



Architecture des réseaux sans fil

Daniel AZUELOS
Architecture réseau & sécurité
Institut Pasteur

13 octobre 2004



Du 802.11 au 802.11n

Réseaux sans fil	3	Sécurité	37
Ondes électro-magnétiques	4	Sécurité des personnes	38
Spectre électro-magnétique	5	Sécurité des réseaux	40
802.11b	6	Contrôle d'accès	41
802.11b : canaux	7	WEP : un extincteur vide	42
Fonctionnement	8	Extranet	43
Types de réseaux	10	Filtrage	44
Mobilité	11	Audit	45
802.11a	12	Syndrome Maginot	47
802.11a : canaux	13	Améliorer la sécurité des réseaux	49
802.11a : avantages & inconvénients	14	Futur	50
802.11g	15	Évolutions	51
OFDM	16	Conseils pratiques	52
802.11a, 802.11b ou 802.11g ?	17	Annexes	53
Réglementation	18	Loi de Shannon	54
Déploiement	19	Réflexion, absorption	55
Propagation	21	Glossaire	56
Transparence	22	Sécurité des personnes	57
Interférences	23		
Couverture	25		
Antennes	26		
Intégration dans l'ordinateur	28		
Configuration client	29		
Classes d'usage	32		
Plan des fréquences	34		
Réglage des PA	35		
Gestion des PA	36		



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 fat) label de qualité ;

→ **réseaux sans fil** !

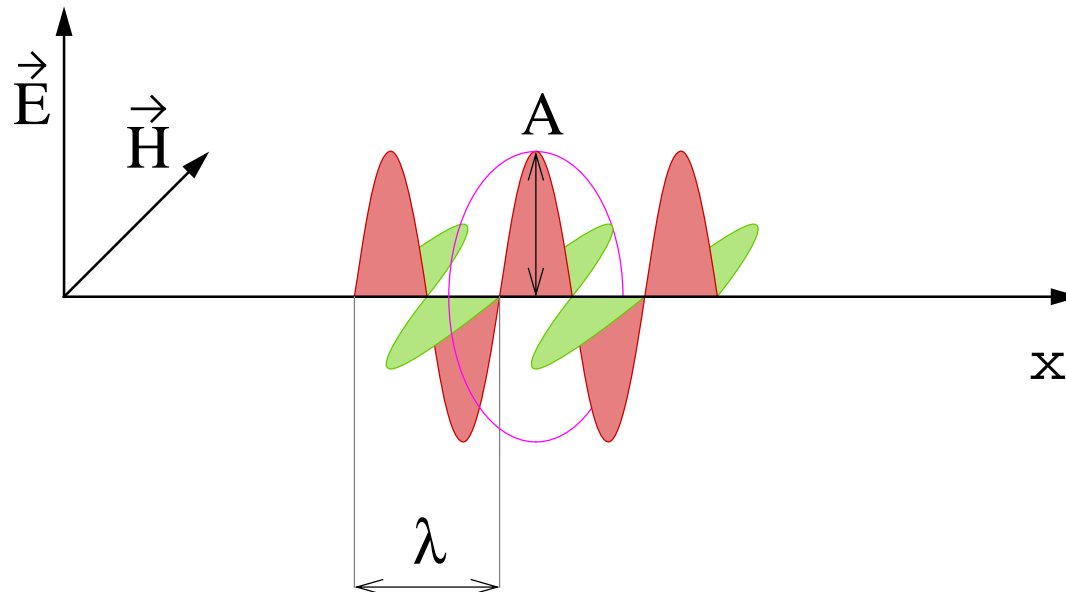
Principe : onde hertzienne = porteuse
+ transport de données numériques / porteuse.

Utilisée pour les transmissions satellite.

Ondes électro-magnétiques

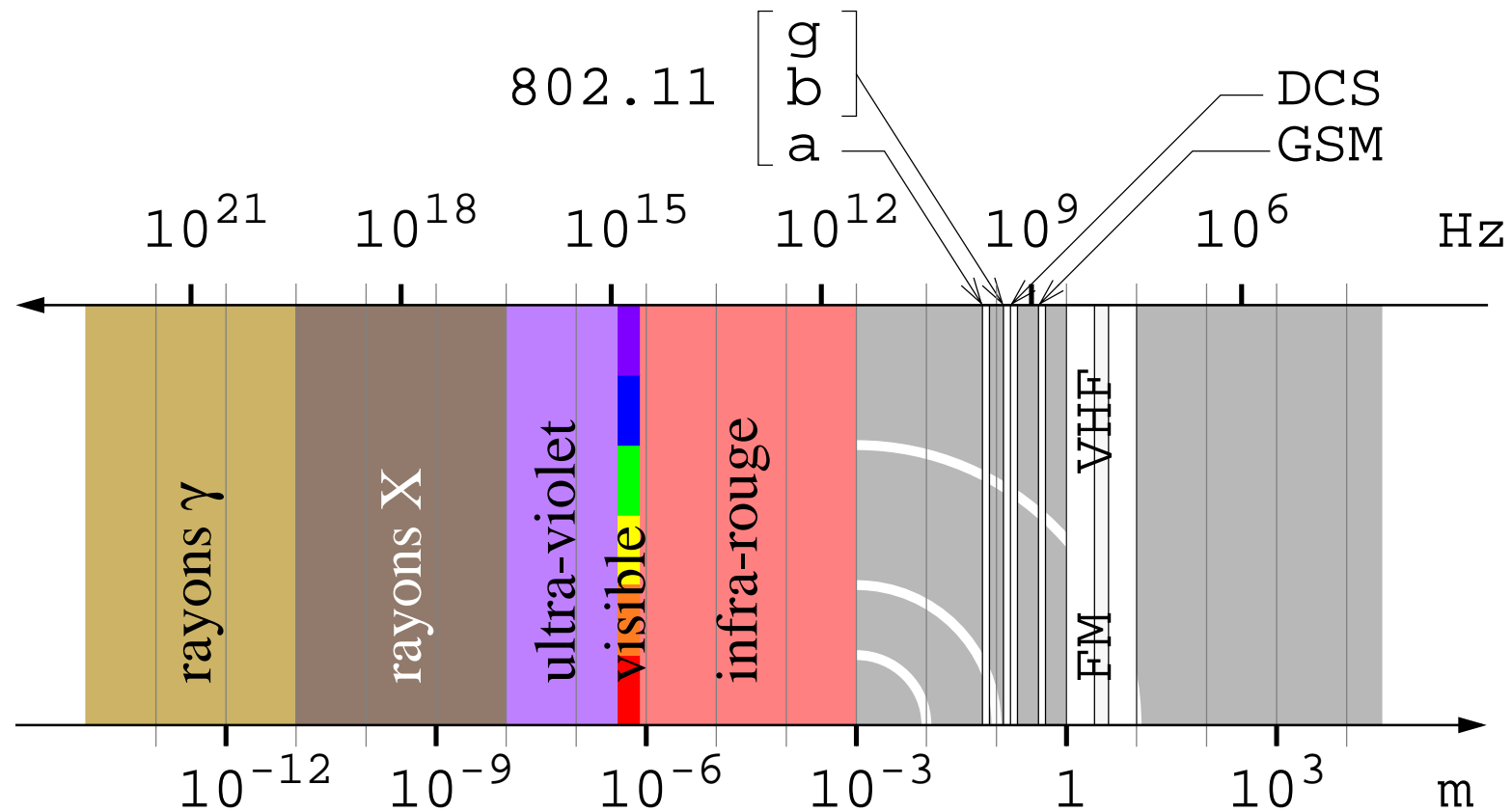
Ondes radios, infra-rouge, visible, ultra-violet, X, γ ...

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



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
 2000 → 802.11a
 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**.

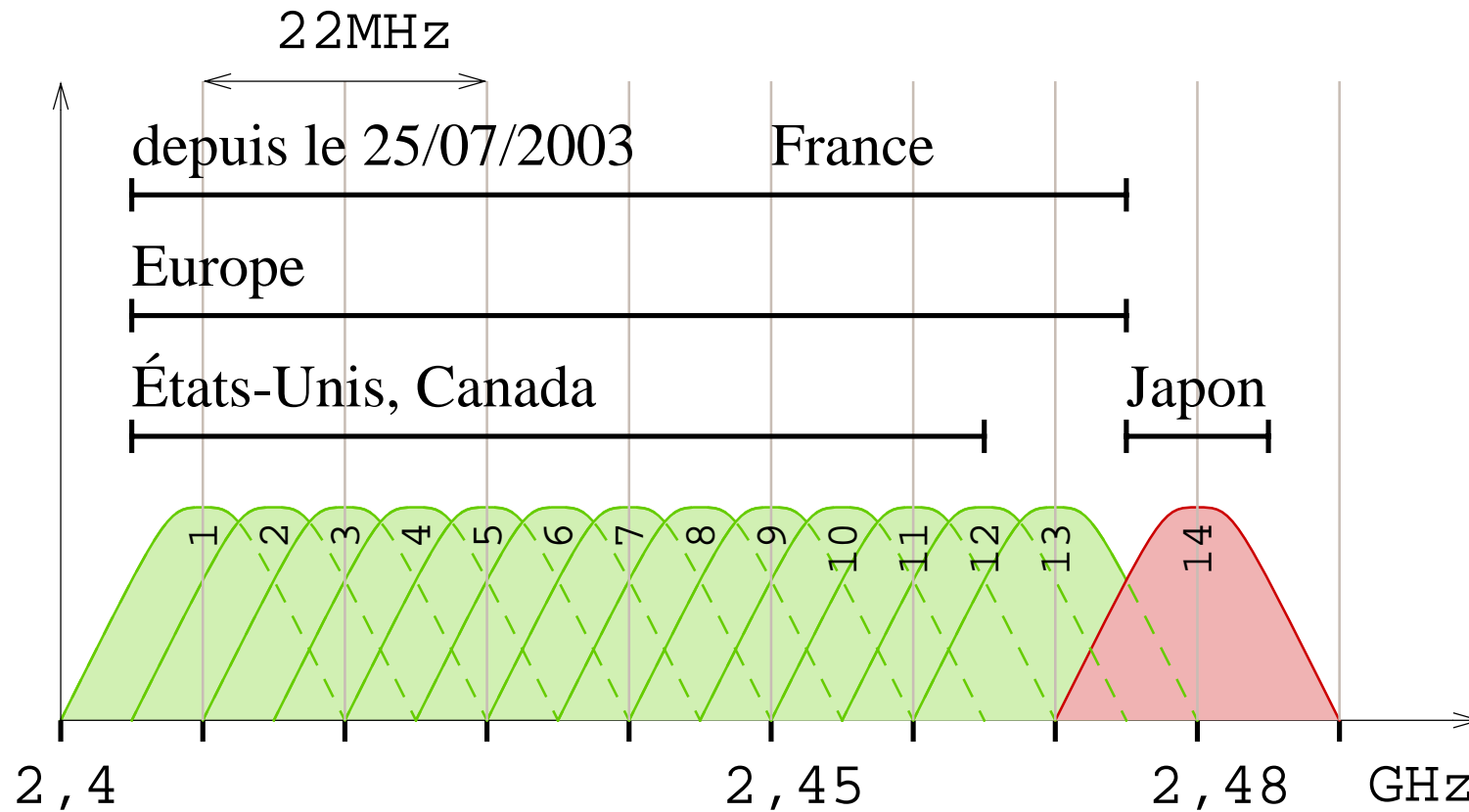
Utilisation du medium : DSSS.

14 canaux, 11 sont utilisables aux U.S.A., 13 en France : [1 ; 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

Carte sans-fil (côté 802.11) \approx carte Ethernet (côté 802.3).

Un équipement actif de réseau sans-fil =
équipement ayant au moins 2 interfaces.

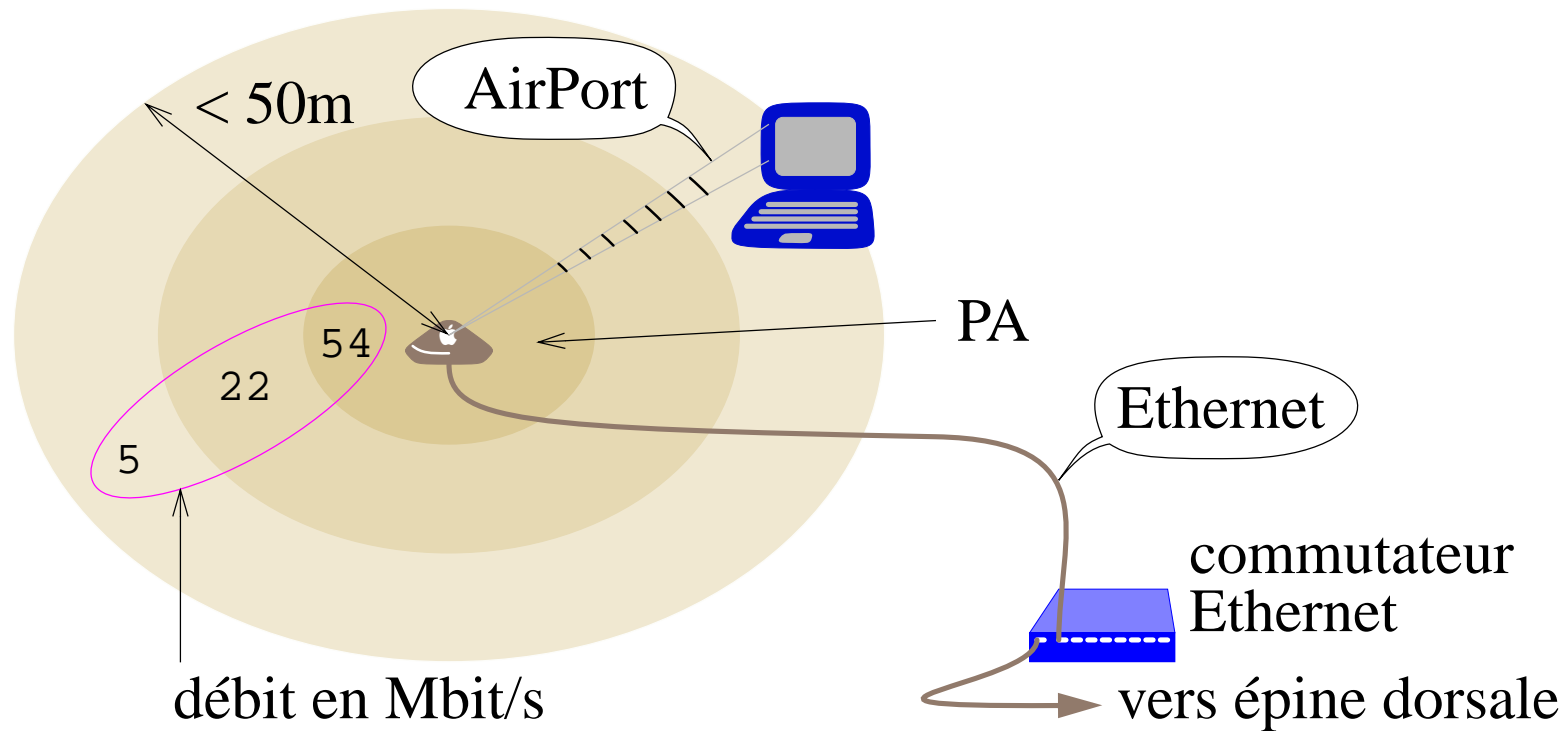
Visibilité radio \Rightarrow établissement d'une liaison.

Déplacement \Rightarrow variabilité du S/B
 \Rightarrow renégociation de la vitesse utilisable.

Éloignement, obstacle \Rightarrow perte de la liaison.

Techniques d'utilisation d'une bande de fréquence venant des techniques modem : QAM64, OFDM.

Fonctionnement



Une liaison sans fil

⇒ 2 cartes AirPort !

Raccordement au reste du réseau

⇒ liaison Ethernet.



Types de réseaux

Multi-point \approx câble Ethernet croisé.

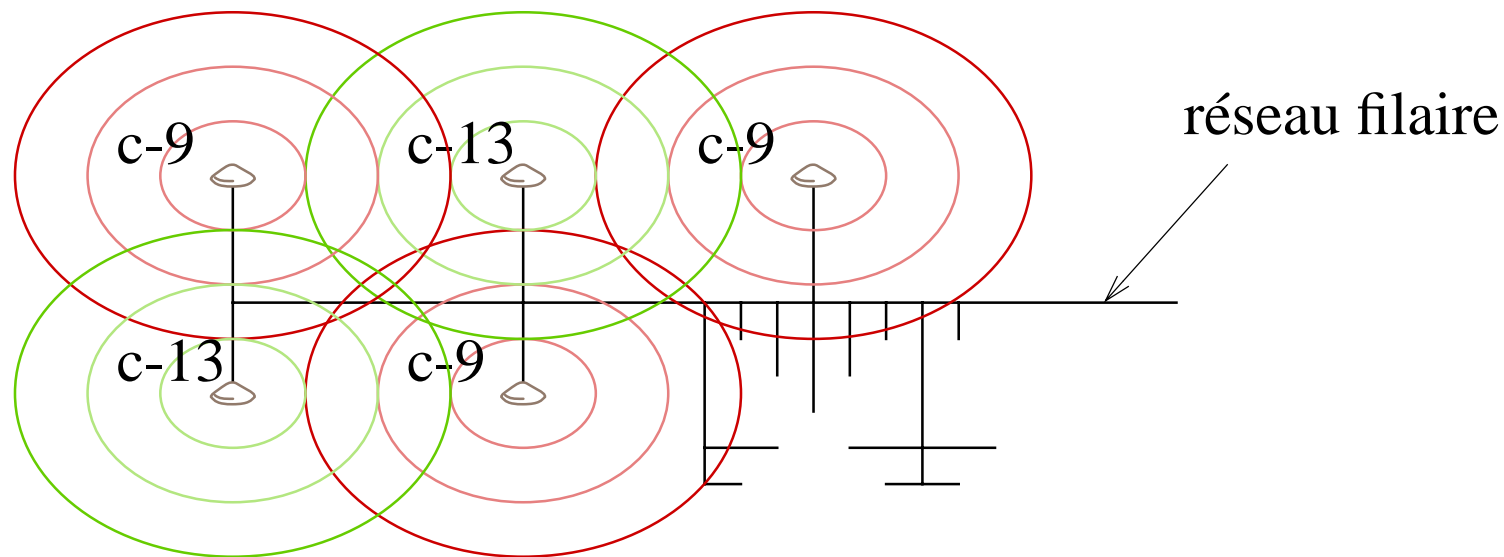
On peut être plus de 2 sur le même support (réunion des portées des différentes cartes participant).

Réseau d'infrastructure : même nom de réseau (SSID), plusieurs PA (points d'accès), 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 23).





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.

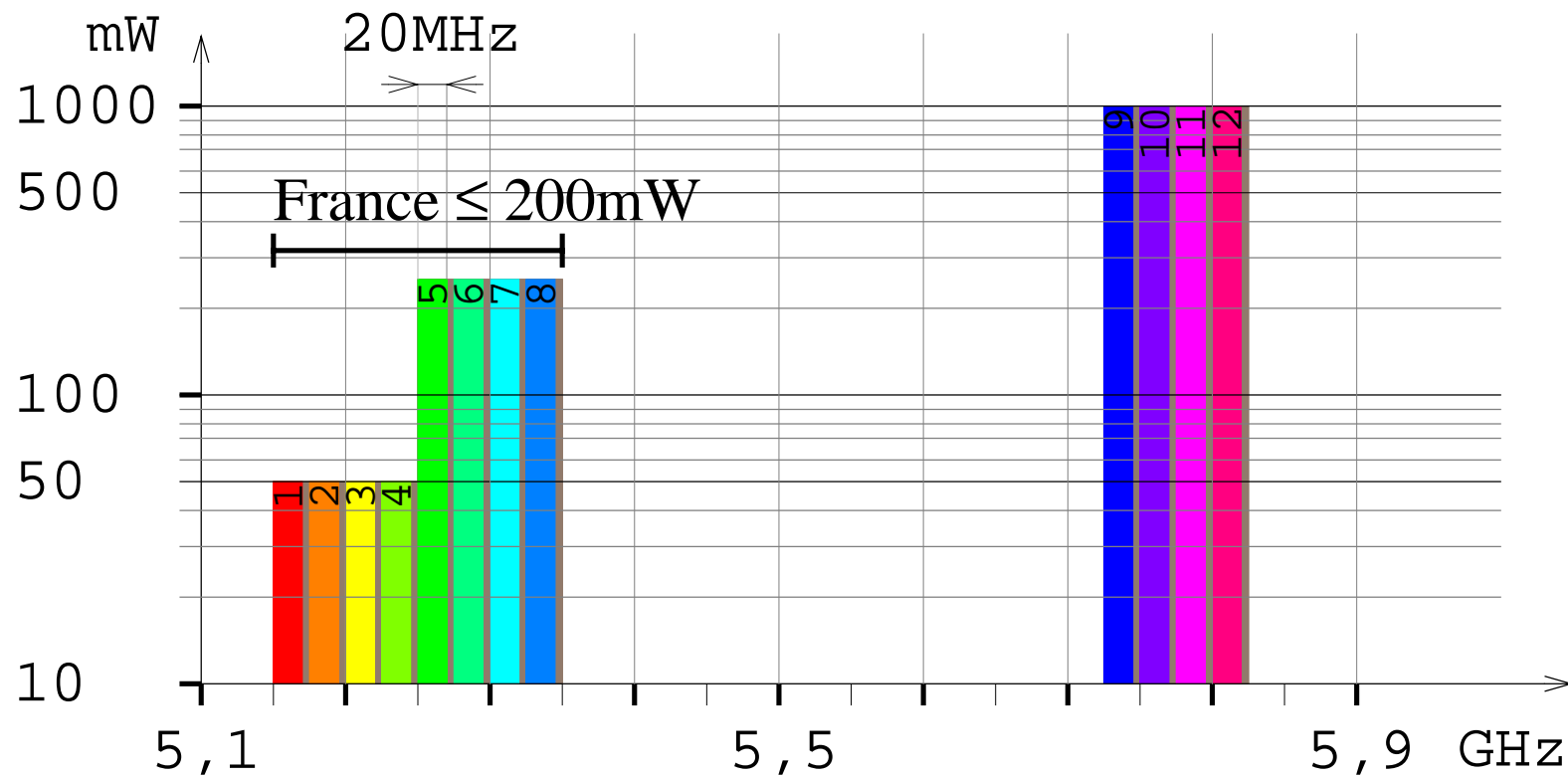
Technique de modulation :

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 \neq

⇒ difficulté d'utilisation pour les voyageurs.

Fréquence élevée

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

⇒ énergie consommée élevée (inadapté au portable) ;

⇒ absorption élevée (⇒ $n_{PA} \times 2$ 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.

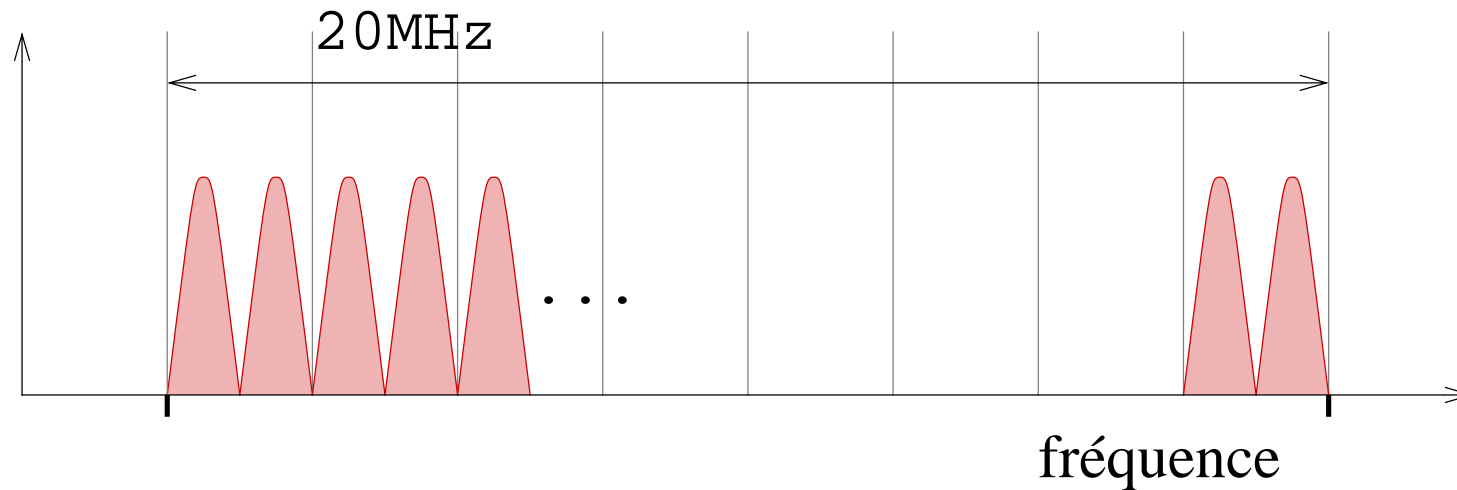
Débit : **1 → 54 Mbit/s**.

Méthode d'accès : CSMA/CA.

802.11g est compatible avec le 802.11b. Gabarit d'atténuation plus faible qu'en 802.11b ⇒ chevauchements à proscrire.

En mode compatible utiliser une distance de canaux = 5.

OFDM



52 porteuses espacées : $f = n \times 312,5 \text{ kHz}$
 \Rightarrow nœuds de toutes les porteuses coïncident
 \Rightarrow n'interfèrent pas entre-elles.
Débit sur chaque porteuse plus bas
 \Rightarrow BER + bas.



802.11a, 802.11b ou 802.11g ?

Les utilisateurs qui tirent le sans-fil sont les utilisateurs nomades
⇒ besoin de compatibilité : canaux identiques dans le monde,
⇒ 802.11g !

En réseau d'entreprise :

802.11a → $n_{PA} \times 8$ 😞 !

802.11b → $d < 5$ Mbit/s

⇒ 802.11g !

⇒ 802.11g !



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>

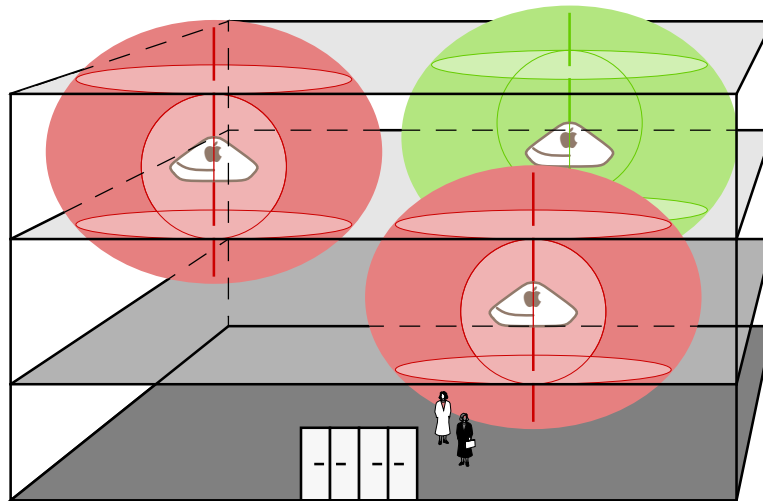
- utilisation à l'intérieur des bâtiments : libre, PIRE < 100mW ;
- utilisation à l'extérieur : 1-7 < 100 mW, 8-13 < 10 mW 😞 !

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 ?

Déploiement



Contraintes à respecter :

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



Où déployer ?

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 \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
→ 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 :

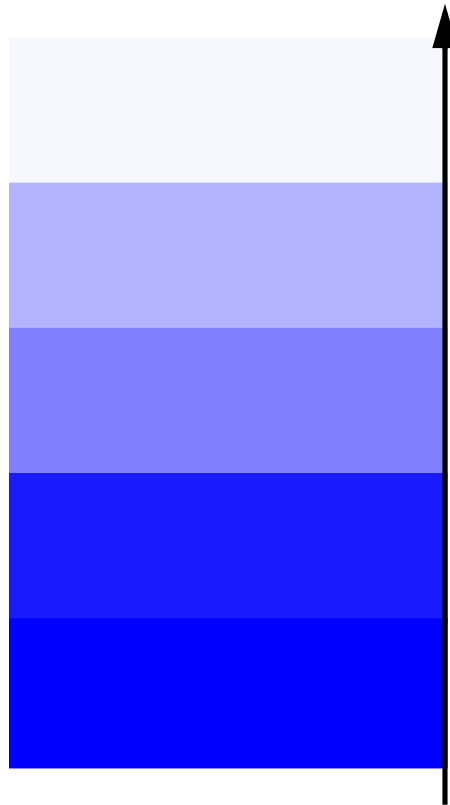
- réfractée ;
- réfléchie ;
- diffractée ;
- absorbée.


Une onde électro-magnétique est absorbée par un circuit résonnant à sa fréquence : plomb, nos os, O₂, l'atmosphère, H₂O, la pluie, le maillage du béton armé.

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

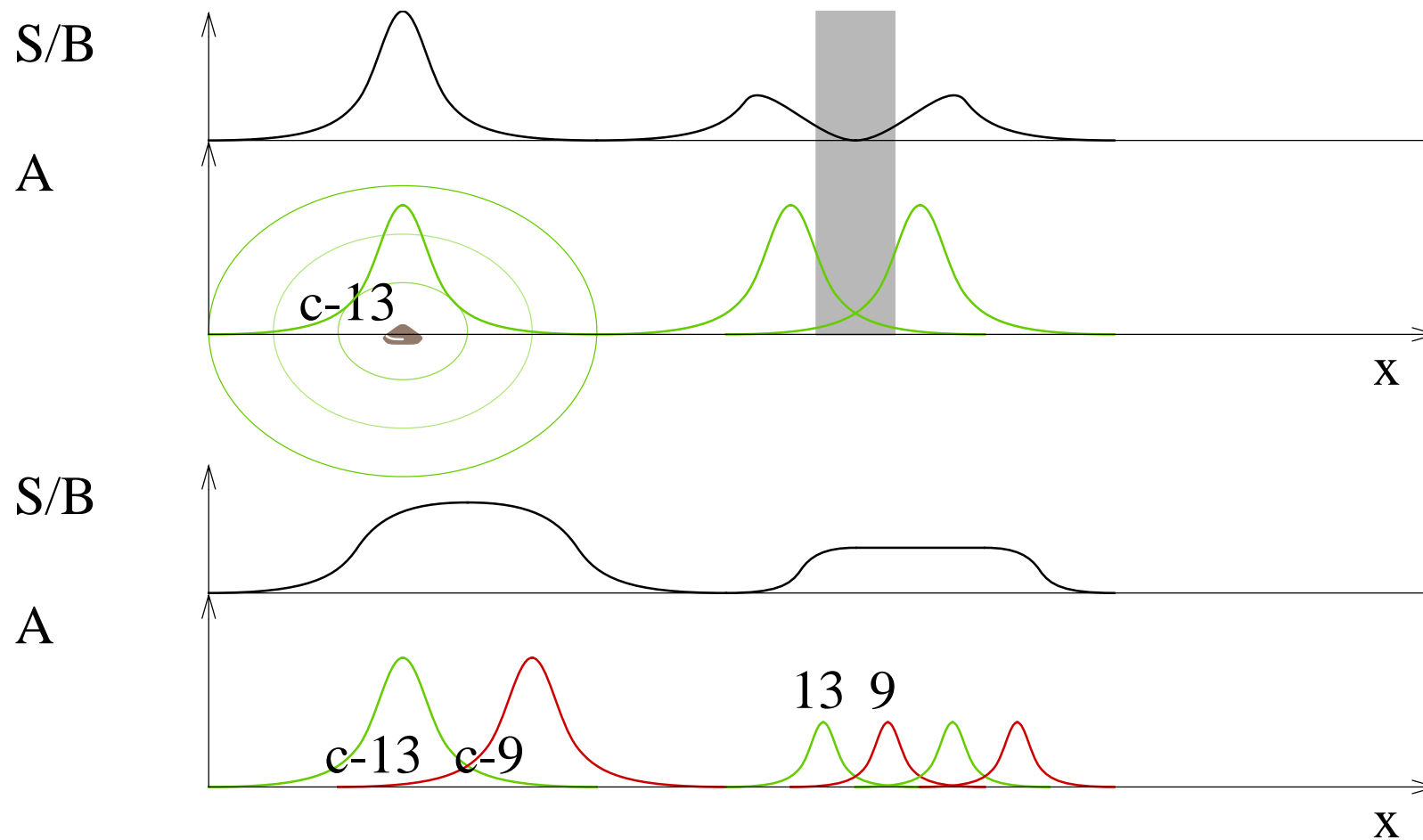


Transparence

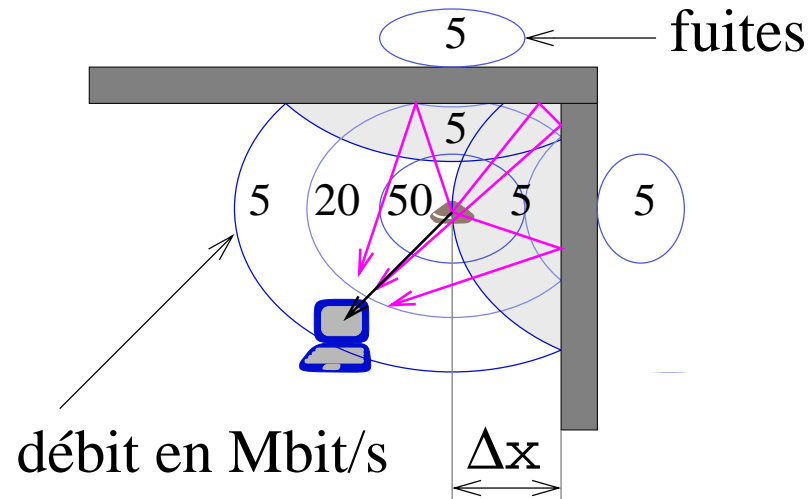


air
bois
air humide
plastique, verre
eau, végétation
animaux, nous : 
cloisons en plâtre, brique
béton
verre blindé
métal conducteur

Interférences



Interférences

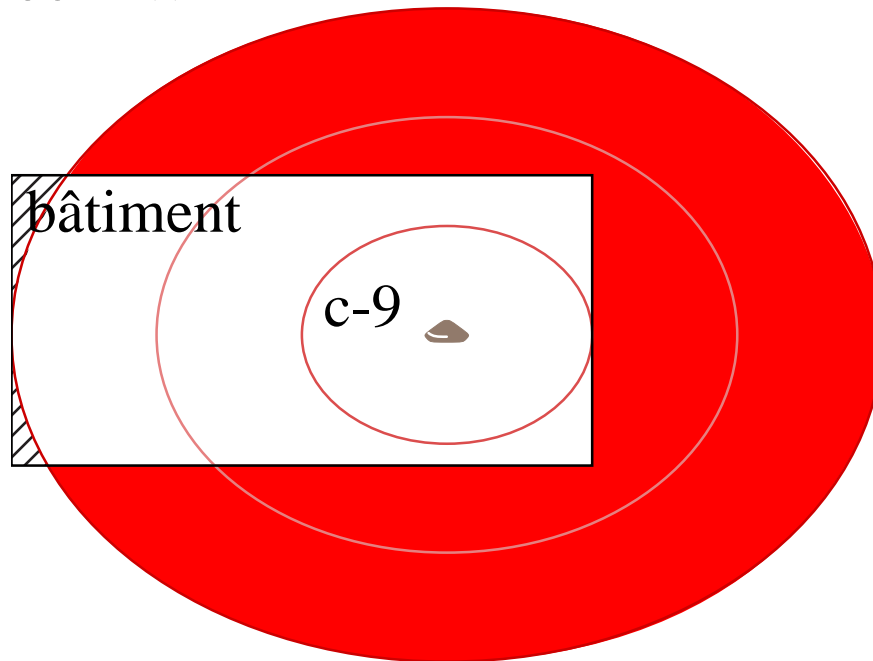




Plus la distance à un obstacle \pm transparent est petite,
plus la zone d'interférence est grande,
plus la zone de diffraction est grande et difforme.

Problématique d'éclairage.

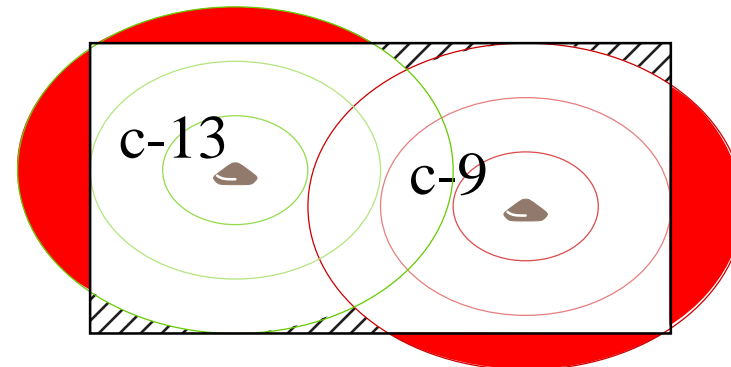
Couverture

60 mW



défaut de :  couverture
 sécurité

30 mW





Antennes

Omni-directionnelles (isotrope) :

les ondes électro-magnétiques vont dans toutes les directions ;
et le rapport signal/bruit décroît 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.

⇒ placement précis, et sensibilité aux réfractions.

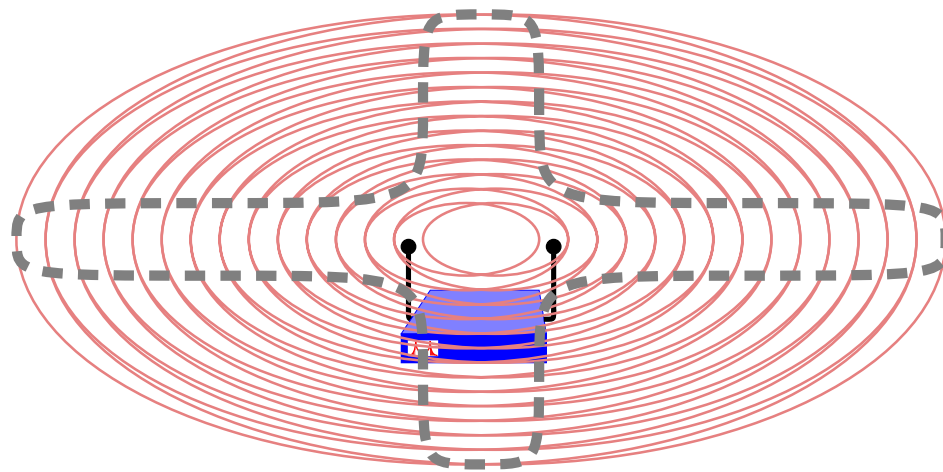
Analogie :

éclairer un auditorium avec des projecteurs de scène 😞 !

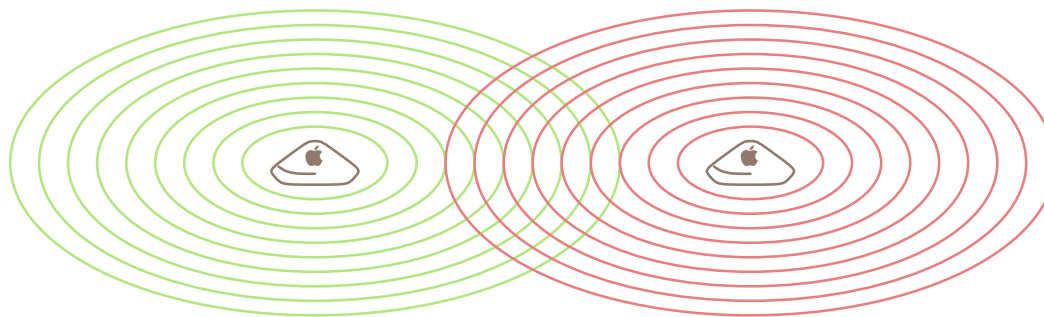
Fait vendre plus d'antennes et les services d'un installateur 😞 !

Antennes

antennes multiples orientables



PA multiples





Intégration dans l'ordinateur

Les solutions à base de carte PCMCIA ou de carte externe sur port USB sont médiocres 😞 : la sensibilité maximale d'une antenne dipôle replié $\lambda/4$ est dans le plan orthogonal à son axe.

L'intégration dans les portables est très peu pensée, sauf chez Apple qui tient en ce domaine 4 ans d'avance.

Ils ont aussi pensé à intégrer une antenne dans les ordinateurs fixes.

L'intégration dans les S.E. est très liée à une fonction que certains S.E. n'ont pas encore pensée :

commutation de réseau, commutation d'environnement.



Configuration client

Chaque utilisateur souhaitant connecter un ordinateur à nos réseaux doit :

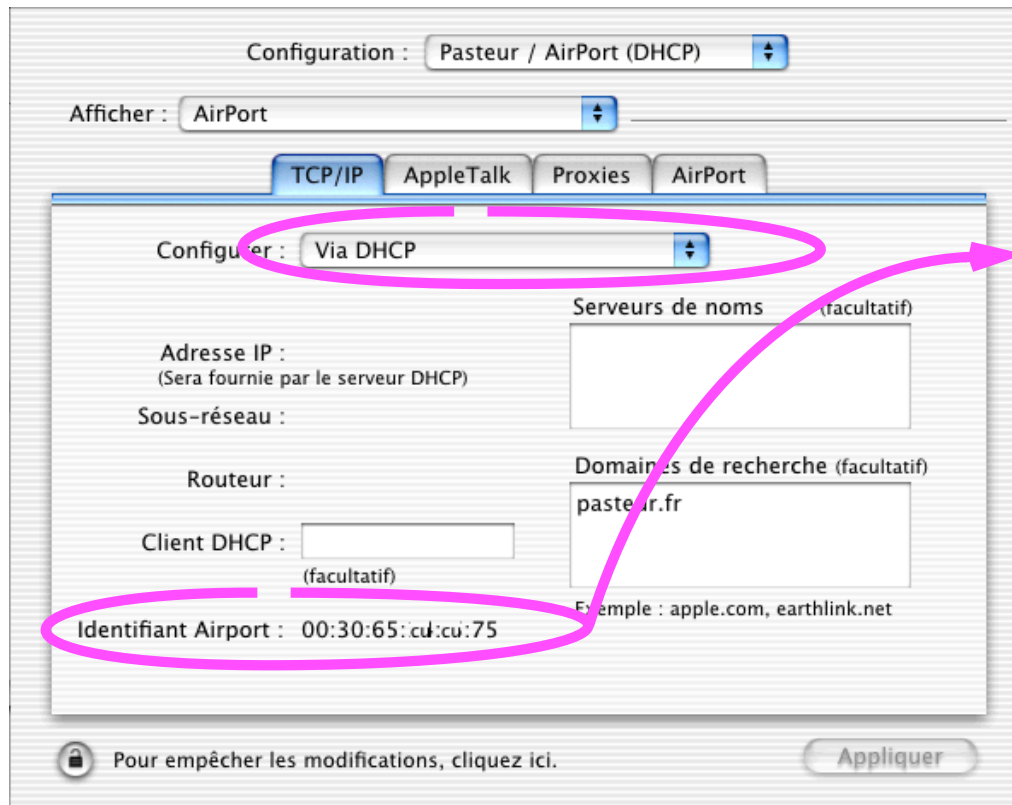
- nous communiquer l'adresse MAC (Ethernet ou AirPort) ;
- configurer TCP/IP via DHCP.

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.



Construction du réseau

- recherche des zones difficiles de l'espace à couvrir ;
- étalonnage du PA dans une zone caractéristique et détermination d'une couverture correcte pour le débit visé ;
- à partir de plans masse de l'espace à couvrir dessiner les zones couvertes par les PA ;
- en fonction de **classes d'usage** à définir, éventuellement densifier les PA à partir de ce 1er plan ;
- faire le **plan des fréquences** ;
- faire poser les prises RJ45 & secteur (ou bien commutateurs 802.3af) à une hauteur d'environ 2 m sans coller au plafond ;
- régler les PA en commençant par les plus difficiles et en présence de la population typique.



Classes d'usage

Amphi :

100 utilisateurs à 128 kbit/s (max), équipés à : 50% (max)

$$d_{\max} = 50 \times 128 \text{ kbit/s} = 5 \text{ Mbit/s} \Rightarrow$$

$$n_{PA}(d) = \left\lceil \frac{d_{\max}}{20 \text{ Mbit/s}} \right\rceil = 1$$

$$n_{PA}(u) = \left\lceil \frac{u_{\max}}{10} \right\rceil = 5$$

$$d'où : n_{PA} = \max(n_{PA}(u), n_{PA}(d)) = \mathbf{5}$$

Contrôle d'accès : 0

confidentialité : 0

\Rightarrow confinement en **extranet** (page 43) !



Classes d'usage

Labo :

10 utilisateurs à 1 Mbit/s, équipés à 70 %

$$d_{\max} = 7 \times 1 \text{ Mbit/s} = 7 \text{ Mbit/s} \Rightarrow$$

$$n_{PA}(d) = \left\lceil \frac{d_{\max}}{20 \text{ Mbit/s}} \right\rceil = 1$$

$$n_{PA}(u) = \left\lceil \frac{u_{\max}}{10} \right\rceil = 1$$

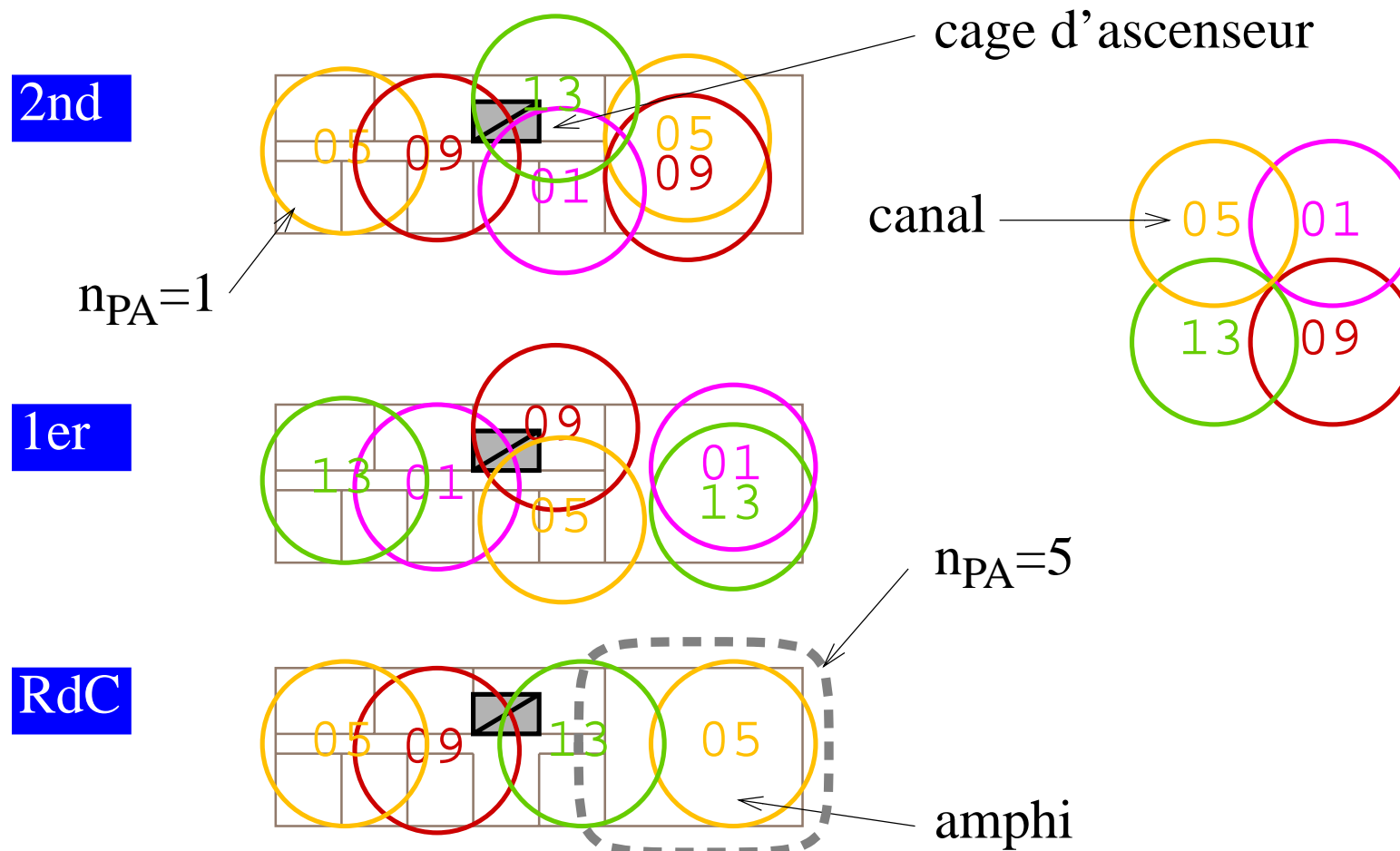
$$d'où : n_{PA} = \max(n_{PA}(u), n_{PA}(d)) = \mathbf{1}$$

Contrôle d'accès : MAC, 802.1X (page 41)

confidentialité : 0

\Rightarrow chiffrement de bout en bout !

Plan des fréquences





Réglage des PA

Placement : 1 ou 2 clients en position limite, mesure.



initial (densité faible)
→ 1/2 j ;

densité élevée
→ 1 j.

⇒ 1 prise secteur +
1 prise Ethernet !
ou bien 802.3af
→ 15 j - 1 mois.



Gestion des PA

3 approches possibles :

- PA lourd :
système sophistiqué embarquant toutes les fonctions de contrôle d'accès, de routage...
= ceinture, bretelles, coquille + casque ;
⇒ centraliser la gestion de ces PA
/ logiciel fiable / S.E. fiable !
- PA léger :
simple répéteur Ethernet - sans-fil configurable via un serveur de configuration
= gestion centralisée ;
⇒ équipement serveur de configuration de PA.
- PA quelconque + ensemble d'outils développés pour gérer des équipements réseau.



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 \approx **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 (page 57):

GSM :	< 2W ;
DCS :	< 1W ;
Antennes GSM :	20 à 50 W ;
four à micro-ondes :	1 kW ;
émetteur de la tour Eiffel :	6 MW !

Tout champ électro-magnétique décroît 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 genoux,

100 000 dans une classe.



Sécurité des réseaux

Transport de données \Rightarrow champ électro-magnétique,
 \Rightarrow sensibilité aux autres champs.

Ces transports de données (sauf fibre optique) peuvent être facilement écoutés et brouillés :

- un câble Ethernet craint tubes fluorescents et câbles électriques,
- un réseau sans fil craint les fours à micro-onde qui fuient et les téléphones DECT de mauvaise qualité.

Réseaux sans fil \Rightarrow écoute + simple que sur un réseau Ethernet :
0 prise ou plutôt prise de 50 m de rayon.

\Rightarrow communication sur les risques ;

\Rightarrow contrôle d'accès, protection des données : confidentialité.



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 : un extincteur vide

WEP : Wired Equivalent Privacy.

Comment 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),

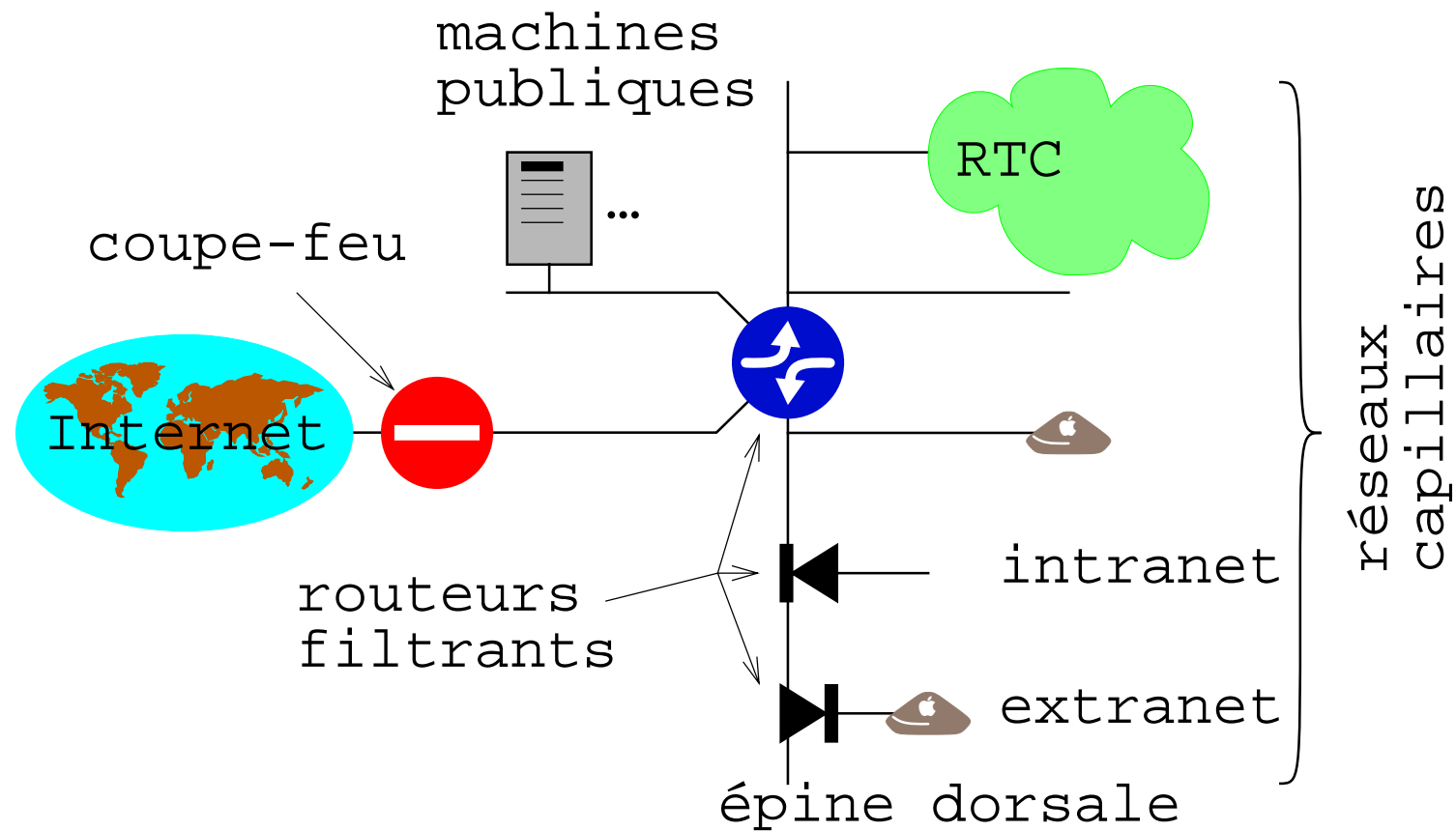
et ils ont laissé dans l'ombre un vrai problème :

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 😞 !

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.



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 de voisins dans lesquels nos utilisateurs naïfs pourraient se connecter automatiquement ;
- recherche de signal en bordure :
<http://istumbler.net/> ;
- triangulation à partir de 3 relevés de niveau de signal.

Constat pragmatique :

- écouter un réseau sans fil dans un environnement **bien couvert** \Rightarrow « entrer » dans la zone de couverture ;
- la connexion d'un PC porteurs d'un nid de vers Windows
= risque \gg à celui du guerrier des ondes 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-waule ».

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 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 résident 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 :
tout accès à une prise Ethernet est contrôlé : utopie 😞 !

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.



Améliorer la sécurité des réseaux

Risques par ordre décroissant à maîtriser :

- Qualité des S.E. : interdire les PC sous Windows ou bien engager clairement la responsabilité des utilisateurs dans le maintien de leur outil en bon état : PSI, RI, note de service.
- Raccordement de n'importe quoi au réseau : répéteur sauvage, borne AirPort pirate... :
même remède
+ contrôle d'accès (Ethernet & AirPort → 802.1X)
+ déploiement de réseau sans-fil (occuper l'espace, détecter les anomalies, acquérir la compétence).
- Confidentialité des communications : chiffrement au niveau 2 (802.11i) ou bien au niveau 3 (tunnel chiffré).



Futur

- 1999** : 802.11b ; label de qualité Wi-Fi ;
- 2000** : 802.11a : 54 Mbit/s / 5 GHz ;
- 2003** : 802.11g : 54 Mbit/s / 2,4 GHz ;
Centrino (802.11b : 4 ans de retard 😞 !).
- 2004** : **802.11i** : chiffrement AES / 802.11? ;
802.1X : authentification d'accès au réseau ;
802.16 ? WMAN (fixe),
802.20 ? WMAN (mobile).
- 2005** ? **802.11n** : 540 Mbit/s / 40 MHz @ 2,4 GHz,
135 Mbit/s / 20 MHz @ 2,4 GHz...



Évolutions

Des débits :

$$\text{loi de Shannon : } d = B \times \log_2 \left(1 + \frac{s}{b} \right)$$

$$\Rightarrow 20 \text{ Mhz, } 20\text{dB} : 130 \text{ Mbit/s}$$

$$\Rightarrow 40 \text{ Mhz, } 30\text{dB} : 400 \text{ Mbit/s}$$

Des PA :

taille & consommation en baisse régulière ;

le PA sera intégré dans la prise RJ45, puis la remplacera.

De la gestion des PA :

le commutateur 10baseT va évoluer vers un commutateur de PA.



Conseils pratiques

Choix techniques ayant un avenir :

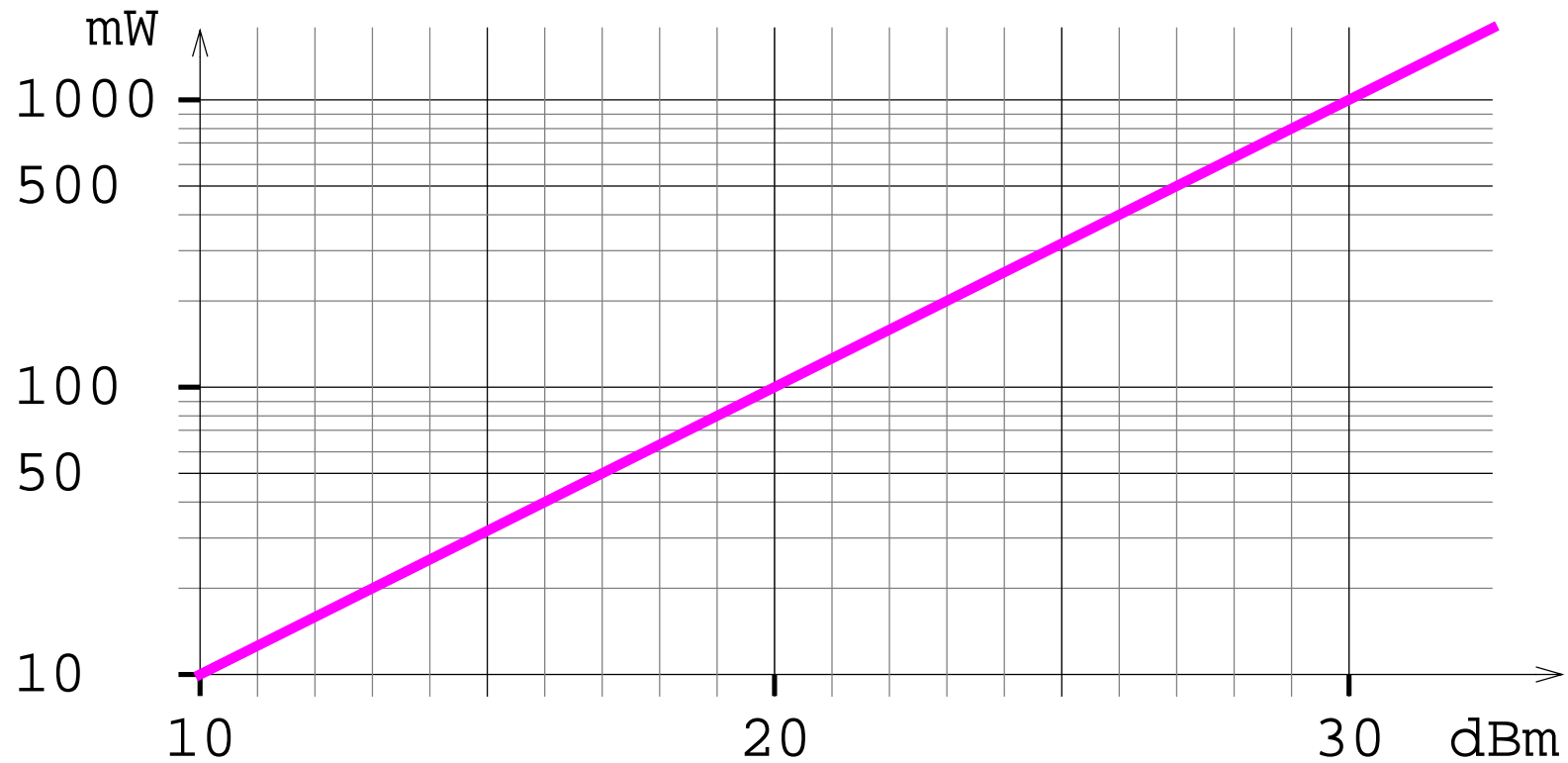
- déployer aujourd'hui du **802.11g** :
rester maître d'œuvre du réseau de demain ;
- éviter des techniques en retard de 4 ans (Centrino) ;
- éviter tout ce qui est basé sur WEP ;
- éviter les protocoles propriétaires d'une complexité que seul le commercial peut certifier.

Communiquer clairement sur les **risques réels** :

- 1 mobile >> 100 000 carte 802.11g ;
- 1 PC sous Windows > **10 h / an** en dégâts, 10 réseaux sans fil raccordant 100 ordinateurs < **20 h / an** !
- faire du chiffrage fiable sur un S.E. fiable !

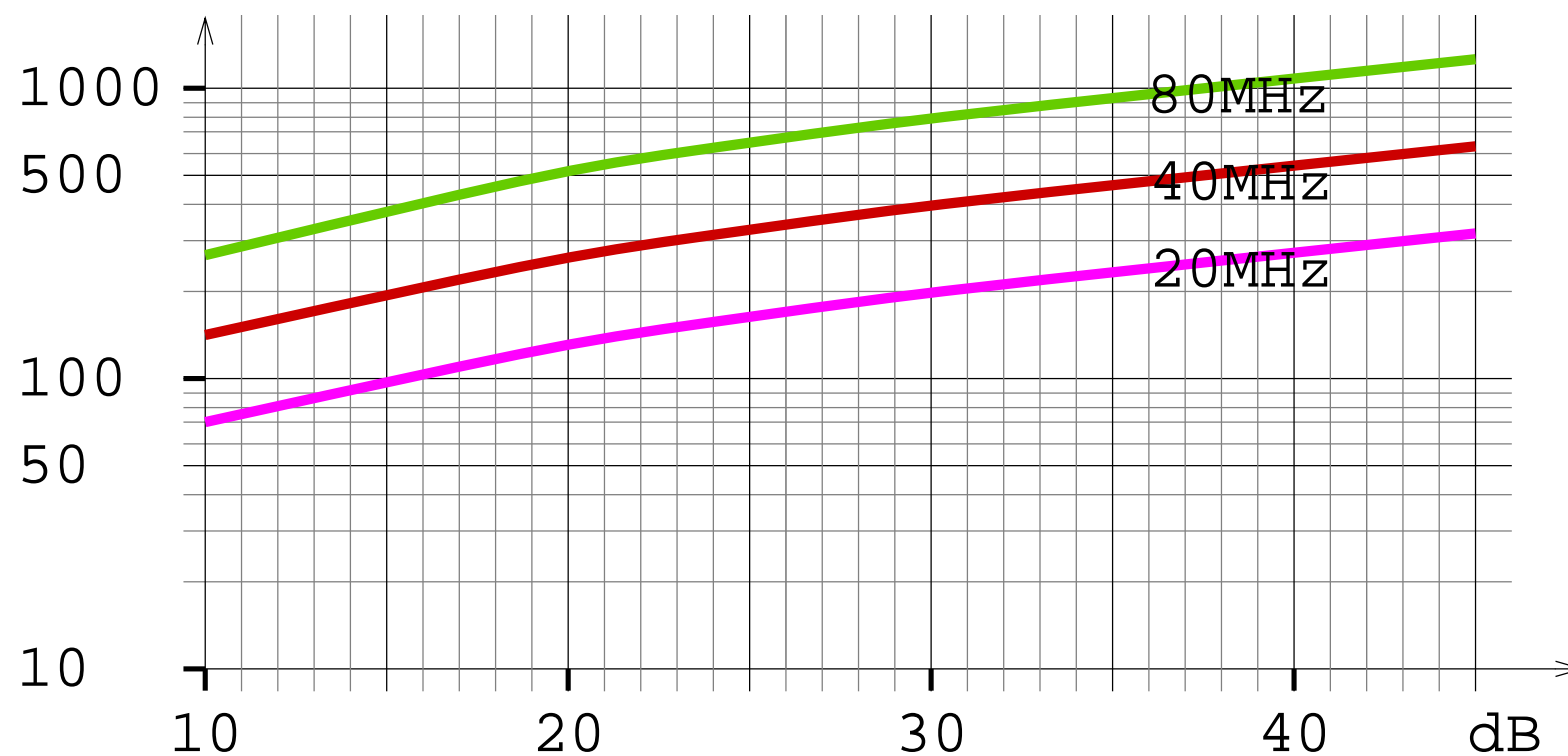


Annexes



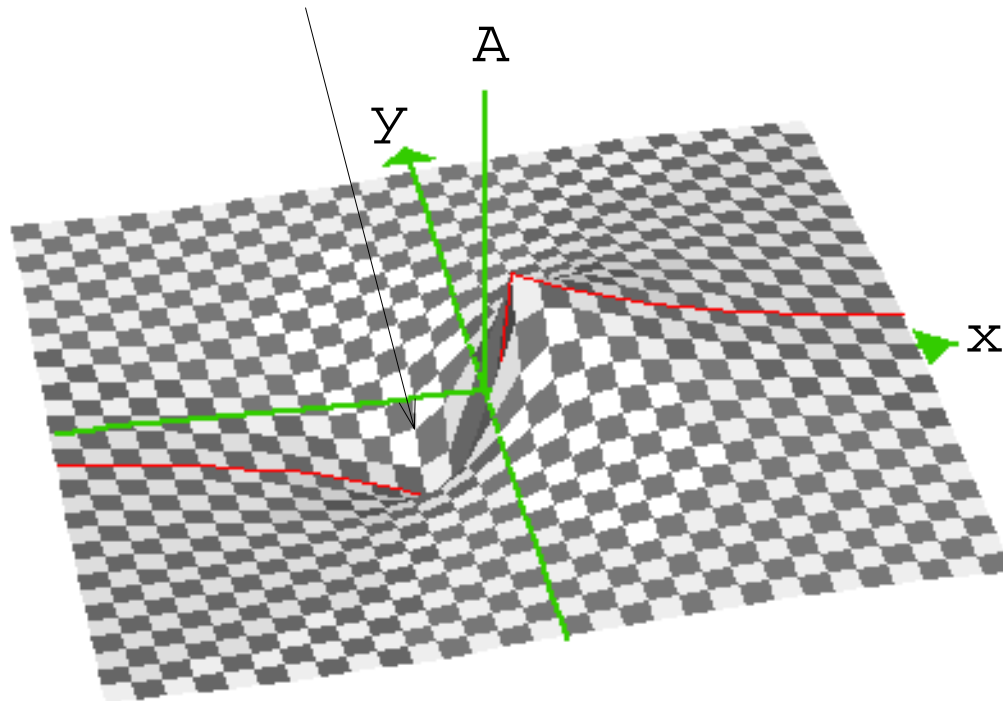
Loi de Shannon

Mbit/s



Réflexion, absorption

onde réfléchie \Rightarrow 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
DSSS	Direct Sequence Spread Spectrum
EAPOL	Extended Authentication Protocol Over LAN
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolution Coding
PIRE	Puissance Isotrope Rayonnée Équivalente
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial-In User Service
SSID	Service Set Identifier
WECA	Wireless Ethernet Compatibility Alliance



Sécurité des personnes

Organismes et programmes de recherche :

OMS : international EMF project :

<http://www.who.int/peh-emf/project/fr/index.html>

ministère de la santé :

http://www.sante.gouv.fr/htm/dossiers/telephon_mobil/

ICNIRP : International Commission on Non-Ionizing Radiation Protection

<http://www.icnirp.de/>

AFSSE : Agence Française de Sécurité Sanitaire Environnementale

<http://www.afsse.fr/>