INSTITUT PASTEUR

Évolution des réseaux sans fil

Daniel AZUELOS
Architecture réseau & sécurité
Institut Pasteur

20 novembre 2003

INSTITUT PASTEUR

Du 802.11 au 802.11g

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 ;
Wi-Fi	: (ouaille fit) norme d'interopérabilité ;

→ **réseaux sans fil** !

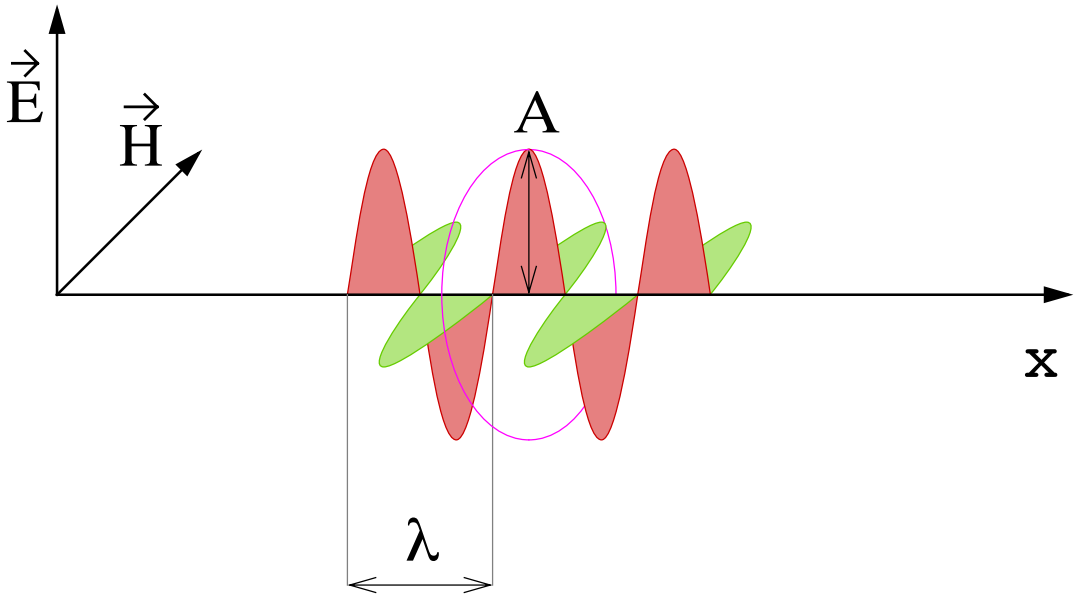
Principe : onde hertzienne = porteuse
+ transport de données numériques / porteuse.

Utilisée pour les transmissions satellite.

Ondes électro-magnétiques

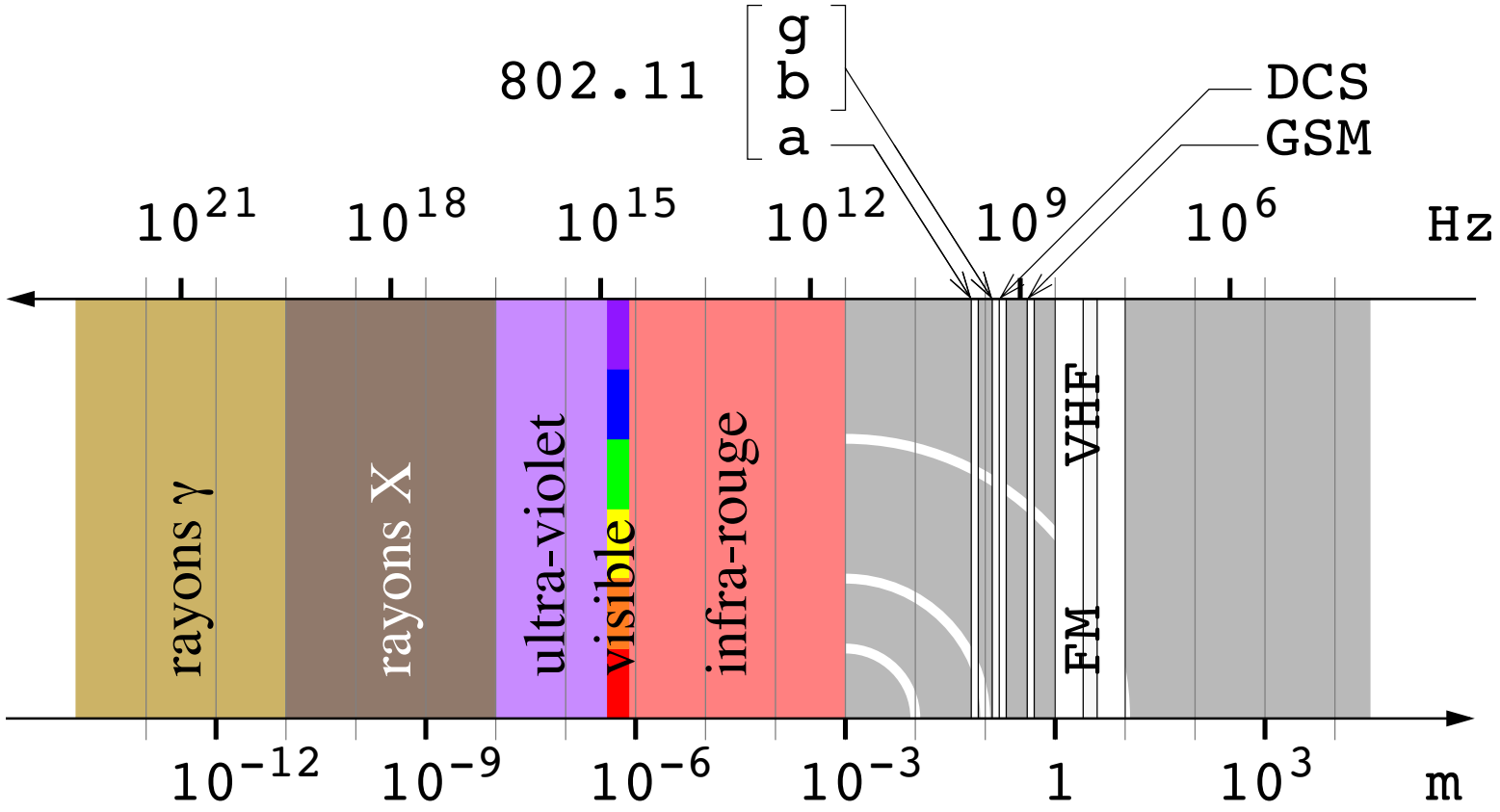
Ondes radios, infra-rouge, visible, ultra-violet, X, γ…

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



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
2003 → **802.11g**

Standards spécifiant les méthodes d'accès au medium physique permettant la construction de liaison.

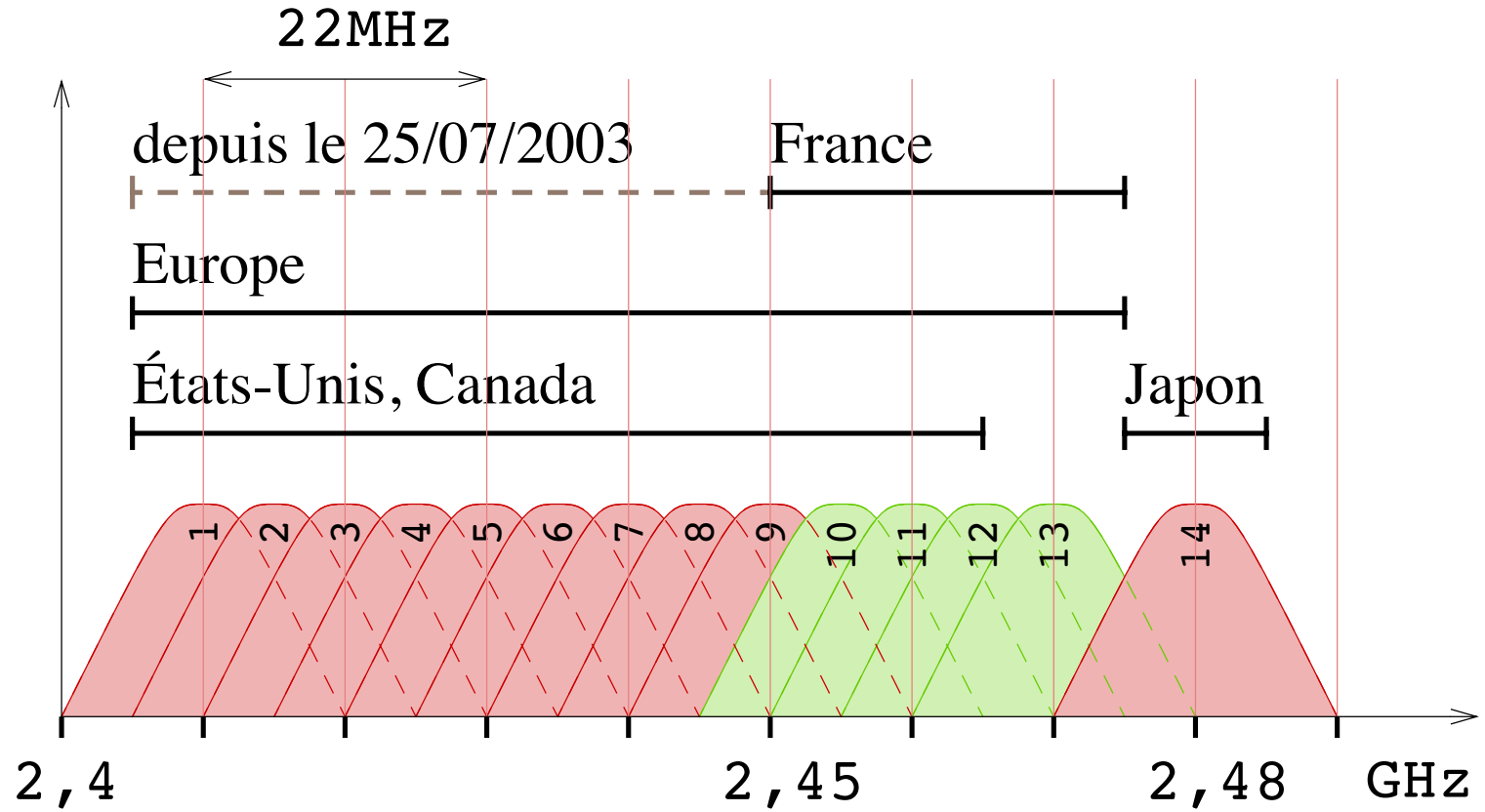
Medium physique = bande de fréquence : **2,4 GHz**.

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

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

Débit : **11 Mbit/s** ; 5,5 Mbit/s ; 2 Mbit/s ou 1 Mbit/s
adapté automatiquement en fonction du rapport S/B.

802.11b : canaux



Bande ISM (Industrial, Scientific, and Medical).

Fonctionnement

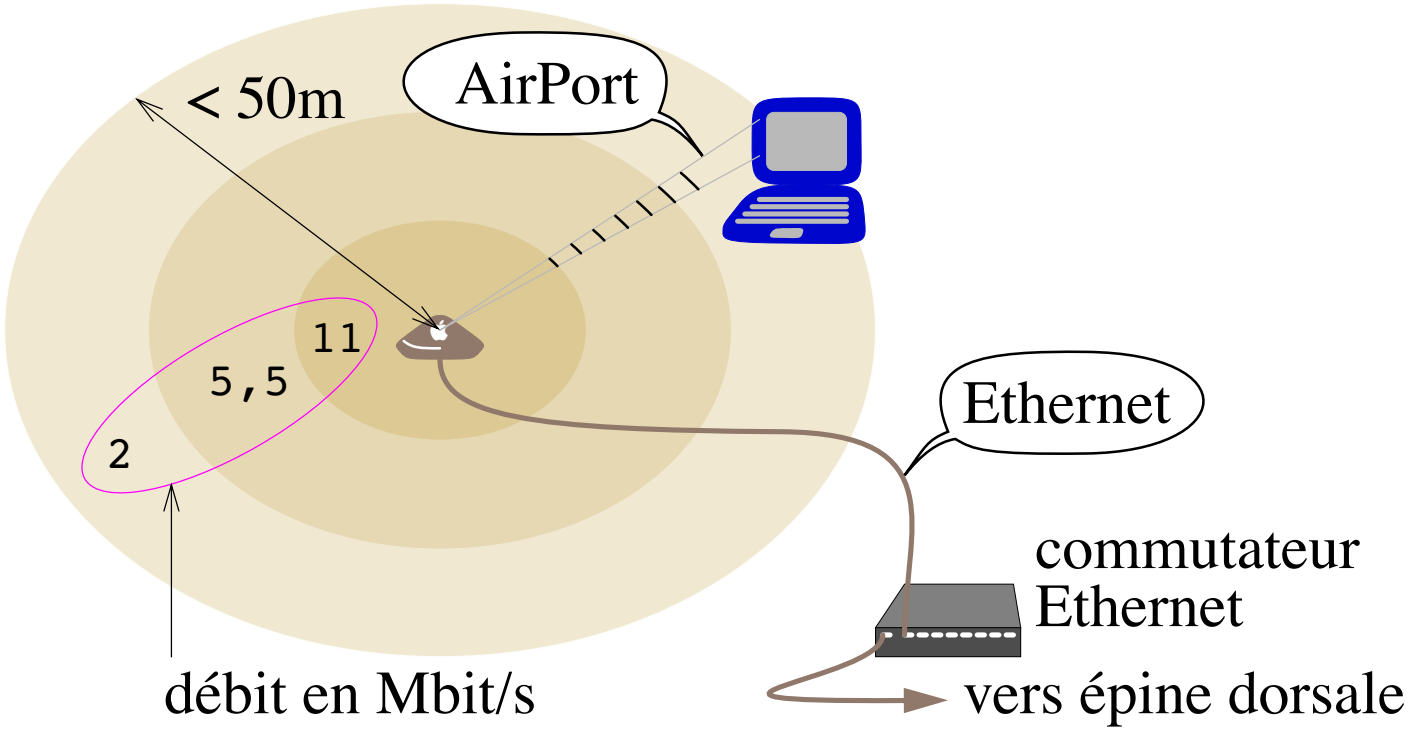
Antenne (= émetteur & récepteur) : carte AirPort.

Carte AirPort ≈ modem + émetteur/récepteur radio.

Une borne AirPort = répéteur à 2 interfaces :
1 carte Ethernet + 1 carte AirPort.

Visibilité radio	⇒ établissement d'une liaison.
Déplacement	⇒ variabilité du S/B ⇒ renégociation de la vitesse utilisable.
Éloignement, obstacle	⇒ perte de la liaison.

Fonctionnement



Une liaison sans fil ⇒ 2 cartes AirPort !

Raccordement au reste du réseau ⇒ liaison Ethernet.

Types de réseaux

Multi-point ≈ câble Ethernet croisé.
On peut être plus de 2 sur le même support (réunion des portées des différentes cartes participant).

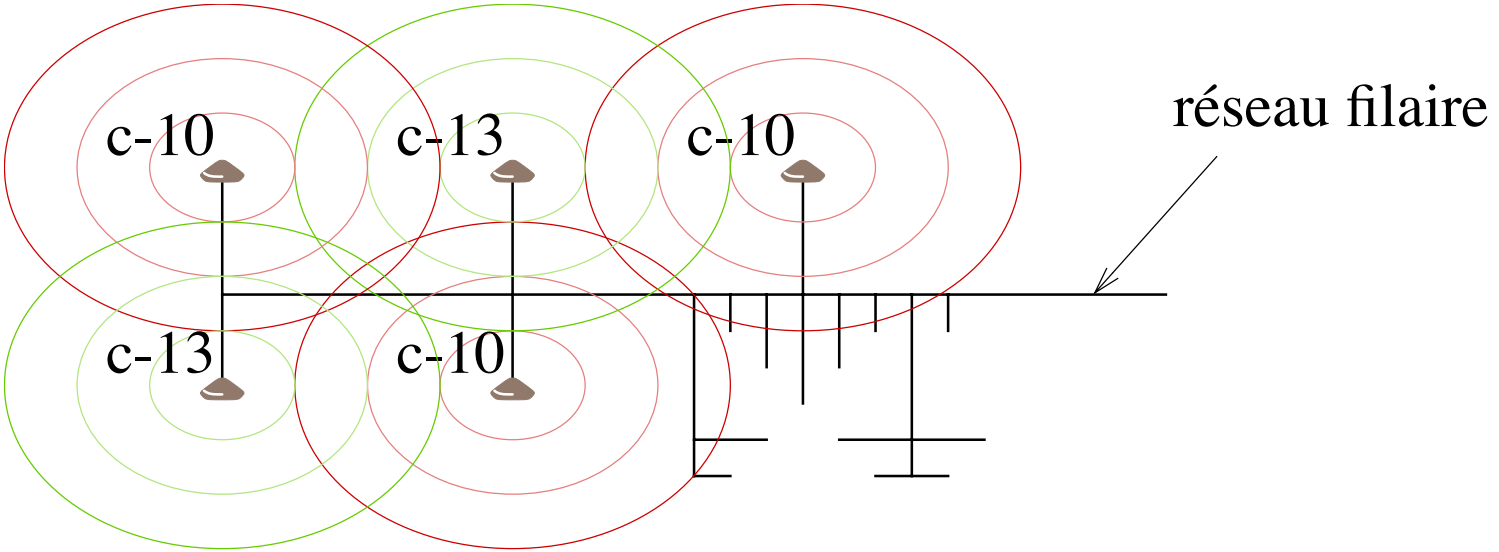
Réseau d'infrastructure : même nom de réseau, plusieurs antennes, canaux distincts
→ accès / grand espace & nombreux utilisateurs
⇒ mobilité.

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 (page 17).



Réglementation

L'ART (Autorité de Régulation des Télécommunications) définit les limites d'utilisation des fréquences pour des RLAN :

arrêté du 25/07/2003 ;

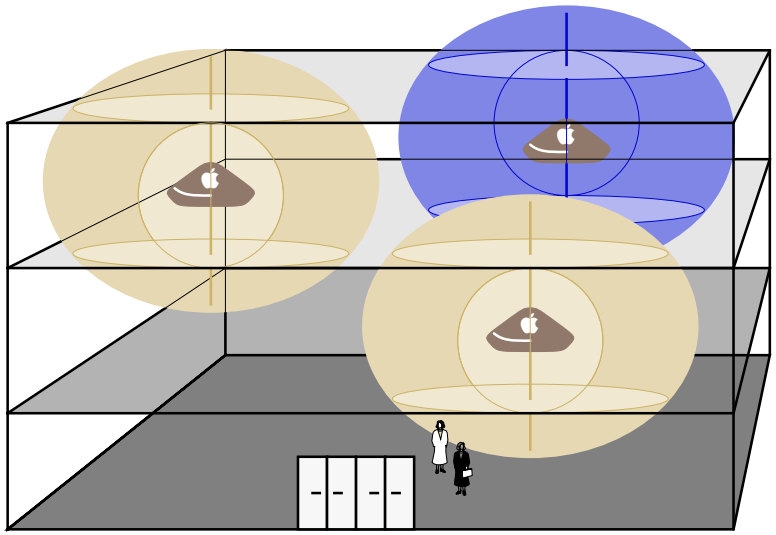
→ `http://www.art-telecom.fr/↲`
`dossiers/rlan/menu-gal.htm`

- utilisation à l'intérieur des bâtiments : libre, PIRE <100mW ;
- utilisation à l'extérieur : 1-7 < 100 mW, 8-13 < 10 mW ☹ !

Utilisation à la maison : libre (à l'intérieur des bâtiments)
⇒ attention aux voisins (perturbation, écoute) !

[2400 - 2483,5] MHz libre partout (en Europe) → 01/2011 ?

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 partagent un même espace 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

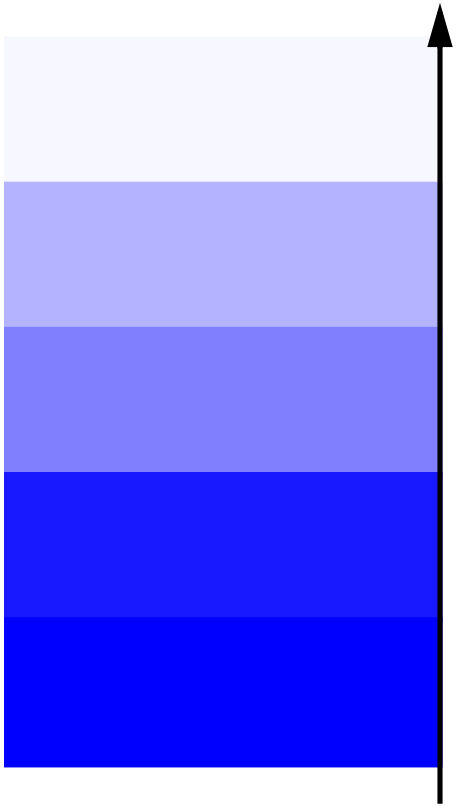
Une onde électro-magnétique se propage en ligne droite, à vitesse $c \approx 3 \times 10^8 m/s$ dans le vide. Dans tout autre milieu, elle peut être :

- 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.

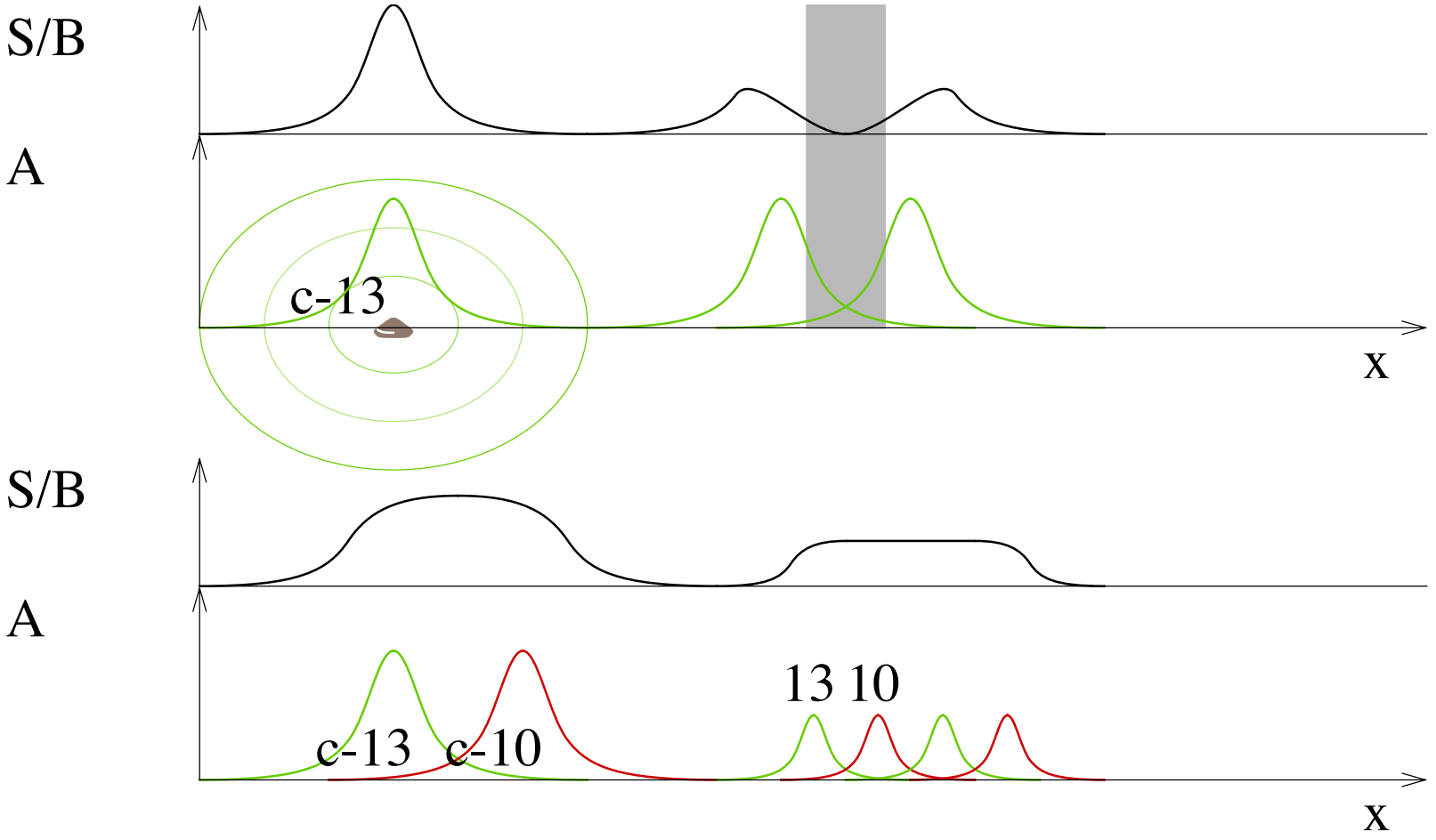
Elle interfère avec toute autre onde de fréquence proche
→ battement spatial & temporel.

Transparence

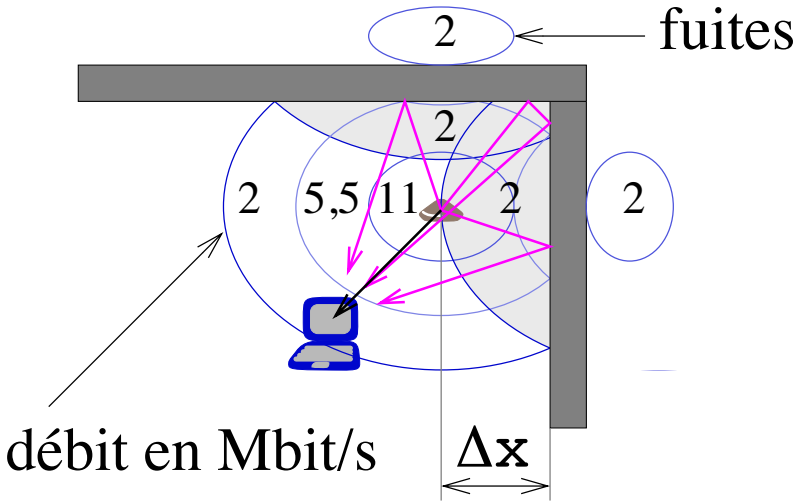


air
bois
air humide
plastique, verre
eau, végétation
animaux, nous :
cloisons en plâtre, brique
béton
verre blindé
métal conducteur

Interférences



Interférences

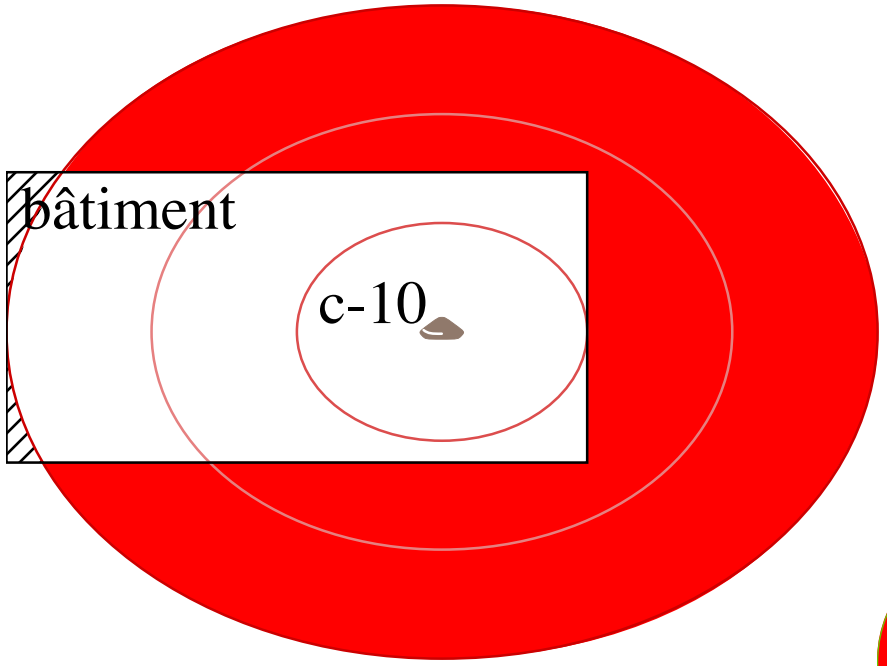


Plus la distance à un obstacle ± transparent est petite,
plus la zone d'interférence est grande,
plus la zone de diffraction est grande et difforme.

Problèmatique d'éclairage.

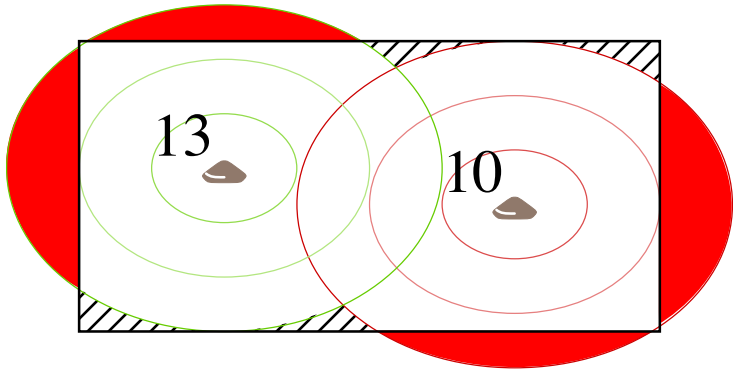
Couverture

60 mW



défaut de : couverture
sécurité

30 mW



Types d'antennes

Omni-directionnelles (isotrope) :
les ondes électro-magnétiques vont dans toutes les directions ;
et le rapport signal/bruit décroit presque uniquement géométriquement (i.e. en $1/r^2$).

Directionnelles :
les ondes sont dirigées par une ou plusieurs antennes selon une direction ou bien un secteur angulaire.
$\Rightarrow$ placement précis, et sensibilité aux réfractions.

Analogie :

éclairer un auditorium avec des projecteurs de scène ☹ !

Fait vendre plus d'antennes et les services d'un installateur ☹ !

Prérequis

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

transportables : Mac (sauf 1er modèle).

Les solutions à base de carte PCMCIA ou de carte externe sur port USB sont médiocres  !

Systèmes : MacOS ≥ 9.0.4, MacOS X,
*BSD, Linux,
Windows 98  , Windows XP.

Critères : dessin d'antenne intégré dans l'ordinateur ;
pilote intégré dans le système d'exploitation ;
maîtrise de connectivité dans le S.E..

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 les systèmes modernes que nous avons sélectionnés.

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

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

Configuration client

Chaque utilisateur souhaitant connecter un ordinateur à nos réseaux doit :

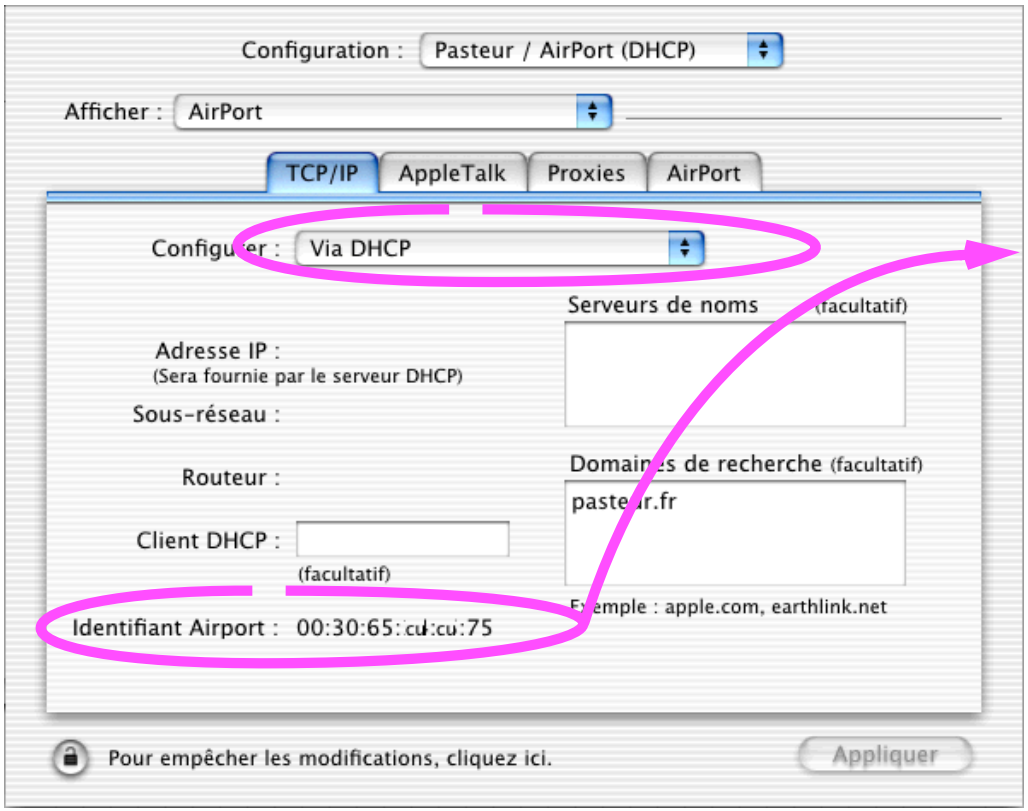
- nous communiquer l'adresse MAC (Ethernet ou AirPort) ;
- configurer TCP/IP via DHCP.

Nous intégrons cette adresse MAC dans la config. de notre serveur DHCP,

puis en dérivons (`sed(1)`) des ACL dans le cas d'AirPort.

⇒ Aucun état local à gérer.

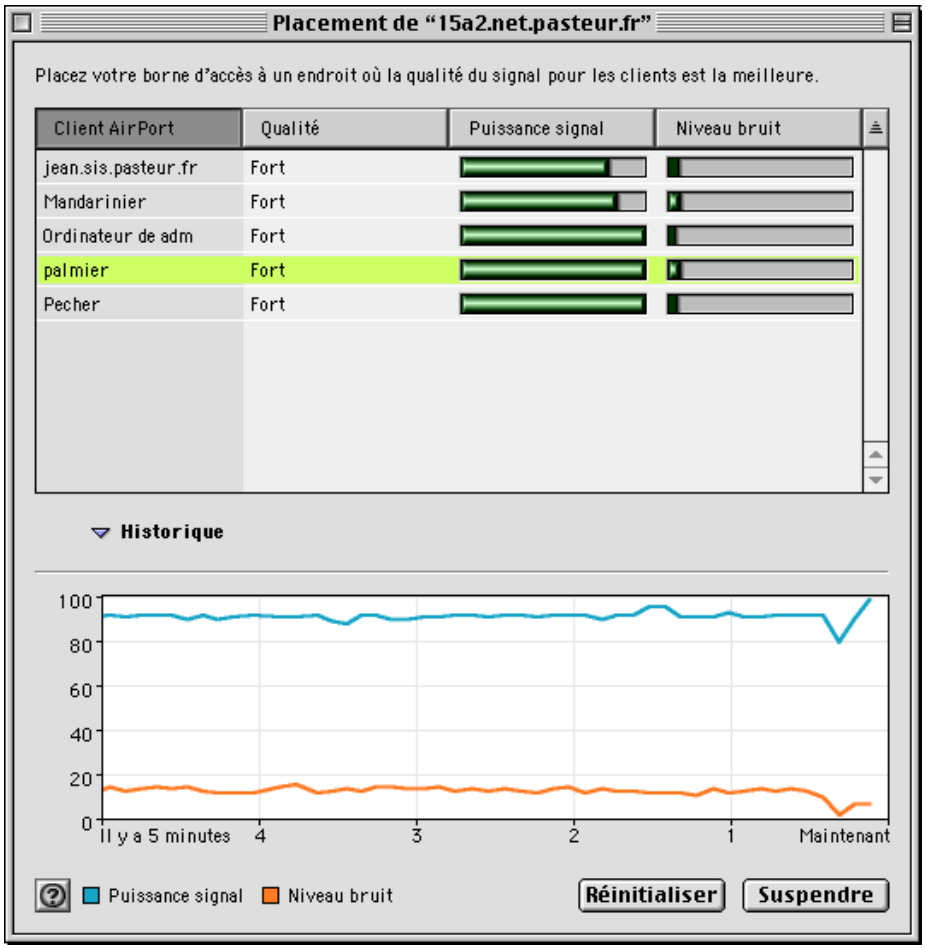
Configuration client / MacOS X



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 **syndrome 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.

Depuis 2002, presque tous les constructeurs se sont ralliés à ce principe de précaution.

L'utilisation de radio-fréquences suscite des interrogations légitimes.

⇒ consultation du CHSCT pour avis avant déploiement ;

⇒ communication claire sur le risque.

Sécurité des personnes

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** !

Tout champ électro-magnétique décroit en $1/r^2$.

L'équivalent d'un mobile (600 mW) à l'oreille, avec des iBook équipés d'une carte AirPort c'est :

10 sur la tête, 1 000 sur les genous,
100 000 dans une classe.

Sécurité des SI

Transport de données ⇒ champ électro-magnétique !

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

Tous ces transports de données (ormis la fibre optique) 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.

⇒ communication sur les risques ;

⇒ 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.

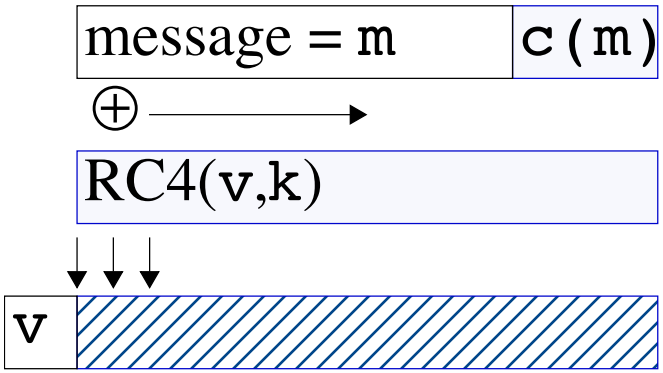
Protocole de chiffrement à clé symétrique partagée : RC4,
mais sans protocole de gestion de clé.

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(1)`).

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.

WEP : un extincteur vide

Beaucoup de papiers et d'outils ont été diffusés sur la façon de casser WEP :

`http://airsnort.shmoo.com`

Ils ont grossi artificiellement un faux problème :

faiblesse du chiffrement (car il s'agit de faiblesse de mise en œuvre dans WEP),

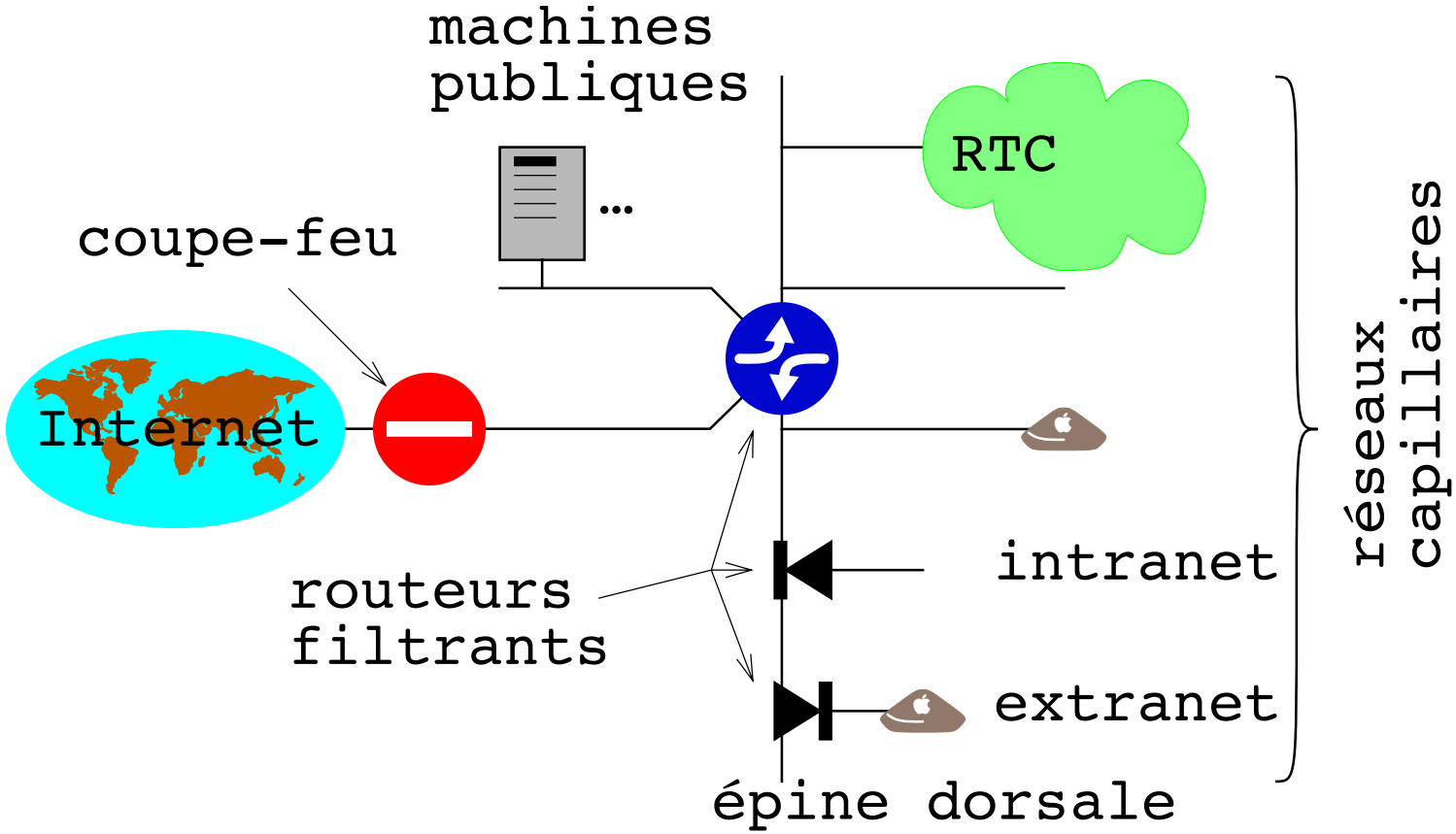
et ils ont laissé dans l'ombre un vrai problème :

absence dans la famille 802.11 d'un protocole de gestion de clés à zéro état local.

WEP : à jeter !

Coller des rustines sur WEP pour le réutiliser : pire ☹ !
Ramener ça à un problème d'IGC : faire l'œuf sans la poule.

Extranet


machines
publiques
RTC
coupe-feu
Internet
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.

Audit

Localisation sur le terrain :

- détection de réseaux pirates internes ;
- détection de réseaux voisins « très hospitaliers » dans lesquels les ordinateurs d'utilisateurs naïfs pourraient tomber ;
- recherche de signal en bordure ;
- triangulation à partir de 3 relevés de niveau de signal.

Constat pragmatique :

- écouter un réseau sans fil dans un environnement bien couvert ⇒ « entrer » dans la zone de couverture ;
- écouter, se connecter à un réseau :
  utiliser une prise Ethernet assis dans un coin ou bien se promener à pied avec son portable ouvert ou en décapotable dans le parking voisin avec une antenne d'1 m ?

Syndrome Maginot

Architecture réseau traditionnelle :
« intranet » délimité par un périmètre de sécurité et protégé de l'horrible Internet par un « failleur-waulle ».

Malheureusement, ce modèle de périmètre ne tient plus, il est franchi par :

- le PC portable truffé de vers attrapés dans le réseau d'un collègue ;
- le PC portable d'un collègue qui vient de l'autre bout du monde ;
- l'ordinateur du directeur qui doit partir en réparation ;
- le tunnel chiffré (vipi-haine) connectant un ordinateur interne au réseau de l'entreprise voisine ;

Syndrome Maginot

- le PC avec carte Ethernet et carte Wi-Fi allumée en permanence faisant pont entre la rue et le réseau interne ;
- le réseau sans-fil d'un résidant de l'hôtel voisin.

Échelle des risques :

- risque dominant plutôt du côté de la qualité déplorable de certains S.E. comme Windows ;
- vient ensuite l'accès à la connexion Ethernet :

  utopie que tout accès à une prise Ethernet est contrôlé ☹ !

Enfin l'absence de déploiement de réseaux sans fil en interne est une source de risque :
0 audit, 0 communication sur ce problème, 0 compétence.

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** + **802.1X**.
Futur ?	802.11g + 802.1X + 802.11i - WEP.

Évolutions

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

2002 : 802.11a ;

2003 : 802.11g ; Centrino (802.11b : 4 ans de retard ☹ !).

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.

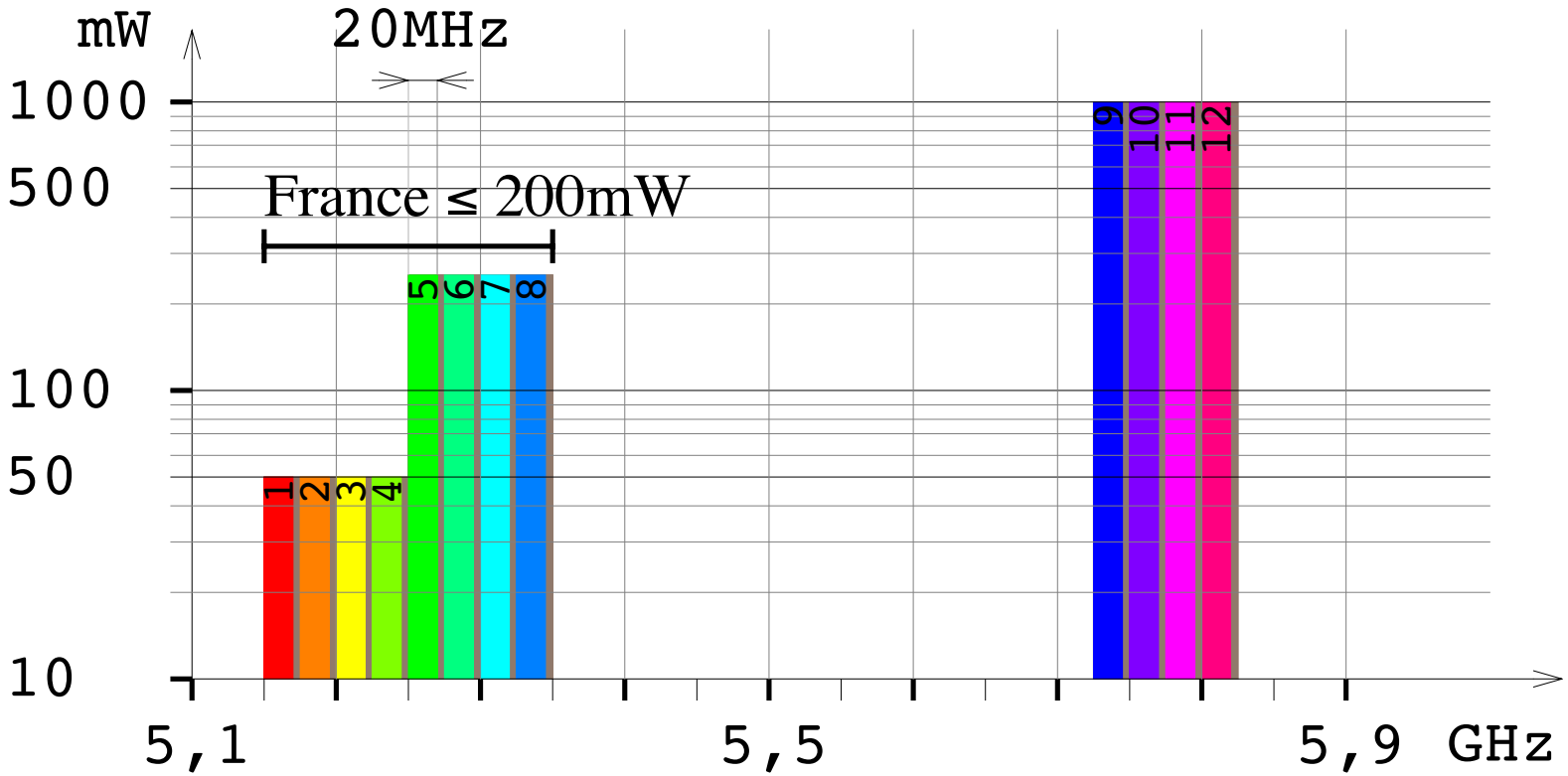
Technique de modulation :

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

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

⇒ énergie consommée élevée (inadapté au portable) ;

⇒ absorption élevée (⇒ P.A. × 2 sur une dimension !);

⇒ 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.

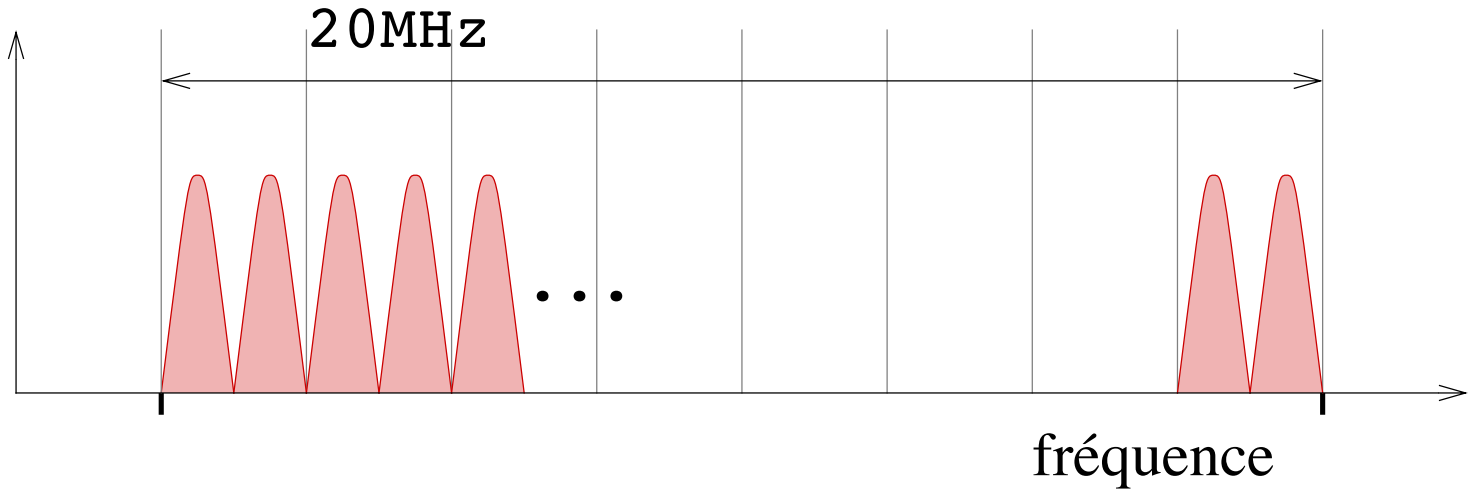
Technique de modulation :

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

Débit : **1 → 54 Mbit/s**.

Méthode d'accès : CSMA/CA.

OFDM



52 porteuses espacées : f = n × 312,5 kHz

⇒ nœuds de toutes les porteuses coïncident

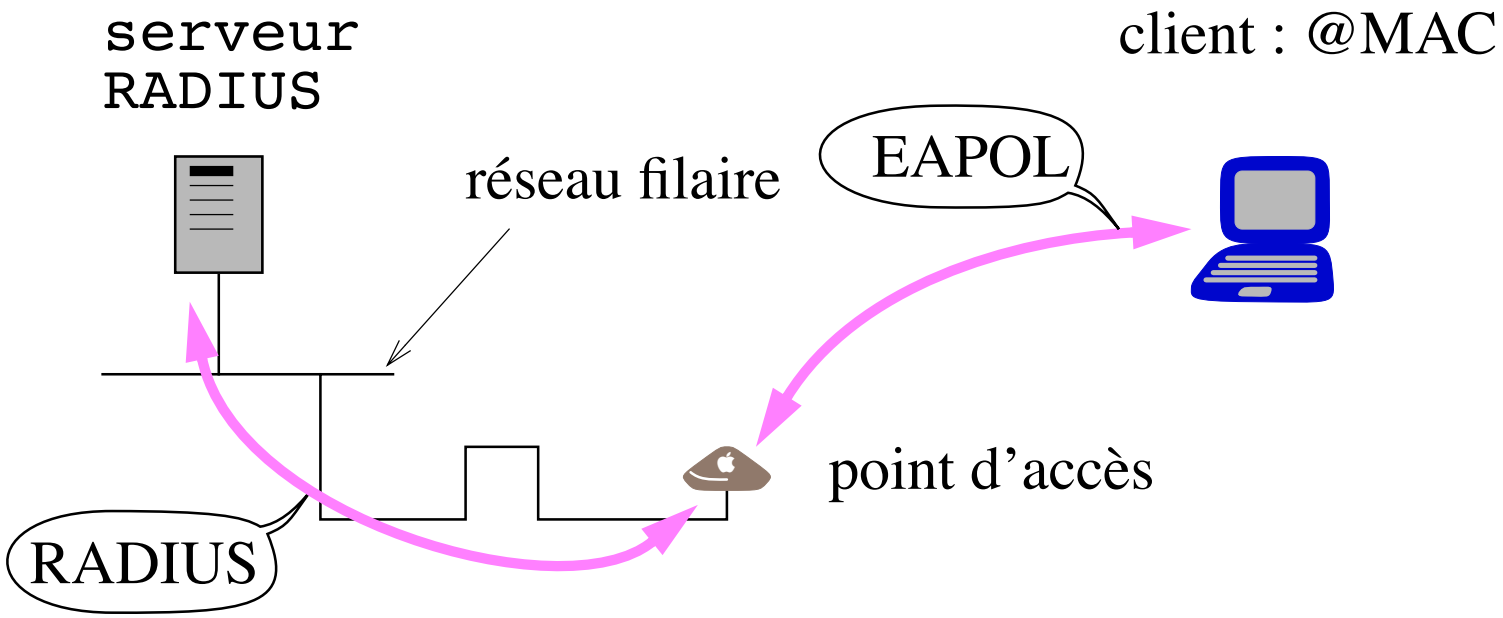
⇒ n'interfèrent pas entre-elles.

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.

utiliser WEP : mauvais départ ?

Conseils pratiques

Choix techniques ayant un avenir :

- déployer aujourd'hui du **802.11g** :
  rester maître d'œuvre du réseau de demain ;
- éviter des techniques en retard de 4 ans (Centrino) ;
- éviter tout ce qui est basé sur WEP ;
- éviter les protocoles propriétaires d'une telle complexité que seul le commercial peut les certifier.

Communiquer clairement sur les **risques réels** :

- éteignez un mobile et allumez 100 000 carte 802.11g ;
- profitez du raffut médiatique pour inciter les utilisateurs concernés à s'approprier les outils de chiffrement.

Annexes

Atténuation géométrique

Un rayonnement électro-magnétique se propage en ligne droite

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

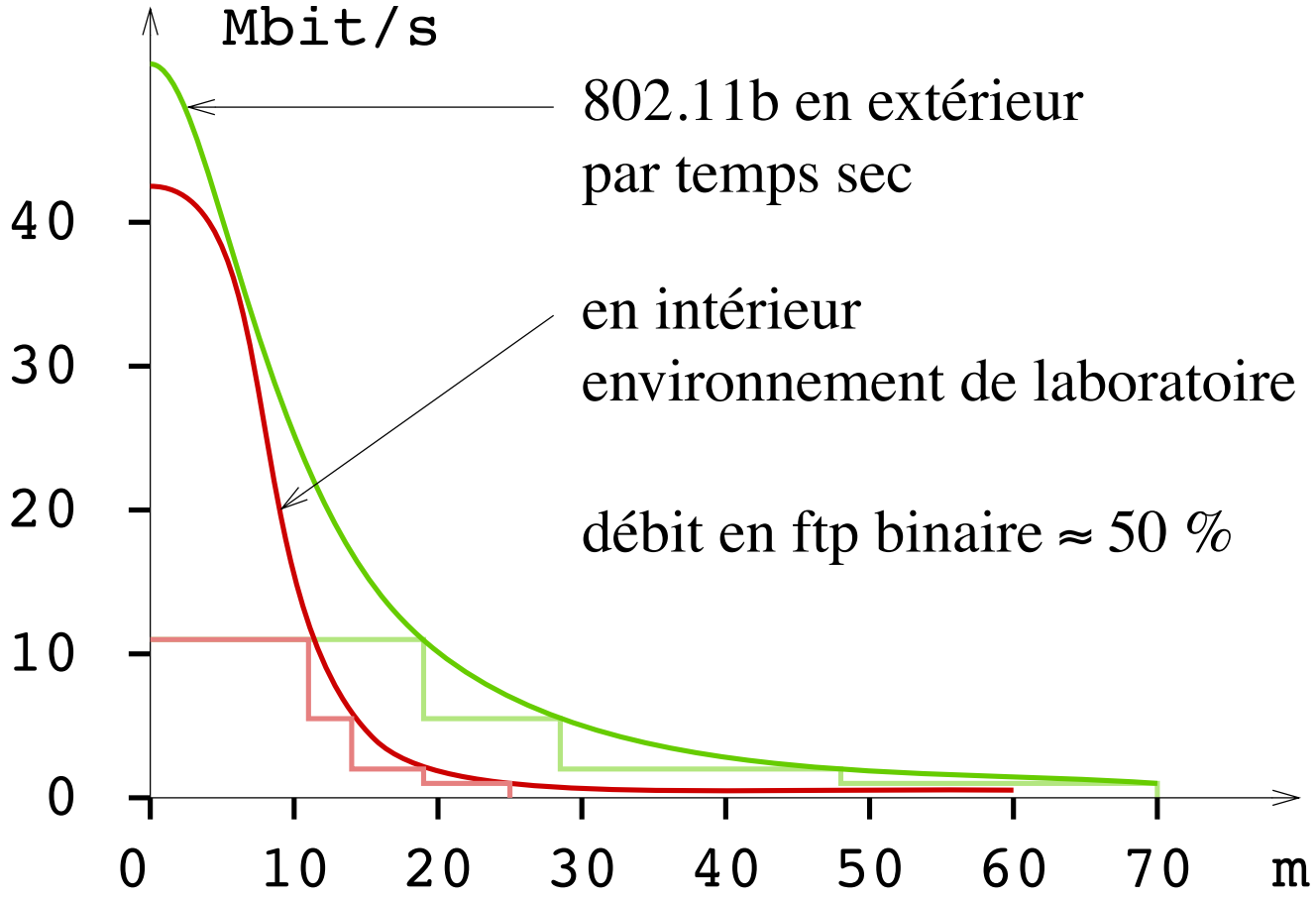
$\Rightarrow$ puissance distribuée décroît comme son inverse.

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

Fonctions utilisées en 1ère approximation :

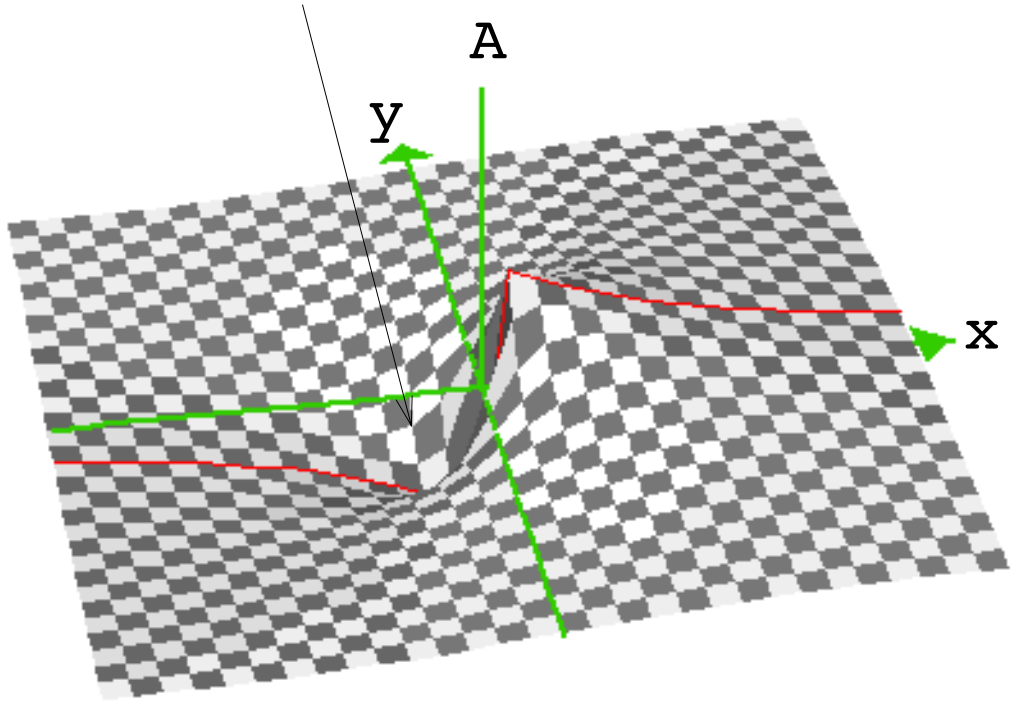
$$d \approx \frac{50}{1 + \left(\frac{r}{10}\right)^2} \; ; \; d \approx \frac{50}{1,2 + \left(\frac{r}{10}\right)^4}.$$

Débit : d = f(r)


Mbit/s
802.11b en extérieur
par temps sec
en intérieur
environnement de laboratoire
débit en ftp binaire ≈ 50 %
0
10
20
30
40
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