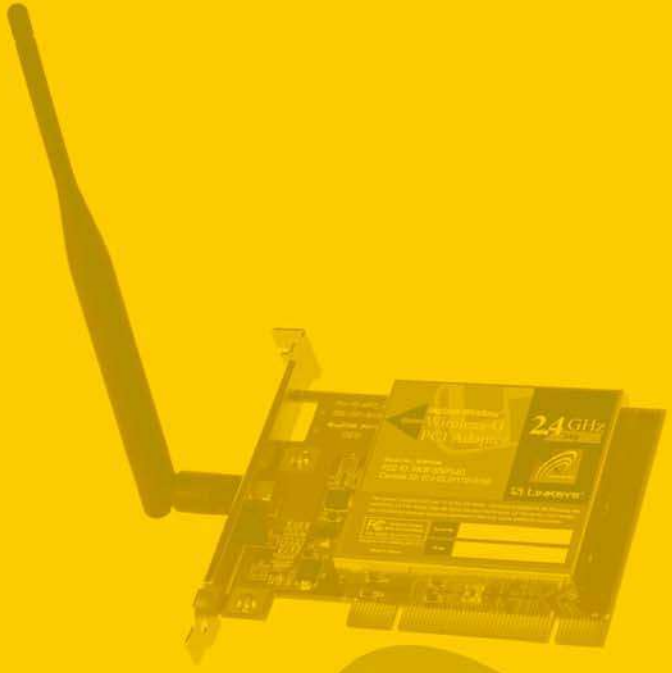


802.11
LES RÉSEAUX SANS FILS

Nantes Wireless

angers Wireless

INFRACOM
Online 24/24h
http://online.infracom.fr

1. Avant Propos

1.1. A qui s'adresse l'Ebook

Ce E-book s'adresse à tout le monde, au débutant découvrant le wireless et souhaitant une documentation complète, à ceux ayant des connaissances dans le domaine du wireless et souhaitant approfondir certains points telle la transmission de données par exemple.

Ce E-book 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 réseau.

1.2. Comment à été rédigé l'Ebook

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

Personnes ayant contribué à sa réalisation :

- Fanfoue (fa) : François Gerthoffert : f.gerthoffert@caramail.com
- Prospère (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

Note : A la fin de chaque partie vous trouverez sur la droite les initiales de l'auteur

1.3. Dans les prochaines versions

- Installation d'un node
- Analyse de la sécurité et solutions
- Liens et lexique améliorés
- Réalisation d'une liaison longue distance
- Test de l'antenne avec module wifi intégré
- Détails sur les antennes directionnelles
- …

2. Introduction

2.1. Les Réseaux sans fils

Voici les différents modes de transmission de données informatiques par ondes radio :

Le Wi-Fi :

Développé pour la création de réseaux locaux sans fil, liaison possible jusqu'à 100km environ, de 2mbps à 11mbps pour la norme 802.11b jusqu'à 54mbps voir 108mbps pour la norme 802.11g sur 2,4 Ghz ou en 5 Ghz pour la norme 802.11a, le plus utilisé étant le 802.11b du fait de son faible coût et de son débit acceptable.

Le Bluetooth

Le Bluetooth est une technologie limitée surtout aux liaisons de petites distances et à faibles débits

Le GPRS

Utilisé pour la téléphonie

L'UMTS

Utilisé pour la téléphonie

La Boucle Locale Radio (BLR)

Identique à la boucle locale filaire (téléphonique), limitée à 4 opérateurs en France, par l'art. Réservée à Internet, de ce fait, peu intéressant pour réaliser des réseaux locaux.

Le Packet Radio

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

(fa)

2.2. Le Wi-Fi ou la norme IEEE 802.11b

La norme Wi-Fi (Wireless Fidelity) est le nom commercial donné à la norme IEEE 802.11b par Weca.
Le terme Wi-Fi est une marque déposée, ce qui a obligé "Wifi Paris" à se renommer en "Paris Sans Fil".

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.

L'émission simultanée sur plusieurs canaux demande à ce que les canaux soit disjoints. Fréquence du wifi

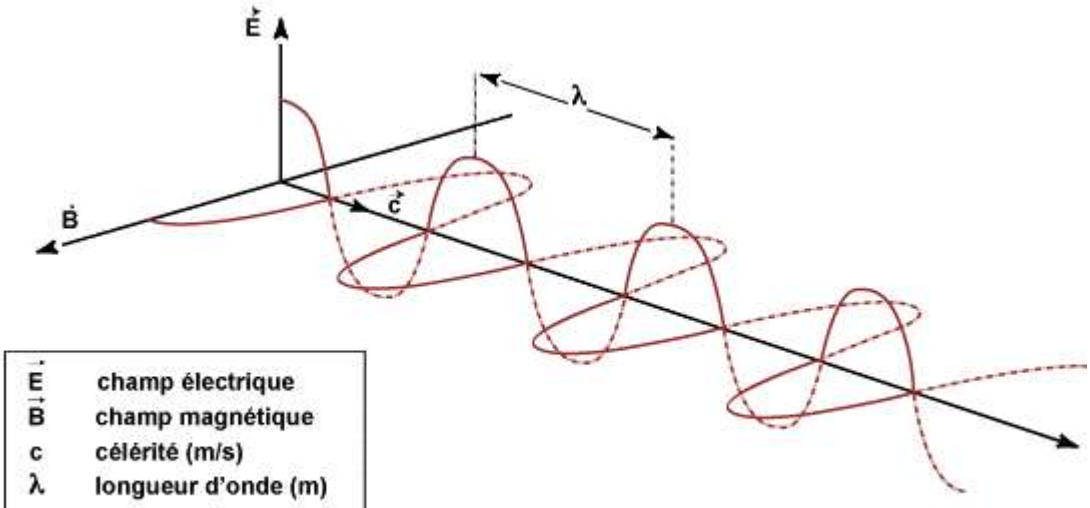
Note: L'Ethernet est définie par l'IEEE 802

(ps)

3. Les ondes électromagnétiques

3.1. La propagation des ondes

Ci-dessous la représentation d'une onde électromagnétique:



$\vec{E}$	champ électrique
$\vec{B}$	champ magnétique
c	célérité (m/s)
λ	longueur d'onde (m)
T	période = λ / c (s)
f	fréquence = 1 / T (Hz)

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.

3.2. 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).

$$F = \frac{C}{\lambda}$$

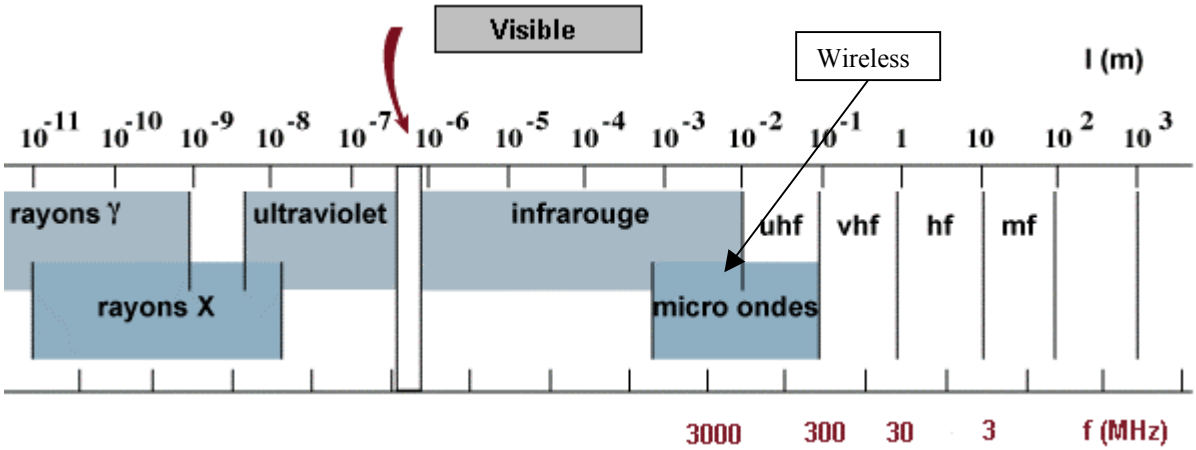
Notes :

- F = Fréquence en Hz
- C = Célérité (m/s)
- λ = 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, …).
Certains matériaux et milieux laisseront en effet plus facilement passer les ondes que d'autres.

3.3. Le Spectre

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



source www.radioamateur.org

Pour avoir plus de précision au niveau des canaux, allez voir la page des **FréquencesDuWifi**.

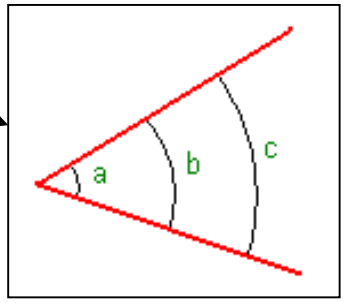
3.4. Les Phénomènes

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 manière :



La densité de puissance du flux en a sera plus important qu'en b ou en c et ainsi de suite.
L'atténuation de parcours peut se mesurer à l'aide de l'équation suivante :

$$Ploss = 10 \text{ Log } (4 \pi d / \lambda) ^2$$

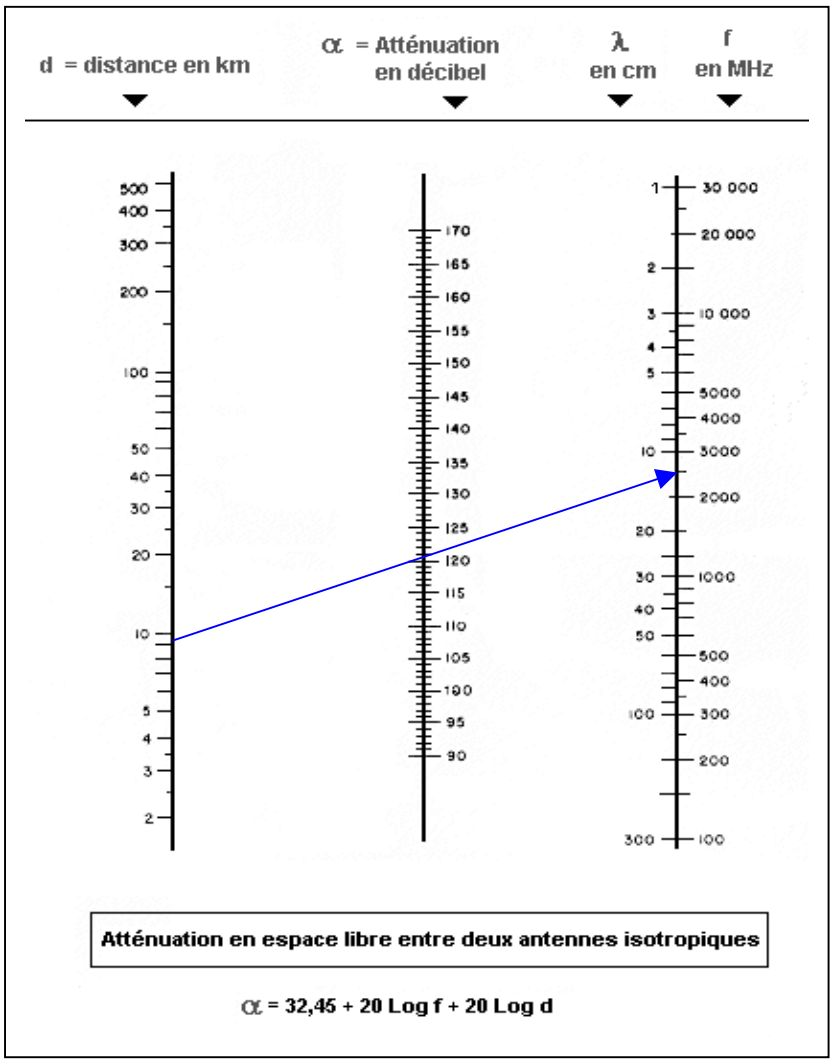
d : distance en m
Alpha : longueur d'onde en m

Ploss ou path loss correspond à la perte de parcours qui se mesure en Db (décibels). Le ploss obtenu grâce à l'équation ci dessus correspond à l'atténuation de parcours en espace libre, c'est à dire au résultat que l'on pourrait obtenir dans un espace libre s'il n'y avait vraiment aucune perturbation.
Exemple d'application :
La longueur d'onde se calcule de la manière suivante :

$$\lambda = \frac{30}{F}$$

F : fréquence en Ghz
λ : Longueur d'onde en cm

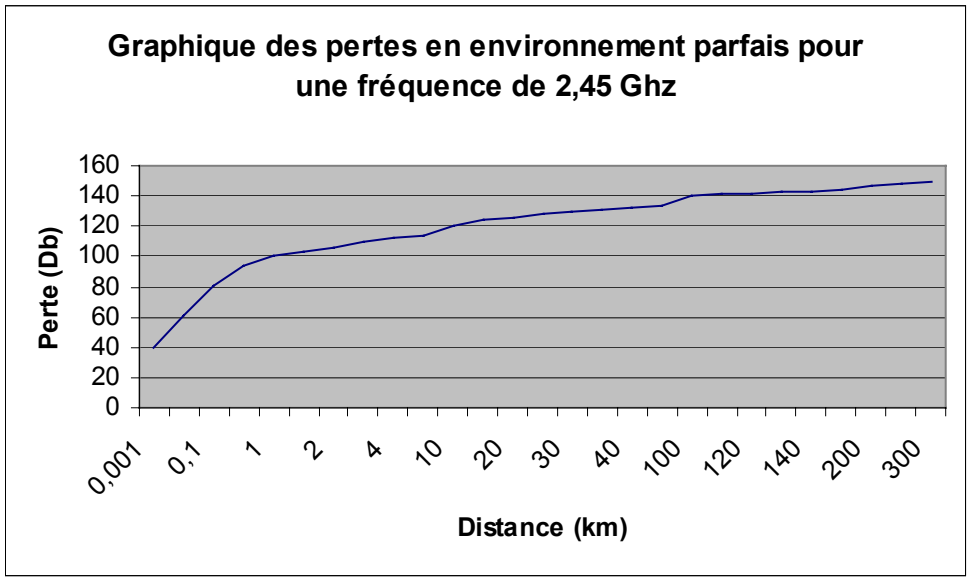
Pour une fréquence de 2.45 Ghz, alpha = 12,2448 cm
On peut aussi plus simplement utiliser un graphique de mesure tel que celui ci :



Exemple : Pour une distance de 10 Km quelle sera l'atténuation pour un réseau Wireless (fréquence 2,45 Ghz)

→ L'atténuation sera d'environ 120 dB

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.

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

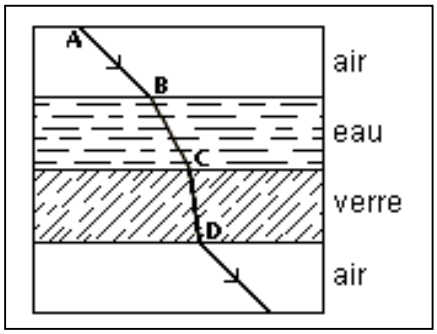
En wireless, par exemple on peut difficilement faire plus de 5km avec du matériel « classique » (nous aborderons ce point plus loin).

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

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

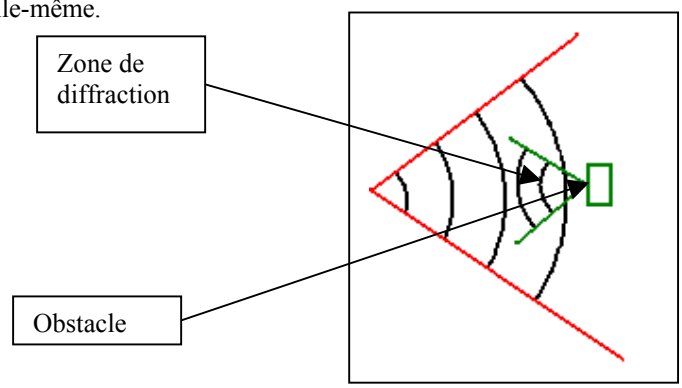


3.4.4. La réflexion

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.

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.



(fa)

4. Le matériel

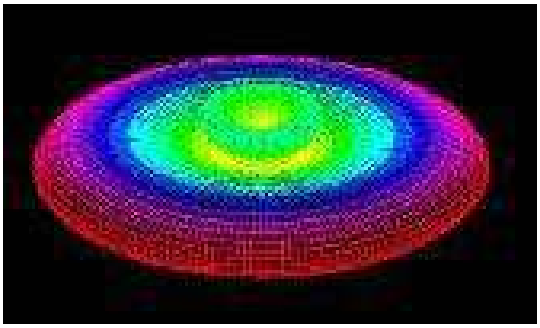
4.1. Les antennes

4.1.1. Les 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'antenne omni (24 1360) :

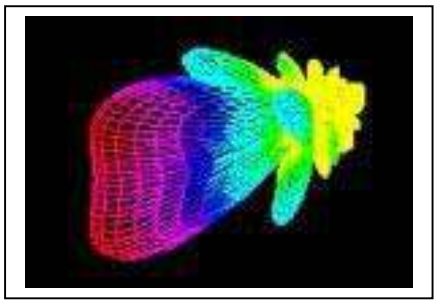
Vue en 3D de la propagation des ondes
avec une antenne Omnidirectionnelle



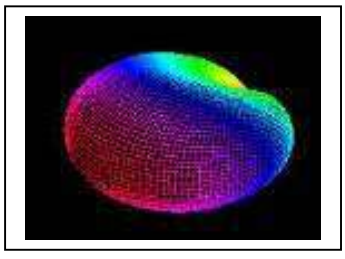
4.1.2. Les antennes directionnelles

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 : **Vue 3D de sa propagation**



Antenne Patch : **Vue 3D de sa propagation**



Il existe plusieurs modèles d'antennes directives : panneau, paraboles, paraboles grillagées, patch (= panneau en général), 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.

4.1.3. 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 Retour 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.

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 commercialisée.

4.2. La connectique

4.2.1. 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)
- Certains modèles sur des sections plus importantes, via des connecteurs adaptés.

4.2.1.1. RG 58 CU

Ce type de câblage est principalement utilisé pour les réseau Ethernet (BNC) assez peu utilisé en Wireless.

Le RG58CU a des pertes de 82.37 dB/100 m.

Pigtail utilisant du câble RG58 CU

4.2.1.2. RG 174

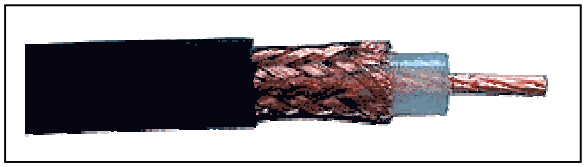
Câble 2 mm, destiné aux connecteurs miniatures, atténuation 144,50 dB aux 100 m.

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

A éviter pour de longues distances

4.2.1.3. RG 213

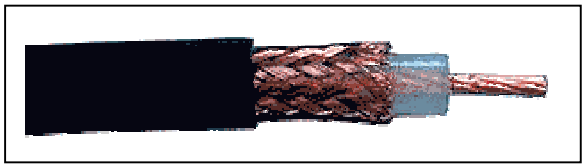
Diamètre : 10.3 mm
Perte : 41,66 dB / 100 m
Masse : 155,0 grammes / mètre
Blindage : Simple tresse



Le même câble avec un blindage double tresse : **RG214**

4.2.1.4. RG 214

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



4.2.1.5. Aircom +

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.

4.2.2. 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
- MCX
- MMCX
- Lucent

Chacun de ces types ayant des variantes (polarité inversée (RP), filetage à gauche, à droite, male, 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 un 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 :

4.2.2.1. 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'un antennes "Pringles" ou "Ricoré" cette embase N femelle est généralement utilisée :

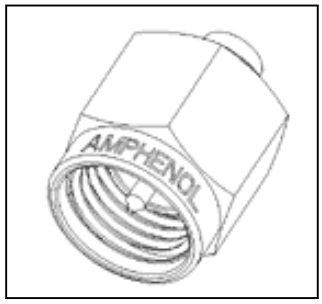
Connecteur N mâle :

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

Nous avons rajouté à cette antenne Omnidirectionnelle un adaptateur N vers SMA.

4.2.2.2. Type SMA

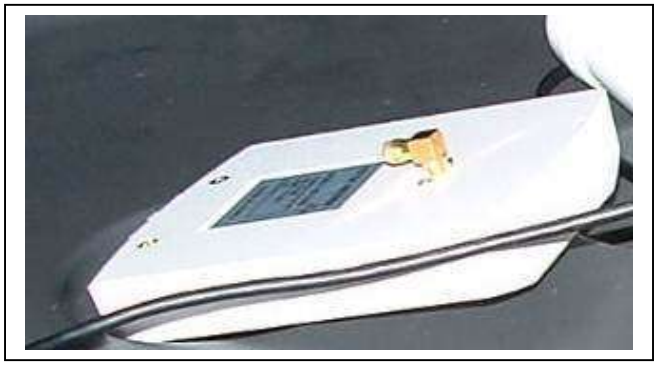
Les connecteurs SMA, sont les connecteurs généralement rencontrés sur les cartes PCI et certaines antennes.



Voici par exemple une Antenne Omnidirectionnelle a Gain de 2 dB. Cette antenne possède un connecteur TNC, en passant par du BNC nous sommes arrivés à du SMA, le dernier connecteur est donc un SMA (attention aux pertes occasionnées par un grand nombre d'adaptateurs).

Voici un adaptateur SMA male vers SMA male :

Antenne patch avec connecteur SMA :



4.2.2.3. 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.

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

4.2.2.4. 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 :

(fl)

4.3. Le matériel informatique

4.3.1. Les chipsets

4.3.1.1. Prism II

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

Quelques cartes utilisant le chipset Prism II :

- D-Link DWL 650
- D-Link DCF 650
- Linksys WMP11
- Actiontec (Usb, PCMCIA, PCI)

4.3.1.2. TI ACX 100

Chipset apparut durant le second semestre 2002, à 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 mis sur ces cartes la , il permet de faire du 44mbit (a tester).

Quelques cartes utilisant le chipset TI ACX 100 :

- DWL 520 +
- DWL 650 +
- DWL 900 + (AP)
- WAP 11 v2 (AP)

4.3.1.3. Hermes

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

4.3.1.4. ATMEL

Chipset utilisé sur certaines cartes

4.3.2. Les Clients

4.3.2.1. Cartes PCMCIA

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

Connecteur Antenne
Généralement de type Lucent (Orinoco, avaya), MCX, MMCX il permettent de rajouter une antenne à gain, ce qui peut être intéressant si vous êtes situés assez loin d(un point d'accès par exemple.
Ce type de carte coûte généralement plus cher.
Note: Il est possible de modifier certaines cartes (D-Link DWL650 par exemple) pour rajouter un connecteur antenne, mais la garantie de la carte est bien évidemment perdue.

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 (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).

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 couvrir des distances importantes
  - Carte avec connecteur antenne et puissance importante

4.3.2.2. Cartes PCI

La différences principale entre les cartes PCI est l'antenne, qui est soit intégrée à la carte soit amovible (donc possibilité de connecter une antenne)

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)

4.3.2.3. Cartes USB

Les cartes USB de divisent en 2 grandes familles

Les cartes "adaptateur"
Un parties 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 vends une carte USB qui ressemble à un Pen-drive, donc qui peux intéresser les possesseurs de portables sans ports PCMCIA.

Un bonne parties des cartes USB sont modifiables pour y ajouter un connecteur antenne.

4.3.2.4. Cartes Compact Flash

Il y a peu de différence entre les cartes Compact Flash, si ce n'est les drivers, certains cartes sont fournies avec des drivers Windows (pour pc de bureau et portable) en plus des drivers pocket PC et d'autres juste avec les drivers pocket PC, renseignez vous avant.

Je n'ai jamais entendu parler de cartes Compact Flash avec connecteur antenne, ni de modification.
(fa)

4.3.2.5. Pont Réseau

Un pont sert à relier 2 réseaux filiaires entre eux généralement. En gros il converti les trames 802.11 en trames Ethernet donc c'est comme un fil ,un gros avantage des ponts (ou bridge en anglais) c'est qu'il na pas besoin de drivers et c'est autonome et totalement invisible niveau réseau ,aucun routage à faire ni rien.

Grâce à son invisibilité vous pouvez vous en servir pour des amplis exotiques :

Le mettre sur une PS2 pour jouez avec votre voisin. Xbox aussi grâce a son interface réseau. Le mettre sur votre imprimante.

Tous les équipements qui ont une prise RJ45 peuvent l'avoir.

Pont réseaux de chez Linksys le WET11.

4.3.2.6. Autres

4.3.2.6.1. Antenne avec module Wireless intégré

Un fabricant vends maintenant des antennes 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.

Trois versions d'antennes existent :
8 dB, 12 dB, et 18 dB.

4.3.3. Les Points d'accès

4.3.3.1. Le Linksys WAP 11

Le Linksys Wap11 est un point d'accès IEEE 802.11b.

Le WAP11 de linksys, est un AP très répandu chez les wifistes.
Il existe plusieurs versions du WAP11 la v1.1 et la v2.2.
La différence primordiale entre les deux version 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 à donc été supprimée dans la version 2.2.

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

5. La sécurité

5.1. Le WEP

WEP signifies "Wired Equivalent Privacy".

Norme de cryptage implémenté dans la norme IEEE 802.11b (WiFi)
Elle est basée sur l'algorithme de chiffrement RC4.
Le chiffrement peut être de : 64 bits, 128 bits, voir même avec divers normes propriétaires 256bit.

Les clés peuvent être statiques ou dynamiques:
Soit elles sont insérées manuellement dans la configuration des cartes et des AP.
Soit 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.
Le WEP est facilement cassable avec divers logiciels, avec le logiciel WEPCrack il faut compter 3 heures pour trouver la clef d'encryptage.

Préférez l'IPSec/VPN pour sécuriser votre réseau.

5.2. Le 802.1x et EAP-TLS

IEEE 802.1x : Port Based Network Access Control

Cette norme permet aux points d'accès WiFi de pouvoir authentifier ses clients grâce à un serveur Radius.
L'authentification est basée sur le protocole EAP qui est une extension au protocole PPP.

EAP-TLS

EAP (PPP Extensible Authentification Protocol) est la base de la norme IEEE 802.1x qui est de plus en plus utilisée dans les réseaux WiFi pour gérer l'authentification des clients.

Il existe une nouvelle version du protocole EAP développé par Cisco et Microsoft portant le nom de EAP-TLS.
Celle-ci à le net avantage d'être implantée directement dans Windows XP, de plus il existe des clients pour les autres systèmes :

- Supplicant (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.impossiblereflex.com/8021x/eap-tls-HOWTO.htm
http://www.surfnet.nl/innovatie/wlan/
http://www.freeradius.org/radiusd/doc/rlm_eap
http://www.freeradius.org/doc/EAPTLS.pdf
http://www.freeradius.org/doc/EAP-MD5.html
http://www.missl.cs.umd.edu/wireless/eaptls/?tag=missl-802-1
http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.htm

5.3. 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.

5.4. FreeRadius

FreeRadius est un serveur d'authentification Radius (Remote Authentification Dial-In User Server).
FreeRadius est sous LicenceGPL et est librement téléchargeable.

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

http://www.freeradius.org/
http://freshmeat.net/projects/freeradius/

5.5. 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 grace 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.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

5.6. Les VPN

VPN : "Virtual Private Network" = Réseaux Privés Virtuels

Le standard IPSec (normalisé par l'IETF) permet la création de réseaux privés virtuels.
Les passerelles VPN permettent de créer ces réseaux de manière transparente pour les réseaux existants.
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).

Source: http://www.idealx.com/solutions/vpn.fr.html (pr)

5.7. Analyse de la sécurité

5.7.1. 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 vité 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.

5.7.2. Le cryptage WEP

5.7.2.1. 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.

5.7.2.2. 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.

5.7.3. 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.

5.7.3.1. 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 œuvre 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.

5.7.3.2. 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 œuvre 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 œuvre 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.

5.7.4. Ce qu'il y a de sûr

5.7.4.1. 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 connections 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.

5.7.4.2. 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.

5.7.5. 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 œuvre, 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.

5.7.6. 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 cablé 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. Configuration

6.1. 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 .

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

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

(ka)

6.2. 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 recoit 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 server DHCP sans cryptage wep, les intrusion seront grandement simplifiées.

Configuration

Notion de plages

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

Un plage ressemblera à ça:

Adresse de départ: 192.168.1.20
Adresse de fin: 192.168.1.50

Le nombre maximal de pcs recevant leurs paramètres par DHCP seront donc de 30 (50 - 20).

Notez que cela ne correspond en aucun cas au nombre maximum de pcs pouvant se connecter à votre réseau mais seulement au nombre de pcs 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 ca.

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.

7. 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 plus 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.

8. Mise en pratique, tests

8.1. 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 réaliser une liaison wireless sur une distance de 5km.

dBm = 10 * Log10(P/0,001)
P en Watts

Voici le matériel dont nous disposons :
2 Points d'accès Linksys WAP11 (puissance 100mW soit 20 dBm par AP)
2 antenne Paraboles SD27 (gain 24 dB par antenne)
2 câbles AIRCOM de 2m (perte -0,44 dB par câble)
4 connecteurs (perte – 0,5 dB par connecteur)

Rappels sur le câblage :

Type de câble	*Perte /m*
RG 174	- 2 dB
RG 58	- 1 dB
RG 213	- 0,6 dB
AIRCELL	- 0,38 dB
LMR-400	- 0,22 dB
AIRCOM	- 0,21 dB

Nota : lorsque 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)

LP = 114 dB

Distance en km

Fréquence en Mhz

Puissance reçue

Pr = Pt – Lp + Gt + Gr + Lt + Lr

Pr = 20 – 114 + 24 + 24 + (- 0,44 – 1) + (-0,44 - 1)

Pr = -48.88 dBm

Pr = puissance reçue (dbm ou dbw)
Pt = puissance de l'émetteur en dbm ou dbw
Lp = Atténuation de parcours
Gt = gain de l'antenne en émission de dBi
Gr = gain de l'antenne de réception en dBi
Lt = perte du câble coté émission (dB)
Lr = perte du câble coté réception (dB)

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)

(graphique page suivante)

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

- pour du matériel de base : environ 1,5km
- 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.

Tests :

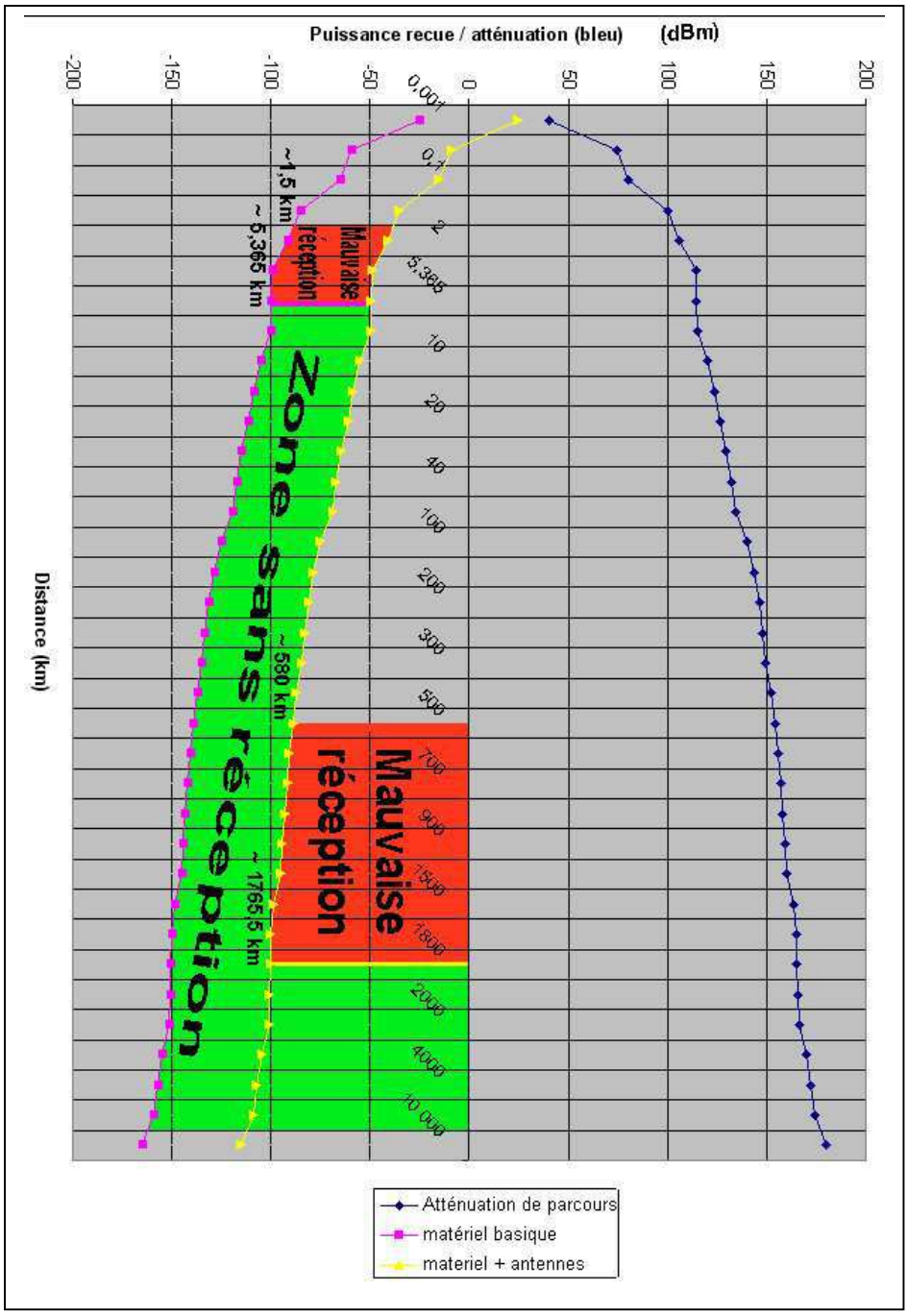
La distance maximum réalisée pour le moment est de 108 km avec amplification (1 W) et au dessus de l'eau avec un débit d' 1 mbit/s.

Sans antenne et avec des cartes d'une puissance de 30 mW nous avons réalisé une distance de 950 m avec un débit de 200ko/s sur un transfert FTP.
Matériel utilisé :

- 1 carte PCI Linksys WMP11
- 1 carte Usb Actiontec

Nous n'avons pas pu tester sur une plus grosse distance à cause d'obstacles.

Voici le graphique de distance maximale exploitable en milieu parfais.


Puissance recue / atténuation (bleu) (dBm)
-200
-150
-100
-50
0
50
100
150
200
Distance (km)
0,001
0,1
2
5,365
10
20
40
100
200
300
500
700
900
1500
1800
2000
4000
10 000
~1,5 km
~ 5,365 km
Mauvaise réception
Zone sans réception
~ 580 km
~ 1765,5 km
Mauvaise réception
Atténuation de parcours
matériel basique
materiel + antennes

(fa)

8.2. Configuration avancée d'un AP/Routeur Linksys BEFW11S4

Introduction

Je vais vous décrire comment installer et configurer votre point d'accès Linksys BEFW11S4 v2 de la manière la plus complète possible.
Le Linksys BEFW11S4 est un point d'accès pouvant de connecter à un modem cable/dsl (notamment) et pouvant faire office de switch 4 ports.

Installation

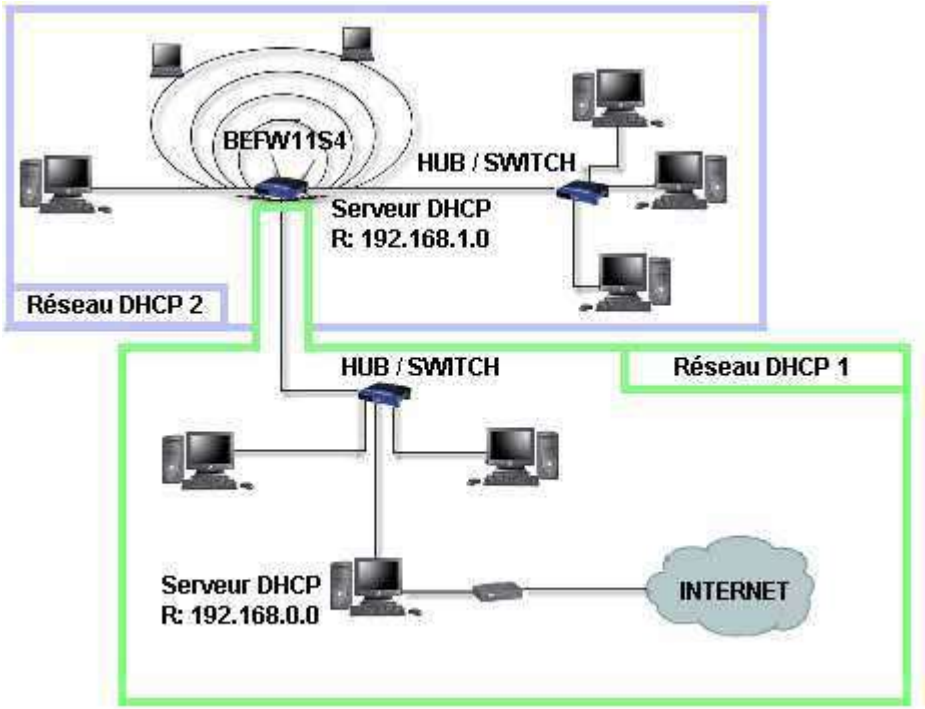
L'installation est on ne peux plus simple, sortez le point d'accès de la boite et branchez-le. Un server DHCP est configuré de base, il vous suffit donc de vous connecter à son réseau (Wireless ou filaire) pour le configurer.

Configuration

Tout d'abord ouvrez votre navigateur internet préféré et tapez l'adresse suivante: 192.168.1.1 un login et un mot de passe vous seront demandés, entrez simplement "admin" comme mot de passe.
Vous arriverez sur cette page:

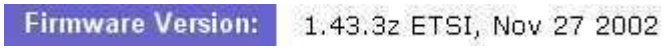
- **Page Setup**

Ces options sont celles qui peuvent être demandées par les FAI (Fournisseur d'Accès à Internet, ISP en anglais) mais elles sont surtout utiles dans le cas de la connexion du routeur à un réseau local. Comme sur le schéma ci dessous:

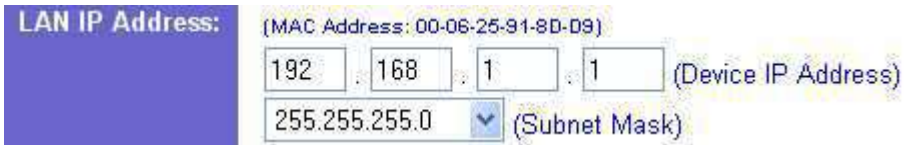


Exemple pratique:

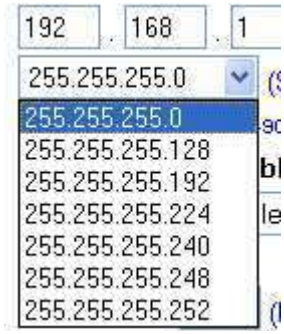
Si un poste du réseau DHCP 1 veut accéder au server ftp d'un poste du réseau DHCP 2 (abordé par la suite) elle doit entrer l'adresse IP du BEFW11S4 qui change en fonction de la durée d'allocation d'une adresse en DHCP, si un nom est configuré il lui suffit de rentrer ftp://nom_du_routeur et elle sera automatiquement redirigé vers le server FTP, elle n'aura pas a chercher l'adresse du routeur.



Version du firmware installé sur le routeur, des firmware sont disponible sur le site de Linksys (www.linksys.com).

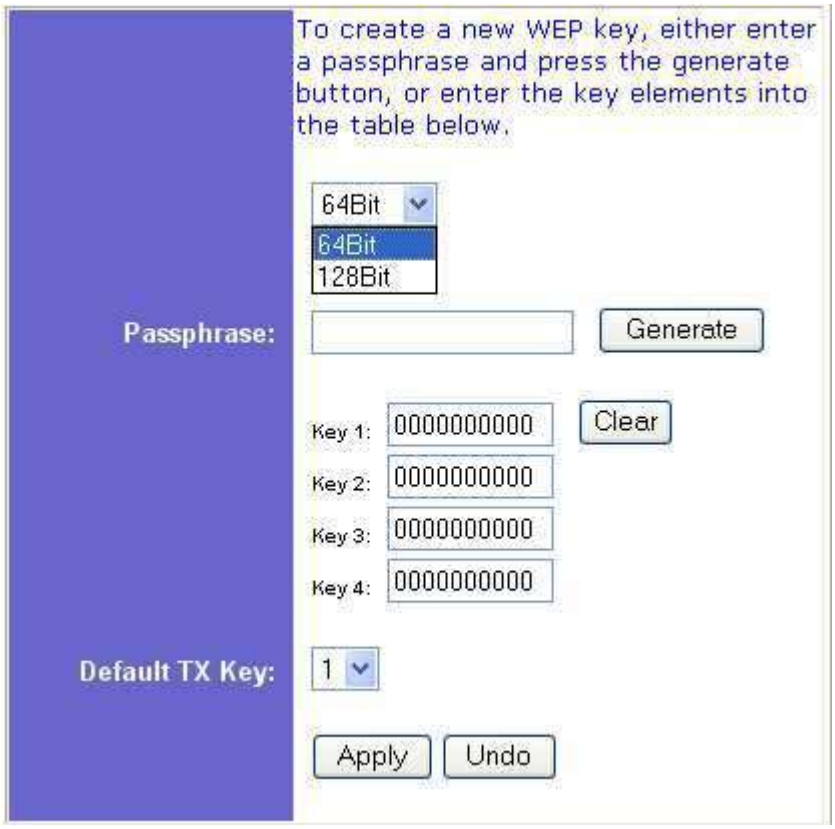


L'adresse MAC est une adresse unique qui ne peux (ne doit pas plutot) être modifiée au risque de ne plus être unique et de créer un conflit si elle doit communiquer avec une carte ayant la même adresse MAC. Vous pouvez choisir l'adresse IP qu'aura votre routeur (sur son réseau local, partie violette sur le schéma si dessus).



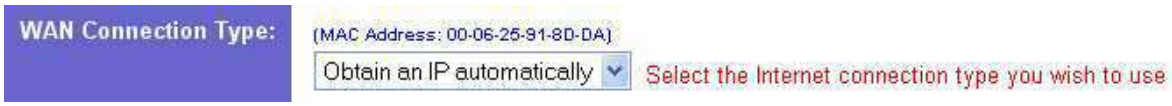
Pour la selection du masque, les personnes ayant un minimum de connaissances réseau se rendront tout de suite compte que le routeur ne peux communiquer sur son interface locale qu'avec un maximum de 252 postes (0, 255 et adresse du routeur exclue) ce qui est largement suffisant.

Cette partie sers à la configuration du réseau Wireless. SSID Broadcast signifie que le routeur accepte les connection provenant de quelqu'un ayant configuré ANY comme SSID, si cette option est "disable" les personne voulant se connecter à l'aide d'un utilitaire de scan (comme celui fourni avec windows XP) ne verront pas le point d'accès (cela ne représente pas vraiement une sécurité).

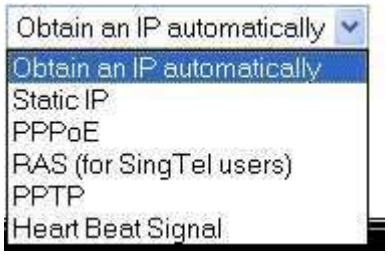


Configuration des paramètres WEP.

Pour les autres options de configuration reportez vous aux autres sections de ce Ebook.



Ceci est la partie la plus interessante de cette section, permet de selectionner de quelle manière sera relié le routeur au reste du monde (par l'intermédiaire de la prise WAN). Selectionnez cette option si votre routeur est connecté à un autre réseau attribuant les adresses en DHCP (comme pour le schéma plus haut).



Voici les autres options:

- Static IP: principalement connection du routeur à un autre réseau n'ayant pas d'attribution dynamique d'adresses IP
- PPPoE: Connection du routeur à un modem (RJ45)
- RAS: Connection du routeur à un modem (RJ45)
- PPPTP: Connection du routeur à un modem (RJ45)
- Heart Beat Signal: Connection du routeur à un modem (RJ45)

Pensez bien à appliquer vos modifications.

- **Page Password**

Permet de changer le mot de passe que vous avez entré au tout début (fortement conseillé)

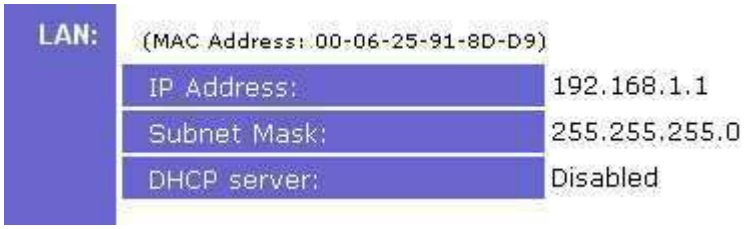
Autoriser UPnP

Permet de remettre à zéro toutes les modifications que vous avez faites sur le routeur (le bouton reset se contentant de remettre à zéro qu'une partie du routeur).

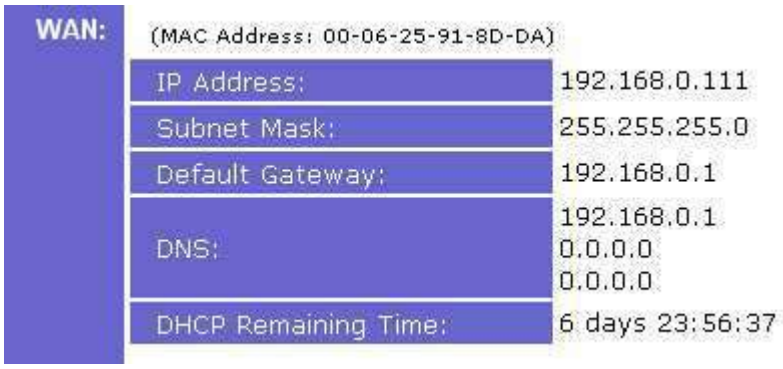
- **Page Status**

Cette page permet d'afficher en temps réel les informations sur la configuration du routeur

Informations classiques.



Informations sur la configuration de l'interface local du routeur.



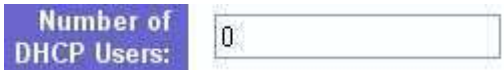
Informations sur l'interface WAN du routeur.

- **Page DHCP**

Cette page permet de configurer toutes les options relatives au server DHCP pour votre réseau local.

Activer ou non le server DHCP.

Adresse de début de la plage d'adresses DHCP.

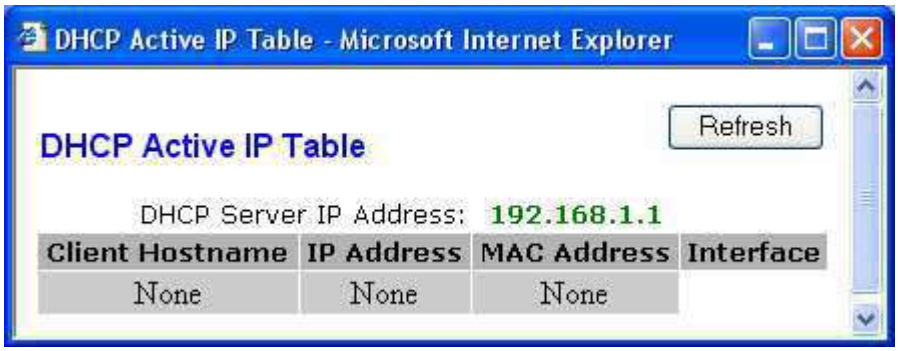


Nombre de postes en DHCP sur le réseau. La plage sera définie en fonction de l'adresse de début et du nombre de postes.

Durée pendant laquelle une adresse IP sera réservée à un poste (depuis sa dernière déconnecion) si ce dernier ne se connete pas et dans la mesure ou toutes les autres adresses IP ne sont pas prises.

Informations qui seront envoyées aux postes clients, inutile si le routeur reçoit déja ses informations (WAN) d'un server DHCP, ou si il y a un autre DNS ou proxy sur le réseau local.

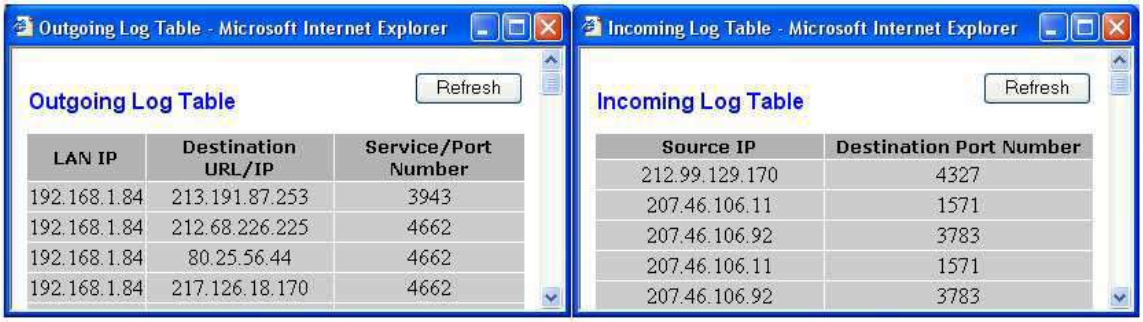
- DHCP Client Table



Affiche les clients ayant recut leur configuration via DHCP (le server DHCP étant ici désactivé aucun client n'est affiché).

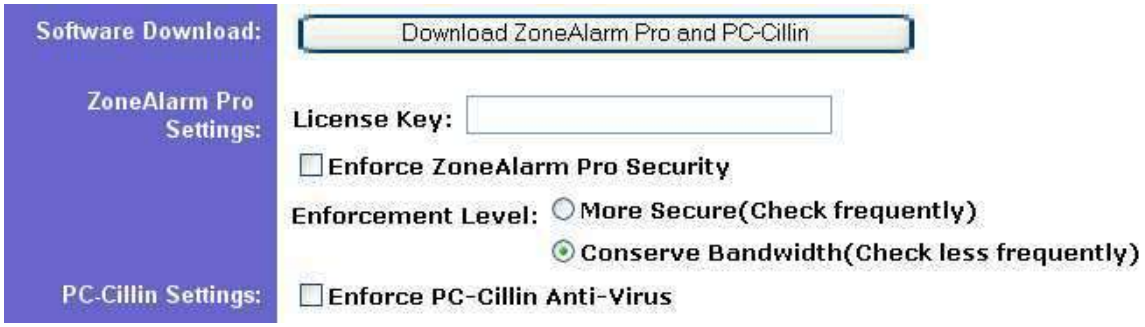
- **Page Log**

Le logging permet de vérifier les trames circulant entre le réseau local et le WAN. Il est important de rappeller que le Logging ne doit s'effectuer que pour résoudre des problèmes et non pour espionner les usagers (ce qui est interdit par la loi).



Pages Logs sortants et entrants.

- **Page Security**



Il est possible de coupler le routeur à utilitaires (PC Cillin et Zone Alarm Pro).

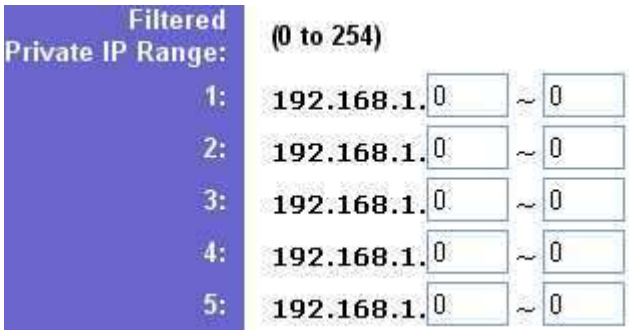
Vous pouvez empecher certaines adresses d'acceder à internet (plus précisément à tout ce qui est branché à partir de la prise WAN)

Vous pouvez utiliser le controle de contenu AOL.

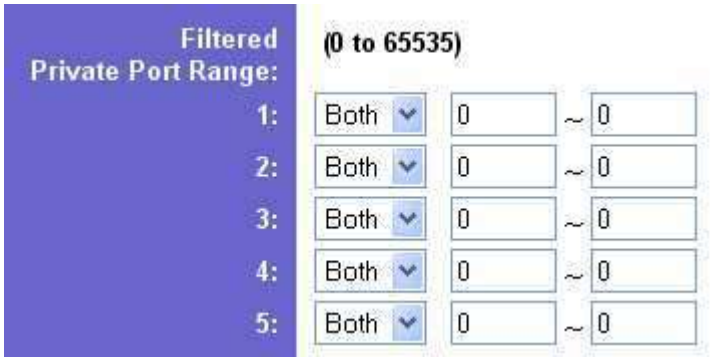
- **Page Help**

Depuis cette page vous pouvez changer de version de Firmware (en selectionnant ce dernier sur votre disque dur).
Les paramètres avancés permettent de configurer le routeur de manière plus précise.

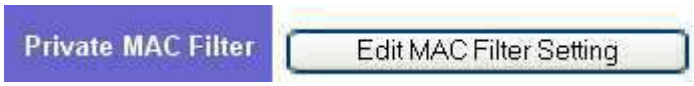
- **Page Advanced**
  - **Section Filters**

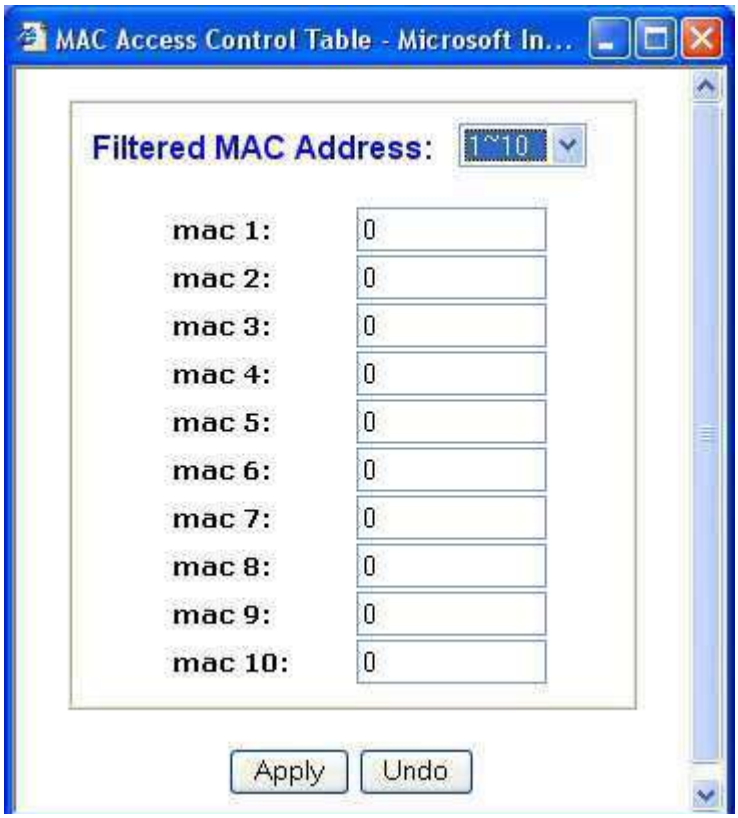


Vous pouvez interdire l'accès à internet à certains de vos postes.



Permet de bloquer certains ports, pour empecher vos utilisateurs à acceder à certaines ressources d'internet (FTP, kazaa, ... par exemple).





Cette option permet d'interdire l'accès à internet à certains postes en précisant leur adresse MAC, plus fiable que la méthode avec les adresses IP, possibilité de bloquer jusqu'a 50 adresses MAC.

Block WAN Request: ○ Enable ◉ Disable

Bloque les requètes provenant de la connexion WAN.

Multicast Pass Through: ◉ Enable ○ Disable

Autoriser le passage de requêtes multicast

IPSec Pass Through: ◉ Enable ○ Disable

Autorise l'utilisation d'IPSec entre le réseau local et le WAN.

PPTP Pass Through: ◉ Enable ○ Disable

Autoriser le PPTP.

Remote Management: ○ Enable ◉ Disable Port: 8080

Permet d'accéder à l'interface de configuration depuis internet (ou réseau local connecté au WAN). Pensez à configurer le Port (attention aux conflit qui peuvent être crées avec la section forwarding. Vous pourrez configurer en tapant l'adresse suivante: http://adresse_wan_routeur:port

Remote Upgrade: ○ Enable ◉ Disable

Permet de changer le Firmware depuis internet (ou réseau local connecté au WAN).

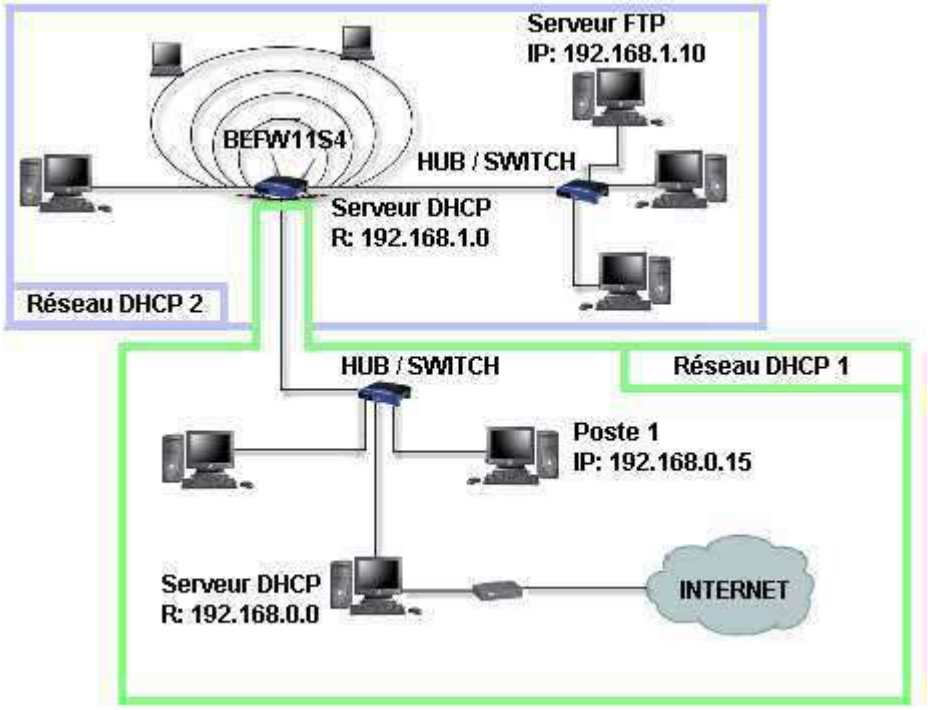
MTU: ◉ Enable ○ Disable Size: 1492

Configuration du MTU

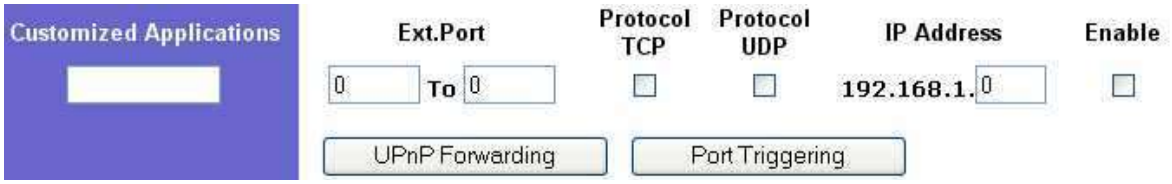
- **Section Forwarding**

Le forwarding permet de faire une redirection depuis le routeur vers un des postes du réseau local.

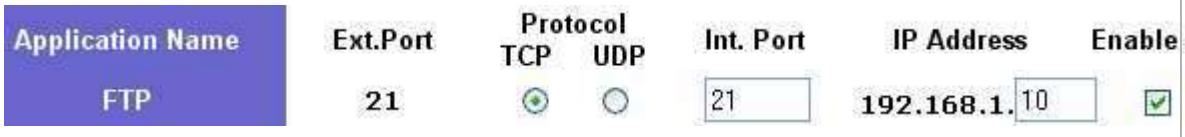
E



Le poste 1 désire accéder au serveur FTP situé sur le Réseau DHCP 2, il doit donc passer par le routeur, pour que tout fonctionne ce dernier doit être en mesure d'interpréter les informations venant du poste 1, il suffit donc de remplir ce formulaire:



En cliquant sur UPnP Forwarding vous trouverez des formulaires pré remplis avec les forwarding les plus couramment rencontrés.



En littéral ça donne (pour le routeur):
Quand je reçoit une requête sur le port 21 (port réservé au FTP) je renvoie les données vers le réseau local sur le port 21 à l'adresse 192.168.1.10 en utilisant le protocole TCP.

N'oubliez pas d'activer l'option.

On va maintenant faire un petit exercice pour voir si vous avez compris.
Remplissez la feuille avec les réponses sur problème suivant:

Nous désirons jouer à quake 3 sur tout le réseau, mais le poste 1 n'arrive pas à accéder à notre serveur ayant pour adresse 192.168.1.101 (note: port: 27960 protocole: UDP)

R

Notes: vous trouverez les informations relatives aux ports et protocoles utilisés par les application en faisant une simple recherche sur internet.

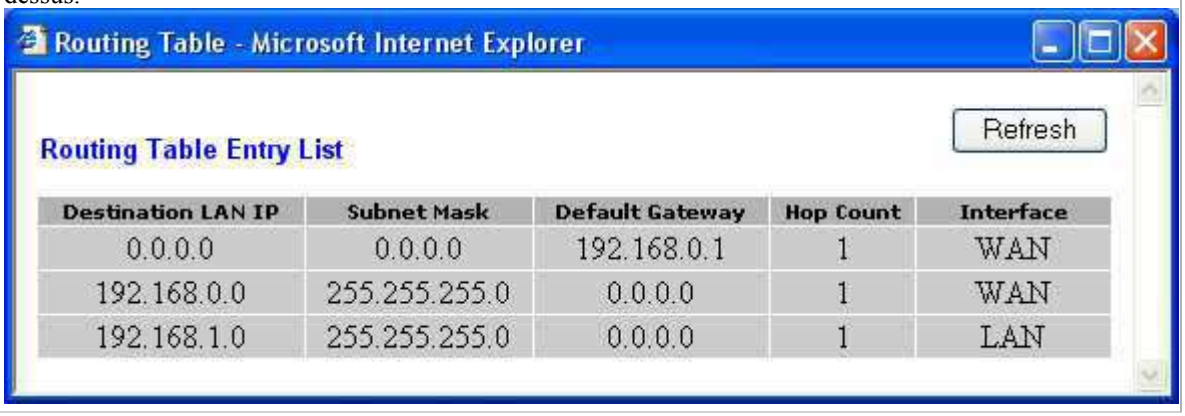
C

- **Section dynamic Routing**

Ici vous pouvez activer le routage (protocoles RIP-1, RIP-1 Compatible, RIP-2) en Transmission (TX) ou en Reception (RX)

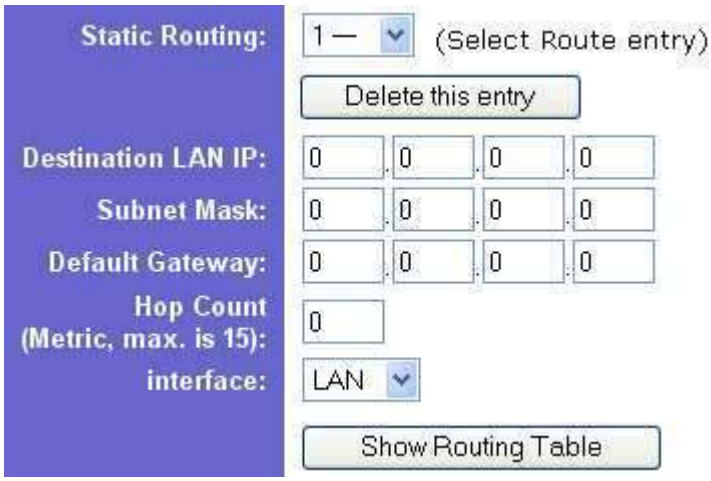
I s attention au Working Mode, si vous mettez Gateway il vous sera nécessaire de configurer le forwarding (voir plus haut) mais vos client DHCP recevront toutes les informations relatives à leur connexion Internet par exemple. Si vous sélectionnez routeur, plus besoin de forwarding mais vous devrez reconfigurer le serveur DHCP, sinon vos clients n'auront plus accès à Internet (dans le cas du schéma ce dessus).

C principalement si le routeur est utilisé dans un cas similaire à celui du schéma ci dessus.

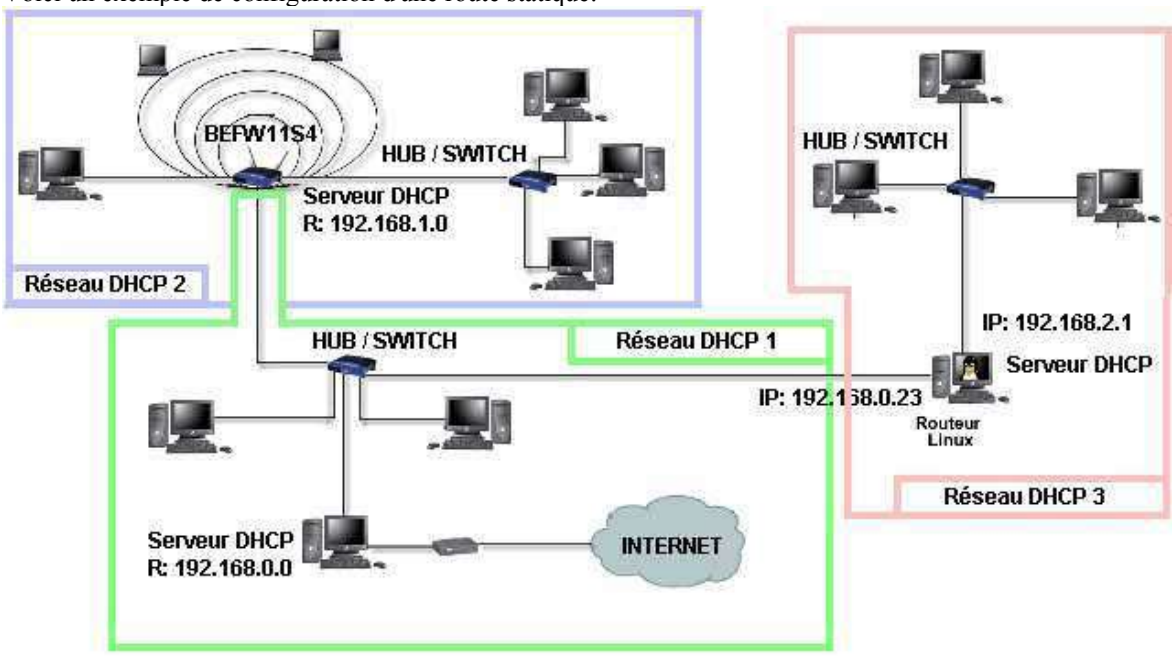


Vous pouvez aussi afficher la table de routage actuellement configurée sur le routeur.

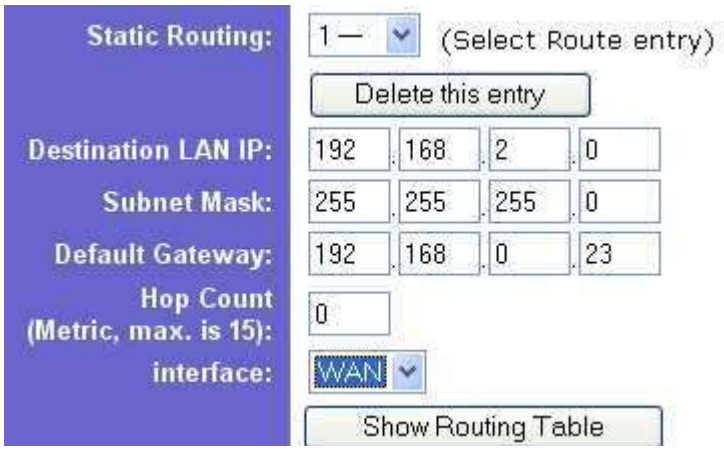
- **Section Static Routing**



Voici un exemple de configuration d'une route statique:



Nous désirons permettre au réseau DHCP 2 d'accéder au réseau DHCP 3 pour cela il faut que la route indique l'adresse de la passerelle vers le réseau DHCP 3 (192.168.2.0).

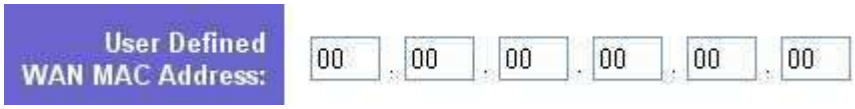


Vous trouverez plus d'informations sur le routage statique sur le site www.commentcamarche.com

- **Section DMZ Host**

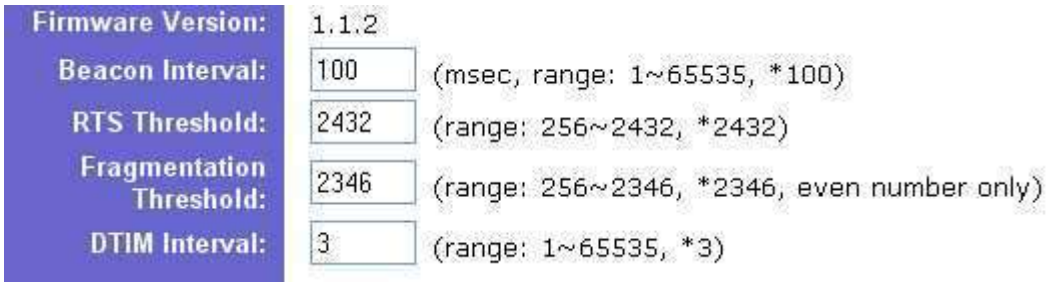
Serveur en zone démilitarisée

- **Section MAC Adress Clone**

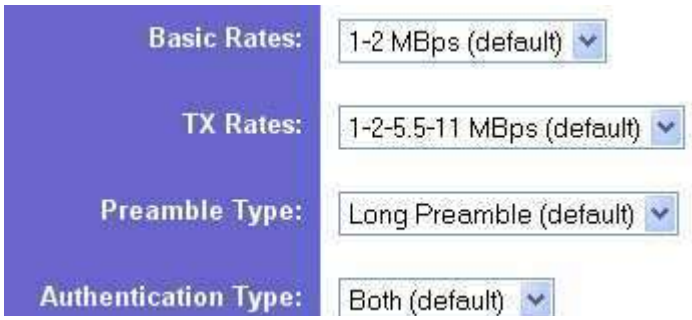


Vous pouvez changer l'adresse MAC de l'interface WAN (fortement déconseillé)

-
- **Section Wireless**



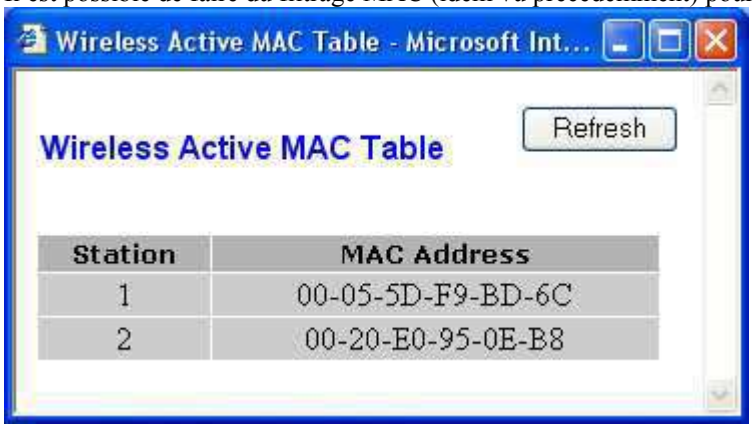
Options de configuration wireless



Taux de transfert et authentification

Possibilité de sélectionner les antennes

Il est possible de faire du filtrage MAC (idem vu précédemment) pour le réseau wireless seulement.



Liste des tout les adresses MAC des postes connectés en wireless au point d'accès.

Conclusion

Ce point d'accès routeur est très intéressant du fait de son (très) faible coût par rapport aux autres marques (150 euros) et permet de réaliser une configuration assez (voir très) complète le seul point négatif étant l'absence de manuel complet expliquant sa configuration (juste un manuel de démarrage rapide) mais maintenant le problème est réglé :) .

(fa)

8.3. 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.

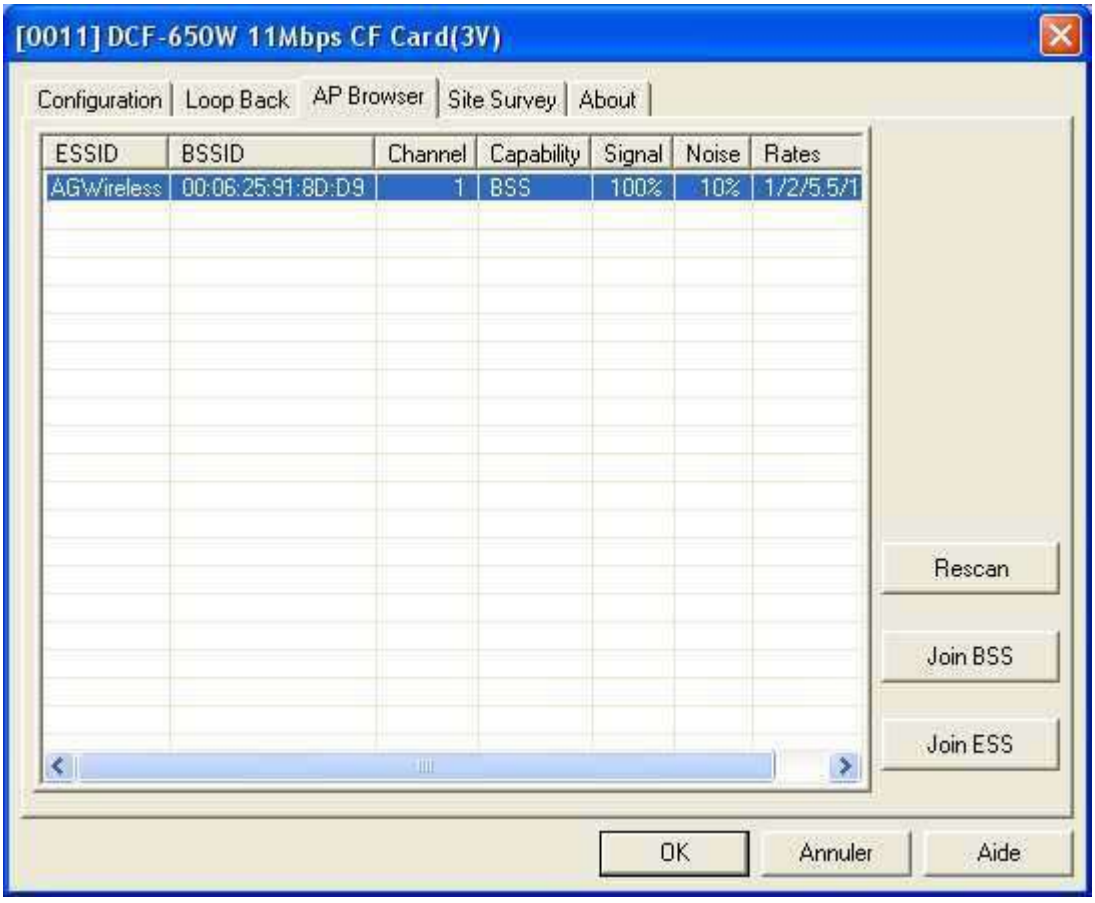
- Lors de la configuration d'un réseau avec AP (point d'accès), il est important de configurer tout d'abord un poste qui servira à configurer le point d'accès.

---

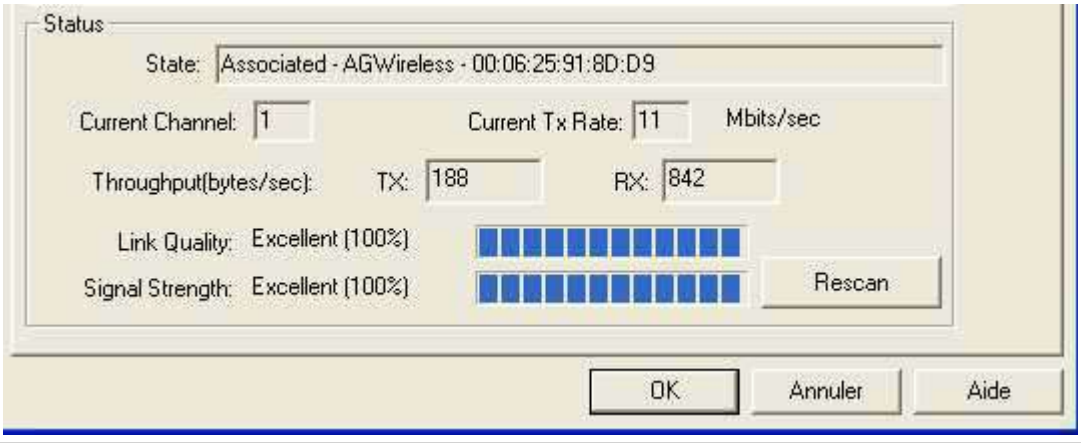
3) Configuration du premier PC

- 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:

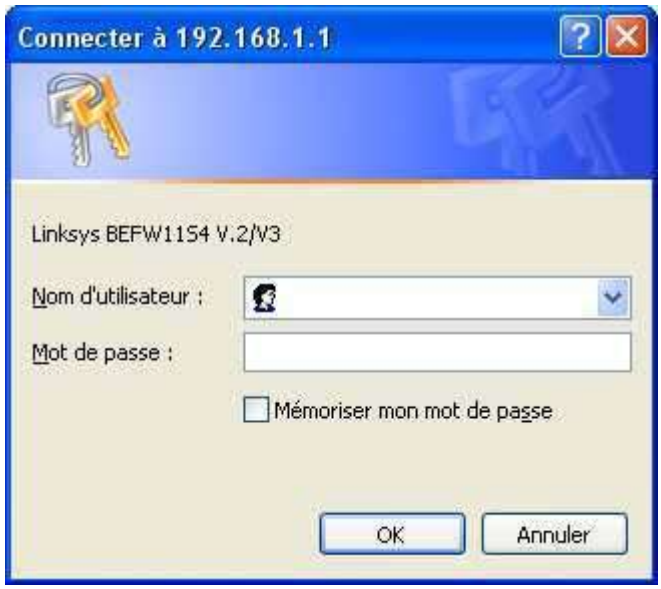


- Cliquez sur "Join" pour vous connecter. Allez dans l'onglet de votre logiciel qui affiche les statuts de la connexion:



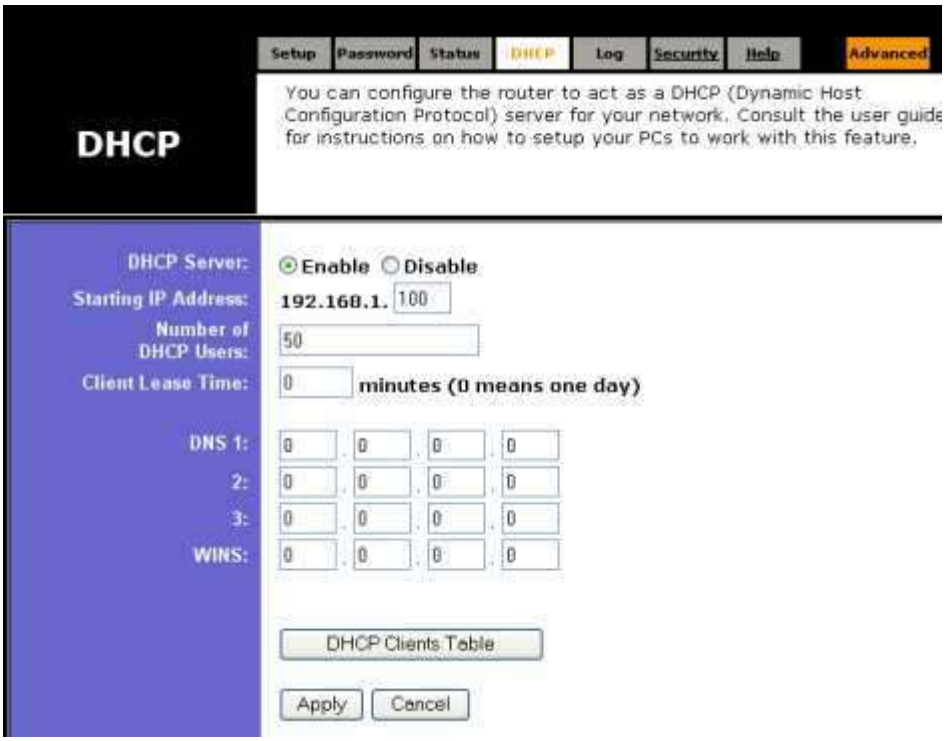
4) Configuration du point d'accès

- 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 PCs 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 PCs connectés en RJ45 ou des PCs 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

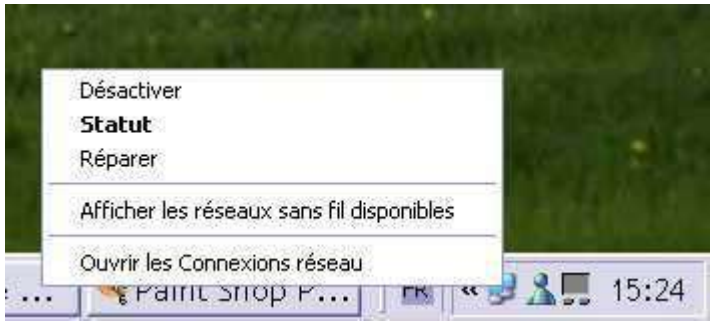
5) Configuration d'une machine cliente

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.



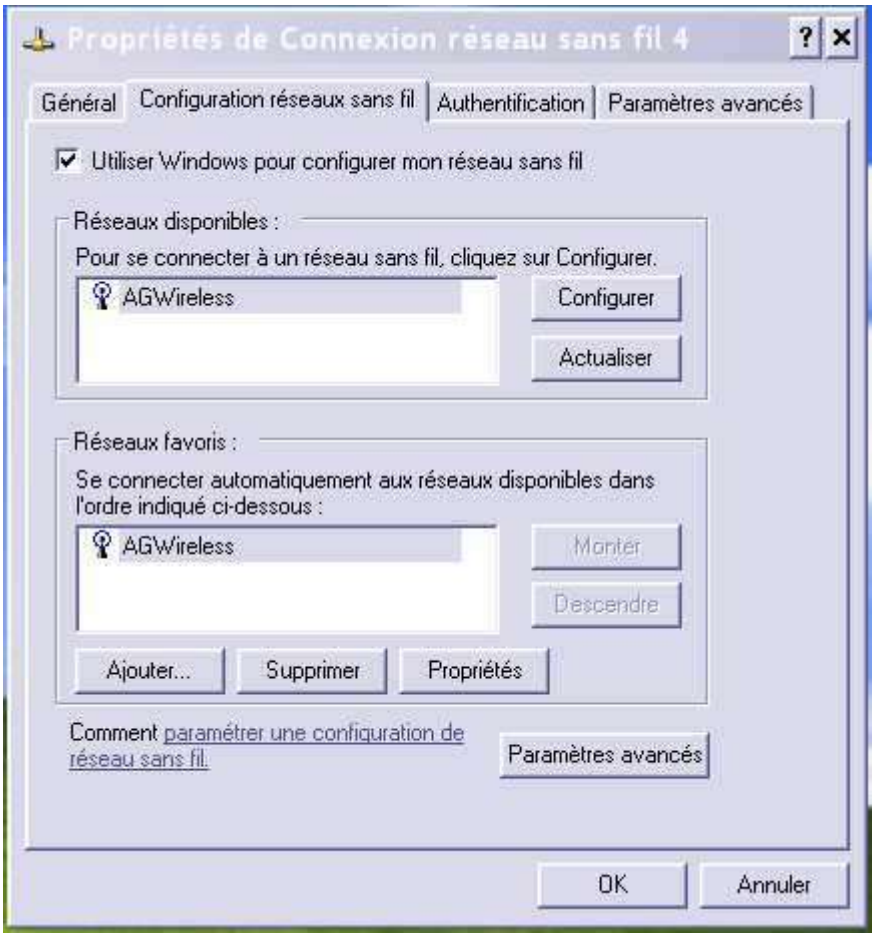
- Et sélectionnez "afficher les réseaux sans fil disponible".

- Cliquez sur connexion et le réseau wireless est configuré.

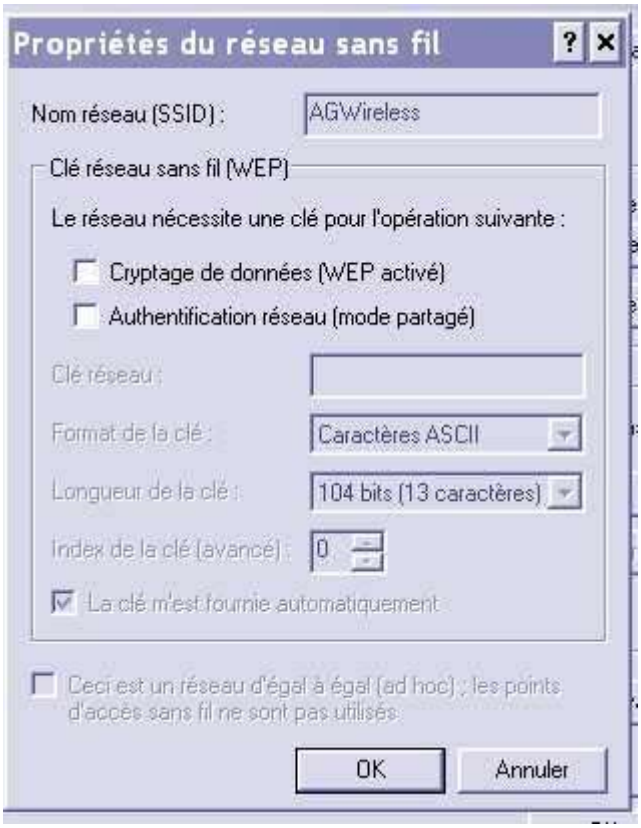
6) Configuration du WEP.

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.

---

7) 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 hub/switchs pour arriver à un total maximal de 253 PCs (déconseillé), en ce moment l'AP que vous avez vu en photo fait serveur DHCP pour 15 PCs (12 en RJ45, 3 en Wireless)

(fa)

8.4. Installation détaillée d'un réseau sans Point d'accès (Ad Hoc)

1) Introduction

Cet article s'adresse à tout le monde, aucune connaissance technique n'est requise.
Le matériel qui va être utilisé pour cet article est le suivant:

- 1 carte Compact Flash DCF650W
- 1 carte PCMCIA Sitecom

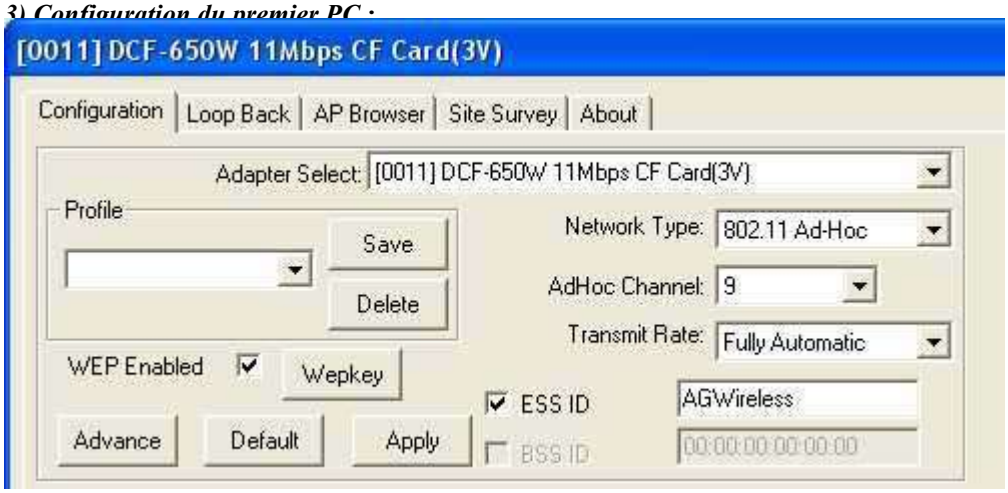
2) Installation du matériel

- Tout d'abord installez les pilotes des cartes wireless, ainsi que le logiciel généralement fourni.
- Vous pouvez vérifier si la carte est bien installée en faisant clic droit sur le 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.

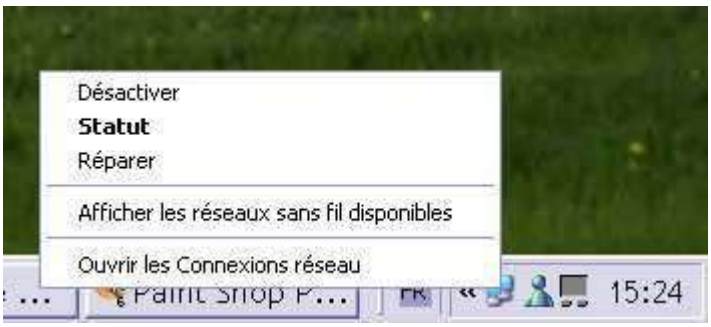
---

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:

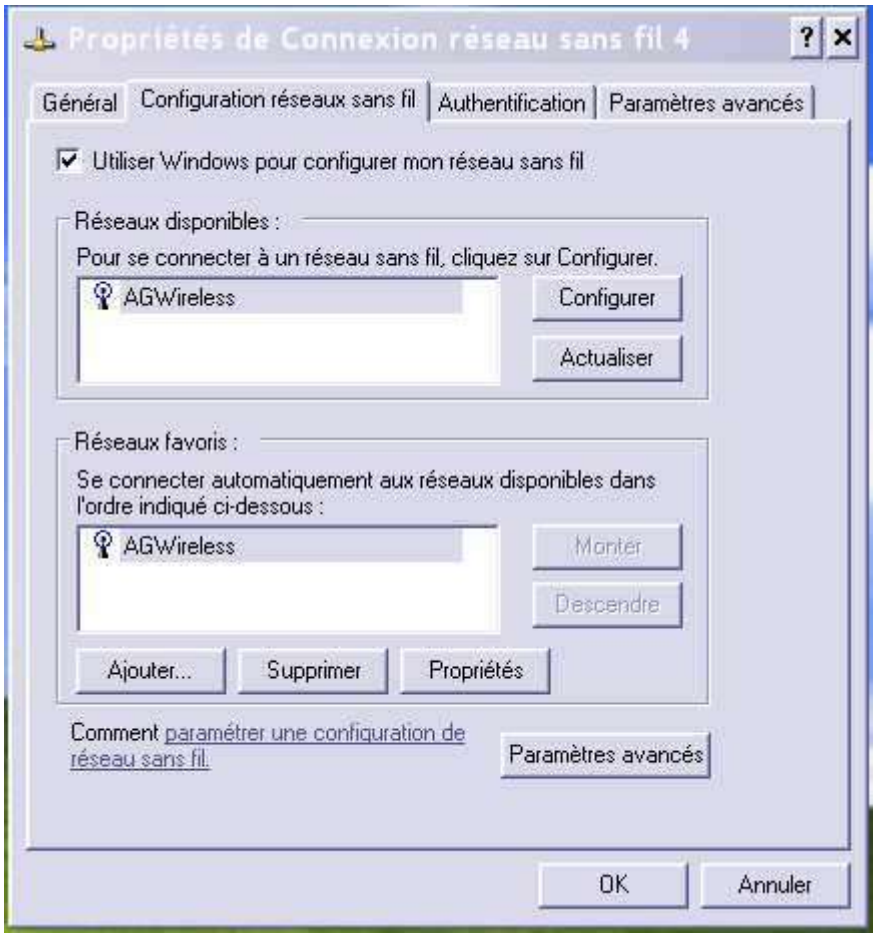
- Faites un clic droit sur l'icône avec les 2 ordinateurs.



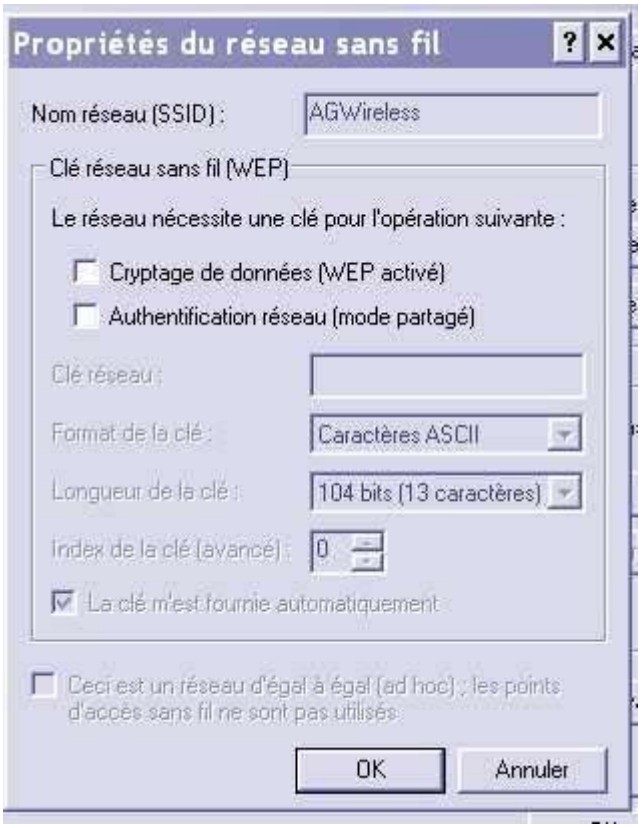
- Et sélectionnez "Afficher les réseau sans fil disponible".

- 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.

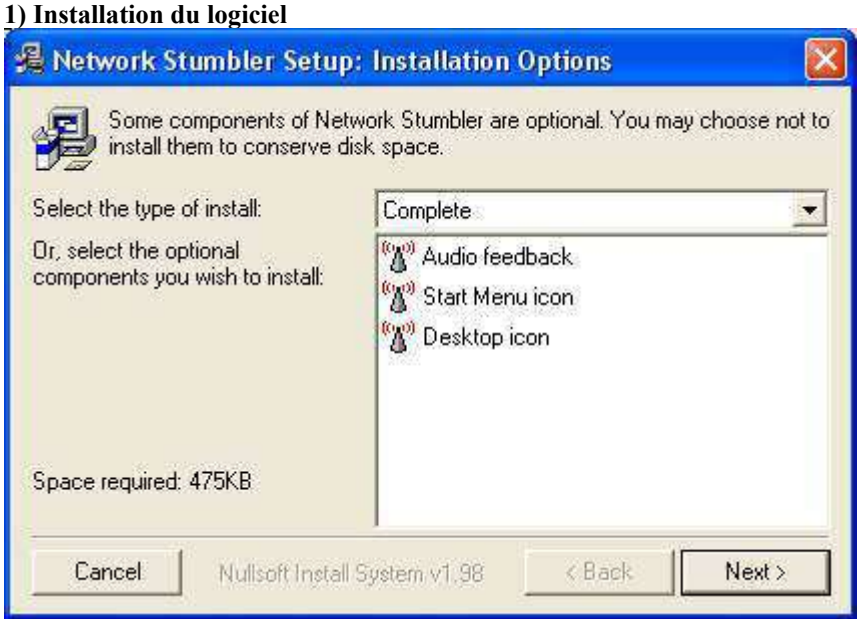
Note :

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)

8.5. Utilisation de NetStumbler

1) Installation du logiciel

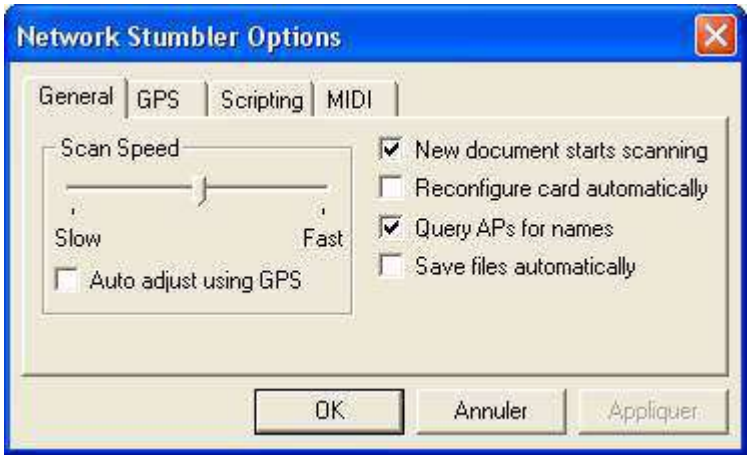


Lors de l'installation il est important et surtout pratique de sélectionner l'option "Audio feedback".

2) Configuration

Pour configurer le logiciel allez dans l'onglet "view" puis "options".

a) Général



- Scan Speed

Permet de sélectionner la vitesse des écoutes, l'option "Auto adjust using GPS" permet de réaliser une écoute en même temps qu'une synchronisation GPS, assez pratique car évite de réaliser une écoute wireless si le GPS n'est pas synchronisé avec des satellites.

- New document start scanning

Commence une écoute sur une page vierge et non la dernière ouverte.

- Reconfigure card automatically

NetStumbler reconfigure la carte pour réaliser les écoutes dans les meilleures conditions possibles.

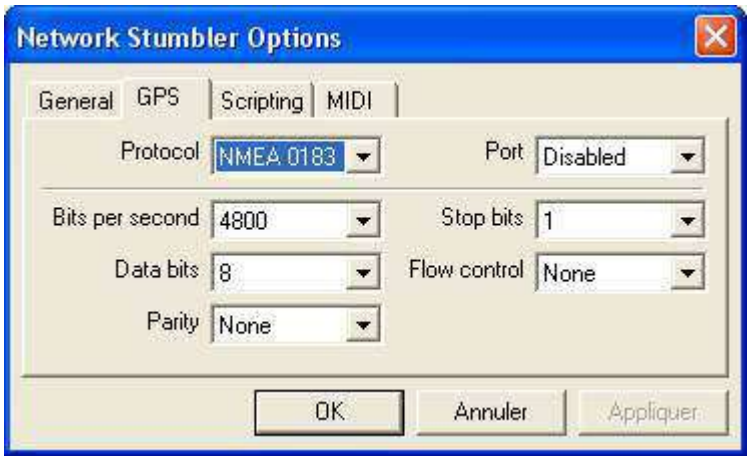
- Query APs for names

Correspond en quelque sorte à un "Whois", permet d'afficher le nom des APs (point d'accès) et pas seulement leurs adresses MAC (adresse physique).

- Save files automatically

Enregistre automatiquement les fichiers d'écoute.

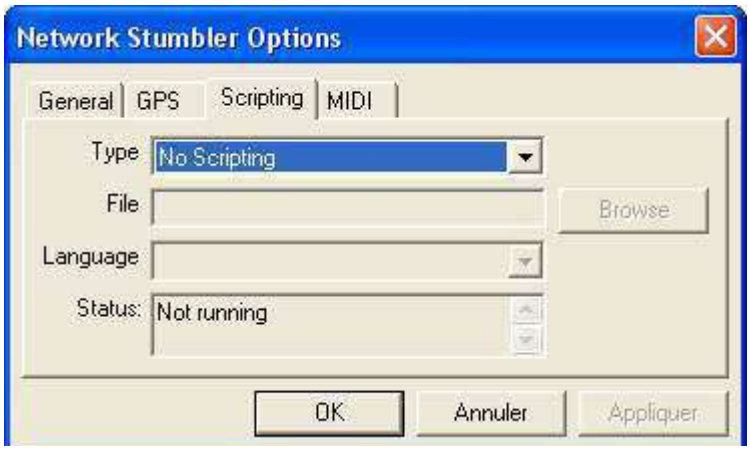
b) GPS



Options permettant de configurer le GPS, dépend surtout du GPS que vous utilisez, voici celles que j'ai utilisé avec un GPS USB:

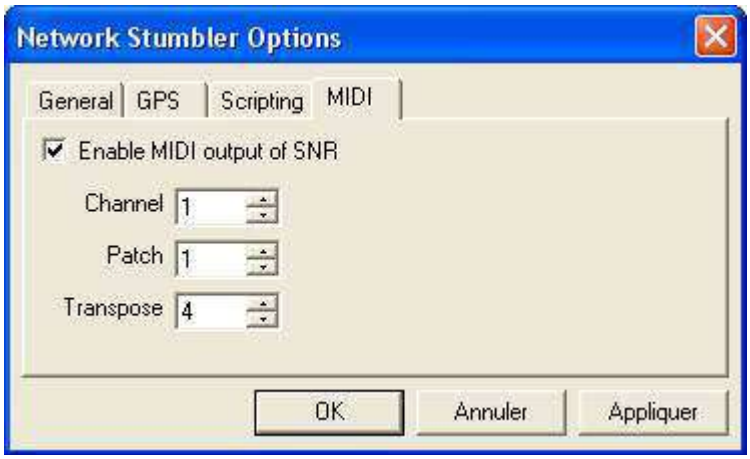
- Protocol: NMEA 0183
- Port: COM3 (correspondant a l'usb chez moi)
- Stop bits: 1
- Data bits: 8
- Flow control: None
- Parity: None

c) Scripting



Permet d'utiliser des scripts dans **NetStumbler**.
Voici une petite documentation sur le "Scripting" avec **NetStumbler** :
http://www.stumbler.net/scripting.html
Netstumbler gère le JScript et le VBScript.

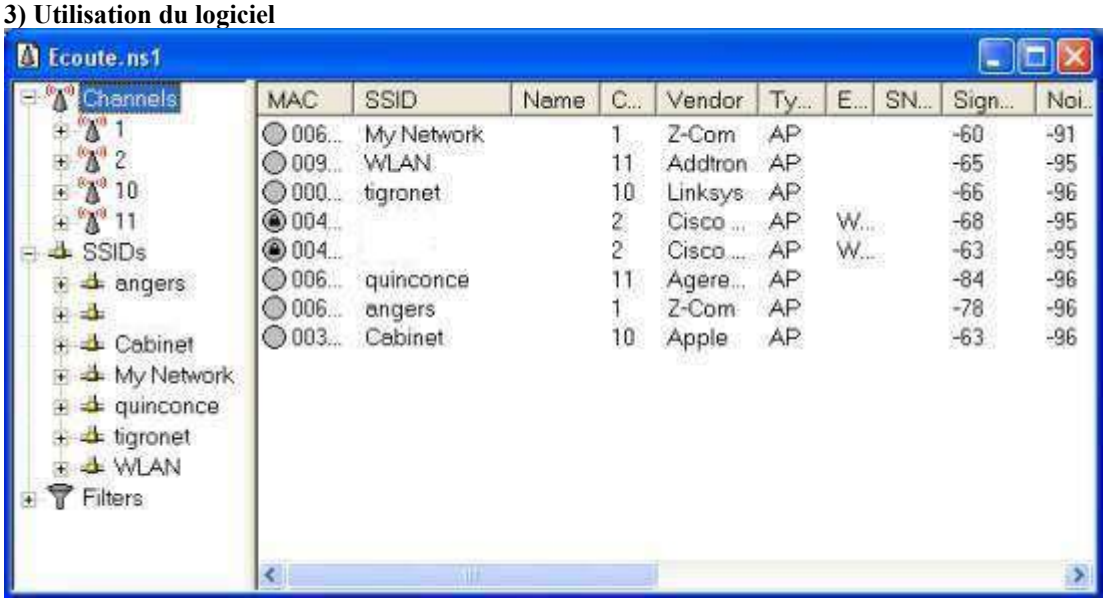
d) MIDI



Permet de sortir du son en fonction de la qualité du signal, très pratique lors d'un écoute avec le portable dans le sac à dos par exemple. Channel, Patch et Transposent modifient le son (tonalité principalement).

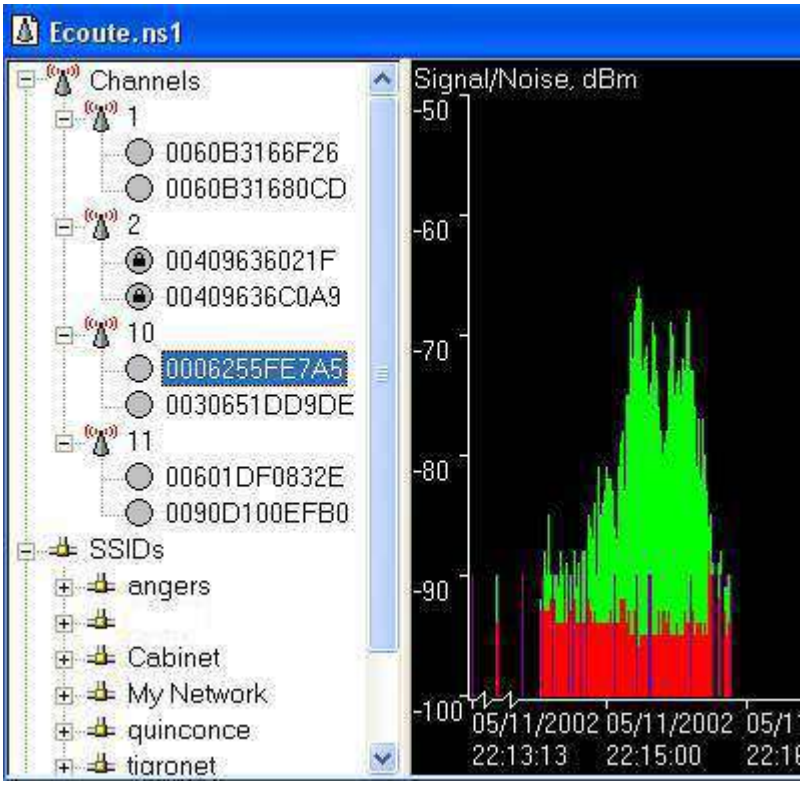
---

3) Utilisation du logiciel



Les points d'accès listés ci dessous appartiennent à l'association et ont étés mis en place pour une session de tests. Lors d'une écoute vous pouvez voir cette fenêtre qui référence toutes les infos concernant les points d'accès détectés.

- Si vous voyez un petit cadenas, cela indique que le réseau est crypté (WEP)
- Si vous cliquez dans l'arborescence sur un point d'accès vous pouvez obtenir une courbe de signal comme celle-ci:



- Avec la qualité du signal sur la droite. Il est important de noter que si la qualité du signal avoisine les 90 dBm, le réseau est inexploitable tel quel.

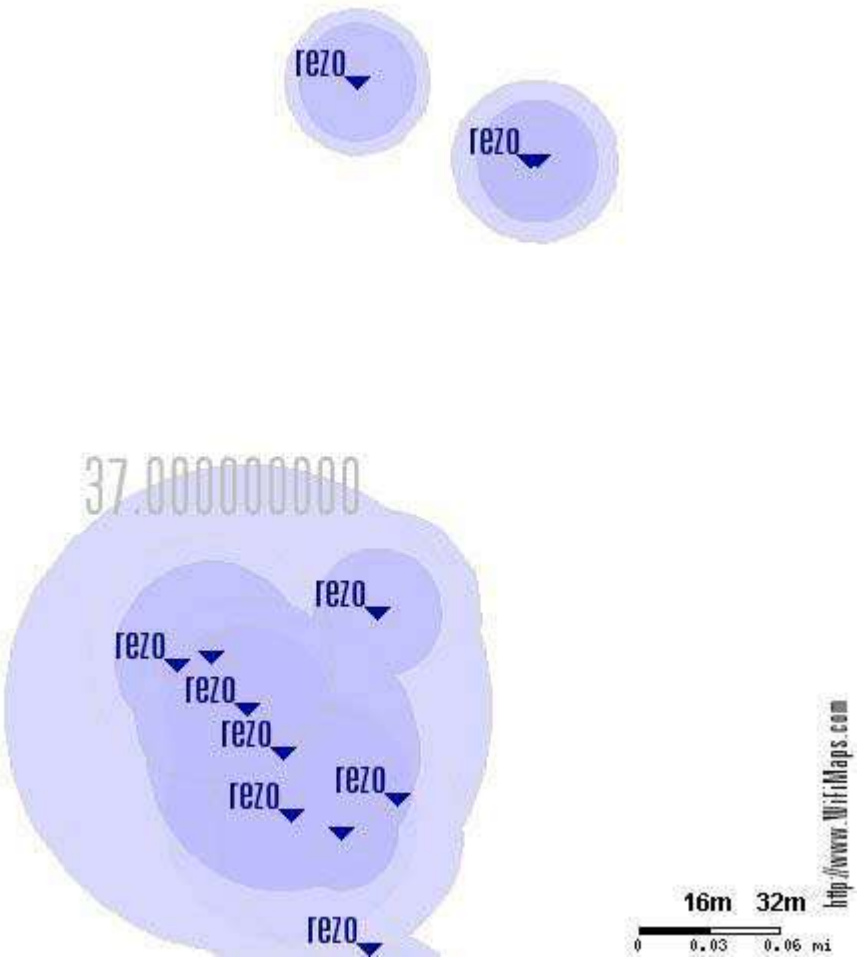
- Vous pouvez exporter vos écoutes, principalement pour les traiter avec un logiciel les couplant à une carte (Microsoft Map Point 2OO2, WifiMaps, ...)

Le fichier de sortie aura cette forme:

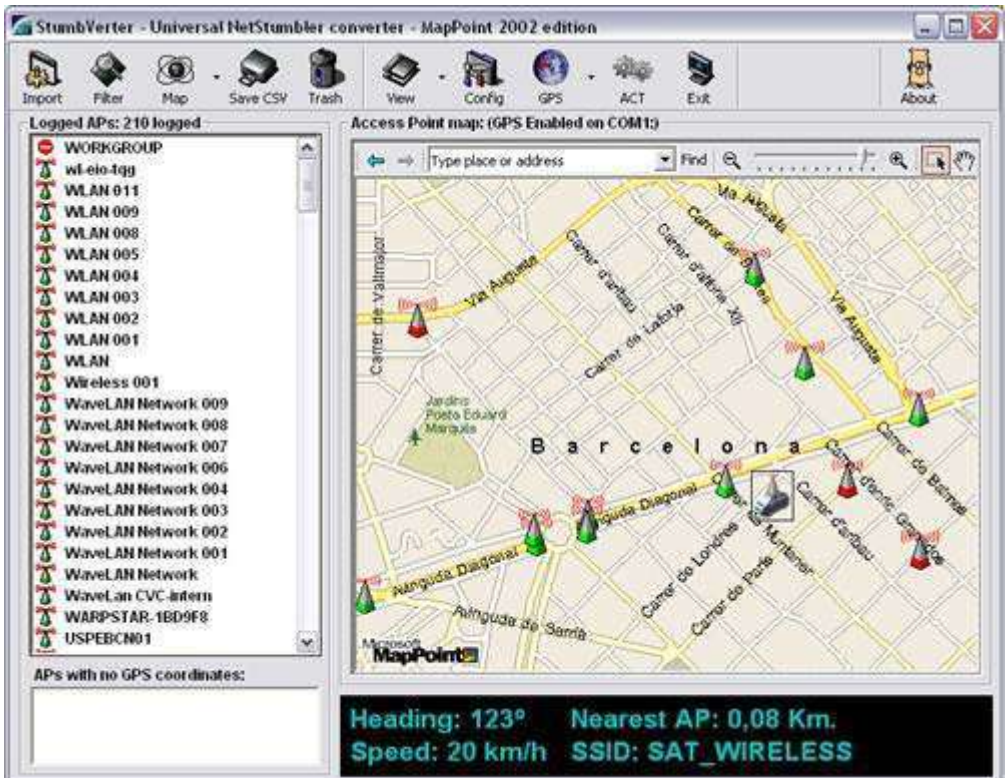
```
# $Creator: Network Stumbler Version 0.3.30
# $Format: wi-scan with extensions
# Latitude      Longitude       ( SSID )        Type    ( BSSID )       Time (GMT)      [
# $DateGMT: 2002-12-14
N 47.4400983    W 2.1003633     ( rezo )        ad-hoc  ( 02:06:8e:e2:5c:0e )   15:47:51
N 47.4400983    W 2.1003633     ( rezo )        ad-hoc  ( 02:06:8e:e2:5c:0e )   15:47:52
N 47.4400967    W 2.1003633     ( rezo )        ad-hoc  ( 02:06:8e:e2:5c:0e )   15:47:53
N 47.4400967    W 2.1003650     ( rezo )        ad-hoc  ( 02:06:8e:e2:5c:0e )   15:47:54
```

Toutes les infos sont enregistrées.

Il est possible d'obtenir gratuitement une carte de couverture de votre Hot Spot grace au site www.wifimaps.com. Voici une image obtenue grâce à Wifimaps, malheureusement comme vous pouvez le voir les rues ne sont pas affichées:



Il existe un autre logiciel de création de plan à partir des données de Microsoft Mappoint : **StumbVerter**



Il sera probablement possible dans quelque temps d'obtenir une carte de couverture de votre Hot Spot pour la ville de Nantes grâce au script PHP de Prospere (**PhpWirelessMap**)

Note: Il existe une version du logiciel pour Pocket PC, appellé MiniStumbler

IMPORTANT: IL EST ABSOLUMENT INTERDIT DE PENETRER EN FRAUDE DANS UN RESEAU, L'UTILISATION DE CE LOGICIEL EST LIMITE AUX TESTS DE COUVERTURE DE VOS PROPRES HOT SPOTS. L'AUTEUR DE CET ARTICLE AINSI QUE L'ASSOCIATION Nantes Wireless DECLINENT TOUTE RESPONSABILITE QUAND A L'UTILISATION QUI POURRAIS ETRE FAITE DE CE LOGICIEL.

(fa)

9. Bibliogrqohie

9.1. Les livres

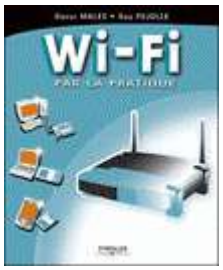
802.11 et les réseaux sans fil

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

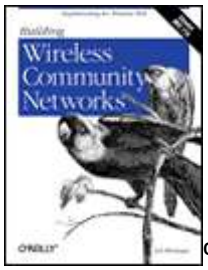
Prix public : 36,00 EUR

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

Building Wireless Community Networks



%%

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)

10. Les ressources sur le web
10.1. Les liens utiles

Liste des 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
- Materiel
  - 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.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
  - http://f1afz.free.fr/patch.htm
- 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/[..]/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
  - Chipsets

- TI ACX100
  - http://focus.ti.com/docs/apps/catalog/tisolutions/tisolutions.jhtml?templateId=977&path=templatedata/cm/level1/data/bband_80211_tisol
- Hermes
- 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 Fabricant materiels
  - 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 USB - Sites persos (Tests, Hack, Tweak, ...)
- 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
- Autres - Sites persos (Tests, Hack, Tweak, ...)

11. 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.

Adresse MAC:
C'est l'adresse d'un ordinateur sur le réseau physique(Par exemple Ethernet).Cette derniere est constituee de 48 bits.

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.

Channel:
"Channel" signifie canal en français. Le 802.11b est composé de 13 canaux avec une largeur de bande de 7 MHz (Voir: FréquencesDuWifi)

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)

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 ou 256 bits. Ce cryptage est executé par le matériel WiFi et est basé sur le RC4.

(ka)

12. Greetings

Remerciements à toute la communauté Wireless-fr pour le simple fait d'exister et de nous fournir un point d'ancrage et de ralliement, et qui font bouger les choses dans notre beau pays la France.

Remerciement à tous ceux qui ont participé a la conception de ce Ebook, notamment les équipes Nantes-wireless et Angers-wireless.

Merci à tous ceux ayant donnés des conseils via IRC, le forum de Nantes-wireless ou directement sur le WikiBook.

A nos partenaires (bulltech, infracom) sans qui une grande partie des tests n'auraient étés réalisés.

Un grand merci à AngelUS (angelus@kloobik.com Web Design & 3D modeling, Lycéen 17 ans) pour cette superbe page de garde.

Remerciements aux différents correcteurs(trices) qui ont enlevé une partie des (trop) nombreuses fautes de cet Ebook.

Et finalement à vous lecteurs de consacrer du temps à vous informer, et faire partager votre intérêt pour le Wireless à votre entourage.

Fanfoué.

Version achevée le 29 MARS 2003

Si vous êtes intéressé par la distribution au format papier de ce document veuillez vous adresser à l'association Nantes-wireless.