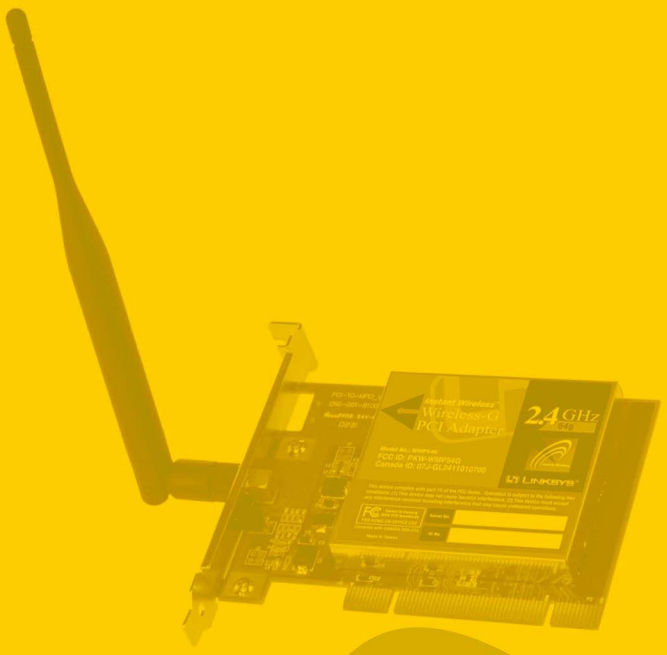
Documentation Officielle

wireless-fr.org



802.11
Les Réseaux Sans Fils

Nantes Wireless

angers Wireless

INFRACOM Online 24/24h

http://online.infracom.fr

Table des matières

1- Avant Propos

1.1- Public visé par l'ebook

Cet Ebook s'adresse à tout le monde:

Les débutants désireux de découvrir la technologie du Wi-Fi et souhaitant une documentation complète.
Les étudiants en quête de documentation technique pour leur présentation ou dossier.
Les particuliers désireux d'installer un réseau sans fil chez eux.
Les professionnels voulant approfondir leurs connaissances dans certains domaines tel que la transmission de données par exemple.

Cet Ebook s'adresse tout de même à des personnes ayant certaines notions en informatique et plus particulièrement en réseaux, il sera fait appel à certaines notions de réseaux tout au long de cet ouvrage.

Note : Tout le contenu de cet Ebook n'est pas forcément correct, cet Ebook étant le travail d'un ensemble de personnes amateurs et parfois professionnels, il se peut que vous y trouviez des erreurs, si c'est le cas veillez à insérer une note en bas de la page concernée sur le wiki pour y avertir son auteur (http://www.nantes-wireless.org/wiki). (Fa / Pr)

1.2- Rédaction de l'ebook

Cet E-Book a été développé par la communauté wireless francophone et plus particulièrement les équipes de Nantes-wireless et d'Angers-wireless.

Voici une liste des personnes ayant contribués à sa réalisation:

Fanfoue (fa) : Francois Gerthoffert : f.gerthoffert@caramail.com
Prospere (pr) : Ludovic Toinel : prospere@nantes-wireless.org
Lessyv (le) : Christophe Malinge : theboss@lessyv.com
Flyer (fl) : Eric, Infracom : infracom@infracom-france.com
Darkkro (da) : Christophe Rabiller : darkkro@free.fr
Psio (ps) : Julien Arbey : psio@nantes-wireless.org
Kartapuce (ka) : Francois Belleil : kartapuce@aol.com
Marc (mr) : Marc Revial : Voodu_air@wireless-guerrilla.org
Gortex : tim69@free.fr
Vsmetal (vs) : Vincent Serpoul : vincent@serpoul.com

(Fa / Pr)

2- Introduction

2.1- Les réseaux sans fils

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radio électriques. Les réseaux sans fil ne sont pas tout récents (cf. : Packet Radio), mais avec le développement de l'informatique et des systèmes d'information, la technologie est venue au besoin primaire de l'homme : la mobilité. Ces réseaux dit "wireless" ou "sans fil" ont leur nom de code : Wi-Fi, BlueTooth, BLL, UMTS etc...

(Pr)

2.2- Les technologies

Les technologies dites "sans fil", le 802.11b en particulier, facilitent et réduisent le coût de connexion pour les réseaux de grande taille. Avec peu de matériel et un peu d'organisation, de grandes quantités d'informations peuvent maintenant circuler sur plusieurs kilomètres, sans avoir recours à une compagnie de téléphone ou de câblage.

Ces technologies peuvent être classées en quatre parties :

Les réseaux personnels sans fil : Wireless Personal Area Network (WPAN)
Les réseaux locaux sans fil : Wireless Local Area Network (WLAN)
Les réseaux métropolitains sans fil : Wireless Metropolitan Area Network (WMAN)
Les larges réseaux sans fil : Wireless Wide Area Network (WWAN)

1) Les réseaux personnels sans fil (WPAN)

Les réseaux sans-fil personnels concernent les réseaux ayant une très faible portée de l'ordre de quelques mètres. Ils sont surtout utilisés pour interconnecter du matériel informatique de poche comme les PDA, téléphones mobiles et même les ordinateurs portables.

1.1- Le Bluetooth

Le Bluetooth (ou "dents bleues") est un standard développé en 1994 par Ericsson et normalisé par l'IEEE 802.15.1. Son débit théorique est de 1 Mb/s mais en pratique il atteint 720 Kb/s. Le bluetooth à une portée de 10 à 20 mètres et permet l'interconnexion de huit terminaux simultanément. Son point fort réside dans sa faible consommation d'énergie. On le voit apparaître de plus en plus dans de nombreux matériels, comme les téléphones mobiles et les PDA.

1.2- Home RF

HomeRF est un standard développé en 1998 par le "Home Radio Frequency Working Group", consortium qui incluait au départ : Compaq, IBM, HP, Intel et Microsoft. Ce standard utilise tout comme le Wi-Fi la bande de fréquence du 2.4GHz. Il offre un débit théorique de 10 Mb/s pour un débit pratique de 3 à 4 Mb/s partagé entre tous les utilisateurs connectés. Sa portée varie entre 50 et 100 m.

1.3- Openair

Openair est un standard proche du 802.11b, il utilise lui aussi la bande de fréquence du 2.4Ghz et propose un débit de 1.6 Mb/s.

2) Les réseaux locaux sans fil (WLAN)

Les réseaux locaux sans fil sont de plus en plus utilisés au sein des entreprises et des réseaux locaux particuliers. Ils permettent la couverture de bâtiment entier.

2.1- Wi-Fi

Le Wi-Fi (Wireless Fidelity) est le nom commercial du standard IEEE 802.11b développé en 1999. Ce standard est actuellement l'un des standards les plus utilisés au monde. Le débit théorique du 802.11b est de 11 Mb/s et le débit pratique varie en fonction de l'environnement. Le Wi-Fi utilise la bande de fréquence du 2.4 GHz. En fonction du milieu la portée d'un point d'accès Wi-Fi varie entre 10 et 200 m.

Il existe aussi le standard 802.11g (encore en développement), nouvelle amélioration du 802.11b qui permet un débit de 54 Mb/s.

2.2- Hiperlan

Hiperlan est une technologie développée par l'ETSI (European Telecommunication Standard Institute). Deux versions de ce standard existent, Hiperlan1 et Hiperlan2 qui peuvent fonctionner ensemble. Ce standard utilise une bande de fréquence proche du 5 GHz. Le débit théorique proposé par Hipperlan1 est proche de 20 Mb/s et celui de l'Hiperlan2 est de 54 Mb/s. La zone de couverture dépend du milieu, la fréquence ayant une longueur d'onde plus petite, celle-ci est plus sensible aux obstacles, cependant dans des milieux dégagés (type point à point) la connexion sera meilleure que pour le Wi-Fi.

3) Les réseaux métropolitains sans fil (WMAN)

Les réseaux métropolitains sans fil sont connus sous le nom de boucle locale radio (BLL). Les BLL sont basés sur le standard IEEE 802.16. La boucle locale radio offre un débit théorique entre 1 et 10Mb/s pour une portée de 4 à 10 kilomètres, cette technologie est principalement utilisée par les opérateurs téléphoniques. En France seulement 4 opérateurs ont une licence pour mettre en place cette technologie dans les grandes villes. Cette licence leur a été délivrée par l'ART.

4) Wireless Wide Area Network (WWAN)

Les réseaux sans fil étendus sont généralement connus sous le nom de réseau cellulaire. Ces WWAN ont une plus grande portée, tous les réseaux mobiles sont connectés à un WWAN.

4.1- Le GSM :
4.2- Le GPRS :
4.3- l'UMTS :
4.4 - Le Packet radio :

Utilisé par les radio amateurs, avec un débit maxi de 9600 Bits/s. De grande distances sont possibles, utilisation de la bande des réseaux amateurs.

(Fa / Pr)

2.3- Les WiFi ou la norme 802.11b

La norme Wi-Fi (Wirelesss Fidelity) est le nom commercial donné à la norme IEEE 802.11b par Weca.

La norme 802.11b est un ensemble de règles définissant la transmission de données informatiques via le medium 'hertzien'.
Cette norme permet de transmettre des données jusqu'à un débit de 11 Mbits/s, et 22 Mb/s grâce à l'utilisation plusieurs canaux simultanés comme le font les cartes D-Link.

En 1997 l'élaboration du standard IEEE 802.11 et son développement rapide fut un pas important dans l'évolution des réseaux sans fil.. Il a ainsi permis de mettre a portée de tous un vrai système de communication sans fil pour la mise en place des réseaux informatiques hertziens. Ce standard a été développé pour favoriser l'interopérabilité du matériel entre les différents fabricants ainsi que pour permettre des évolutions futures compatibles un peu à la manière de l'Ethernet. Ceci signifie que les consommateurs peuvent mélanger des équipements de différents fabricants afin de satisfaire leurs besoins. De plus cette standardisation permet d'obtenir des composants à bas coût ce qui se traduit par des prix plus faibles pour le consommateur.

Le standard définit un choix de différentes couches physiques. Celles-ci sont au choix DSSS (Direct Sequence Spread Spectrum, ou FHSS (Frequency Hopping Spread Spectrum). Dans un premier temps la norme spécifiait pour le DSSS un taux de transfert de 2Mbps avec un taux optionnel de fallback à 1Mbps dans des environnements très brouillés, alors que le taux de transfert était de 1Mbps pour le FHSS. La plupart des vendeurs ont choisis d'implémenter le DSSS après qu'une nouvelle version du standard (la 802.11b High Rate) permettant d'obtenir des taux de 5,5 et 11Mbps fut adoptée, Celle-ci présentait l'avantage de garder la même couche physique. Ces deux normes sont bien sûr compatibles et peuvent coexister sur un même réseau. Elles travaillent toute deux dans la bande ISM de 2.4GHz (2.4000GHz-2.4835GHz) qui est normalement allouée à travers le monde pour des opérations sans licences.

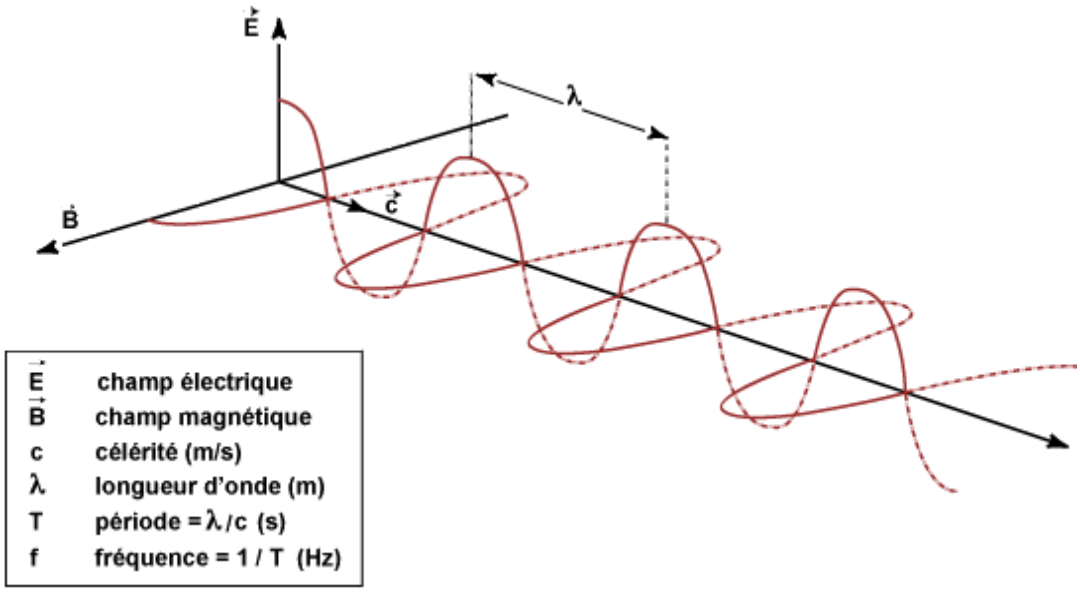
Le protocole 802.11 est très robuste et plein de fonctionnalités. Il présente de nombreux avantages permettant de minimiser les interférences, de maximaliser la bande passante sur les canaux. Le 802.11 peut travailler de manière transparente avec l'Ethernet à travers un pont, ou un point d'accès, de manière à ce que tous les éléments avec et sans fils puissent interagir.

Note : Le terme Wi-Fi est une marque déposée

3- Les ondes électromagnétiques :

3.1- La propagation des ondes

Ci-dessous la représentation d'une onde électromagnétique:



Source www.radioamateur.org

L'onde électromagnétique est formée par le couplage des deux champs ci dessous, le champ électrique (E) et le champ magnétique (B). Nous pouvons grâce à ce schéma nous rendre compte que la fréquence est définie par la célérité et la longueur d'onde.

(Fa)

3.2- La vitesse de propagation

La vitesse de propagation d'une onde électromagnétique est en tout point identique à la vitesse de propagation de la lumière (sauf la fréquence).
On peut donc en déduire grâce à l'équation suivante, la fréquence pour une transmission dans un milieu « parfait » (dans le vide).

Calcul de la Fréquence : F (en Hz)

F = C / Lambda

Notes :
F = Fréquence en Hz
C = Célérité (m/s)
Lambda = longueur d'onde (m)

Calcul de la longueur d'onde : Lambda (en m)

Lambda = C / F

Notes :
C = Célérité (vitesse de propagation de la lumière dans l'air : 299.972458 Km/s)
F = Fréquence (en MHz)
Lambda = longueur d'onde (m)

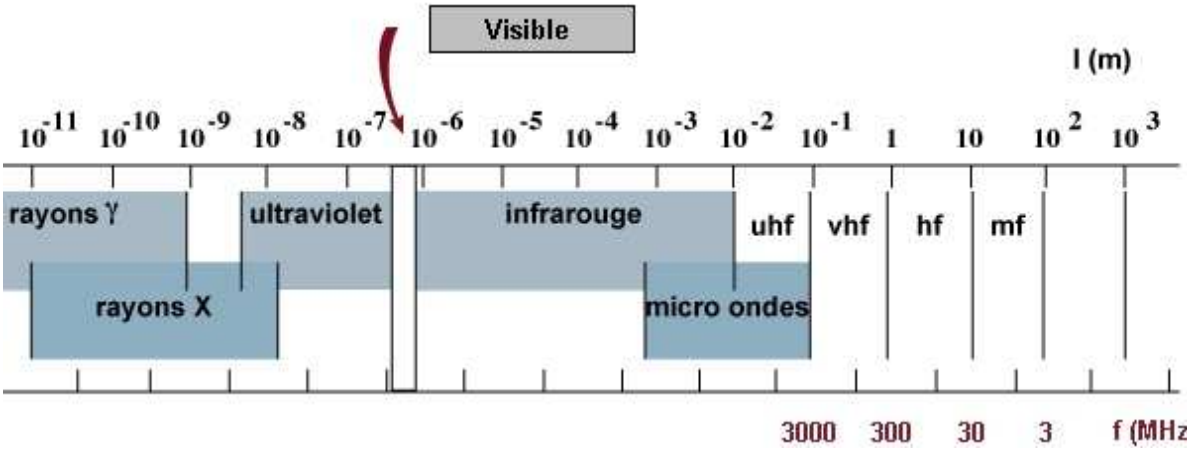
C: correspondant à la vitesse de propagation de l'onde est variable et dépend du milieu traversé (l'air, l'eau, un milieu boisé, etc).

Certains matériaux et milieux laisseront en effet plus facilement passer les ondes que d'autres.

(Fa / Go)

3.3- Le spectre

Voici le spectre électromagnétique, le Wifi opère à une longueur d'onde de 12,2448 cm et une fréquence d'approximativement 2,45 Ghz (précisément : de 2412 Mhz à 2472 Mhz).



Voici la liste des fréquences utilisées par le 802.11b

Canal 1 : 2,412 Mhz	Canal 2 : 2,417 Mhz
Canal 3 : 2,422 Mhz	Canal 4 : 2,427 Mhz
Canal 5 : 2,432 Mhz	Canal 6 : 2,437 Mhz
Canal 7 : 2,442 Mhz	Canal 8 : 2,447 Mhz
Canal 9 : 2,452 Mhz	Canal 10 : 2,457 Mhz
Canal 11 : 2,462 Mhz	Canal 12 : 2,467 Mhz
Canal 13 : 2,472 Mhz	Canal 14 : 2,477 Mhz

(Fa / Ps / Go)

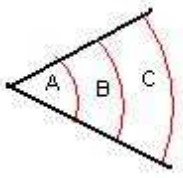
3.4- Les phénomènes électromagnétiques

3.4.1- L'atténuation

Il faut aussi prendre en compte l'atténuation, en effet une onde n'est pas envoyée à l'infini, plus on va s'éloigner de la source plus la qualité du signal diminuera, le phénomène en cause est la dispersion spatiale, qui s'applique lui aussi à la lumière.

Prenez une lampe torche par exemple, vous remarquerez que plus le faisceau sera étroit plus vous verrez loin, mais vous n'éclairerez qu'une faible surface, et inversement si vous agrandissez votre faisceau, vous ne verrez pas très loin mais vous couvrirez une plus grande surface (ce point sera approfondi dans la partie sur les antennes).

L'atténuation peut être représentée de cette maniere:



La densite de puissance du flux en A sera plus important qu'en B ou C et ainsi de suite.
L'atténuation de parcours peut se mesurer à l'aide de l'équation suivante:

Ploss = 10 Log (4 pi d / HL) ^2

d: distance en m
HL : Longueur d'onde en m

Ploss ou Path Loss correspond à la perte de parcours qui se mesure en Db (decibels). Le ploss obtenu grâce à l'équation ci dessus correspond à l'atténuation de parcours en

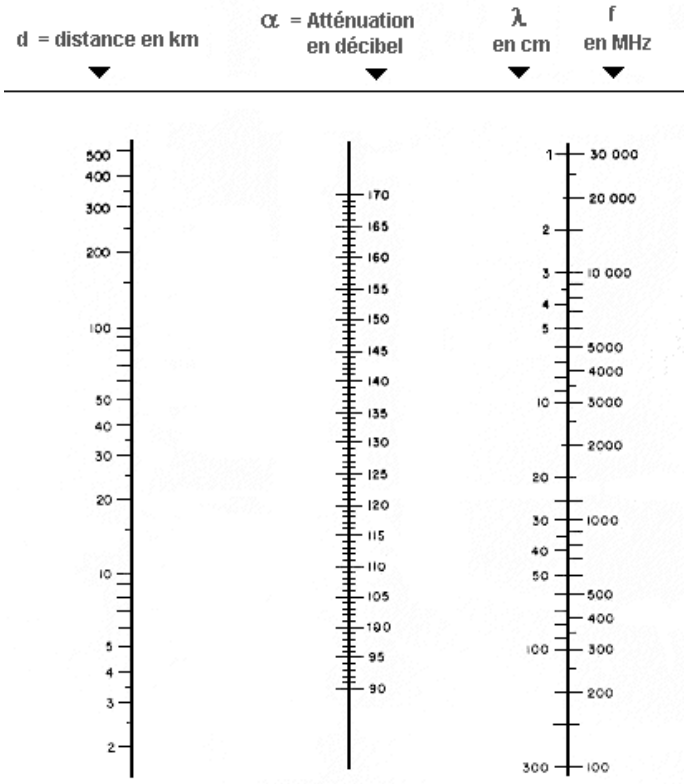
espace libre, c'est à dire au resultat que l'on pourrait obtenir dans un espace libre s'il n'y avais aucune perturbation. Exemple d'application: La longueur d'onde se calcule de la manière suivante:

HL = 30 / F

F : Fréquence en Ghz
HL : Longueur d'onde en cm

Pour une fréquence de 2,45Ghz, HL = 12,2448 cm

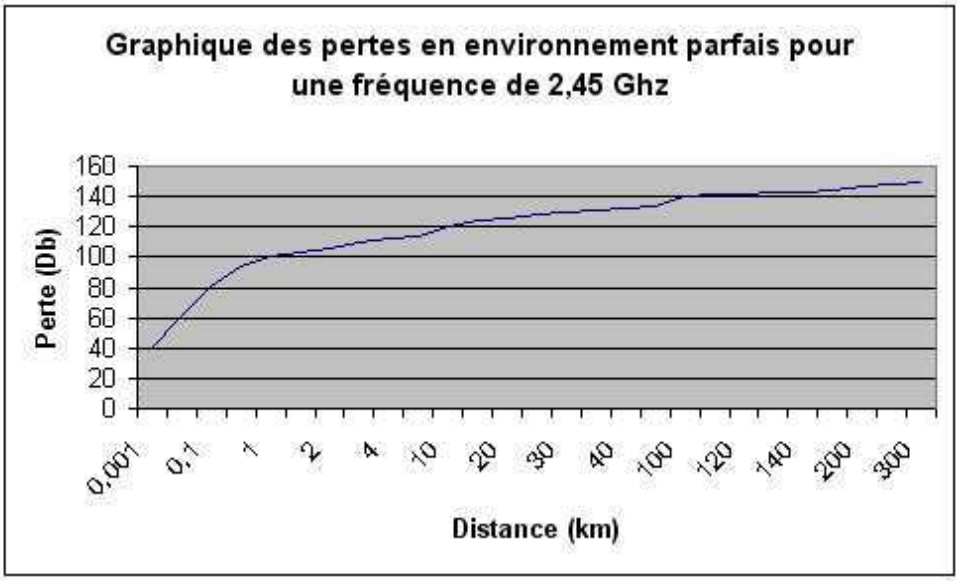
Vous pouvez simplement utiliser ce graphique pour faire vos calculs :



Atténuation en espace libre entre deux antennes isotropiques

$\alpha = 32{,}45 + 20 \log f + 20 \log d$

Donc en fonction de la distance on peut obtenir la courbe de perte (ou atténuation du signal) en dBm suivante.



Cette courbe représente ce qui se passerait dans un milieu parfait, mais en réalité il y a un phénomène d'absorption.

(Fa)

3.4.2- L'absorption

L'onde électromagnétique qui voyage rencontre des électrons qu'elle va exciter. Ceux-ci vont réémettre à leur tour du rayonnement ce qui perturbera le signal et donc l'atténuera.
Il est important de noter que plus la fréquence est élevée plus ce phénomène d'absorption est élevé donc plus la distance de couverture est faible.

C'est pour cela que les communications radio se font sur des fréquences d'une centaine de Mhz. Il est à noter aussi que plus la fréquence est élevée, plus la vitesse de transmission de données peut être importante.

Pour le WiFi, par exemple on peut difficilement faire plus de 10km avec du matériel « classique » (nous aborderons ce point plus loin).

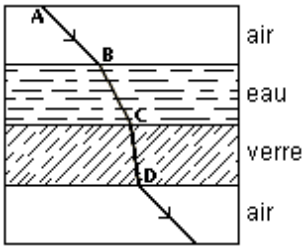
Note : le matériau absorbant le plus le signal est l'eau. Par conséquent le signal aura tendance a être légèrement moins bon les jours de pluie.

(Fa / Pr)

3.4.3- La réfraction

Une onde électromagnétique traversant différents milieux change de direction et ce proportionnellement à l'indice de réfraction des milieux traversés.

Voici l'exemple d'une onde traversant différents milieux :

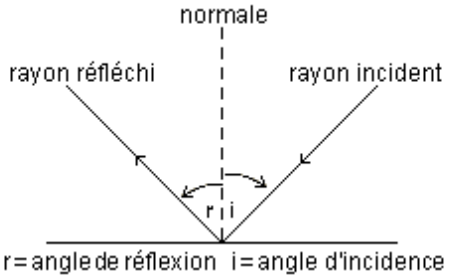


(Fa)

3.4.4- La réflexion

Les ondes électromagnétiques peuvent être réfléchies totalement ou en partie, exactement de la même manière que pour la lumière, mais ce phénomène est plus utilisé par les radio amateurs que pour les transmissions wireless.

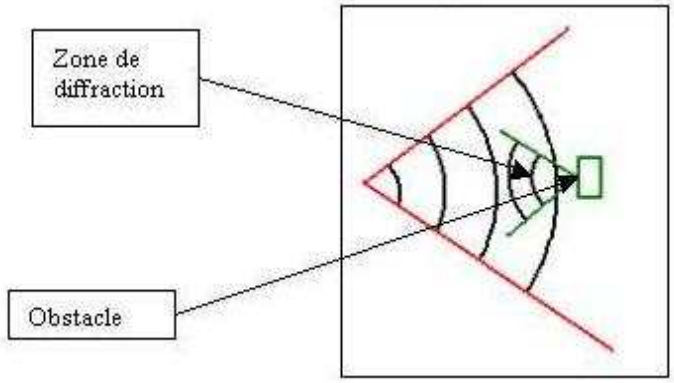
En effet, à la fréquence de fonctionnement du wireless, les obstacles auront davantage tendance à absorber les onde qu'à les réfléchir.



Dans ce schéma ci-contre, un rayon (nous prenons des analogies "lumineuses", car ce que nous émettons à le même comportement que la lumière puisque de même nature) dit rayon incident est réfléchi par une surface plane d'un angle "i".
Le rayon réfléchi l'est d'un angle identique "r".
La différence angulaire entre le rayon incident et le rayon réfléchi est donc de 2 i, ou 2r.
(Fa / Go)

3.4.5- La diffraction

La diffraction est une zone d'interférence entre l'onde directe d'une source et l'onde réfléchie par un obstacle, en quelque sorte l'onde s'interfère elle même.



Il s'agit de zones d'interférences entre l'onde directe d'une source et l'onde dont la direction est modifiée par un obstacle tel que montage ou immeuble. Ces deux ondes, issues de la même source, interfèrent entre elles de manière à ce que l'on se retrouve soit avec une augmentation importante liée au couplage en phase, soit à une diminution, voire une annulation totale. En fait, nous avons affaire à la modification du trajet d'une onde lorsqu'elle passe à proximité d'un obstacle. Par exemple, dans un milieu homogène, la lumière se propage en ligne droite. Après traversée d'une ouverture, cette onde plane ne se propage plus selon la même direction. La diffraction, qui existe pour toutes les ondes électromagnétiques, s'observe dans les cas où les dimensions de l'ouverture sont petites devant la longueur d'onde
(Fa / Go)

3.5- Le Gain (dBm, dB, dBi)

Le Gain est exprimé en déciBel.

Calcul du Gain :

$$G_{db} = 10 \text{ Log } \frac{P_{sortie}}{P_{entrée}}$$

P = Puissance en mW
Tableau mettant en relation le rapport

$$\frac{P_{sortie}}{P_{entrée}}$$

et le Gain :

Coeff	dB
1	0
2	3
3	4.77
4	6
5	6.99
6	7.78
7	8.45
8	9
9	9.54
10	10
11	10.4
12	10.8
13	11.14
14	11.46
15	11.76

Coeff	dB
20	13
25	13.98
30	14.77
35	15.44
40	16
45	16.53
50	17
55	17.4
60	17.8
65	18.1
70	18.45
75	18.75
80	19
85	19.3
90	19.54

Coeff	dB
100	20
150	21.76
200	23
250	23.98
300	24.77
350	25.44
400	26
450	26.53
500	27
550	27.4
600	27.78
650	28.13
700	28.45
750	28.75
800	29

Coeff	dB
1 000	30
2 000	33
3 000	34.77
4 000	36
5 000	36.99
6 000	37.78
7 000	38.45
8 000	39
9 000	39.54
10 000	40
20 000	43
30 000	44.77
40 000	46
50 000	47
100 000	50

Puissance dBm :

C'est une relation mettant en rapport le Gain (en dB) et la puissance (en mW à une impédance de 50 Ohms)

$$G_{dbm} = 10 \text{ Log } P$$

$$P = 10^{\frac{G_{dbm}}{10}}$$

P = Puissance en mW

G_{dBm}	0	6,99	10	14	15,2	17	18,8	20
P (en mW)	1	5	10	25	33	50	75	100

Puissance dBi :

Le dBi exprime en dB le gain d'une antenne par rapport à un aérien isotrope qui émet la même quantité d'énergie dans toutes les directions.
Pour les fréquences supérieures à 890 MHz, le gain de l'antenne est exprimé relativement à un radiateur isotrope (dBi).

Calcul du Gain théorique d'une parabole :

Avec :
d = diamètre en m
l = longueur d'onde en m
h = rendement (comptez 50%)
Log = Log base 10
G en dBi

(Go)

4- Spécifications

4.1- Le roaming itinérance

La norme 802.11 permet de "roamer" entre plusieurs points d'accès étant sur le même ou sur différents canaux.

Par exemple toutes les 100ms le point d'accès peut transmettre un signal de balise (beacon signal) qui contient une marqueur temporel pour la synchronisation avec le client, une carte de trafic, une indication des taux de transfert supportés, ainsi que d'autres paramètres.
Le client en roaming peut utiliser ce signal pour déterminer la puissance de sa connexion avec la station de base.
Si ce signal est jugé insuffisant ou faible le client en roaming peut décider de s'associer à une nouvelle station.

4.2- Le power management

Le 802.11 ajoute des fonctionnalités de power management pour augmenter la durée de vie des batteries.

Les schémas d'économie d'énergie habituels posent des problèmes avec le système WLAN. Ceux-ci mettent généralement le système en mode veille (peu ou pas de courant consommé), lorsqu'une inactivité se produit pendant une période de temps définissable par l'utilisateur. Malheureusement lorsque le système est dans cet état, il peut manquer de la transmission d'informations importantes.

Afin de supporter les clients qui entrent en mode veille régulièrement, le 802.11 inclut un buffer (tampon) dans la borne d'accès afin de stocker les messages du client. Les clients en mode veille doivent récupérer ces messages à intervalles réguliers. Les bornes d'accès ont un mécanisme pour effacer les messages qui n'aurait pas été récupérés après un certain laps de temps.

4.3- L'interopérabilité du matériel

L'un des plus grand avantage du standard 802.11 est la capacité pour des produits venant de fabricants différents à opérer entre eux. Ceci signifie que vous pouvez acheter des cartes WLAN de fabricants différents et les utiliser pour communiquer et ce quelque soit la marque de la borne d'accès. Ceci permet à l'utilisateur de trouver le matériel répondant spécifiquement à ses besoins. Il a été dit dans le passé que la compatibilité n'était pas parfaite, ce n'est plus le cas aujourd'hui avec le 802.11b (High Rate), ou la plupart des équipements ont passé les tests de compatibilité.

5- Le matériel

5.1- Le matériel informatique

5.1.1- Les Chipsets

5.1.1.1- Prism II

Chipset le plus couramment rencontré sur du materiel Wireless, il est parfaitement reconnu sous linux et permet un débit maximal de 11mb/s.

Quelques cartes utilisant un chipset Prism II:

D-Link DWL 650
D-Link DCF 650
Linksys WMP11
Actiontec PCMCIA
Actiontec USB
Actiontec PCI
...

(Fa)

5.1.1.2- TI ACX 100

Chipset apparu durant le second semestre 2002, a tout de suite remporté un très grand succès du fait de son faible coût. Adopté par D-Link pour sa carte PCI DWL 520+ il permet de réaliser des transfert allant jusqu'a 22 Mbits/s, un mode 4X a été inséré permettant de faire du 44Mbit/s en débit théorique, mais seulement 1 Mo/s en pratique.

Il est supporté par Linux de manière non officielle.

Voivi quelques cartes utilisant le chipset Texas Instrument:

D-Link DWL520+
D-Link DWL650+
La carte du WAP11
Le DWL-900AP+
...

Concernant le support Linux : http://seattlewireless.net/index.cgi/DlinkDwl650Plus

Nous expliquerons plus loin l'installation d'une carte DWL 520+ sous Linux.

(Fa / Mi)

5.1.1.3- Hermes

Chipset utilisé par les cartes Orinoco, & Co assez répandu et supporté par Linux.

5.1.1.4- ATMEL

Les chipsets ATMEL peuvent être utilisés par des adaptateurs PCMCIA et USB. Beaucoup des cartes utilisent ce chipset.

Les cartes Sitecom WL-011(PCMCIA) et WL-012(USB) utilisent le chipset Atmel AT76C503A.
Des drivers Open-Source sont disponibles pour Linux :
http://atmelwlandriver.sourceforge.net/

(Ma)

5.1.2- Les clients

5.1.2.1- Cartes PCMCIA

Il existe plusieurs sortes de Cartes PCMCIA, si distinguant par leur puissance ou la présence d'un connecteur antenne.

1) Le connecteur antenne

Généralement de type Lucent (Orinoco, avaya), MCX, MMCX il permettent de rajouter une antenne à gain, ce qui peut être interessant si vous êtes situés assez loin d'un point d'accès par exemple.

Ce type de carte coute généralement plus chère.

Note: Il est possible de modifier certaines cartes (D-Link DWL-650 par exemple) pour rajouter un connecteur antenne, mais la garantie de la carte est bien évidemment perdue.

2) La puissance

La puissance des cartes Wireless va de 30mW à plus de 200mW, habituellement les cartes que vous rencontrerez dans le commerce auront une puissance de 30 mW (env. 15 dBm).

Ces cartes sont peu chères (moins de 60 euros) mais ne possèdent généralement pas de connecteur antenne.

Les cartes 100 mW (Orinoco, avaya, ...) possèdent généralement un connecteur antenne.

Les cartes de plus de 100 mW ne sont pas vendues en France (trop puissante par rapport à la législation).

3) Quelle carte choisir ?

Que voulez vous faire:
Des expérimentations:
Carte avec connecteur antenne et puissance importante
Vous découvrez le wireless et vous voulez juste vous connecter à l'AP que vous venez d'acheter:
Carte la moins chère possible
Vous connecter à un AP situé assez loin, ou faire des distances importantes:
Carte avec connecteur antenne et puissance importante
(Fa / Go)

5.1.2.2- Cartes PCI

L'atout principal des cartes PCI par rapport aux cartes PCMCIA est l'antenne, qui est soit intégrée à la carte soit amovible (donc possibilité de connecter l'antenne de votre choix).

Il est important de ne pas prendre une carte PCI avec antenne intégrée, le PC étant généralement situé sous un bureau la qualité de réception sera souvent médiocre, optez donc pour une carte avec connecteur antenne.

En ce moment la carte la plus intéressante est la DWL-520+ de chez D-link (SMC vend apparemment un modèle similaire), elle fait partie des cartes les moins chères du marché et possède un mode 22 Mbits/s + 4x pouvant atteindre une vitesse de 44 Mbits (théoriquement).

(Fa / Go)

5.1.2.3- Cartes USB

Les cartes USB de divisent en 2 grandes familles :

Les cartes "adaptateur"

Une partie des cartes USB sont en fait des adaptateurs avec à l'intérieur une carte PCMCIA (généralement orinoco) comme certains modèles HP par exemple.
Ces cartes sont assez intéressantes car elles possèdent généralement un connecteur antenne sous leur coque, la modification est donc à la portée de tout le monde.

Les cartes "classiques"

Les cartes usb classiques n'ont généralement pas de connecteurs antennes, mais sont intéressantes dans le sens qu'elles peuvent êtres orientées, grâce à généralement 2m de câble, donc êtres considérées comme des petites antennes.

A noter que Linksys a sortie une carte Usb qui ressemble à un "Pen drive", donc qui peux intéresser les possesseurs de portables sans ports PCMCIA.

Une bonne partie des cartes USB sont modifiables pour y ajouter un connecteur antenne.

(Fa)

5.1.2.4- Cartes COMPACT FLASH

Il y a peu de différences entre les cartes Compact Flash et les cartes PCMCIA, si ce n'est leur format et leurs pilotes, certaines cartes sont fournies avec des pilotes Windows (pour PC de bureau et portable) en plus des pilotes pocket PC et d'autres non, renseignez-vous avant de vous en procurez une.

Les cartes Compact Flash sont le plus souvent dépourvues d'un connecteur pour antenne externe.

(Fa / Go / Pr / Re)

5.1.2.5- Ponts réseaux

Pont réseau de chez Linksys : le WET11.

Un pont réseau ou "bridge" en anglais permet d'étendre un réseau et de diminuer ta taille de la zone de broadcast, il agit comme un switch à deux ports.
Le rôle d'un pont réseau Wi-Fi est de convertir les trames 802.11b ou g en trames Ethernet.

Le gros avantage d'un pont c'est qu'il est invisible sur le réseau, tout le traitement des

données se fait sur la couche deux du modèle OSI. Un pont n'exécute aucun routage.

Grâce à son "invisibilité" vous pouvez vous en servir pour des aplications exotiques :
- Le mettre sur une PS2 pour jouer avec votre voisin.
- Xbox aussi grâce a son interface réseau.
- Le mettre sur votre imprimante.

(Da / Pr)

5.1.2.6- Antenne avec module wireless intégré

La SW24003 élimine tous les problèmes de pertes dans les liaisons antenne/module WiFi :
Tout est intégré dans le même boîtier, avec un booster USB de 5 m et jusqu'à 10 m de câble USB.

Pilotes:
Windows 98,2000,XP
Linux
MAC
Trois versions d'antennes sont disponibles : 8 dB, 12 dB, et 18 dB.

(Fl)

5.1.3- Les Points d'Accès

5.1.3.1- Le Linksys WAP11

Le Linksys Wap11 est un point d'accès IEEE 802.11b.
http://www.linksys.com/international/product.asp?coid=15&ipid=68

Le WAP11 de Linksys, est un AP très répendu chez les wifistes.
Il existe plusieurs versions du WAP11 la v1.1 et la v2.2.
La différence primordiale entre les deux versions est que la configuration du v1.1

pouvait se faire grâce à un port USB présent à l'arrière de l'appareil. La configuration par USB s'étant avérée une mauvaise idée, le port USB a donc été supprimé dans la version 2.2.

Documentation :
Tests complets du Wap11 v2.0 (par Origin):
http://www.nantes-wireless.org/pages/materiel/fiches/LinkSys-WAP111.pdf
Son démontage:
http:///www.nantes-wireless.org/pages/wiki/index1240.html?pagename=D%E9montageDuWap11

Notes :

Sur le modèle v2.2 il est possible d'upgrader le firmware avec celui du DLink DWL 900+, pour plus d'infos à ce sujet:
http://www.nantes-wireless.org/index.php?page=doc/waphack

(Da)

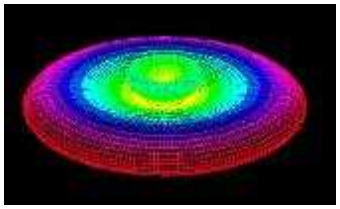
5.2- Les antennes

5.2.1- Antennes Omnidirectionnelles

Ces antennes ont un gain variant de 0 à 15 dBi environ, sachant que 8 dBi correspond encore à un prix acceptable.
Leur rayonnement s'effectue sur 360°.
Elles sont utilisées pour établir une réseau urbain de type client - serveur, permettant de fournir un accès au réseau, dans un parc par exemple.

Exemple d'antennes omni (24 1360) :

Vue en 3D de sa propagation:

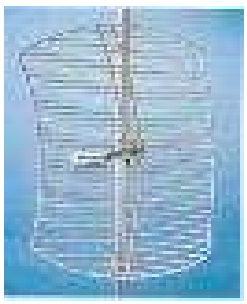


(Fl)

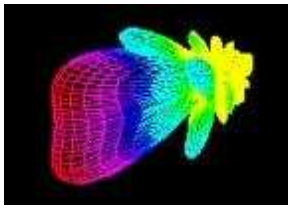
5.2.2- Antennes Directionnelles

Ces antennes ont habituellement un gain élevé, de 5 dB minimum jusqu'à 24 dB environ, avec un rayonnement directif.
Elles permettent d'établir des liaisons point à point pour réaliser le backbone d'un réseau urbain, mais également de couvrir une zone limitée dans le cas d'une antenne à angle d'ouverture important.

Antenne parabole (gain 13 dB):

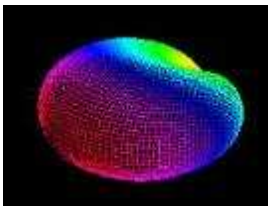



Vue en 3D de la propagation des ondes :

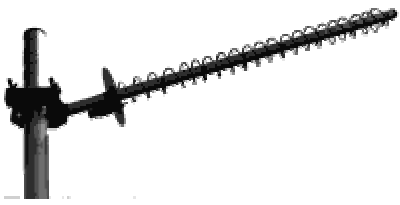


Antenne panneau :

Vue en 3D de la propagation des ondes :



Antenne hélicoïdale :



Il existe plusieurs modèles d'antennes directives : panneau, paraboles, paraboles grillagées, patch, Yagi (bande étroite, peu conseillée pour le WiFi), hélicoïdales (pour les liaisons lointaines en milieu urbain ou perturbé eau, océan, fleuve, etc.).

Une antenne directive se caractérise par son gain (cf: ci-dessus), mais également par son angle d'ouverture :

Une antenne de 10 dB et 60° d'ouverture, pourra tout à fait convenir pour couvrir, par exemple, une place en centre ville, voir un quartier

complet.
Une antenne de 14 dB avec 40° d'ouverture couvrira elle une zone plus longue, mais plus étroite.

Chaque application nécessite par conséquent une étude sérieuse, de façon à utiliser l'antenne la plus adaptée.

(Fl / Pr / Go)

5.2.3- Fabrication d'antennes

Il est tout à fait possible pour un particulier de se fabriquer ses propres antennes, mais il faut savoir que ce n'est pas sans risques : il faut respecter les cotes au millimètre près.

Le R.O.S (ou Rapport d'Ondes Stationnaires) et un phénomène constaté lorsqu'une antenne à un défaut de fabrication, cela s'apparente à la diffraction, en quelque sorte il y a un phénomène de diffraction à l'intérieur de l'antenne et l'émetteur reçoit donc des ondes, mais il n'est pas conçu pour ça, il risque donc d'être endommagé.

Le brouillage des ondes est un point à ne pas négliger, si votre antenne artisanale a été conçu pour une autre bande de fréquence que le Wi-Fi, cette antenne émettra sur cette bande de fréquence et brouillera donc ces fréquences avec des signaux parasites. La solution pour une antenne de fabrication personnelle est de la tester grâce à un ROS-mètre, mais cet appareil coûte très cher. Dans la majorité des cas le résultat obtenu par une antenne de fabrication artisanale sera plus faible que celui obtenu par son équivalent commercialisé.

Vous trouverez ici des liens pour la fabrication d'antennes :
http://www.nantes-wireless.org/index.php?page=materiel/antennes

(Fa / Pr / Ri)

5.2.3.1- Antenne Ricoré

Après avoir visité de nombreuses pages sur la construction d'antennes, je me suis dit qu'il fallait passer à l'acte et je vais tâcher de détailler davantage la construction. Ne sous-estimez pas la précision des mesures à faire, elles déterminent l'efficacité de l'antenne.

PHASE 1 : Calcul et Dimensionnement

Une boite de ricoré à un diamètre intérieur de 9.9mm, sa longueur ne nous intéresse pas trop en fait, tant pis de toute facon elle n'a pas la longueur idéale. J'ai pris la bande de fréquence suivante pour mon calcul :

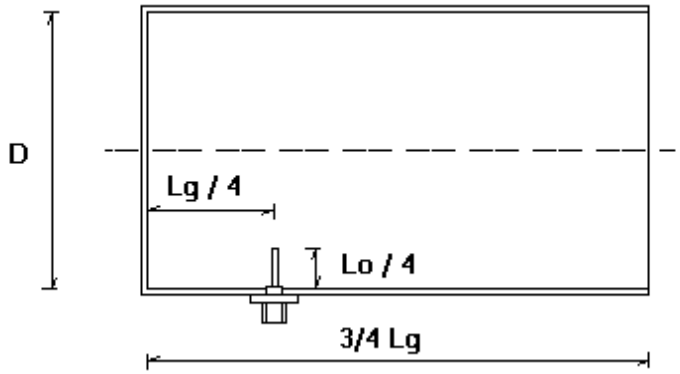
mini : 2.412 ghz (canal 1) maxi : 2.472 ghz (canal 13) moyenne : 2.43 ghz (environ canal 7)

Jusque là ca doit aller, c'était la partie intellectuelle.
Ensuite à l'aide du calculateur http://www.saunalahti.fi/elepal/antenna2calc.php

Vous rentrez les valeurs trouvées précédemment, et si tout se passe bien nous obtenons :

Results:
Lo = 123 mm
Lo/4 = 31 mm
Lg = 181 mm
Lg/4 = 45 mm

Je vous renvoie à cette image pour la compréhension



31 mm désigne la longueur du fil de cuivre qui doit dépasser (être visible), 45 mm désigne la longueur à partir de laquelle vous devrez percer un trou, en partant du fond de la boite jusqu'au couvercle.

PHASE 2 : Matériel et Perçage

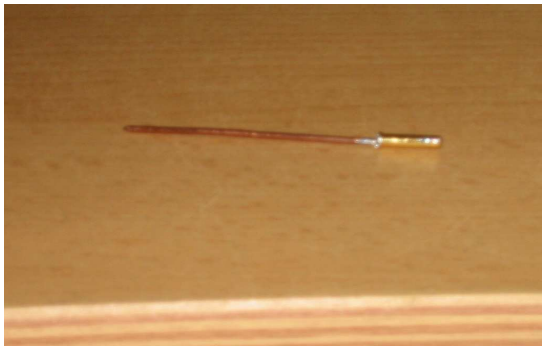
Vous aurez certainement besoin du matériel suivant :

- une perceuse
- un forêt à métal du diamètre de votre connecteur (16mm pour moi)
- un connecteur N femelle diam 16mm
- la boite de ricoré évidemment

Ne vous inquiétez pas si vous posez la pointe du fôret sur le point à 45mm vous êtes sur que ca va marcher. Ensuite il faut souder l'âme du connecteur N à votre fil de cuivre.

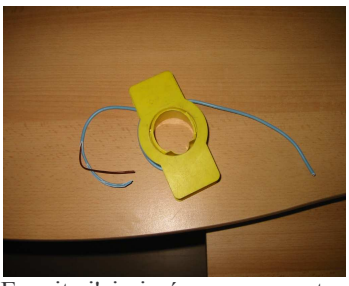
Pour dimensionner votre fil de cuivre, il faut que vous calculiez, de facon à ne faire sortir que 31mm de fil, quelle longueur le fil doit avoir pour buter dans l'âme. Chez moi il faisait :
4 (butée dans l'âme) + 24 (pour aller jusqu'à la boite) + 31 (longueur à faire sortir) soit un total de 59mm

Le fil est soudé à l'âme du connecteur :



J'ai utilisé du fil de cuivre qu'on utilise en électricité pour relier les douilles de lampe au courant, il semble avoir un bon diamètre et n'est ni trop maléable, ni trop rigide. Une simple soudure à l'étain fonctionne parfaitement.

Le fil utilisé :



Ensuite j'ai vissé mon connecteur N, en faisant bien attention qu'il soit en contact avec l'intérieur de la boite, vu que l'extérieur est peint ca ne conduit pas.

L'antenne ricoré à côté d'une règle pour estimer sa dimension :

L'intérieur avec le connecteur N qui fait masse, et le bout de fil qui sort :

Une autre vue de l'antenne en position verticale :

PHASE 3 : Les tests

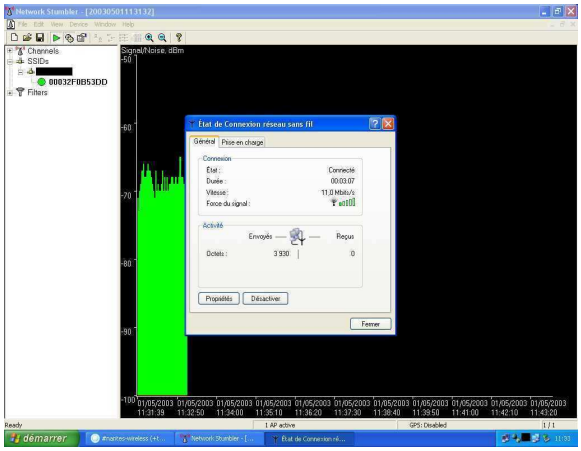
Si déjà vous n'avez pas abîmé quoi que ce soit jusqu'ici c'est bien, mais maintenant voyons si vos efforts sont récompensés, ce qui sera mieux.

Déjà en branchant votre antenne si votre gain dépasse les -100 dbm, vous pouvez le voir

sous netstumbler, mieux vaut remettre l'antenne de base, ca marchera mieux avec.

En revanche si vous avez un gain acceptable, essayez de la tester en pointant sur un voisin par exemple. Alors on voit pas que recois des paquets mais après ca marche, je recois et tout. j'ai même pu aller sur internet avec sa connexion internet, il a un routeur/modem ou ap smc visiblement.

Je suis à une distance de 50m, l'antenne est chez moi dans mon bureau, son ap n'a pas d'antenne avec gain, bref tout se fait à travers les murs. Donc si j'ai faible signal c'est peut etre du à son côté. Pour que vous puissiez établir une connexion sans fil, il faut débasser 70 dbM pendant quelques secondes, ensuite si ca diminue un peu (débit, dbM), c'est pas grave, mais faut pouvoir établir la liaison avant tout. Tout du moins c'est ce que j'ai pu constater avec mon matériel.



Un petit ping la dessus nous donne les résultats suivants :

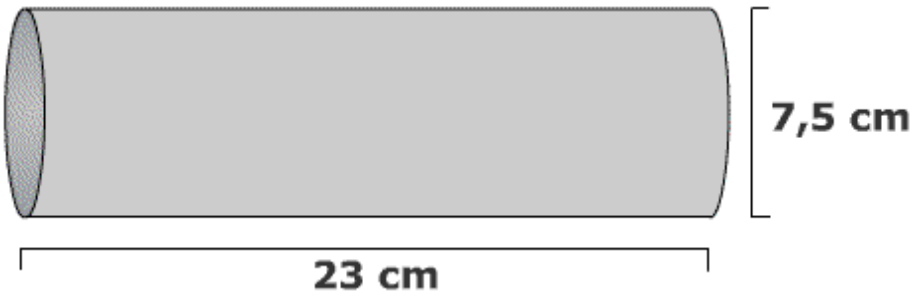
```
Envoi d'une requête 'ping' sur 192.168.2.1 avec 32 octets de données :

Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 192.168.2.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
```

Ca promet de belles parties de counter-strike. Je vais tâcher de joindre quelques photos d'ici là bon courage. Je vais me mettre à la construction d'une AntenneBiQuad et dès que c'est terminé je mettrais une page aussi pour raconter sa construction et mettre quelques tests

(Ri)

5.2.3.2- Antenne Pringles

1) La Structure :



Il y a quelques mois, il y a une question que je me posais :
Les boites pringles américaines ont elles la même matières que nos boites de Pringles

Européennes ?

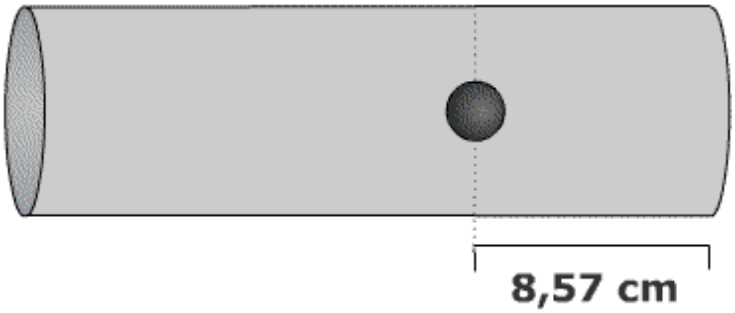
D'après un ami américain, il semble que oui ...

Vérification de la matière de la boîte, ça ressemble à de l'aluminium collé sur du carton à priori. C'est bien ça .. C'est bien un metal conducteur qui entoure l'intérieur de la boîte de Pringles.

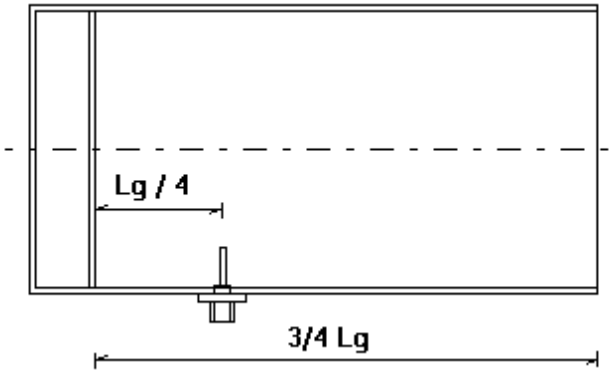
2) Les calculs :
Pour le canal 11 (2.462 GHz) :
W = (299792458 / 2462) * 10^-4
W = 12.18 cm
1/4W = 3.04 cm

Le quart de la longueur d'onde est donc de 3.04 cm.

3) Perçage de la boite
D'après l'article du site d'Oreilly, ils préconisent de percer la boite à 3 3/8" (soit 8.57 cm) à partir du bas.



Utilisons cet outil : http://www.saunalahti.fi/elepal/antenna2calc.php



source : http://www.saunalahti.fi/elepal/antenna2.html

8.57 cm correspond donc en fait à un diamètre de 76.5mm et une fréquence de 2.457Ghz (canal 10).
Mais après vérification, on s'apperçoit que le diamètre des boîtes de Pringles Européenes fait plutôt 75 mm.
Si on insere 2.462 GHz comme fréquence et 75 mm de diamètre on obtient :

Lo = 122 mm
Lo/4 = 30 mm
Lg = 399 mm
Lg/4 = 100 mm

Il faut donc perser un trou à 10 cm du bas si on veut utiliser le canal 11.
Conclusion :

La longueur du tube joue t'elle dans les calculs ? Si oui il va falloir diminuer la taille du tube.

Références :
http://www.oreillynet.com/cs/weblog/view/wlg/448
http://reseaucitoyen.be/index.php?HomeMade
http://www.turnpoint.net/wireless/has.html
http://me.jeremiahwhite.com/pringles.html
http://www.arwain.net/evan/pringles.htm
http://www.netscum.com/clapp/wireless.html
http://www.seattlewireless.net/index.cgi/DirectionalWaveguide

(Pr)

5.3- La connectique

5.3.1- Les câbles

Il existe une importante variété de câbles, chacun ayant ses spécificités techniques.

Lors de l'achat de votre câble, vérifiez sa fréquence maximale de fonctionnement ainsi que ses pertes au mètre.

Un PigTail est généralement long de 30 cm à 2 m, voir jusqu'à 4 m dans certains cas. Les pertes occasionnées par le câble coaxial sont largement compensées par le gain des antennes utilisées.

Il peut être intéressant de noter que généralement plus le câble est gros et rigide plus ses pertes seront faibles.

Certains connecteurs ne peuvent pas s'adapter à tous les câbles :

Les connecteurs MMCX ou Lucent ne se trouvent que pour du coaxial 3 mm

Les BNC, TNC, N, SMA s'utiliseront sur des 6 mm (RG58), ou sur des 10,3 mm (Aircom +). Les SMA et BNC existent également pour du 3 mm.

Certains modèles sur des sections plus importantes, via des connecteurs adaptés, c'est le cas par exemple de l'Aircom +, un câble à très faibles pertes, avec âme (le conducteur interne) monobrin semi rigide, un diélectrique (le composant "plastique" entourant l'âme) semi aéré pour plus de souplesse.

Plusieurs câbles coaxiaux sont employés en WiFi :

RG58 CU : à ne surtout pas confondre avec le RG58, un câble en cuivre rouge, inutilisable au delà de 1 GHz. Le RG58CU est lui donné jusqu'à 3 GHz, avec des pertes de 0,825 dB/m sur 2,4 GHz. Diamètre extérieur : 4,85 mm

RG174 : coaxial 3 mm (2.60 mm exactement), pertes de 1,445 dB/m, réservé aux très petits connecteurs (MCX, MMCX, Lucent, etc.)

Aircom + : coaxial de 10,30 mm, pertes de 0,215 dB/m, sans doute le plus performant de tous les câbles coaxiaux de ce diamètre, et le meilleur rapport qualité prix du marché pour des installations de grandes longueurs.

LMR195 : coaxial 4,95 mm, compatible RG58CU, pertes de 0,595 dB/m, âme monobrin. Un coaxial performant mais hélas hors de prix comparé à de l'Aircom +, techniquement plus cohérent et plus abordable.

LMR400 : coaxial 10,30 mm, pertes 0,222 dB/m, là encore un coaxial performant mais inabordable pour le grand public.

Les coaxiaux et connecteurs pour LMR sont visibles sur

http://www.timesmicrowave.com/telecom/wireless/
Les coaxiaux et connecteurs pour RG58CU, RG174 / RG316, Aircom + sont visibles sur http://online.infracom.fr

5.3.1.1 RG 58 CU

Ce type de câblage à une perte de 0,82 dB/m mais est principalement utilisé pour les réseaux Ethernet (BNC). Il est utilisable en WiFi (fréquence max. 3 GHz). A ne pas confondre avec le RG58 ordinaire, en cuivre rouge, utilisable lui jusqu'à 1 GHz uniquement.

Le RG58CU a des pertes de 82.37 dB/100 m Impédance : 50 Ohms

(Source : www.vanoostvoorn.nl)

Pigtail utilisant du câble RG58 CU:

(Fl)

5.3.1.2- RG 174

Câble destiné aux connecteurs miniatures

Diamètre :2,60 mm
Atténuation : 144,50 dB / 100 m
Impédance : 50 Ohms
Masse : 11 kg / km

C'est le câble généralement utilisé pour ce type de pigtails:

Réservé aux très petits connecteurs (MCX, MMCX, Lucent, etc.) et donc à éviter au delà d'un mètre de longueur.

(Fl)

5.3.1.3- RG 213

Câble très courant en communications radio, perte de 0,66 dB.

Perte : 41,66 db / 100 m
Diametre : 10.3 mm
Masse : 155,0 grammes / mètre

Blindage : Simple tresse

Le même câble avec un blindage double tresse : RG214

(Fl)

5.3.1.4- RG 214

Identique au RG213 mais avec un blindage double tresse

Diametre : 10.8 mm
Perte : 41,50 db / 100 metres
Masse : 195,0 grammes / metre
Blindage : Double tresse

(Fl)

5.3.1.5- LMR 400

Un câble coaxial très performant mais hélas trop coûteux pour les applications grand public.

Perte : 0,222 dB par mètre
Masse : 0.10 kg/m
Impédance : 50 Ohms
Diamètre externe : 10.29 mm

http://www.timesmicrowave.com/telecom/wireless/

(Fl)

5.3.1.6- Aircom

Câble coaxial ayant d'excellentes propriétés :

Perte : 21.5 dB / 100 m
Impédance : 50 Ohms
Diamètre externe : 10.3 mm
Diamètre de l'âme du conducteur : 2.8 mm
Masse : 15 kg / 100 m

Avec seulement 21,5 dB de perte aux 100 m sur 2,4 GHz, l'Aircom + est sans hésiter l'un des meilleurs câbles coaxiaux de sa catégorie, avec un rapport qualité prix le plaçant en tête des câbles concurrents. Il nécessite des connecteurs spéciaux. A ce jour sont facilement trouvables les N, RP TNC, RP SMA.

(Fl)

5.3.1.7- Aircell

Câble coaxial dit hautement flexible

Perte : 0,38 dB / mètre
Impédance : 50 Ohms
Diamètre extérieur : 7.30mm
Masse : 7.2 kg / 100 m

http://www.wimo.de/download/aircell.pdf

(Fl)

5.3.2- Les connecteurs

Il existe de très nombreux connecteurs différents (plusieurs centaines) en fonction du type d'antenne et du type de matériel informatique.
Il y en a 7 principaux :

- N
- SMA
- BNC
- TNC
- MCX
- MMCX
- Lucent

Chacun de ces types ayant des variantes (polarité inversée (RP), filetage à gauche, à droite, mâle, femelle, ...) plus des adaptateurs pour passer de N en SMA par exemple.

On identifie un connecteur, quel qu'il soit, en commençant par regarder son filtage :

EXTERNE, c'est une femelle.
S'il possède un trou, c'est un xx femelle, pas inversé du tout dans ce dernier cas.
S'il possède une pinoche, c'est un RP xx femelle.

INTERNE, c'est un mâle.
S'il possède un trou à l'intérieur, c'est un RP xx mâle, xx étant le type de connecteur (RP SMA mâle, RP TNC mâle, etc...).
S'il possède une pinoche, c'est alors un connecteur mâle ordinaire.

Connecteurs N mâle, RP TNC mâle, RP SMA mâle :

(Fl)

5.3.2.1- Type N

Les connecteurs N sont très souvent utilisés au niveau des antennes, la grosse majorité des antennes possèdent un connecteur de ce type.

Pour la réalisation d'une antenne "Pringles ®" ou "Ricoré" cette embase N femelle est généralement utilisée :

Voici un connecteur N mâle :

Il existe de nombreux adaptateurs pour connecteurs N, N vers TNC, N vers SMA, ...

Plus d'informations sur les connecteurs N et les adaptateurs
(Fl / Go)

5.3.2.2- Type SMA

Les connecteurs SMA, sont les connecteurs généralement rencontrés sur les cartes PCI et certaines antennes.

Connecteur SMA male:

Adaptateur SMA mâle -> SMA mâl

Antenne patch avec connecteur SMA :

(Fl / Go)

5.3.2.3- Type TNC

Deuxième par la taille après les connecteurs N, les connecteurs TNC sont généralement présents sur les Points d'accès, le Linksys Wap 11 par exemple possède un connecteur de type RP-TNC.

Ils ressemblent en quelque sorte à une version réduite des connecteurs N.

(Fl / Go)

5.3.2.4- Type MCX, MMCX, Lucent

Ces types de connecteurs sont principalement utilisés sur les cartes Wireless PCMCIA, ou Mini-PCI, le connecteur Lucent par exemple convient aux cartes Orinoco.

Connecteur MCX :

Connecteur MMCX :

(Fa / Go)

6- La sécurité

6.1- Analyse de la sécurité

1-Introduction

Nous traiterons ici de toute la sécurité environnant le protocole réseau 802.11b, car il est le plus répandu et le plus utilisé en ce moment, nous ne ferons qu'évoquer les protocoles à venir, tel que le 802.11i, bien plus puissant en terme de sécurité, car ce protocole tire la leçon de toutes les erreurs permettant une infiltration depuis un réseau 802.11b.

Lors de l'officialisation de la norme 802.11b par l'IEEE (Institute of Electrical and Electronics Engineers) peu de monde se préoccupait de ce genre de technologie, sa validation a donc été vite effectuée sans trop faire attention à la sécurité. Maintenant, cette norme est devenue une référence en matière de communication informatique sans fil, et son très faible niveau de sécurité se retrouve ici remis en cause, c'est pourquoi de nombreux cryptages et autres solutions techniques sont venus en aide au 802.11b. Par défaut la norme 802.11b dispose d'un cryptage nul, en option on dispose d'un cryptage, appelé WEP, pour « Wired Equivalent Privacy », ou « Intimité Équivalente à celle d'un câble ». De nos jours la plupart des intéressés considèrent le WEP comme un cryptage fiable, tout simplement car les constructeurs le qualifient tel quel, il est donc utilisé comme seul cryptage dans les entreprises, lors de conférences, par nous, particuliers, alors qu'il est prouvé qu'il fournit des performances bien médiocres face aux promesses d'intimité comparables à un réseau câblé.

Pour parer à ça on peut utiliser un renforcement au niveau même du cryptage, une modification du WEP ou bien une gestion différente de celui-ci ; la plupart de ces méthodes ne sont pas sûres non plus, certes à un niveau d'ouverture vers l'extérieur bien inférieur à une pseudo sécurité WEP. On distingue 3 générations de sécurité WiFi :

1ère :	Le WEP, basé sur le chiffrement RC4, a clé fixe
2nd :	Le WEP2, toujours basé sur le RC4 mais utilisant des clés dynamiques et un système poussé d'authentification de l'utilisateur.
3ème :	802.11i, principe de chiffrement WEP, mais RC4 remplacé par AES

1ère et 2nd sont compatibles entre elles, un access point disposant en option d'un cryptage WEP de niveau 1 pourra parfaitement fonctionner en utilisant un WEP de niveau 2 à clés dynamiques. La 3ème est matériellement incompatible avec les anciennes, cette dernière génération est encore en cours de validation actuellement et n'est donc pas publique.

2- Le cryptage WEP

2.1- Le cryptage même

Ce cryptage travaille avec l'algorithme RC4 pour chiffrer les données, le WEP utilise des clés de 64, 128 ou 256 bits (256, suivant les constructeurs). 24 bits de ces clés servent de vecteurs d'initialisation (IV : Initialisation Vector), la clé RC4 est donc minorée de 24 bits, le vecteur d'initialisation change à chaque trame, généralement incrémenté de 1. La clé n'est pas transmise lors des communications ... elle est secrète, mais elle est connue des deux côtés. Le vecteur d'initialisation IV est lui par contre transmis en clair dans une trame, il change à chaque trame.

Problèmes :

Le cryptage RC4 présente des faiblesses, avec une clé de 64 bits, la clé RC4 tombe à 40 bits car dans une trame il y a 24 bits servant de vecteur d'initialisation, un cryptage RC4 de 40bits est très facilement cassable par force brute, (du RC5 40 bits a été cassé en 3 heures avec un réseau de calcul distribué en 1997...) On dispose de 24 bits pour les vecteurs d'initialisation, or ces vecteurs sont incrémentés à chaque trame, il suffit d'écouter les communications pendant 2^24 = 16,8 millions de trames pour pouvoir réussir à identifier des données, car le vecteur est le même que 16,8 millions de trames avant et la clé est toujours la même, ça correspond à 4 ou 5 heures de communication. Ces deux problèmes permettent une capture et une analyse des données après avoir trouvé la clé RC4 utilisée : un attaquant potentiel est donc capable de voir des données cryptées, et ce librement, en pleine rue.

2.2- L'intégrité des données

Un système de contrôle de l'intégrité des trames est implémenté dans le WEP, le CRC32, mais ce système utilisé avec le WEP comporte une faille permettant la modification de la chaîne de vérification du paquet à comparer à la chaîne finale issue des données reçues, ce qui permet à un attaquant de faire passer ses informations pour des informations valides.

3- WEP2 ou 802.1x

Le standard 802.1x normalisé par l'IEEE pour sécuriser des transmissions à base de 802.11 se décline en deux sous parties importantes. Une gestion et une création dynamique des clés à utiliser avec le WEP du 802.11 et une authentification de l'utilisateur. L'utilisation du 802.1x pour sécuriser une connexion 802.11 ne nécessite pas de changer de matériel, il est implantable dans un réseau 802.11b. L'authentification par 802.1x se fait à l'aide de RADIUS (Remote Authentification Dial-In User Service), en utilisant un serveur RADIUS qui centralise les informations d'authentification des différents clients.

3.1- Clefs dynamiques

La mise en place de clés dynamiques effectuée par le WEP2 permet de contrer l'attaque qui consiste à « écouter » les communications afin de trouver 2 vecteurs d'initialisation identiques toutes les 16,8 millions de trames environ. Puisque cette écoute est à mettre en oeuvre durant 4 ou 5 heures, si les clés de chiffrement sont changées toutes les minutes, il n'est plus possible de trouver la même clé au bout de 16,8 millions de trames.

Infiltrer un réseau en attaquant ce système de clés dynamiques est à ce jour difficilement concevable ; seulement le système d'authentification comporte lui de sérieux problèmes.

3.2- L'authentification

Le 802.1x est extensible à souhait, au minimum l'authentification se fait par le biais du protocole EAP (Extensible Authentication Protocol) qui permettra un cryptage de l'authentification sur le serveur RADIUS, ensuite on peut y rajouter divers autres moyens et protocoles d'identification. Le 802.1x est faillible et l'EAP utilisé ici l'est aussi.

Il a été démontré, il y a déjà plus d'un an par deux chercheurs de l'université de Maryland, que l'authentification de l'utilisateur à l'aide du 802.1x basique présentait deux gros problèmes et n'est donc pas quelque chose de sûr (http://www.cs.umd.edu/waa/1x.pdf).

Ces deux gros problèmes sont que le système est fragile face à deux attaques bien connues de nos amis experts en sécurité informatique, « man in the middle » et « session hijacking ».Jusqu'alors ces attaques n'étaient misent en oeuvre que sur des réseaux physiques. Mais depuis plus d'un an tout réseau sans fil reposant sur un cryptage 802.1x est pénétrable.

L'attaque de type « man in the middle » consiste à se mettre au milieu comme son nom l'indique. L'attaquant mettant en oeuvre cette méthode se place entre un access point et un client et est en mesure de capturer tout le trafic passant entre ces deux points.

L'attaque de type « session hijacking » consiste à « hijacker » une connection, à la voler. Toujours sur le principe de l'access point et du client, l'attaquant fait fermer la connection au client en se faisant passer pour l'access point, en spoofant (usurpant) l'adresse MAC de cet access point. L'attaquant n'a plus qu'à utiliser l'adresse MAC du client qui a été hijacké et l'access point ne le refusera pas.

De nombreuses attaques de dénis de service (DoS : denial of service) sur le protocole EAP permettent aussi des actions nocives sur un access point, le faire crasher par exemple.

Nous parlerons certainement plus en détails dans le futur de tous les problèmes qui entourent le 802.1x dans un prochain article.

4- Ce qu'il y a de sûr

4.1- Tunneling

Pouvant être de différentes sortes, le tunneling est actuellement une des meilleures sécurités en matière de communication sans fil. Cette technologie travaille au niveau du protocole IP même, en amont de la couche matérielle cryptant par exemple avec le WEP.

Le tunnel de communication cryptée le plus utilisé en WiFi est certainement le standard IpSec, permettant la mise en place de réseaux privés virtuels (VPN ; Virtual Private Network). Un VPN s'installe de manière complètement transparente dans une infrastructure réseau, créant un réseau parallèle à fort niveau de cryptage, ce réseau parallèle crypté étant donc un tunnel.

On peut aussi utiliser des tunnels de cryptage propres à chaque protocole IP, par exemple pour les connexions d'administration à distance (telnet) ou des transferts de fichier (ftp), on utilise un tunnel SSH (Secure Shell) qui crypte à la volée la totalité des informations transitant entre les utilisateurs.

4.2- Authentification par portail Web

Lorsque l'utilisateur est connecté sur le réseau, il est filtré et bloqué au niveau TCP/IP tant qu'il n'a pas effectué l'authentification HTTP.

Pour ce faire il doit consulter un document en ligne, cette première requête HTTP est détectée et est remplacée par un système d'authentification demandant un nom d'utilisateur et un mot de passe. C'est la méthode employée par les fournisseurs d'accès à des réseaux sans fils.

Un outil tel que NoCatAuth permet une gestion d'un tel système, pouvant être allié à un serveur RADIUS disposant des informations utilisateurs et des autorisations.

Une sécurité de ce type permet de bloquer un attaquant une fois qu'il est introduit. On ne peut pas compter uniquement sur ça pour sécuriser tout un réseau, car lorsque seul le WEP est activé, les transactions sont donc facilement décryptables et un attaquant peut réussir à espionner un client en train d'autoriser une session avec son couple nom d'utilisateur / mot de passe.

5- A éviter et à savoir

Le SSID (Service Set Identifier) n'est en aucun cas une sécurité, c'est seulement le nom propre de votre réseau ; si un attaquant peut pénétrer votre réseau il arrivera facilement à obtenir le SSID. Optez pour un SSID qui ne veut rien dire pour ne pas tenter le client qui arriverait sur votre réseau par hasard, « potdeyaourt » sera tout de suite oublié, tandis qu'un SSID s'appelant « basededonneesclients » sera lui très vite retenu !!

Le filtrage par adresse MAC est maintenant très facilement contournable ; spoofer une adresse MAC est très simple à mettre en ?uvre, même sous plateforme Windows, en utilisant par exemple un outil tel que SMAC (http://www.klcconsulting.net/smac), filtrer les adresses MAC de ses clients reste quand même une sécurité à ajouter à la liste des bases à activer dans le cas de clients fixes.

6- Conclusion

Un simple cryptage WEP doit absolument être utilisé en complément d'un ou plusieurs autres systèmes.

Le réseau sans fil doit être protégé par une machine de type firewall du réseau câblé lequel pouvant être utilisé pour transiter ou stocker des informations sensibles du fait de sa sécurité importante lors des transactions. Il ne faut en aucun cas utiliser le 802.11b pour transiter ou stocker des données sensibles.

On attend avec impatience le 802.11i, en espérant que l'IEEE aura pris le temps de bien analyser la chose avant de la valider. Car les faiblesses du 802.11b ont fait naître une multitude de systèmes de cryptage, se rajoutant au WEP, propre à chaque fabriquant de matériel 802.11b, engendrant ainsi une certaine incompatibilité lorsque plusieurs marques sont employées.

(Le)

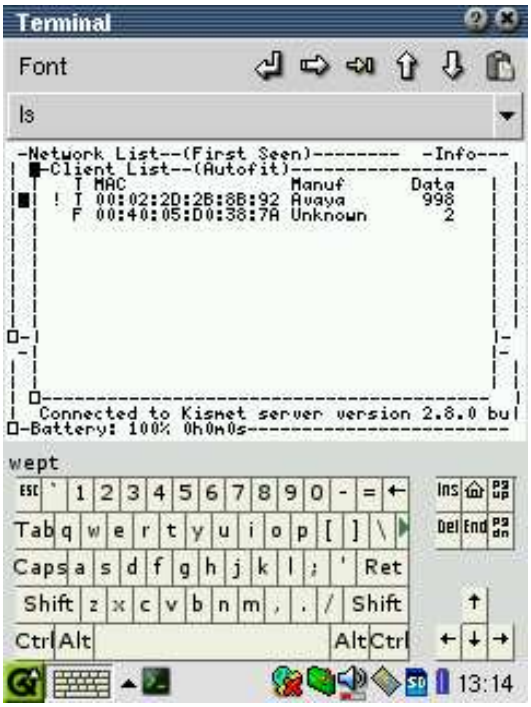
6.2 Les différents moyens matériels

6.2.1- Le filtrage par adresses MAC

Le filtrage par adresse MAC

Le filtrage par adresse mac est une fonctionnalité de sécurité que l'on trouve dans certains point d'accès. Cette fonctionnalité permet d'exclure ou de tolérer que certaines adresses mac dans le réseau. Une adresse mac est en fait un identifiant unique pour chaque carte réseau. Donc ce système permet de contrôler quelles cartes réseau peut rentrer sur le réseau. Dans le meilleur des mondes ce système aurait permis une grande sécurité malheureusement le protocole 802.11b n'encrypte pas les trames ou apparaissent ces adresses MAC. Un logiciel sniffer comme kismet permet de voir les adresses mac des clients et comme il existe des outils ou des commandes pour modifier son adresse mac et ainsi singer celle d'un client, le réseau devient ainsi une passoire.

Voici un screenshot du logiciel sniffer kismet sur un pda zaurus de chez sharp



En conclusion, le filtrage par adresse mac associé au WEP fera fuir les pirates pressés vers des bornes totalement ouvertes comme il y en a beaucoup mais ce système ne suffira pas contre un pirate motivé ayant du temps et quelques compétences.

(Ma)

6.2.2- Le WEP

WEP signifie "Wired Equivalent Privacy".
Norme de cryptage implémenté dans la norme IEEE 802.11b (Wi-Fi)

Une importante question que l'on peut se poser lorsque l'on met en place un réseau sans fil, est :
Quelle est la sécurité d'un tel système ?

Tant que le réseau est câblé peu d'inquiétudes surgissent, mais dès que celui-ci passe par les airs une certaine anxiété arrive. Après tout généralement on peut mieux surveiller quelque chose d'observable. Le standard définit un mécanisme par lequel le WEP peut être atteint. Celle ci correspond à une encryptage 40 bits RC4.

Si le WEP est mise en oeuvre alors toutes les données transmises sont encryptées. Toutefois une étude de l'université de Californie à Berkeley a démontré qu'il existait une faille de sécurité pouvant compromettre la confidentialité de données transmise sur le WLAN. Cette faille est facilement exploitable grâce à des logiciels comme WEPCrack fonctionnant sous Linux et qui permettent de casser des clefs WEP en 3 heures.

De toute façon si l'importance des données transmises le requiert des mesures supplémentaire d'authentification et d'encryptage des données doivent être prises (ex : VPN). Une norme supérieure d'encodage des données au nom de WEPA est en train d'être mise en place pour remédier à ce problème.

Le chiffrement peut être de : 64 bits, 128 bits, voir même avec divers normes propriétaires 256 bits.

Les clés peuvent être :

Statiques : elles sont insérées manuellement dans la configuration des cartes et des AP.

Dynamiques : elles sont gérées dynamiquement par les AP grâce à un système de rotation de clef.

L'utilisation du WEP réduit de beaucoup le débit de la connexion.

6.2.3- La gestion dynamique des clefs WEP

La gestion dynamique des clefs WEP est une technique permettant de résoudre le problème de sécurité du WEP.
Ce mécanisme génère des clefs WEP à intervalles réguliers : 1 min, 5 min, 10 min etc...
Ce qui rend impossible le piratage des données.

Pour qu'un pirate puisse casser une clef WEP, il faut que celui-ci 'sniffe' assez de données.
Si votre connexion change de clef toutes les 5 minutes, le pirate ne pourra 'sniffer' que 5 minutes de données encryptées, ce qui n'est pas assez suffisant pour qu'il puisse casser la clef d'encryptage.

(Pr)

6.2.4- Le 802.1x

IEEE 802.1x : Port Based Network Access Control

Cette norme permet aux points d'accès WiFi et au matériel réseau gérant le 802.1x de pouvoir authentifier ses clients grâce à un serveur Radius.
L'authentification est basée sur le protocole EAP (PPP Extensible Authentication Protocol) qui est une extension du protocole PPP.

EAP contient une douzaine de méthodes d'authentification, par mis elles, voici les plus connues :

- MD5
- TLS (développé par Cisco et MicroSuck)
- TTLS
- PEAP

Voici un document intéressant sur ces méthodes :
http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html

MD5 :
EAP-MD5 est reconnu comme étant facilement piratable.
Pour avoir plus d'infos sur EAP-MD5 :
http://www.freeradius.org/doc/EAP-MD5.html

TLS :

Clients :	Cisco, Funk, Meetinghouse, MicroSuck, Open1x (open source)
Plateformes :	Linux, Mac OS X, Windows 95/98/ME, Windows NT/2000/XP
Serveurs Radius :	Cisco, Funk, HP, FreeRADIUS (open source), Meetinghouse, MicroSuck

Cette méthode d'authentification est basée sur des certificats à installer sur chaque client. Celle-ci est relativement lourde à mettre en place au niveau de la gestion des utilisateurs et des certificats. Cependant celle-ci à le net avantage d'être implantée directement dans Windows XP et avec un patch dans Windows 2000, de plus il existe des clients pour les autres systèmes :

- XSupplicant (Linux)

- FUNK Odyssey (Win95, 98, 2K)
- Meetinghouse(Win95, 98, 2K)

Pour utiliser EAP-TLS vous devez pour cela avoir un serveur RADIUS supportant ce protocole.
FreeRadius supporte depuis peu EAP-TLS.
Pour avoir plus d'infos sur EAP-TLS :

http://www.freeradius.org/doc/EAPTLS.pdf
http://www.impossiblereflex.com/8021x/eap-tls-HOWTO.htm
http://www.koumoula.com/wifi/eap-tls/eap-tls.htm

TTLS :

Clients :	Funk, Meetinghouse
Plateformes :	Linux, Mac OS X, Windows 95/98/ME, Windows NT/2000/XP
Serveurs Radius :	Funk, Meetinghouse

Cette méthode est plus classique que TLS, celle-ci est basée sur l'envoie d'un identifiant et d'un mot de passe au serveur Radius. Malheureusement, TTLS n'est pas encore implémenté dans FreeRadius.

(Pr)

6.2.5- FreeRadius

FreeRadius est un serveur d'authentification Radius (Remote Authentification Dial-In User Server).
FreeRadius est sous LicenceGPL et est librement téléchargeable ICI.
Pour comprendre le fonctionnement d'un serveur Radius voici une petite explication :

Principe de fonctionement :

RADIUS (Remote Anthentification Dial-In User Service) est un système client/serveur qui permet de sécuriser des réseaux contre des accès à distance non authorisés.

Fonctionnalité du protocole RADIUS :

- Le protocole RADIUS fonctionne selon un modèle client/serveur.

- Un NAS (Network Access Server) (routeur, vpn serveur, serveur NT, etc ...) fonctionne comme un client RADIUS. Un client effectue des requètes RADIUS et agit en fonctions des réponses reçues.

- Un serveur RADIUS peut agir en tant que proxy RADIUS pour d'auter serveures RADIUS, ainsi que pour d'autres systèmes d'authentification (LDAP, SQL serveur, ...)

- Toutes les transactions RADIUS sont authentifiées par l'utilisation d'un secret qui n'est jamais transmis sur le réseau. De plus les mots de passe sont encryptés en utilisant cette même clé secrete.

Exemple d'authentification :

- Un NAS reçoit une requète pour une connexion à distance (via Internet ou entre réseaux LAN/MAN/WAN), il envoi une demande d'anthentification au serveur RADIUS. Si l'utilisateur est accepté, le serveur RADIUS authorise et détermine les services auxquels l'utilisateurs pourra accéder ainsi que les paramètres de connexion.

En détails :

- L'utilisateur entre le login et password.
- Le login et password sont encrypté et envoyé sur le

réseau au serveur RADIUS, l'utilisateur reçoit alors l'une des réponses suivante :

- ACCEPT - l'utilisateur est authentifié.
- REJECT - l'utilisateur est refusé.
- CHALLENGE - l'utilisateur reçoit uen requète par le serveur RADIUS pour recevoir des informations supplémentaires.
- CHANGE PASSWORD - une requète est envoyé par le serveur RADIUS à l'utilisateur pour que ce dernier change sont mot de passe.

Remarque : Le protocole RADIUS est uniquement utilisé pour les authentifications d'utilisateurs, une fois l'authentification effectuée, son travail est terminé.

(To)

FreeRadius implémente:

- EAP-MD5
- EAP-TLS

FreeRadius supporte :

- MySQL
- Oracle
- IBM DB2
- Sybase
- Kerberos
- PAM
- MPPE
- Python
- ...
- PostgreSQL
- IODBC
- MS-SQL
- LDAP
- EAP
- MS-CHAP
- Digest authentication
- X9.9

Voici une doc d'installation : http://earxtacy.free.fr/doc/radius.pdf
Pour plus d'informations sur FreeRadius :
http://www.freeradius.org
http://freshmeat.net/projects/freeradius/

(Pr)

6.3- Les différents moyens logiciels

6.3.1- NoCatAuth

NoCatAuth est un système d'authentification utilisé au niveau de la passerelle Internet. (http://www.nocat.net)
Celui-ci est une bonne alternative voir même un bon complément au 802.1x EAP-TLS dans le cas d'un partage Internet.
NoCatAuth permet de restreindre l'accès à Internet grâce à un système d'authentification centralisé.

Quand un client lance son navigateur, la passerelle du réseau sans fil le redirige directement vers la page Web du serveur d'authentification.
Tant que le client ne s'est pas authentifié, celui-ci n'a accès à aucune ressource sur Internet sauf celles que l'administrateur de la passerelle a autorisées.
La passerelle gère ses règles de pare-feu dynamiquement en fonction du niveau d'authentification du client.
L'authentification est basée sur l'adresse MAC du client.

NoCatAuth gère plusieurs modes d'authentification : Radius, MySQL, Shadow Passwd ...

NoCatAuth est sous licence GPL et fonctionne sous Linux.

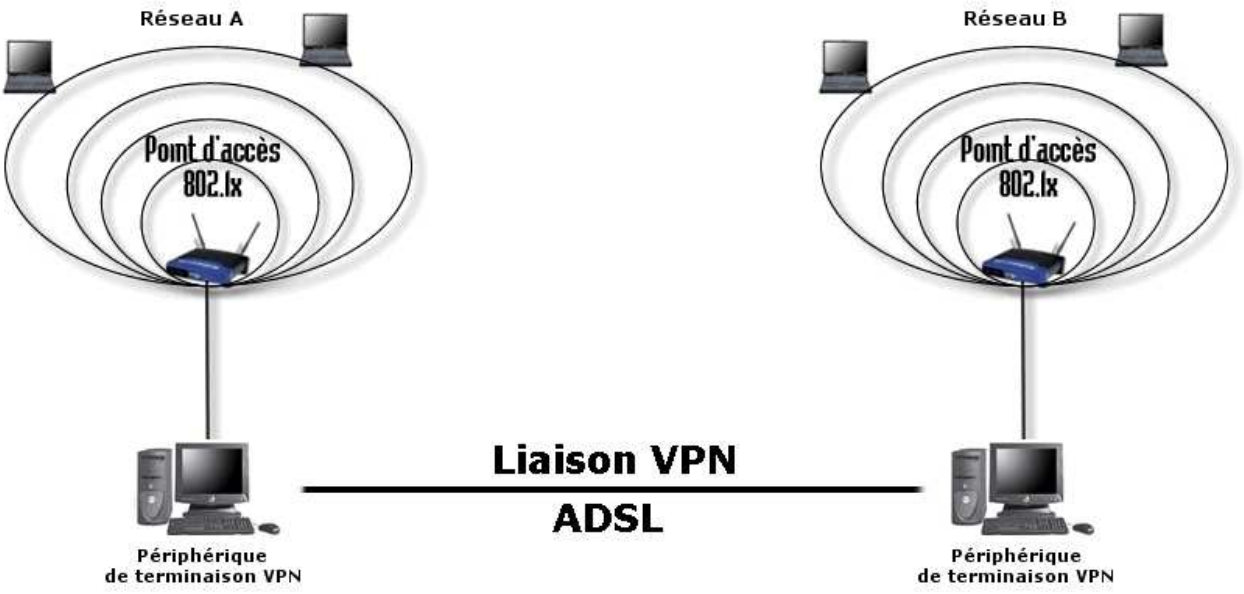
Pour plus d'infos :
http://www.nocat.net

http://www.labo-wireless.com/articles.php?id=14
http://www.nantes-wireless.org/index.php?page=doc/nocatauth
http://cterix.free.fr/Reseau/NoCatAuth
http://www.traduc.org/docs/HOWTO/lecture/Authentication-Gateway-HOWTO.html
(Pr)

6.3.2- Les VPNs

VPN : "Virtual Private Network" = Réseaux Privés Virtuels

Principe du VPN :



Les 2 réseaux A et B peuvent communiquer de façon transparente grâce à la liaison VPN.
Les passerelles VPN permettent de créer ces réseaux de manière transparente pour les réseaux existants.
Le standard IPSec (normalisé par l'IETF) permet la création de réseaux privés virtuels. Toutes les communications sont chiffrées et toutes les connexions authentifiées (secret partagé ou certificat X509).
Une alternative aux liaisons spécialisées:
Une application courante des VPN est de relier différents sites par l'intermédiaire d'Internet. Ces solutions sont nettement moins onéreuses que les liaisons spécialisées qu'elles remplacent donc souvent avantageusement.

Une solution pour les travailleurs mobiles:
Les VPNs peuvent permettre aux travailleurs nomades d'accéder par Internet aux ressources de l'entreprise de manière sécurisée (authentification et confidentialité).

Tiré de : http://www.idealx.com/solutions/vpn.fr.html
(Go)

6.3.3- PPP, PPTP, L2PT

PPP (Point to Point Protocol) est un mécanisme qui permet de faire fonctionner IP (Internet Procotol) et tous les autres protocoles réseaux à travers une liaison série - qui peut être une connexion série directe (avec un câble null-modem), à travers une liaison par un telnet, ou encore une liaison utilisant les modems et les lignes téléphoniques (et bien sûr utilisant les lignes numériques comme RNIS).

Tiré de : http://www.freenix.fr/unix/linux/HOWTO/PPP-HOWTO-1.html

Point-to-Point Tunneling Protocol
Le protocole PPTP a été la première offre VPN de Microsoft pour ses OS 32 bits.
En plus du support IPX/SPX et de NetBEUI, PPTP fournit un mécanisme de communication sécurisé au-dessus de TCP/IP.

Layer 2 Tunneling Protocol
PPTP constitue une solution VPN robuste qui n'a malheureusement pas été largement acceptée par les institutionnels des réseaux informatiques.
Le standard de l'industrie est le protocole L2TP, défini par la RFC 2661.

Le protocole PPTP supporte les protocoles NetBEUI et IPX/SPX uniquement alors que L2TP ne supporte pas de protocole réseau spécifique,
Il peut s'interfacer avec n'importe quel protocole réseau car il offre des fonctionnalités définies au niveau de la couche Liaison de donnée connu aussi sous le nom de "Data Link" (Niveau 2 du Modèle OSI).

(Go)

6.3.4- SSH

Le protocole SSH (Secure Shell) est un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisé :

Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau).
Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être.
Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

La version 1 du protocole (SSH1) proposée dès 1995 avait pour but de servir d'alternative aux sessions interactives (shells) telles que Telnet, rsh,
rlogin et rexec.
Ce protocole possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré.

C'est la raison pour laquelle en 1997 la version 2 du protocole (SSH2) a été proposée.
Secure Shell Version 2 propose également une solution de transfert de fichiers sécurisé (SFTP, Secure File Transfer Protocol).

SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée.
A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH.
Ce protocole permet des tunnels (liaison d'un à un point) cryptés comme le montre ce lien :

http://www.miscmag.com/articles/index.php3?page=105

(Go)

6.3.5- Tunnel SSH et Proxy

Un tunnel SSH permet de crypter les données entre deux points, un Proxy est un filtre entre le réseau privé et Internet qui permet de surfer. La combinaison des deux permet donc de façon magique de crypter les liaisons entre les clients et la passerelle et avec le Proxy de permettre aux données qui arrivent à la machine passerelle de faire des requêtes sur Internet et ainsi de surfer. Ainsi on a la bonne combinaison pour la confidentialité des données entre les clients et une passerelle avec un point d'accès sans fil. Il ne faut néanmoins pas oublier de fonction d'authentification (Proxy d'authentification, autpf sous OpenBSD ou toute autre système ayant cette fonction). Créer un tunnel sous linux ou BSD est assez simple

Quelques exemples ici :
http://www.miscmag.com/articles/index.php3?page=105

Il y aussi putty sous Windows pour cela :
http://www.chiark.greenend.org.uk/sgtatham/putty/

Un exemple un peu vieux du couplage de SSH et d'un Proxy (malheureusement un Proxy que pour le http) :
http://www.thismetalsky.org/magic/articles/wireless_security.html

Donc il y a beaucoup d'idées à tirer de cette solution.

(Ma)

6.3.6- IPsec

Extensions de sécurité au protocole Internet IPv4, requises pour l'IPv6.
Un protocole pour le chiffrement et l'authentification au niveau IP (hôte à hôte).
Contrairement au protocole SSL qui sécurise uniquement une Socket d'application, à SSH qui ne sécurise seulement qu'une session et à PGP qui sécurise uniquement un fichier spécifique ou un message,
IPSec chiffre toutes les communications entre deux hôtes.

(Go)

6.3.7- Authpf

C'est une application qui tourne sur le système OpenBSD (www.openbsd.org), authpf est donc le diminutif de authentification + pf, pf étant le Firewall d'OpenBSD.

Quel est son utilité ?

Toute personne qui se logge et s'authentifie avec SSH, le système détermine des règles de Firewall personnalisées à cette utilisateur connecté , tout ceci grâce à Authpf. Ce qui veut dire que par la gestion d'Autpf nous pouvons par exemple interdire ou autoriser un utilisateur à surfer si OpenBSD et Authpf sont sur la passerelle. C'est une sorte de gestion dynamique du Firewall, c'est donc un moyen efficace de sécuriser sa passerelle sans fil relié à Internet Ou tout autre réseau.

La page du manuel

Pour éviter le spoofing, je vous conseille d'ajouter ces deux lignes dans votre /etc/ssh/sshd_config:

```
ClientAliveInterval 15
ClientAliveCountMax 3
```

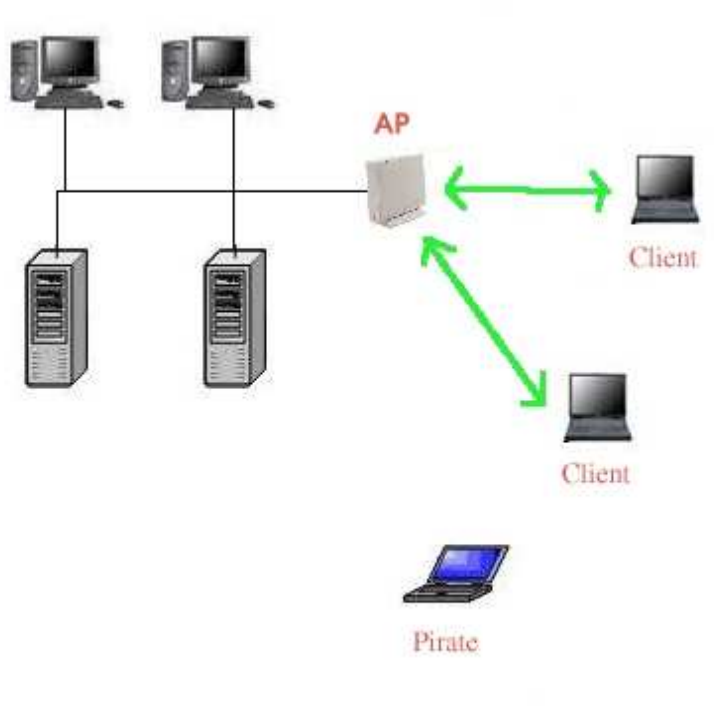
(Ma)

6.4- Les attaques possibles

6.4.1- Par usurpation

Usurpation d'adresse MAC

Tous les AP proposent le filtrage d'adresse MAC, ils donnent un sentiment de sécurité mais malheureusement l'adresse MAC peut être modifiée comme expliqué dans le chapitre précédent sur le filtrage par adresse mac.
Nous allons donc cette fois expliquer l'attaque par des schémas
En filtrant par adresse MAC en ne laissant que certaines adresses passer l'AP, vous limitez l'accès à juste quelques Scripts-kiddies de 6 ans ;).
Voila un exemple d'intrusion pour montrer la facilité de pénétrer ce type de protection :

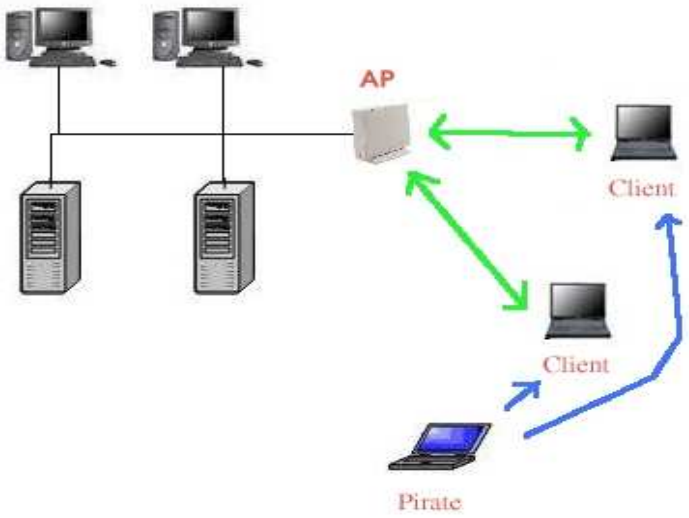


Voila situation :
Un réseau LAN ayant un point d'accès, des clients se connectent dessus, il y a juste un filtrage par adresse MAC.
Le pirate qui veut rentrer a besoin de :

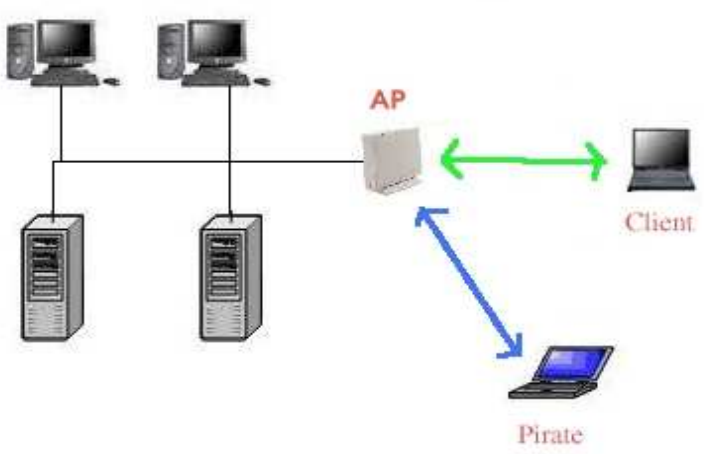
- Le SSID du réseau
- Une adresse MAC autorisée à rentrer.

Le pirate va d'abord scanner le réseau pour savoir le SSID. Avec un logiciel comme Kismet.
Ne sachant pas qu'il y a une protection il se verra refuser l'entrée.

Toujours avec son scanneur de réseaux, il va regarder les autres AP/Clients en marche, il en trouvera deux et il aura leurs adresses MAC d'inscrits:



Après qu'un client soit parti, le pirate va "spoofer" l'adresse MAC de sa carte avec l'adresse MAC du client partit. Il pourra se connecter au réseau et le client ne pourra plus se connecter tant que le pirate est connecté sur l'AP:



Usurpation d'un AP

Cette méthode de hack consiste à se faire passer pour un autre point d'accès (Rogue AP en anglais, l'AP sournois), petites explications :

Un client qui veut se connecter à un réseau met le SSID dans le client de configuration de la carte, Il se connectera a l'AP qui a ce SSID et aussi celui qui a le meilleurs signal.

Le problème est que l'AP qui a le même SSID et qui possède un meilleur niveau de signal que l'autre, sera choisi par le client et se connectera à lui.

Le pirate a donc trompé le client et peut lui faire subir les pires outrages informatiques.

Cette technique permet de :

- De bloquer l'accès à un réseau, il suffit d'une grosse antenne pour le faire (ou un amplificateur)
- De pirater les ordinateurs qui se connectent normalement au réseau d'origine.

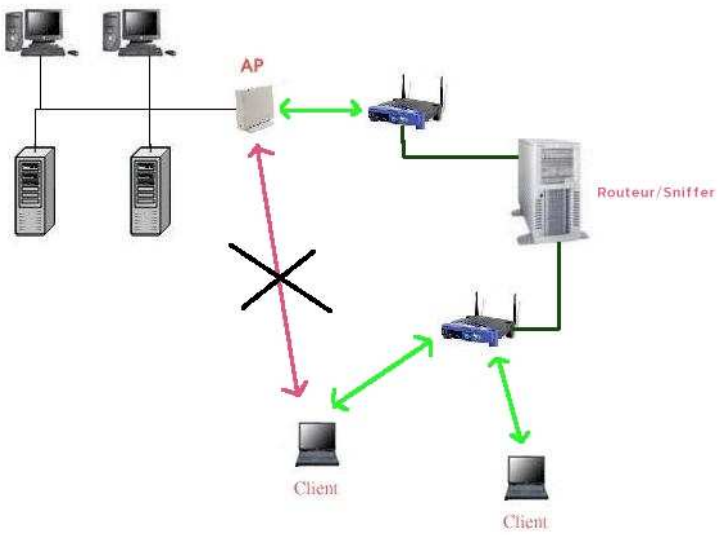
Pour contrer cette technique :

- Mettre un système d'authentification du type WEP, 802.1x, VPN,...
- De ne pas mettre l'option Broacast SSID dans l'AP, mais les logiciels de scan voient le SSID quand même.

Une technique plus évoluée (est l'attaque "de l'homme du milieu" ou man in the middle attaque) permet de sniffer énormément de clients :

Avec son AP où les clients se font pigeonner, le pirate va mettre une machine en supplément qui va avoir une carte Wifi qui sera configurée pour être connectée au réseau normal (on prend un réseau sans protection pour plus de simplicité).

Avec un soft de routage qui fonctionne avec un niveau bas, les clients se connecteront au faux AP, lui même connecté au client du pirate, tout le flux sera redirigé vers la carte Wifi qui sera connectée au réseau normal, cela permettra d'être transparent pour les clients et permettre de les sniffer.



Donc les clients ne peuvent pas se connecter au vrai AP car le faux AP a un meilleur signal. Les clients se connectent au faux AP. Le pirate a pris soit de prendre les bonnes classe IP, le routeur ou plutôt bridge redirige le flux des clients vers l'AP du haut. Le

bridge peut sniffer tout les paquets et donc trouver les mdp/login en clair.

Pour contrer cette attaque :

Mettre le filtrage par MAC qui ralentira le pirate (faut prendre que des cartes et les spoofer avec l'adresse MAC des clients). Mettre le WEP, le pirate ne le connaît pas mais pourra très bien le savoir avant de pirater juste en écoutant le réseau pendant quelques heures. Une des solutions acceptable est le 802.1X qui bloquera cette attaque si le pirate n'a pas le certificat.

(Da)

7- Configuration

7.1- SSID, BSSID, ESSID

Le SSID:
Service Set Identifier également appelé SSID .Il en existe plusieurs formes dont le BSSID (Basic SSID) et le ESSID (Extend SSID) .Ces deux appellations différencient leurs utilisations .Lorsque un client voudra s'assigner à un AP, il devra fournir cet identifiant.

Le BSSID:
Cette appellation désigne le SSID assigné à un point d'accès isolé.

Le ESSID:
Cette appellation désigne lorsque le SSID est le même pour tous les AP ainsi cela permet de pouvoir couvrir une plus grande zone avec le même réseau ainsi lorsque une personne se déplace entre des AP assignés avec le même SSID, il pourra toujours être connecté au même réseau.

(Ka)

7.2- Le WEP

WEP signifie "Wired Equivalent Privacy".
Norme de cryptage implémenté dans la norme IEEE 802.11b (Wi-Fi), voir plus haut.

7.3- Le DHCP

DHCP signifie Dynamic Host Configuration Protocol.

Cela veut donc dire qu'il n'y a rien à configurer coté client, un client une fois connecté au point d'accès reçoit automatiquement toutes les informations nécessaires à son bon fonctionnement (Proxy, Dns, ...). Il n'y a absolument aucune configuration à faire du coté client.

Faites donc attention si vous avez chez vous un point d'accès avec un serveur DHCP sans cryptage WEP, les intrusions seront grandement simplifiées.

Configuration

Notion de plages

Un plage d'adresse IP se configure depuis le serveur DHCP (votre point d'accès par exemple) permettra de déterminer le nombre de PC qui pourront se connecter à votre réseau et leurs adresses IP.

Une plage ressemblera à ça:
Adresse de départ : 192.168.1.20
Adresse de fin : 192.168.1.50
Le nombre maximal de PC recevant leurs paramètres par DHCP seront donc de 30 (50 - 20).

Notez que cela ne correspond en aucun cas au nombre maximum de PC pouvant se connecter à votre réseau mais seulement au nombre de PC recevant automatiquement leurs paramètres.

Notion d'exclusion

Le problème qui peux donc se poser est le suivant, vous désirez définir une grande plage d'adresses IP mais votre serveur principal qui lui à une adresse IP fixe (conseillé) se trouve en plein milieu de cette plage.

Les plages d'exclusions sont conçut pour ça.

Exemple :

Plage :
Adresse de départ : 192.168.1.10
Adresse de fin : 192.168.1.200
Adresse du serveur : 192.168.1.50

L'exclusion peut se configurer de 2 manières. Le plus souvent une plage d'exclusion nous aurons donc :

Exclusion :
Adresse de départ : 192.168.1.49
Adresse de fin : 192.168.1.51
(On prends un peu de marge, en effet 3 adresses seront bloquées (1.49, 1.50, 1.51) mais vous pouvez aussi marquer (192.168.1.50 - 192.168.1.50)

Certaines fois il n'est possible de ne rentrer que des adresses pour l'exclusion :
Adresse d'exclusion 1 : 192.168.1.50
Adresse d'exclusion 2: ...
etc...

DNS, Proxy, ...

Vous devez indiquez les paramètres que recevront les postes clients DHCP, référez vous à votre configuration réseau pour plus de détails.

(Fa)

8- Conclusion

Le Wireless est une technologie, qui commence à faire son apparition dans les entreprises depuis un peu plus de 2 ans, il devient de plus en plus courant d'en rencontrer, plus principalement dans les entreprises utilisant des ordinateurs portables ou dans les entreprises ne désirant pas investir dans du réseau filaire, bien que les performances soient légèrement moins bonnes.

Le débit du Wireless va augmenter, dans les prochaines années, les normes vont changer, il est aujourd'hui possible de trouver du Wireless utilisant la bande de fréquence des 5 Ghz, (norme 802.11a) bien que le débit est élevé (54 Mbits/s), la distance couverte est plus faible (du fait des phénomènes abordés plus haut).

Par contre, l'axe principal du développement de réseaux dans les prochaines années devra être la sécurité, en effet un réseau Wireless est la porte ouverte à toutes les tentatives de piratage, d'autant plus qu'il est quasi impossible de retrouver le responsable d'une telle tentative.

Le WEP (Wireless Encryption Protocol), qui permet de crypter les données transitant sur le réseau avec une sécurité allant jusqu'à 256 bits à l'heure actuelle, n'est pas fiable à 100%.

Il est donc important de considérer le réseau Wireless de la même manière qu'Internet, en le mettant derrière un Firewall, n'autorisant que les postes donc les adresses MAC ont étés déclarées préalablement par exemple.
Le Wireless est aussi étudié comme moyen de diffuser Internet en haut débit en zone rurale, le gouvernement propose un soutien financier aux personnes voulant développer un tel projet. (Fa)

9- Mise en pratique, tests

9.1- Théorie

9.1.1- Bilan de liaison

En fonction de ce que nous avons vu précédemment, il est possible d'établir un bilan de liaison pour une installation Wireless donnée.

Voilà la procédure à suivre pour réaliser un bilan de liaison :
- Calcul de l'atténuation de parcours
- Intégration des pertes dues aux câbles
- Intégration des gains des antennes en émission réception
- Intégration de la puissance d'émission
- Intégration des phénomènes évoqués plus haut (pour un calcul en condition réelles, très difficile à évaluer)

Exemple:
Nous souhaitons réaaliser une liaison Wireless sur une distance de 5km
Voici le matériel dont nous disposons:
2 Points d'accès Linksys WAP11 (puissance 100mW soit 20 dBm par AP)
2 antennes paraboles SD27 (gain 24 dB par antenne)
2 câbles AIRCOM de 2m (perte -0.43 dB par câble)
4 connecterus (perte -0,5 dB par connecteur)

Nota: Lorsque que l'on parle en dB, une valeur négative signifie de la perte, une valeur positive du gain.

Atténuation de parcours:
LP = 32,4 + 20 Log(2450) + 20 Log(5) ==> 2450: Fréquence en Mhz
==> 5: Distance en Km

LP = 114 dB

Puissance reçue:

Pr = Pt – Lp + Gt + Gr + Lt + Lr

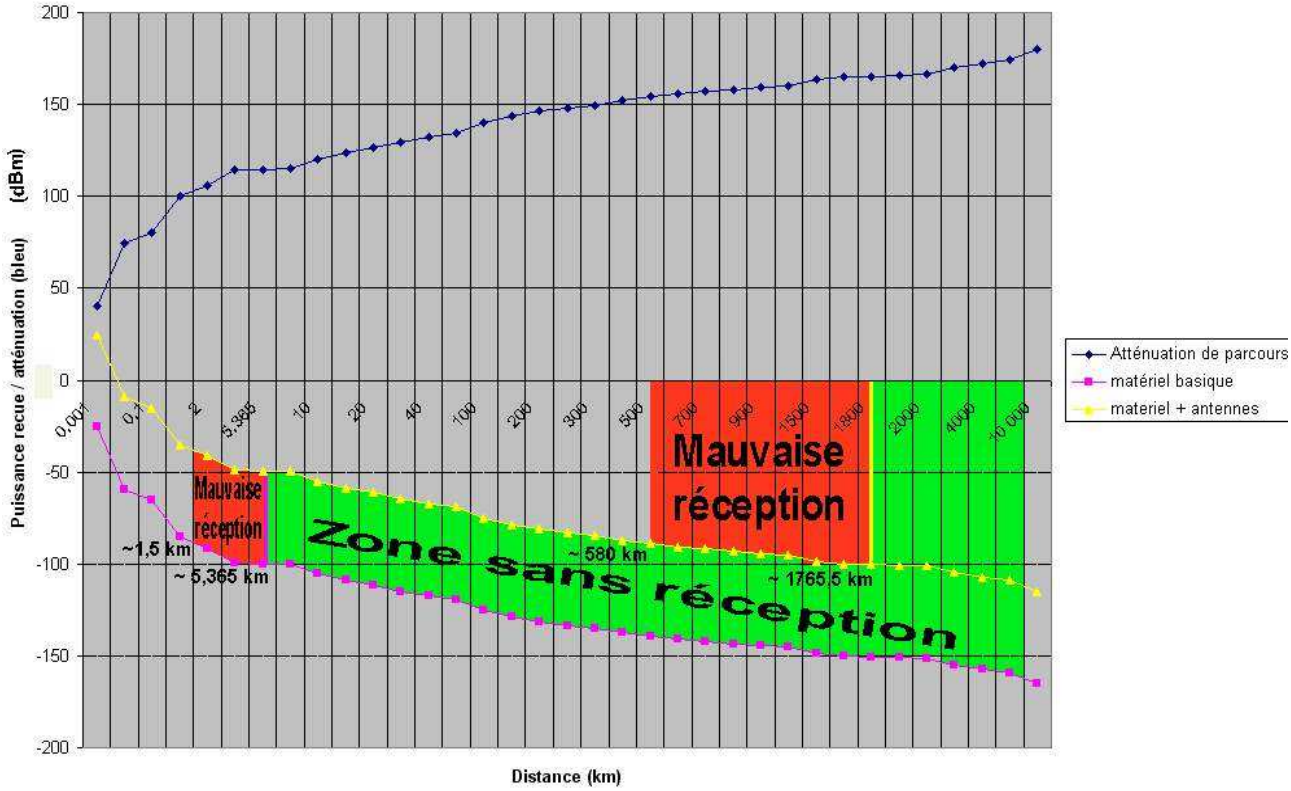
Pr ==> Puissance reçue (dBm ou dBw)
Pt ==> Puissance de l'emetteur en (dBm ou dBw)
Lp ==> Atténuation de parcours
Gt ==> Gain de l'antenne en emission (dBi)
Gr ==> Gain de l'antenne en reception (dBi)
Lt ==> Perte du cable coté emission (dB)
Lr ==> Perte du cable coté reception (dB)

Pr = 20 – 114 + 24 + 24 + (-0,43 – 1) + (-0,43 – 1)
Pr = -48,88 dBm

Il est important de noter que si le résultat est inférieur à – 100 dBm il n'est plus exploitable, dans la réalité, il vaut mieux ne pas aller en dessous de – 90 dBm

Nous pouvons en déduire 2 courbes:

- courbe pour du matériel basique (carte PCMCIA 30mW, pas d'antenne a gain) (violet)
- courbe pour l'exemple utilisé précédemment (jaune)



On peut donc déduire de ce graphique que la distance maximale exploitable en milieu parfait, sans obstacles est :

- pour du matériel de base : environ 1,5 Km
- avec des antennes : environ 580 Km

Evidemment ces résultats ne seront pas exacts dans notre atmosphère, il faut en effet rajouter tous les phénomènes évoqués dans la première partie, mais ils permettent de nous donner une idée des distances maximales, par exemple, on peut affirmer que sans antenne et avec des cartes wireless de 30mW, une liaison performante de plus de 2km est impossible à réaliser.

(Fa)

9.2- Installation

9.2.1- Installation détaillée d'un réseau avec Point d'Accès

1) Introduction

Cet article s'adresse à tout le monde, aucune connaissance technique n'est requise, les notions de réseau abordées seront détaillées pour une meilleure compréhension.

Le matériel qui va être utilisé pour cet article est le suivant :

- 1 carte Compact Flash DCF650W
- 1 carte PCMCIA Sitecom
- 1 AP Linksys BEFW11S4 (modèle routeur du WAP 11)

2) Installation du matériel

Tout d'abord installez les pilotes des cartes réseaux Wireless, ainsi que le logiciel généralement fourni.

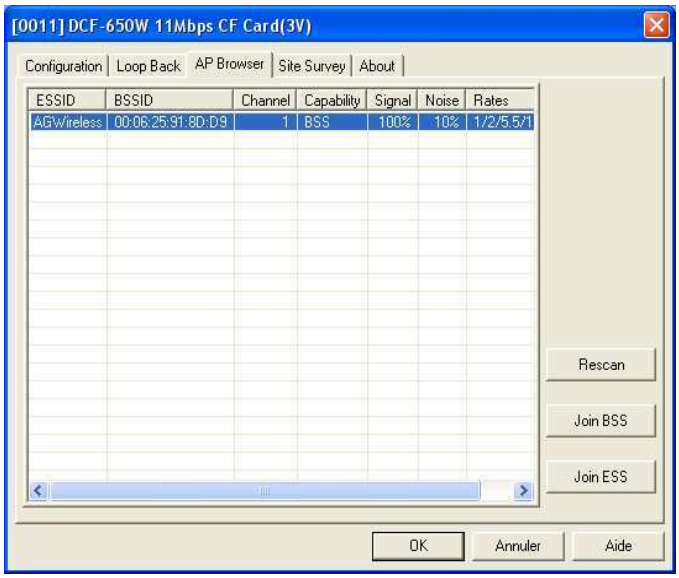
Vous pouvez vérifier si la carte est bien installée en faisant clic droit sur l'icône "Poste de travail", "propriétés", "matériel", puis "Gestionnaire de périphérique".

Une fois le logiciel installé vous devriez voir une icône dans la barre des taches, icône différente selon le modèle de carte.
Pour la D-Link j'ai une sorte de diagramme en barres.

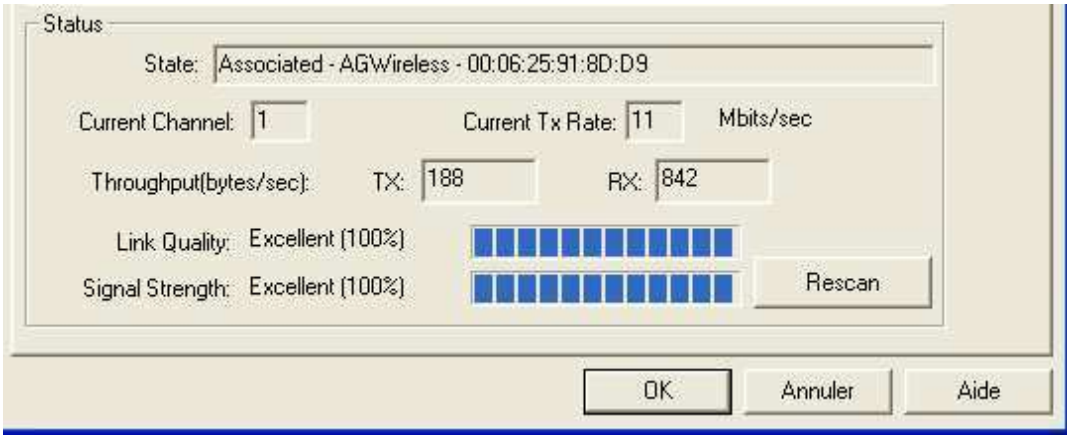
Lors de la configuration d'un réseau avec AP (point d'accès), il est important de configurer tout d'abord un poste qui servira à configurer le point d'accès.

3) Configuration du premier PC

Utilisez le logiciel fourni avec votre carte Wireless ou l'utilitaire fourni avec Microsoft Windows XP (voir plus bas) pour vous connecter au réseau.
Voici l'utilitaire D-Link:



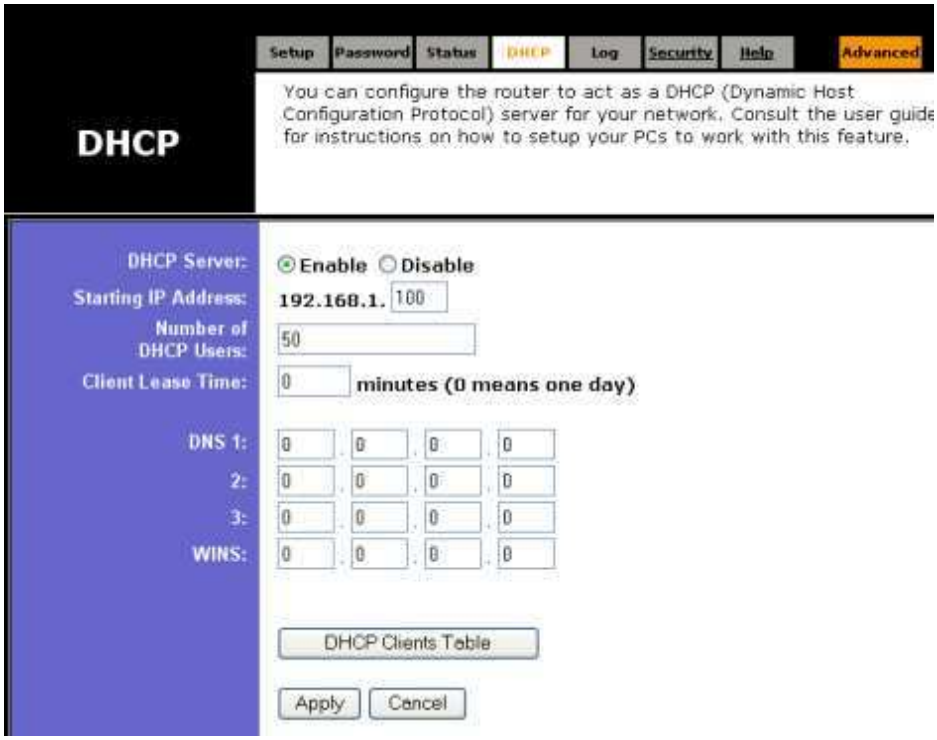
Cliquez sur "Join" pour vous connecter. Allez dans l'onglet de votre logiciel qui affiche les statuts de la connexion :



4) Configuration du point d'accès

Ouvrez votre navigateur Internet et connectez vous sur l'adresse suivante: http://192.168.1.1
Entrez le login par défaut précisé dans la documentation de votre point d'accès.
L'interface de configuration dépendra des modèles de points d'accès, le mieux est de suivre la documentation fournie avec votre matériel, je vais tout de même expliquer comment faire la configuration de base d'un WAP11/BEFW11S4.

Dans cette fenêtre vous pouvez entrer les informations concernant la configuration de votre réseau Wireless.



Un serveur DHCP est intégré à l'AP.
Le DHCP permet d'attribuer automatiquement aux postes clients une adresse IP ainsi que tous les paramètres de connexion Internet par exemple.
Notez qu'avec un serveur DHCP sur un point d'accès si il n'y a pas de WEP, vous diffusez Internet dans tout votre quartier, n'importe qui peux se connecter dessus sans aucune difficultés.

Vous pouvez configurer le nombre de PC que vous souhaitez voir utiliser le DHCP, ainsi que l'adresse

de départ pour l'attribution.

Si vous avez une partie de votre réseau en adresse IP fixe, veillez à ce qu'elle ne soit pas inclut dans la plage d'attribution DHCP.

Sur mon réseau par exemple j'ai des adresse IP fixe en dessous de 192.168.1.100, je fait donc commencer la plage à cette adresse.

Si vous possédez des DNS chez vous entrez les, si votre AP fait routeur et est connecté à un modem n'entrez rien, le serveur DHCP récupérera les infos venant du net.

Le bouton "DHCP Clients Table", vous permet de voir à qui a été attribué les adresses IP.

L'onglet "Status" vous permettra de voir si tout fonctionne parfaitement.

Les autres onglets permettent des configurations plus avancées mais je ne les décrirai pas ici.

Note : Un point d'accès fonctionne comme un hub, il n'y a donc pas de différence quand à l'accès aux PC connectés en RJ45 ou des PC connectés en wireless.

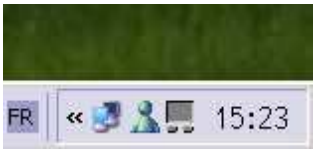
Votre point d'accès est maintenant configuré, n'importe quel PC peut se connecter dessus, exemple avec un poste sous Microsoft Windows XP

5) Configuration d'une machine cliente.

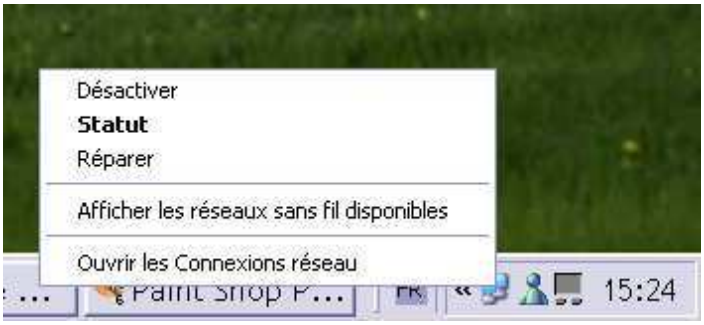
Sous Windows XP:

Sous Microsoft Windows XP, un utilitaire est fourni de base permettant la détection des réseaux wireless, généralement il fonctionne sans problème, nous allons donc l'utiliser pour nous simplifier la tâche.

Vous devriez voir une icône dans la barre des taches ressemblant à ça:



Faites un clic droit sur l'icône avec les 2 ordinateurs.

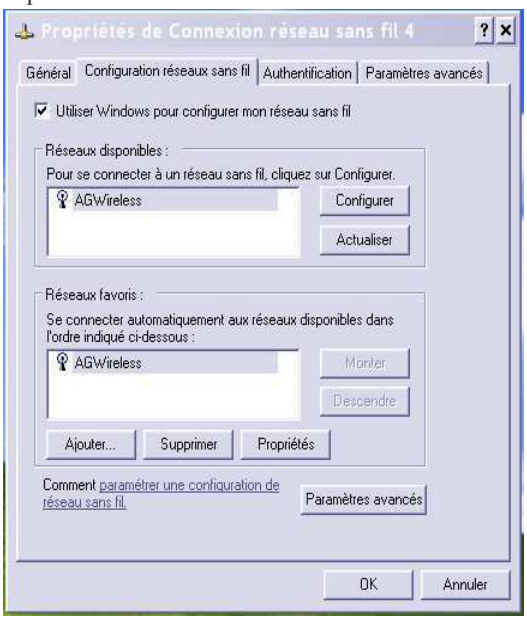


Et sélectionnez "afficher les réseaux sans fil disponible".

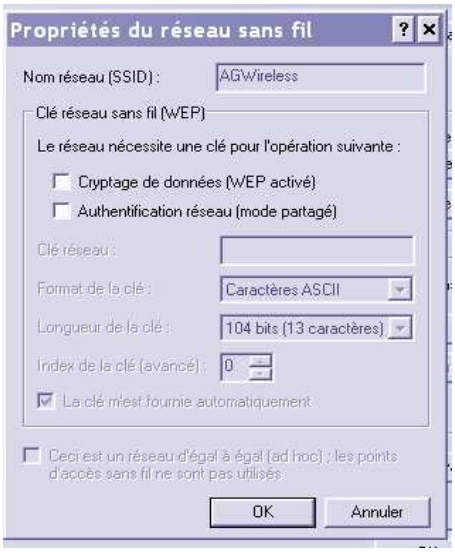
Cliquez sur connexion et le réseau Wireless est configuré.

6) Configuration du WEP.

Vous pouvez utiliser du WEP avec l'outil intégré à Microsoft Windows XP.
Cliquez sur "Paramètres avancés" dans la fenêtre affichant les réseaux.



Cliquez sur "configurer" vous pouvez maintenant configurer le cryptage.



En cas de problèmes :

Si vous ne voulez pas utiliser l'outil de Windows XP ou si il y a un quelconque problème, il suffit de décocher l'option "utiliser Windows ..." dans la fenêtre ci dessus.

6) Utilisation d'une Antenne

Vous pouvez rajouter une antenne (omnidirectionnelle de préférence) sur votre point d'accès.

Que pouvez vous faire avec un Point d'accès faisant routeur CABLE/DSL ?

Le relier à un réseau ayant déjà un serveur DHCP (sur la prise WAN), le routeur redistribue alors les informations qu'il a obtenu sur son réseau, le réseau derrière le routeur est invisible au premier réseau.

Le connecter sur son switch interne d'autres hubs / switchs pour arriver à un total maximal de 253 PC (déconseillé), en ce moment l'AP que vous avez vu en photo fait serveur DHCP pour 15 PC (12 en RJ45, 3 en Wireless)

(Fa)

9.2.2- Installation détaillée d'un réseau sans Point d'Accès

1) Introduction

Cet article s'adresse à tout le monde, aucune connaissance technique n'est requise, les notions de réseau abordées seront détaillées pour une meilleure compréhension.

Le matériel qui va être utilisé pour cet article est le suivant :

- 1 carte Compact Flash DCF650W
- 1 carte PCMCIA Sitecom

2) Installation du matériel

Tout d'abord installez les pilotes des cartes réseaux Wireless, ainsi que le logiciel généralement fourni.

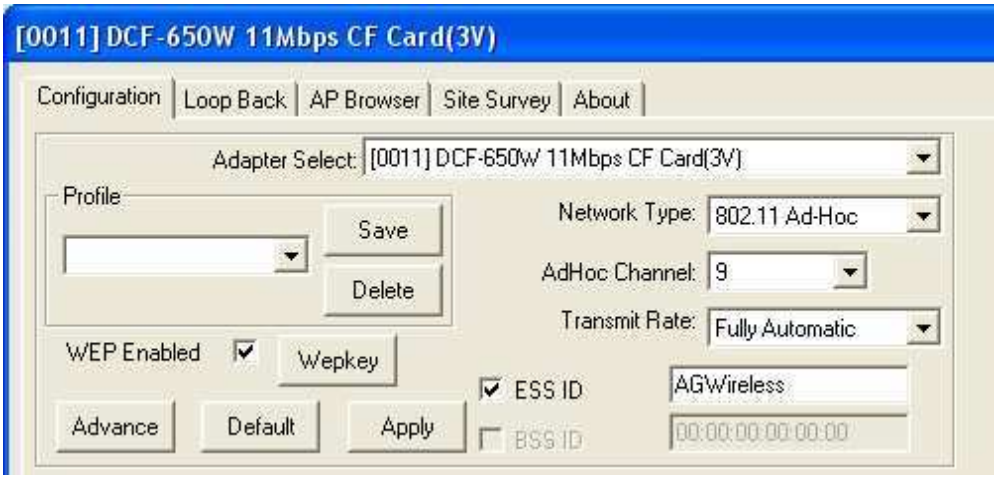
Vous pouvez vérifier si la carte est bien installée en faisant clic droit sur l'icône "Poste de travail", "propriétés", "matériel", puis "Gestionnaire de périphérique".

Une fois le logiciel installé vous devriez voir une icône dans la barre des taches, icône différente selon

le modèle de carte.
Pour la D-Link j'ai une sorte de diagramme en barres.

Lors de la configuration d'un réseau sans AP (point d'accès), il est important de configurer tout d'abord un poste complètement, ensuite les postes suivant se connecterons sur ce poste en quelque sorte.

3) Configuration du premier PC



Sélectionnez le mode Ad-Hoc (appelé aussi "poste à poste" ou "point à point").

Sélectionnez un "Channel" (canal), si il y a d'autres réseaux wireless dans votre entourage choisissez un canal qui n'est pas utilisé, cela limitera les perturbations.

Choisissez l'identifiant de votre réseau (SSID), NE LAISSEZ PAS ANY POUR LE PREMIER POSTE.

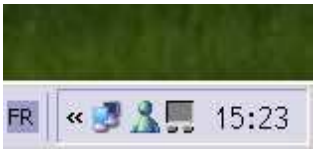
Cliquez sur "Appliquer".

Voilà votre premier poste est maintenant configuré, passons à la suite.

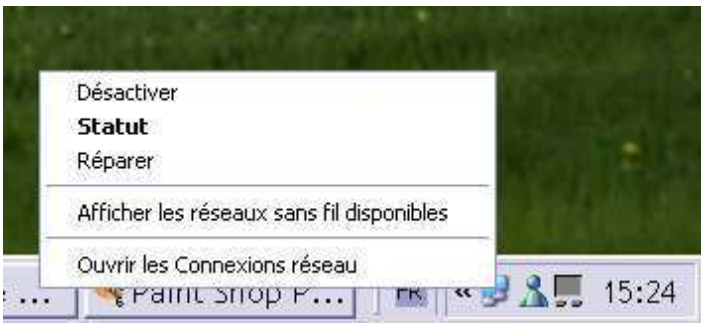
4) Configuration du deuxième PC :

L'autre poste utilisé fonctionne sous Windows XP, un utilitaire est fourni de base permettant la détection des réseaux wireless, généralement il fonctionne sans problème, nous allons donc l'utiliser pour nous simplifier la tâche.

Vous devriez voir une icône dans la barre des taches ressemblant à ça:



Faites un clic droit sur l'îcone avec les 2 ordinateurs.

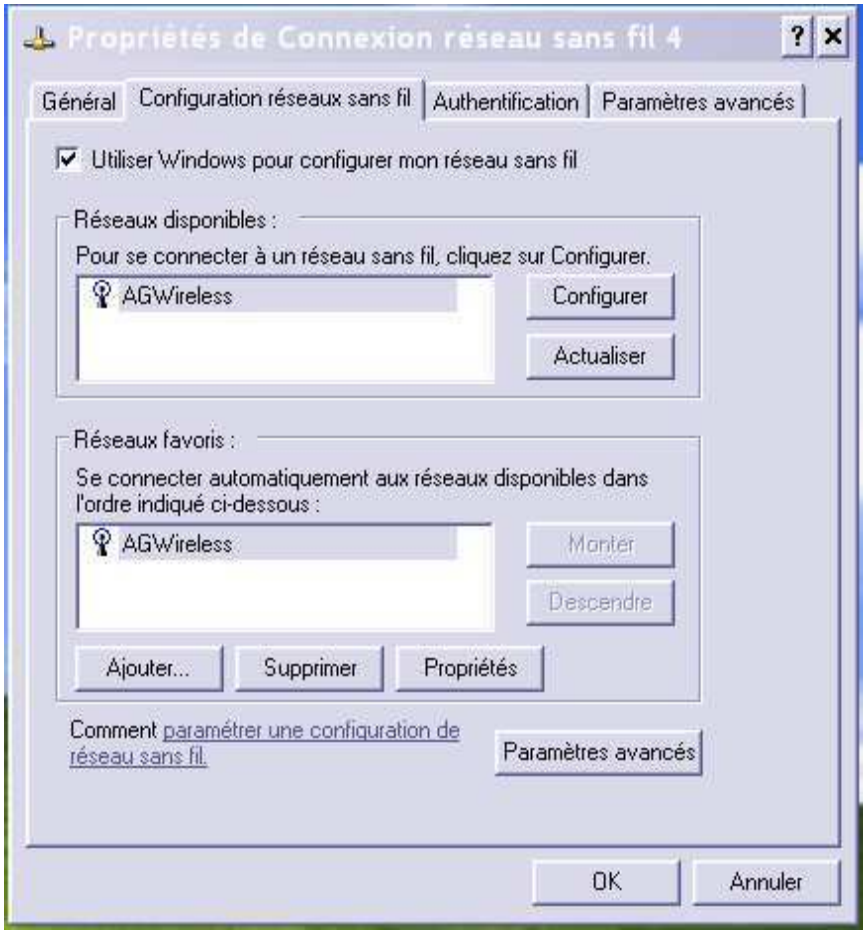


Et sélectionnez "Afficher les réseau sans fil disponible".

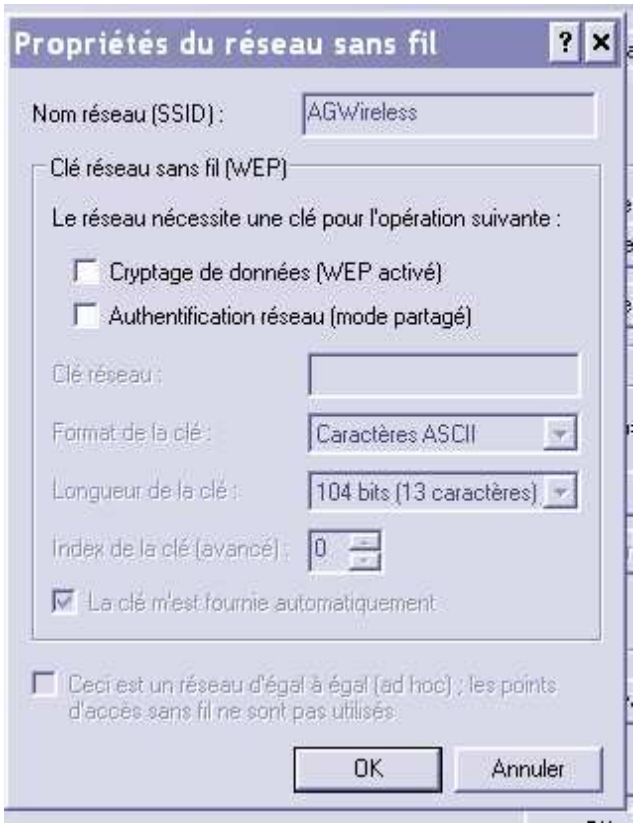
Sélectionnez votre réseau, puis cliquez sur "connexion" et le réseau wireless est configuré.

5) Note à propos du Wep :

Vous pouvez utiliser du wep avec l'outil intégré à windows XP, pour cela cliquez sur "Paramètres avancés" dans la fenêtre affichant les réseaux.



Cliquez sur "configurer" vous pouvez maintenant configurer le cryptage.



En cas de problèmes, si vous ne voulez pas utiliser l'outil de windows XP ou si il y a un quelconque problème, il suffit de décocher l'option "utiliser Windows ..." dans la fenêtre ci dessus.

Note :

Dans le logiciel fourni avec votre carte, si vous avez des onglets affichant la qualité de la liaison il ne fonctionnent généralement pas si il n'y a pas de points d'accès donc ne soyez pas étonné.

(Fa)

9.3- Configuration

9.3.1- Configuration avancée d'un AP/Routeur Linksys BEFW11S4

VOIR ANNEXE 1 EN PDF DE L'EBOOK

9.3.2- Configuration d'une carte WiFi sous xBSD

Avant de configurer vos cartes, verifiez que vous avez la derniere version du firmware, si ce n'est pas le cas, upgradez le, c'est une source de probleme notament avec les Orinoco.
Pour les cartes Lucent : http://www.wavelan.com/

1) Configuration des interfaces :

La majoritée des cartes wireless sont reconnues par defaut, vous n'aurez donc pas a recompiler le noyau (ce qui est tout de meme fortement conseillé). Pour trouver le nom attribué a votre carte, tapez :

dmesg | more

Et cherchez la ligne mentionnant votre interface. Son nom est composé de wi ou awi et un chiffre (la pluspart du temps 0), il y en a autant que de cartes wireless. Si votre cartes est une Aironet, le prefixe est alors an. Une fois trouvée, elle se configure comme une carte reseau standard, a l'aide de l''outil fconfig.

Exemple :
ifconfig wi0 192.168.0.1 netmask 255.255.255.0 up
configure et active (up) l'interface (wi0) avec l'ip 192.168.0.1 et le netmask 255.255.255.

Sous OpenBSD, pour que la carte soit configurée à chaque démarrage, ajoutez dans votre repertoire /etc un fichier :

hostname.<votre interface> (echo "inet 192.168.0.1 255.255.255.0 NONE" > /etc/hostname.wi0)

exemple : dans /etc/hostname.wi0
inet 192.168.0.1 255.255.255.0 NONE

A le meme effet que la commande précedente et est executée a chaque demarrage. Pour plus d'informations, lisez la page man (man hostname.if).

Sous NetBSD, le fichier est ifconfig.if

exemple: dans /etc/ifconfig.wi0
192.168.0.1 netmask 255.255.255.0 media autoselect

Sous FreeBSD, il faut rajouter la ligne suivante dans le fichier /etc/rc.conf :

ifconfig_wi0="inet 192.168.0.1 netmask 255.255.255.0"

Une fois ceci terminé, vous devriez pouvoir lancer un pingsur l'addresse ip que vous avez entré, vous pouvez alors passer à la suite.

2) Paramètres du reseau :

La configuration se fait de la meme maniere sous les 3 BSD, la seule difference est le nom de la commande, sous FreeBSD et OpenBSD la commande est wicontrol, alors que sous NetBSD, la commande est wiconfig. Les arguments sont les memes a quelques exeptions, mais nous ne les utiliserons pas, pour plus d'informations, reportez vous aux pages man.

La commande generale est :

/usr/sbin/wicontrol -i wi0 -n <network_name> -p 1 -s <station_name>

Note: Pour les Lucent Orinoco il faut rajouter -c 1 en argument.

3) Options du programme :

L'option -i sert a selectionner l'interface en question.
n : donne un nom au reseau, avous de le choisir comme bon vous semble, elle est composé de characteres alphanumerique,au maximum 30.
p : defini le type de reseau, les deux possibilitées sont 1 pour centralisé, et 3 pour peer-to-peer
s : donne un nom a la machine. Cet argument n'est pas nessecaire, mais il est utile lors d'un diagnostique reseau en cas de problemes
c : active le mode IBSS (1 = activé, 0 = désactivé).

A partir de la, vous pouvez essayer de vous connecter au reseau que vous venez de créer avec un client, puis lancez des pings sur les différentes machines connectées. Si ca marche, alors bien joué, vous n'avez presque plus rien a faire, sinon, c'est pas gagné, essayez de tout recommencer depuis le debut.

Pour automatiser la configuration du reseau,sous NetBSD et OpenBSD rajoutez la ligne que vous venez d'utiliser precedement precedé d'un ! dans les fichiers ifconfig.if ou hostnam.if que vous avez crées precedement. Sous FreeBSD, ajoutez la ligne que vous avez tapez dans le fichier /etc/rc.local.

(Ma)

9.4- Logiciels

9.4.1- Utilisation de NetStumbler

VOIR ANNEXE 2 EN PDF DE L'EBOOK

9.4.2- Utilisation de WEPCrack

WepCrack est sous Licence OpenSource disponnible à cette adresse : http://wepcrack.sourceforge.net/

WepCrack est un logiciel qui montre les réelles faiblesses du WEP, celui-ci est en effet destiné au crackage de clef WEP d'un réseau sans fil. WepCrack fonctionne avec des captures de flux vennant des logiciels prismdump ou Ethereal(patch).

Ce logiciel se compose principalement de 4 scripts en Perl :

WeakIVGen.pl : Le générateur de clef.
prism-getIV.pl : Recherche les faiblesses du fichier encrypté capturé.
WEPCrack.pl : Trouve la clef.
prism-decode.pl : Le decodeur de flux une fois la clef WEP trouvée.

(Pr)

9.4.3- Utilisation de Trepia

VOIR ANNEXE 3 EN PDF DE L'EBOOK

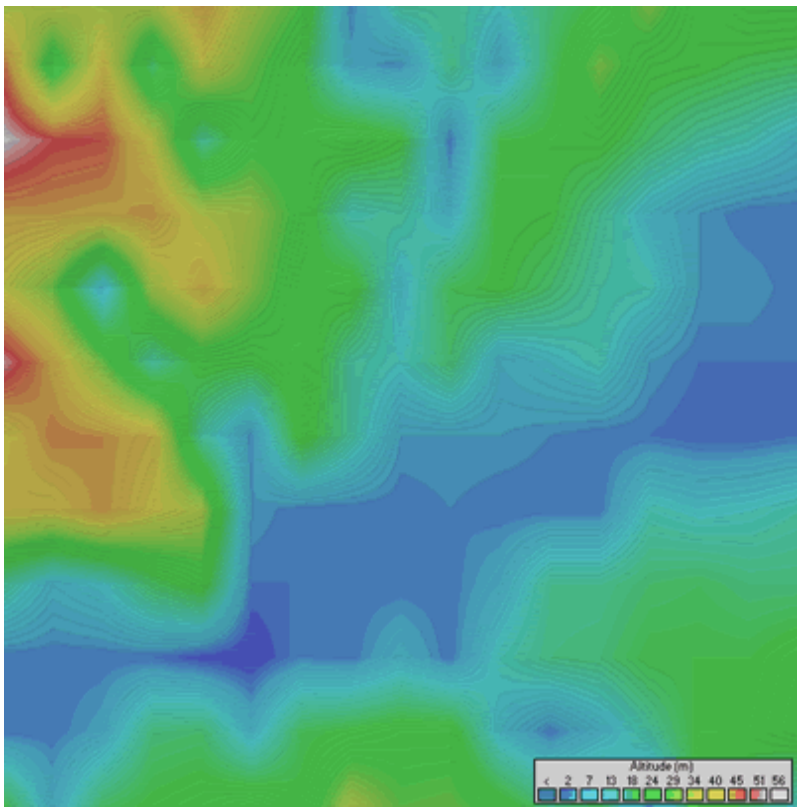
9.4.4- Utilisation de RadioMobile

RadioMobile est un logiciel permettant de créer des simulations d'émissions radio.

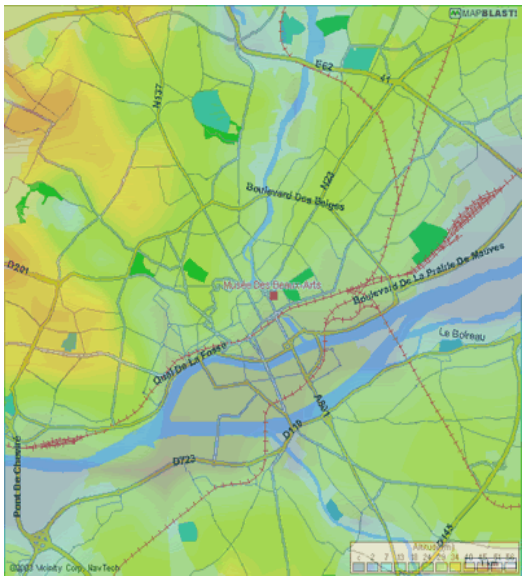
Le logiciel "Radio Mobile" permet de simuler:

- La puissance de l'émission
- Les pertes de la connectique (cable et connecteurs)
- Le gain de l'antenne d'emission
- Le gain de l'antenne de réception
- Les pertes dues au relief
- Les pertes dues au climat
- Le seuil de sensibilité du récepteur
- Les caractéristiques du térrain

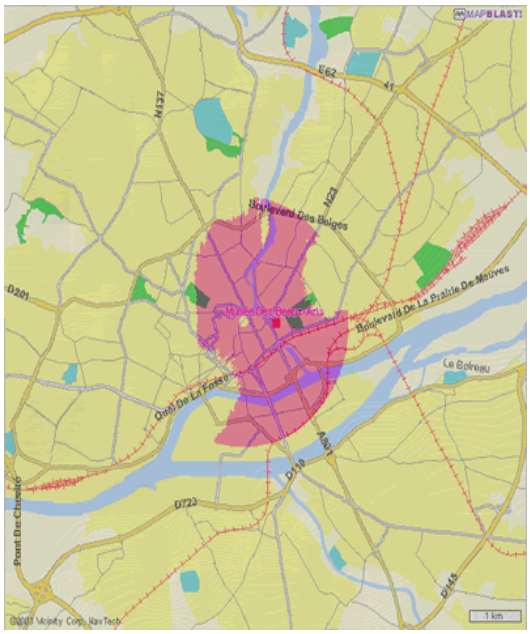
Voici une image du relief de Nantes généré par le logiciel RadioMobile :


Altitude (m)
< 2 7 13 18 24 29 34 40 45 51 56

Voici l'image du relief intégré avec le plan de Nantes :



Voici un exemple (omni 15db - 2 km de portée) :



Beaucoup de fonctions et de paramètres me sont encore inconnues du logiciel. Si quelqu'un à des données plus précises sur les différents facteurs entrant en compte, n'hésitez pas à les faire partager.

Télécharger le logiciel : http://www.cplus.org/rmw/downloadfr.html
Données cartographiques du relief (DTED) : http://f4ahw.free.fr/datanum.htm
Données cartographiques du relief (GTOPO30):
ftp://edcftp.cr.usgs.gov/pub/data/gtopo30/global/w020n90.tar.gz
Manuel d'utilisation : http://perso.wanadoo.fr/fmerle/index.htm

(Pr)

9.5- Pratique

9.5.1- Le WarDriving (ou Trébucher sans fils)

Le terme "WarDriving" vient des états unis et à été francisé par Wifi-Montauban en "Trébucher Sans Fil" : http://www.wifi-montauban.net/communaute/index.php/TrebucherSansFil

Le concept du "WarDriving" est simple :
Vous avez besoin d'un ordinateur ou d'un PDA avec une carte WiFi, d'un GPS, et de deux logiciels :

- Un logiciel d'écoute (ex: NetStumbler).
- Un logiciel de création de plan (ex: StumbVerter).

Ensuite vous avez juste à prendre votre voiture et vous baladez de point en point avec votre matériel sur le siège passager, votre ordinateur enregistrera tout ce qu'il trouve comme réseau sans fil.

Le logiciel le plus souvent utiliser pour faire du WarDriving est NetStumbler

Voici un exemple de plan obtenu :

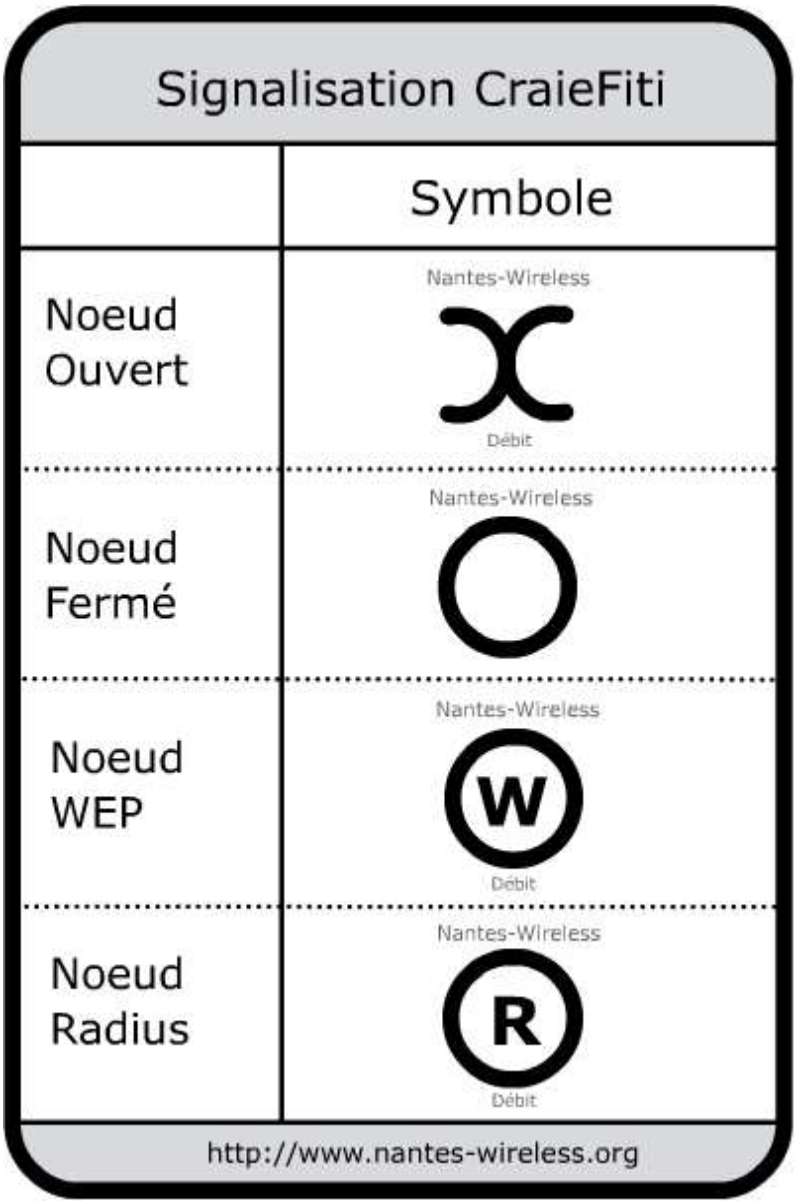
Voici une petit HOWTO sur le WarDriving : http://www.wardriving.com/doc/Wardriving-HOWTO.txt
Pour plus d'infos :
http://www.wardriving.com/
http://www.bitshift.org/wardriving.shtml
http://www.sans.org/rr/wireless/wardriving.php
http://enthios.com/trading/wardriving.htm
http://www.wardrive.net/
Une technique pour contrer le WarDriving est de simuler plusieurs milliers d'AP avec un logiciel comme FakeAP (marche que sur Prism2) (Pr)

9.5.2- Le CraieFiti

Le CraieFiti est un langage pictural permettant d'indiquer la position d'un point d'accès.
CraieFiti est le terme francisé de "Warchalking".

Ces symboles sont inspirés du langage Hobos utilisé aux états unis durant la grande dépression :
http://www.slackaction.com/signroll.htm

Voici une approche de CraieFiti pour le réseau de Nantes-Wireless :



La présence de l'un de ses symboles sur un mur ou sur un trottoire indique que vous pouvez vous connecter à un réseau sans fil.
Pour plus d'infos :
http://craiefiti.free.fr/
http://www.warchalking.org/
http://www.theregister.co.uk/content/59/26353.html
http://www.vivrele.net/node/793.html
http://www.afnet.fr/portail/news/06_off-shore/231_off
http://vlan.org/breve14.html
http://www.a-brest.infini.fr/bzh-armorique/article.php?id_article=26 (Pr)

10- Bibliographie

10.1- Livres

Montez votre réseau sans fil WI-FI

Ce guide pratique et tout en couleur délivre toutes les informations utiles pour installer, configurer et profiter des ressources du réseau sans fil Wi-Fi.

Micro Application - 04/2003
14,8 x 21 - 192 pages
ISBN: 2-742-93025-6
Broché - Couleur
Prix public : 10,47 EUR

802.11 et les réseaux sans fil

Dans l'ensemble très technique, ce livre est destiné à découvrir les spécificités des normes 802.11x dans son ensemble.

Eyrolles - 08/2002
19 x 23 - 304 pages
ISBN: 2-212-11154-1
Broché - Noir et Blanc
Prix public : 40,00 EUR

Wi-Fi par la pratique

Simple à lire, celui ci satisfera tout le monde.

Eyrolles - 10/2002
19 x 23 - 304 pages
ISBN: 2-212-11120-7
Broché - Noir et Blanc
Prix public : 36,00 EUR

802.11 Wireless Networks

O'Reilly - 05/2002
18 x 23,5 - 444 pages
ISBN: 0-596-00183-5
Broché - Noir et Blanc
Prix public : 50,00 EUR

Reseaux sans fil amateurs, installation et mise en oeuvre

O'Reilly - 01/2002
15,2 x 23 - 126 pages
ISBN: 0-596-00204-1
Broché - Noir et Blanc
Prix public : 28,00 EUR

Build Your Own Wi-Fi Network

Mc Graw Hill - 11/2002
21,5 x 27,5 - 266 pages
ISBN: 0-07-222624-2
Broché - Noir et Blanc
Prix public : 36,10 EUR

(Pr / Tg)

11- Les ressources sur le Web

11.1- Les liens utiles

Voici la liste des tous les liens qui peuvent vous êtres utiles pour des renseignents supplémentaires ainsi que les liens utilisés pour nous aider à rédiger ce E-book.

Transmission d'ondes, théorie

http://www.radioamateur.org/formation/index1.html

Théorie radio et calculs de liens pour Wireless LAN (WLAN)
http://www.swisswireless.org/wlan_calc_fr.html

Sites d'information sur le Wi-Fi

FR
http://blog.netpartoo.com/
http://www.francispisani.net/wirelessence/blogger.html
http://www.wlanfr.net/
http://www.wireless-info.org/
http://rubb.free.fr/802-11/
US
http://www.80211insider.com/
http://80211b.weblogger.com/
http://reiter.weblogger.com/
http://www.80211-planet.com/
http://wireless.ziffdavis.com/

Sites des communautés Wi-Fi

FR
Wifi Montauban
Nantes Wireless
Angers Wireless
Wireless France
Paris Sans Fil
US
Seattle Wireless
Belgique
Reseau Citoyen

Antennes

Antennes Commercialisées
http://online.infracom.fr
http://www.hflan.com
http://www.ges-lyon.fr

Fabrication d'antennes artisanales

Omnidirectionnelles
http://reseaucitoyen.be/index.php?OmniDirectionnelleSimple

Pringles
http://www.oreillynet.com/cs/weblog/view/wlg/448
http://www.wireless-fr.org/[..]//Homebrew_fr.htm
http://reseaucitoyen.be/index.php?PringlesCan

Cantenna
http://www.turnpoint.net/wireless/cantennahowto.html
http://reseaucitoyen.be/index.php?BoiteDeConserve1
http://www.wifi-montauban.net/communaute/index.php/CaroTenne

http://www.turnpoint.net/wireless/cantennahowto.html
http://www.paris-sansfil.net/index.php/RicoreRJ45

Antenne Hélicoidale
http://helix.remco.tk/
http://www.wireless.org.au/jhecker
http://www.guerrilla.net/[..]/2ghz_helical/index.html
http://reseaucitoyen.be/index.php?AntenneHelicoidale2
http://reseaucitoyen.be/index.php?AntenneHelicoidale3

Antenne Yagi
http://www.netscum.com/clapp/wireless.html
http://seattlewireless.net/?BuildingYagiAntenna
http://www.student.uwa.edu.au/bover/yagi/

Antenne Parabolique
http://www.jrmiller.demon.co.uk/products/s_ant.html

Antenne Colinéraire
http://reseaucitoyen.be/index.php?AntenneColineaire1

Antenne Biquad
http://reseaucitoyen.be/index.php?BiQuad

Antenne Uda-Yagi
http://reseaucitoyen.be/index.php?UdaYagi

Antenne Patch
http://reseaucitoyen.be/index.php?AntennePatch

Antennes 100% Originales
http://reseaucitoyen.be/index.php?CornetPortable
http://reseaucitoyen.be/index.php?LittleBigHorn
http://reseaucitoyen.be/index.php?BombolongMobile
http://reseaucitoyen.be/index.php?CornetDeCarton
http://reseaucitoyen.be/index.php?BoiteDeLait
http://reseaucitoyen.be/index.php?BoiteDeLait2
http://reseaucitoyen.be/index.php?SlottedWaveGuide
http://reseaucitoyen.be/index.php?SlottedWaveGuide2
http://www.geocities.com/lincomatic/homebrewant.html
http://www.wifi-montauban.net/communaute/index.php/CamembertAntenna

Projets Etudiants
http://www.emclab.umr.edu/courses/ee373/W01proj.html
http://eewww.eng.ohio-state.edu/roblin/Design.html
http://www.acusd.edu/ekim/ant_proj/

Materiel Informatique

Les Chipsets

TI ACX100
http://focus.ti.com/docs/apps/catalog/tisolutions/tisolutions.jhtml?templateId=977&path=templatedata/cm/level1/data/bband_80211_tisol

Prism II, 2,5, 3
http://www.intersil.com/product_tree/product_tree.asp?x=1

Atmel
http://www.atmel.com/dyn/products/devices.asp?family_id=657

Site Fabricants :
http://www.dlink.com/products/wireless/index.asp

Cartes PCI - Sites persos (Tests, Hack, Tweak, ...)
Dlink - DWL 520+ - http://www.angers-wireless.net/v3/modules.php?name=News&file=article&sid=11&mode=&order=0&thold=0
Actiontec - PCI - http://fanfoue44.free.fr/Actiontec/Carte-PCI/html/pci.html
Linksys - WMP11 - http://fanfoue44.free.fr/Linksys/WMP11/html/wmp11.html

Cartes PCMCIA - Sites persos (Tests, Hack, Tweak, ...)
Orinoco - http://www.wireless-fr.org/contributions/lucent/orinoco.htm
Compaq - http://www.wireless-fr.org/contributions/tcoder/www_lesmanos_com.htm
D-Link DWL 650 - http://reseaucitoyen.be/?DWL-650
- http://c0rtex.com/will/antenna/
Micronet
SP906A - http://www.wireless-fr.org/communaute/index.php?Micronet-SP906A
SP905V2 - http://www.wireless-fr.org/communaute/index.php?Micronet-SP905V2
Actiontec - PCMCIA - http://fanfoue44.free.fr/Actiontec/Carte-PCMCIA/html/pcmcia.html

Cartes Compact Flash - Sites persos (Tests, Hack, Tweak, ...)
D-Link - DCF 650W - http://www.angers-wireless.net/v3/modules.php?name=News&file=article&sid=10&mode=&order=0&thold=0

Ponts Ethernet - Sites persos (Tests, Hack, Tweak, ...)
Linksys WET 11
http://www.wireless-fr.org/communaute/index.php?WET11
http://www.wireless-fr.org/communaute/index.php?WET11%20%E0%20nu
http://www.wireless-fr.org/communaute/index.php?changer%20la%20carte%20pcmia%20interne%20du%20WET11
http://www.wireless-fr.org/communaute/index.php?Alimenter%20son%20Wet%2011%20par%20un%20POE
http://www.wireless-fr.org/communaute/index.php?RicoreRJ45

(Fa)

12- Lexique

AP:

"Access Point" (AP) signifie Point d'accès, celui-ci permet de controler un réseau wirelesss, il est similaire à l'utilisation d'un hub RJ45. On le designe egalement sous le nom "node".

Antenne:

Directionnnelle : type d'antenne ayant un rayonement optimisé dans une direction, contrairement à une antenne omnidirectionnelle. Ce type d'antenne est géneralement utilisé pour faire des liaisons point à point ou couvrir des zones de faibles dimensions.

Omnidirectionnelle : type d'antenne ayant un rayonnement à 360°. Les gains varie de 0 à 15 dB environ.

ART:

Autorité de Régulations des Télécommunications. http://www.art-telecom.fr

Adresse MAC:

Il s'agit de l'adresse physique de la cartes Wifi. Cette adresse est codée en 48 bits par les constructeurs de matériels réseau.

Les adresses sur 48 bits sont uniques: l'IEEE attribue à chaque constructeur un numéro (6 chiffres hexadécimaux) spécifique. Le constructeur gère ensuite lui-même les autres bits disponibles de l'adresse. Ainsi, quel que soit l'origine du matériel, il est théoriquement impossible qu'il y ai des conflits d'adresses physiques sur le réseau.

Adresse IP:

On la trouve sous la forme ci xxx.xxx.xxx.xxx (xxx étant compris entre 0 et 255) pour la version IPV4. Cette adresse est unique et n'est allouée qu'à un seul ordinateur, permettant ainsi d'identifier chaque ordinateur. En IPv6, cette adresse aura la forme xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (avec héxadécimal), et implèmentera une sécurité renforcée ne nécessitant pas d'autre protocoles

Channel:

"Channel" signifie canal en français. Le 802.11b est composé de 13 canaux avec une largeur de bande de 7 MHz (Voir: FréquencesDuWifi)(C'est pas plutot 5Mhz?)

DHCP:

C'est un protocole permettant d'attribuer automatiquement une adresse IP aux utilisateurs de ce réseau (Dynamic Host Configuration Ptotocol).

Firmware:

C'est un prologiciel(une sorte de bios) inclus dans la memoire du materiel lui permettant ainsi de fonctionner correctement .Il est important de mettre à jour son firmware regulierement ce qui ammenera un niveau de performance optimal du materiel .

Pigtail:

Câble spécifique permettant de relier une carte wireless à une antenne.

PIRE:

Abreviation désignant la puissance d'émission rayonnée, c'est à dire la puissance réelle qui sort d'une antenne. (Puissance Isotrope Rayonnée Equivalente)

Routeur:

Un routeur envoie des paquets de données de pc à pc ,il "aiguille" ces paquets de données sur le chemin optimal .Ce chemin optimal est choisit en fonction de plusieurs paramètres comme la vitesse ,le trafic ...

VPN:

Autre moyen de sécuriser les données, chemin virtuel créé entre la source et le destinataire; les données passent par un système de tunneling, c'est a dire qu'une sorte de tunnel est créé entre ces deux points. Dans ce tunnel, les données sont cryptées .(Virtual Private Network)

WEP:

Wireless Encryption Protocol Encryptage utilisé dans les réseaux WiFi; il peut être de 64, 128, 256 ou 512 bits. Ce cryptage est executé par le matériel WiFi et est basé sur le RC4.

(Ka)

14- Mot des rédacteurs

Tout d'abord nous tenons à remercier les nombreux sites ayant participés à la diffusion de la première version de l'ebook:

http://www.zonehd.net/news.php#355
http://www.tt-hardware.com/article.php?sid=4082
http://blog.netpartoo.com/index.php?p=191&c=1
http://www.newdimension-fr.net/t1658.html
http://www.materiel.be/news.php?start=0#news1256
http://www.rue-montgallet.com/news/materiel/lire/1256/
http://www.wlanfr.net/?op=tnews&id=62
http://www.rue-hardware.com/news/materiel/lire/1256/
http://www.cybernews-fr.net/modules/news/article.php?storyid=171
http://www.linuxfrench.net/article.php?id_article=1250

L'ebook à généré depuis sa publication plus de 20 000 hits sur le mirroir fanfoue44.free.fr avec des pics à plus de 4000 accès par jour les premiers jours.

Cet ebook est et restera un ouvrage libre, dynamique et gratuit, vous pouvez le redistribuer gratuitement mais la revente de ce ebook est interdit sauf:

- autorisation écrite de la part des principaux rédacteurs
- vente dont tous les bénéfices sont reversés à une association ayant pour but de developper les réseaux sans fils, association qui doit elle-même être membre de l'association www.wireless-fr.org

Si vous désirez intégrer une partie de cet ebook dans un document diffusé gratuitement, vous êtes priés de citer l'auteur de la partie intégrée, de citer un lien permettant le téléchargement de cet ebook et d'avertir l'association nantes-wireless ou angers-wireless, par le biais d'un de leurs forums par exemple.

Si vous désirer intégrer une partie de cet ebook dans un ouvrage commercialisé, veuillez contacter par mail l'auteur de la partie que vous désirerez intégrer ainsi qu'une des association Nantes-wireless ou Angers-wireless

Si vous désirez publier cet ebook et le commercialiser contactez les associations Angers-wireless et Nantes-wireless, sachez que tous les bénéfices réservés habituellement aux auteurs pour ce genre d'ouvrage seront intégralement reversés à part égales aux associations Nantes-wireless et Angers-wireless.

Vous pouvez aussi contribuer à la réalisation de cet ebook et apporter vos connaissances par l'intermédiaire du WIKI du site www.nantes-wireless.net

Pourquoi les associations wireless francophones ont-elle besoin de fonds ?

> L'objectif final des associations ayant adhéré à l'association Wireless France est de mettre en place un réseau national permettant depuis n'importe quelle ville de france (si une association membre y est présente) d'acceder de manière sécurisée au réseau national.
>
> Chaque association a donc besoin d'un PC faisant office de serveur, d'une connexion internet haut-débit ainsi que de points d'accès permettant de proposer aux membres des Hot-spots libres et gratuits permettant d'accedder au réseau.

Si vous désirez faire un don (matériel, monétaire) n'hésitez pas à contacter les associations.
Vous pouvez aussi faire un prêt de bande passante en permettant à une association d'installer son serveur dans votre entreprise ou chez vous, le serveur est peu gourmand en bande passante puisque faisant seulement de la réplication de base de donnée et de la validation d'accès, vous pouvez aussi preter le materiel ainsi que votre bande passante (un vieux PC faisant très bien l'affaire)

Les associations proposent généralement leurs conseils pour du choix de materiel ou de l'aide à la configuration, n'hésitez pas à les contacter.

Association Nantes-wireless: www.nantes-wireless.net

Association Angers-wireless: www.angers-wireless.net
Association Wireless France et liste des associations membres: www.wireless-fr.org

(Fa)