

## **V. Précisions et exemples**

Certaines règles sont à respecter lors du déploiement de solutions sans fil. Certains points ont été abordés dans les chapitres précédents, mais méritent d'être plus détaillées comme les distances entre chaque borne, les peurs que ces déploiements engendrent ...

### **V.1 Technique des ondes**

Il ne faut pas oublier que les ondes se propagent en ligne droite et que le moindre obstacle les réfléchies. Selon la nature de cet obstacle, cette réflexion ou cette perméabilité est plus ou moins importante.

#### **➤ Quelques chiffres**

Les ondes se déplacent à la vitesse de la lumière à savoir 300.000 km/s ou  $3 \times 10^8$  m/s et plus exactement à 299 792 458 m/s. Cette vitesse est celle obtenue par le parcours de la lumière dans le vide. Par contre ce chiffre décroît selon le milieu dans lequel elle évolue.

Par exemple à travers le verre la vitesse est de 200.000 km/s, à travers le quartz de 194.805 km/s ...

Les ondes radio ne sont pas des ondes lumineuses dans le sens où nous les voyons pas. Mais elles gardent les mêmes propriétés (à quelque chose près).

#### **➤ Caractéristiques**

Une onde possède une fréquence (Hz) et une longueur d'ondes (cm). Les deux multipliées doivent donner comme résultat 300.000 km/s soit la constante c (dans le vide).

La formule est : (longueur d'onde) x (fréquence) = c

Par exemple pour la norme 802.11g où la fréquence est de 2,4GHz, la longueur d'onde est 12,5 cm. Pour la norme 802.11a, où la fréquence est 5,5GHz, la longueur d'onde est 5,5 cm.

### **Définition**

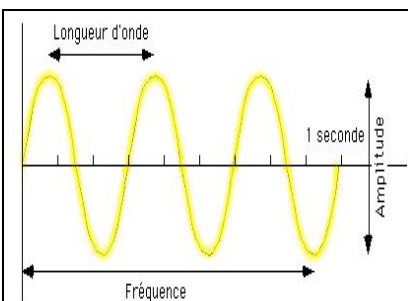
« La fréquence est le nombre de fois qu'un phénomène a été ou est observable pendant une unité de temps.
--



Un phénomène est périodique si les caractéristiques observées se reproduisent à l'identique pendant des durées égales consécutives. La période du phénomène est la durée minimale au bout de laquelle il se reproduit avec les mêmes caractéristiques.

La période est l'inverse (au sens mathématique) de la fréquence. Si l'unité de temps choisie est la seconde, la fréquence est mesurée en hertz (symbole: Hz), du nom du physicien Heinrich Hertz. »

[http://fr.wikipedia.org/wiki/Propagation\\_des\\_ondes\\_radio](http://fr.wikipedia.org/wiki/Propagation_des_ondes_radio)



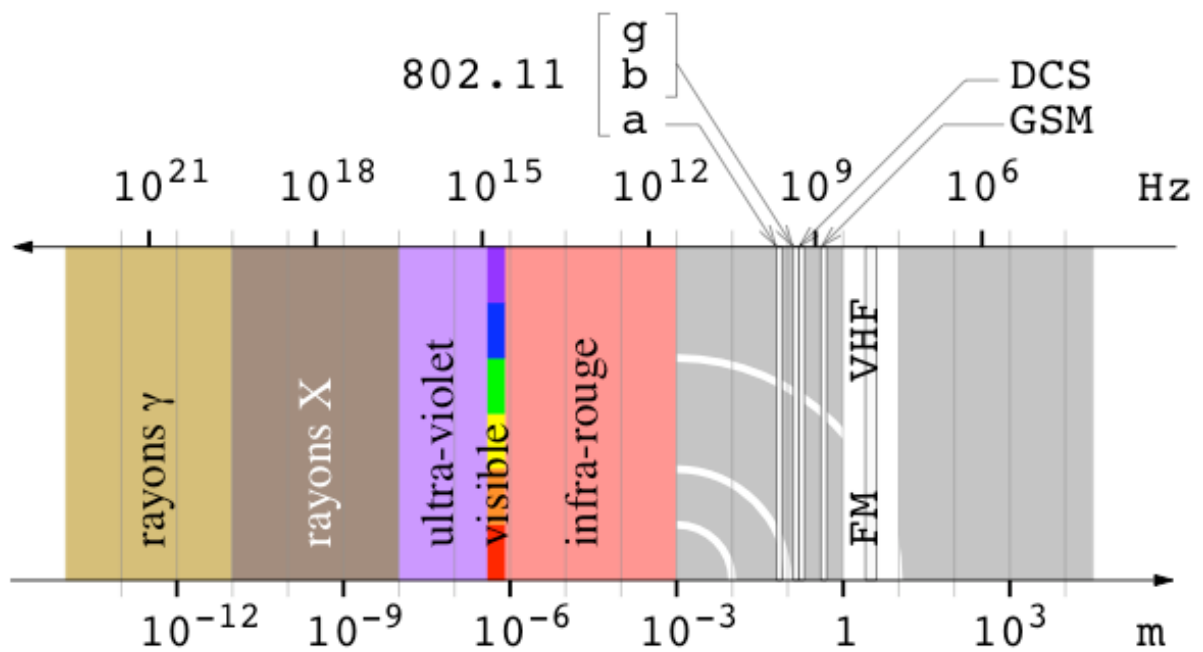
La longueur d'onde est la distance séparant deux crêtes successives d'une onde périodique. On la dénote communément par la lettre grecque  $\lambda$  (lambda).

[http://fr.wikipedia.org/wiki/Propagation\\_des\\_ondes\\_radio](http://fr.wikipedia.org/wiki/Propagation_des_ondes_radio)

### Voici le spectre électromagnétique

[\(http://www.wifi-montauban.net/\)](http://www.wifi-montauban.net/) :

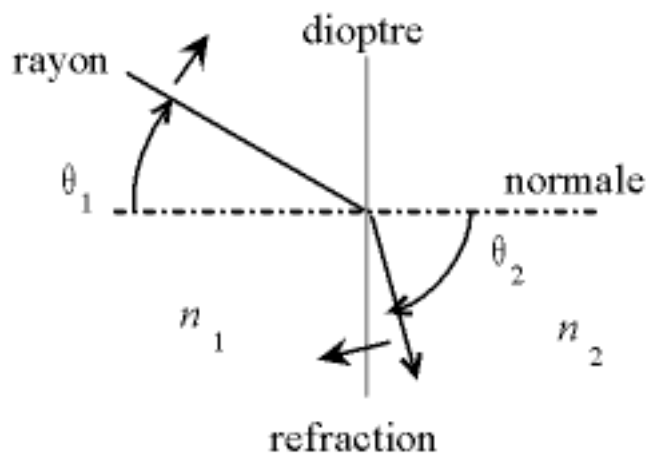
Longueur d'onde	Domaine	Commentaire
> 10 cm	radio	(150kHz – 3GHz)
de 1 mm à 10 cm	micro-onde et radar	(10 cm - +- 1cm, 3 - 300 GHz)
de 1 $\mu$ m à 500 $\mu$ m	infrarouge	
de 400 nm à 700 nm	lumière visible	rouge (620-700 nm) orange (592-620 nm) jaune (578-592 nm) vert (500-578 nm) bleu (446-500 nm) violet (400-446 nm)
de 10 nm à 400 nm	ultraviolet	(400 - 280 nm)
de 10 <sup>-8</sup> m à 10 <sup>-7</sup> m		
de 10 <sup>-11</sup> m à 10 <sup>-8</sup> m	rayon X	
de 10 <sup>-14</sup> m à 10 <sup>-12</sup> m	rayon gamma	



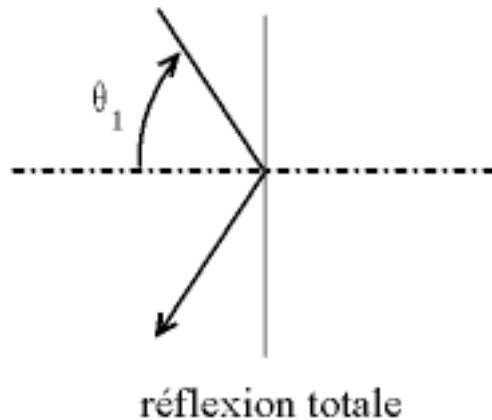
### ➤ Le parasitage

Une onde (comme celle du WiFi) peut être

- ✓ Réfractée



- ✓ Réfléchi



✓ Diffractée

« La diffraction est la diffusion d'une onde par un objet. Plus la longueur d'une onde est grande par rapport à un obstacle, plus cette onde aura de facilité à contourner, à envelopper l'obstacle. Ainsi les grandes ondes (longueurs d'ondes hectométriques et kilométriques) peuvent pénétrer dans le moindre recoin de la surface terrestre tandis que les retransmissions de télévision par satellite ne sont possibles que si l'antenne de réception « voit » le satellite. »

[http://fr.wikipedia.org/wiki/Diffraction\\_des\\_ondes](http://fr.wikipedia.org/wiki/Diffraction_des_ondes)

✓ Absorbée

Le rayon est « capturé » par l'objet qu'il tente de traverser. L'onde est alors détruite.

On parle alors de « transparence » des matériaux.

Voici quelques exemples

(<http://didier.82.free.fr/images/transparence.jpg>) :

## Transparence



air  
bois  
air humide  
plastique, verre  
eau, végétation  
animaux, nous  
cloisons en plâtre, brique  
béton  
verre blindé  
métal conducteur

## V.2 La mobilité

### ➤ Plus de câblage ?

L'intérêt de la technologie sans-fil est de s'affranchir du câble. Ceci est en effet vrai mais dans une certaine mesure seulement. En effet, créer un réseau sans-fil est une chose mais il ne faut pas oublier que pour le connecter à l'internet par exemple, ou au réseau d'entreprise, il faudra à un moment ou un autre lier la borne avec la structure filaire.

Autre point extrêmement important et souvent oublié, la partie électrique. Un portable a une autonomie limitée, allant de 2h à 4h généralement et ces chiffres « constructeur » varient fortement. Par exemple, l'utilisation d'une carte réseau sans-fil provoque une diminution d'autonomie du portable de près de 50%.

On voit tout de suite que proposer un réseau sans-fil au sein d'une université par exemple, c'est très bien, mais, si à côté de cela aucune prise électrique n'est disponible, le problème va être déporté.



## ➤ Positionnement des bornes

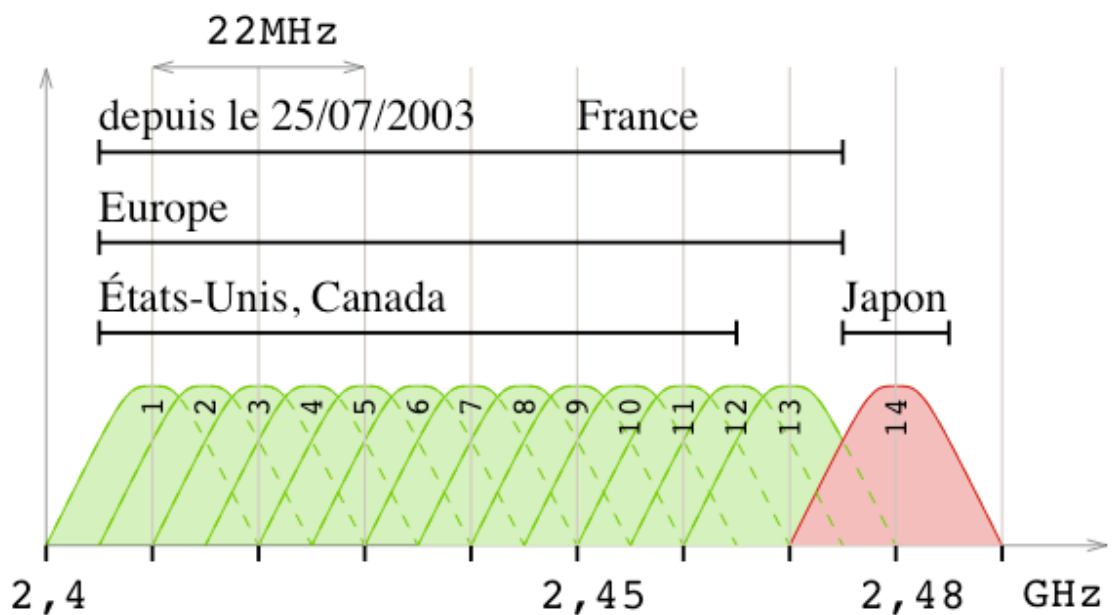
Nous l'avons déjà évoqué, mais il est nécessaire de le redire. Lorsque vous décidez d'offrir une couverture sans-fil sur un domaine étendu, une seule borne ne peut suffire. Il est donc nécessaire d'en déployer plusieurs.

Il faut alors faire attention au recouvrement des signaux afin d'éviter des perturbations entre bornes.

✓ 802.11b

Les canaux se « chevauchent » sur 5 canaux successifs. Par exemple les canaux 1 à 5 se perturbent ainsi que les 2 à 6 ... Il est donc nécessaire, si vous positionnez plusieurs bornes, de définir des canaux non consécutifs et séparés de 5 canaux à savoir 25MHz (5 x 5MHz).

### 802.11b : canaux

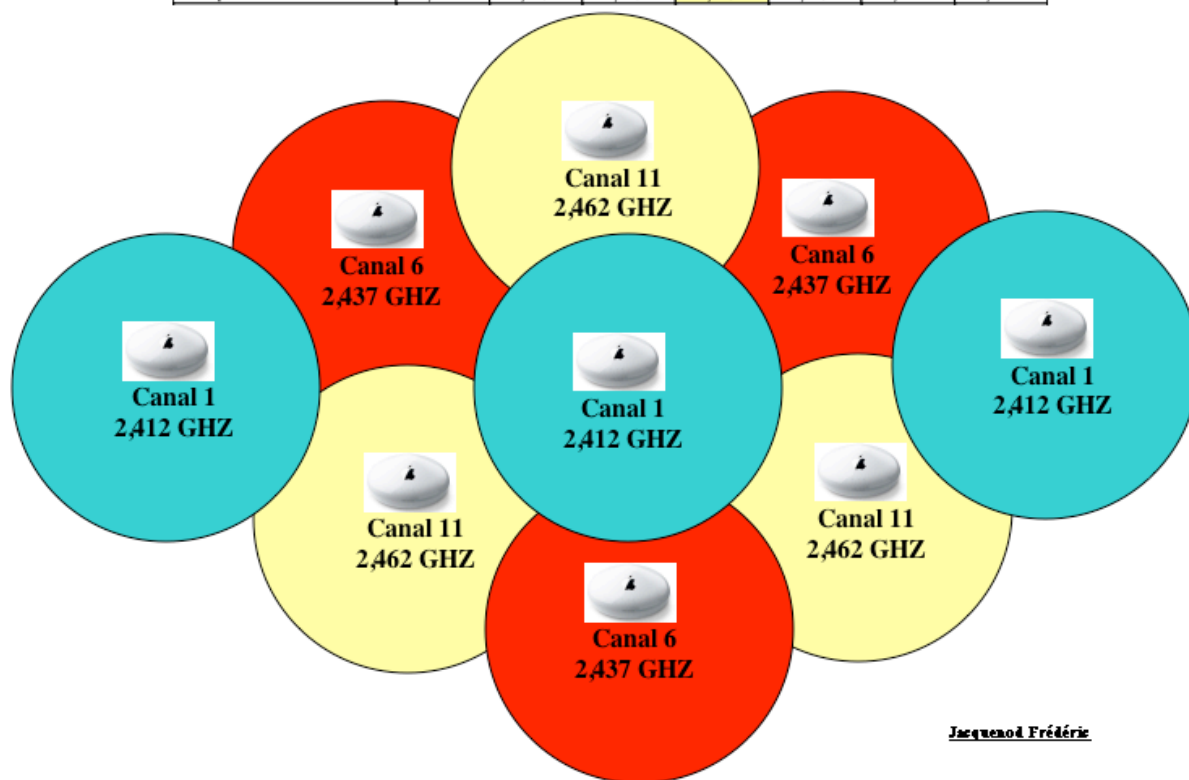


Bande ISM (Industrial, Scientific, and Medical).

Par exemple vous pouvez avoir la configuration suivante pour une couverture maximale :

Canal	1	2	3	4	5	6	7
Fréquence GHZ	2,412	2,417	2,422	2,427	2,432	2,437	2,442

Canal	8	9	10	11	12	13	14
Fréquence GHZ	2,447	2,452	2,457	2,462	2,467	2,472	2,477



✓ 802.11g

Seuls 3 canaux peuvent être utilisés pour réaliser un « maillage ». Vous ne pouvez donc pas réaliser un réseau de plus de 3 bornes.

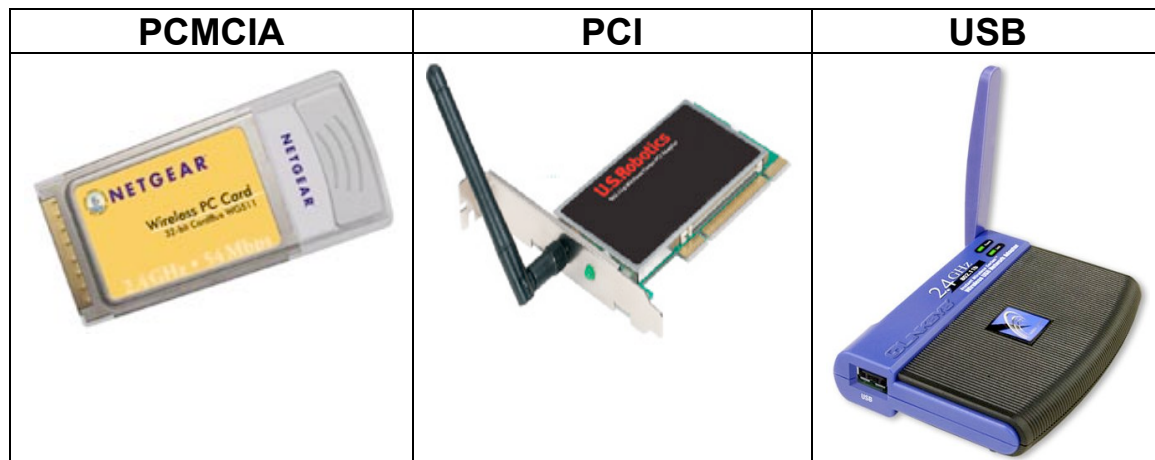
### ➤ Les bornes et les cartes sans-fil

Il existe plusieurs solutions aussi bien au niveau des cartes sans-fil à intégrer dans les ordinateurs qu'au niveau des bornes.

Certaines bornes possèdent des antennes, généralement 2, on parle d'émission directionnelle. Non pas parce que les ondes ne vont aller que vers le point voulu mais les ondes seront plus puissantes dans la direction vers laquelle se tournent les antennes. Lorsqu'une borne ne possède pas d'antenne orientable, on parle d'émission omnidirectionnelle (dans toutes les directions). Dans ce cas, aucune direction ne sera privilégiée.

Côté carte, il existe deux grandes familles :

- ✓ Les cartes PCMCIA qui se branchent dans le port du même nom ou les cartes USB ou PCI ou FireWire qui se branchent respectivement sur le port USB ou PCI ou FireWire.



- ✓ Les cartes intégrées à l'ordinateur.

Les cartes pcmcia ou usb ont mauvaise réputation car leur zone de réception n'est pas large et donc la qualité de réception des ondes est médiocre même si parfois, la présence d'une antenne peut faire croire l'inverse.

Dans le cas d'une carte intégrée, là aussi tout n'est pas rose. Certains constructeurs comme Apple (précurseur dans le domaine) l'intègrent dès la construction du PC en mettant par exemple l'antenne dans l'écran permettant ainsi une réception optimale. Ce n'est pas le cas de tous les constructeurs. Résultat, selon le constructeur, pour une puissance équivalente de la carte, la réception ne sera pas du tout de la même qualité.

### **V.3 Les craintes**

#### **➤ Le piratage**

Si vous lisez des articles sur le net ou même des livres, vous vous apercevez qu'il paraît extrêmement simple de pirater une borne sans-fil non protégée ou même protégée par un cryptage Wep.

Il faut mettre à ce genre d'article un bémol. Le piratage n'est pas à la portée du premier venu. Les « y'a qu'à récupérer les paquets », « y'a qu'à décrypter la clé Wep », « y'a qu'à faire de l'IP spoofing » et autres recettes ne sont pas toujours simples à mettre en œuvre dès que l'administrateur de la borne met un minimum de sécurité.

De plus certaines cartes wifi bloquent la possibilité de passer la carte en mode promiscuous (ou debug), mode qui permet de faire remonter aux



couches hautes (logiciels de scan) les paquets récupérés. Certains logiciels n'acceptent que certaines cartes  
Bien évidemment, si l'administrateur ou plutôt dans ce cas le simple utilisateur non prévenu des risques met en place une borne en ne faisant que la brancher (voir plus bas) sans rien configurer, il est très simple de le pirater.

Par contre dès que le minimum est fait :

- ✓ Modification du mot de passe de l'administrateur pour la connexion sur la borne
- ✓ Activation d'une clé Wep statique
- ✓ Pas de broadcast du SSID

Un pirate « de base » aura alors du mal à vous casser la borne... ☺

Il est de coutume de dire qu'avec ce genre de configuration, le pirate doit récupérer environ 2Millions de paquets pour trouver votre clé Wep. La simple récupération n'est pas forcément si facile que cela.

Si vous mettez une clé dynamique, que vous faites en plus un filtrage des adresses Mac et que vous empêchez l'administration de votre borne à partir de l'extérieur de votre réseau, vous augmentez d'autant votre sécurité.

Avec la « démocratisation » du sans-fil, vous pouvez être sûr que votre pirate essaiera alors de cracker une autre borne peut être moins bien protégée que la votre.

Pensez aussi à regarder souvent les logs de la borne. Pensez à mettre la borne à l'heure pendant que vous y êtes. ☺

### ➤ La nocivité des ondes

Là aussi, il est nécessaire de relativiser cette notion. Non pas qu'il n'y a aucun problème. Les ondes dégagent de l'énergie et nous sommes entourés de ces ondes (télévision, téléphone portable, sans-fil, lumière ...). Tout va dépendre de la puissance de ces ondes.

Les cartes sans-fil ont généralement une puissance de 30mW.

Le tableau ci-dessous montre d'autres matériels qui émettent des ondes dans la vie de tous les jours :

Technologie	Puissance
Sans-Fil	30mW
Borne Sans-Fil	< 100mW
GSM (Global System for Mobile)	< 2 W
Antenne GSM	20 à 50 W

Four à micro-ondes	1kW
Emetteur de la tour Eiffel	6 MW

### **Rappel**

Le champ magnétique décroît selon la formule  $1/r^2$ .  $r$  étant le rayon ou la distance en mètres.



Vu les chiffres ci-dessus, il faudrait pour obtenir la puissance équivalente à un téléphone GSM positionné à l'oreille (soit 600mW) environ 10 portables munis d'une carte sans-fil (c'est moins lourd) sur la tête ou 1000 portables sur les genoux ou mieux, 100.000 dans une classe ... Comme disait Einstein : « tout est relatif ».

### **V.4 Exemple 1 : le basique**

#### **Exemple 1 : le basique**

Il existe de nombreux logiciels (voir ceux cités dans les chapitres précédents) pour scanner les bornes (trouver les bornes) et pour sniffer le trafic (récupérer les paquets de données). Certains sont payants et d'autres gratuits.

Pour ma part j'ai utilisé, pour la démonstration les logiciels suivants :

	KisMac	Il permet de détecter les bornes, tout en affichant les informations de configuration. Il offre aussi la possibilité de sniffer le trafic et de tenter de casser les sécurités. <a href="http://binaervarianz.de/projekte/programmieren/kismac/">http://binaervarianz.de/projekte/programmieren/kismac/</a>
	MacSniffer	Il permet de sniffer le trafic à partir d'une interface réseau et de décoder les paquets. <a href="http://personalpages.tds.net/~brian_hill/macsniffer.html">http://personalpages.tds.net/~brian_hill/macsniffer.html</a>

### **Conseil**

Faites attention car vous aussi vous laissez des traces (si tant est que l'administrateur les consulte ou même sache que cela existe). Si vous avez appelé votre ordinateur par votre nom de famille, si vous vous connectez à votre site web personnel ... Il est alors très simple pour le propriétaire de la borne de remonter jusqu'à vous.

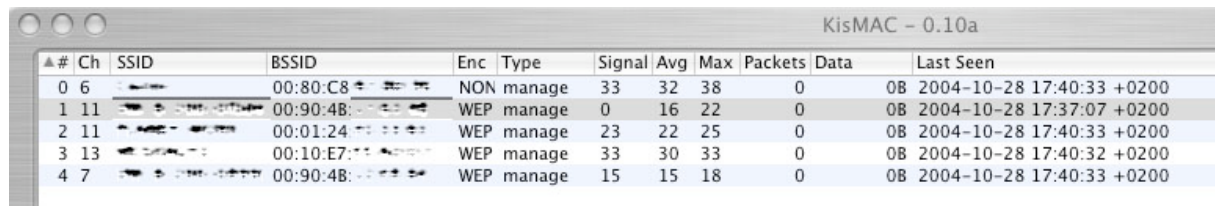
## ➤ Etape 1 (scan)

Il faut tout d'abord « se renseigner » sur les bornes qui se situent dans le périmètre de réception où vous êtes.

Pour cela lancez KisMac après avoir vérifié que le driver de votre carte sans-fil est supporté KisMac -> Preferences -> Driver.

Réglez les autres préférences comme le « dump filter » (quoi sniffer), les canaux d'écoutes (mettez all au début, vous affinerez plutard) ...

A partir de là, vous pouvez enclencher le processus de scan et vous allez découvrir toutes les bornes qui se situent au alentour.



The screenshot shows the KisMAC application window with a table of scan results. The table has columns for channel number, SSID, BSSID, encryption type, and signal strength. The first row shows a channel 6 with no encryption (NON manage). The other rows show channels 11, 11, 13, and 7, all with WEP encryption (WEP manage).

▲ #	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen
0	6		00:80:C8	NON	manage	33	32	38	0	0B	2004-10-28 17:40:33 +0200
1	11		00:90:4B	WEP	manage	0	16	22	0	0B	2004-10-28 17:37:07 +0200
2	11		00:01:24	WEP	manage	23	22	25	0	0B	2004-10-28 17:40:33 +0200
3	13		00:10:E7	WEP	manage	33	30	33	0	0B	2004-10-28 17:40:32 +0200
4	7		00:90:4B	WEP	manage	15	15	18	0	0B	2004-10-28 17:40:33 +0200

Pour des raisons de confidentialité, j'ai masqué les SSID (nom des bornes) et la fin des BSSID (adresse Mac) des bornes que j'ai trouvées. Autour de chez moi j'en ai trouvé 8 (6 ici dans le salon).

On peut voir les canaux utilisés (colonne Ch) et surtout le type d'encrytptage (Enc).

On peut tout de suite voir que la première borne n'est pas du tout protégée, elle est donc utilisable sans effort.

Les autres possède le minimum à savoir une clé wep activée.

### **Remarque**

Selon le type de borne, vous pouvez ensuite cibler les canaux voulus pour sniffer les paquets. N'oubliez pas que pour des bornes en 802.11g, les paquets transitent sur 3 canaux consécutifs. La première borne est une 802.11g, elle est vue à ce moment sur le canal 6. Si je veux affiner mon scan, je dois activer les canaux 5, 6 et 7 dans le menu préférences.

Vous pouvez en cliquant sur la ligne correspondante avoir plus d'informations, comme la marque de la borne ... très utile pour obtenir les identifiants et mot de passe par défaut ☺ (voir exemple 2).

Property	Setting
SSID	[redacted]
BSSID	00:01:24:00:00:00
Vendeur	Acer/SMC
vu la premiere fois	2004-10-28 17:35:11 +0200
Derniere Fois Vu	2004-10-28 17:40:34 +0200
canaux	11
Setuped-Channel	11
Signal	0
SignalMax	25
SignalMoyen	22
Type	manage
Cryptage	WEP
Paquets	0
Paquets faible	0
Paquets de donnée	0
Bytes	0B
Clef	<non resolu>
DernierIV	00:00:00
Latitude	
Longitude	
Elevation	No Elevation Data

## ➤ Etape 2 (connexion)

Pour utiliser la borne non protégée, il suffit (sous mac) d'activer sa carte airport et de choisir parmi les réseaux proposés.

Si vous choisissez une des bornes « wepisée », un mot de passe (la clé wep) vous est demandé. Si vous ne la possédez pas la connexion échoue.

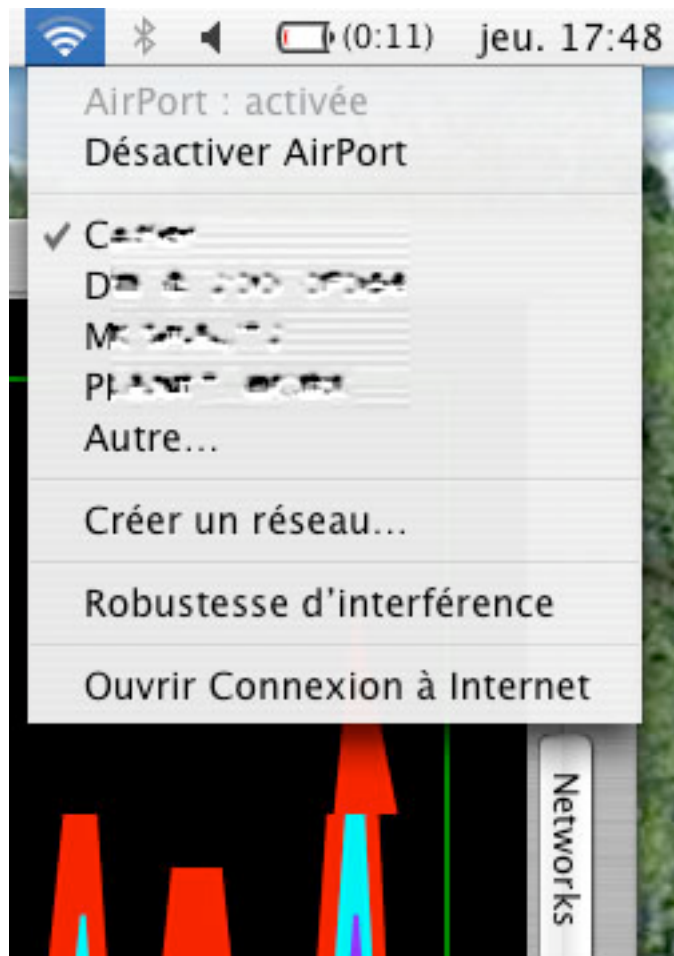
Dans mon cas, la première borne n'est pas « sécurisée », je la choisit et le tour est joué.

## **ATTENTION**

Ce type de borne peut être dangereux et peut cacher un piège. Vous ne devez en aucun cas utiliser des protocoles non sécurisés pour vous connecter à des pages web, ou à des services (compte mél ...) qui requièrent une authentification. En effet, si le propriétaire de la borne sniffe le trafic, il récupère sans problème vos informations et là c'est

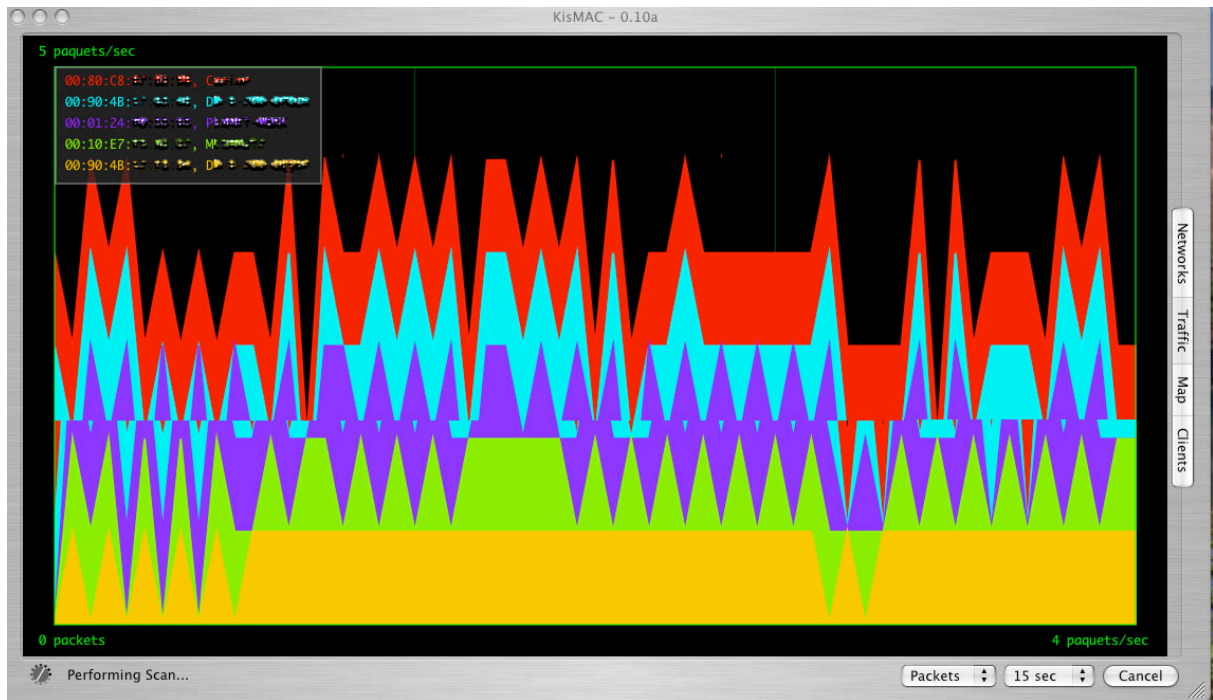
vous qui êtes piratés ...

Utilisez donc des protocoles comme https, pops, ssh, sftp ...



### ➤ Trafic sur les bornes

Il est possible de voir avec KisMac le trafic sur les bornes.



## V.5 Exemple 2 : Les dangers d'une borne « par défaut »

### Exemple 2 : où peut amener l'ignorance ?

#### Rappel

Si un délit est commis à partir de votre connexion internet c'est vous qui êtes responsable, jusqu'à preuve du contraire. Une affaire récente et symptomatique des risques encourus a eu lieu aux USA mais peut très bien avoir lieu en France. La police a fait une descente chez un particulier qui possédait une borne sans-fil « non protégée ». Depuis cette borne des accès à des sites pédophiles avaient lieu. Il s'est ensuite avéré que le propriétaire n'y était pour rien et qu'il ignorait tout. Son voisin utilisait sa borne à son insu.

Voici un autre scan :

#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	L
0	7	C	00:80:C8:51:10:10	NON	manage	11	10	17	273	21.57KiB	2
1	11	N	00:09:5B:51:10:10	NON	manage	10	10	15	173	13.68KiB	2

La deuxième borne a conservé son SSID d'origine et n'est pas sécurisée. En regardant sur le web on trouve tout de suite le login et le

mot de passe de base de cette borne de type Netgear. C'est une borne 11g car le scan montre qu'elle émet sur 3 canaux.

Le site du constructeur est alors très utile <http://www.netgear.fr/support/>

On trouve la documentation suivante :

## 2 Connexion au routeur

**Remarque :** pour se connecter au routeur, votre ordinateur doit être configuré pour pouvoir obtenir automatiquement une adresse IP via DHCP. Pour savoir comment procéder, référez-vous au chapitre Windows TCP/IP Configuration Tutorials du *Manuel de référence* sur le *site web de Netgear* :

*<http://www.NETGEAR.com/docs/wgt624/index.htm>*.

- a. Connectez-vous au routeur en tapant *<http://192.168.0.1>* dans la zone d'adresse d'Internet Explorer ou de Netscape® Navigator.



- b. Pour des raisons de sécurité, le routeur a son propre nom d'utilisateur et son propre mot de passe. Lorsque le programme vous y invite, tapez **admin** pour le nom d'utilisateur et **password** pour le mot de passe (en minuscules).

ou sur le site bien en gras

A screenshot of a Mozilla browser window displaying the Netgear website. The browser title is 'How is Port Forwarding Configured? - Mozilla {Build ID: 2004090508}'. The address bar shows 'http://kbserver.netgear.com/k'. The website has a purple header with the 'NETGEAR' logo. Below the logo is a navigation menu with buttons for 'Products', 'Applications', 'Where to Buy', 'Support', 'Partners', and 'News &amp; Events'. A secondary menu includes 'Registration', 'Premium Support', 'Rebate Status', 'Give Feedback', 'RMA Status', and 'Contact Support'. The main content area features the title 'How is Port Forwarding Configured?' in orange. Below the title is a paragraph of text explaining software ports and their security risks. On the right side, there is a grey circular callout box containing two lines of text: 'The router username is always admin' and 'The default password is password or 1234'.

On voit dans ces documentations qu'à aucun moment, le constructeur indique un risque potentiel si le login et le mot de passe ne sont pas changés...

Une fois connecté à ce réseau via l'accrochage à cette borne, j'obtiens une adresse via le serveur DHCP de la borne qui me montre (commande `ifconfig -a`) que je suis sur le réseau interne en 192.168.0.5. Le tour est joué.

Je me connecte alors via mon navigateur à la borne `http://192.168.0.1` en utilisant l'adresse par défaut de celle-ci.

Si l'adresse a été changée, rien de grave, lancez MacSniffer et regardez qui dialogue (adresse IP) constamment avec votre ordinateur ... c'est la borne.

La borne vous demande de vous authentifier **admin** pour le login et **password** pour le mot de passe ... vous êtes administrateur de la borne.

### ➤ **La configuration de la borne**

- ✓ Configuration réseau



# NETGEAR settings

54 Mbps Wireless Router WGR614 v4

- Basic Settings
- Wireless Settings
- Content Filtering
- Logs
- Block Sites
- Block Services
- Schedule
- E-mail
- Maintenance
- Router Status
- Attached Devices
- Backup Settings
- Set Password
- Router Upgrade
- Advanced
- Port Forwarding
- Port Triggering
- WAN Setup
- LAN IP Setup

## LAN IP Setup

---

### LAN TCP/IP Setup

IP Address:

IP Subnet Mask:

RIP Direction:

RIP Version:

---

Use Router as DHCP Server

Starting IP Address:

Ending IP Address:

---

### Address Reservation

#	IP Address	Device Name	Mac Address

---

- ✓ Vous pouvez même changer le mot de passe de la borne ... pour la protéger d'éventuels pirates ☺

## Router WGR614 v4

### Set Password

---

Old Password:

New Password:

Repeat New Password:

---

- ✓ La borne est même administrable via internet sans restriction

**NETGEAR settings**  
54 Mbps Wireless Router WGR614 v4

**Remote Management**

Turn Remote Management On

Remote Management Address:  
http://80.80.80.123:8080

Allow Remote Access By:

Only This Computer: [ ] . [ ] . [ ] . [ ]

IP Address Range : From [ ] . [ ] . [ ] . [ ]  
To [ ] . [ ] . [ ] . [ ]

Everyone

Port Number: [ 8080 ]

Apply Cancel

- ✓ Etat de la borne

## Router WGR614 v4

### Router Status

Account Name	WGR614v4
Firmware Version	Version 4.04 Jan 15 2004

#### Internet Port

MAC Address	00:09:5b:0c:00:00
IP Address	192.168.1.139
DHCP	PPPoE
IP Subnet Mask	255.0.0.0
Domain Name Server	192.168.1.100 192.168.1.36

#### LAN Port

MAC Address	00:09:5b:0c:00:00
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0

#### Wireless Port

Name (SSID)	NETGEAR
Region	France
Channel	11
Mode	g and b
Wireless AP	On
Broadcast Name	On

[Show Statistics](#)[Connection Status](#)

- ✓ Les logs (On remarque que la borne n'est pas à l'heure...)  
Il est ainsi possible de voir ce que fait le propriétaire de la borne, les heures de connexions pour ensuite pouvoir sniffer aux heures de présence ses connexions.

**Logs**

Current time: Sunday, 31 Oct 2004 04:45:45

```
[ALLOW:www.wanadoo.fr] Source:192.168.0.2
Sunday, 31 Oct 2004 00:55:51
[ALLOW:www.wanadoo.fr]
Source:192.168.0.2 Sunday, 31 Oct 2004
00:56:27
[ALLOW:www.wanadoo.fr] Source:192.168.0.2
Sunday, 31 Oct 2004 01:21:14
[ALLOW:home.wanadoo.fr] Source:192.168.0.2
Sunday, 31 Oct 2004 01:21:53
[ALLOW:perso.wanadoo.fr] Source:192.168.0.2
Sunday, 31 Oct 2004 01:27:31
[ALLOW:www.wanadoo.fr] Source:192.168.0.2
Sunday, 31 Oct 2004
01:29:15
```

## V.6 Exemple 3 : Récupération des paquets de données non cryptés

### Exemple 3 : Sniffer les paquets de données non cryptés

Le but de la manipulation est de récupérer les paquets qui transitent sur le réseau.

Cette manipulation est simple dans le cas d'une borne sans cryptage, car tous les paquets passent en clair.

Par contre, dans le cas de la mise en place d'une protection de base comme une clé WEP, le travail est plus compliqué (voir exemple 4).

Si vous pouvez vous associer à la borne, le logiciel MacSniffer est tout à fait suffisant.

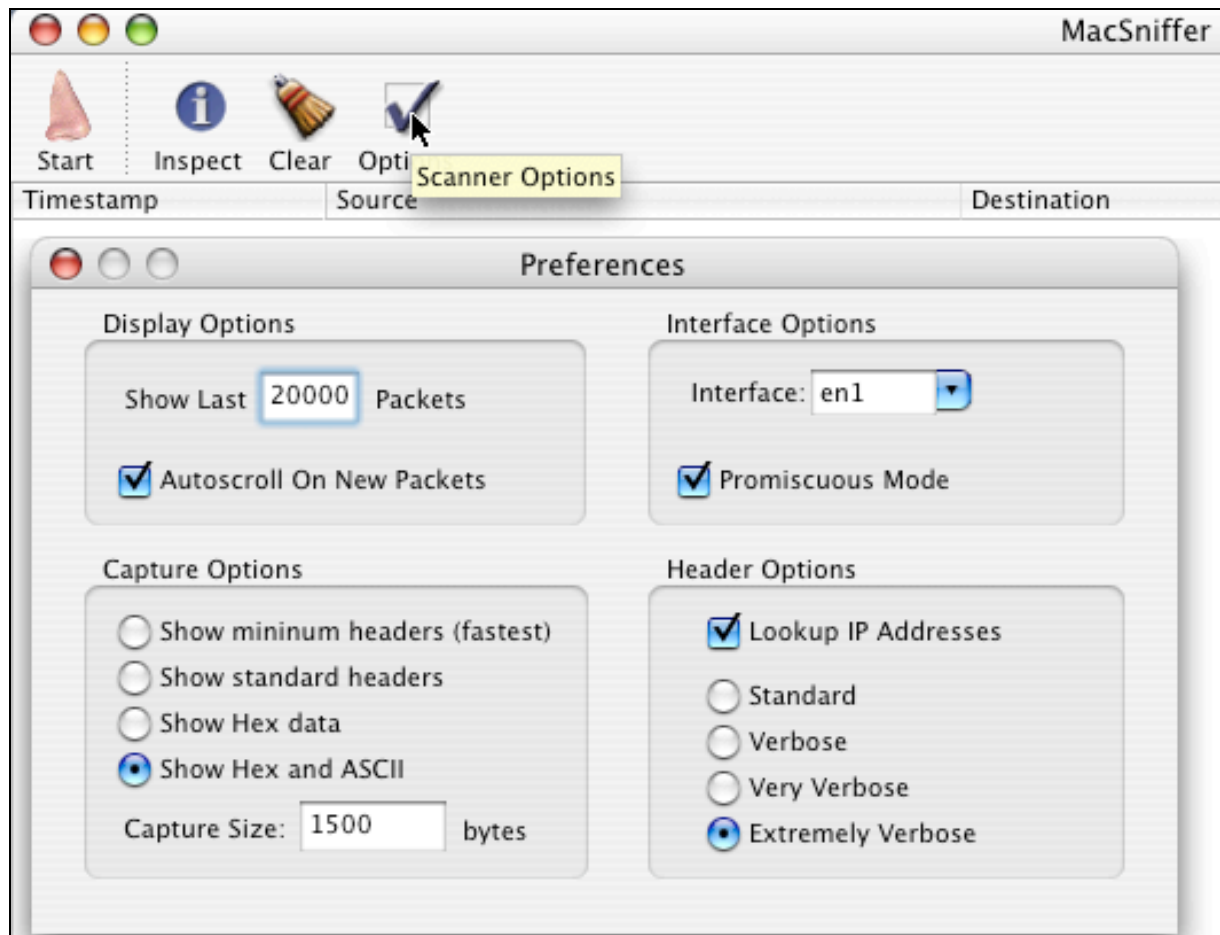
Il fonctionne avec tous types de cartes WiFi.

Pour utiliser MacSniffer, vous devez paramétrer les options. Réglez le nom de l'interface. Pour découvrir laquelle c'est vous pouvez dans une fenêtre de terminal (applications->Utilitaires->Terminal) taper la commande **ifconfig -a**. Cette commande permet de voir la configuration des différentes cartes réseau (Ethernet, sans fil ...).

Les options se règlent simplement en cliquant sur **Options**.

Il est conseillé d'augmenter le nombre de paquets visibles (200 par défaut à la ligne **-Show last-**) ainsi que la taille de la capture (68 Octets par défaut) et le contenu de la récupération (verbose par défaut).

N'oubliez pas de cocher, si ce n'est pas fait, la case **Promiscuous Mode** sinon seuls vos paquets seront capturés ...



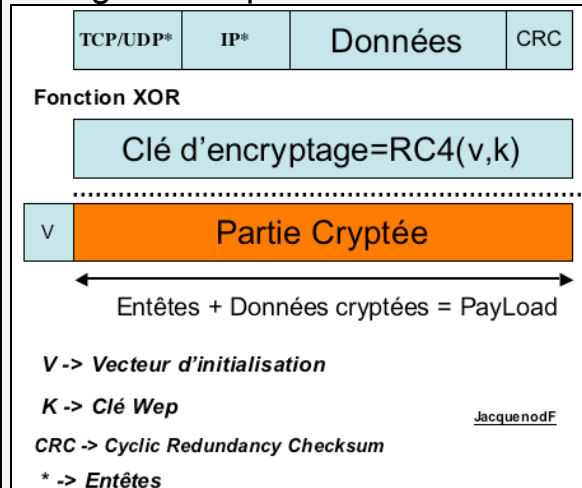
## V.7 Exemple 4 : Cracker une borne « sécurisée »

### Exemple 4 : Sniffer les paquets de données

Vous ne pouvez vous associer à la borne. Il faut alors récupérer un maximum de paquets pour espérer tomber sur la clé WEP et la décrypter pour ensuite vous connecter à travers la borne ou décrypter les paquets de données récupérés. Pour cela j'utilise KisMac qui propose de récupérer les paquets et notamment ceux contenant les vecteurs d'initialisation (Weak Packet -> initialization vector).

### Rappel

Pour crypter les données, et afin d'éviter que le cryptage se fasse sur une même base (la clé Wep), le protocole ajoute un élément aléatoire pour le codage. Le vecteur d'initialisation (Initialization Vector ou IV). Problème, le client ne possède pas ce vecteur, il faut donc lui envoyer. Ceci se fait, en clair, dans le paquet de données transmis. Ce vecteur change à chaque envoi.



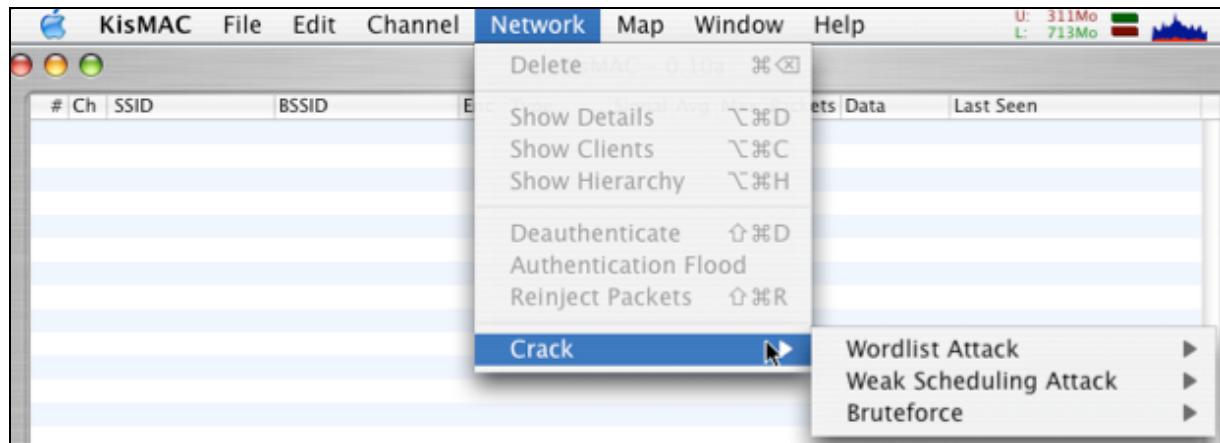
Hélas, le vecteur d'initialisation du protocole WEP est un champ de 24 bits (sur les clés de 64 bits et 128 Bits). Une si petite taille entraîne la réutilisation du même vecteur au bout d'un certain temps. Un point d'accès surchargé, qui envoie constamment des paquets de 1500 octets à 54Mbps par exemple, épuise l'espace d'initialisation (IV) après  $(1500 \cdot 8 / (54 \cdot 10^6)) \cdot 2^{24} = 3728$  secondes, ou 1 heure.

Il est alors possible d'effectuer des comparaisons entre les paquets codés pour en déduire la clé.

Selon le type d'attaques, Il peut être nécessaire de récupérer un grand nombre de paquets. Certains sites parlent de 2.000.000 de paquets pour avoir une chance de cracker la clé. KisMac demande un minimum de 500 à 1000 paquets avant de pouvoir travailler et utiliser les actions prédéfinies de crackage. Mais comptez plutôt sur un nombre avoisinant les 200.000. Ce nombre représente déjà, dans le cas où il y a une activité faible sur la borne, 20 heures environs.

Vous pouvez bien sûr augmenter cette activité avec une autre ordinateur en envoyant du « spam » vers la borne. Celle-ci répondra à vos requêtes, augmentant ainsi le flux de paquets sur le réseau ☺.

Il est possible de sauvegarder les paquets et de reprendre le scan à un autre moment.



### **Attention**

Les cartes Airport Extreme n'acceptent pas le mode passif. Elles ne sont donc pas utilisables pour ce genre de travail.

### **Attention**

Il est évident que si la borne utilise une clé Wep dynamique, il est peu probable que vous réussissiez à la récupérer assez vite et à l'utiliser avant le prochain changement.

## **Exemple 4 : Casser la clé Wep**

Vous pouvez aussi utiliser des logiciels comme

- WepCrack (<http://wepcrack.sourceforge.net/> )
- jc-wepcrack ( <http://www.hick.org/~johnycsh/code/> )
- dwepcrack (<http://www.e.kth.se/~pvz/wifi/>)
- WepLab (<http://weplab.sourceforge.net/> )
- WepAttack (<http://wepattack.sourceforge.net/> non testé par mes soins).

WepCrack, jc-wepcrack ou WepLab utilisent des programmes perl qui vont chercher l'information dans des fichiers de log au format PCAP (obtenu avec des logiciels comme ethereal).

WepAttack possède une documentation très étoffée mais ... en allemand uniquement. Il se base sur un énorme dictionnaire pour tester les différents mots. Le problème est que si la clé n'est pas dans le dictionnaire rien ne se passera.

Différentes attaques sont possibles :

➤ Brute force (force Brutale)

Ce système teste systématiquement toutes les possibilités de combinaison pour trouver la bonne. Il n'est donc pas nécessaire de récupérer énormément de paquets. En théorie, un seul est nécessaire, mais il est bon d'en posséder un autre pour la vérification de la clé trouvée. Autant dire que ce n'est pas la méthode idéale. En effet, sur une clé de 64Bits (40 effectifs), il y a  $2^{40}$  possibilités. Il faut quelques jours (ou heures) selon la puissance de calcul à votre disposition.

Ce système peut être amélioré :

- en travaillant avec un dictionnaire de mots clés prédéfinis
- en ne testant que les lettres en minuscules
- en utilisant la méthode Newsham qui se base sur les algorithmes de création des clés qui permet de descendre le nombre de possibilités à  $2^{21}$
- ...

Le décryptage s'effectue grâce à la partie ICV (Integrity Check Value) du paquet 802.11 récupéré.

<b>Entête 802.11</b>	<b>IV (24 bits)</b>	<b>Numéro de la clé*</b>	<b>Partie cryptée</b>	<b>ICV (32 bits)</b>
--------------------------	---------------------	------------------------------	---------------------------	----------------------

\* Le numéro de la clé (Key Number) varie entre 1 et 4 lorsqu'elle permet de définir une clé par défaut pré-définie dans votre matériel pour une utilisation du Wep sans fournir une clé à vous... A éviter !

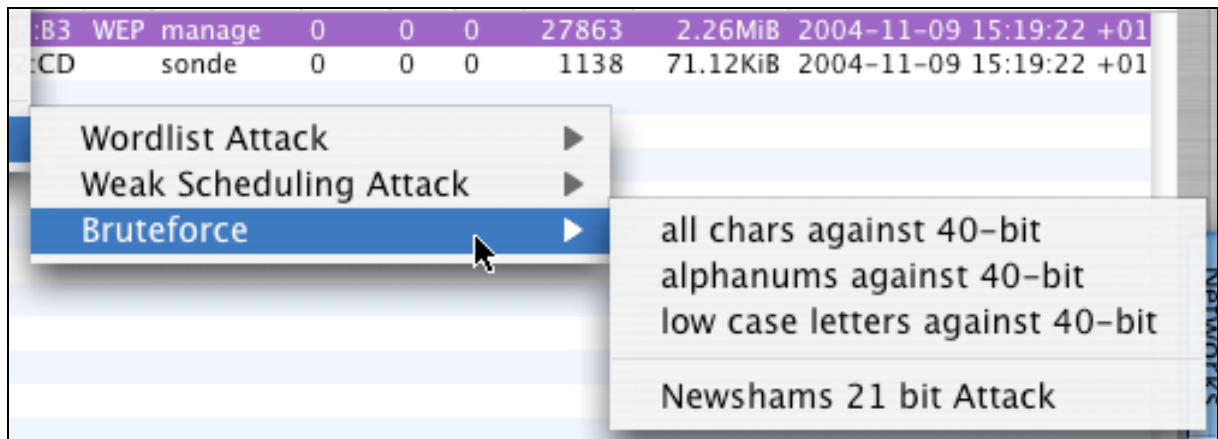
ICV qui correspond au checksum du paquet.

Le principe est donc de :

- récupérer le IV + la taille de la clé (en clair)
- de créer une clé à partir de ces informations
- décrypter le payload + ICV avec cette clé
- de recalculer l'ICV à partir du paquet « décrypté »
- de comparer les 2 ICV

Si les checksum sont les mêmes, la clé est trouvée sinon, on refait la même chose avec la clé potentielle suivante.





### ➤ WordListAttack

Ce système se base sur un liste de mots en clair et effectue une comparaison. Vous trouvez ce genre de liste à l'adresse :

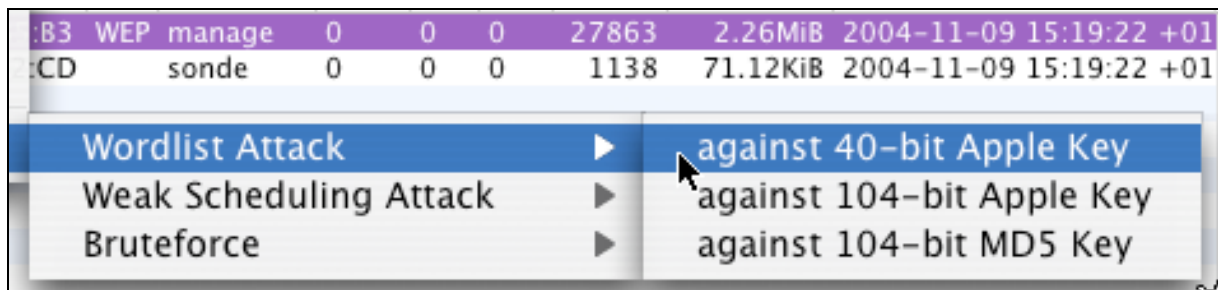
<ftp://ftp.openwall.com/pub/wordlists/>

Le logiciel WepAttack fonctionne sur cette base

Syntaxe : `wepattack -f /tmp/fichier.dump -w /path/to/wordlist`

(<https://sourceforge.net/projects/wepattack>).

KisMac propose la même chose :

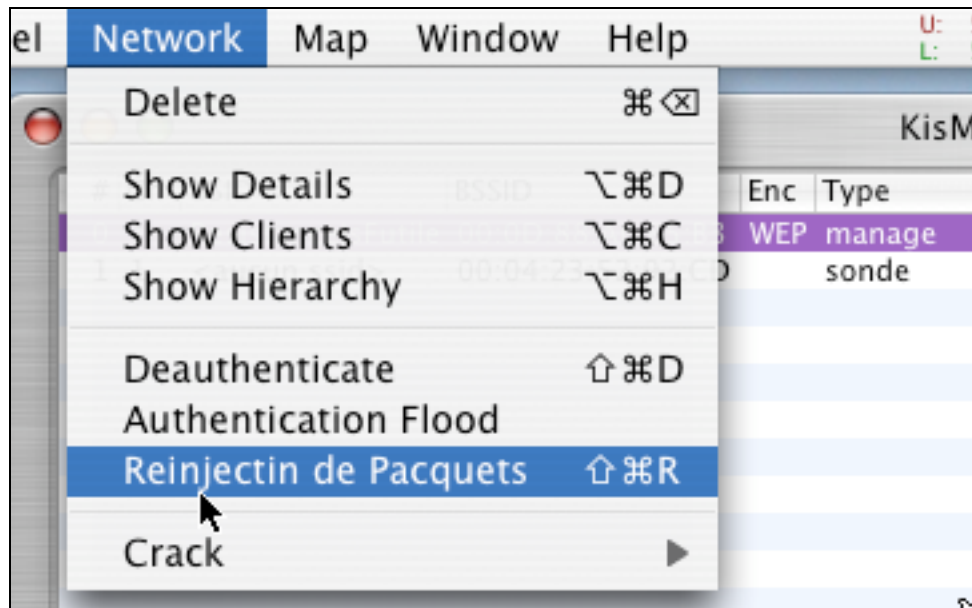


### ➤ FMS Attack (Fluhrer, Mantin, et Shamir Attack)

Cette attaque consiste à récupérer un très grand nombre de paquets et à effectuer une attaque « statistique » sur ces paquets. Le principe est de solliciter au maximum la borne afin de générer un maximum de trafic.

Pour cela la méthode « packet injection » est utilisée.

Un paquet crypté est capturé, exemple un paquet ARP dont la structure est connue. Ce paquet est ensuite renvoyé à la borne de nombreuses fois afin que cette dernière génère beaucoup de trafic en réponse.



### Attention

Les cartes actuelles sur les bornes détectent ce genre d'attaques. Ainsi, la récupération d'un flux de l'ordre de 1Go de paquets devient beaucoup plus longue.

La plupart des outils, comme dwepcrack, essaient de déterminer quel est le premier octet crypté, et seulement celui-ci. En effet, en combinant cet octet et le vecteur d'initialisation (selon un algorithme savant ☺), la clé de cryptage peut être déduite. Ceci permet un gain de temps énorme. Pour plus d'informations, consulter le site du logiciel airtort qui propose des liens expliquant le fonctionnement de cette attaque <http://airtort.shmoo.com/>.

A partir du moment où vous avez récupéré les bonnes informations vous pouvez utiliser des outils de crack. Ils sont plus au moins performant et simple à utiliser.

Le logiciel dwepcrack est assez simple à utiliser. Il existe même une « interface » en shell qui permet de simplifier son utilisation ainsi que l'utilisation des outils de scan.

```
usage: ./dwepcrack [-j <jobs>] [-b [-e] | -w [-f <fudge>]] [-s] <logfile> [wordfile]
-j: number of processes to run (useful for smp systems)
-b: brute force key by exhausting all probable possibilities
-e: search the entire key width (will take a while)
-w: use weak ksa attack
-f: fudge the probability scope by specified count (might take a while)
-s: file uses 104-bit wep
```

```

*****
**
**          wi0 is Ready!
**
**      What do you want to do with it?
**
**      1) dstumble
**      2) dwepdump
**
**      Or what else can we do for you?
**
**      3) stumble report
**      4) dwepcrack
**
**      q) quit (rehab is for quitters)
**
*****

Well what will it be?[1] : 

```

```

*****
**
**          WEP CRACK
**
**      1) 40bit  2) 104 bit  q) rehab
**
*****

hmmm? : 1

What is the name of the file? ../Scan127/ScanG3/Dump/DumpLogEnCours

```

Si le nombre de vecteur d'initialisation et de paquets contenant les informations nécessaires ne sont pas présents le logiciel vous affiche l'écran suivant :

```
* dwepcrack v0.4 by h1kari <h1kari@dachb0den.com> *  
* Copyright (c) Dachb0den Labs 2002 [http://dachb0den.com] *
```

```
reading in captured ivs, snap headers, and samples... done  
total packets: 29105
```

```
calculating ksa probabilities...
```

```
0: 0/768 keys (!)  
1: 0/131328 keys (!)  
2: 0/197376 keys (!)  
3: 0/197120 keys (!)  
4: 0/328703 keys (!)  
5: 0/328192 keys (!)  
6: 0/459520 keys (!)  
7: 0/459264 keys (!)  
8: 0/590592 keys (!)  
9: 0/590336 keys (!)  
10: 0/721664 keys (!)  
11: 0/721408 keys (!)  
12: 0/852736 keys (!)
```

```
(!) insufficient ivs, must have > 60 for each key (!)  
(!) probability of success for each key with (!) < 0.5 (!)
```

```
warming up the grinder...
```

```
packet length: 516  
init vector: 8b:96:2c  
default tx key: 0
```