INSTITUT PASTEUR

Réseaux sans fil

Daniel AZUELOS
Architecture réseau & sécurité
Institut Pasteur

22 mai 2003

Table des matières

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 !

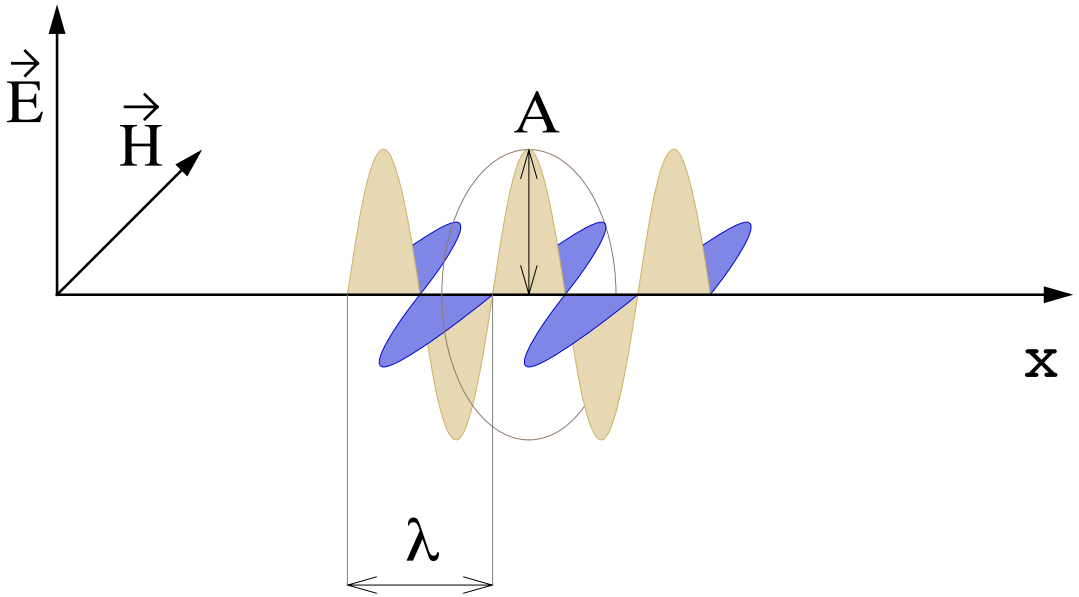
Principe : onde hertzienne = porteuse
+ transport de données numériques / porteuse.

Utilisée pour les transmissions satellite.

Ondes électro-magnétiques

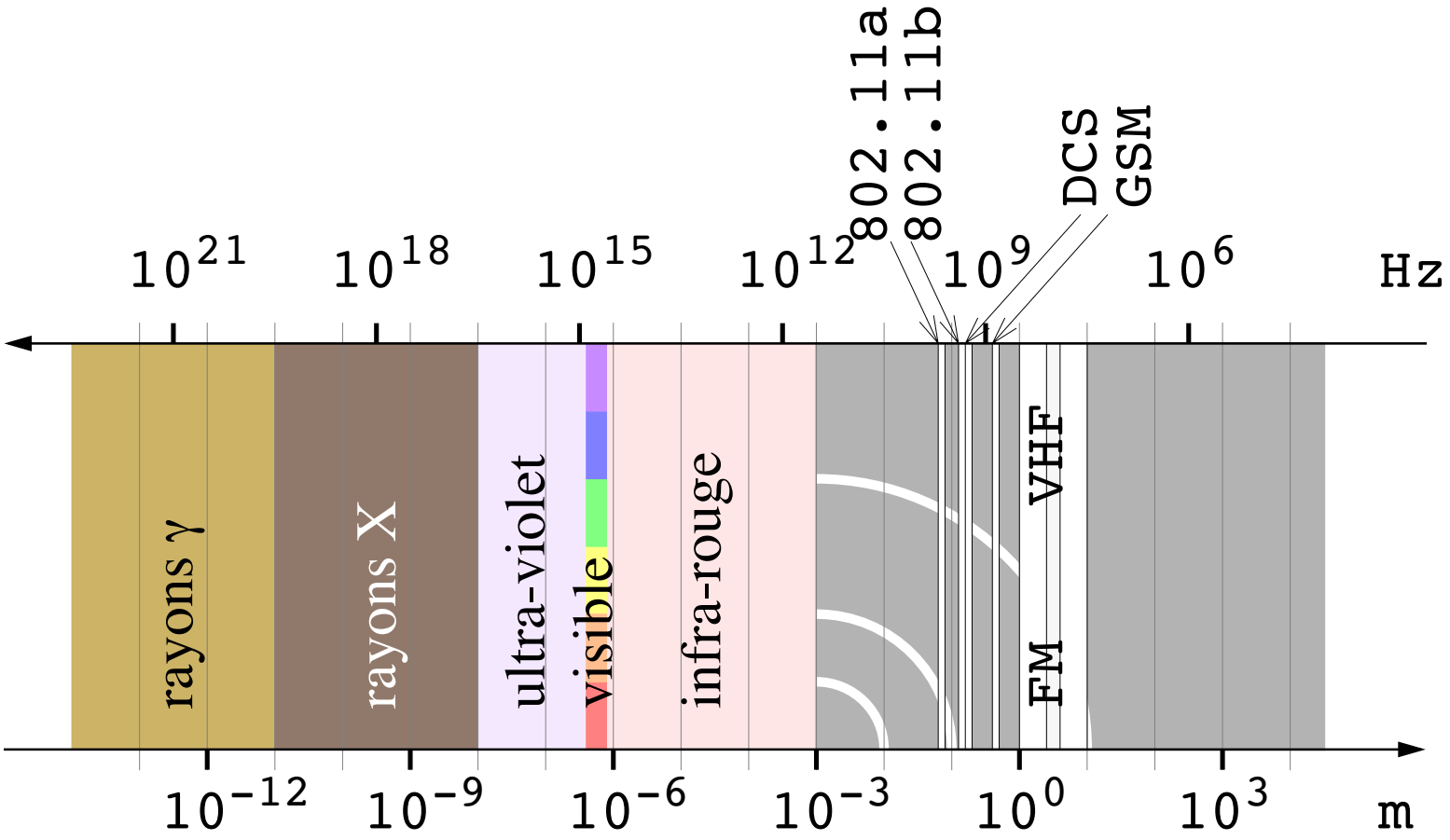
Ondes radios, infra-rouge, visible, ultra-violet, X, γ…

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



f (GHz)	λ (cm)
0,9	33,3
1,8	16,5
2,4	12,5
5,5	5,5

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**.

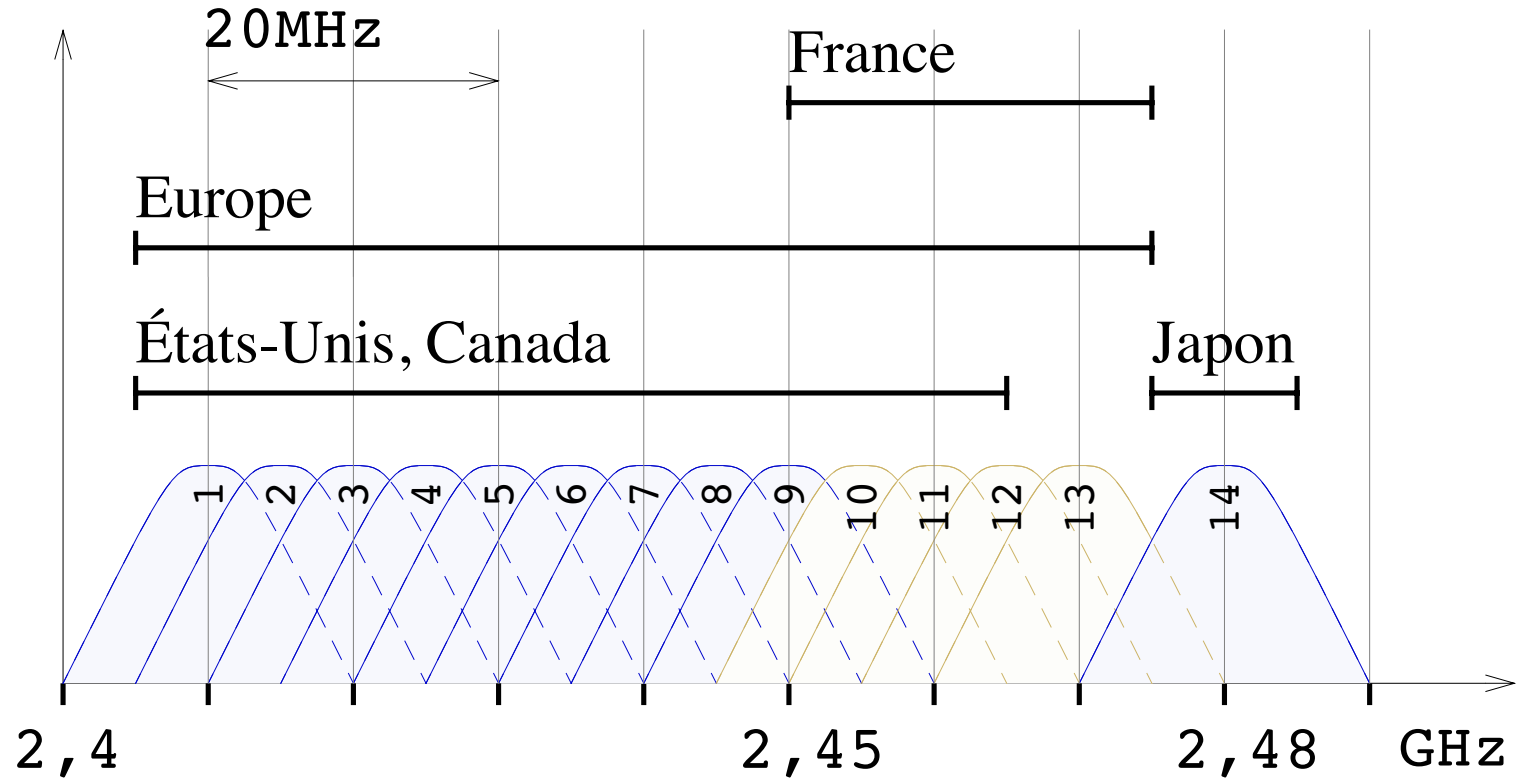
Utilisation du medium : DSSS (Direct Sequence Spread Spectrum). 14 canaux, seuls 11 sont utilisables aux U.S.A., 4 en France : [10 ; 13].

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.

802.11b : canaux



Bande ISM (Industrial, Scientific, and Medical).

Fonctionnement

Antenne (= émetteur & récepteur) : carte AirPort.

Carte AirPort ≈ modem + émetteur/récepteur radio.

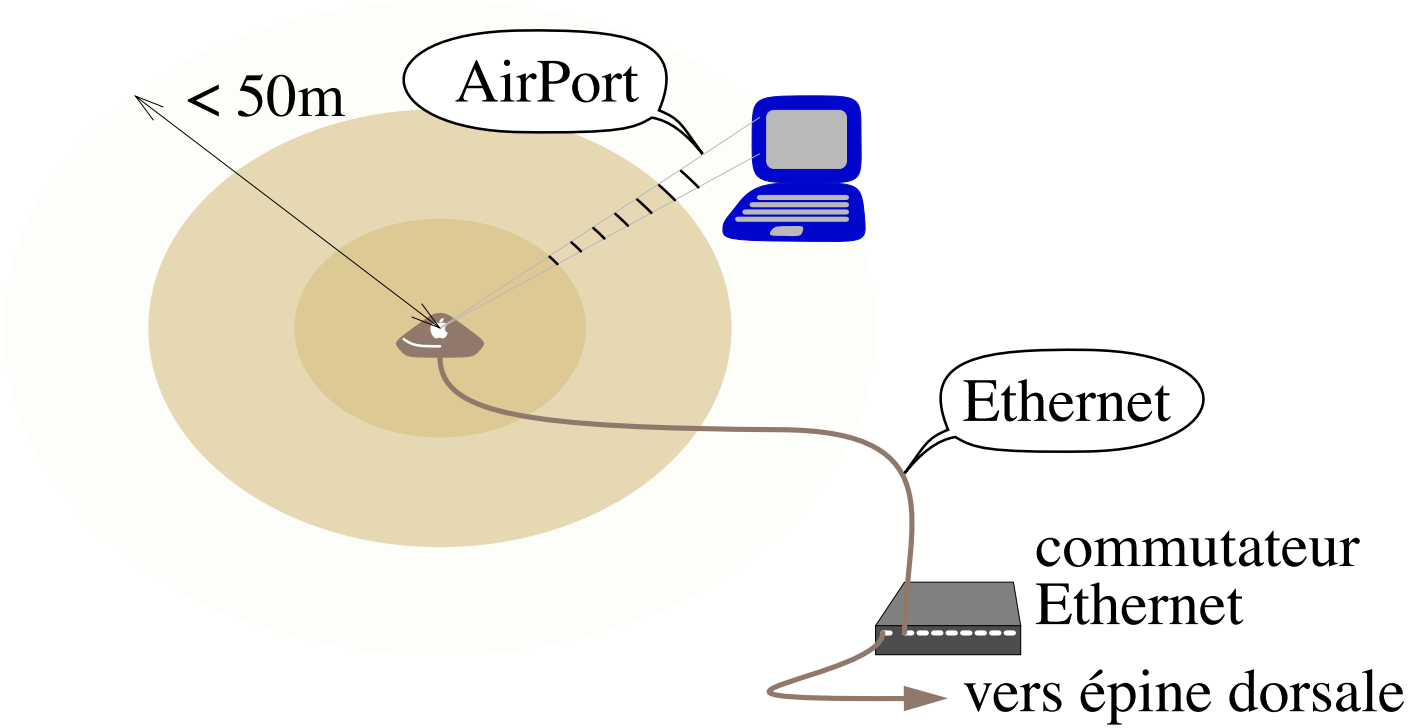
Une borne AirPort = répéteur à 3 interfaces :
1 modem V90 +1 carte Ethernet + 1 carte AirPort.

Visibilité radio ⇒ établissement d'une liaison.

Déplacement
⇒ variabilité du S/B
⇒ renégociation de la vitesse utilisable sur la liaison.

Éloignement, obstacle ⇒ perte de la liaison.

Fonctionnement



Une liaison ⇒ 2 cartes AirPort !

Raccordement au reste du réseau ⇒ liaison Ethernet.

Types de réseaux

Point à point ≈ câble Ethernet croisé.
On peut être plus de 2 sur le même support (l'espace somme des portées des ≠ 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.

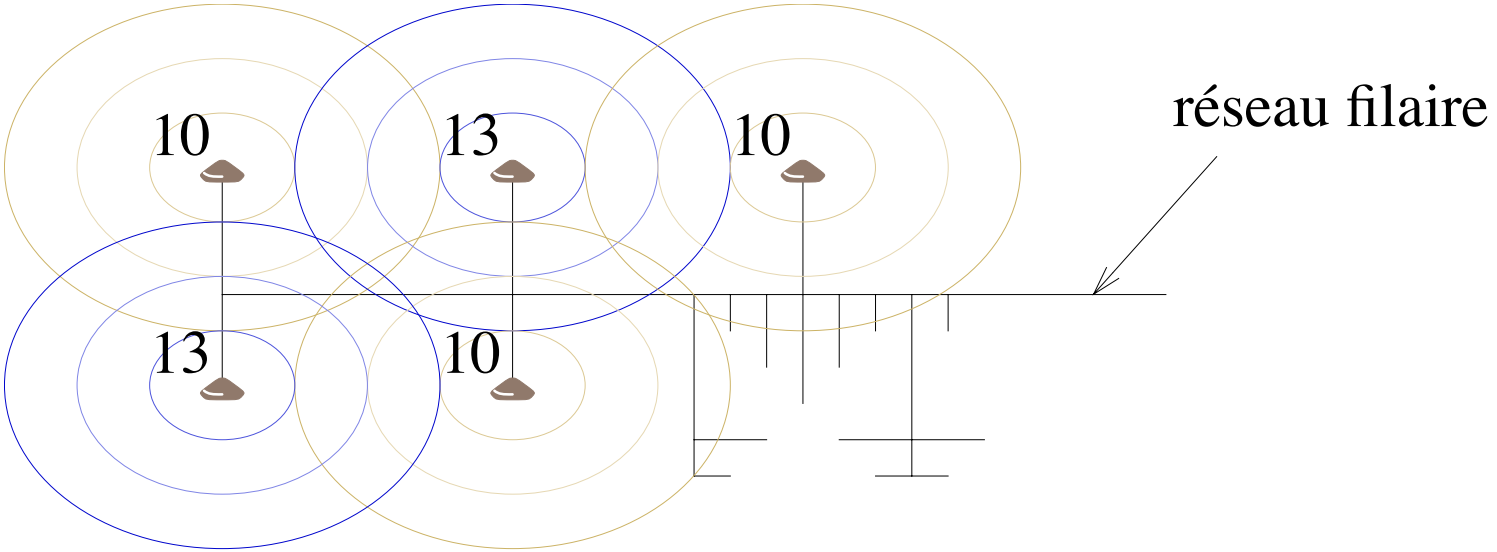
Réseaux fermés : réseau dont l'accès est protégé par un mot de passe (secret partagé = :O).

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 31/10/2002 ;

→ `http://www.art-telecom.fr/↵ dossiers/rlan/corps.htm`

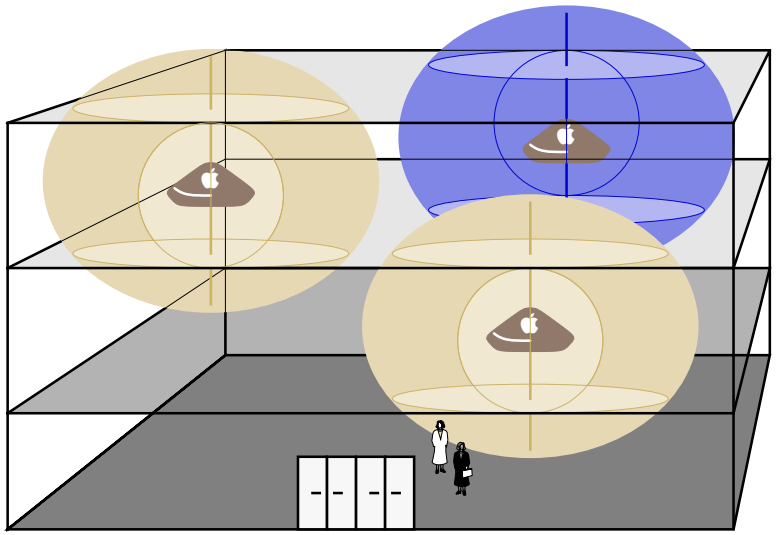
- puissance rayonnée < 100 mW ;
- utilisation à l'intérieur des bâtiments : libre ;
- utilisation sur la voie publique : **interdite** !

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

⇒ attention aux voisins (perturbation, écoute) !

[2400 - 2446,5] MHz libre (en intérieur) → 01/2004 ?

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 ≠ moments ;
- loin d'une baie informatique (> 100m) ;
- 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 → bibliothèques, salles de réunion ou conférence ;
- extensions de réseaux Ethernet en attente de réfection ou extension difficile.

Propagation

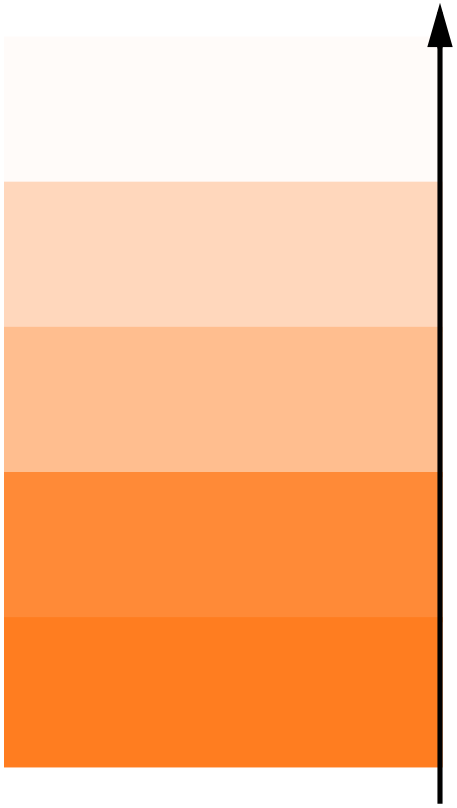
Une onde électro-magnétique se propage en ligne droite, à vitesse $c \approx 3 \times 10^8 m/s$ dans le vide. Dans tout autre milieu, elle peut être :

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

Une onde électro-magnétique est absorbée par un circuit résonnant à sa fréquence : plomb, nos os, O_2, l'atmosphère, H_2O, la pluie, le maillage du béton armé.

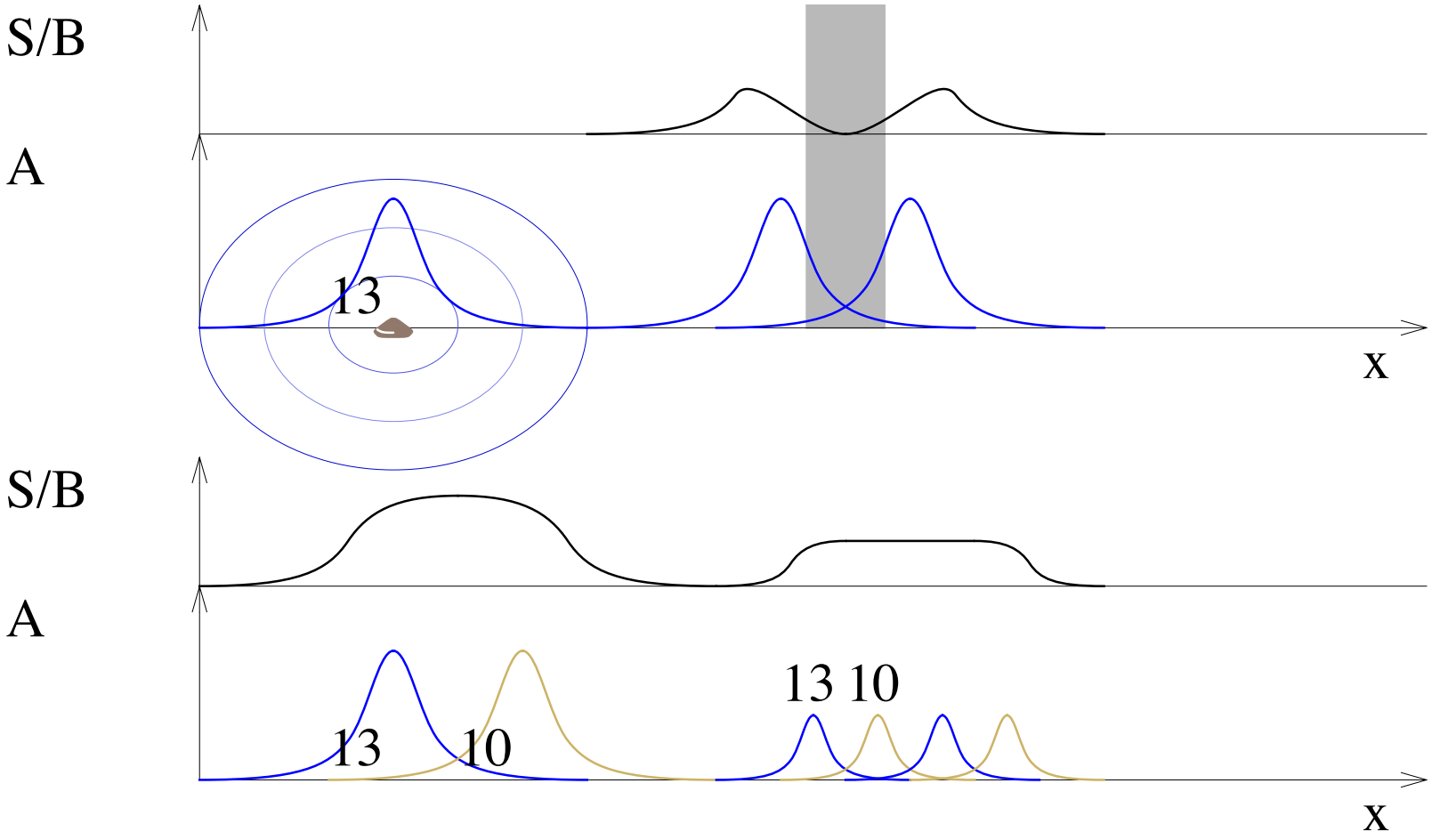
Elle interfère avec toute autre onde de fréquence proche
→ battement spatial & temporel.

Transparence

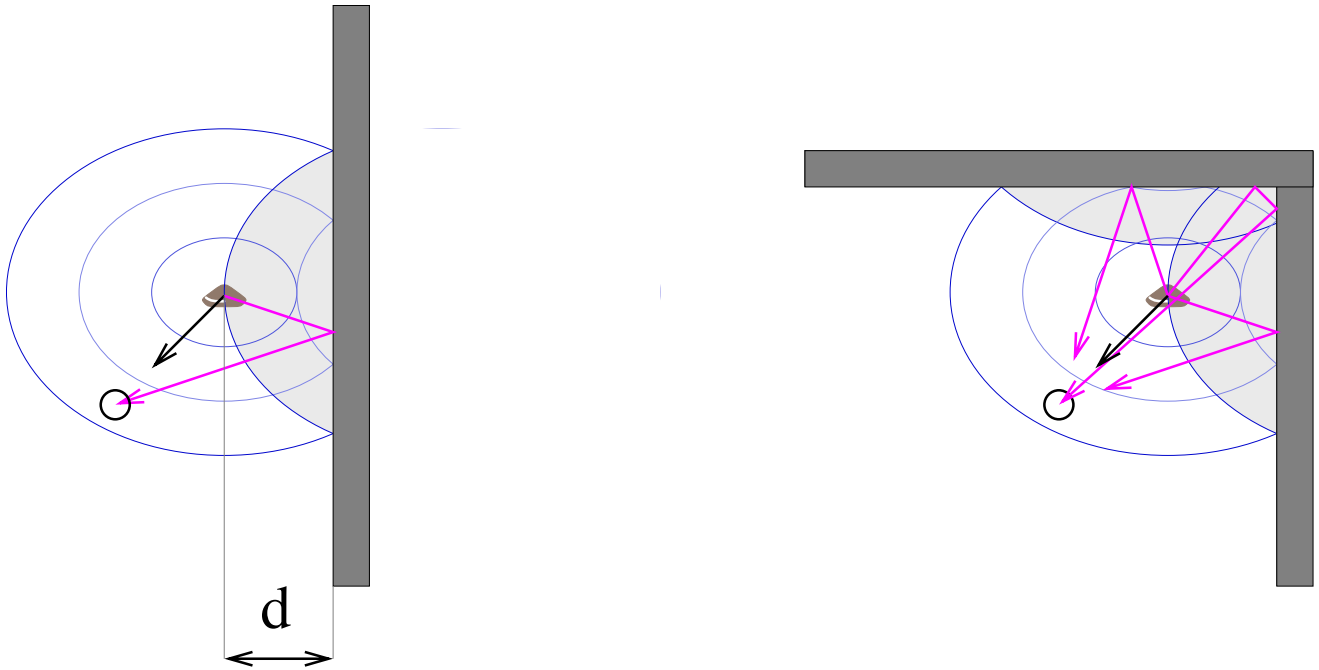


air
bois
air humide
plastique, verre
eau, végétation
animaux, nous :
cloisons en plâtre, brique
béton
verre blindé
métal conducteur

Interférences



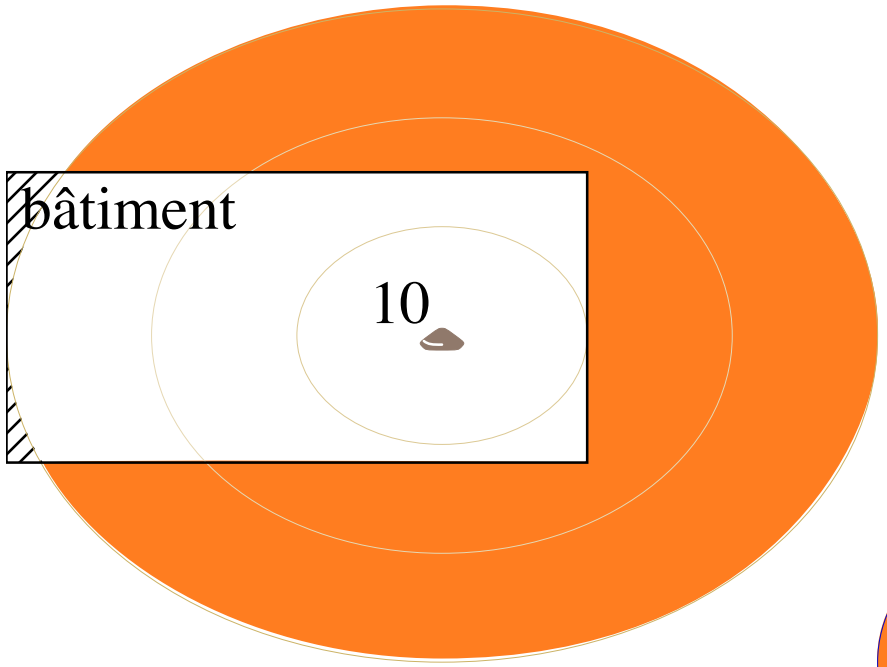
Interférences



Plus la distance à un obstacle réfléchissant est petite, plus la zone d'interférence est grande.

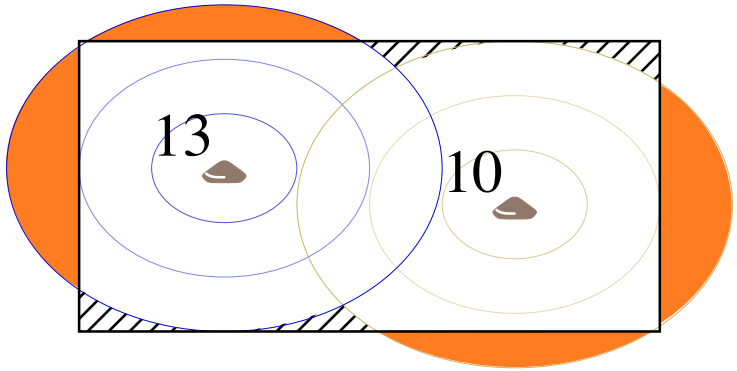
Couverture

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) ;
Système :	MacOS ≥ 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 :
⇒ trop coûteuses en temps de maintenance.

Installation

2 possibilités :

- pré-installation acheté à la commande d'un portable :
  `http://docs.info.apple.com/article.html?artnum=58521` ;
- nous acheter une carte AirPort :
  interne (≈ 80 €) ou bien PCMCIA (≈ 100 €).

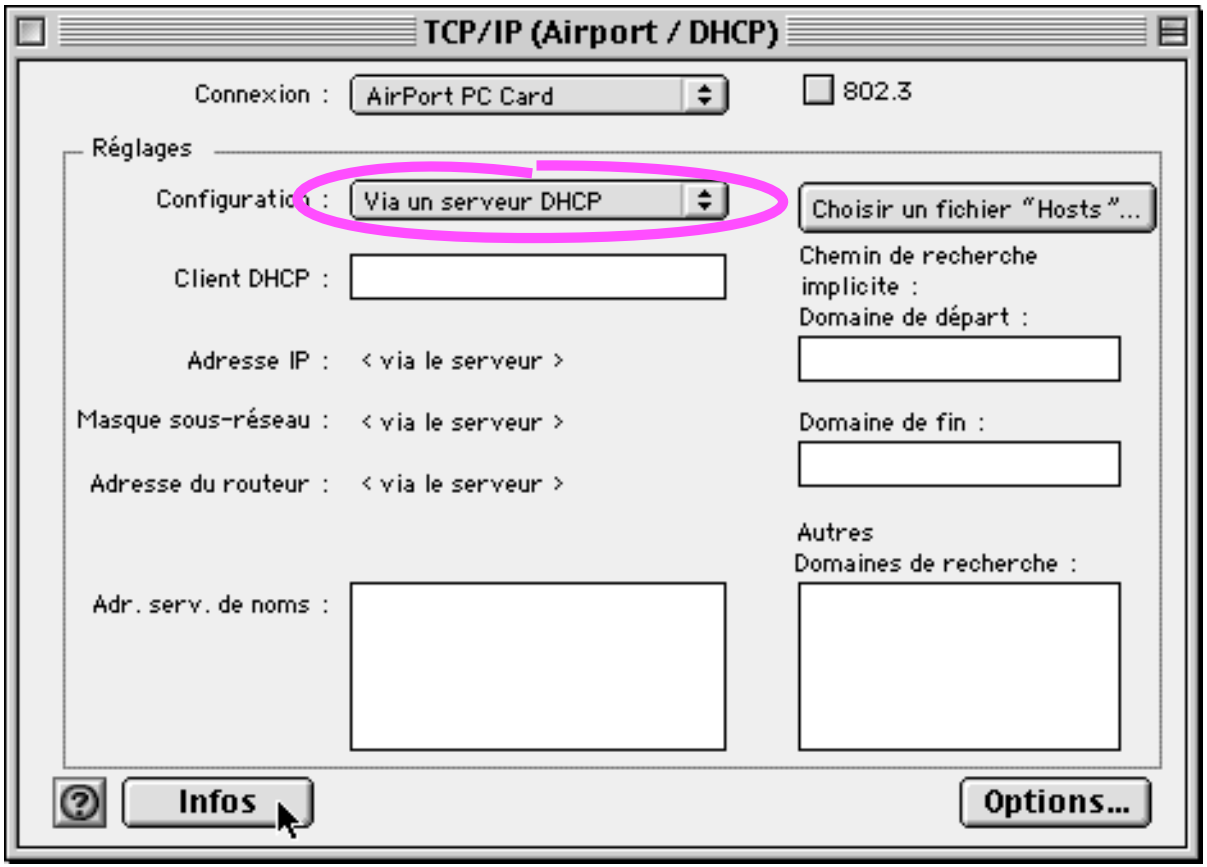
Le logiciel est automatiquement inclus avec MacOS 9.0.4.

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

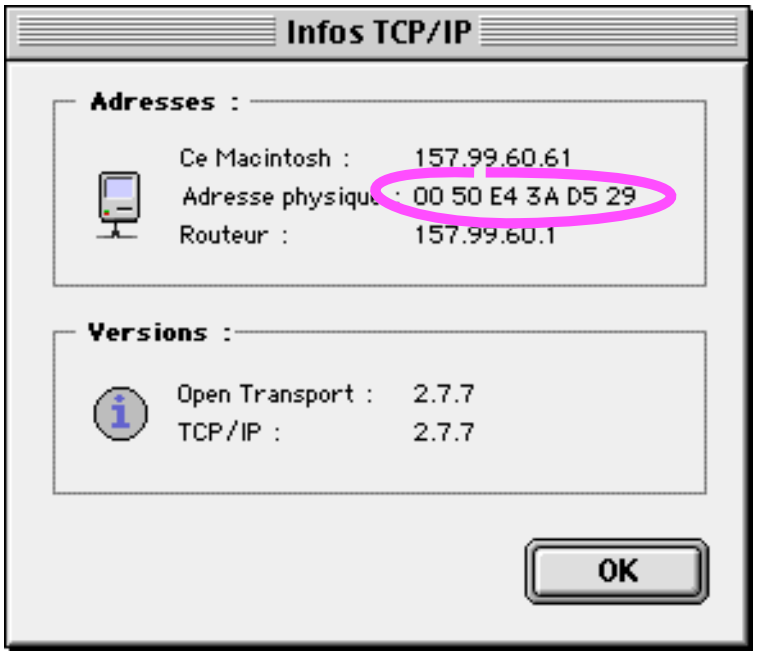
Temps d'installation & configuration d'une borne : 1 j.
Croissant vite avec le recouvrement des portées.

Configuration client

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



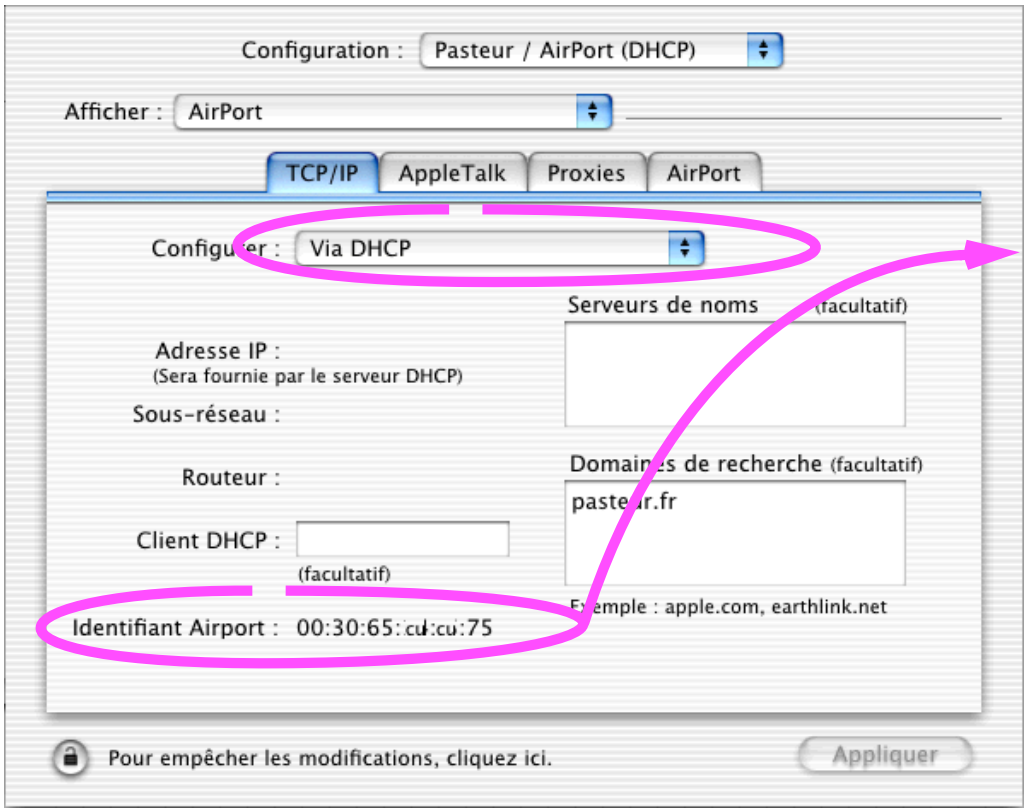
Configuration client



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.

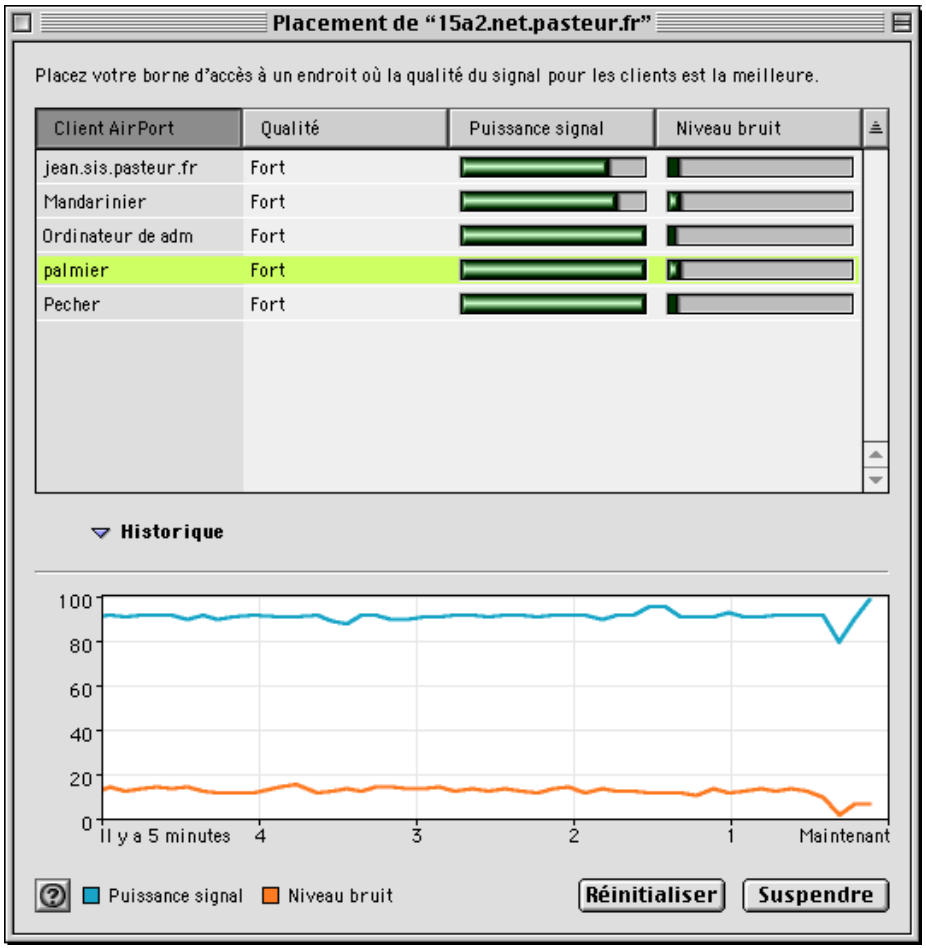
Configuration client / MacOS X



Adresse physique = adresse Ethernet.

À nous communiquer → intégration sur notre serveur DHCP.

Configuration réseau



Placement :

initial (densité faible)
→ 1/2 j ;

densité élevée
→ 1 j.

⇒ 1 prise secteur +
1 prise Ethernet !

Sécurité

Pas de nouveau problème de sécurité.

Remise en exergue de problèmes connus :

- impact des rayonnements électro-magnétiques sur le vivant,
  entre autres sur nous ;
- maîtrise du périmètre de sécurité de l'entreprise :
  mise en évidence du **syndrôme Maginot** ;
- maîtrise des accès en libre service sur un medium partagé,
  entre autres l'Ethernet partagé.

Sécurité des personnes

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

Apple a choisi d'utiliser une puissance ≈ **30 mW** !

⇒ champs réduits en puissance et portée ;

⇒ 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/`

GSM :	< 2W ;
DCS :	< 1W.
Antennes GSM :	20 à 50 W ;
émetteur de la tour Eiffel :	**6 MW** !

Sécurité des SI

Transport de données ⇒ champ électro-magnétique !

(⇒ 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 facilement écoutés. Dans le cas du 802.11b, les possibilités d'écoute sont plus simples que sur un réseau Ethernet partagé : 0 prise.

⇒ 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.

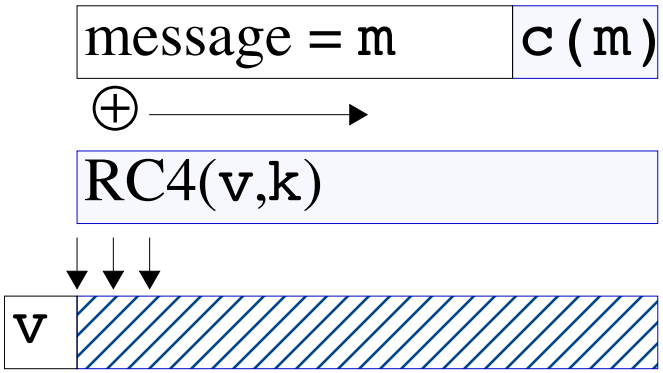
Protocole de chiffrement à clé symétrique partagée : RC4,
mais sans protocole de gestion de clé.

Mise en œuvre mal adaptée à un grand réseau :

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

RC4

RC4 = Rivest Code



$|v| = 24$ bits

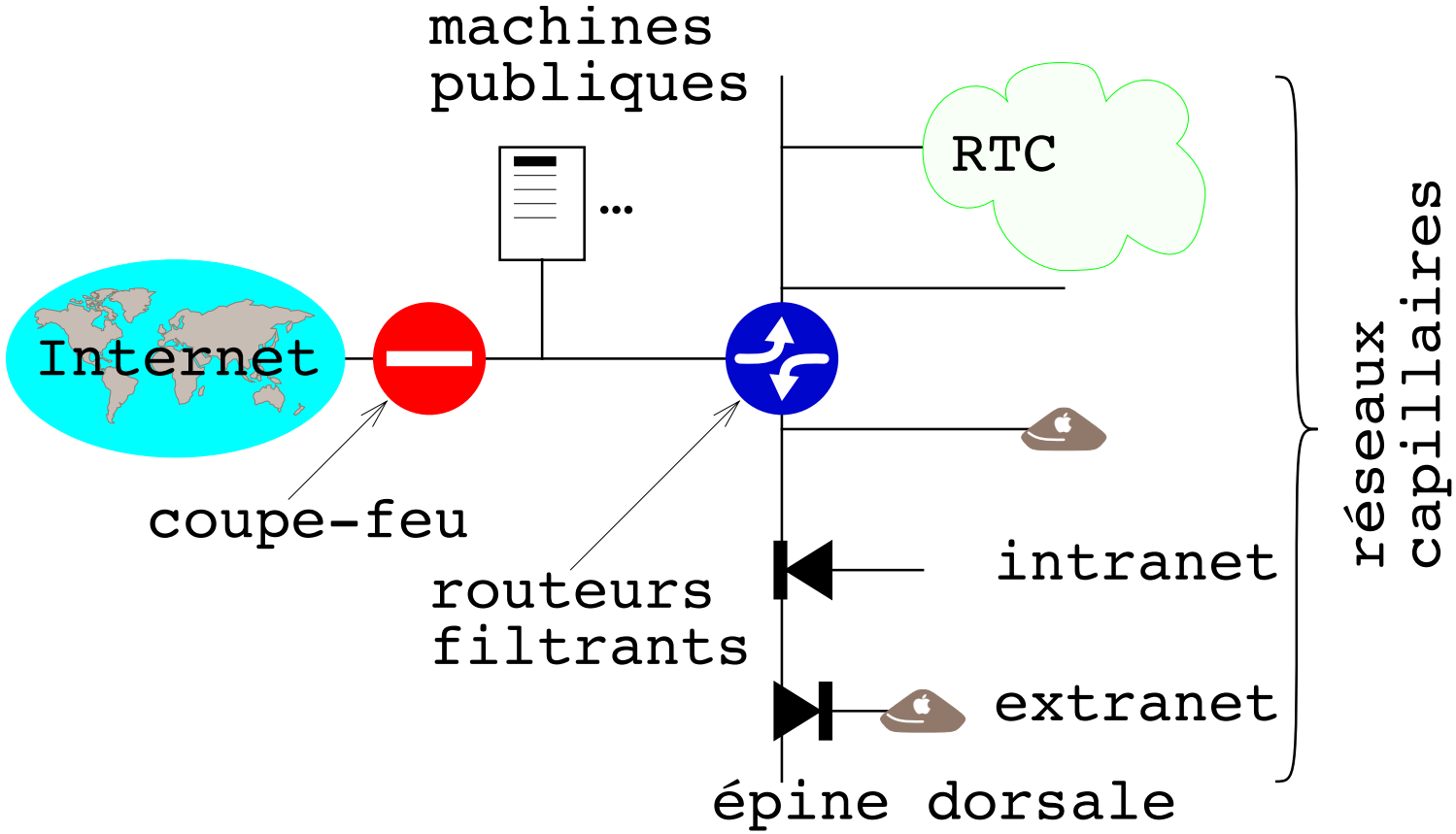
$|k| = 40$ ou bien 104

$c : m \rightarrow c(m)$

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


machines
publiques
...
RTC
Internet
coupe-feu
routeurs
filtrants
intranet
extranet
épine dorsale
réseaux
capillaires

Filtrage

Aucun accès IP aux équipements actifs.

DNS vers nos serveurs ;
DHCP (⇒ 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.

Audit

Filtrage systématique en sécurité positive
⇒ journalisation des tentatives d'insertion ou d'attaque :

scan en UDP/192,
ICMP → adresse de diffusion,
scan depuis `10.0.1.x`.

Effets de bord de réseaux squatteurs :

- adresses sources hors plan d'adressage
  ⇒ journalisation ;
- dysfonctionnements des réseaux existants.

Localisation sur le terrain :

- recherche de signal en bordure ;
- triangulation à partir de 3 relevés de niveau de signal.

Plan de déploiement

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

2002 : 15 bornes ; 75 ordinateurs sans fil ;
essais d'autres équipements, interopérabilité.

2003 : tests / 802.11a, 802.11g + 802.1x.

Pourquoi continuer ? Le périmètre de sécurité **avance** là !

Pourquoi Apple ? 2 ans d'avance + intégration antenne + qualité du logiciel ;
maîtrise des problèmes de sécurité,
choix du 802.11g.

Évolutions

1999 : 802.11b ; norme d'interopérabilité Wi-Fi ;

2002 : 802.11a ;

2003 : 802.11g ?

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

802.11g : 54 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 / 802.11?) ;

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

802.11a

Bande de fréquence **5 GHz** : [5,15 GHz ; 5,825 GHz],
divisée en :

- 3 bandes de fréquence de 100 MHz ;
- 12 canaux séparés de 20 MHz.

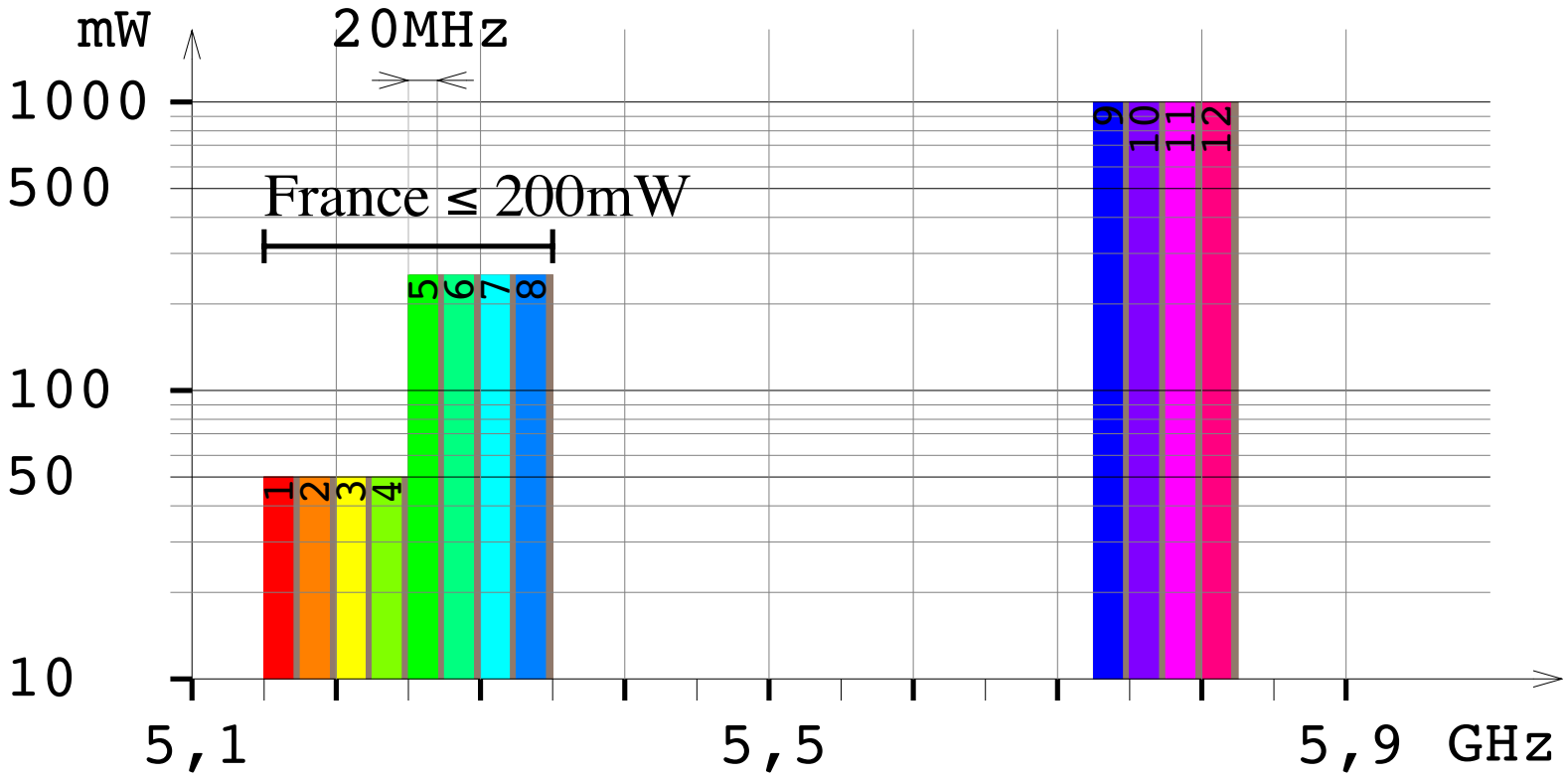
Technique de modulation :

OFDM (Orthogonal Frequency Division Multiplexing),
sur 52 porteuses distinctes (utilisée en xDSL).

Débit : **6 → 54 Mbit/s**.

Méthode d'accès : CSMA/CA.

802.11a : canaux



Bande UNII (Unlicensed National Information Infrastructure).

802.11a : avantages & inconvénients

Bande de fréquence libre

⇒ problèmes de cohabitation à venir.

Plages de fréquences et puissances ≠

⇒ difficulté d'utilisation pour les voyageurs.

Fréquence élevée

⇒ $E = h \times \nu$: énergie transportée élevée ;

⇒ absorption élevée ;

⇒ puissance rayonnée + élevée.

Canaux séparés

⇒ possibilité de les utiliser tous en un même point ;

⇒ débit & nombre d'utilisateurs élevés ;

⇒ puissance rayonnée + élevée.

802.11g

Bande de fréquence **2,4 GHz** : [2,4 GHz ; 2,4835 GHz],

divisée en 3 canaux séparés de 30MHz.

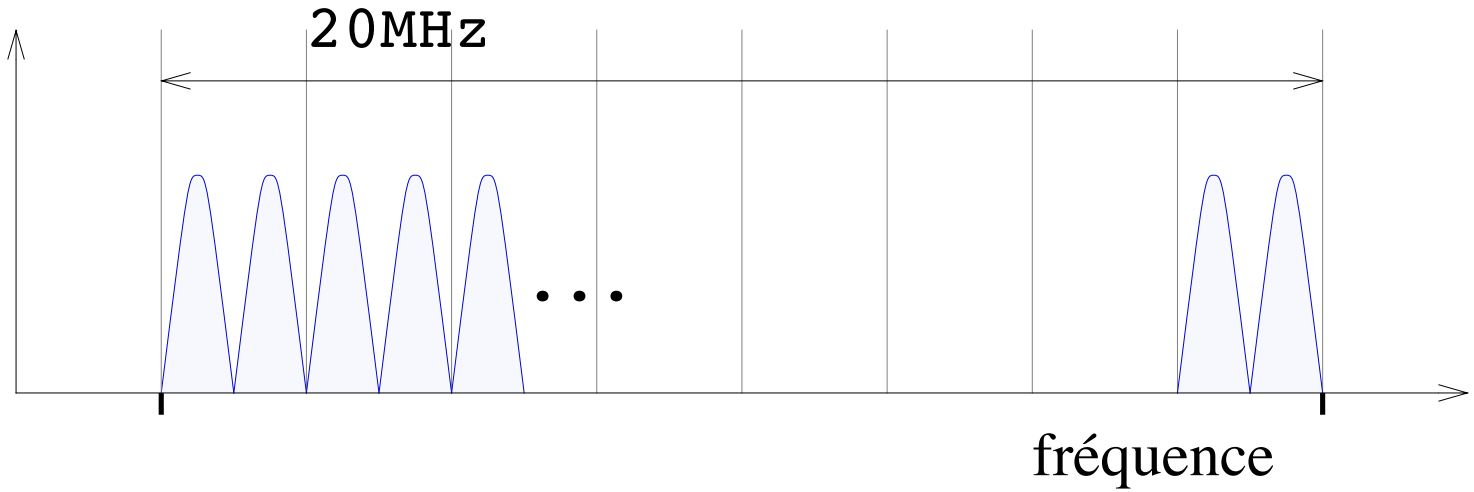
Technique de modulation :

- CCK ;
- OFDM ;
- en option CCK/OFDM ou bien PBCC.

Débit : **1 → 54 Mbit/s**.

Méthode d'accès : CSMA/CA.

OFDM



52 porteuses espacées : $\nu = n \times 312{,}5$ kHz

⇒ nœuds de toutes les porteuses coïncident

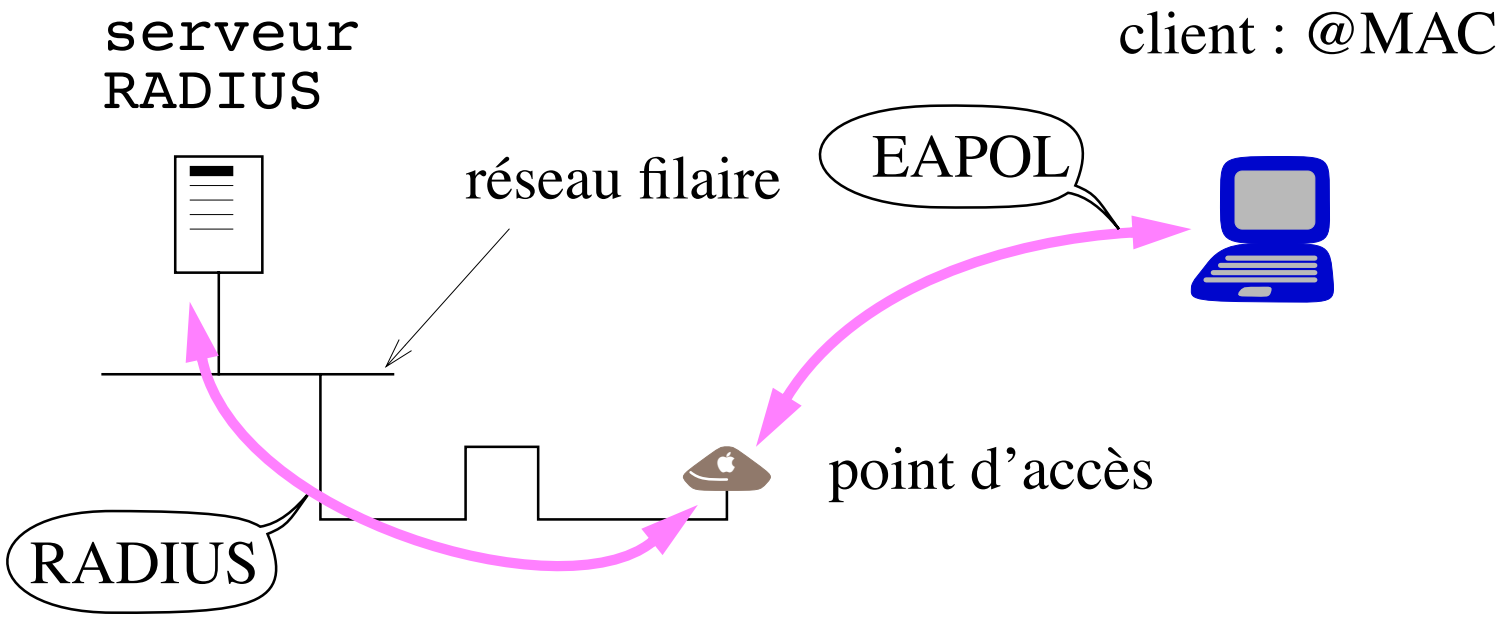
⇒ n'interfèrent pas entre-elles.

Débit sur chaque porteuse plus bas

⇒ BER + bas.

802.1X

Authentification de l'accès au réseau



EAPOL = Extended Authentication Protocol Over LAN
RADIUS = Remote Authentication Dial-In User Service

→ association @MAC - point d'accès : trafic autorisé.

802.11i

WEP est mort : mort-né + mises en œuvre médiocres.

802.11i (fin 2003) définit 2 techniques de chiffrement :

- TKIP = Temporal Key Integrity Protocol :
  |v| = 48 bits ;
  MIC = message integrity code / 64 bits;
- CCMP = Counter mode with CBC-MAC Protocol :
  |v| = 48 bits ;
  AES en mode chaîné sur blocs de 128 bits
  ⇒ puissance de calcul.

WPA = Wi-Fi Protected Access (défini par la Wi-Fi Alliance) :
version intérimaire de 802.11i basée sur WEP & TKIP.

Annexes

Atténuation géométrique

Un rayonnement électro-magnétique se propage en ligne droite

$\Rightarrow$ angle solide couvert constant σ, de surface : σr^2 ;

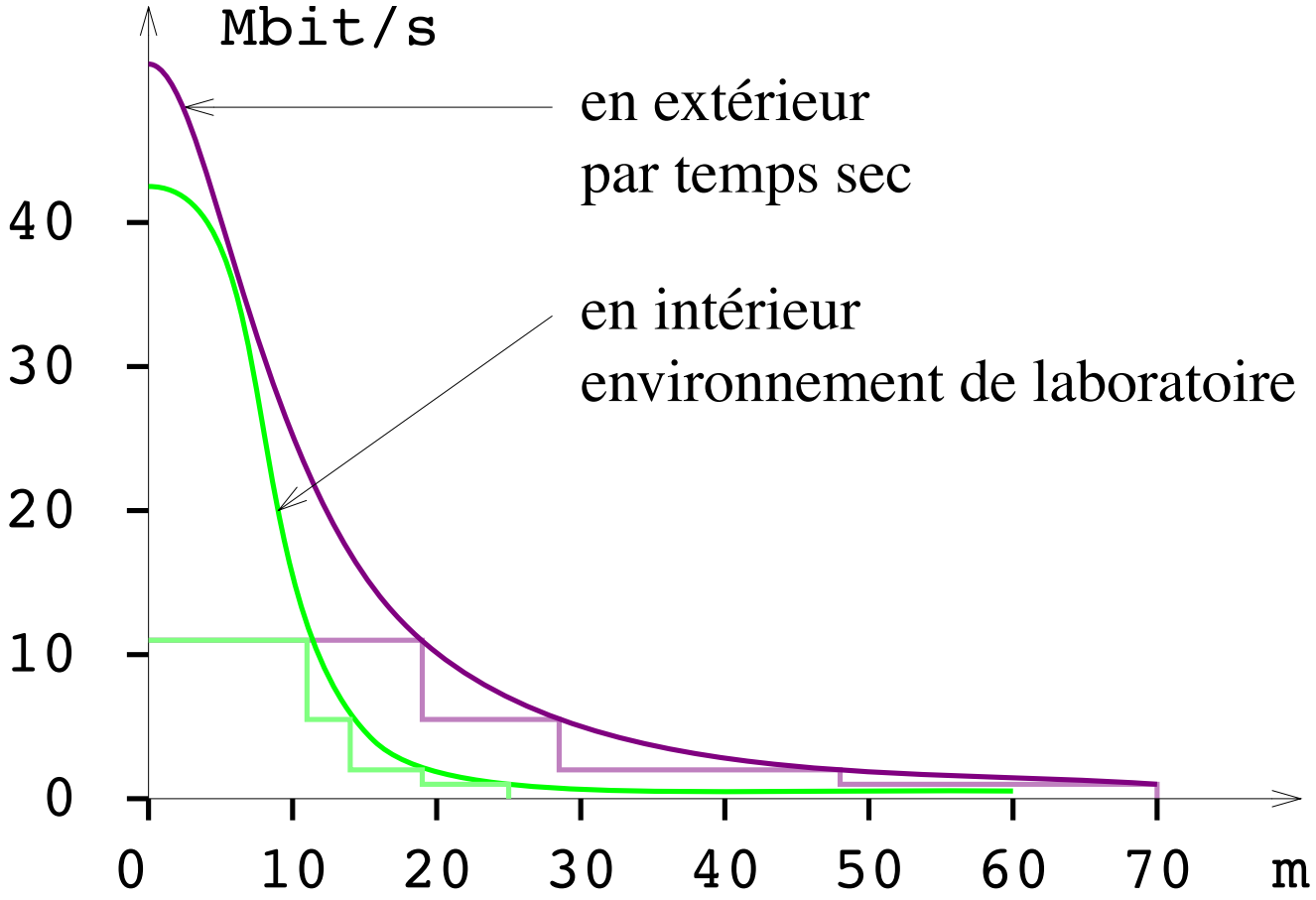
$\Rightarrow$ puissance distribuée décroît comme son inverse.

En extérieur : $W \approx \frac{1}{r^2}$, en intérieur : $W \approx \frac{1}{r^4}$.

Fonctions utilisées en 1ère approximation :

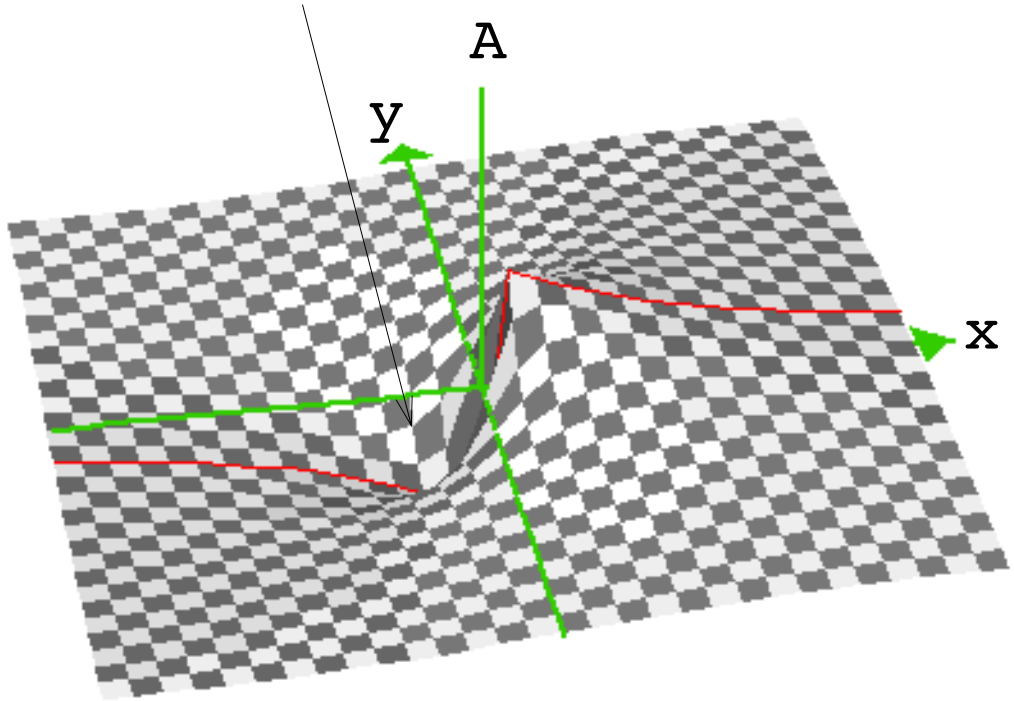
$$d \approx \frac{50}{1 + \left(\frac{r}{10}\right)^2} \; ; \; d \approx \frac{50}{1,2 + \left(\frac{r}{10}\right)^4}.$$

Débit : d = f(r)


Mbit/s
en extérieur
par temps sec
en intérieur
environnement de laboratoire
40
30
20
10
0
0
10
20
30
40
50
60
70
m

Réflexion, absorption

onde réfléchie ⇒ atténuation



Exemple :
amplitude du signal au voisinage d'un mur en béton.

Borne proche du mur aligné sur l'axe des y.

Glossaire

BER	Bit Error Rate
CCK	Complementary Code Keying
EAPOL	Extended Authentication Protocol Over LAN
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
OFDM	Orthogonal Frequency Division Multiplexing (Intersil)
PBCC	Packet Binary Convolution Coding (Texas Instruments)
RADIUS	Remote Authentication Dial-In User Service