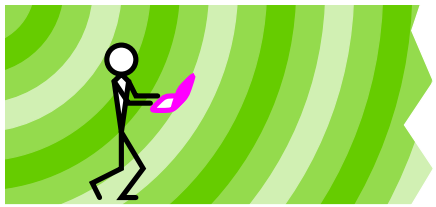
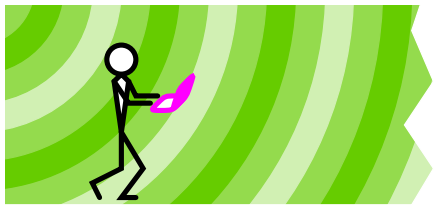


Architecture des réseaux sans fil

Daniel AZUELOS
Architecture réseau & sécurité
Institut Pasteur

05 décembre 2005

Du 802.11 au 802.11n



Fonctionnement

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

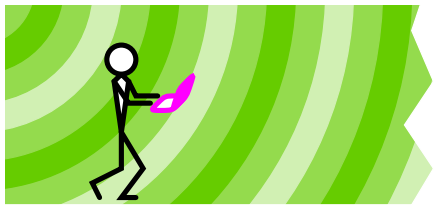
Dénominations :

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.

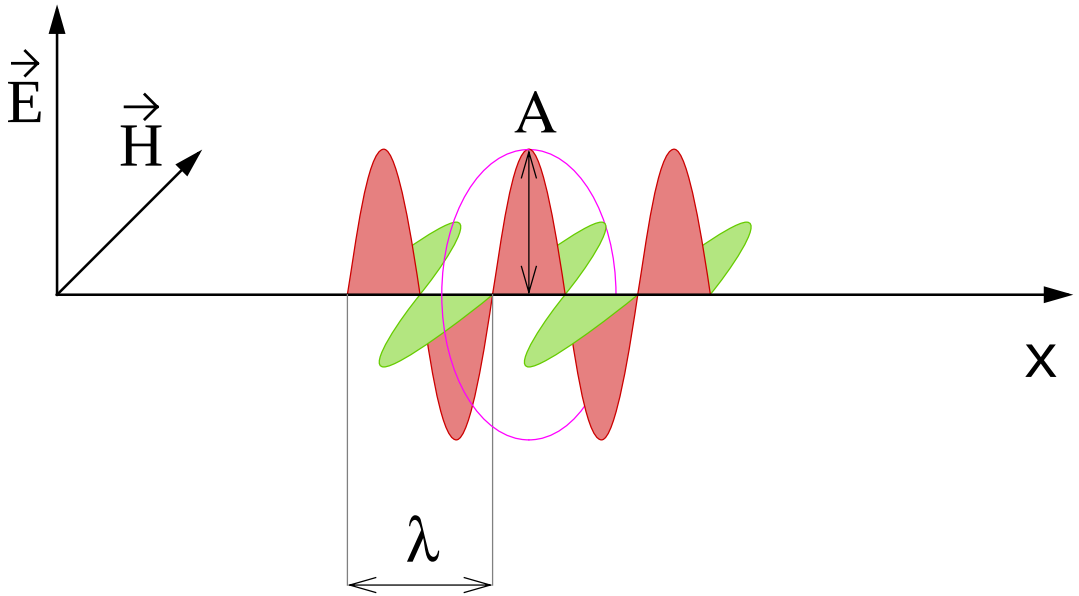
Utilisée pour les transmissions satellite.



Ondes électro-magnétiques

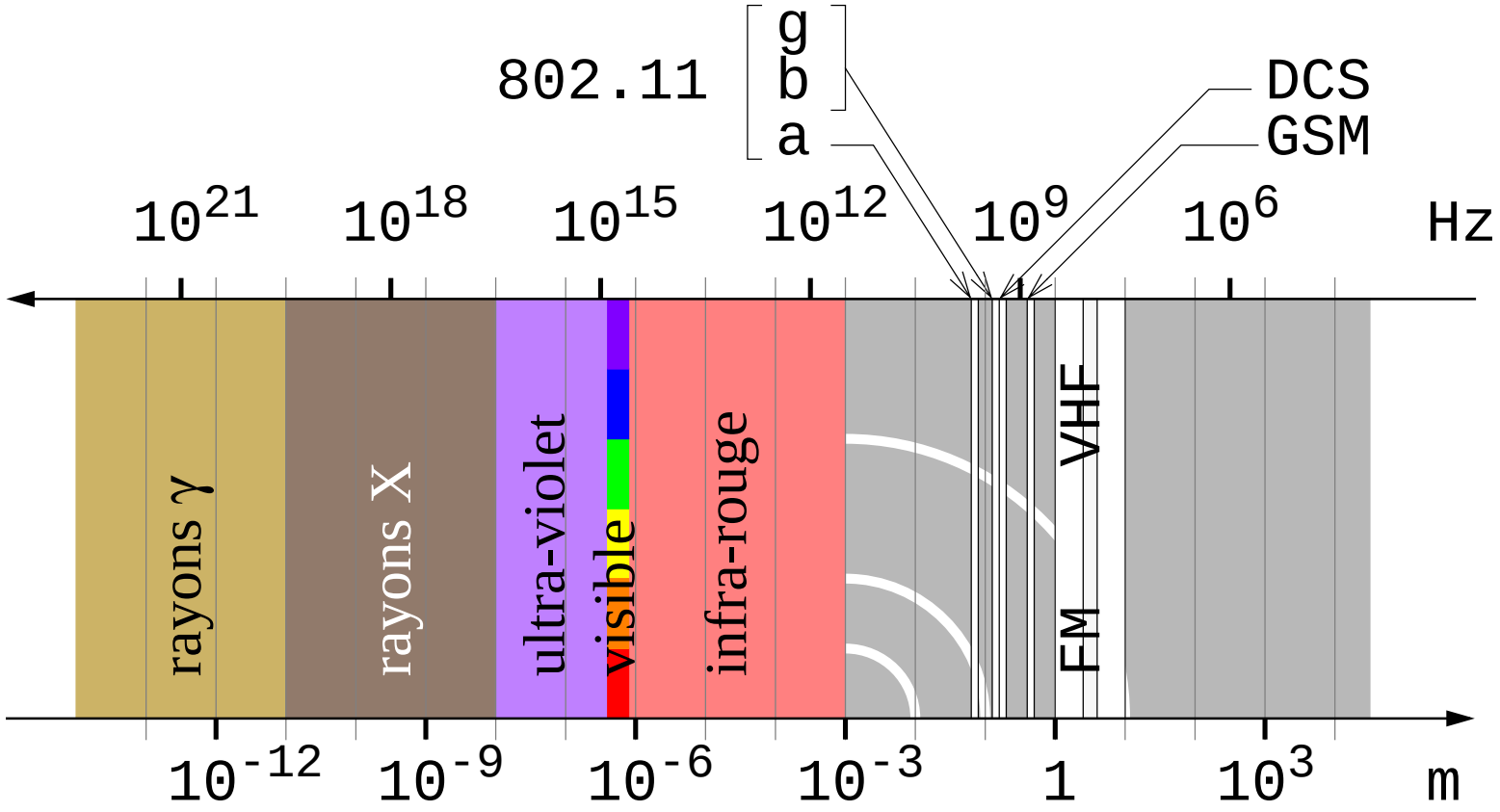
Ondes radios, infra-rouge, visible, ultra-violet, X, γ…

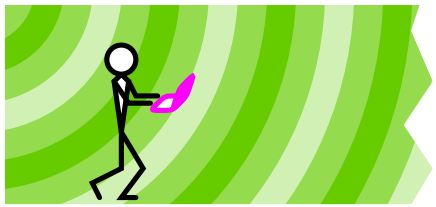
$$\lambda \times f = c \approx 3 \times 10^{8} m/s .$$



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	2 Mbit/s
	1999 → **802.11b**	11 Mbit/s
	2000 → 802.11a	
	2003 → 802.11g	

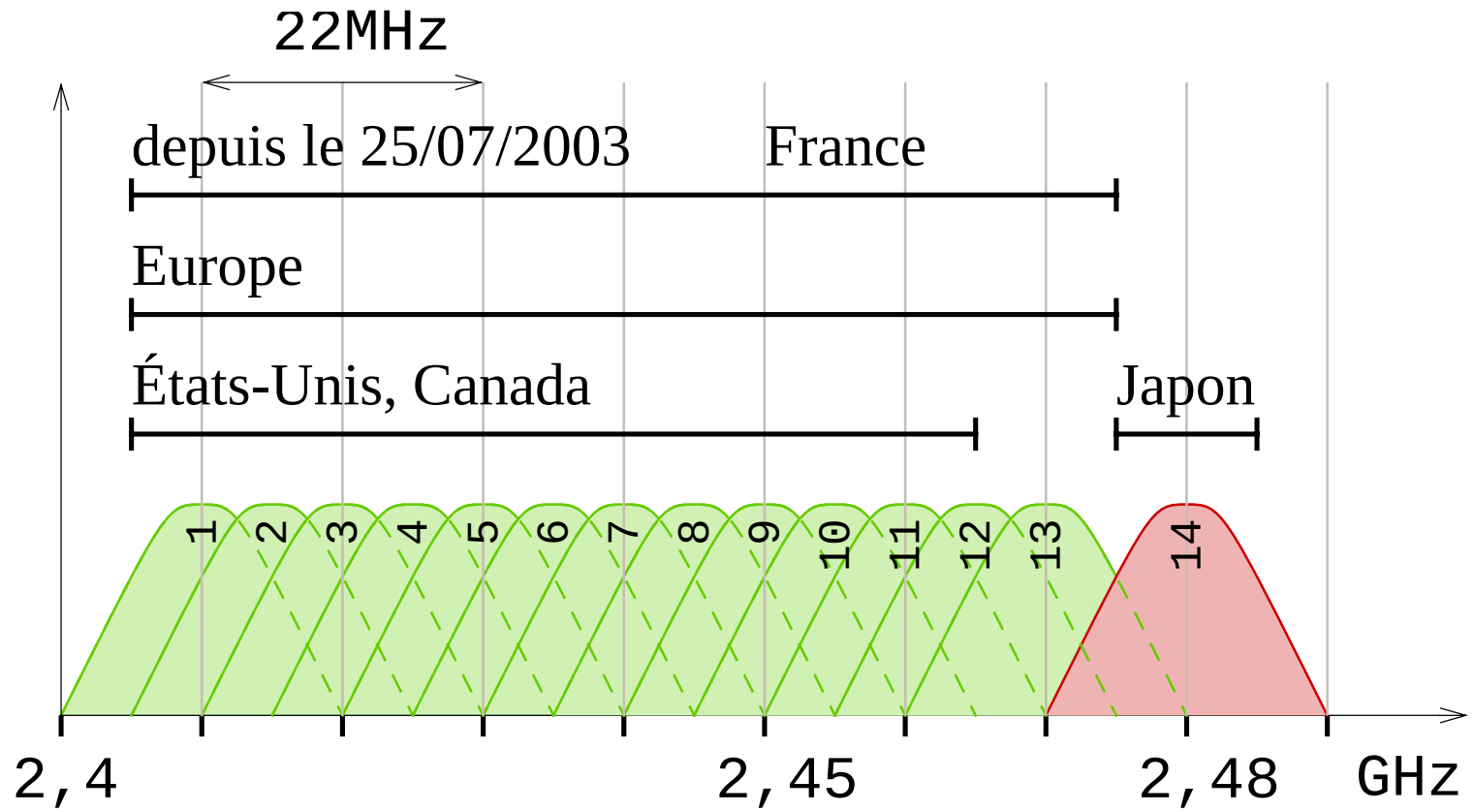
Standards spécifiant les méthodes d'accès au medium physique permettant la construction de liaison.

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

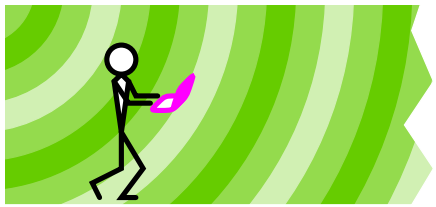
Utilisation du medium : DSSS.
14 canaux, 11 sont utilisables aux U.S.A., 13 en France : [1 ; 13].

Méthode d'accès : CSMA/CA.

802.11b : canaux



Bande ISM (Industrial, Scientific, and Medical).



Connexion

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

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

Pour les PDA, seule interface.

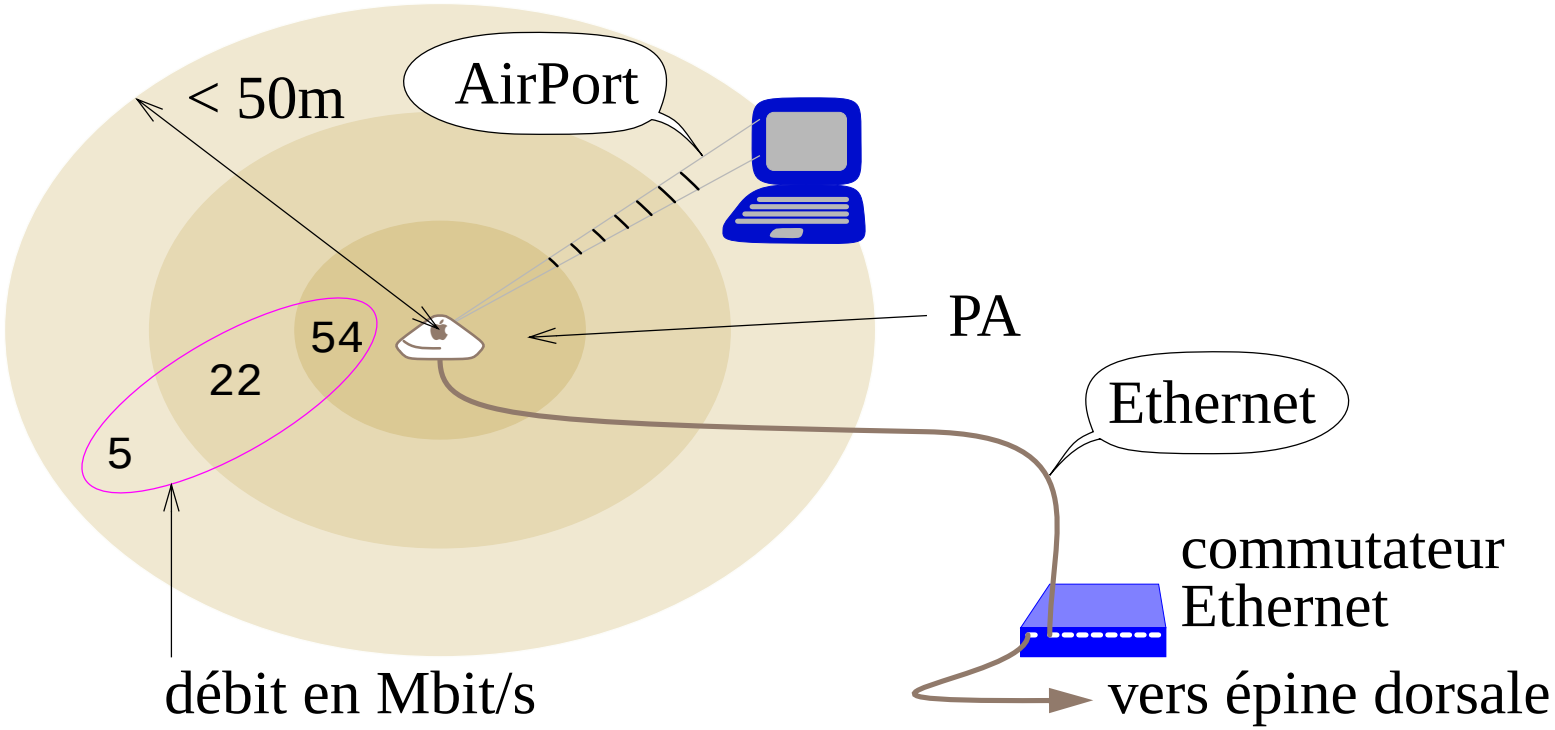
Visibilité radio ⇒ établissement d'une liaison.

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

Éloignement, obstacle ⇒ perte de la liaison.

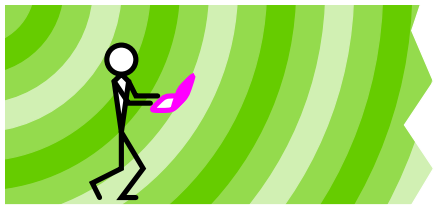
Techniques d'utilisation d'une bande de fréquence venant des techniques modem : QAM64, OFDM.

Point d'accès



Une liaison sans fil ⇒ 2 cartes AirPort !

Raccordement au reste du réseau ⇒ liaison Ethernet.



Débits

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

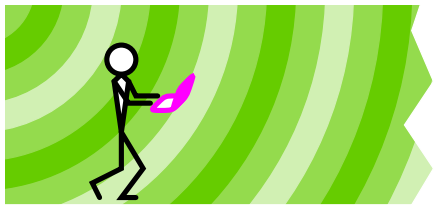
Débit en ftp binaire ≈ 50 % débit en bit/s.

Méthode d'accès CSMA/CA ⇒ débit divisé par :

- le partage du medium,
- la diffusion,
- les erreurs.

Pourquoi CA et pas CD (comme Ethernet) ?
Car les collisions peuvent être cachées.

1 PA de réseau sans fil est un répéteur ⇒ débit monopolisé par le plus lent (dénis de service).



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).

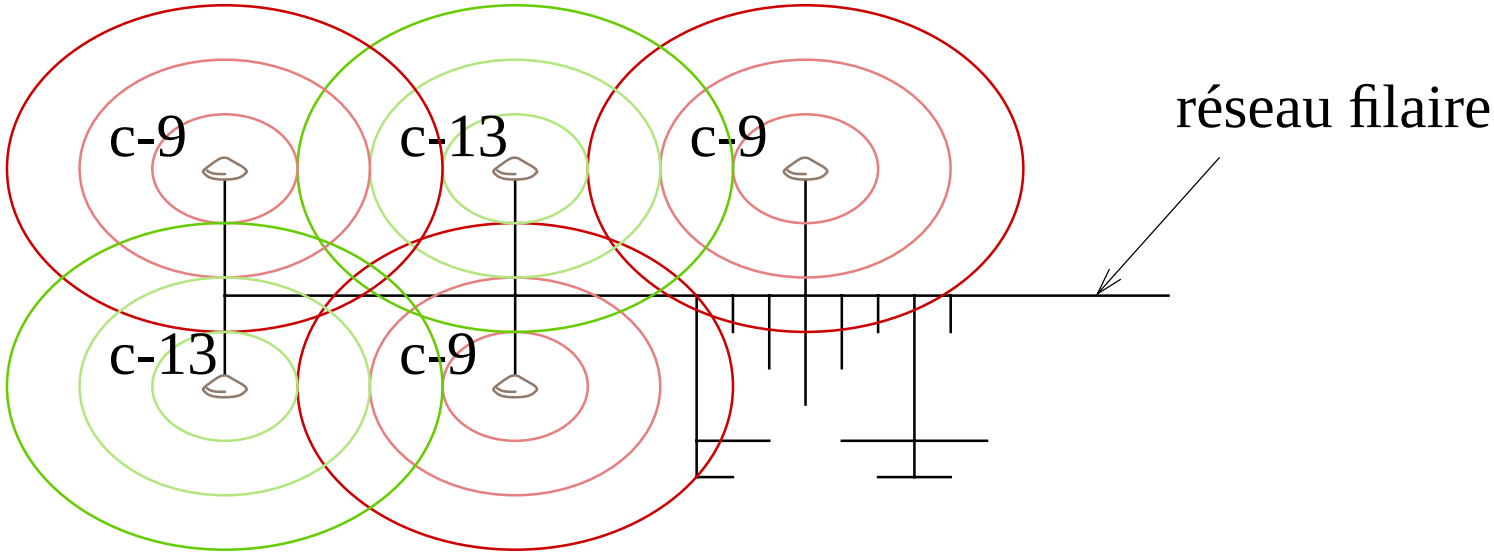
Réseau d'infrastructure : même nom de réseau (SSID), plusieurs PA (points d'accès), canaux distincts
→ accès / grand espace & nombreux utilisateurs
⇒ mobilité.

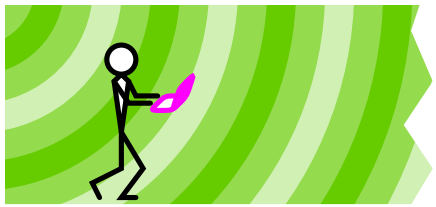
Mobilité

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 (p. 27).





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.

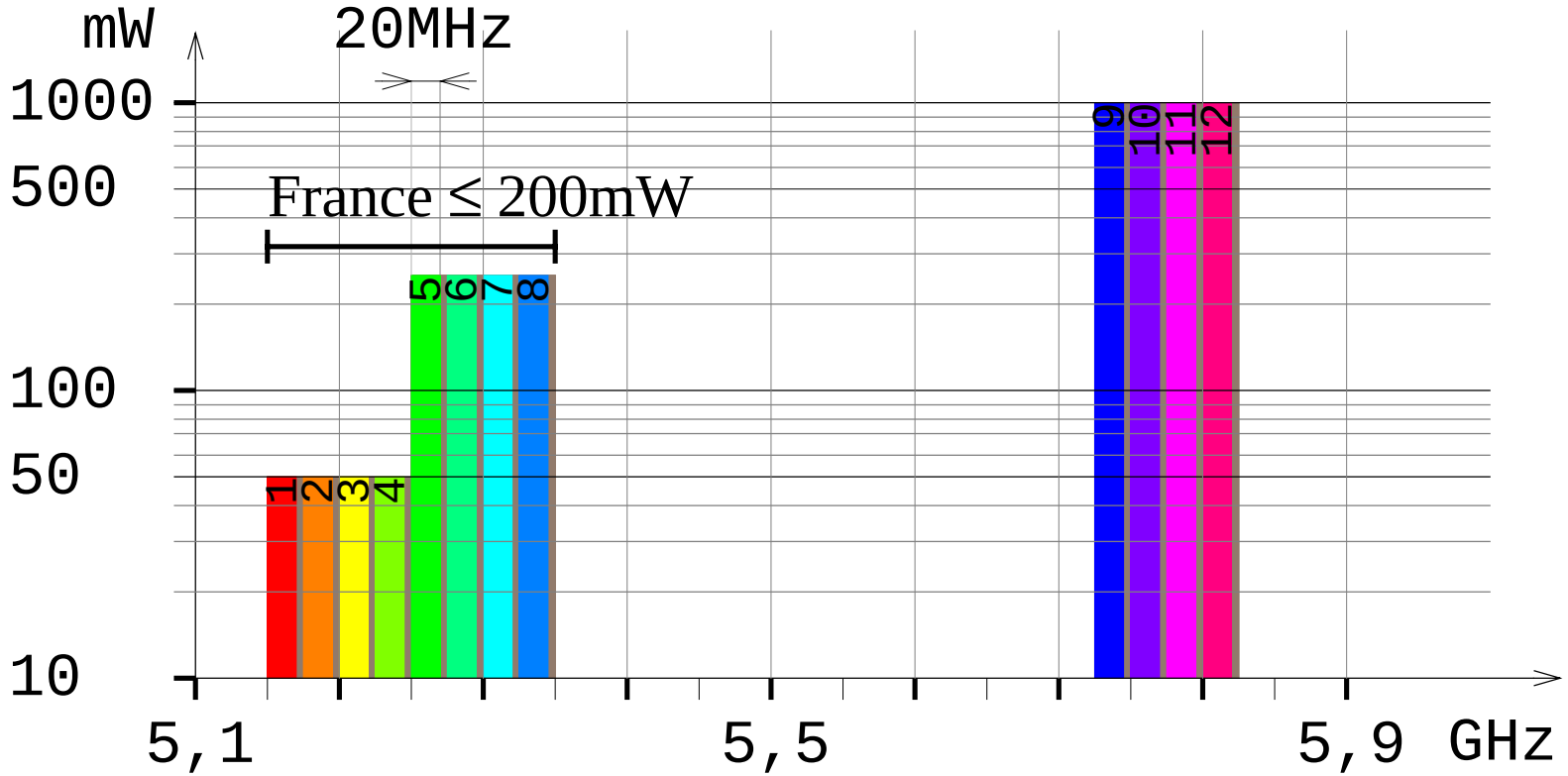
Technique de modulation :

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

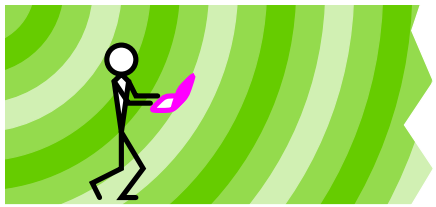
Débit : **6 → 54 Mbit/s**.

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 ($\Rightarrow n_{PA} \times 2$ sur une dimension !) ;

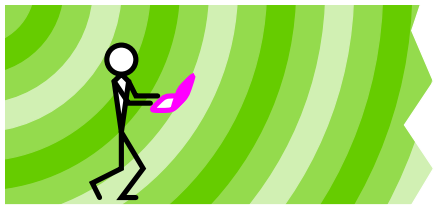
⇒ puissance rayonnée + élevée.

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 :

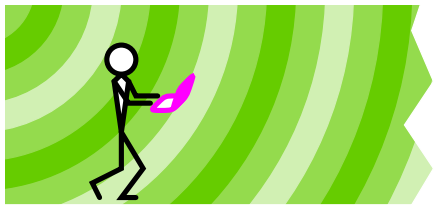
- CCK ;
- OFDM ;
- en option CCK/OFDM ou bien PBCC.

Débit : **1 → 54 Mbit/s**.

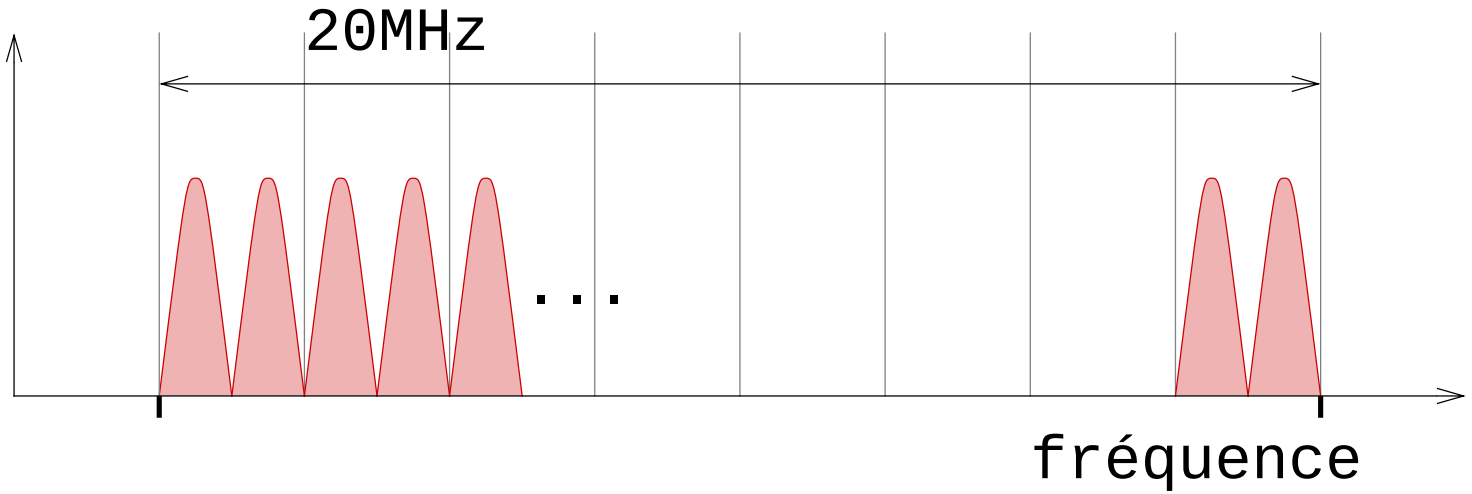
Méthode d'accès : CSMA/CA.

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 : $f = n \times 312{,}5$ 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 ou 802.11g ?

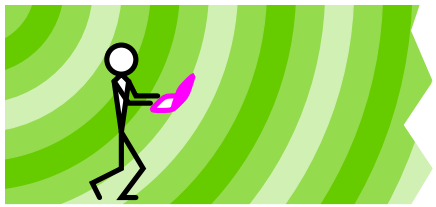
Les utilisateurs qui tirent le sans-fil sont les utilisateurs nomades
⇒ besoin de compatibilité : canaux identiques dans le monde,
⇒ 802.11g !

En réseau d'entreprise :

802.11a → $n_{PA} \times 8$ ☹ !

802.11b → d < 5 Mbit/s
⇒ 802.11g !

⇒ 802.11g !



Wi-Fi

Wi-Fi ou Wireless Fidelity = fidélité sans-fil

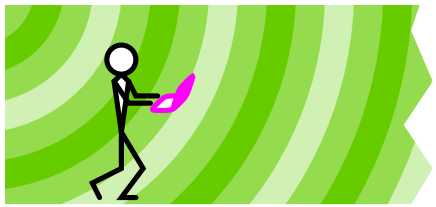
terme commercial défini par la WECA :
Wireless Ethernet Compatibility Alliance
qui

> « a pour objectif de promouvoir l'usage de WLAN basés sur le standard IEEE 802.11 ».

Elle n'a fait que ce label de certification
⇒ Wi-Fi Alliance.

Wi-Fi n'est ni un protocole réseau, ni un standard réseau, ni une technique de réseau, ni une architecture de réseau,

c'est juste… une marque déposée .



Réglementation

L'ARCEP (Autorité de Régulation des Communications Électroniques et des Postes ex. ART) définit les limites d'utilisation des fréquences pour des RLAN :

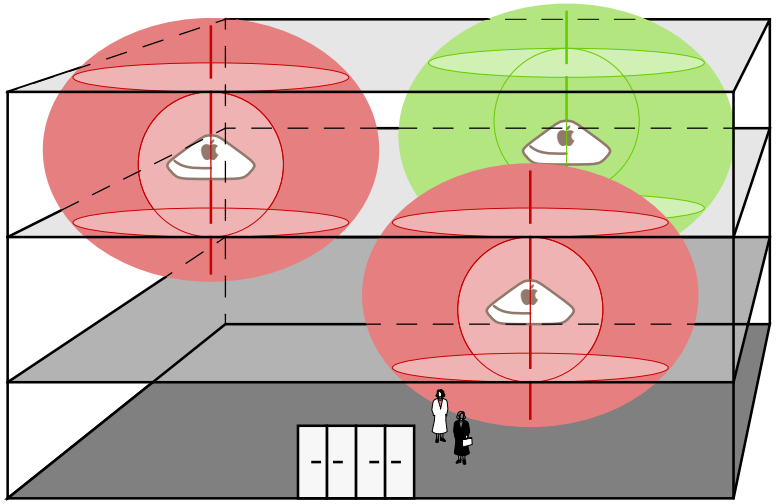
arrêté du 25/07/2003 :
http://www.arcep.fr/↵
dossiers/rlan/menu-gal.htm

- 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) !

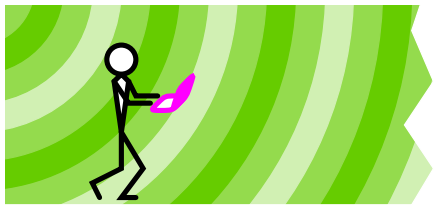
[2400 - 2483,5] MHz libre partout (en Europe) → 01/2011 ?

Déploiement



Contraintes à respecter :

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



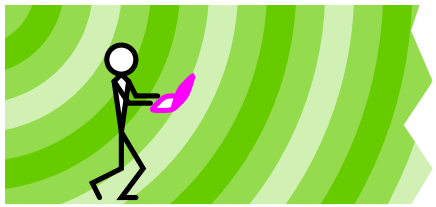
Où déployer ?

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 ≠ 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

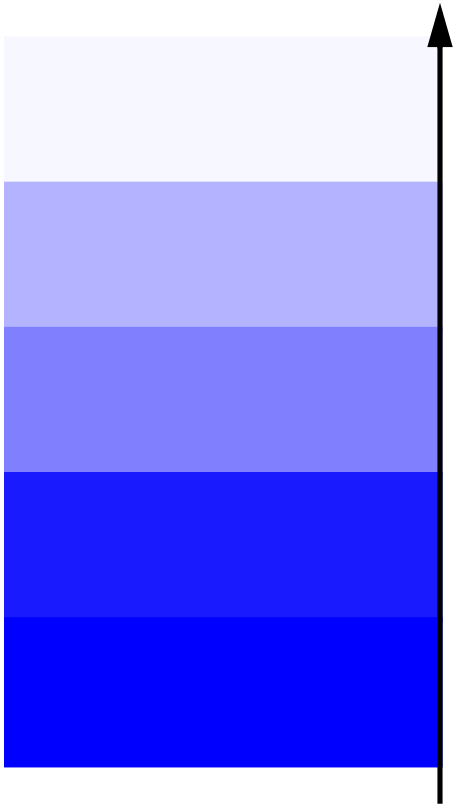
Une onde électro-magnétique se propage en ligne droite, à vitesse $c \approx 3 \times 10^8 m/s$ dans le vide. Dans tout autre milieu, elle peut être :

- 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.

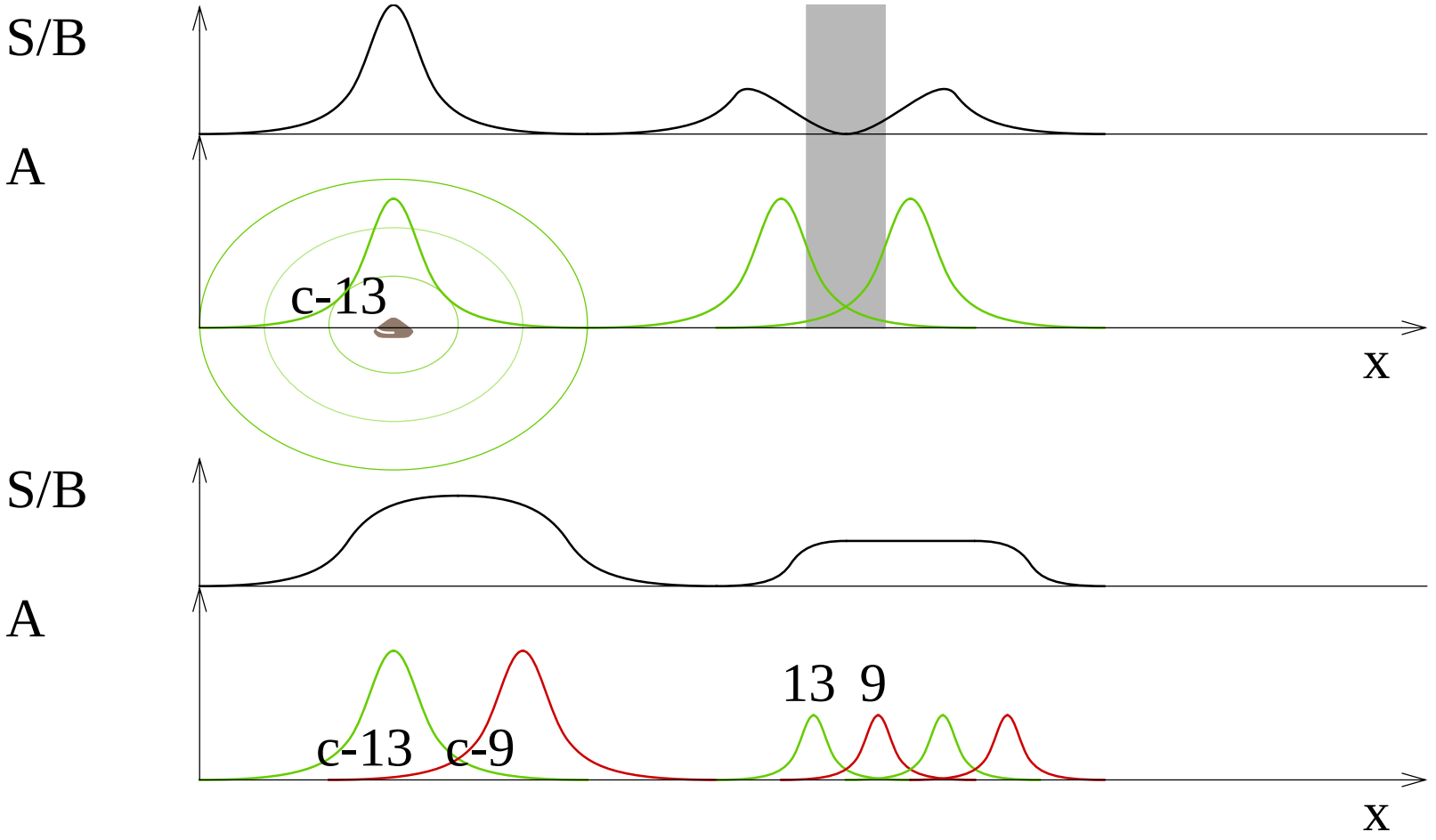
Elle interfère avec toute autre onde de fréquence proche
$\rightarrow$ battement spatial & temporel.

Transparence

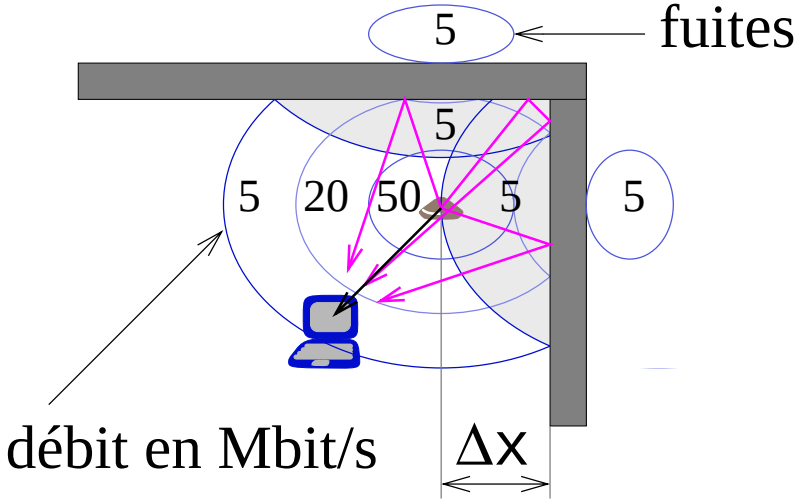


air
bois
air humide
plastique, verre
eau, végétation
animaux, nous :
cloisons en plâtre, brique
béton
verre blindé
métal conducteur

Interférences



Interférences

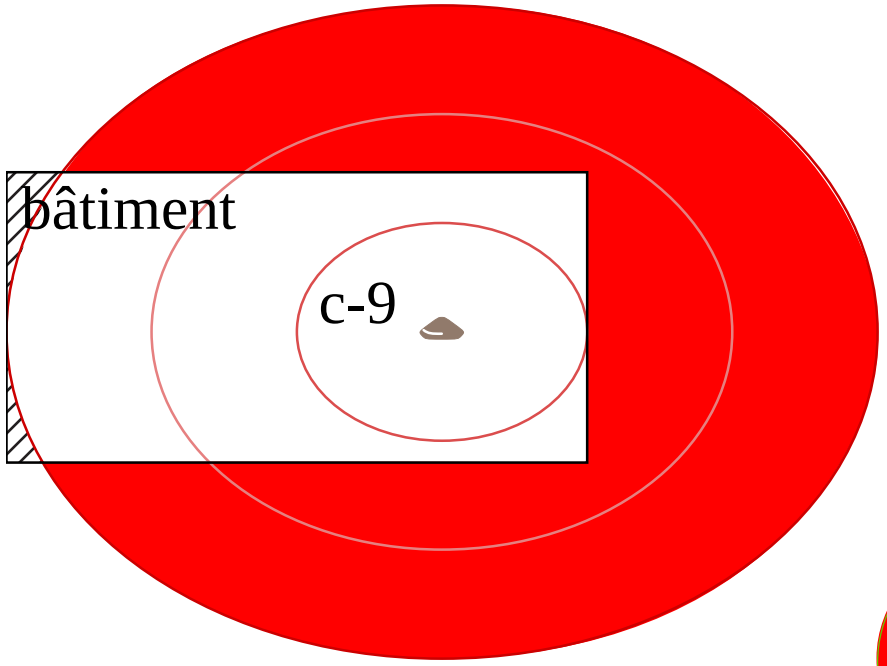


Plus la distance à un obstacle ± transparent est petite,
plus la zone d'interférence est grande,
plus la zone de diffraction est grande et difforme.

Problématique d'éclairage.

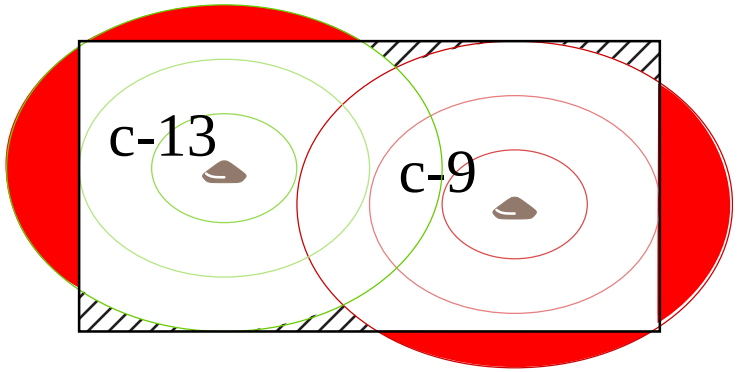
Couverture

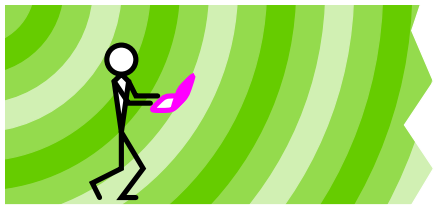
60 mW



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.
$\Rightarrow$ placement précis, et sensibilité aux réfractions.

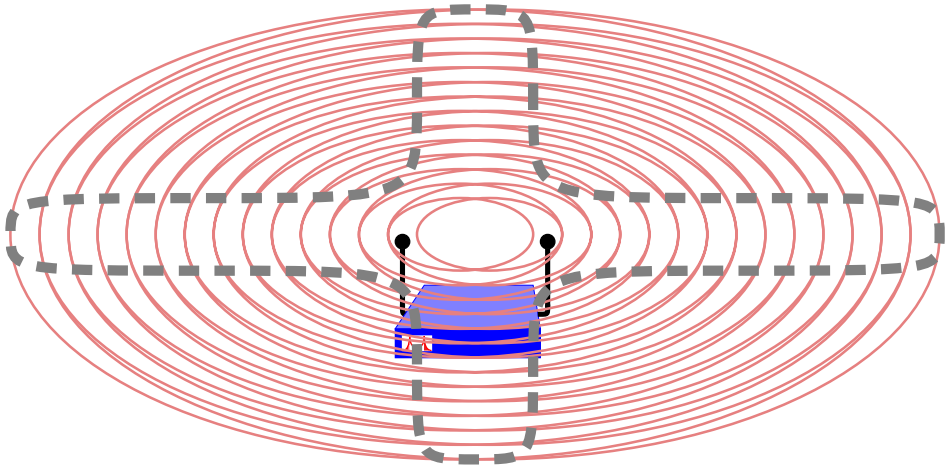
Analogie :

éclairer un auditorium avec des projecteurs de scène ☹ !

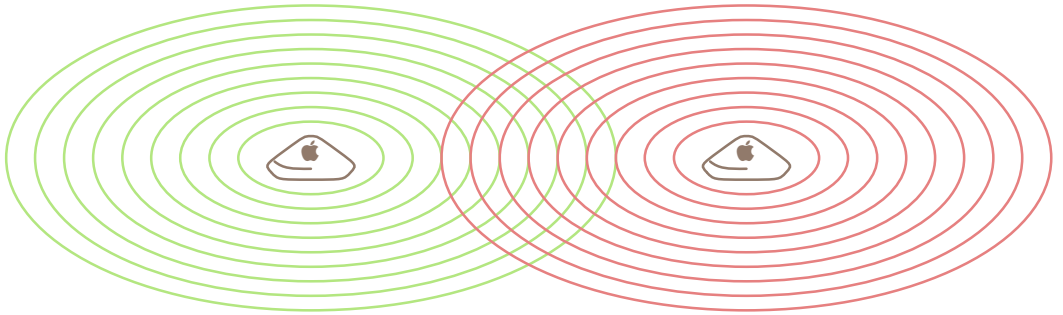
Fait vendre plus d'antennes et les services d'un installateur ☹ !

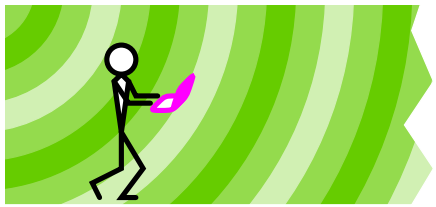
Antennes

antennes multiples orientables



PA multiples





Intégration dans l'ordinateur

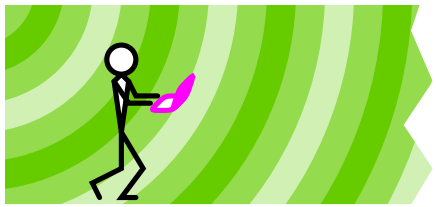
Les solutions à base de carte PCMCIA ou de carte externe sur port USB sont médiocres ☹ : la sensibilité maximale d'une antenne dipôle replié $\lambda/4$ est dans le plan orthogonal à son axe.

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

Ils ont aussi intégré une antenne dans les ordinateurs fixes,
beaucoup mieux qu'une antenne externe
collée à la paroi métallique arrière.

L'intégration dans les S.E. est très liée à une fonction rendue vitale par le nomadisme :

commutation de réseau et d'environnement.



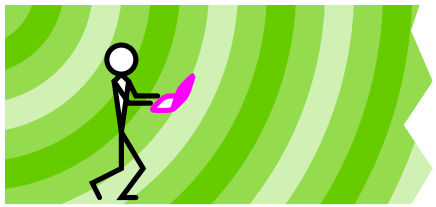
Inadéquation des batteries

Une connexion réseau sans fil continue consomme de l'énergie.
Suivant les constructeurs, et la gestion de la batterie,
autonomie : 1 h à 5 h.

Course à la fréquence :  !

Intel a du revoir à la baisse sa frénésie de GHz :
→ réduction du risque de fonte du cœur de processeur ;
→ utilisabilité décente d'un portable en réseau sans fil.

⇒ unité de gestion de l'énergie (PMU) !



Configuration client

Objectifs : contrôle d'accès & impact minimum sur le parc.

Chaque utilisateur souhaitant connecter un ordinateur à nos réseaux doit :

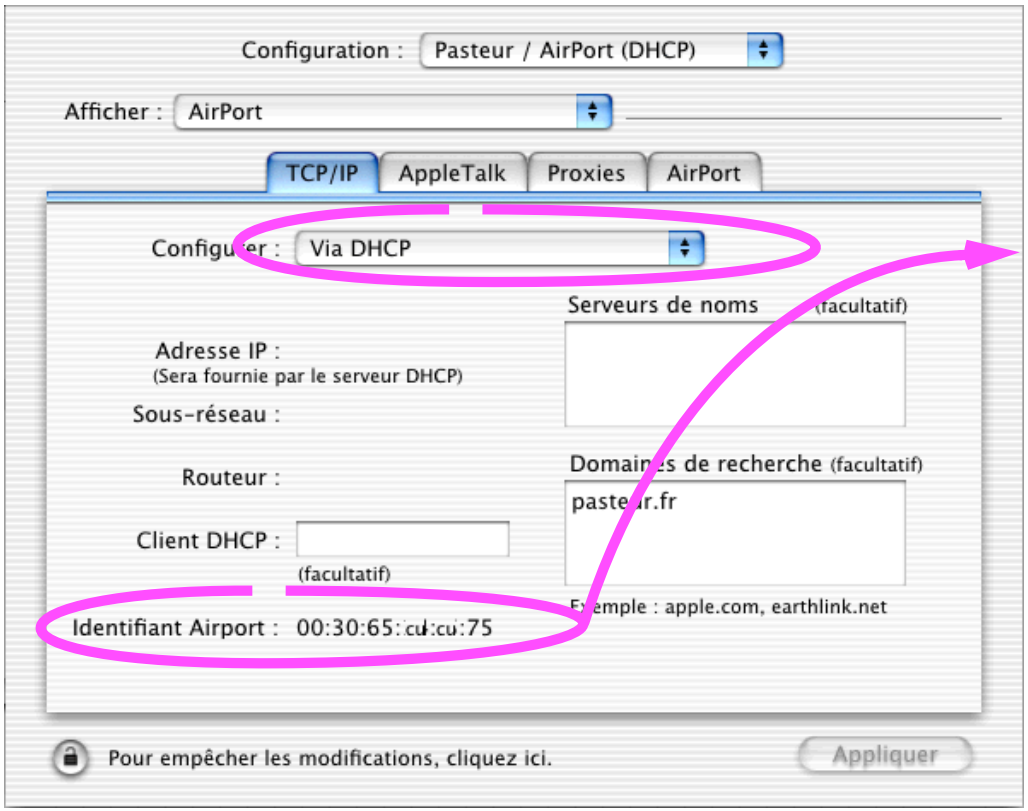
- nous communiquer l'adresse MAC (Ethernet ou AirPort) ;
- configurer TCP/IP via DHCP.

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

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

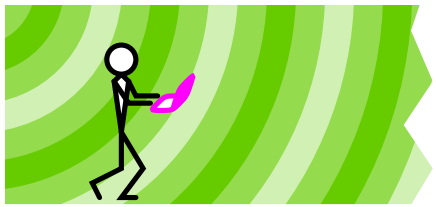
⇒ Aucun état local à gérer.

Configuration client / MacOS X



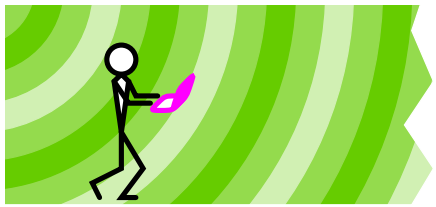
Adresse physique = adresse Ethernet.

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 (p. 43) 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)

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

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

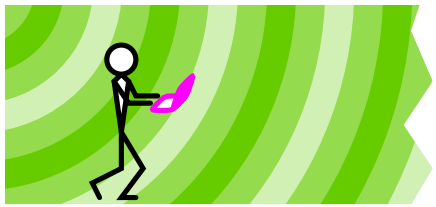
$$n_{PA}(u) = \left\lceil \frac{u_{max}}{10} \right\rceil = 5$$

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

Contrôle d'accès : 0

confidentialité : 0

$\Rightarrow$ confinement en **extranet** (p. 50) !



Classes d'usage

Labo :

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

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

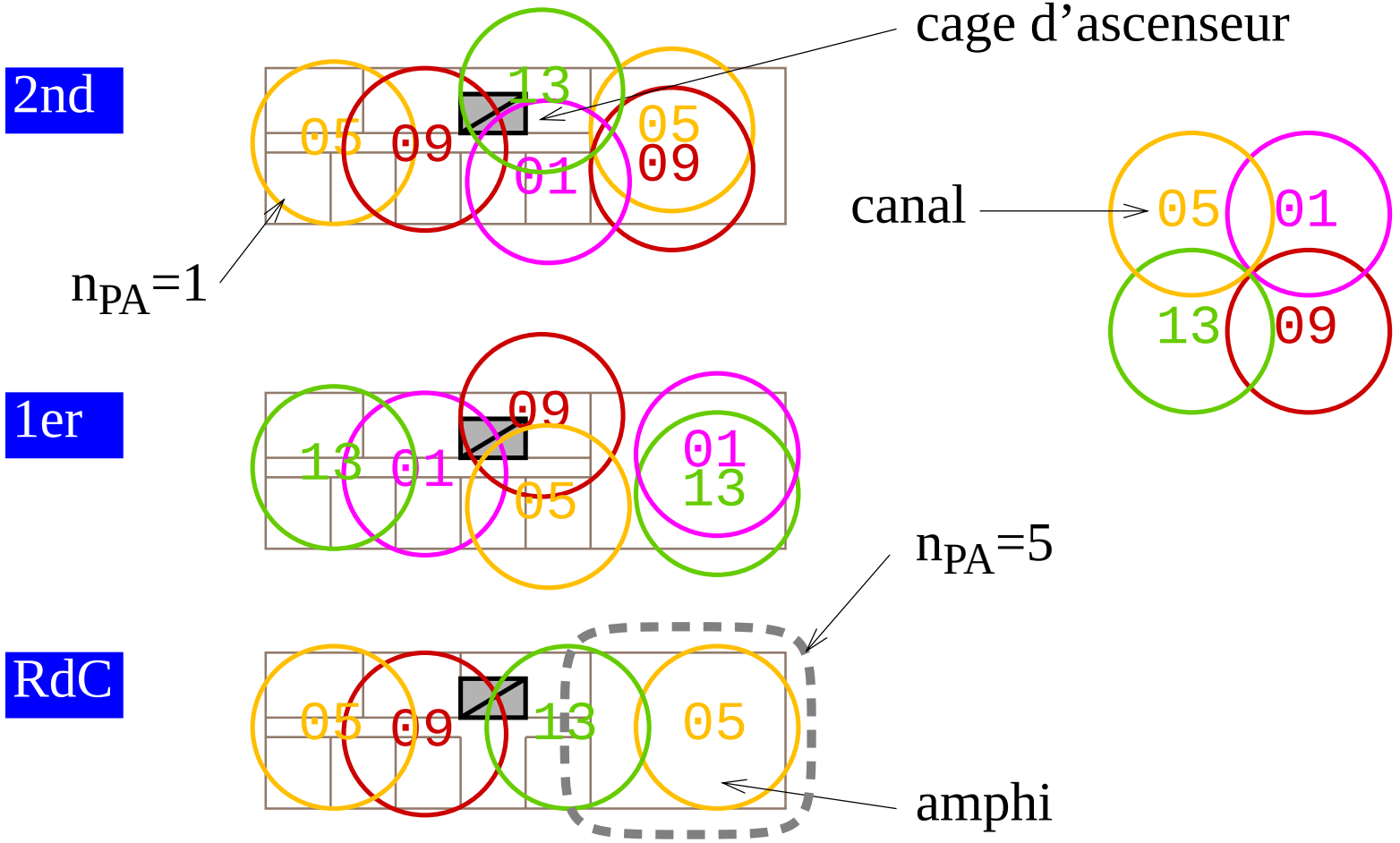
$$n_{PA}(d) = \left\lceil \frac{d_{max}}{20 \text{ Mbit/s}} \right\rceil = 1$$

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

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

Contrôle d'accès : MAC, 802.1X (p. 60)
confidentialité : 0
$\Rightarrow$ chiffrement de bout en bout !

Plan des fréquences



Réglage des PA

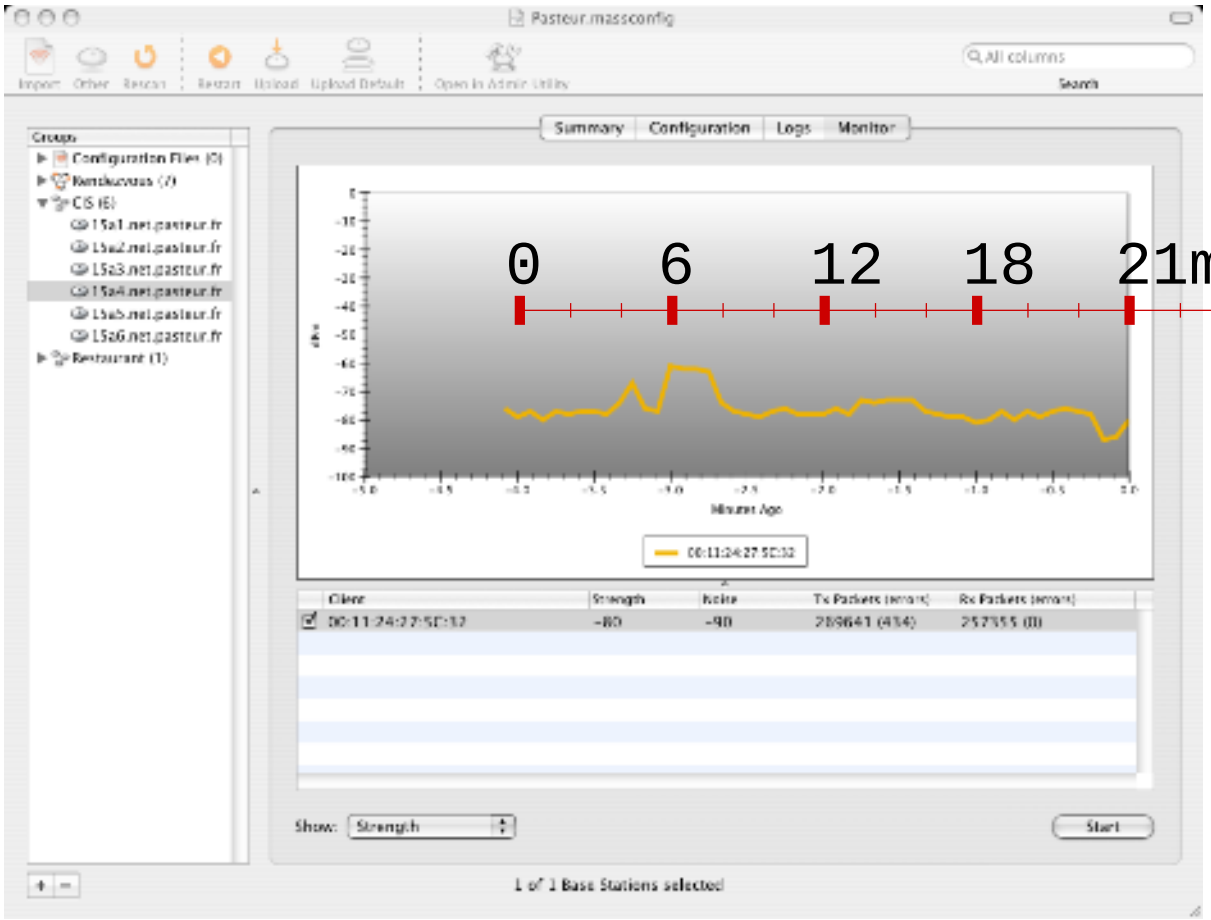
Placement : 1 ou 2 clients en position limite, mesure.

initial (densité faible)
→ 1/2 j ;

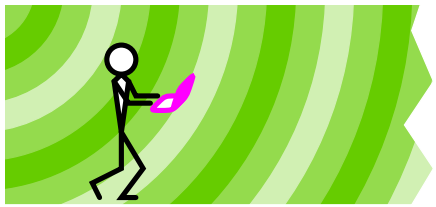
densité élevée
→ 1 j.

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

Réglage des PA



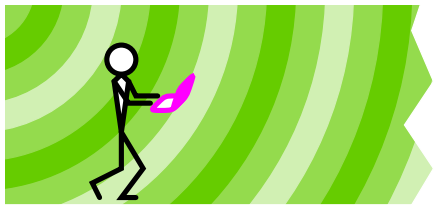
1 m / 10 s
→ mesure spatiale



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.



802.3af

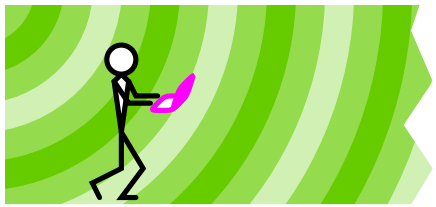
Installation d'1 PA ⇒ prise secteur
⇒ temps, coût.

Standard 802.3af (2003) : comment transporter l'alimentation électrique sur un câblage Ethernet.

L < 100 m, V ≤ **48 V** ([36, 57]), I < 400 mA, P < **12,95 W**
utilisation des paires 1-2, 3-6 ou bien 4-5, 7-8,
compatible 10, 100baseT, et alternative A : 1000baseT.

2 techniques de mise en œuvre :

- directement depuis le commutateur réseau ;
- depuis un injecteur prenant en entrée un câble Ethernet standard, et sortant sur un câble Ethernet avec alimentation.

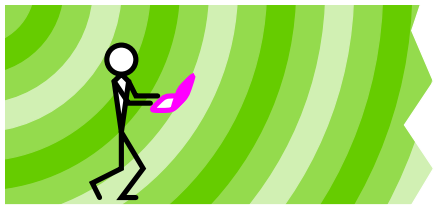


Sécurité

Pas de nouveau problème de sécurité.

Remise en exergue de problèmes connus :

- impact des rayonnements électro-magnétiques sur le vivant, sur la santé ;
- maîtrise du périmètre de sécurité de l'entreprise : **syndrome Maginot** ;
- maîtrise des accès en libre service sur un medium partagé, comme l'Ethernet partagé ;
- écoute et brouillage des communications.



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 ;

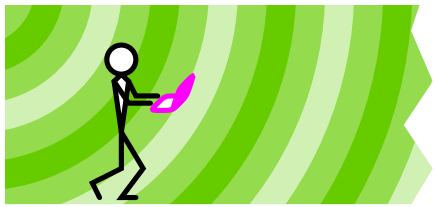
⇒ facilité de couverture de volumes complexes.

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

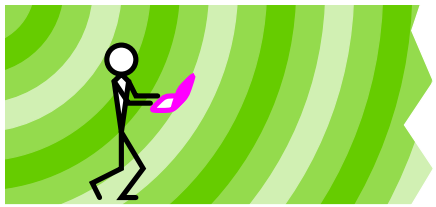
Santé publique : nombreuses études en cours, surtout au sujet de l'utilisation des téléphones mobiles (p. 85):

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 $1/r^2$ (en P).

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 ⇒ champ électro-magnétique,
⇒ sensibilité aux autres champs.

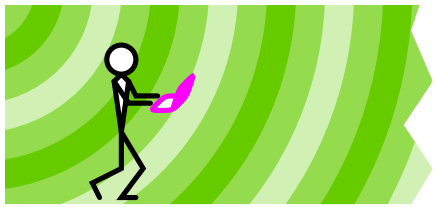
Ces transports de données (sauf fibre optique) peuvent être facilement écoutés et brouillés :

- 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 ⇒ écoute + simple que sur un réseau Ethernet : 0 prise ou plutôt prise de 50 m de rayon.

⇒ communication sur les risques ;

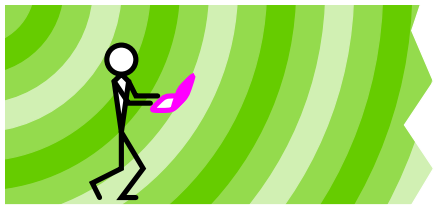
⇒ contrôle d'accès, protection des données : confidentialité.



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 (p. 34) ;
- 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 confinés à un **extranet** ;
- par 802.1X (p. 60).



WEP : un extincteur vide

WEP : Wired Equivalent Privacy.
Comment casser WEP :

http://airsnort.shmoo.com
http://www.cr0.net:8040/↵
code/network/aircrack/

Ils ont grossi artificiellement un faux problème :

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

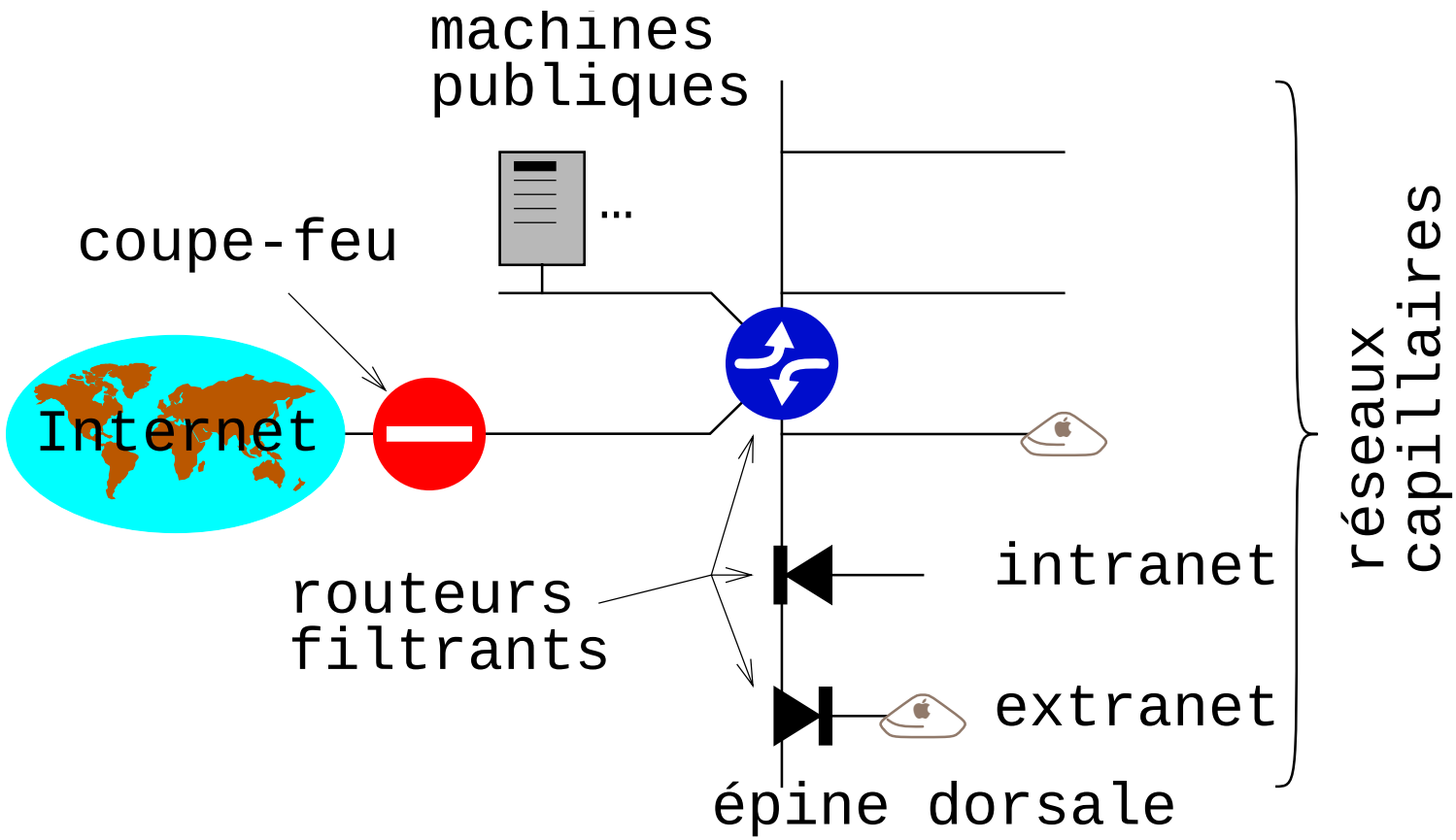
et ils ont laissé dans l'ombre un vrai problème :

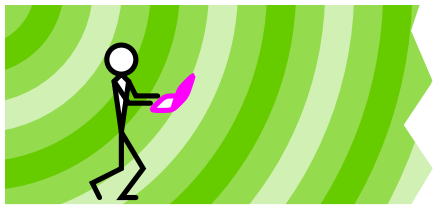
absence d'un protocole de gestion de clés sans état local.

⇒ WEP : à jeter !

Coller des rustines sur WEP pour le réutiliser : pire ☹ !

Extranet


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



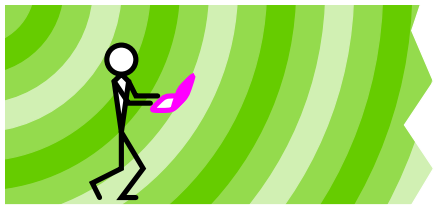
Filtrage

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.



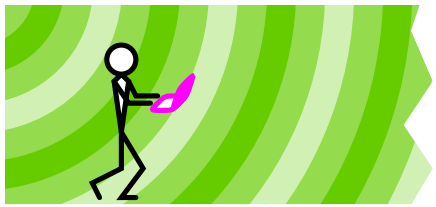
Audit

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

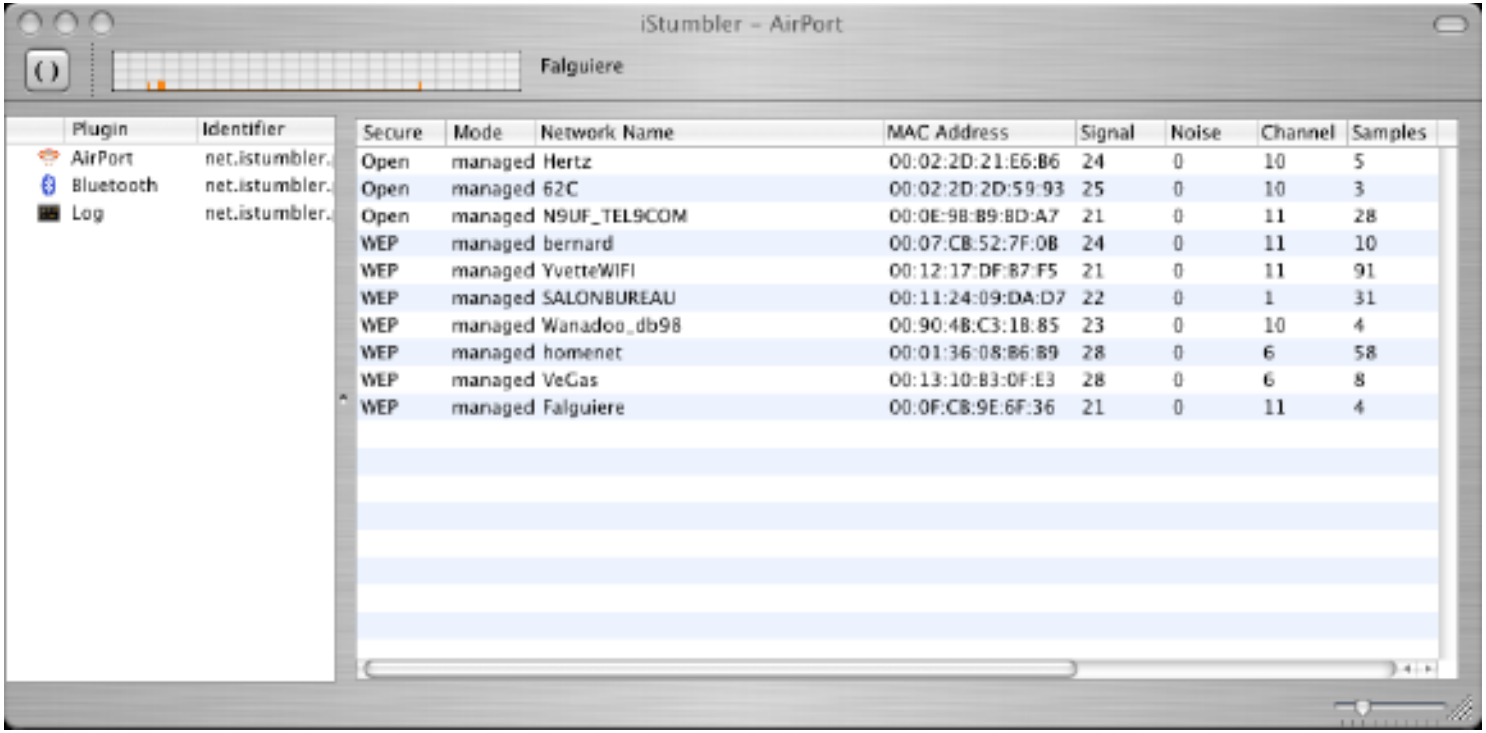
Localisation sur le terrain :

- détection de réseaux pirates internes ;
- détection de réseaux 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.

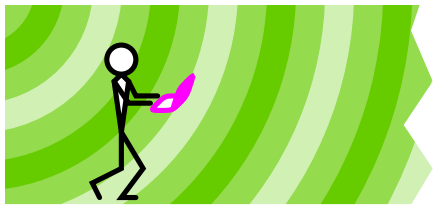
Constat pragmatique :

- écouter un réseau sans fil dans un environnement **bien couvert** ⇒ « entrer » dans la zone de couverture (p. 39).

Audit



La nature a horreur du vide !

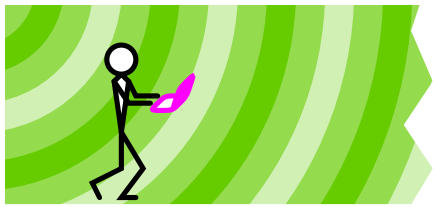


Syndrome Maginot

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 connectant un ordinateur interne au réseau de l'entreprise voisine ;



Syndrome Maginot

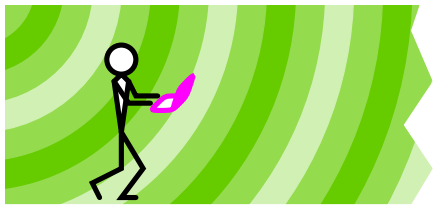
- le PC avec carte Ethernet et carte Wi-Fi allumée en permanence faisant pont entre la rue et le réseau interne ;
- le réseau sans-fil d'un résidant de l'hôtel voisin.

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 :

  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, intrusion des réseaux des voisins.

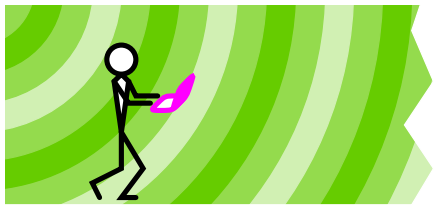


Guerrier des ondes en décapotable

La connexion d'un PC « nid-de-vers » Windows
= risque (probabilité × impact) : $\mathbf{R_{nidevers}}$.

Visite du « guerrier des ondes en décapotable »
dans le parking voisin avec une antenne d'1 m !
= risque : $\mathbf{R_{guerrier}}$.

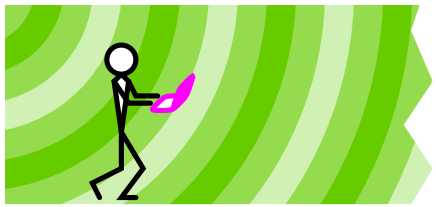
$$R_{nidevers} >> R_{guerrier}$$



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 : P.S.I., R.I., note de service.
- Plateforme d'administration des réseaux **invulnérable**
  ⇒ choix d'un S.E. fiable,
  mise en place d'ACL le protégeant au niveau
  du système et du réseau.



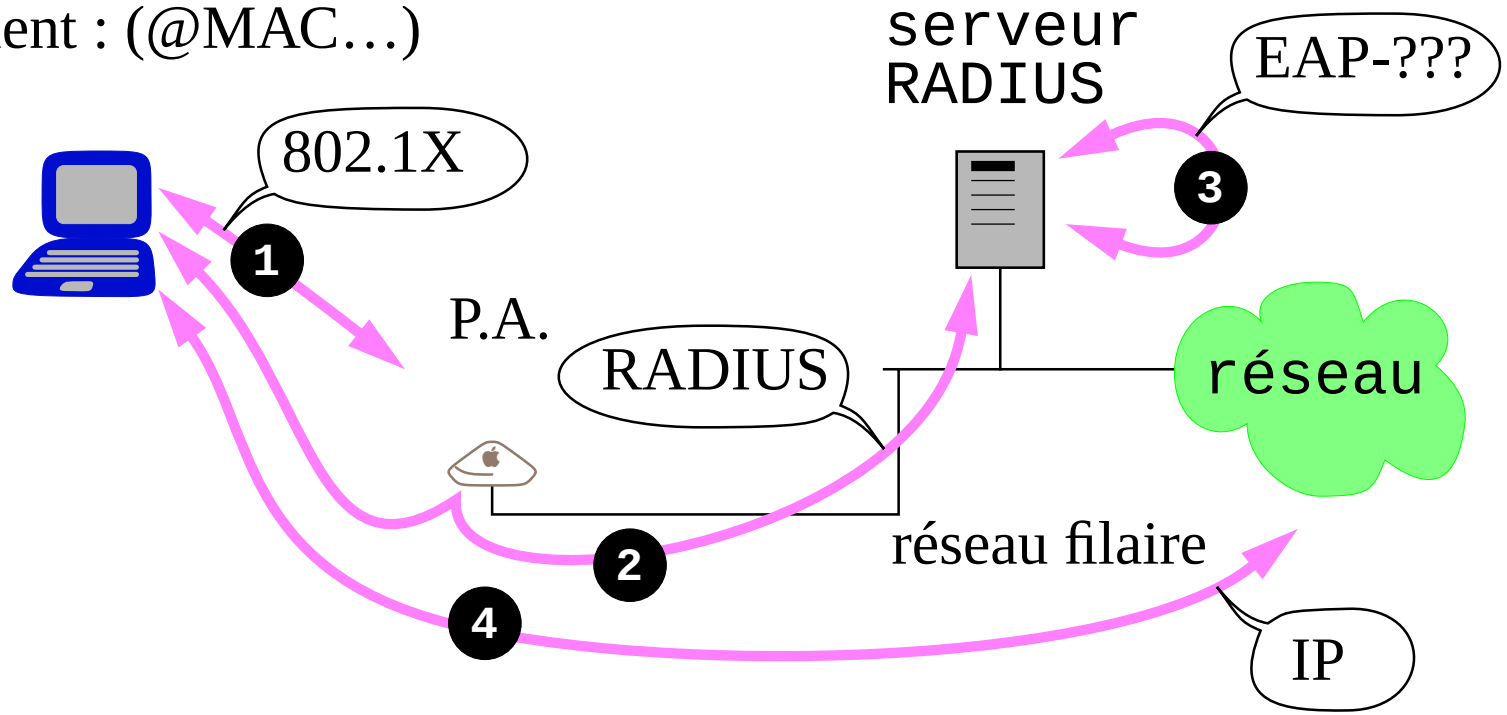
Améliorer la sécurité des réseaux

- Raccordement de n'importe quoi au réseau : répéteur sauvage, borne AirPort pirate… :
  même remède : interdits
  ⇒ communication,
  + 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).

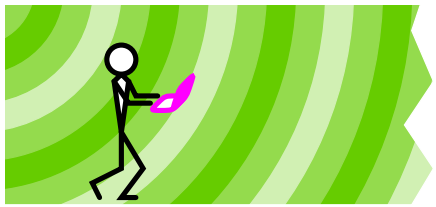
802.1X

Autorisation de l'accès au réseau :

client : (@MAC…)



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



802.1X

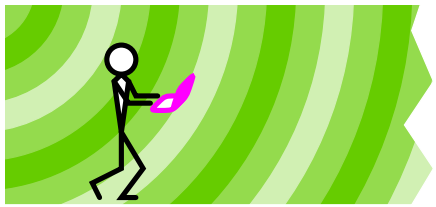
802.1X ne peut suffire à identifier, ni à authentifier un ordinateur ou un utilisateur

⇒ appel à un serveur d'accès, typiquement un serveur RADIUS.

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

802.1X est stérile si il peut être écouté et rejoué

⇒ utilisation d'un protocole de chiffrement et de gestion de clés.



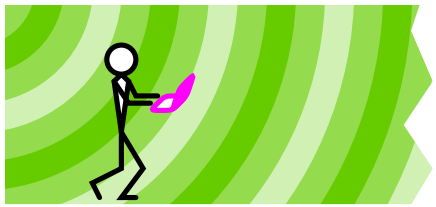
802.11i

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.

Ethertype = **0x88C7**.



802.11i

Versions de la Wi-Fi Alliance :

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

utiliser WEP : mauvais départ ?

WPA est vulnérable et offre des modes d'utilisations très dégradés, encore un extincteur vide :
http://wifinetnews.com↵
archives/002453.html

WPA2 = Wi-Fi Protected Access y compris pour un réseau multi-point,
basé sur TKIP ou bien CCMP.

RADIUS : principe

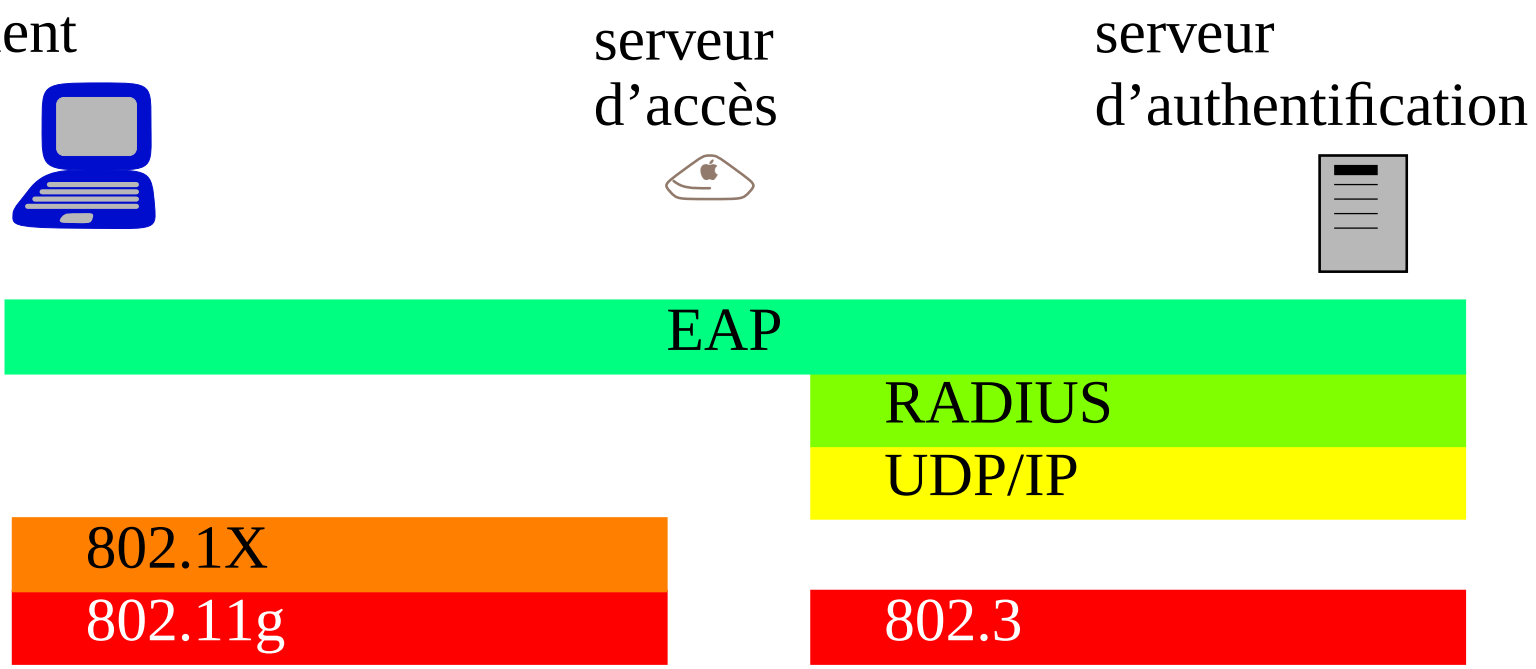
Nom	traduction	fonction
supplicant	~~pénitent~~ client	client identifié comme machine ou utilisateur
NAS = Network Access Server	serveur d'accès	ouvre l'accès réseau si accord de l'AS
AS = Authentication Server	serveur d'authentification	vérifie l'autorisation d'accès

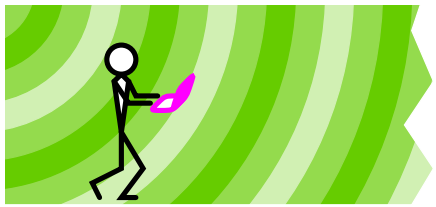
Utilise 1812/UDP = radius, 1813/UDP = radacct.
Peut aussi utiliser 1814/UDP pour des relais.

Met en œuvre le RFC ~~2865~~ 3579.

RADIUS : principe

Un serveur RADIUS va aussi mettre en œuvre EAP (p. 70), et des extensions d'authentification (sur EAP).





RADIUS : installation

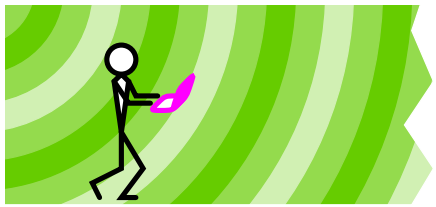
ftp://ftp.freeradius.org/pub/↵
radius/freeradius-1.0.4.tar.gz

```
$ ./configure --prefix=/local --localstatedir=/var --disable-shared
[...plein de lignes ...]
$ make
[...]
$ /usr/bin/sudo /bin/zsh
# make install
[...]
#
```

Sur FreeBSD, utilisation des portages FreeBSD :

```
# mv freeradius-1.0.4.tar.gz /usr/ports/distfiles
# chown root:wheel /usr/ports/distfiles/freeradius-1.0.4.tar.gz
# cd /usr/ports/net/freeradius
# make PREFIX=/local ; make install PREFIX=/local
[...]
#
```

⇒ ça marche !

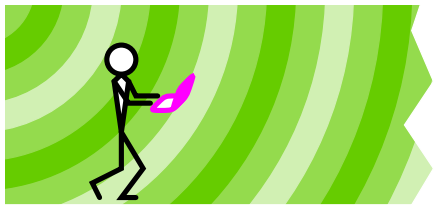


RADIUS : configuration

Tests :

```
# vi /local/etc/raddb/clients.conf
client 127.0.0.1 {
    secret = testing123
    shortname = localhost
    nastype = other
}
# radiusd -X
[...]
$ radtest test_user test_pass localhost 0 testing123
Sending Access-Request of id 100 to 127.0.0.1:1812
        User-Name = "test_user"
        User-Password = "test_pass"
        NAS-IP-Address = comte.sis.pasteur.fr
        NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1:1812, id=100, length=20
$
```

⇒ ça marche !



RADIUS : configuration

Ouvrir les ACL vers le serveur :

```
access-list <n> permit udp <sous_réseau_PA> eq 1812 host <serveur> eq 1812
access-list <n> permit udp <sous_réseau_PA> eq 1813 host <serveur> eq 1813
```

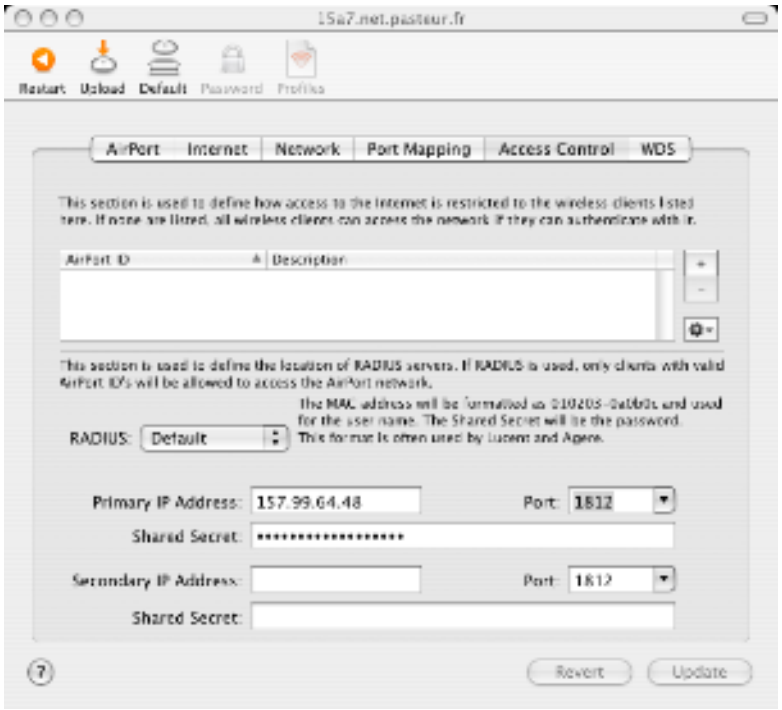
ouvrir les règles de filtrage du serveur :

```
# vi /etc/ipf.rules
pass in on sk0 proto udp from <sous_réseau_PA> to any port = radius \
keep state keep frags
pass in on sk0 proto udp from <sous_réseau_PA> to any port = radacct \
keep state keep frags
# ipf -Fa -f /etc/ipf.rules
```

définir un nouveau serveur d'accès = client pour RADIUS :

```
# vi /local/etc/raddb/clients.conf
client 15a7.net.pasteur.fr {
        secret  = errare humanum est
        shortname = 15a7.net
        nastype = other
}
```

RADIUS : configuration

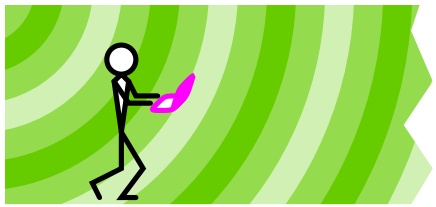


Configurer ce client pour faire du contrôle d'accès basé sur RADIUS.

définir un nouvel utilisateur identifié par son adresse MAC :

```
# vi /local/etc/raddb/users
001124-275c32 Auth-Type := Local, User-Password == "errare humanum est"
```

⇒ ça marche !



EAP

Extensible Authentication Protocol : RFC 3748,

= protocole de construction d'une méthode d'authentification,

≠ protocole d'authentification.

Conçu pour utiliser le niveau liaison (PPP, IEEE 802).

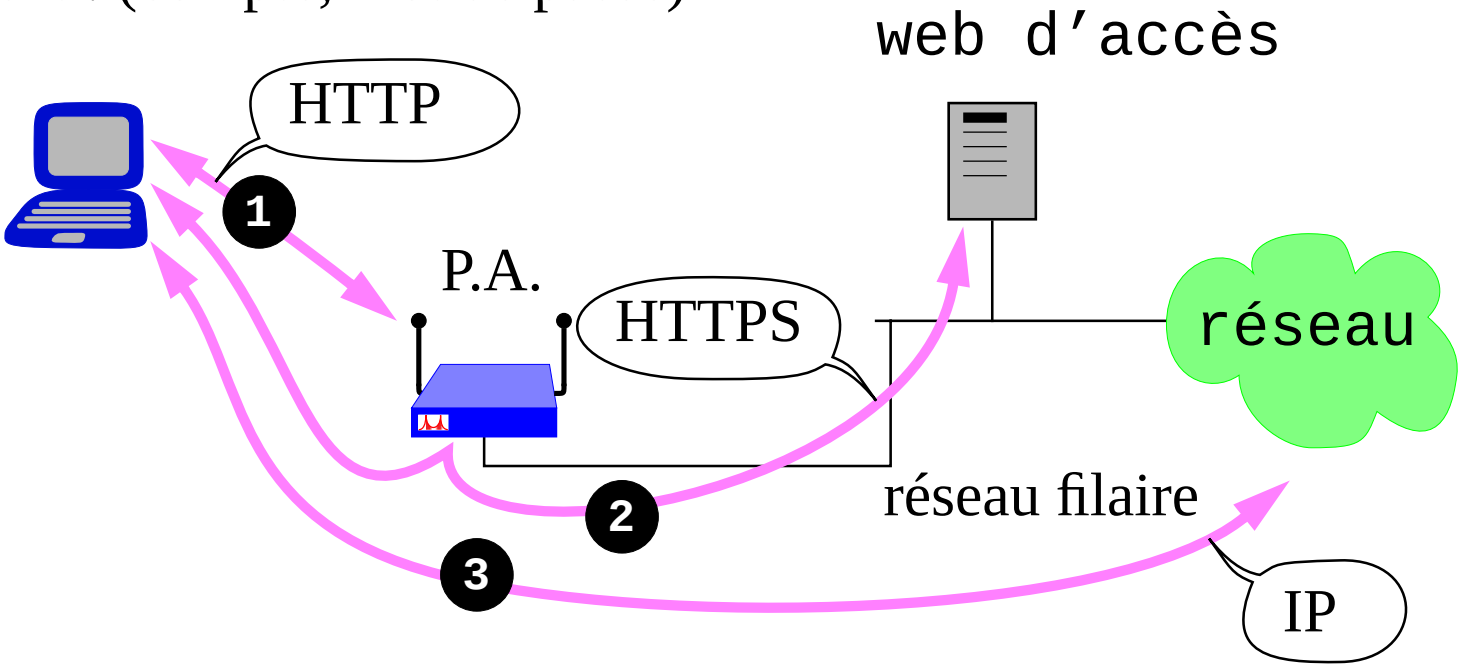
2 protocoles mettent en œuvre EAP :

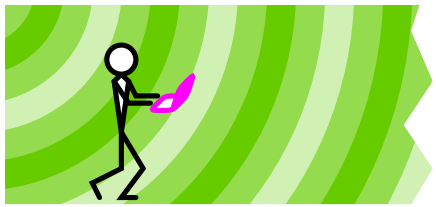
- RADIUS : RFC 3579, http://www.freeradius.org/ ;
- Diameter : RFC 4072, http://www.opendiameter.org/ .

Portail web d'accès

En mauvais anglais : « captive portal ».
Fonctionnement : redirection du trafic HTTP vers un serveur web dédié à l'autorisation d'accès.

client : (compte, mot de passe)





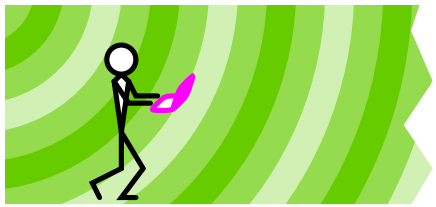
Portail web d'accès

Réalisation au moyen de matériel :
PA, routeurs ou serveurs d'accès,
+ serveur web qui peut être embarqué (⇒ PA lourd).

Versions à base de logiciel libre :

NoCatAuth :	http://nocat.net,
talweg :	http://sourcesup.cru.fr/talweg/,
m0n0wall :	http://m0n0.ch/wall/

Avantage :	pas de logiciel client ;
inconvénient :	tout dans le navigateur web, IP → HTML ?



Utilisation d'IPSEC

2 approches possibles :

- certificats utilisateurs ;
- authentificateurs utilisateurs externes.

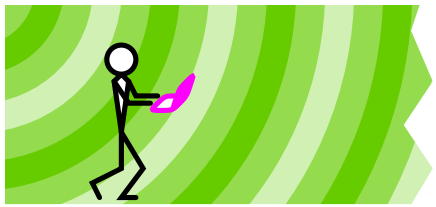
⇒ IGC ou gestion d'un parc d'authentificateurs (SecurID…).

Règle « bien » le problème de confidentialité.

Ne règle pas le problème d'accès différents au réseau sans fil (typiquement public, administratif, labo.)
en un même point.

Attention, mal utilisé IPSEC peut démolir le concept de périmètre de sécurité

⇒ parler de « **tunnel chiffré** » non de **VPN**.



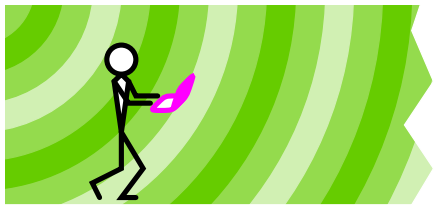
Nomadisme

Confidentialité & contrôle d'accès peuvent être obtenus dans un réseau d'infrastructure.

Le nomade peut rechercher ces 2 garanties hors de ce réseau :

- se ramener au cas du réseau d'infrastructure :
  construire un tunnel chiffré, depuis un système fiable,
  et empêchant tout autre accès du réseau local ;
- utiliser des moyens locaux :
  construire un réseau sans fil multi-point à partir d'un système fiable équipé d'un coupe-feu
  + utilisation de chiffrement applicatif.

Nous recherchons des techniques de mise en œuvre de la 1re :
simples & visibles pour l'utilisateur, tout-terrain,
et gérables à grande échelle.



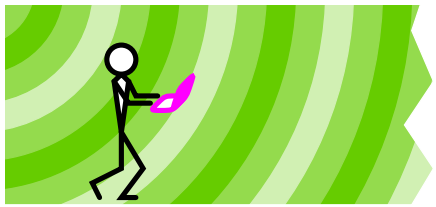
Communication

Fixer des règles d'utilisation des réseaux sans fil :

- hors du campus : interdit ;
- sur le campus : autorisé dans les zones couvertes ;
- interdiction de raccorder n'importe quoi au réseau.

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 chiffrement fiable sur un S.E. fiable !



Futur

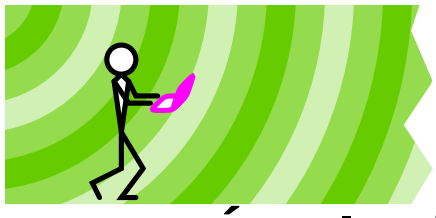
1999 : 802.11b ; label de qualité Wi-Fi ;

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 / B = 40 MHz @ 2,4 GHz,
135 Mbit/s / B = 20 MHz @ 2,4 GHz…



Évolutions

Des débits :

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

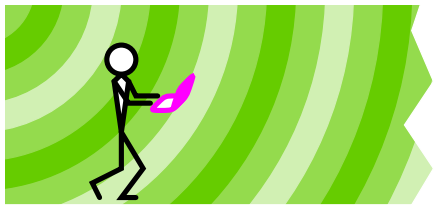
$\Rightarrow$ 20 Mhz, 20dB : 130 Mbit/s
$\Rightarrow$ 40 Mhz, 30dB : 400 Mbit/s

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

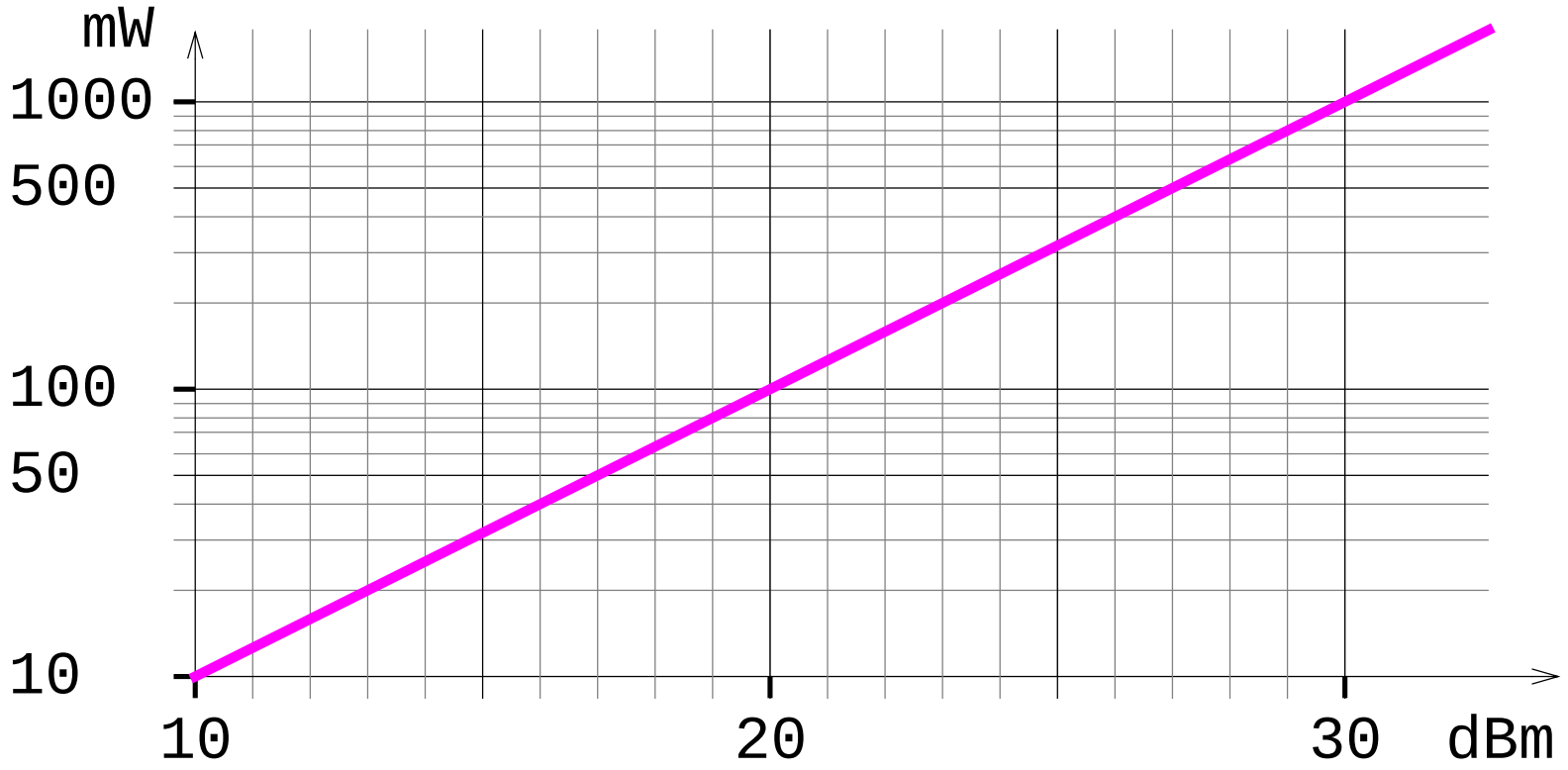
Choix techniques ayant un avenir :

- **802.11g**, **802.3af**, **802.1X** :
- éviter des techniques en retard de 4 ans (Centrino) ;
- éviter tout ce qui est basé sur WEP ;
- éviter les PA en boîtiers métalliques ;
- éviter les antennes externes ;
- éviter les protocoles propriétaires d'une complexité que seul le commercial peut certifier.

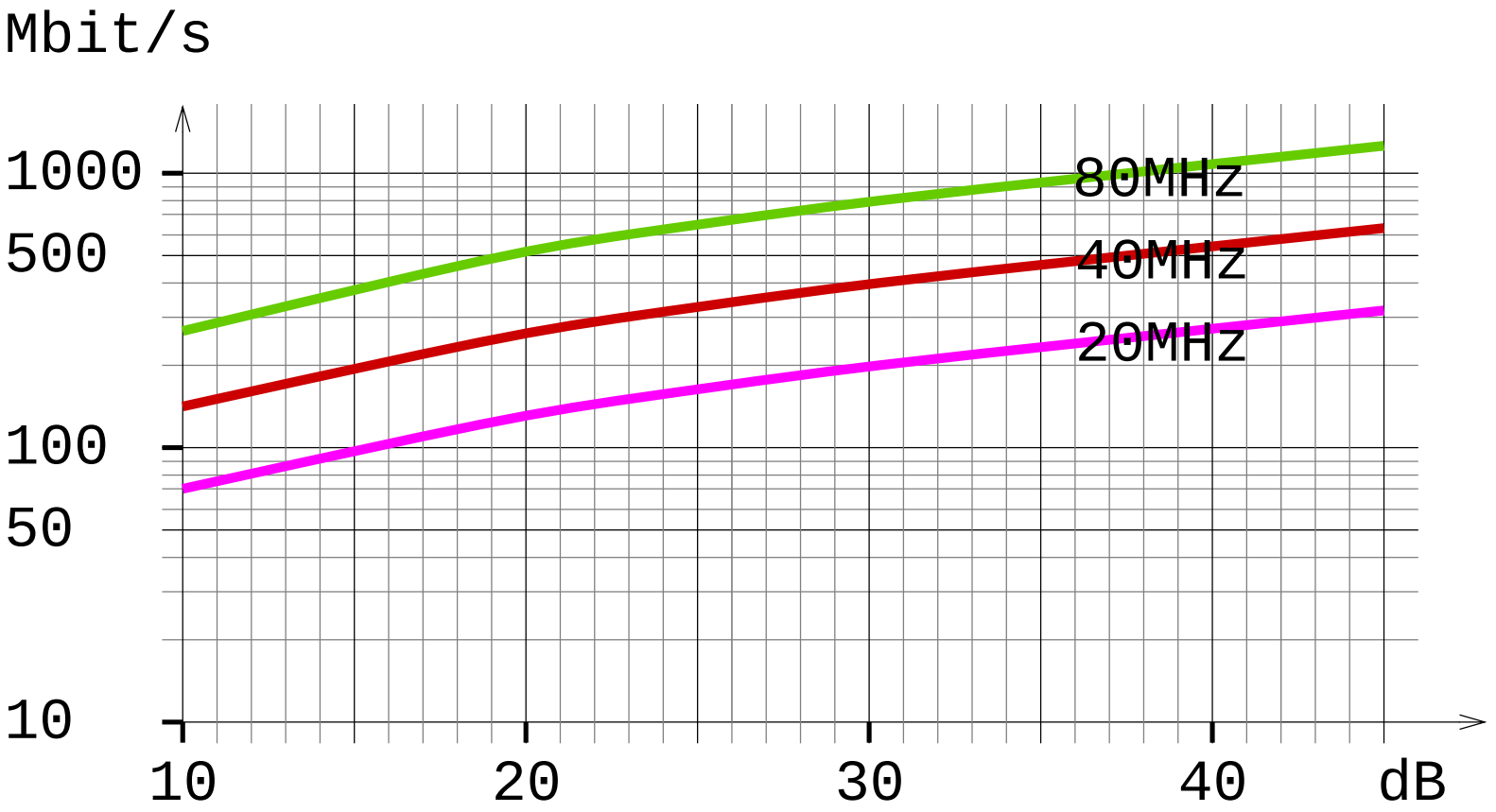
Couvrir pour éviter l'apparition de réseaux pirates internes et les conflits avec les réseaux des voisins.

Veiller à ce que la plateforme d'administration ne soit pas le point le plus faible de l'architecture.

Annexes

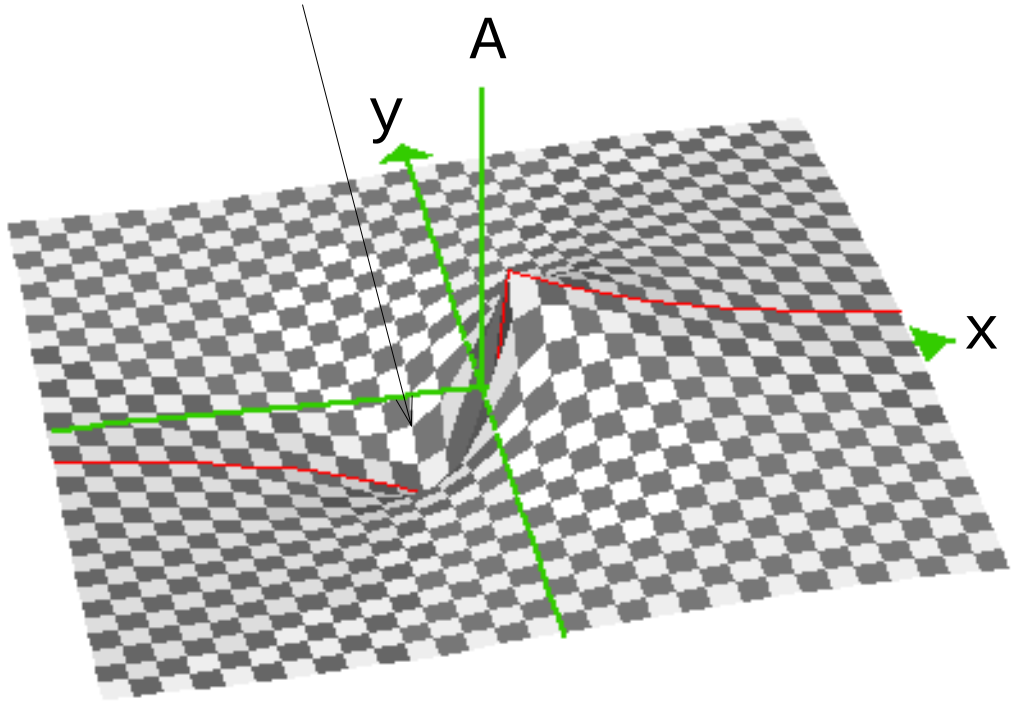


Loi de Shannon



Réflexion, absorption

onde réfléchie ⇒ atténuation



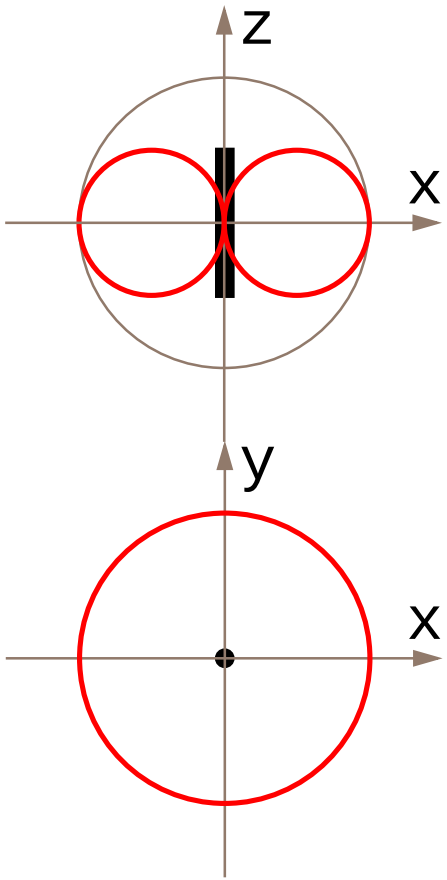
Exemple :
amplitude du signal au voisinage d'un mur en béton.

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

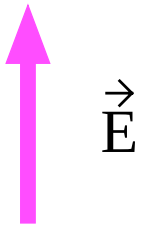
⇒ pour traverser les murs il faut attaquer à 90° !

Diagramme de rayonnement

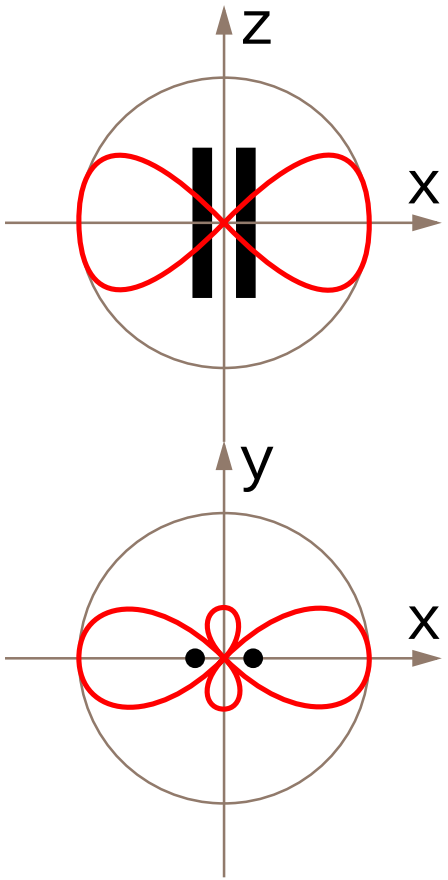
dipôle

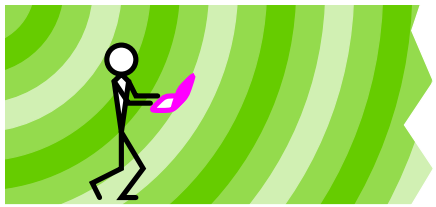


polarisation



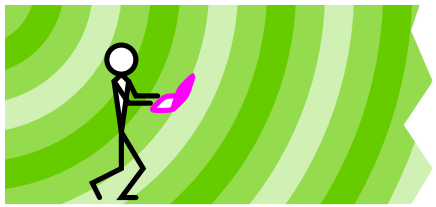
multi-brin



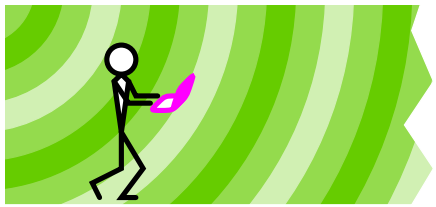


Glossaire

BER	Bit Error Rate taux de bits en erreur
CCK	Complementary Code Keying technique de codage utilisant 64 (sur 256) mots de 8 bits pour leur facilité d'identification en présence de bruit
DSSS	Direct Sequence Spread Spectrum étalement de spectre
EAPOL	Extended Authentication Protocol Over LAN
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
OFDM	Orthogonal Frequency Division Multiplexing



PA	Point d'Accès (p. 11)
PBCC	Packet Binary Convolution Coding
PIRE	Puissance Isotrope Rayonnée Équivalente
PSI	Politique de Sécurité Informatique
QAM	Quadratic Amplitude Modulation technique de modulation en amplitude et phase définissant 16 ou 64 symboles ≠ par Hz
RADIUS	Remote Authentication Dial-In User Service (p. 64)
SSID	Service Set Identifier nom de réseau sans fil = chaîne de caractère
TKIP	Temporal Key Integrity Protocol (p. 63)
WECA	Wireless Ethernet Compatibility Alliance



Sécurité des personnes

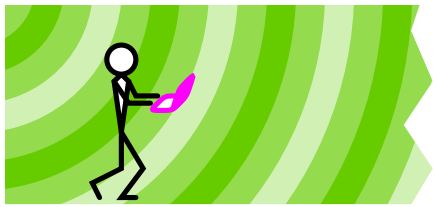
Organismes et programmes de recherche :

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/sommaire.htm

ICNIRP : International Commission on Non-Ionizing Radiation Protection
http://www.icnirp.de/

AFSSE : Agence Française de Sécurité Sanitaire Environnementale
http://www.afsse.fr/



Constructeurs

Apple :

http://www.apple.com/airportexpress/

Aruba :

http://www.arubanetworks.com/

Broadcom :

http://www.broadcom.com/

Linksys (en cours d'ingestion par Cisco) :

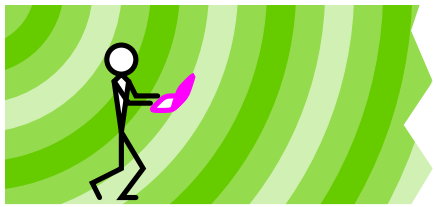
http://www.linksys.com/

Proxim (ex. Orinoco, ex. Lucent) :

http://www.proxim.com/

Trapeze :

http://www.trapezenetworks.com/



Listes de diffusion

http://listes.cru.fr/sympa/info/sans-fil