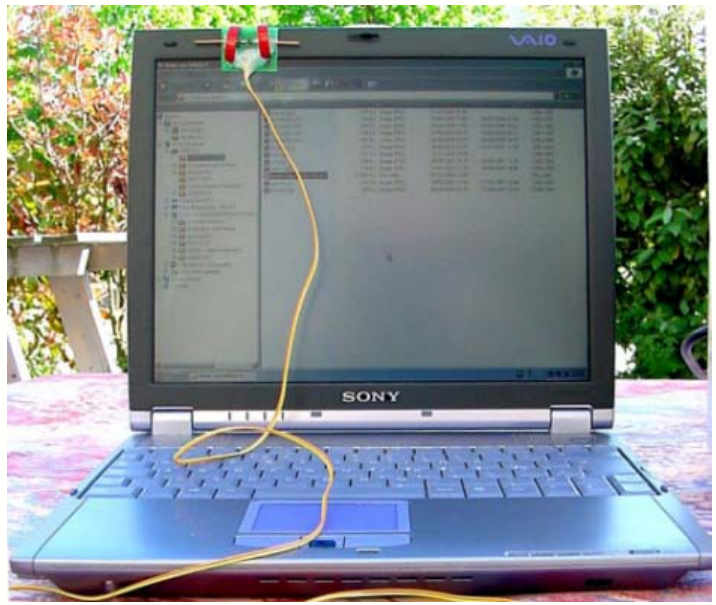
Les réseaux locaux radio

Sommaire



1- Les réseaux et la mobilité

L'informatique mobile permet aux utilisateurs de se déplacer tout en restant connectés au réseau.

Pour cela, les machines doivent disposer d'interfaces de communication sans fil utilisant des ondes radio ou lumineuses comme mode de transmission.

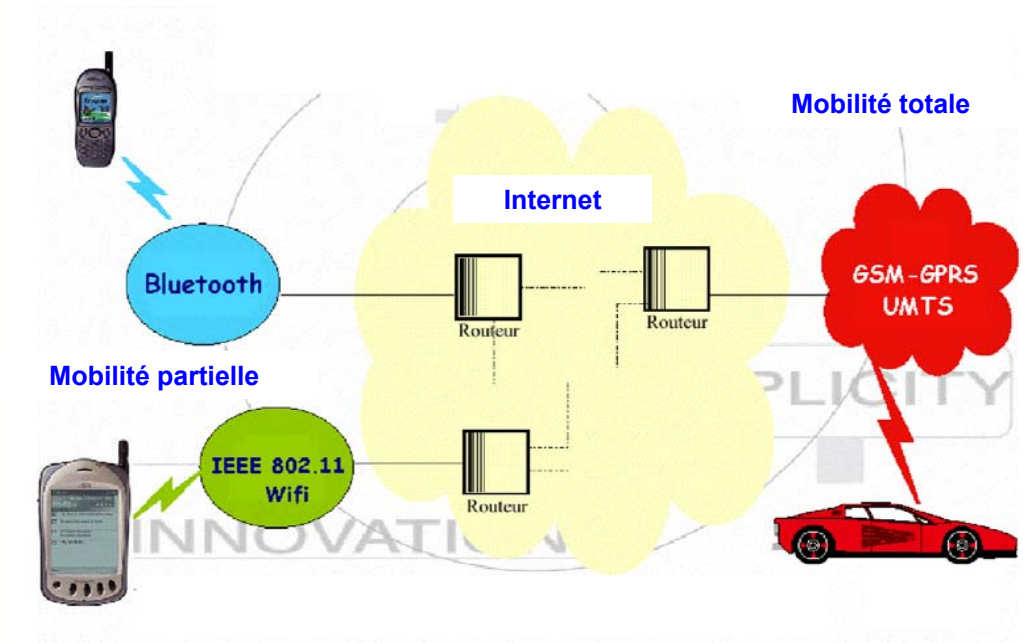
⇒ solution 1 : le téléphone GSM-GPRS

- abonnement « data » pour l'échange des données par GSM à 9600 bits/s
- augmentation du débit avec le GPRS par l'utilisation de plusieurs time-slots par trame
- augmentation de débit et changement de technologie avec l'UMTS (à venir)
- avantage : offre une mobilité totale
- inconvénient : dépendance d'un opérateur, coût

⇒ solution 2 : les réseaux locaux radio

Bluetooth ou Wifi qui offrent :

- un coût d'installation réduit
- la facilité de mise en oeuvre
- un débit intéressant (720 kbits/s pour Bluetooth, jusqu'à 22 Mbits/s pour Wifi)
- inconvénient : mobilité limitée à une zone (100m pour Wifi, 10m pour Bluetooth), mais ceci est rarement gênant



Les réseaux locaux radio se positionnent comme des concurrents pour les opérateurs de téléphonie mobile et pourront même, selon certains, gêner le développement de l'UMTS.

2- Les zones de couverture des réseaux radio

⇒ WPAN (Wireless Personal Area)

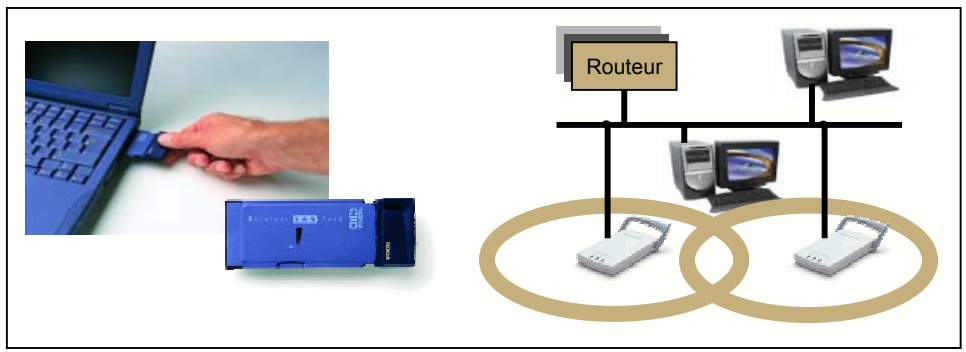
Le téléphone mobile, le baladeur MP3, la montre, l'écharpe communicante, le PDA et bien sûr le micro-ordinateur échangent des informations entre eux, tous situés "autour" de la personne ou d'un point fixe.

La norme Bluetooth lancée par Ericsson et Nokia semble actuellement la mieux adaptée pour ce type de liaison et les premiers objets Bluetooth (téléphones, PDA...) sont d'ores et déjà disponibles.

⇒ WLAN (Wireless Local Area Networks)

Un réseau sans fil Wlan est installé dans la maison, dans l'entreprise, dans un espace public tel qu'un campus universitaire, un café, un centre de conférence, un hôtel, un aéroport... Tous les appareils situés dans la zone de couverture et dotés d'une interface peuvent s'y raccorder.

Les normes les plus utilisées pour ces type de réseaux sont l'IEEE802.11b ou Wifi et l'Hiperlan.



Le WLAN autorise une totale mobilité sur la zone couverte, mais il ne permet pas de passer d'une cellule à une autre (couverte pas une autre borne) sans couper la liaison.

⇒ WMAN (Wireless Metropolitan Area Network)

Un réseau sans fil peut se tisser sur une ville, permettant à tous les habitants d'être connecté entre eux. Relié à l'Internet ou non, il permet des échanges à haut débit, entre voisins, entre entreprises, etc…

3- Les normes IEEE802.11

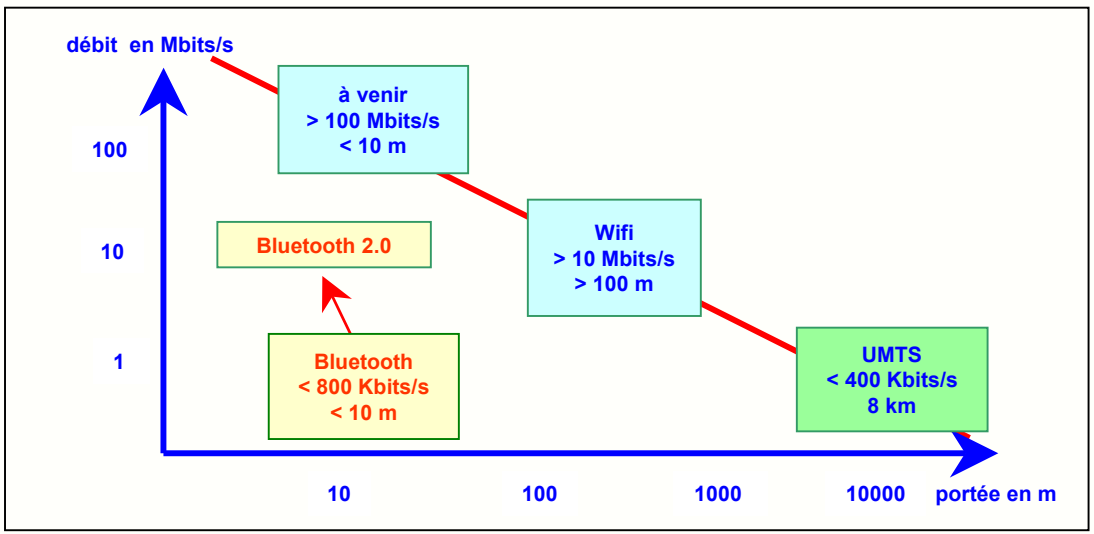
La famille des normes IEEE802.11 concerne la transmission de données par liaison radio dont les caractéristiques générales ont été définies par plusieurs versions :

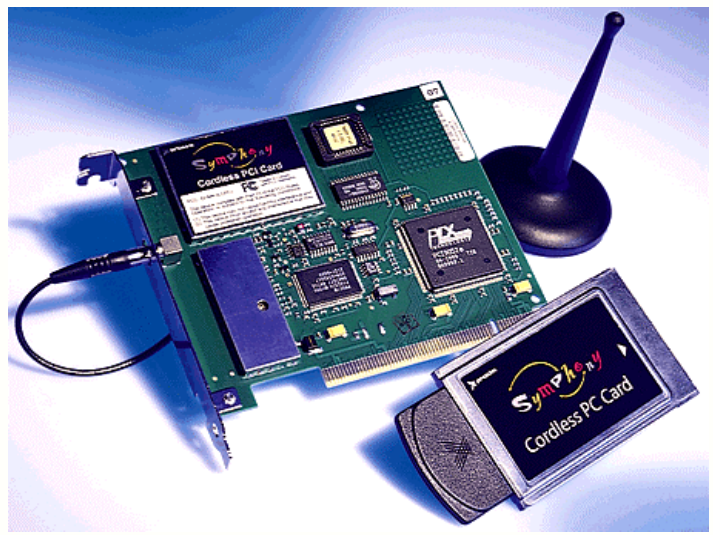
4- Les normes concurrentes

La norme IEE802.11 est en concurrence avec :

- la liaison infra-rouges IrDA (Infrared Data Association) avec une portée de quelques mètres et un débit élevé supérieur à 20 Mbits/s
- le standard Bluetooth qui offre des débits allant jusqu'à 730 kbits/s sur une dizaine de mètres
- la norme radio « HomeRF » similaire à Bluetooth, 127 appareils par réseau, portée de 50 mètres, droits d'utilisation à payer
- la norme DECT à 1,8 GHz, portée de 500 mètres grâce à une puissance d'émission plus élevée, mais débit inférieur à Bluetooth
- la norme Hiperlan dans la bande des 5 GHz, réponse européenne au standard Wifi, débits de 10 à 20 Mbits/s

La norme Wifi se développe rapidement depuis 1999 et est passe de devenir le standard pour les réseaux locaux sans fil.



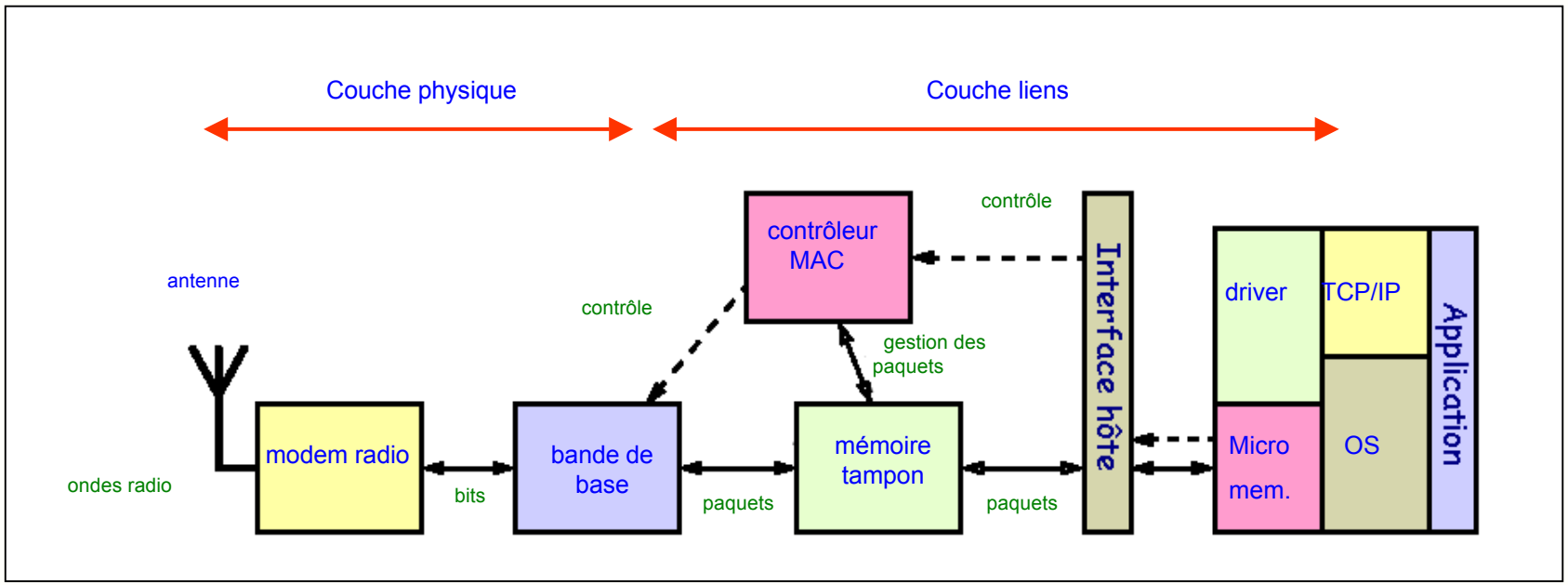


Le standard Wifi utilise des interfaces du même type que Bluetooth, avec une puissance d'émission plus élevée, une portée plus importante qui peut atteindre 100 mètres, ainsi qu'un mode de modulation différent.

Le débit offert théorique est de 11 Mbits/s soit 3 à 4 Mbits/s en réalité.

5- La constitution de l'interface radio

L'interface radio permettant de réaliser un réseau est constituée le plus souvent d'une carte ISA ou PCMCIA à installer dans un PC ou une station de travail.

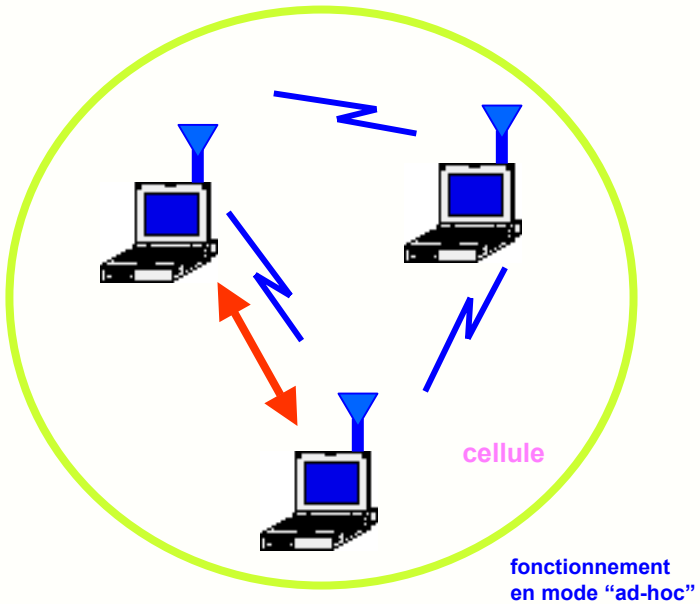


- le modem radio, qui émet et reçoit, en modulant et démodulant la porteuse avec les données binaires à transmettre. Il est surtout constitué de fonctions analogiques (antennes, amplificateurs, synthétiseur de fréquence, filtres etc …)
- le contrôleur MAC (Medium Access Controller) met en œuvre le protocole d'accès au support physique radio. Souvent piloté par un microcontrôleur, il est étroitement associée à sa mémoire tampon qui permet de stocker temporairement les données entrantes et sortantes.
- l'interface hôte, qui utilise un des bus du PC (ISA, PCI, PCMCIA) ou un des ports de communication (série, parallèle, USB, Ethernet…). Elle permet au logiciel (driver) de communiquer avec le contrôleur MAC, la plupart du temps en écrivant à des emplacements mémoire dédiés.

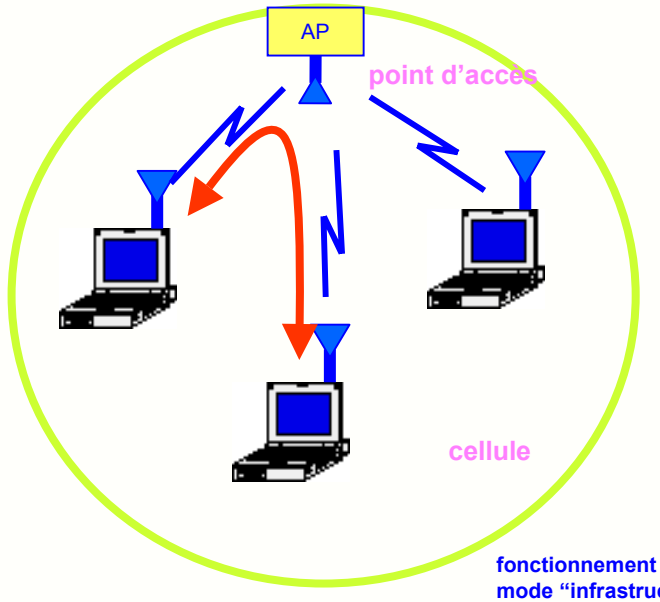
6- Topologie d'un réseau en mode « ad-hoc »

Les WLAN peuvent fonctionner de deux façon différentes :

- en mode ad-hoc : un équipement échange des données directement avec un autre équipement situé dans sa zone de couverture radio
- en mode infrastructure : les équipements communiquent entre eux par l'intermédiaire d'une base ou point d'accès AP



fonctionnement
en mode "ad-hoc"

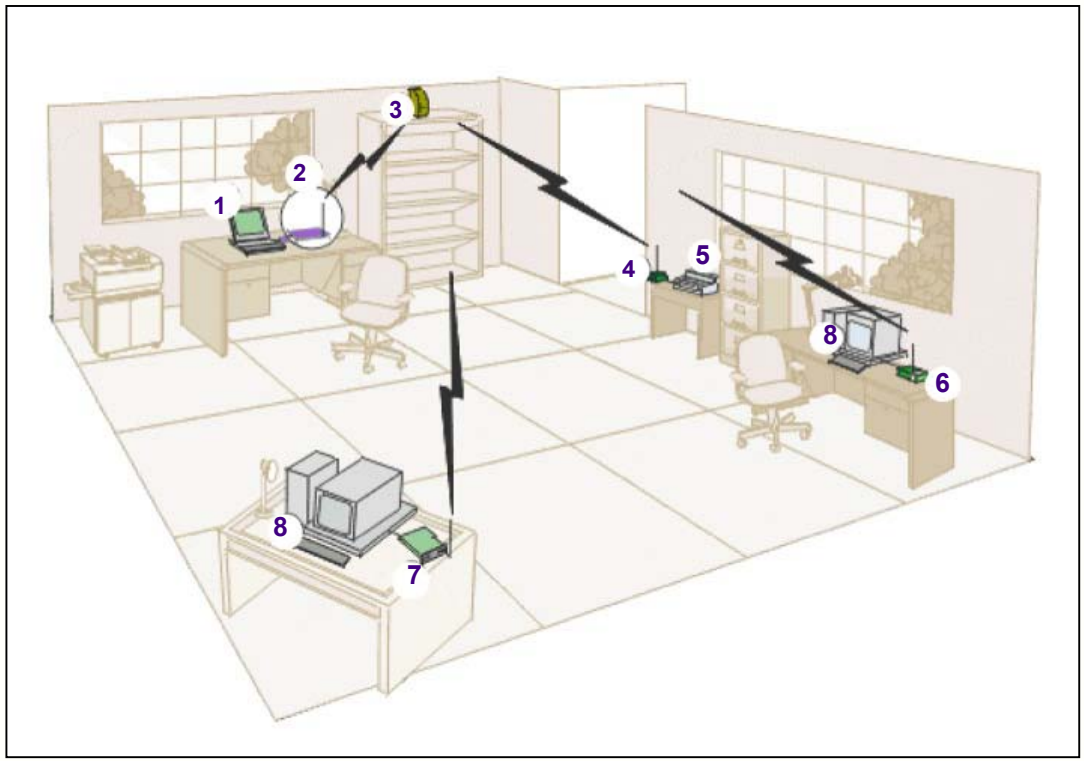


fonctionnement en
mode "infrastructure"

- le réseau ad hoc est auto-configurable : lorsque deux machines mobiles se retrouvent dans le même secteur géographique, elles peuvent se reconnaître puis échanger des données.
- chaque machine peut échanger des informations avec n'importe quelle autre machine à portée de réception
- dans un mode de fonctionnement idéal (à venir), chaque nœud du réseau peut servir de routeur lorsque deux machines ne peuvent se joindre directement
- deux équipements équipés d'interfaces IEEE802.11b peuvent communiquer directement entre eux dans le mode ad-hoc sans nécessiter de point d'accès à proximité.

7- Topologie d'un réseau en mode infrastructure

Le mode infrastructure fait appel à des bornes appelées points d'accès qui gèrent l'ensemble des communication dans une même zone ou cellule, comme dans les réseaux GSM.



1 - ordinateur portable

2- carte interface radio PCMCIA

3- point d'accès AP (access point)

4 et 6 – interface radio externe

5- imprimante

7- carte interface radio

8 – PC de bureau

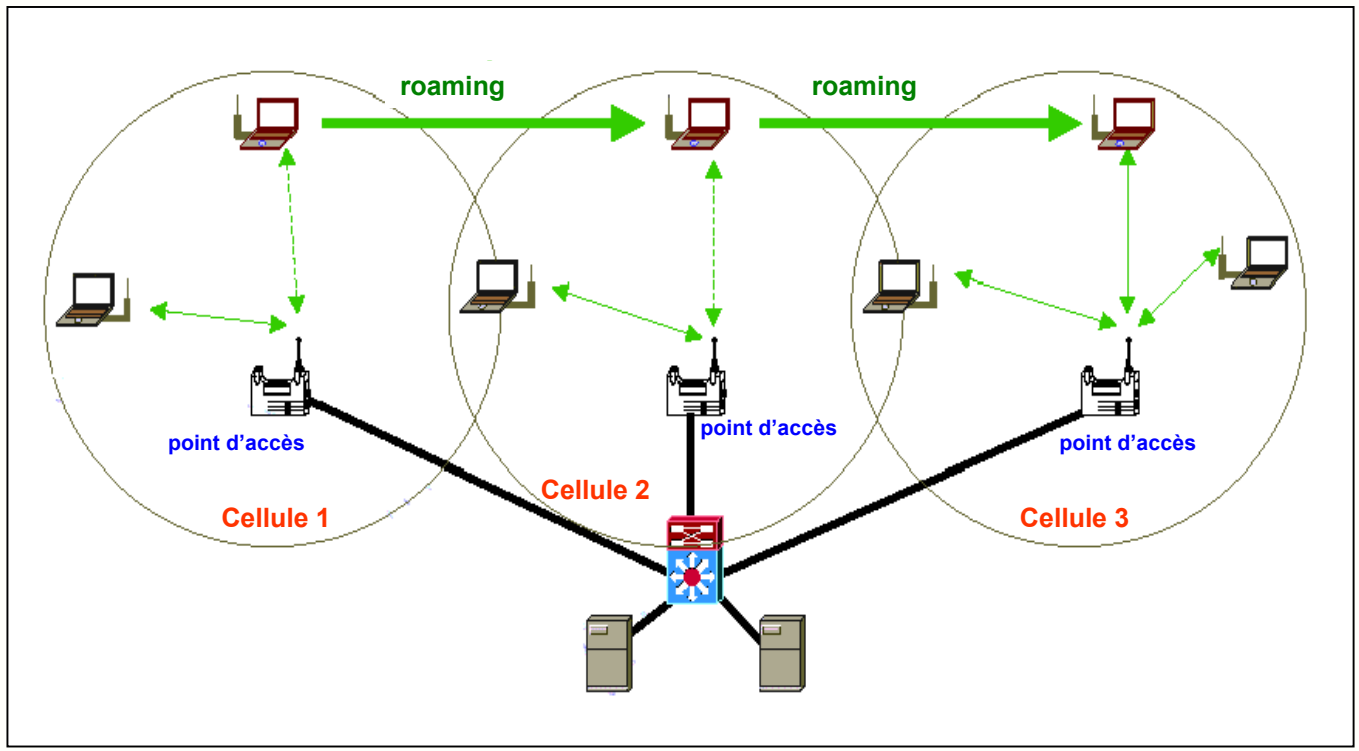
Les réseaux IEEE802.11b ou Wifi fonctionnent le plus souvent selon ce mode :

- les équipements mobiles communiquent entre eux en passant par le point d'accès, leur nombre maximal est de 128 par cellule
- le réseau Wifi est formé de cellules appelées BSS (Basic Service Set)
- l'ensemble des cellules et de leur point d'accès est l'ESS (Extended Service Set)
- l'ESS est relié au réseau Ethernet câblé par un portail, souvent intégré dans l'AP

8- Topologie d'un réseau à plusieurs cellules

Dans un réseau à infrastructure et à plusieurs cellules :

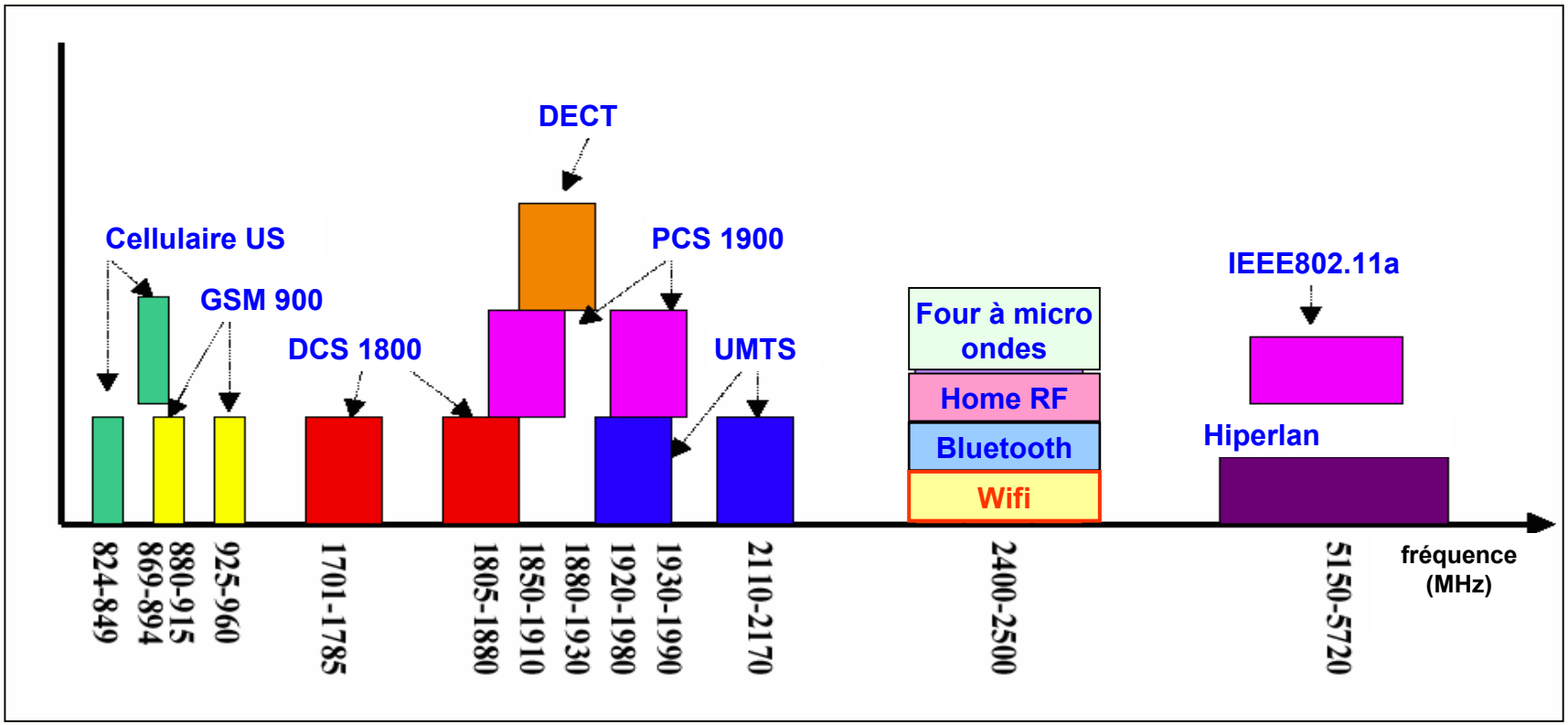
- les bornes sont connectées entre elles par une liaison ou un réseau filaire ou hertzien
- les terminaux peuvent alors se déplacer au sein de la cellule et garder une liaison directe avec le point d'accès
- ils peuvent aussi changer de cellule, ce qui s'appelle le roaming
- l'ensemble des cellules et de leur point d'accès est l'ESS (Extended Service Set)
- les cellules sont reliées au réseau Ethernet câblé par un portail, souvent intégré dans le point d'accès



Remarque : dans certains cas, les différentes cellules se superposent complètement, ce qui permet d'offrir plusieurs fréquences aux utilisateurs de la cellule, et donc un débit plus satisfaisant.

9- La bande ISM allouée à Wifi

Les bandes de fréquences affectées aux réseaux locaux radio sont les bandes ISM (Industrial, Scientific and Medical), destinées à l'origine aux chauffages micro-ondes, aux réseaux hertziens...



Deux bandes sont utilisées :

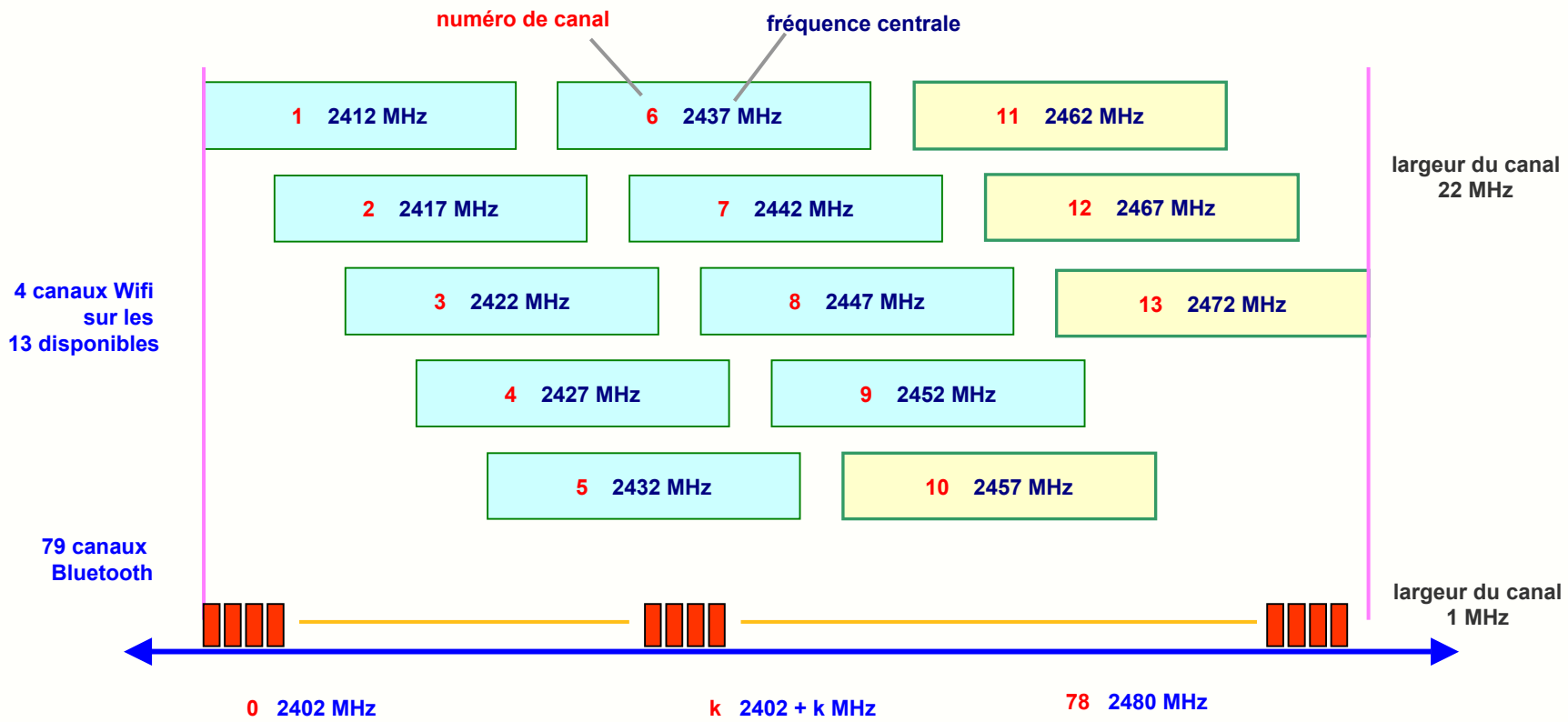
- la bande des 2,4 GHz, commune à la plupart des pays, pour les standards IEE802.11b (Wifi), Bluetooth et HomeRF
- la bande des 5,5 GHz moins encombrée et perturbée que la précédente, pour IEEE802.11a et Hiperlan

Remarque : l'utilisation de la bande ISM des 2,4 GHz est libre à condition de limiter la puissance d'émission et de protéger la liaison vis-à-vis des perturbations par l'utilisation d'une technique d'étalement de spectre

10- Les fréquences de travail

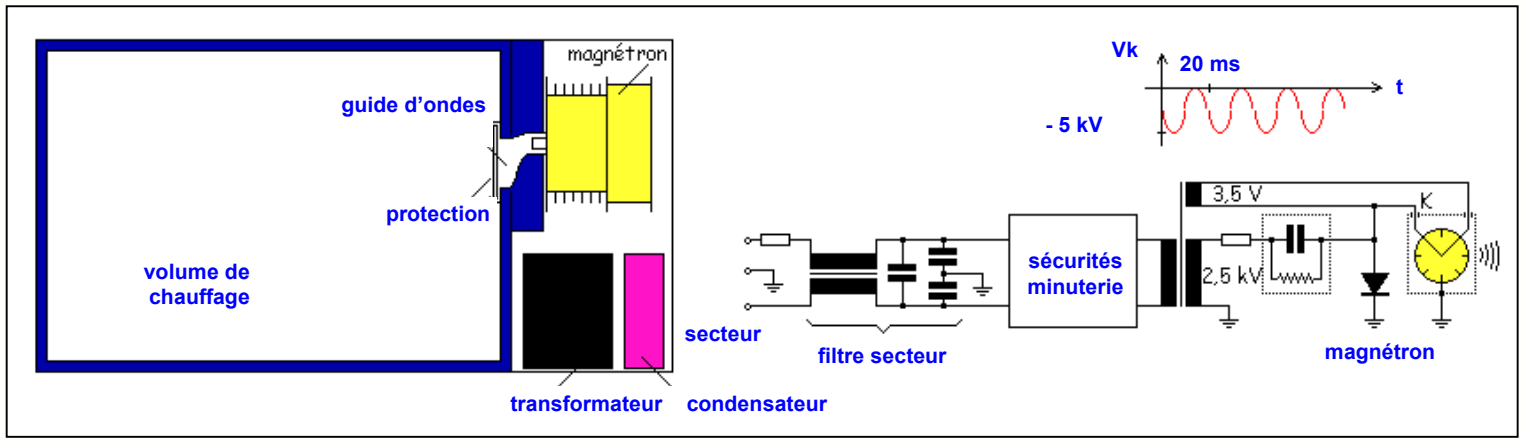
En France, une partie de la bande ISM est utilisée par l'Armée :

- pour Wifi : seuls les canaux 10 à 13 sont disponibles, pas d'autorisation nécessaire à l'intérieur des bâtiments si la puissance d'émission reste inférieure à 100 mW
- pour Bluetooth : 79 canaux de 1 MHz allant 2400 à 2483,5 MHz , utilisation libre à l'intérieur des bâtiments pour des puissances inférieures à 10 mW, et à l'extérieur si la puissance d'émission reste en-dessous de 4mW

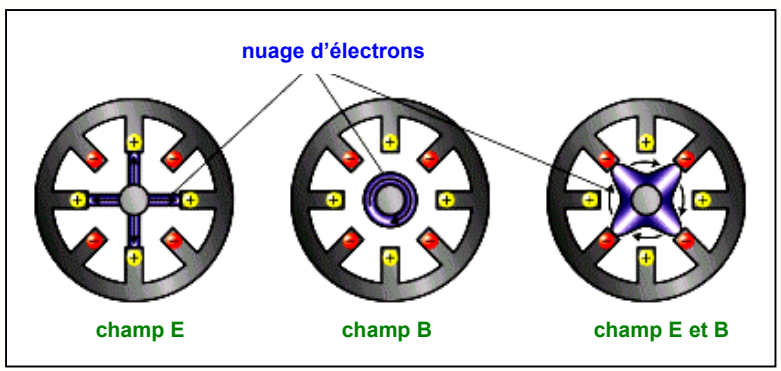


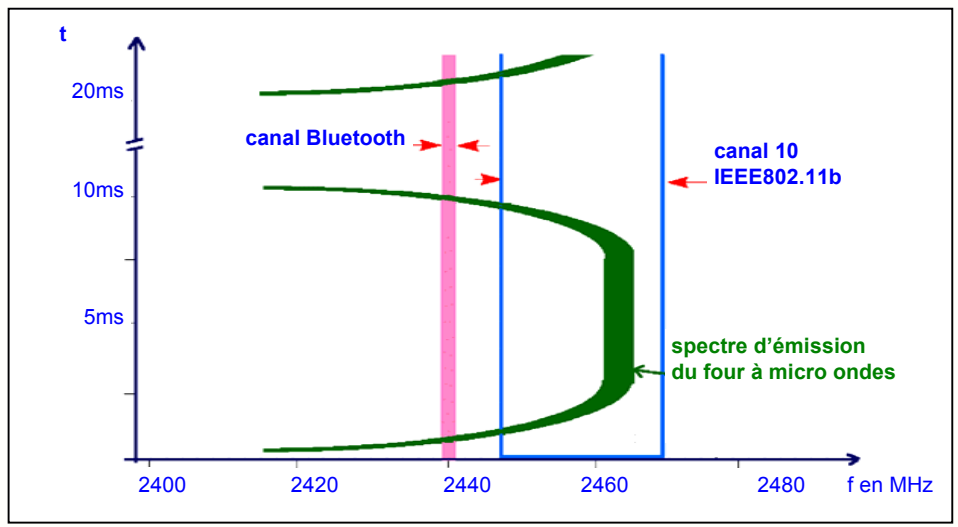
11- Les perturbations des fours à micro ondes

Le four à micro ondes est construit autour d'un générateur appelé magnétron qui comporte une cathode chauffée émettant des électrons dans une cavité métallique, une alimentation fournissant la haute tension Vk pulsée polarisant la cathode (-5kV, 400 mA) et un tronçon de guide d'onde conduisant les ondes du magnétron dans le four.



- les électrons s'éloignent de la cathode en tournant sous l'effet conjugué des champs électrique et magnétique
- le mouvement de ce nuage d'électrons induit des courants dans la structure de la cavité et produit une onde EM
- la fréquence de l'onde dépend essentiellement des dimensions et du nombre d'ailettes de la cavité.
- l'onde produite est pulsée comme l'alimentation et dérive en fréquence



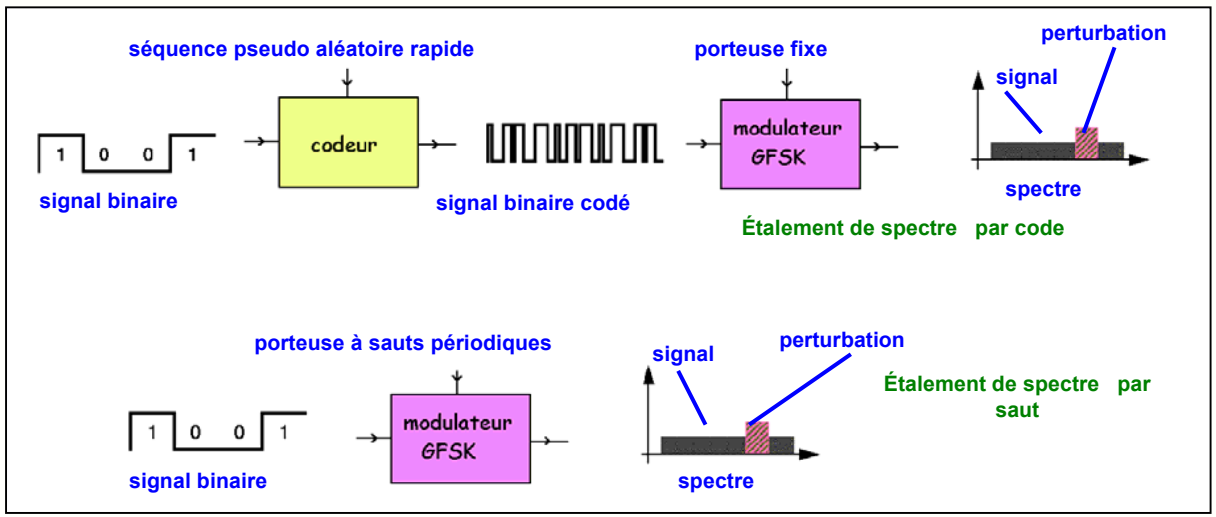


Conclusion : les fuites d'un four à micro ondes polluent « allègrement » toute la bande ISM

12- La protection contre les brouillages

A cause des perturbations, il a fallu protéger la transmission radio contre les brouillages par une technique d'étalement de spectre qui consiste à utiliser une bande de fréquence beaucoup plus large que celle qui est nécessaire :

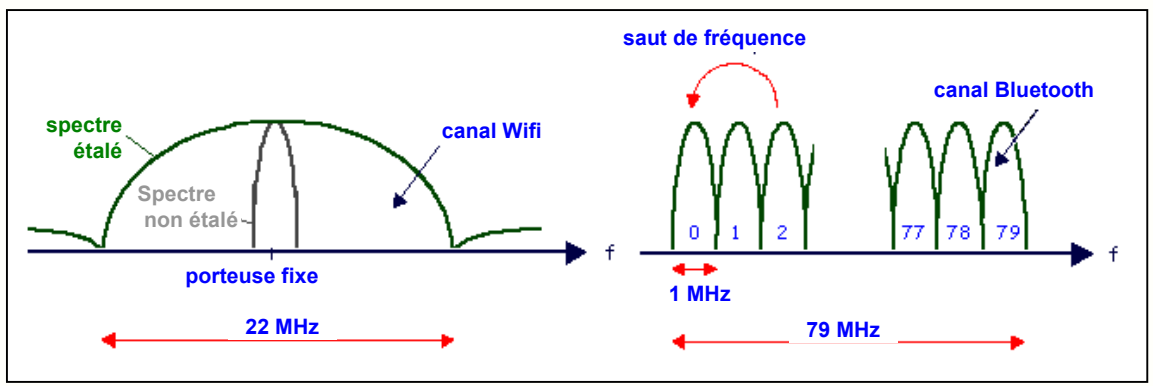
- par saut de fréquence : la porteuse saute d'un canal à l'autre, ce qui conduit à l'utilisation de la totalité des canaux (Bluetooth)
- par code binaire : avant de moduler la porteuse, on mélange le signal binaire à une séquence numérique pseudo aléatoire de débit nettement plus élevé (Wifi, CDMA, UMTS)



- chaque transmission Bluetooth utilise les 79 canaux et occupe la bande dans sa totalité, soit une largeur d'environ B=80 MHz pour un débit maximal de 1 Mbits/s
- pour une transmission Wifi le signal est mélangé à une séquence pseudo aléatoire à 11 Mbits/s, ce qui donne un spectre de largeur B=22 MHz

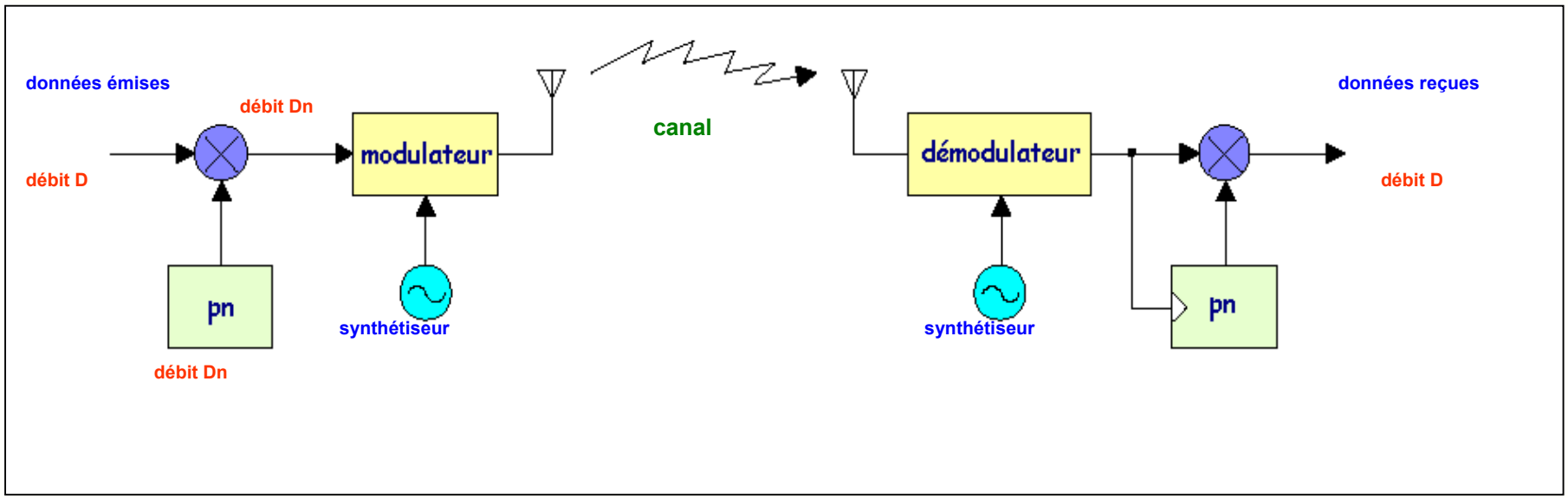
L'avantage est une relative insensibilité à la présence de signaux de brouillages au prix d'un encombrement spectral supérieur.

Remarque : pour éviter les perturbations mutuelles, certains préconisent d'interdire les sauts Bluetooth dans les canaux utilisés par Wifi.



13- L'étalement de spectre par code DSSS

L'étalement de spectre par code appelé aussi DSSS (direct sequence spread spectrum) utilisé dans le standard Wifi met en œuvre les traitements suivants :



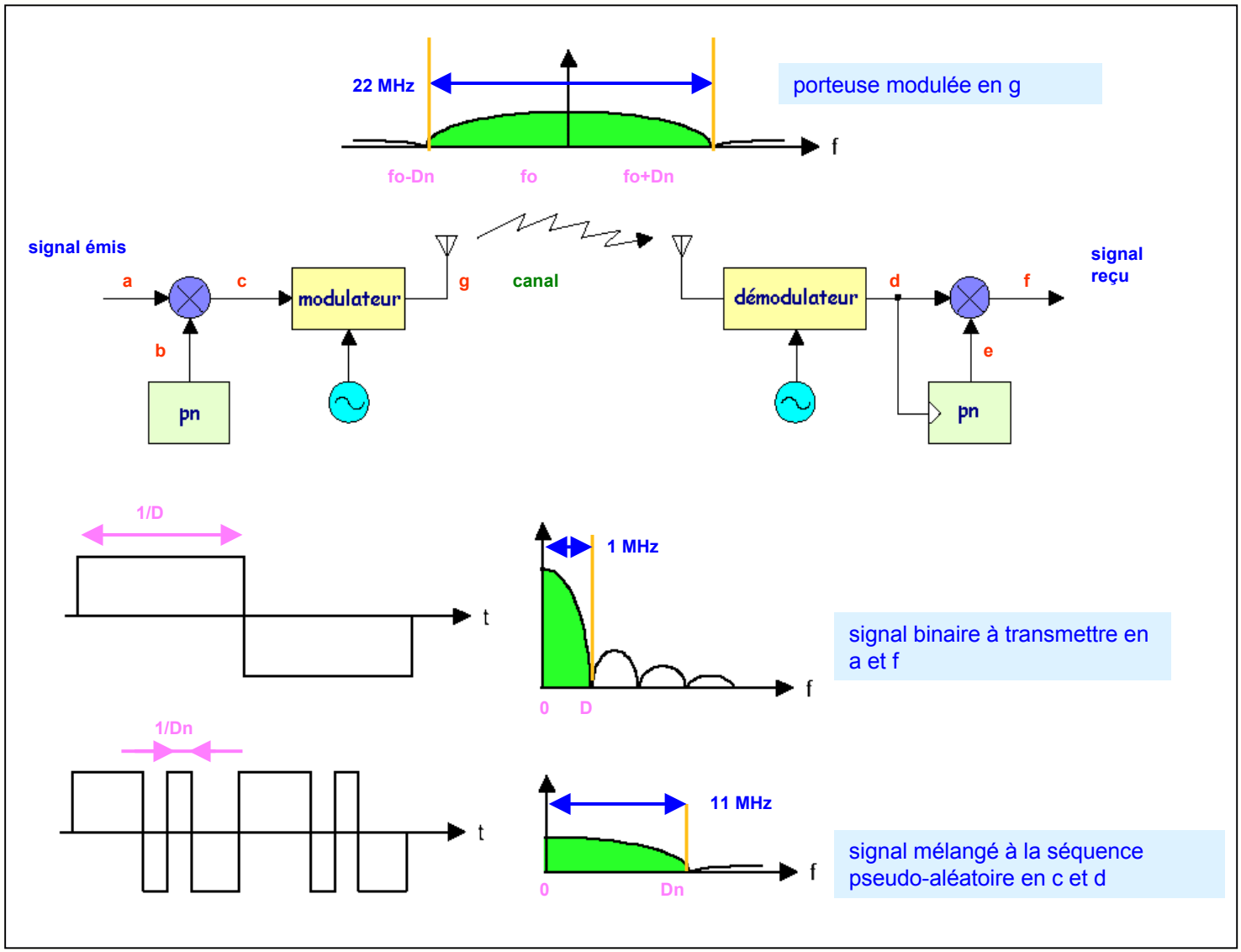
- le signal binaire des données ayant un débit de base D = 1 MHz est mélangé par OU exclusif à une séquence pseudo-aléatoire pn de débit plus élevé Dn = 11 MHz
- le signal résultant, de débit Dn, module la porteuse de l'émetteur en modulation de phase à 2 états ou BPSK, la porteuse modulée occupe alors une bande égale à 2.Dn = 22 MHz
- à la réception, la porteuse est démodulée et le résultat mélangé à la même séquence pseudo aléatoire pour récupérer les données binaires

Remarques :

- le spectre de la porteuse modulée est plus large que celui qui serait strictement nécessaire
- l'élargissement du spectre rend le signal moins sensible aux perturbations à bande étroite
- l'étalement de spectre permet aussi d'introduire un cryptage de données permettant la sécurisation de la transmission

14- Les spectres dans l'émission DSSS

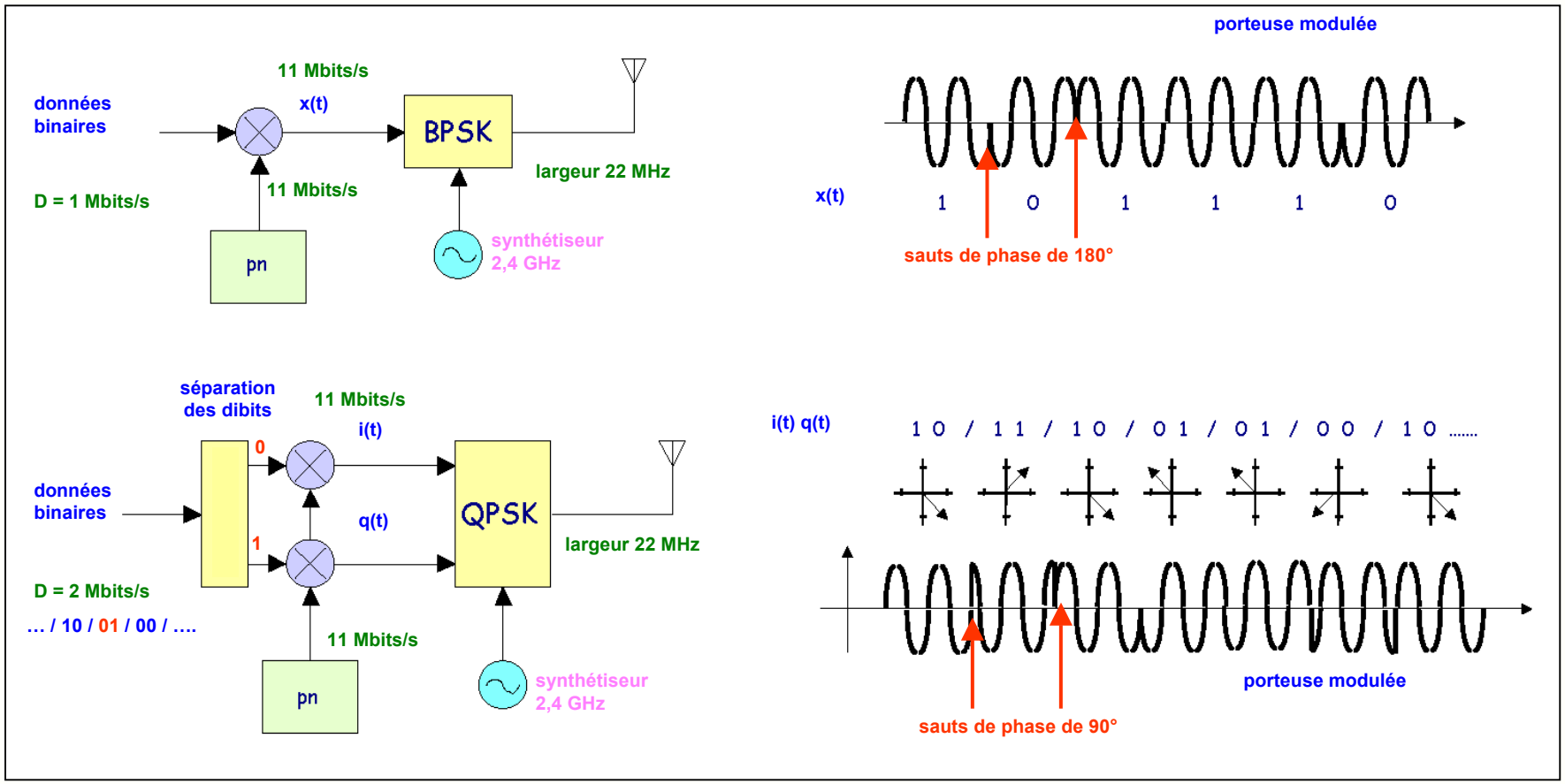
L'étalement de spectre par code produit une porteuse modulée dont le spectre occupe une largeur de 22 MHz :



15- Le principe de l'émission DSSS

Les modulations utilisées sont celles utilisées dans toutes les applications de communication numérique (modems, TV satellite …) :

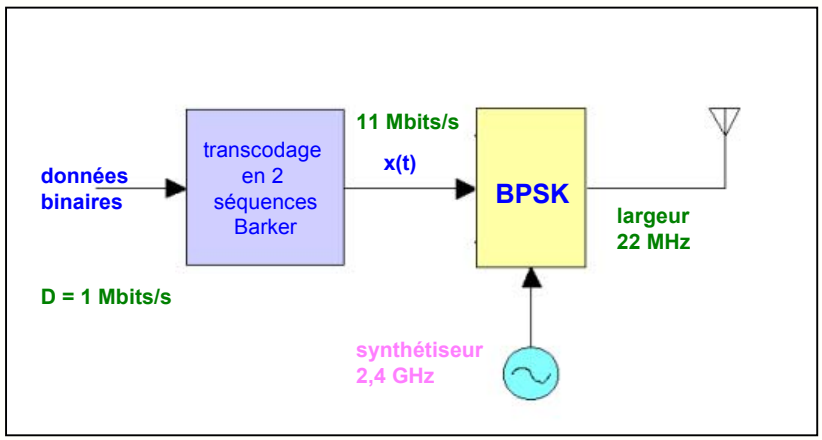
- la modulation de phase à 2 états est utilisée pour un débit de 1 Mbits/s
- la modulation de phase en quadrature ou QPSK est utilisée dès que le débit dépasse 1 Mbits/s

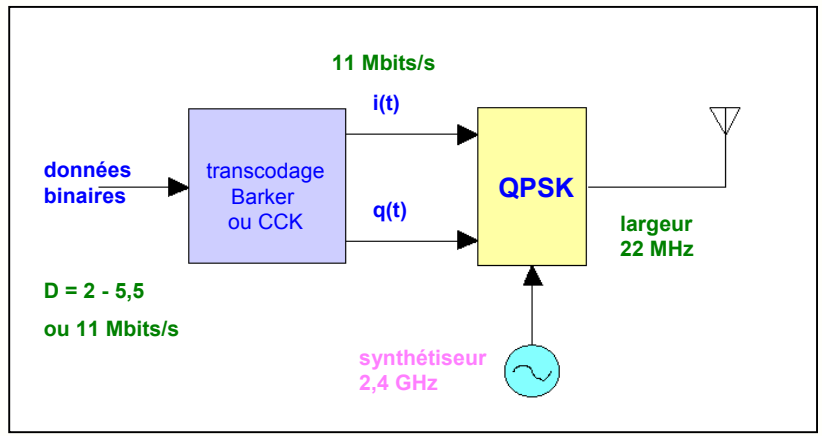


16- La pratique de l'émission DSSS pour Wifi

Dans la pratique, les techniques utilisées sont un peu différentes :

- au lieu d'utiliser un générateur de séquence pseudo aléatoire, le système effectue simplement un transcodage des données binaires
- pour un débit de 1 Mbits/s, le système associe deux séquences « Barker » différentes de 11 bits au « 0 » et au « 1 »
- en utilisant une modulation de phase à 4 états le débit a pu être doublé à 2 Mbits/s
- le transcodage CCK remplace des groupes de 4 (ou 8) bits par un mot de 8 bits, ce qui permet d'atteindre des débits de 5,5 (ou 11) Mbits/s





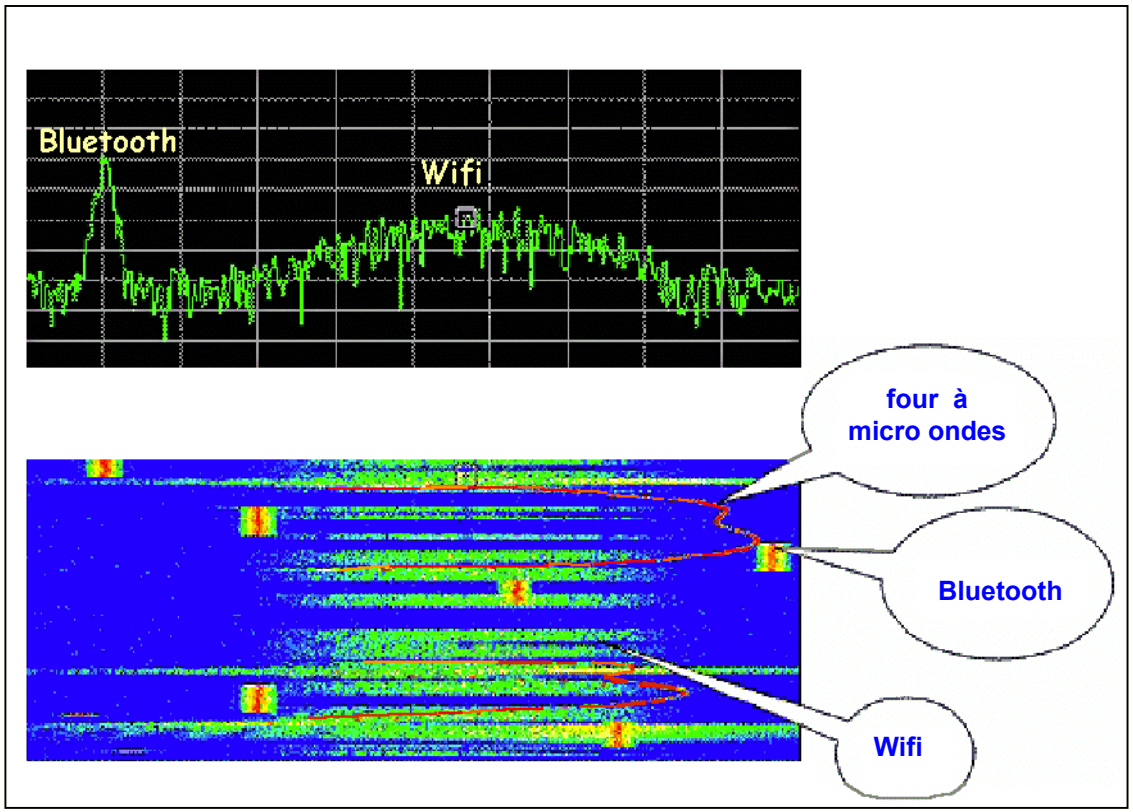
Débit binaire	Séquence	Modulation	Transcodage
1 Mbits/s	séquence Barker	**BPSK**	1 bit de donnée = 11 bits en x(t)
2 Mbits/s	séquence Barker	**QPSK**	2 bits de données = 11 bits en i(t) et q(t)
5.5 Mbits/s	CCK : complementary code keying	**QPSK**	4 bits de données = 8 bits en i(t) et q(t)
11 Mbits/s	CCK : complementary code keying	**QPSK**	8 bits de données = 8 bits en i(t) et q(t)

Pour réduire le taux d'erreurs dans les environnements bruyants, les WLANs 802.11b mettent en oeuvre :

- le transcodage Barker ou CCK utilisant des séquences binaires particulières résistantes aux erreurs de transmission
- comme les modems, le repliement vers un débit plus faible appelé dynamic rate shifting lorsque le taux d'erreurs a tendance à augmenter

17- Le spectre d'émission DSSS

Quelque soit le débit binaire au niveau des données (1,2,5,5 ou 11 Mbits/s) et quelque soit le type de modulation utilisé (BPSK ou QPSK), l'essentiel de la puissance émise se trouve dans une bande de largeur 22 MHz centrée sur la fréquence de la porteuse .



Fréquence centrale : 2447 MHz

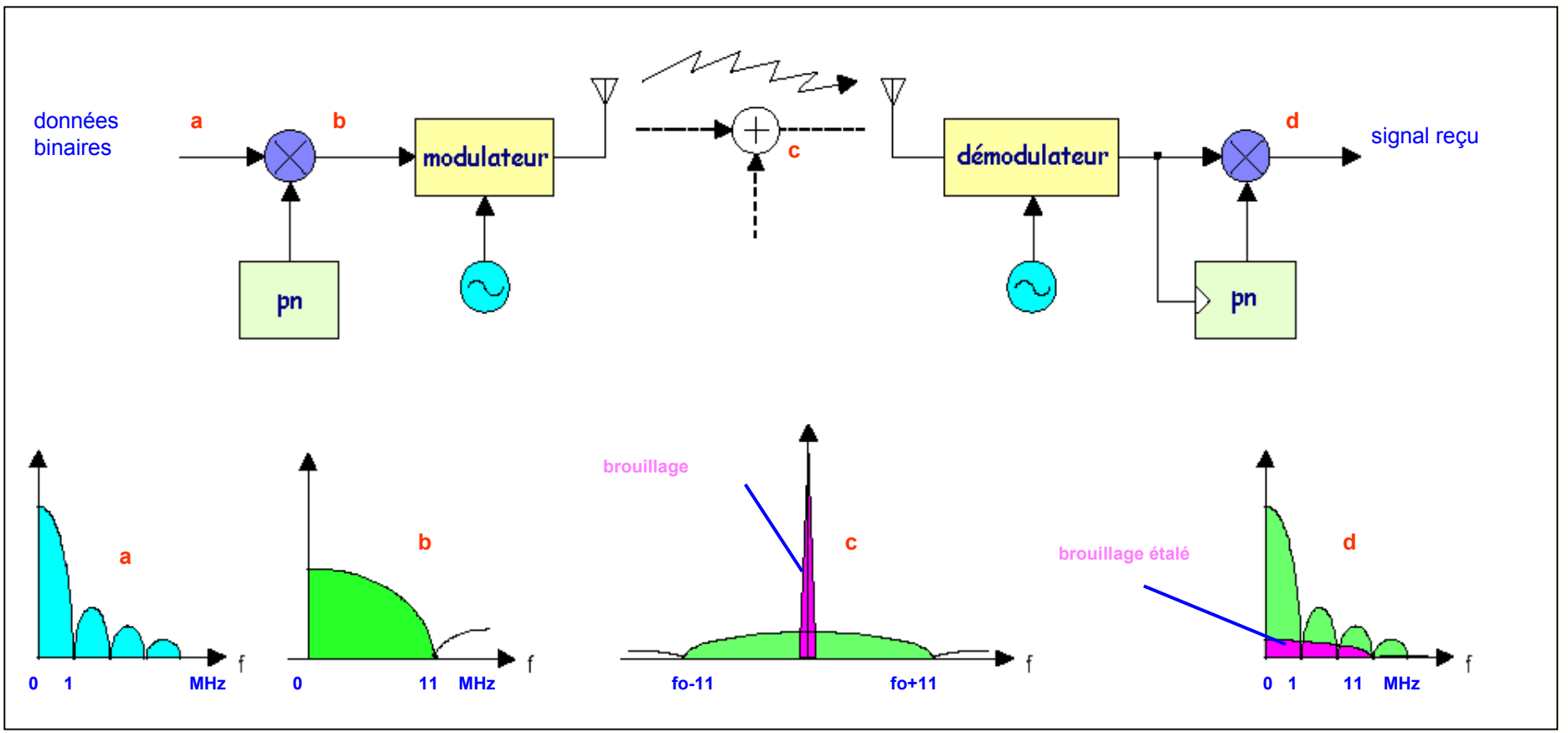
Échelle : 3 MHz/carreau

La transmission radio avec la technique d'étalement de spectre par code se fait à fréquence de porteuse fixe. Ce spectre est discontinu (phases d'émission et de réception), mais contrairement à Bluetooth reste fixe en fréquence.

18- L'émission DSSS en présence de brouillage

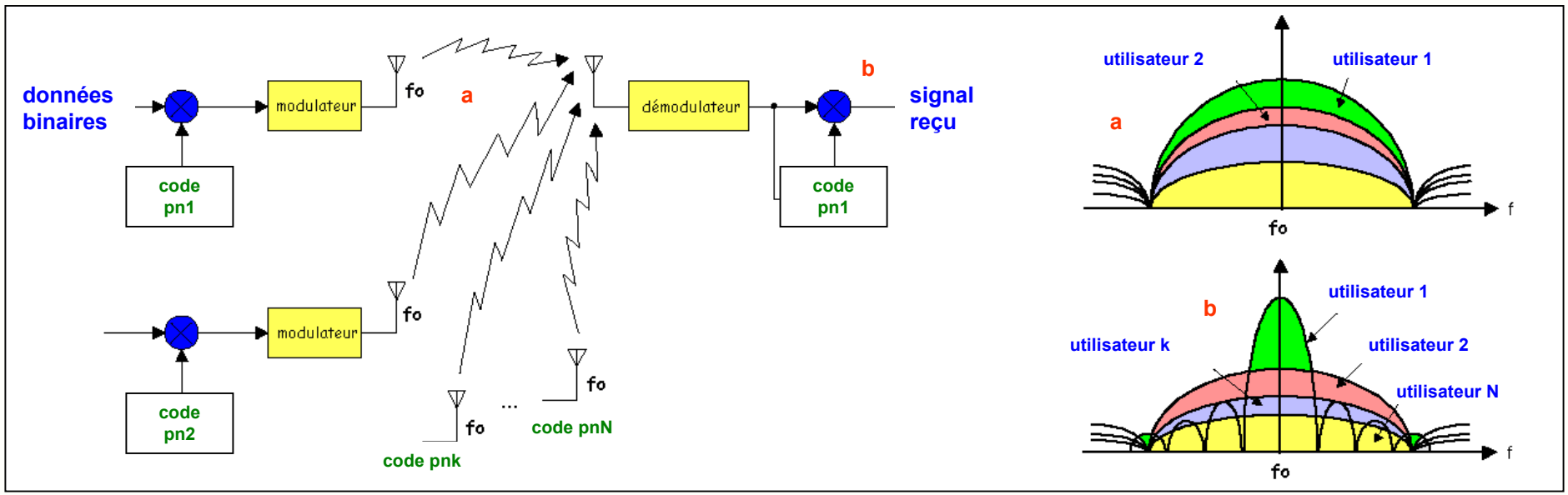
L'efficacité de l'étalement de spectre par séquence pseudo aléatoire réside dans sa robustesse par rapport aux signaux de brouillage qui se superposent au signal lors de la propagation

- le spectre du signal modulant (données) est étalé par la séquence pn à l'émission, et contracté par mélange avec la même séquence pn à la réception
- un brouillage (émission Bluetooth, four à micro ondes …) se superposant au signal durant la transmission voit son spectre étalé par la séquence pn à la réception
- le signal correspondant est assimilable à un bruit qui ne gêne pas la réception des données tant que son niveau n'est pas excessif



19- Un autre type d'émission DSSS : l'UMTS

- dans le standard Wifi, l'algorithme générant la séquence pseudo aléatoire est figé, et tous les étalements se font donc avec le même code pn.
- dans l'UMTS, un grand nombre d'utilisateurs travaille sur la même fréquence et chacun a un code différent. Une séquence pseudo-aléatoire à 5 Mbits/s est mélangée au signal d'information binaire dont le débit est compris entre 9,6 kbits/s et 2 Mbits/s.
- un grand nombre de communications peuvent ainsi être transmises simultanément sur la même fréquence, chaque correspondant étant caractérisé par un code particulier

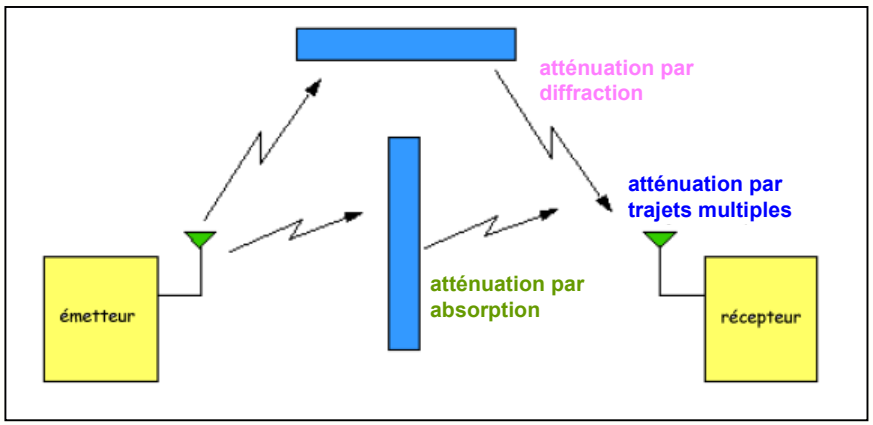


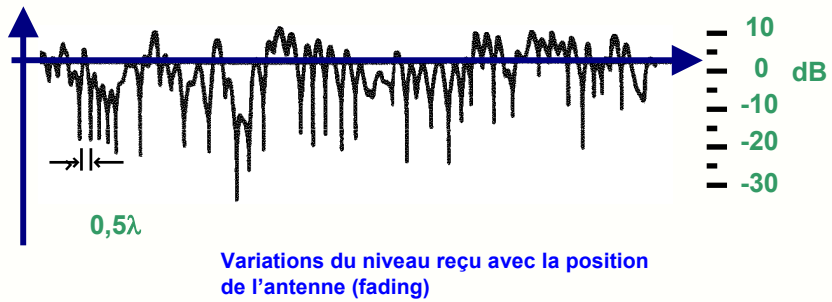
- le récepteur mélange le signal reçu avec le code numérique et sépare ainsi les usagers en récupérant l'information binaire

20- La portée d'une liaison à 2,4 GHz

La portée d'une liaison RF à 2,45 GHz dépend :

- de la puissance émise et du gain de l'antenne : la puissance est un paramètre essentiel, et un dispositif d'adaptation de la puissance émise permet d'optimiser la liaison et de maintenir le taux d'erreur à un niveau suffisamment bas. Une antenne de bonne qualité permet d'augmenter la portée, mais est difficile à installer à l'intérieur d'un portable.





Variations du niveau reçu avec la position de l'antenne (fading)

- de l'environnement : avant d'arriver sur le récepteur, l'onde doit traverser des obstacles (corps humain, cloisons …) qui absorberont une partie de l'énergie émise, ce qui diminuera d'autant la portée du système.
- du fading **:** l'arrivée sur l'antenne du récepteur d'ondes ayant suivi des trajets différents conduit à des variations de niveau du signal reçu (interférences constructives ou destructives appelées fading).
- de la sensibilité du récepteur qui passe –90 dBm (1 Mbits/s) à –83 dBm pour le débit maximal de 11 Mbits/s.

La portée dépend de la puissance d'émission, mais aussi du taux de transfert.

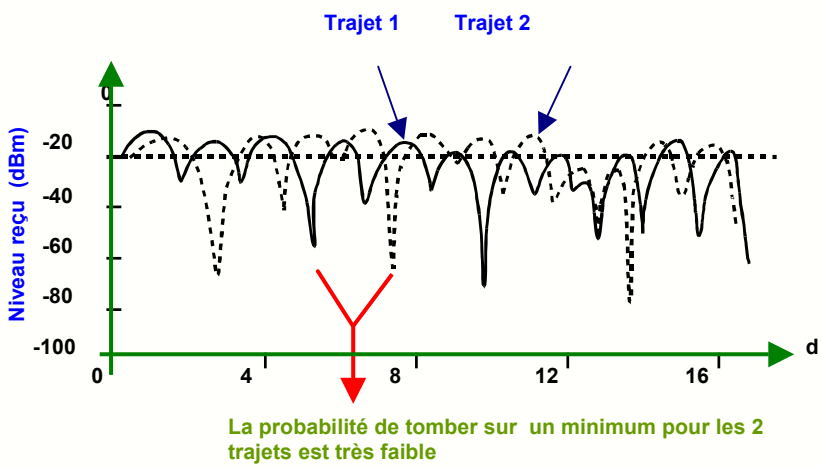
Débit en Mbits/s	11	5,5	2	1
Portée en extérieur @ 100mW	65 m	90 m	125 m	180 m
Portée en intérieur @ 100mW	30 m	35 m	45 m	55 m

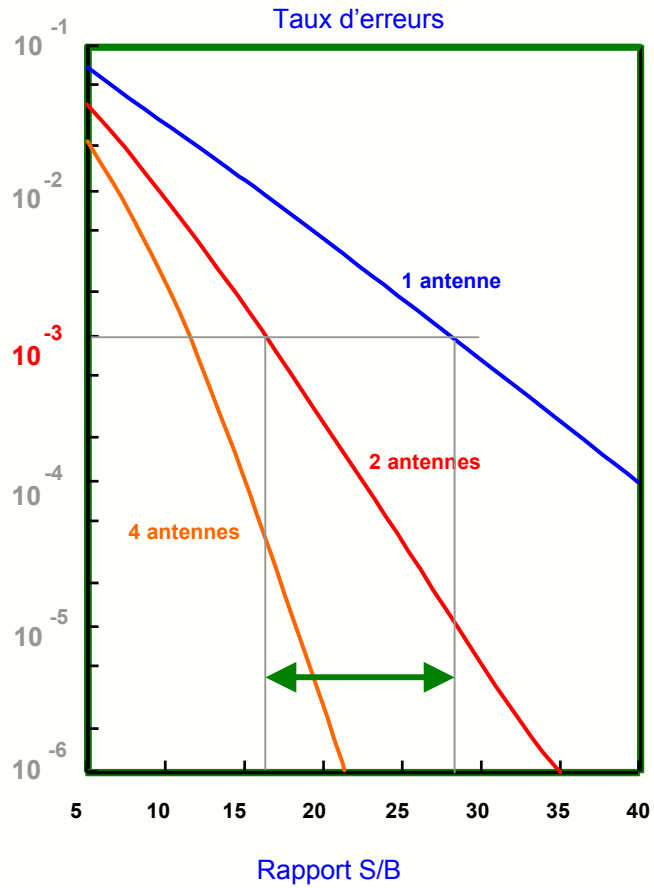
Remarque : si la station s'éloigne du point d'accès, le débit s'ajuste pour maintenir un taux d'erreurs suffisamment bas.

21- La technique des antennes multiples

La réponse au problème des trajets multiples et du fading associé est l'utilisation de plusieurs antennes au niveau du point d'accès :

- la probabilité de tomber exactement sur un minimum pour deux trajets différents est très faible, même si la différence de trajet parcouru est faible (λ = 12,5 cm à 2,4 GHz)
- si on utilise plusieurs antennes pour la réception au niveau de la station de base, on peut optimiser la réception en commutant l'antenne qui procure le signal le plus élevé





L'obtention d'un taux d'erreurs de 10^{-3} par exemple nécessite :

- un rapport S/B moyen S/B= 28 dB avec 1 antenne
- un rapport S/B moyen S/B=16 dB avec 2 antennes

Le gain de 12 dB obtenu par l'utilisation de 2 antennes permettra :

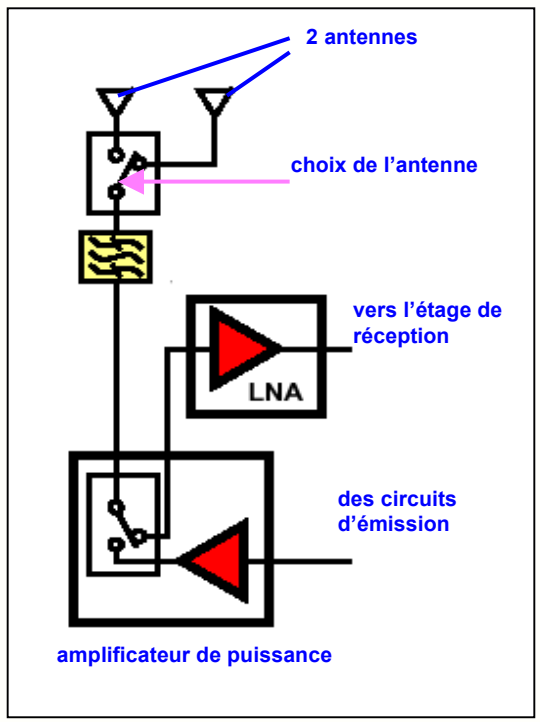
- de diminuer le taux d'erreurs ou
- d'augmenter la portée de la base

22- Exemples de dispositifs à antennes multiples

La technique de l'antenne multiple est facile à mettre en oeuvre :

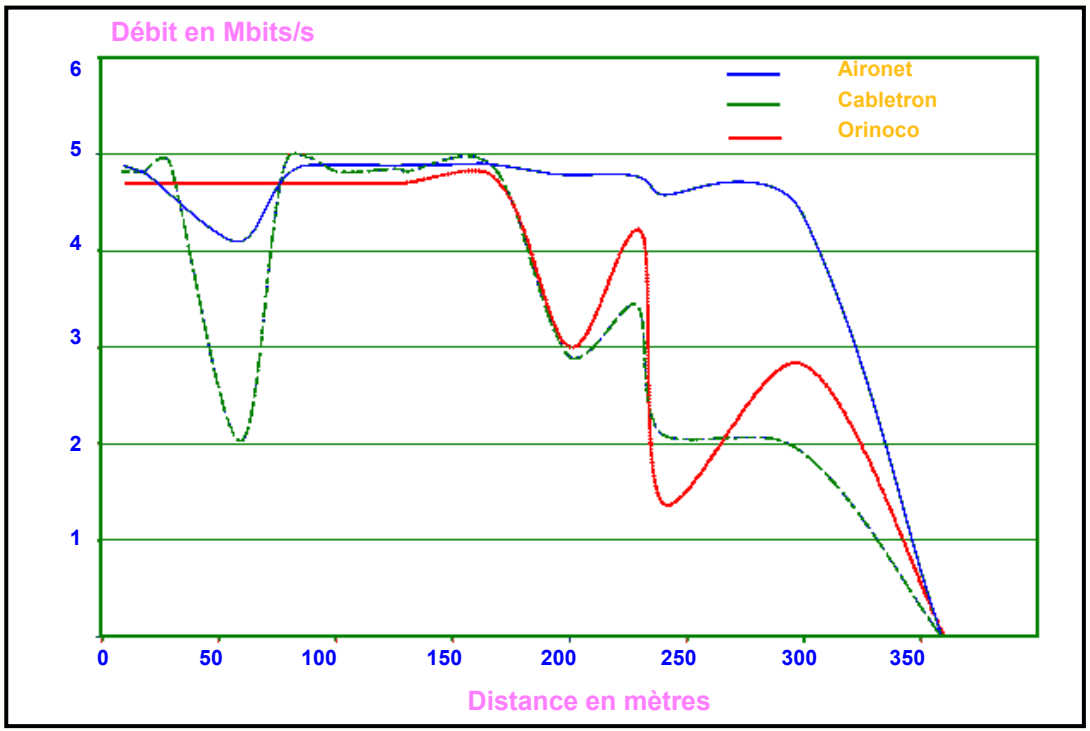
- la plupart des points d'accès disponibles dans le commerce sont équipés de 2 antennes
- les PC portables équipés en standard de l'interface Wifi sont souvent équipés de 2 antennes placées autour de l'écran en polarisation croisée
- le circuit contrôleur de l'interface, après une mesure de niveau reçu, choisit l'antenne donnant le meilleur signal en réception
- en émission, on peut utiliser une seule antenne, ou les deux simultanément

Exemple de point d'accès Ericsson



23- Portées obtenues avec différentes interfaces

Des mesures de débit et de portée sur des systèmes Wifi disponibles dans le commerce montrent que le débit réel dans les conditions optimales est toujours inférieur à 5 Mbits/s, loin sous les 11 Mbits/s théoriques :

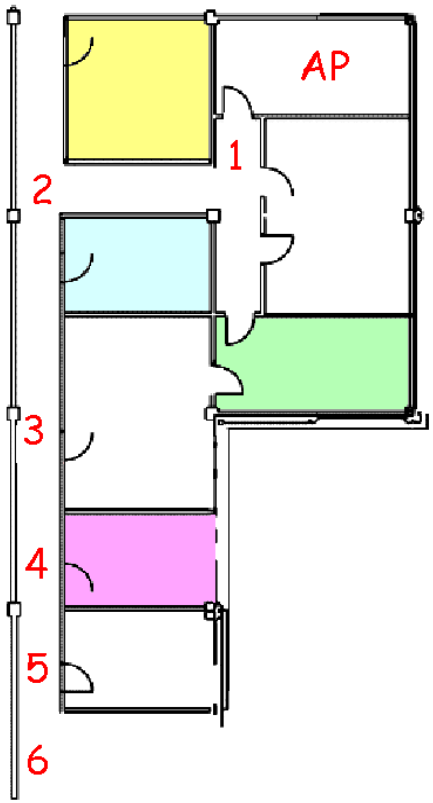


Exemples de portées obtenues avec différentes cartes d'interface

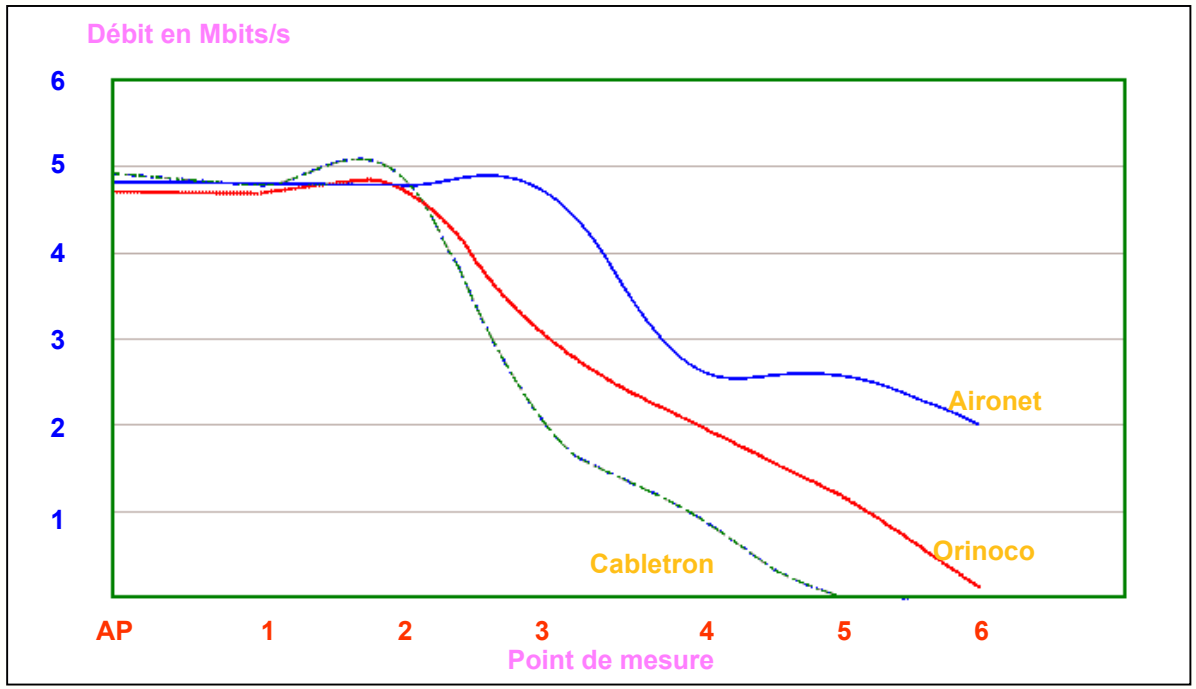
- Wifi est un média partagé, c'est-à-dire que le débit diminue si le nombre d'utilisateur dans la cellule augmente
- les problèmes de confidentialité sont résolus en partie par l'utilisation d'algorithmes de cryptage qui ralentissent le débit
- la norme Wifi prévoit 3 canaux (1,6 et 11) non chevauchants dans la bande de fréquence des 2.4 GHz
- en France, la situation est plus délicate et interdit pratiquement le chevauchement des cellules mais la législation évoluent

24- Influence de l'environnement sur la portée

En environnement de bureau avec des cloisons en briques, la portée est sensiblement plus faible qu'en espace libre.



Diminution du débit réel avec la distance



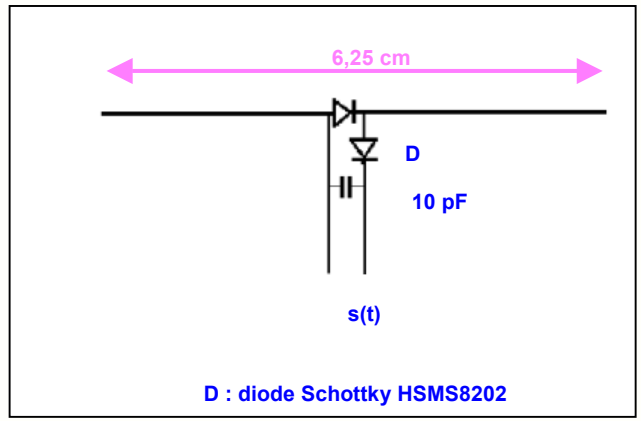
Remarque : la mise en place d'un réseau sans fil dans un bâtiment nécessite une bonne dose de patience et d'expertise dans la mise en place des diverses antennes, afin d'éviter les zones d'ombre et les interférences entre antennes.

25- La visualisation des échanges radio

Pour mettre en évidence l'émission d'une onde électromagnétique par l'interface radio, on utilise :

- une antenne dipôle demi-onde de longueur 6,25 cm
- suivie d'un détecteur crête doubleur de tension à 2 diodes Schottky

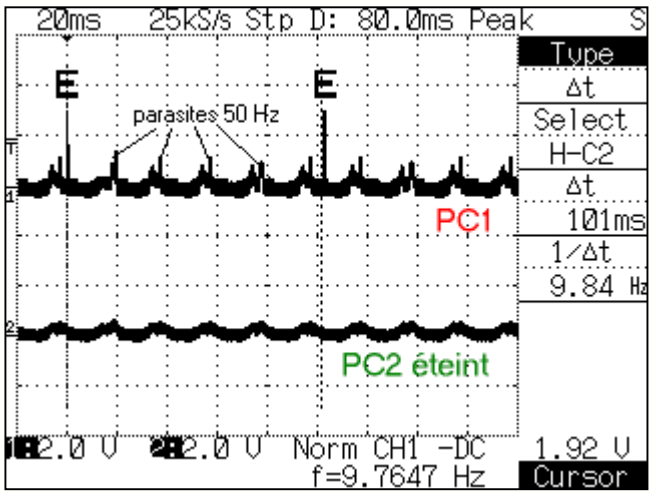
A chaque émission, une tension s(t) de quelques centaines de mV apparaît en sortie du détecteur crête.



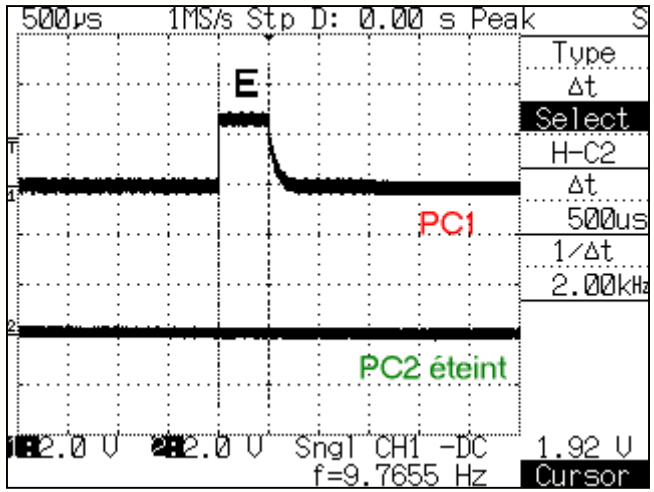
26- L'activité du point d'accès

Dans un réseau, les différentes stations doivent rester synchronisées pour la bonne gestion des échanges de données :

- le point d'accès transmet régulièrement des trames appelées «balise» contenant la valeur de son horloge
- les stations réceptrices vérifient la valeur de leur horloge et la corrigent pour rester synchronisées avec le Point d'Accès
- ceci compose les dérives entre PA et stations qui pourraient causer la perte de la synchronisation au bout de quelques heures



Émission des trames « balise » toutes les 100 ms



Zoom montrant la durée de la « balise » : 500us

La norme Wifi permet aussi la gestion de l'énergie afin d'étendre l'autonomie des batteries des appareils portables et prend en charge deux modes de gestion de l'alimentation :

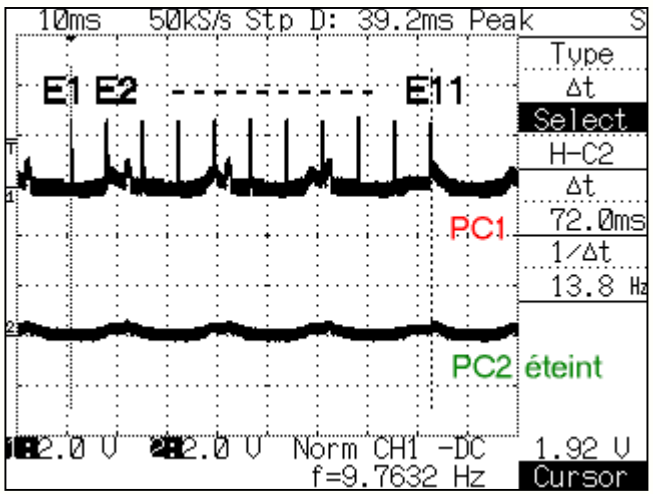
- le mode CAM (Continuous Aware Mode) : l'interface radio, toujours allumée, consomme de l'énergie en permanence
- le mode PSPM (Power Save Polling Mode) : la radio est mise en veille et le PA place en file d'attente les données destinées aux stations

Dans le mode PSPM, les émissions balises incluent des informations sur d'éventuelles données en attente de transmission. La radio cliente s'active au moment d'une émission balise du point d'accès, vérifie s'il y a ou non des données pour elle dans le tampon, reçoit le cas échéant ses données et repasse ensuite en veille.

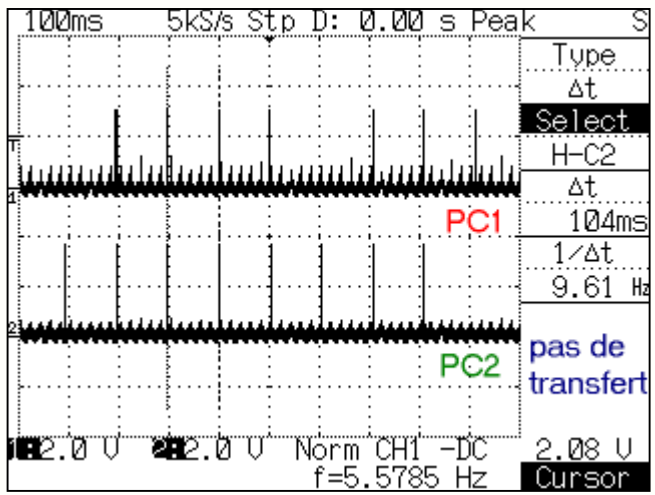
27- La constitution du réseau

Après démarrage d'une station, son raccordement au réseau passe par un certain nombre d'étapes :

- recherche par balayage du canal utilisé par le réseau le plus proche détecté par une mesure de niveau reçu
- synchronisation avec l'horloge du point d'accès ou des autres stations dans le cas du mode ad-hoc par écoute passive (attente d'une voie balise) ou par écoute active (en émettant une Probe Request Frame)
- authentification de la station par échange d'informations avec le point d'accès, où chacune des 2 parties prouve son identité par la connaissance d'un mot de passe
- association au réseau par échange d'informations sur les différentes stations et les capacités de la cellule et enregistrement de la station par le Point d'Accès



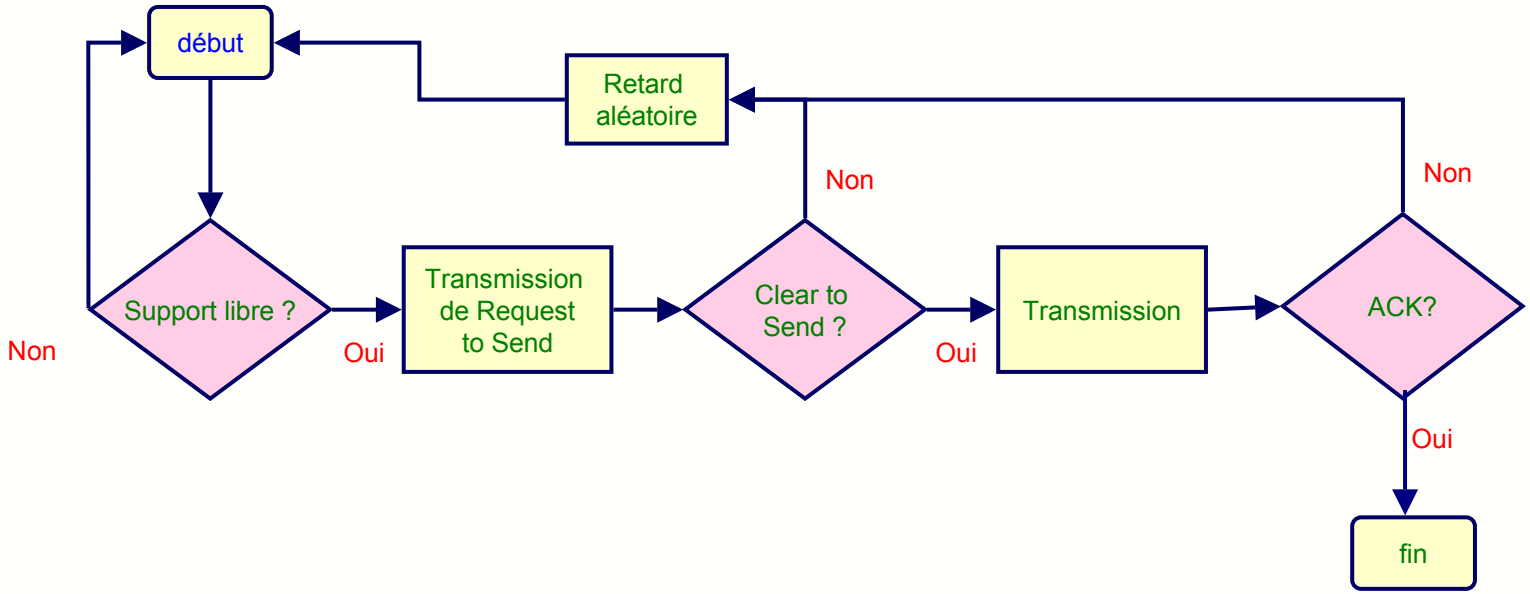
L'AP interroge les 11 canaux



Activité d'un réseau de 2 PC au repos

28- Le protocole d'échange de données

Le mécanisme d'échange utilisé pour la transmission de données est le Carrier Multiple Access with Collision Avoidance (CSMA/CA) :



La transmission par radio de données doit surmonter un certain nombre d'écueils :

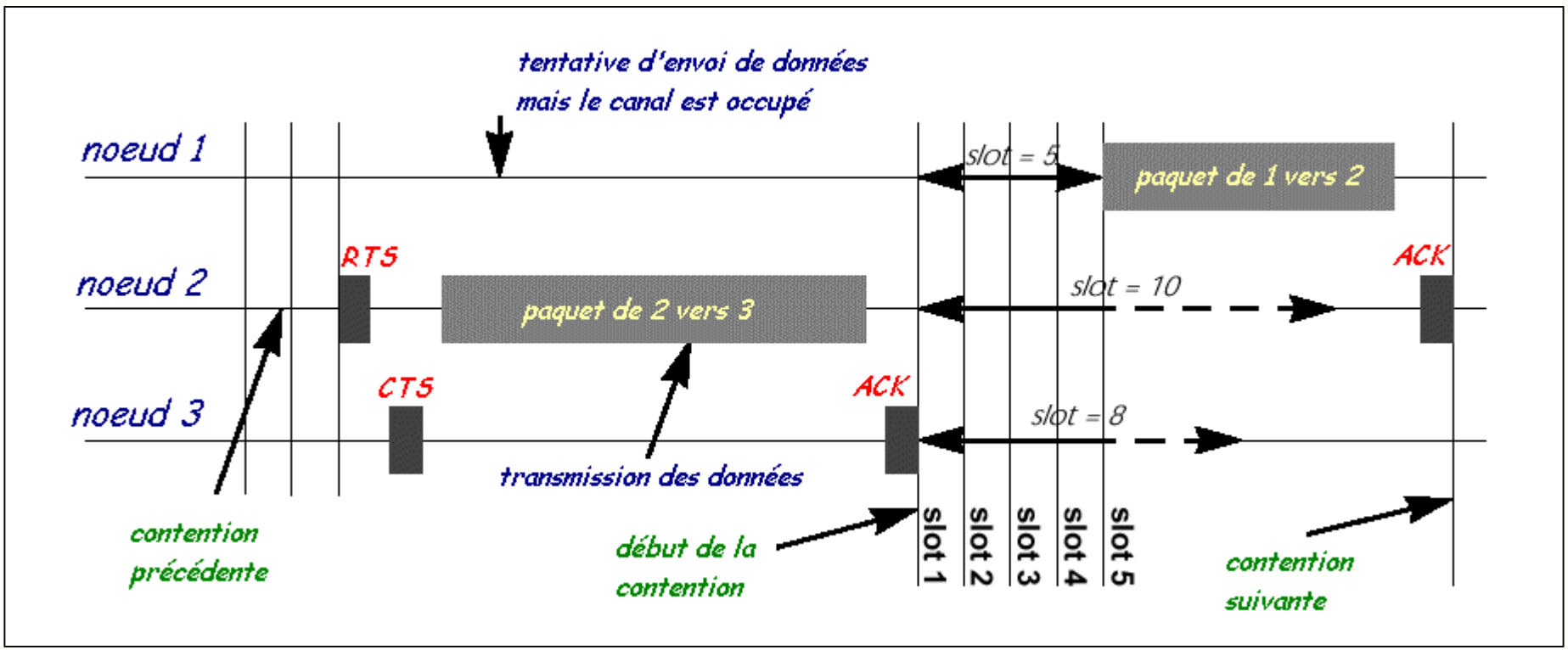
- il peut arriver que le canal Wifi soit occupé par un autre équipement, la transmission doit alors être différée
- le correspondant vers lequel les données doivent être envoyées peut être occupé par un autre échange, la transmission doit également être différée
- la transmission peut être perturbée par un brouillage ou l'émission Wifi d'un autre équipement : les données sont alors perdues et la transmission doit être renouvelée

Différents mécanismes ont été mis en place au niveau du protocole d'échange pour gérer ces différents problèmes.

29- La détection de l'occupation du canal

L'équipement qui démarre une transmission vérifie que le canal radio est libre par le mécanisme de Virtual Carrier Sense (sensation virtuelle de porteuse) :

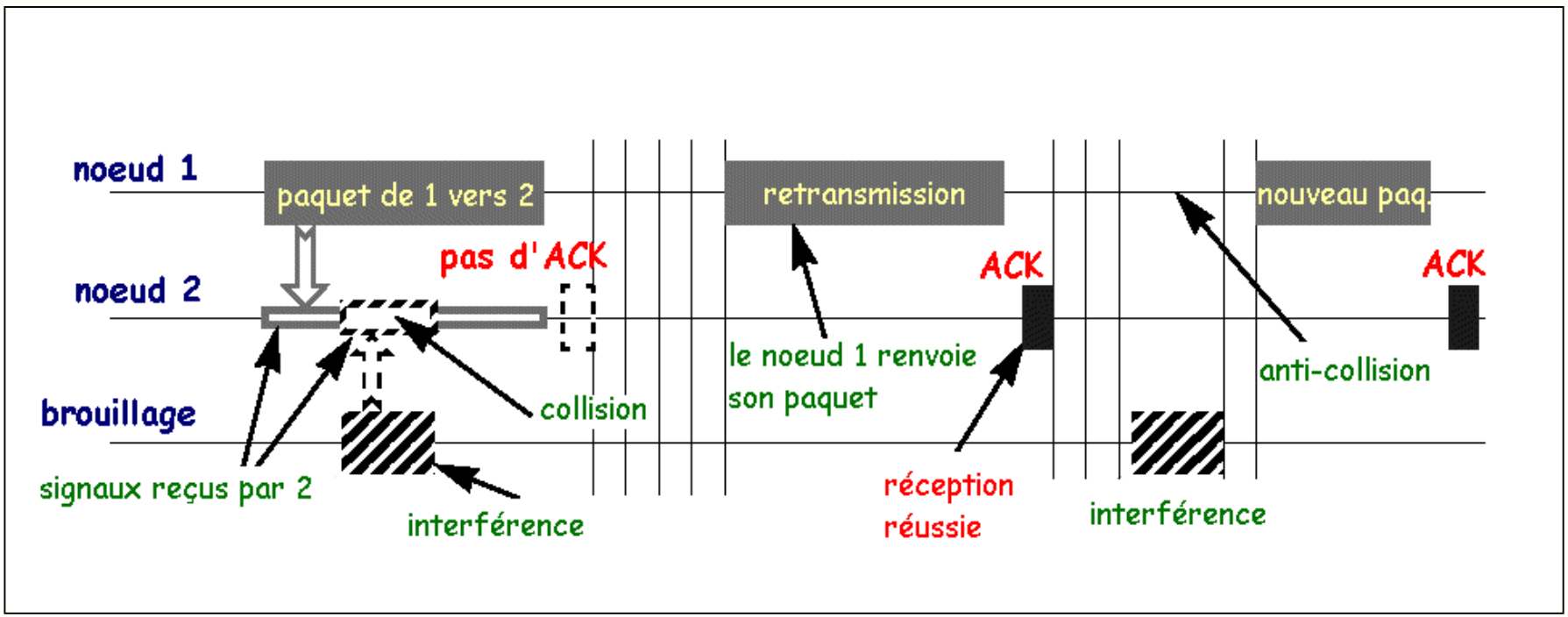
- la station 2 voulant émettre transmet d'abord un paquet de contrôle court (risque de collision faible) appelé RTS (Request To Send), qui donnera la source, la destination, et la durée de la transaction
- la station destination 3 répond (si le support est libre) avec un paquet de contrôle de réponse appelé CTS (Clear To Send), qui inclura les mêmes informations sur la durée
- après réception de CTS, la station peut transmettre ses données, dont la bonne réception est confirmée par un paquet ACK (Acknowledge)
- les différents nœuds mettent alors en œuvre un mécanisme de **contention** (retard de durée aléatoire) à l'issue duquel le nœud au retard le plus faible peut envoyer ses données



30- La protection contre les brouillages

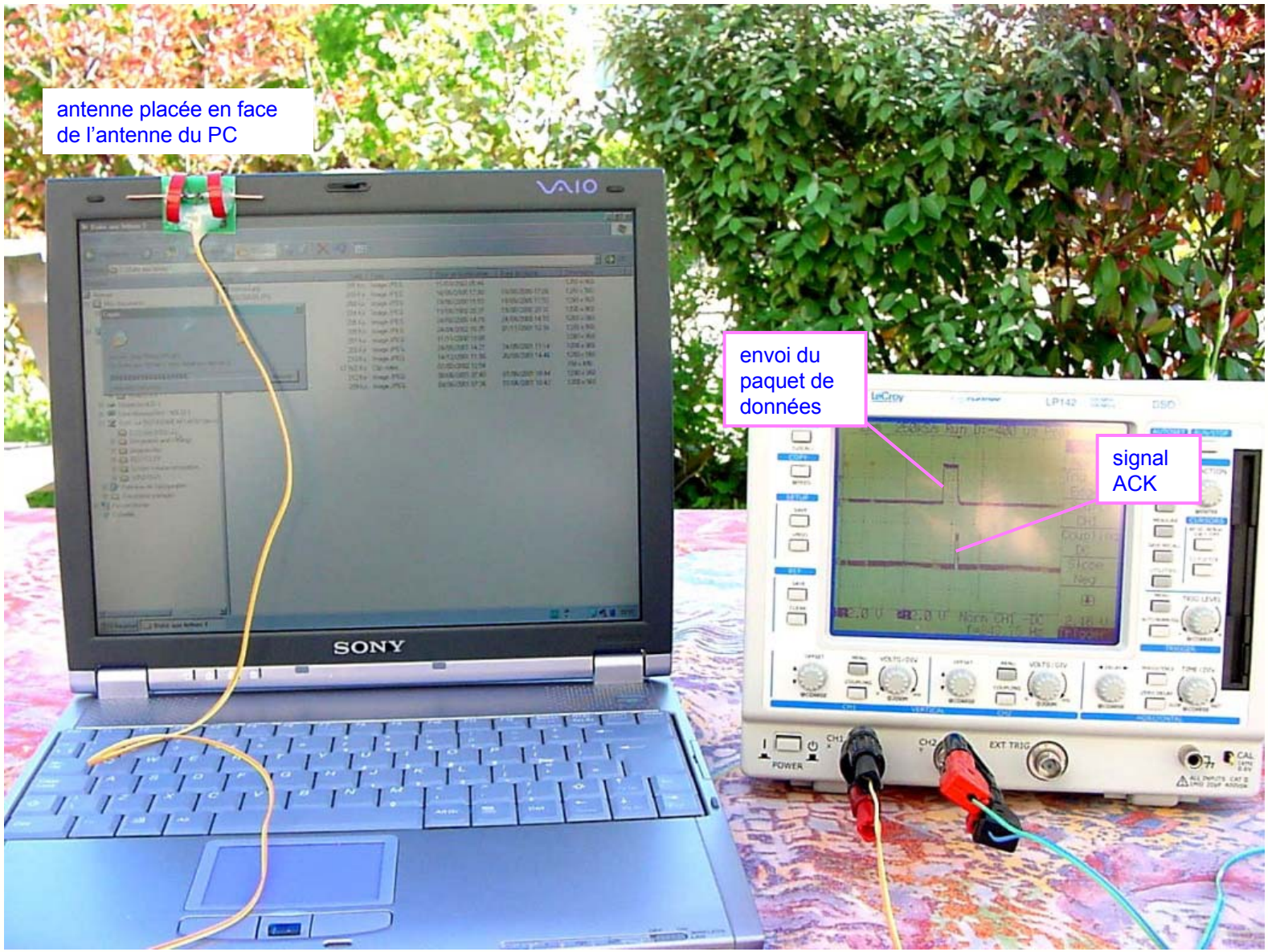
Les brouillages (four à micro ondes par exemple) empêchant la bonne réception d'un paquet de données sont gérés par le protocole :

- la station émettrice sait que la transmission ne s'est pas bien effectuée si elle ne reçoit pas de paquet ACK
- elle renvoie alors le même paquet, après un temps de contention aléatoire
- ce mécanisme se reproduit jusqu'à la réception d'un ACK qui valide la transmission
- la station émettrice peut maintenant procéder à l'envoi du paquet suivant



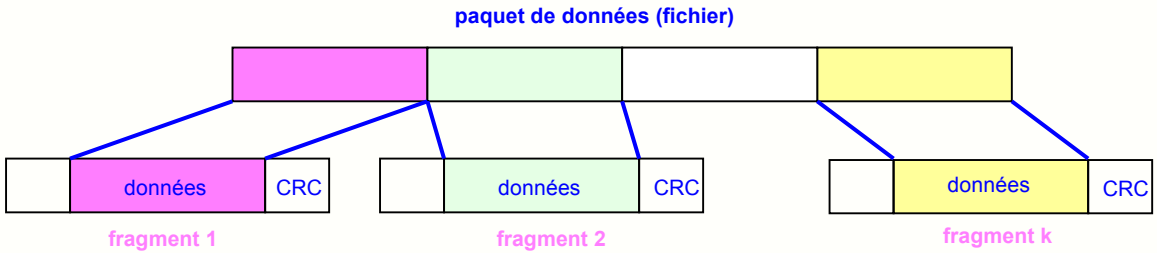
Remarque : ce mécanisme de retransmission ne ralentit pas trop les échanges si la taille des paquets est courte.

31- L'oscillogramme des échanges



32- La fragmentation des données

Pour éviter de ralentir la transmission par la perte de longs paquets, ceux-ci sont divisés par fragmentation en paquets plus courts, qui ont une meilleure probabilité d'être transmis par radio sans pertes.

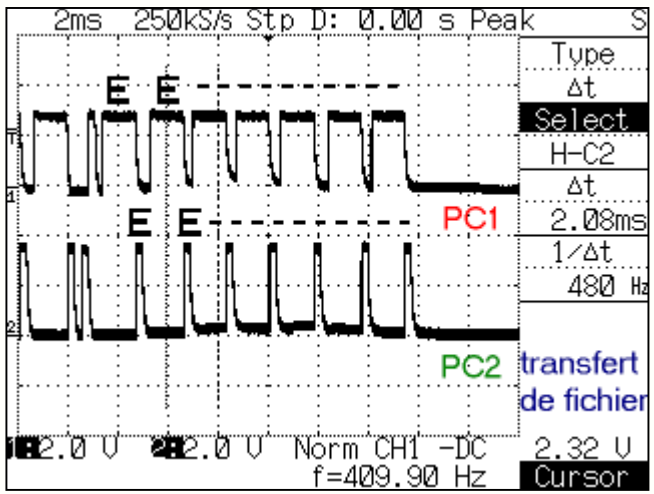


Taille maximale d'un paquet :

- 2312 octets de données
- 30 octets en-tête …
- total 2342 octets, soit N=18736 bits
- durée N/D = 1,7 ms max à 11 Mbits/s

Les oscillogrammes ci-dessous représentent l'activité radio lors de l'échange d'un fichier entre 2 PC portables :

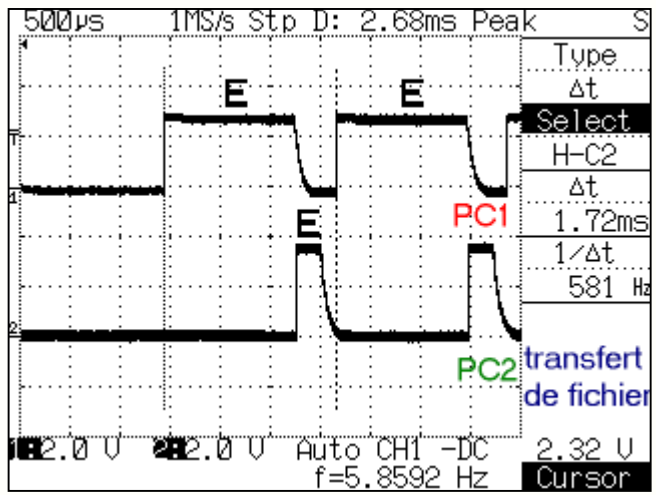
- PC1 envoie des données à PC2 par paquets
- PC2 valide la réception de chaque paquet par un ACK



PC1 envoie des données vers PC2

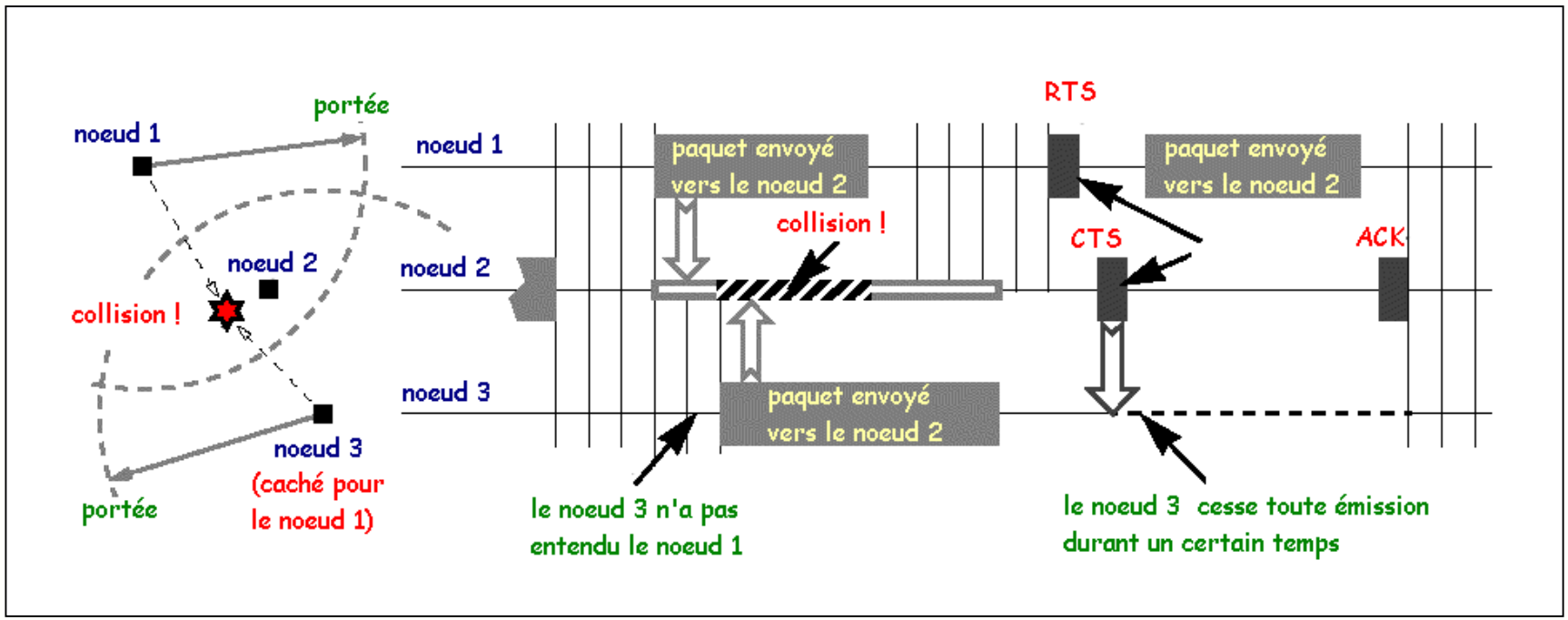
Durée du paquet 1,2 ms

Acquittement : 0,2 ms



33- Le problème des stations cachées

Dans un réseau radio, la portée limitée des interfaces pose le problème des stations cachées accessibles par certaines interfaces et inaccessibles à d'autres.



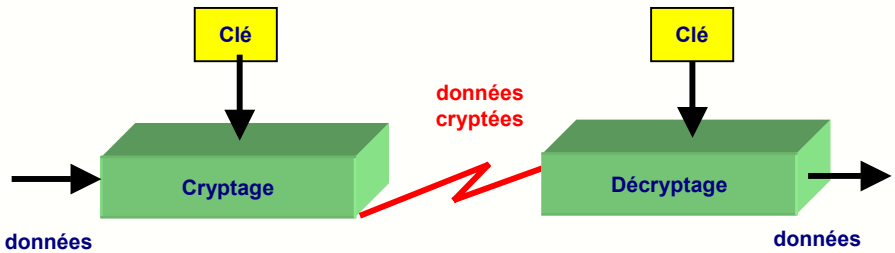
Dans l'exemple ci-dessus, la station n° 3 est une station cachée pour la n° 1. Pour éviter les collisions :

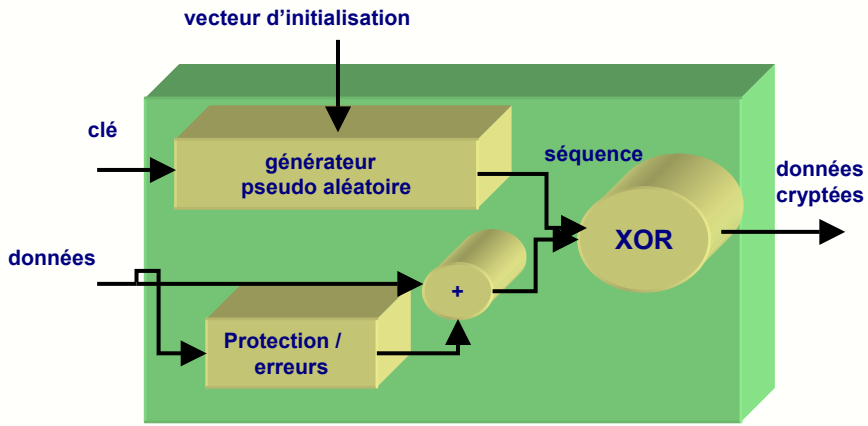
- la station n°1 voulant émettre transmet le paquet court de contrôle RTS, qui donnera la source, la destination, et la durée de la transaction
- la station n°2 répond (si le support est libre) avec un paquet de contrôle de réponse CTS qui inclura les mêmes informations sur la durée
- toutes les stations recevant soit le RTS ou le CTS et en particulier la n°3 sauront ainsi que le support radio est occupé et arrêteront d'émettre pendant la durée indiquée dans le paquet RTS
- il est également à noter que grâce au fait que le RTS et le CTS sont des trames courtes (30 octets), le nombre de collisions est réduit, puisque ces trames sont reconnues plus rapidement que si tout le paquet devait être transmis

34- La sécurité des échanges

Diverses méthodes permettant de sécuriser les échanges peuvent être mis en place :

- l'identificateur de réseau SSID (Service Set Identifier) qui permet de donner au réseau un nom unique de manière à ce que seules les personnes autorisées puissent y accéder
- la liste de contrôle d'accès permet de spécifier les adresses MAC des utilisateurs autorisés à utiliser le réseau sans fil
- le cryptage WEP (Wireless Equivalent Protocol) optionnel protège les données contre l'écoute clandestine en cryptant les transmissions entre le point d'accès et les périphériques





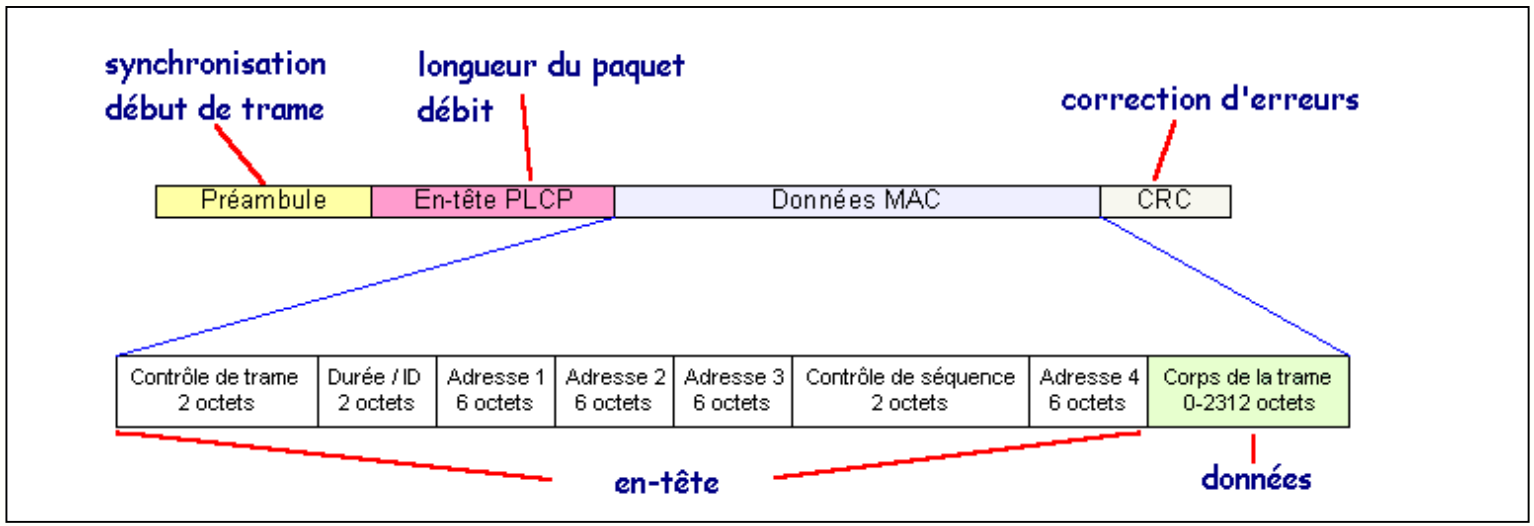
Le cryptage des données WEP est obtenu par l'utilisation de l'algorithme RC4 basé sur un générateur de nombres pseudo aléatoires initialisé par une clé secrète partagée :

- à partir du vecteur d'initialisation de 24 bits et d'une clé choisie par l'utilisateur (40 ou 104 bits), le générateur de nombres pseudo aléatoires produit une séquence de bits de 64 ou 128 bits
- cette séquence pseudo aléatoire est mélangée au données lors de la transmission, les en-têtes de paquets n'étant pas cryptés
- l'attaque de cet algorithme est rendue difficile par le fait que chaque paquet de données est envoyé avec un vecteur d'initialisation qui relance le générateur de nombres pseudo aléatoires
- cette resynchronisation pour chaque message est de toutes façons nécessaire compte tenu du fait que des paquets peuvent être perdus lors de la transmission

Annexe 1- Le format des trames

Le standard Wifi met en œuvre essentiellement trois types de trames :

- les trames de données, utilisées pour la transmission des données
- les trames de contrôle, utilisées pour contrôler l'accès au support (RTS, CTS, ACK)
- les trames de gestion, transmises de la même façon que les trames de données pour l'échange d'informations de gestion



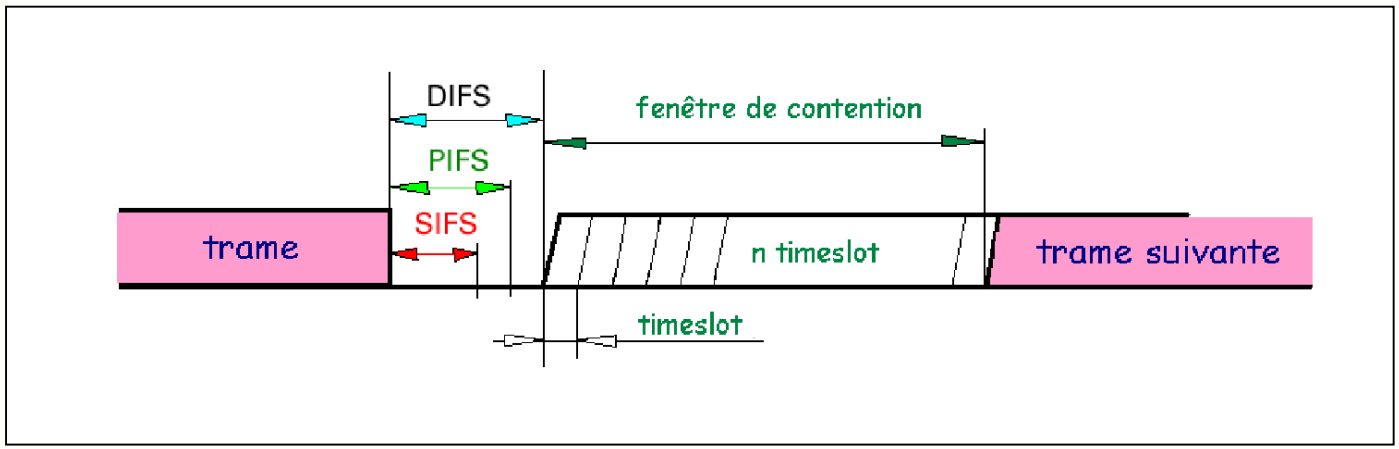
Toutes les trames 802.11 renferment les composants suivants :

- le préambule formé de la Synch, séquence de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne appropriée , et pour corriger l'offset de fréquence et de synchronisation et du Start Frame Delimiter, suite de 16 bits 0000 1100 1011 1101 utilisée pour définir le début de la trame.
- l'en-tête PCLP, toujours transmis à 1 Mbits/s, contient des informations logiques utilisées par la couche physique pour décoder la trame comme le nombre d'octets que contient le paquet et l'information de taux
- l'en-tête MAC, qui précise entre autres s'il s'agit d'une première transmission ou non du paquet, si le paquet est crypté par l'algorithme WEP ou pas, les adresses de l'expéditeur, du destinataire, du point d'accès et le numéro du fragment si le paquet de données a été fragmenté
- le code de redondance cyclique permettant de détecter et de corriger un certain nombre d'erreurs sur 4 octets

Annexe 2- Les espaces entre trames

Le standard définit 4 types d'espace en entre deux trames, utilisés pour leurs différentes propriétés :

- le SIFS (Short Inter Frame Space) de 28 µs est utilisé pour séparer les transmissions appartenant à un même dialogue (par exemple Fragment – ACK).
- le PIFS (Point Coordination IFS) de 78 µs est utilisé par le AP pour obtenir l'accès prioritaire au support
- le DIFS (Distributed IFS) de 128 µs est l'intervalle utilisé par une station voulant commencer une nouvelle transmission
- le EIFS (Extended IFS) est l'intervalle le plus long utilisé par une station recevant un paquet qu'elle ne comprend pas, pour éviter que la station qui ne comprend pas l'information de durée ne provoque de collision avec un futur paquet



A la fin de la transmission d'un paquet de données, le support redevient libre, et il est possible que deux stations démarrent un échange simultanément

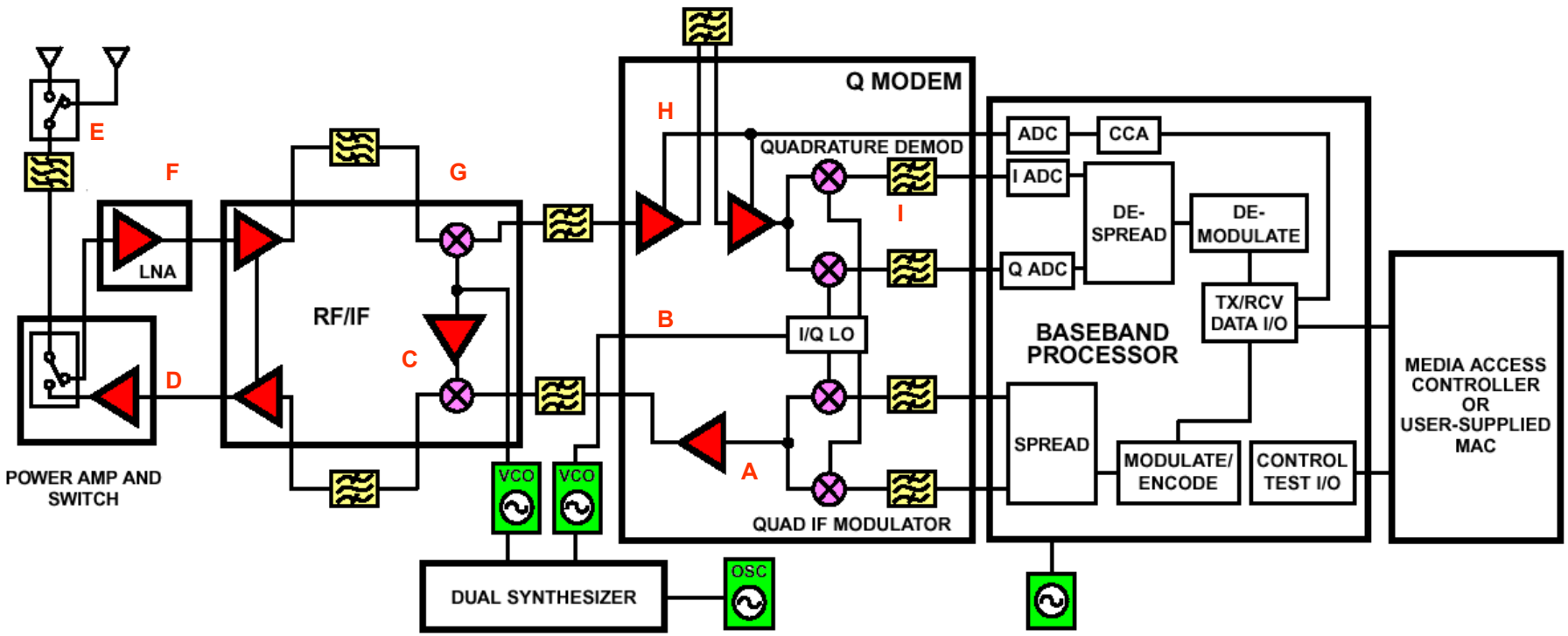
Pour éviter ce genre de situation aboutissant à la collision des RTS que la norme IEEE802.11 a mis en place une temporisation aléatoire appelée contention ou back off :

- chaque station choisit un nombre aléatoire entre 0 et N et attend ce nombre de slots avant d'accéder au support
- le back off est exponentiel, c'est-à-dire qu'à chaque fois qu'une station choisit un slot et provoque une collision, la valeur maximale N est augmentée exponentiellement

Annexe 3 – Exemple de circuit pour interface Wifi

Les circuits d'une interface Wifi sont ceux qu'on retrouve dans tous les systèmes de communication numérique :

- pour l'émetteur : modulation QPSK à quadrature (A) d'une porteuse auxiliaire (B), changement de fréquence vers le canal (C), amplification RF (D)
- pour le récepteur : sélection de l'antenne (E), amplification à faible bruit (F), changement de fréquence (G), amplification et filtrage fi (H), démodulation à quadrature (I)



Annexe 4 – Exemples d'interfaces Wifi

Interface Wifi PCMCIA

Adaptateur de carte PCMCIA pour PC

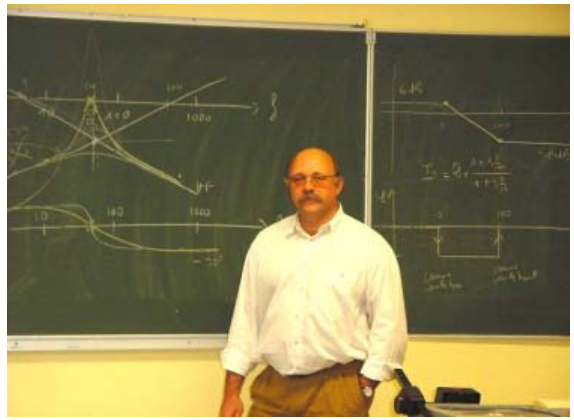
Annexe 5 – Exemple d'antenne pour réseau Wifi

L'ART a récemment assoupli la législation concernant Wifi et des réseaux locaux en extérieur commencent à se constituer :

- pour une liaison point à point, une interface Wifi équipée d'un ampli RF et d'une antenne directive permet de couvrir 8 à 33 km
- avec une antenne directive et une puissance de 100 mW bien placée, on peut couvrir de 400 mètres à 3 kilomètres
- les antennes omnidirectionnelles sont utilisées pour augmenter la portée et donc la taille de la cellule

Antenne directive pour liaison point à point

Antenne omnidirectionnelle



Maison des Tanneurs Strasbourg

FIN