



# Réseaux sans fil

Daniel AZUELOS  
Architecture réseau  
Institut Pasteur



# Table des matières

<b>Réseaux sans fil</b>	<b>3</b>
Ondes électro-magnétiques .....	4
Spectre électro-magnétique .....	5
802.11b .....	6
Fonctionnement .....	7
Types de réseaux .....	9
Mobilité.....	10
Réglementation .....	11
Mise en œuvre .....	12
Propagation .....	14
Transparence .....	15
Interférences .....	16
Couverture .....	17
Prérequis .....	18
Installation .....	19
Configuration .....	20
Sécurité des personnes .....	23
Sécurité des SI .....	24
Contrôle d'accès .....	25
WEP : Wired Equivalent Privacy .....	26
RC4 .....	27
Extranet.....	28
Filtrage .....	29
Plan de déploiement .....	30
Évolutions .....	31



# Réseaux sans fil

Réseaux utilisant des ondes hertziennes pour établir une liaison entre 2 équipements mobiles.

Dénominations :

- WLAN : Wireless LAN ;
- RLAN : Radio LAN ;
- RLR : Réseau Local Radio ;
- AirPort : Apple ;

→ réseaux sans fil !

Idée : onde hertzienne  $\approx$  porteuse  
+ transport de données numériques / porteuse.

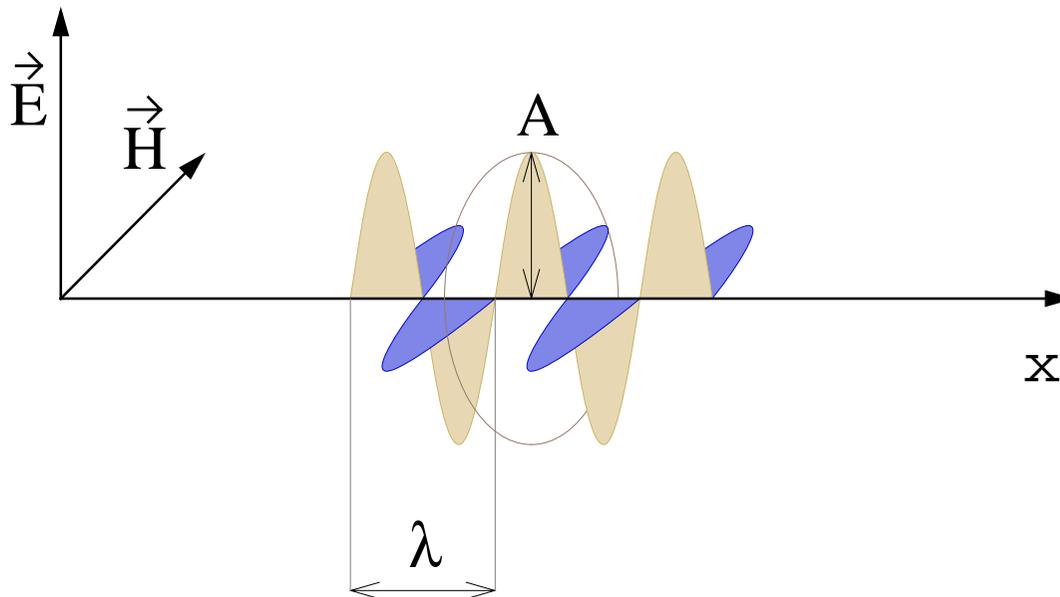
Utilisée pour les transmissions satellite.

## Ondes électro-magnétiques

Ondes radios, infra-rouge, visible, ultra-violet, X,  $\gamma$ ...

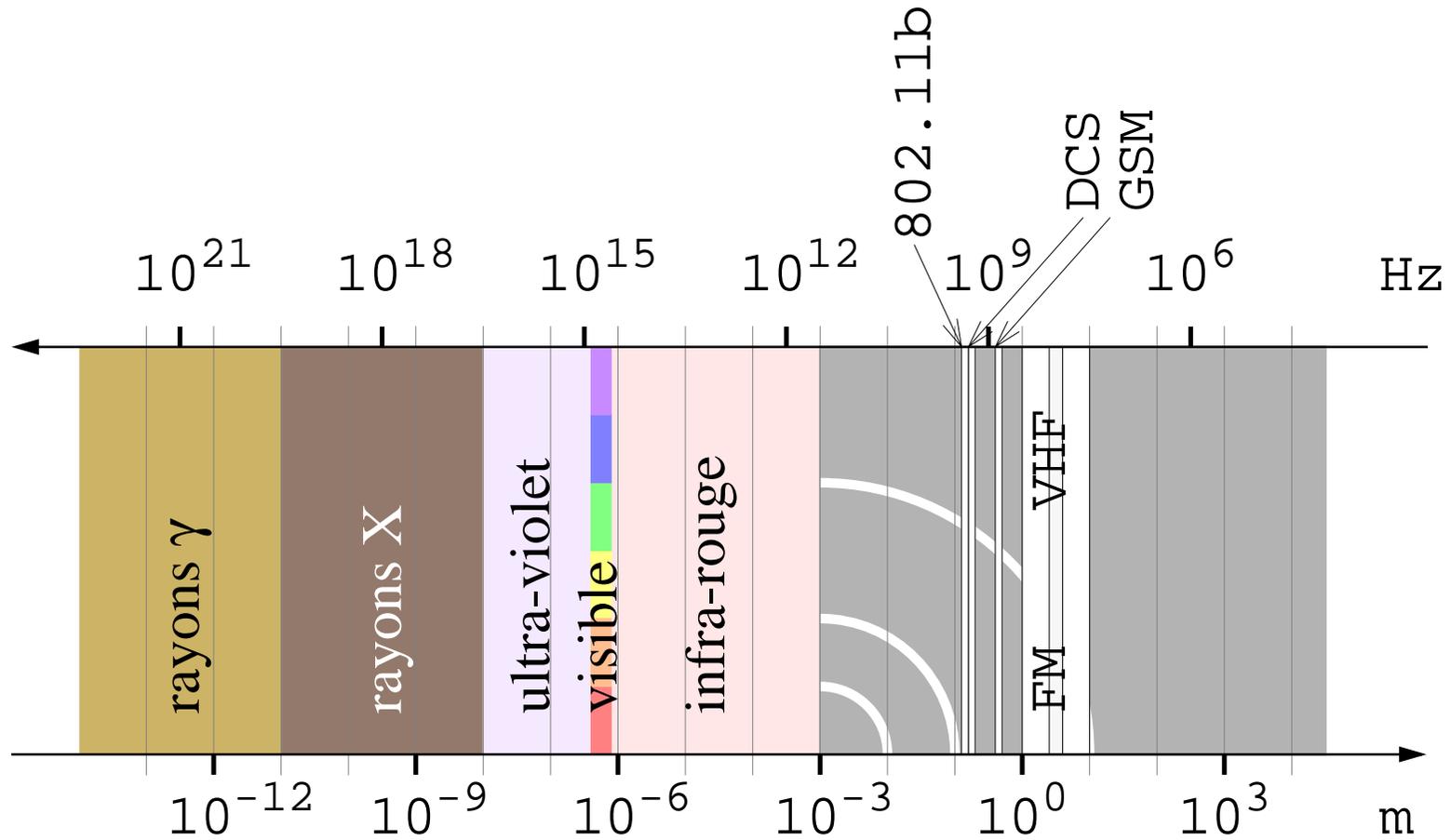
$$\lambda \times f = c \approx 3 \times 10^8 \text{ m/s .}$$

$$f = 2,4 \text{ GHz}$$
$$\lambda = 12,5 \text{ cm}$$





# Spectre électro-magnétique





## 802.11b

IEEE :      1997 → 802.11  
              1999 → 802.11b

Standards spécifiant les méthodes d'accès à un medium physique permettant la construction de réseau.

Le medium physique est ici une bande de fréquence : **2,4 GHz**.

Utilisation du medium : DSSS (Direct Sequence Spread Spectrum). 14 canaux, seuls 11 sont utilisables aux U.S.A., 4 en France : [10 ; 13].

Méthode d'accès : CSMA/CA (diffusion ≈ Ethernet).

Débits : **11 Mbit/s** ; 5,5 Mbit/s ; 2 Mbit/s ou 1 Mbit/s.

Débit adapté automatiquement en fonction du rapport S/B.



## Fonctionnement

Antenne (= émetteur & récepteur) : carte Wavelan (Lucent).

Carte Wavelan  $\approx$  carte Ethernet / modem / émetteur.

Une borne AirPort = répéteur à 3 interfaces :

1 modem V90 ;

1 carte Ethernet 10 Mbit/s ;

1 carte Wavelan 11 Mbit/s.

Visibilité radio  $\Rightarrow$  établissement d'une liaison.

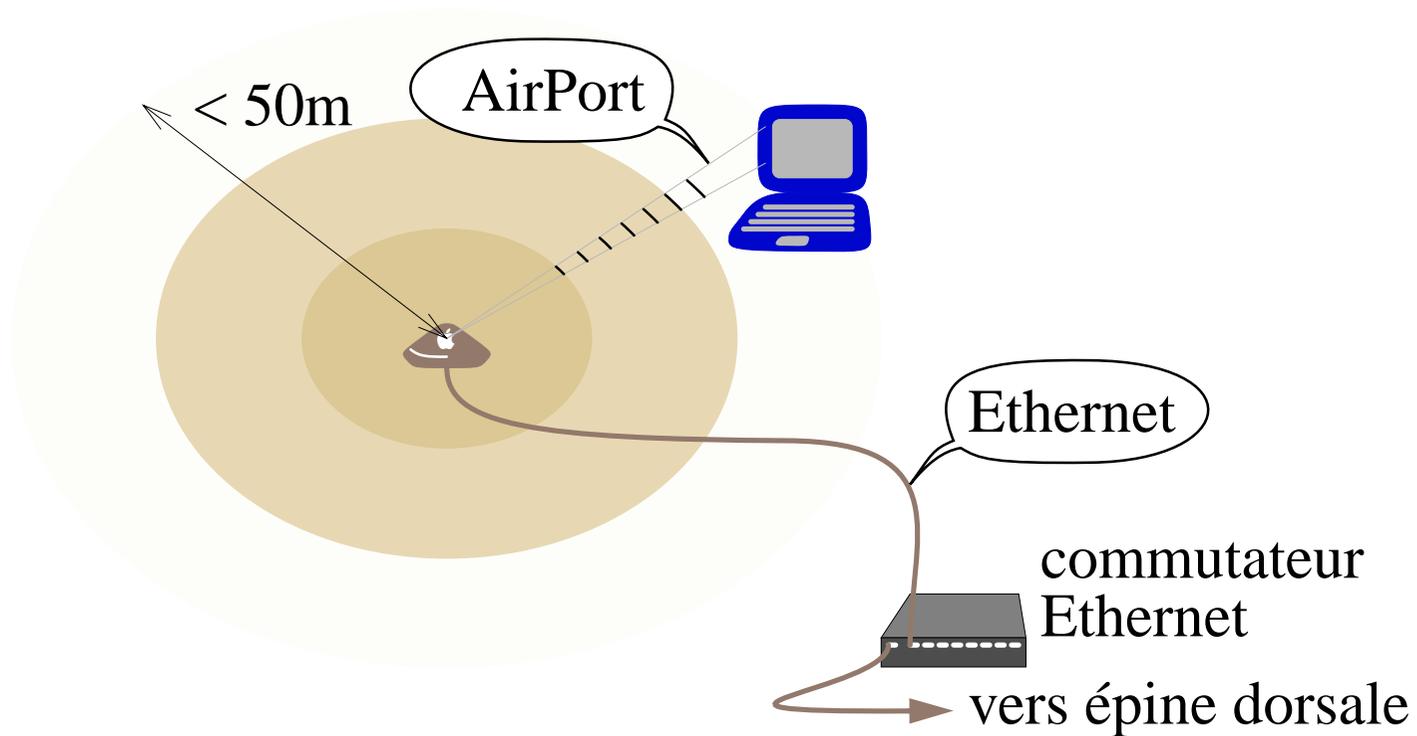
Déplacement

$\Rightarrow$  variabilité du S/B

$\Rightarrow$  renégociation de la vitesse utilisable sur la liaison.

Éloignement, obstacle  $\Rightarrow$  suppression de la liaison.

## Fonctionnement



Une liaison  $\Rightarrow$  2 cartes AirPort !

Raccordement au reste du réseau  $\Rightarrow$  liaison Ethernet.



## Types de réseaux

Point à point : comme avec un câble Ethernet croisé. Par contre, on peut être plus de 2 sur le même support (l'espace somme des portées des  $\neq$  différentes cartes participant).

Réseaux isolés : nom de réseau propre, une seule antenne  
→ accès ponctuel.

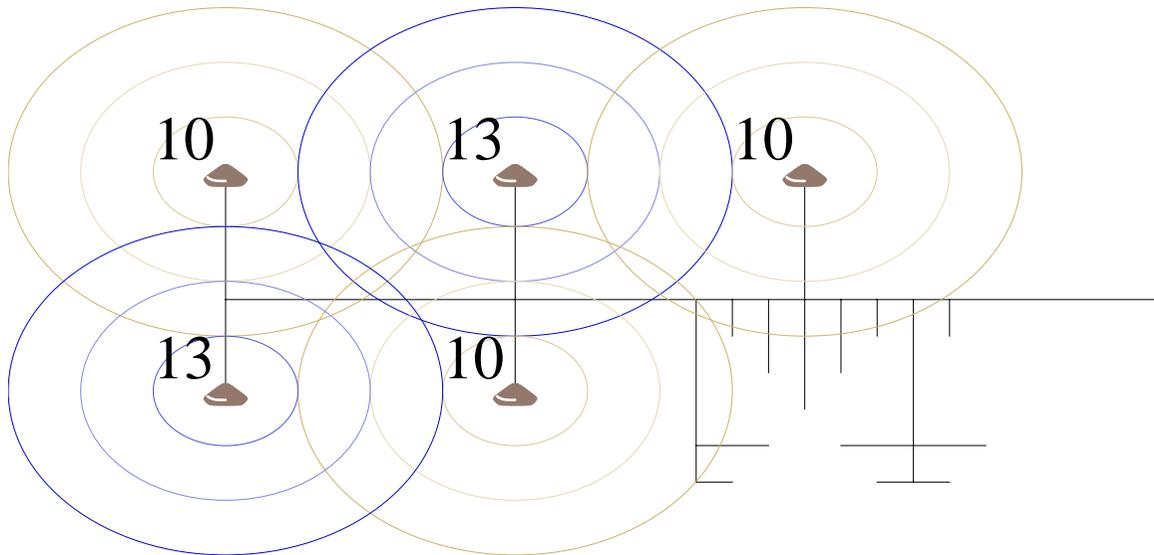
Réseaux pavés : même nom de réseau, plusieurs antennes, canaux distincts  
→ accès / grand espace & nombreux utilisateurs  
⇒ mobilité.

Réseaux fermés : réseau dont l'accès est protégé par un mot de passe (secret partagé = :O).

## Mobilité

La nature de la liaison permet naturellement la mobilité à l'intérieur du champ d'une antenne.

Au delà, un portable peut passer de l'une à l'autre :  
⇒ intersection de champs sans interférence.





## Réglementation

L'ART (Autorité de Régulation des Télécommunications) limite l'utilisation de 802.11b à la bande de fréquences :

2446,5 MHz - 2483,5 MHz :

arrêté du 31/07/2001 ;

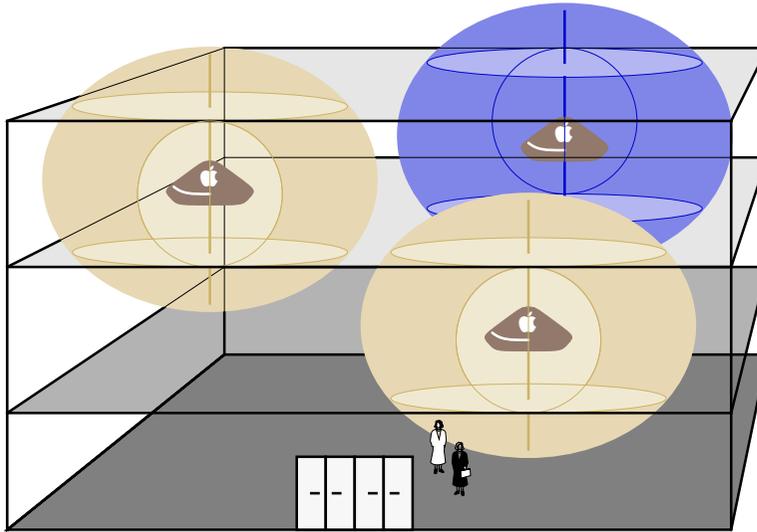
→ <http://www.art-telecom.fr/dossiers/rlan/corps.htm>

- puissance rayonnée doit être  $< 100$  mW ;
- utilisation à l'intérieur des bâtiments : libre ;
- utilisation sur la voie publique : **interdite** !

Utilisation à la maison : libre (à l'intérieur des bâtiments)

⇒ attention aux voisins (perturbation, écoute) !

## Mise en œuvre



### Contraintes à respecter :

- spatiale : couverture maximale, interférence minimale ;
- sécurité : des personnes, des données ;
- matérielle : raccordement aux réseaux électrique et Ethernet.



## Mise en œuvre

Un réseau sans fil est un choix pertinent de construction d'accès :

- dans un grand espace ;
- pour plusieurs portables qui occupent un même lieu mais à  $\neq$  moments ;
- loin d'une baie informatique ( $> 100\text{m}$ ) ;
- en des zones où le passage de câbles Ethernet n'est pas envisageable (labo. + normes de sécurité, bâtiment classé).

Nous construisons 2 types de réseaux sans fil :

- réseau interne en libre service  $\rightarrow$  bibliothèques, salles de réunion ou conférence ;
- extensions de réseaux Ethernet en attente de réfection ou extension difficile.



## Propagation

Une onde électro-magnétique se propage en ligne droite, à vitesse  $c \approx 3 \times 10^8$  m/s dans le vide. Dans tout autre milieu, elle peut être :

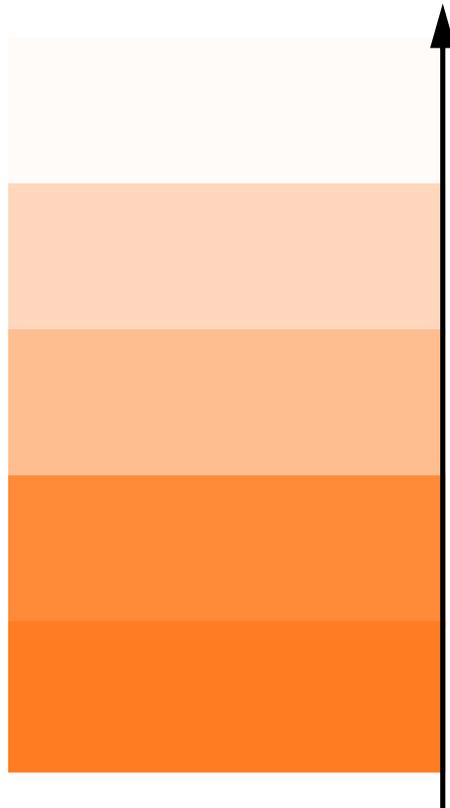
- réfractée ;
- réfléchie ;
- diffractée ;
- absorbée.

Une onde électro-magnétique est absorbée par un circuit résonnant à sa fréquence : plomb, nos os, O<sub>2</sub>, l'atmosphère, H<sub>2</sub>O, la pluie, le maillage du béton armé.

Elle interfère avec toute autre onde de fréquence proche  
→ battement spatial & temporel.



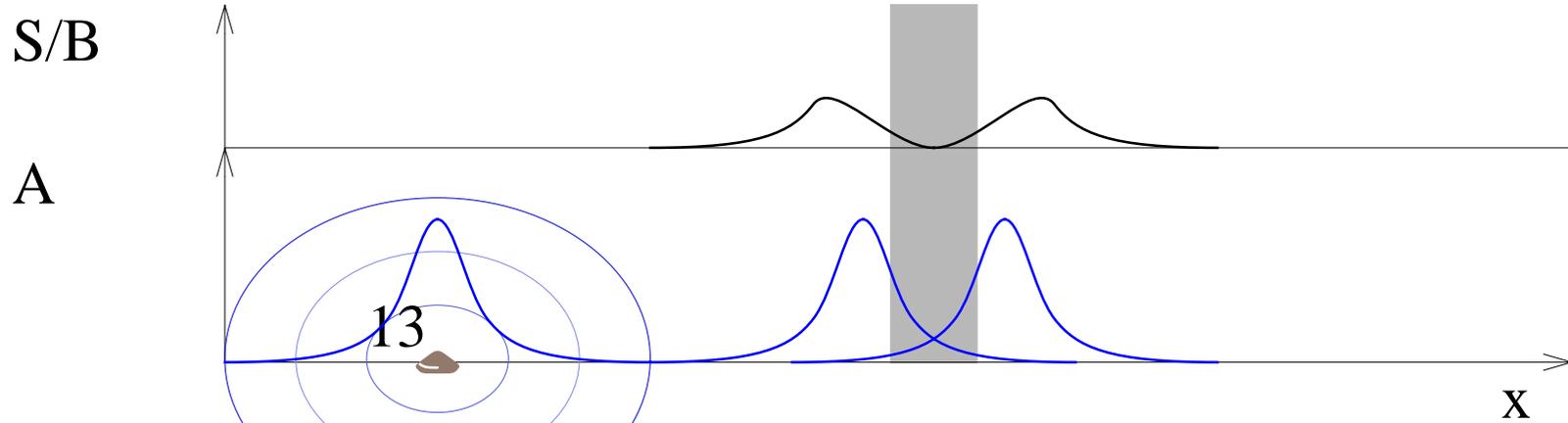
## Transparence



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



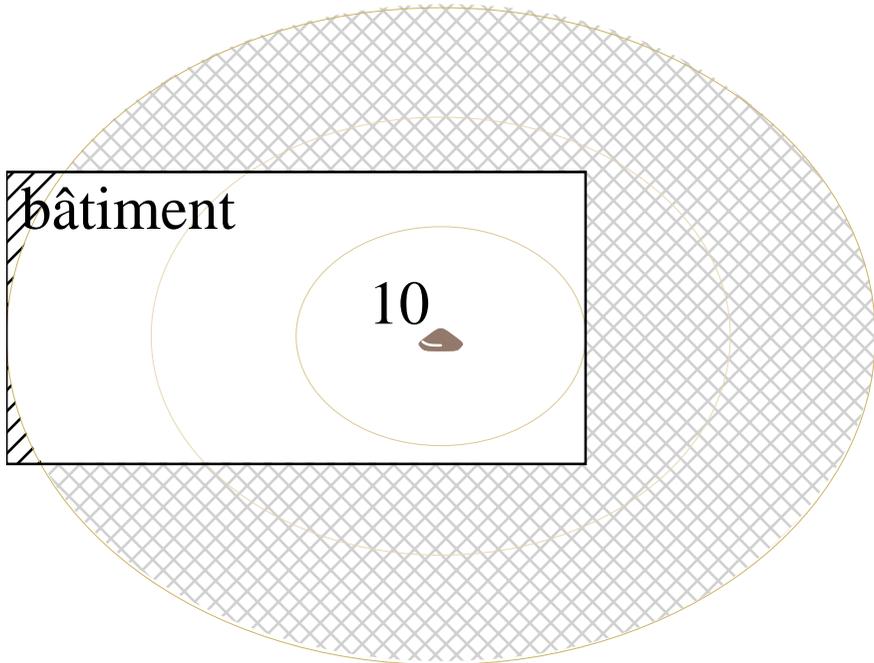
# Interférences





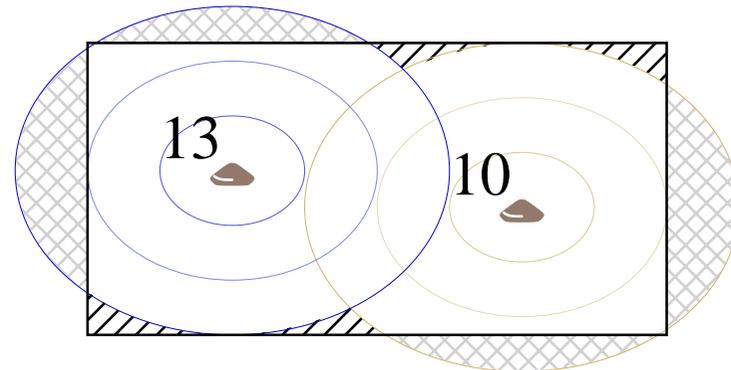
# Couverture

60 mW



défaut de :  couverture  
 sécurité

30 mW





## Prérequis

Portables : iBook, PB G3 (récents), PB G4 ;  
modèles avec emplacement PCMCIA ;

Transportables : iMac (sauf 1er modèle) ;

Systeme : MacOS  $\geq$  9.0.4,  
NetBSD, Linux,  
Windows 98 (sur portable + carte PCMCIA).

Des solutions existent sur d'autres systèmes d'exploitation et d'autres types de matériels. Pour l'instant il s'agit essentiellement de solutions de « suiveurs » qui apportent plus de problèmes que d'innovations :  
 $\Rightarrow$  trop coûteuses en temps de maintenance.



## Installation

2 possibilités :

- pré-installation acheté à la commande d'un portable :  
<http://til.info.apple.com/techinfo.nsf/↵artnum/n95137> ;
- nous acheter une carte AirPort :  
interne ou bien PCMCIA ( $\approx 100$  ).

Le logiciel est automatiquement inclus avec MacOS 9.0.4.

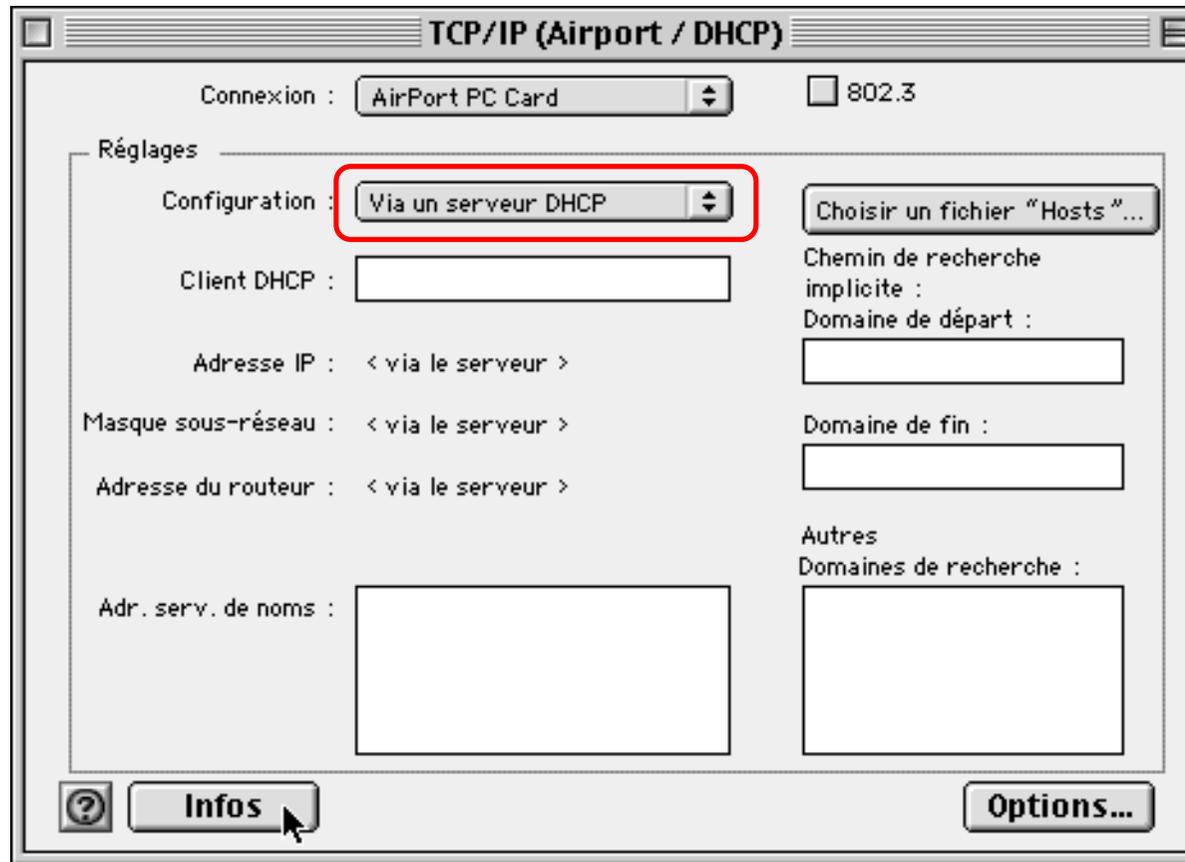
Temps d'installation (matérielle + logicielle) < 30' !

Temps d'installation & configuration d'une borne : 1 j.

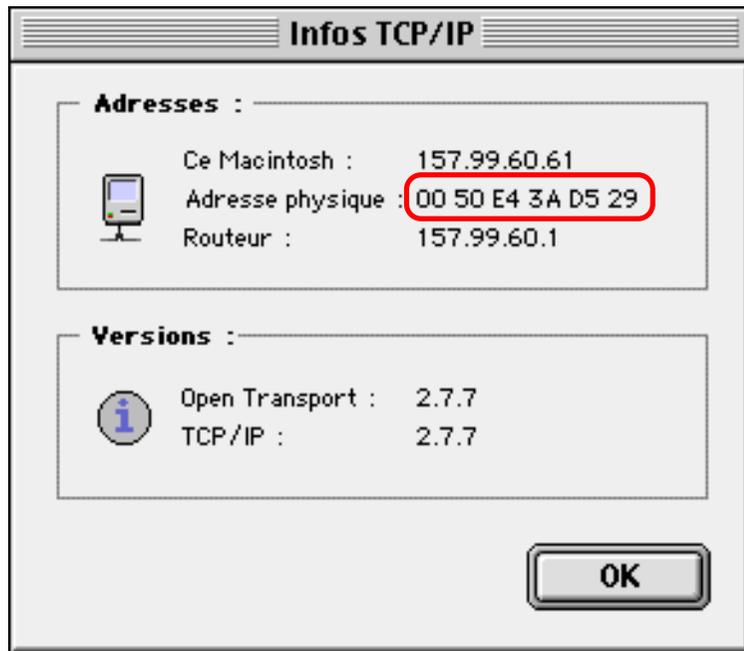
Croissant vite avec le recouvrement des portées.

## Configuration

AppleTalk et TCP/IP sur AirPort (→ Réglages de mobilité).



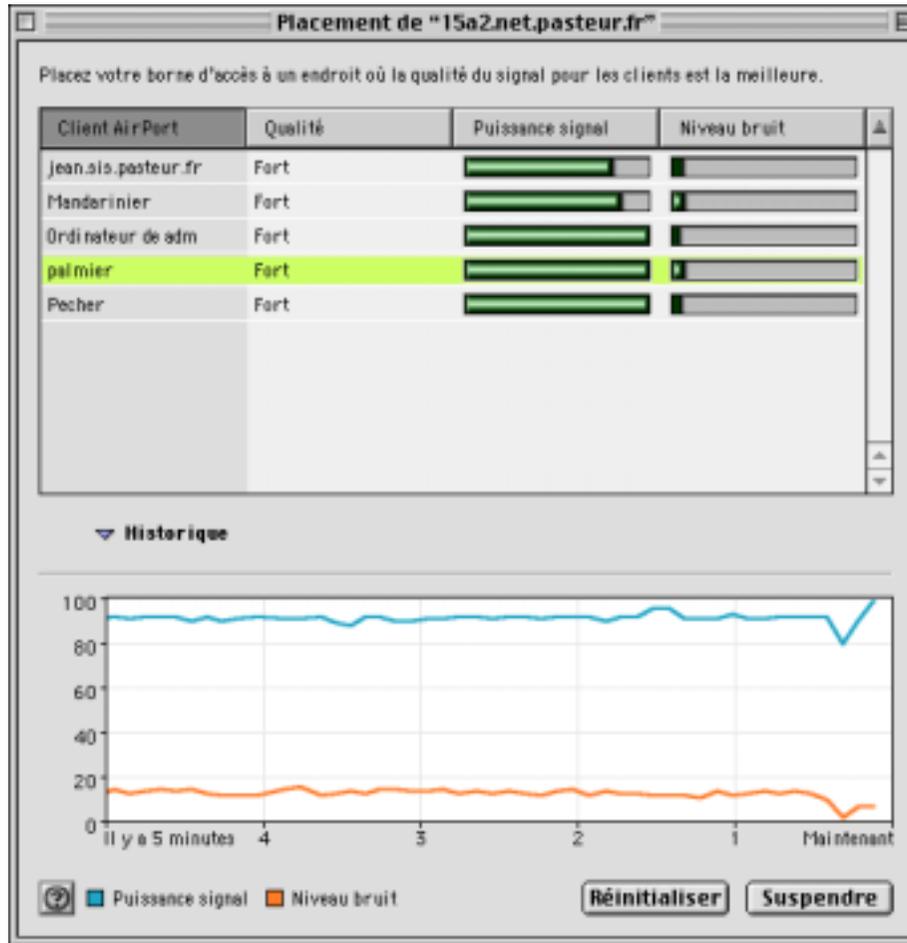
## Configuration



Adresse physique : propre à chaque interface et accessible lorsque le port est actif.

Nous la communiquer à la demande de raccordement  
→ intégration sur notre serveur DHCP.

## Configuration



Placement :

initial (densité faible)

→ 1/2 j ;

densité élevée

→ 1 j.



## Sécurité des personnes

Les normes internationales d'utilisation des radio fréquences spécifient puissance rayonnée  $< 100$  mW.

Apple a choisi d'utiliser une puissance  $\approx$  **30 mW** !

$\Rightarrow$  champs réduits en puissance et portée ;

$\Rightarrow$  facilité de couverture de volumes complexes.

Santé publique : nombreuses études en cours, surtout au sujet de l'utilisation des téléphones mobiles :

[http://www.sante.gouv.fr/↓  
htm/dossiers/telephon\\_mobil/](http://www.sante.gouv.fr/↓<br/>htm/dossiers/telephon_mobil/)

GSM :  $< 2$ W ;

DCS :  $< 1$ W.

Antennes GSM : 20 à 50 W ;

émetteur de la tour Eiffel : **6 MW** !



## Sécurité des SI

Transport de données  $\Rightarrow$  champ électro-magnétique !

(  $\Rightarrow$  un câble Ethernet n'aime ni les tubes fluorescents, ni les câbles électriques !)

3 types d'utilisations de champs :

- canalisée / conducteur : 10baseT, fibre optique, sortie vidéo, câble clavier ;
- directive : ondes hertziennes focalisées sur un axe ;
- diffusive : ondes hertziennes diffusées, tube cathodique.

Tous ces transports de données peuvent être  $\pm$  facilement écoutés. Dans le cas du 802.11b, les possibilités d'écoute sont plus simples que sur un réseau Ethernet partagé : 0 prise.

$\Rightarrow$  contrôle d'accès à ce type de réseau.



## Contrôle d'accès

- spatial : mesures de contrôle de portée, utilisation active des obstacles à la diffusion ;  
maîtrise de toute façon nécessaire à une mise en œuvre de ce genre de réseau ;
- par adresse : seules les adresses MAC enregistrées peuvent se joindre à un réseau ;
- par WEP : Wired Equivalent Privacy ;
- par architecture du réseau : les accès à ce type de réseau dans des espaces où les contrôles précédents ne sont pas souhaités sont limités à un **extranet**.



## **WEP : Wired Equivalent Privacy**

But de l'IEEE : amener le réseau sans fil au niveau de sécurité d'accès d'un réseau Ethernet (partagé).

C'est une réussite et un échec. Objectif atteint, mais objectif ridicule : on écoute aussi bien un réseau 802.11b qu'un Ethernet partagé.

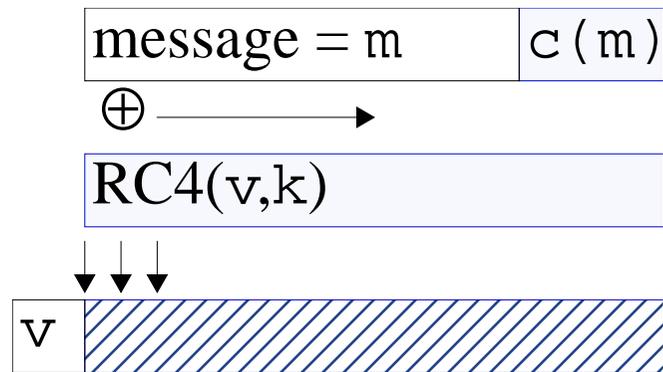
Protocole de chiffrement à clé symétrique partagée, sans protocole de gestion, RC4.

Mise en œuvre mal adaptée à un grand réseau :

- clé secrète partout : non gérable ;
- RC4 mal initialisé ;
- possibilité de générer du texte clair & choisi (ping).

## RC4

RC4 = Rivest Code



$$\begin{aligned} |v| &= 24 \\ |k| &= 40 \text{ ou bien } 104 \\ c &: m \rightarrow c(m) \end{aligned}$$

$k$  est la clé symétrique partagée.

$v$  est un vecteur d'initialisation « aléatoire ».

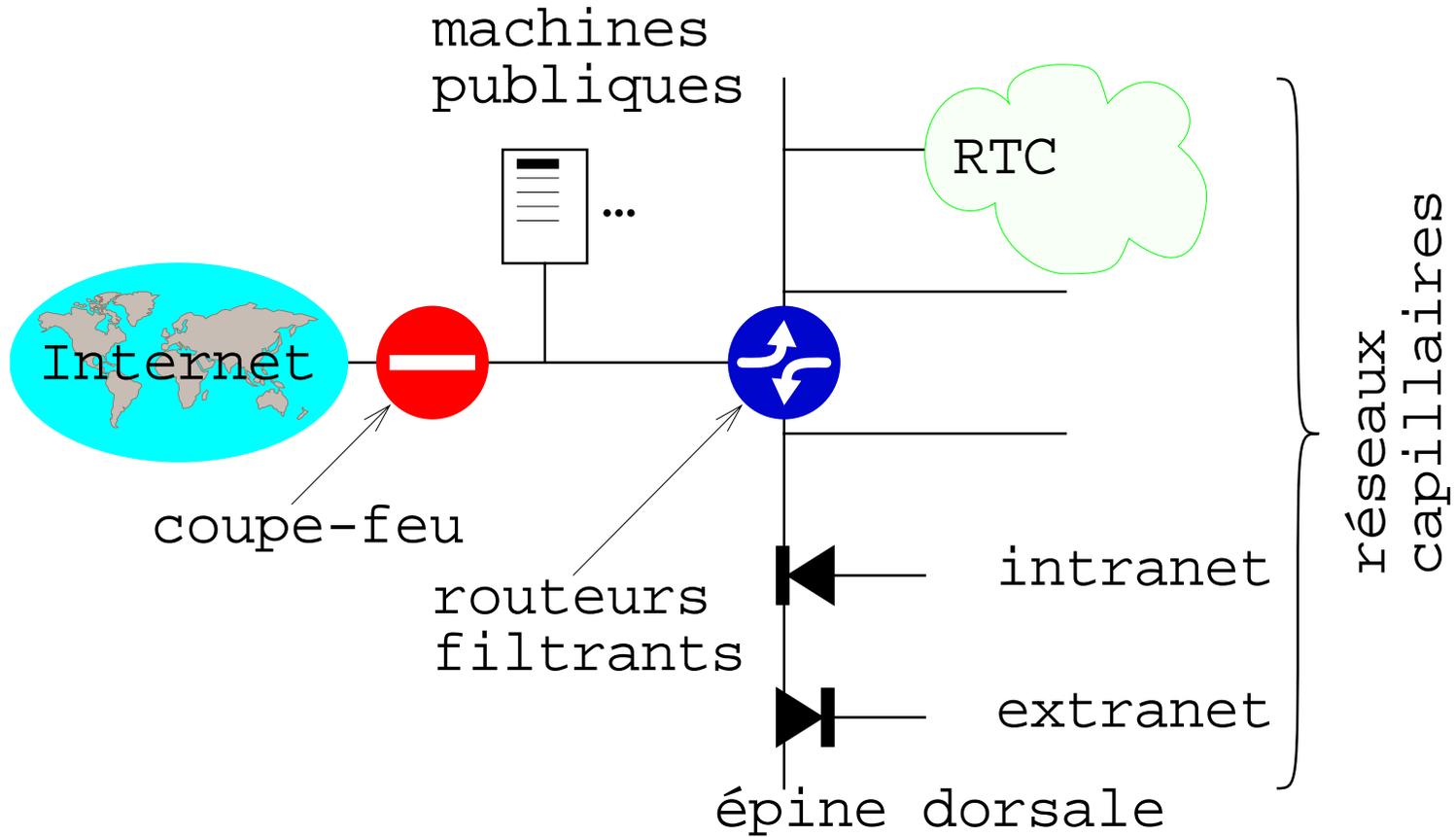
Dans le cas d'AirPort, Apple a amélioré sa qualité :  $k$  est généré à partir d'un mot de passe.



$v$  et  $m$  sont prédictibles.



# Extranet





## Filtrage

Aucun accès IP aux équipements actifs.

DNS vers nos serveurs ;

DHCP ( $\Rightarrow$  bootp) vers nos serveurs ;

TCP vers le réseau des « machines publiques ».

Aucun accès IP vers les autres réseaux capillaires.

Tout autre accès IP (i.e. le reste de l'Internet) autorisé.



## Plan de déploiement

**2001 :** 4 bornes ; 10 Mac raccordés ;  
présentation au CHSCT → accord pour continuer.

**2002 :** 15 bornes ; 50 ordinateurs sans fil ;  
→ 100 ? en fin d'année ;  
essais d'autres équipements plus « gérables » à  
grande échelle ;  
tests d'interopérabilité.

Pourquoi continuer ? Le périmètre de sécurité se tient là !  
Pourquoi Apple ? 2 ans d'avance + intégration antenne +  
qualité du logiciel.



## Évolutions

**1999** : 802.11b ; norme d'interopérabilité WiFi ;

**2002 ?** :

802.11a : 54 Mbit/s / 5 GHz, incompatible 802.11b ;

802.11g :  $\geq 20$  Mbit/s / 2,4 GHz, compatible 802.11b ;

HiperLAN/2 : équivalent européen (ETSI) du 802.11a  
54 Mbit/s / 5 GHz ;

802.11i : groupe de travail sécurité (chiffrement / 802.11b) ;

802.1x : authentification d'accès au réseau par (compte,  
mot de passe).