réseau. La technique étant (pour l'instant) purement passive, si votre réseau est peu utilisé (cas par exemple d'un réseau sans fils personnel, qui ne sert qu'à partager une connexion internet pour deux ou trois clients), l'opération peut durer plusieurs semaines. Dans le cas d'un réseau d'entreprise, ça pourra aller naturellement plus vite.

Si notre pirate est pressé, il peut disposer d'outils qui vont artificiellement générer du trafic sur votre réseau sans fils. La technique n'est plus seulement passive et donc plus facilement repérable, encore faut-il que l'administrateur reste très attentif pour la détecter. Dans un tel cas, quel que soit le trafic "naturel" généré sur votre réseau, le pirate réussira probablement à récupérer son échantillon représentatif en une ou deux journées tout au plus.

Finalement...

WEP ne peut raisonnablement être utilisé que dans des cas très limitatifs et avec de fortes contraintes administratives :

- l'intrusion du réseau ne doit présenter que peu d'intérêt, c'est un élément important qui détermine la motivation de l'intrus. Votre réseau domestique ne sera probablement pas la proie la plus intéressante, ce qui sera certainement moins vrai pour votre réseau d'entreprise,
- le trafic généré naturellement doit être le plus faible possible,
- il vaut mieux s'assurer régulièrement que le trafic reste conforme à l'utilisation que vous avez de votre réseau,

- la clé partagée doit être modifiée le plus souvent possible, puisque dans le pire des cas, on peut estimer que la durée de vie d'une clé à 64 bits n'est que d'environ une journée. Utilisez donc de préférence une clé à 128 bits, qui nécessitera un plus gros échantillon représentatif, ce qui allongera (un peu) sa durée de vie,
- le nombre de noeuds doit être le plus faible possible (moins un secret est partagé, moins il risque de fuir).

Vous l'avez compris, WEP est à proscrire en entreprise et n'est utilisable, avec précautions, qu'en environnement domestique.

Conclusions

Alors, on fait comment ?

A l'heure où ces lignes sont écrites, il existe plusieurs déclinaisons de la norme 802.11. Parmi les plus courantes :

- 802.11b. Comme son nom ne l'indique pas, elle est la plus ancienne et la plus courante, c'est celle qui a été utilisée pour cet exposé, elle offre un débit théorique de 11 Mbit/s et utilise la bande de fréquences des 2,4 GHz,
- 802.11a. Plus rapide (débit théorique de 54 Mbit/s), elle utilise la bande des 5 GHz et n'est pas compatible avec la norme 802.11b,
- 802.11g. Elle propose également un débit théorique de 54 Mbit/s, mais dans la bande des 2,4 GHz, ce qui lui permet de rester compatible avec les équipements 802.11b.

Toutes ces normes incluent le système de protection WEP, dont on a vu les limites.

Devant les risques encourus, il a été développé un système de chiffrement plus fort, le WPA, qui devrait être inclus dans la norme 802.11i.

WPA est plus "solide" que WEP, mais nécessite pour être le plus efficace une infrastructure lourde, incluant un serveur d'authentification comme un serveur RADIUS (utilisé sur les connexions de type PPP). C'est cependant un moyen nécessaire pour obtenir une sécurité acceptable en milieu professionnel. Pour un milieu personnel, WPA peut tout de même être mis en oeuvre sans la présence d'un serveur d'authentification. On se ramène alors à un système proche (dans sa mise en oeuvre) du WEP, mais avec un système de chiffrement plus robuste.

WPA est inclus sur les équipements récents à la norme 802.11g, mais pourrait être ajouté aussi aux normes 802.11a et 802.11b.

Pour la petite histoire, WPA en est déjà à sa seconde version, la première ayant été démontrée trop peu fiable quelques jours seulement après son annonce.

Finalement, en milieu professionnel, il est nécessaire d'adopter la méthode la plus efficace, à savoir WPA, avec un serveur d'authentification, ce qui permettra d'authentifier non seulement le poste qui se connecte, mais également la personne qui s'en sert (ce que WEP ne sait pas faire), et permettra un chiffrement difficile à casser.

En milieu personnel, on pourra utiliser du WPA sans serveur d'authentification, avec une "pass phrase" (sorte de mot de passe beaucoup plus long qu'un mot de passe habituel) si tout l'équipement dont on dispose supporte cette méthode, sinon, il faudra se rabattre sur WEP, avec une clé la plus longue possible, et qu'il faudra penser à changer assez régulièrement. Il est trop risqué, même pour un usage domestique, de mettre en place un réseau Wi-Fi sans chiffrement.

Et MIMO ?

Ça n'a rien à voir avec la sécurité, mais cette technique qui utilise, rappelons-le, plusieurs antennes et plusieurs émissions (sur le même canal ou non, suivant les implémentations), dans le but de gérer au mieux les problèmes liés aux réflexions et aux absorptions des ondes par des obstacles semble

très prometteuse, à en croire les divers tests publiés sur ce sujet.

L'inconvénient majeur, à l'heure où ces lignes sont écrites, est que le procédé n'est pas entièrement normalisé et que les solutions proposées par les divers constructeurs ne sont pas forcément compatibles entre elles, pire, elle peuvent même être parfaitement incompatibles.

A moins de s'astreindre à n'utiliser les services que d'un seul constructeur, il semble donc préférable d'attendre une plus grande maturité de cette technologie qui devrait être incluse dans la norme 802.11n