Les réseaux locaux sans fil (RLANs)

1. INTRODUCTION : LA NORME IEEE802.11B

1.1 INTERET DES LANS SANS FIL (RLANS)

Les LANs permettent de connecter des stations à un réseau numérique de données avec des débits assez élevés et un matériel de raccordement peu coûteux, aussi bien dans les secteurs publics que privés. De nos jours, pratiquement chaque entreprise dispose d'un LAN de type Ethernet, donc filaire. Ethernet (norme IEEE 802.3) est le protocole de base le plus fréquemment utilisé pour les LANs filaires. Cependant, ces LANs sont dépendants de l'infrastructure physique et câblée du bâtiment, ce qui est un problème pour les utilisateurs qui recherchent à être mobiles dans les entreprises.
Les LANs sans fil sont particulièrement sollicités par les hôpitaux (gestion des fichiers des patients), les universités (LANs extrêmement sollicités sur les campus), les aéroports, les chantiers de construction, les usines (gestion de la production, gestion des stocks, inventaires). En effet, tous ceux là trouvent dans les LANs sans fil des solutions particulièrement adaptées.

Pour les entreprises diverses, les LANs sans fil sont une bonne solution pour des applications telles que :

- extension à des LANs filaires
- sites difficiles à câbler (bâtiments anciens, musées, monuments historiques…)
- réalisations temporaires (pour des périodes de surcharge ou des projets spéciaux)
- mise en place rapide de réseaux
- environnement en évolution constante
- LAN préinstallés, prêts à l'emploi ou devant être évolutifs
- accès LAN aux utilisateurs d'ordinateurs mobiles
- liaisons par antennes extérieures pour remplacement rapide de ligne louée
- conférences…

1.2 LA NORME IEEE 802.11B

Il existe plusieurs normes indépendantes et incompatibles entre elles provenant de nombreux constructeurs, mais la plupart des constructeurs ont rejoint l'IEEE pour créer une norme pour les LANs sans-fil. Cette norme s'appelle IEEE 802.11b.

Les caractéristiques générales de la norme 802.11b sont :

- Famille technologique : technologie radio à étalement de spectre

- Plage de fréquence utilisée par cette norme : 2,4000-2,4970 GHz. En France, la gendarmerie se réserve une partie de cette plage de fréquence, faisant que la plage disponible est réduite à l'espace 2,4465-2,4835 GHz. Il est urgent en France de libérer plus de canaux sur la bande des 2,4GHz, car cela limite réellement les possibilités d'installation et d'évolution du LAN sans fil. Dans le monde la France est avec le Japon un pays très restrictif sur cette bande de fréquence. Paradoxalement 4 canaux seulement sont officiellement disponibles en France contre 11 à 13 dans la plupart des autres pays. L'utilisation de cette bande de fréquence est libre et ne nécessite donc pas de licence.

Pays	Plage de fréquence (en GHz)
USA	2,4000-2,4835
Europe	2,4000-2,4835
Japon	2,4710-2,4970
France	2,4465-2,4835
Espagne	2,4450-2,4750

Figure 9 : Bande de fréquence allouée en fonction du pays pour la norme 802.11

- 14 canaux distincts sont définis dans cette plage de fréquence
- Méthode d'étalement de spectre : FHSS ou DSSS (saut de fréquence ou séquence directe)
- Limite de la puissance effective d'émission à 100 mW ce qui ne permet d'établir des liaisons que sur 1 km au maximum en vue dégagée (et en étant optimiste !).
  La norme IEEE 802.11b est entièrement définie par les 2 couches les plus basses du modèle OSI (voir plus loin).

Pour une description plus précise, vous pouvez trouver la norme complète sur le site IEEE : c'est un document rendu public pour favoriser l'utilisation de cette norme.

2. TOPOLOGIES DES RESEAUX IEEE 802.11B

Un LAN sans-fils peut être utilisé pour remplacer ou étendre un LAN filaire. Nous allons décrire quelles sont les différentes topologies de réseau possibles avec la norme 802.11.

2.1 RESEAU AD-HOC

La topologie basique d'un réseau 802.11 est représenté en Figure 2. Un BSS (Basic Service Set) consiste en 2 nœuds sans fil ou plus, ou en des stations qui se reconnaissent et qui communiquent chacune entre-elles. Ces stations peuvent être des PC portables ou des PC fixes. Dans la topologie la plus basique, les stations communiquent directement entre-elles en point à point (peer to peer), tout en partageant une certaine cellule radio limitée en espace. On appelle ce réseau un réseau ad-hoc, ou aussi un IBSS (Independant Basic Service Set).
Ce réseau ad-hoc simplifié permet de réaliser rapidement un petit réseau entre 2 stations sans fils comme par exemple 2 consultants sur le site d'un client qui ont besoin d'échanger des données.

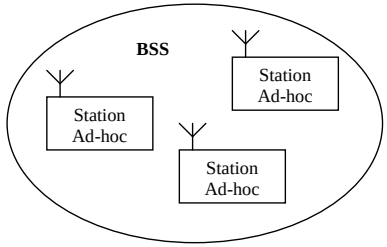


Figure 10 : Communication point à point dans un réseau Ad-hoc

2.2 RESEAU AVEC POINT D'ACCES

Dans la plupart des cas, le BSS renferme un Point d'Accès (AP). La fonction principale d'un AP est de former un pont entre le LAN filaire et le LAN sans-fil. Celui-ci est donc relié au LAN filaire par un câble Ethernet et aux stations du LAN sans fil par radio. Un point d'accès agit en fait comme une passerelle entre le protocole CSMA/CD d'Ethernet et le protocole CSMA/CA du sans fil.
En présence d'un AP, les stations ne communiquent plus en point à point : toutes les communications entre les stations ou entre une station et un LAN filaire passent par l'AP. Les APs ne sont pas mobiles, et font partie du réseau filaire.

Lorsqu'on regroupe une série de BSS qui se superposent (chacun contenant un AP), on forme un ESS (Extended Service Set), représenté en Figure 3. Les APs sont reliés entre-eux par un Système de Distribution (DS). Ce DS est dans la majorité des cas un LAN Ethernet.
Les nœuds mobiles peuvent errer entre les différents APs, on parle alors de "roaming" ; couvrir un campus entier (par exemple) par un LAN sans fil, c'est à dire rester connecté au réseau en tout point du campus est ainsi possible.

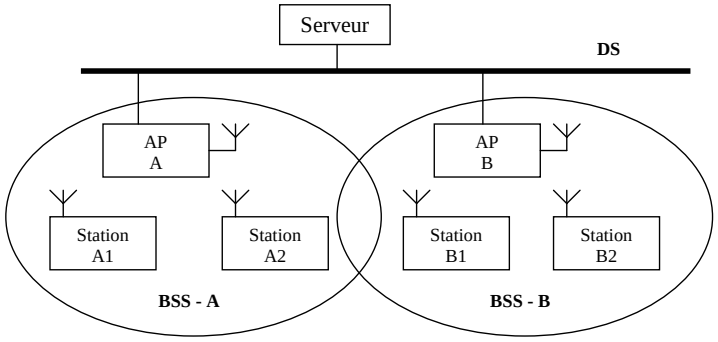


Figure 11 : ESS : Réseau avec points d'accès

2.3 FONCTIONNEMENT : COMMENT UNE STATION REJOINT-ELLE UN BSS ?

2.3.1 Synchronisation

Quand une station veut accéder à un BSS ou à un IBSS, soit après démarrage ou après un passage en mode de veille, la station a besoin d'informations de synchronisation de la part du point d'accès (ou des autres stations dans le cas d'un réseau ad-hoc). Les stations doivent obligatoirement rester synchronisées ; ceci est nécessaire pour garder la synchronisation au cours des sauts (dans le cas de la méthode d'étalement de spectre à saut de fréquence) ou pour d'autres fonctions comme l'économie d'énergie.

La station peut obtenir ces informations par une des 2 techniques suivantes :

- **Ecoute active** : dans ce cas, la station essaie de trouver un point d'accès en transmettant une trame de demande de synchronisation (Probe Request Frame) et attend une trame "balise" (Beacon Frame) de la part du point d'accès.
  La trame balise est une trame contenant les informations de synchronisation. Elles contiennent en fait la valeur de l'horloge du point d'accès au moment de la transmission (notons que c'est le moment où la transmission à réellement lieu, et non quand la transmission est mise à la suite des transmissions à faire. Puisque la trame balise est transmise selon les règles du CSMA, la transmission pourrait être différée significativement).
- **Ecoute passive** : dans ce cas, la station attend simplement de recevoir une trame "balise" (Beacon Frame), celle-ci étant envoyée périodiquement par le point d'accès toutes les 100ms par exemple. Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrige pour rester synchronisées avec l'horloge du point d'accès. Ceci évite des dérives d'horloge qui pourraient causer la perte de la synchronisation au bout de quelques heures de fonctionnement.

La première technique est utilisée lorsque la station veut se connecter à un BSS pour la première fois (ou pour se reconnecter). La deuxième est utilisée pour garder la synchronisation avec le point d'accès une fois que la station a déjà été associée au BSS.

2.3.2 L'authentification

Une fois qu'une station a trouvé un point d'accès et une cellule (BSS) associée, le processus d'authentification s'enclenche (voir chapitre sur la sécurité).

2.3.3 L'association

Une fois la station authentifiée, le processus d'association s'enclenche. Celui-ci consiste en un échange d'informations concernant les différentes stations, les capacités de la cellule et enfin l'enregistrement de la position actuelle de la station par le point d'accès.
C'est seulement après la fin du processus d'association que la station peut transmettre et recevoir des trames de données.
Etant associée à une cellule, la station reste synchronisée avec le point d'accès par écoute passive. Le point d'accès transmet régulièrement les trames appelées trames "balises", qui

contiennent la valeur de son horloge interne et qui permettent aux stations de synchroniser leur horloge.

2.3.4 Le roaming

Le roaming est le processus de mouvement d'une cellule vers une autre sans perdre la connexion au réseau. Cette fonction est similaire au "handover" des téléphones portables, mais avec deux différences majeures :

- Sur un LAN, qui est basé sur une transmission par paquets, la transition d'une cellule à une autre doit être faite entre deux transmissions de paquets, contrairement à la téléphonie où la transition peut subvenir au cours d'une conversation. Ceci rend le roaming plus facile dans les LANs sans fil, mais…
- Dans un système vocal, une déconnexion temporaire peut ne pas affecter la conversation, alors que dans un environnement de paquets, les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Le standard 802.11 ne définit pas intégralement le processus de roaming, mais en définit cependant les règles de base (les processus sont différents selon les constructeurs). Celles-ci comprennent l'écoute active ou passive, le processus de ré-association (une station qui passe d'un point d'accès à un autre sera associée au nouveau point d'accès).
D'autre part le roaming n'est possible que si ces points d'accès sont configurés avec le même "Network ID" (le nom du réseau).

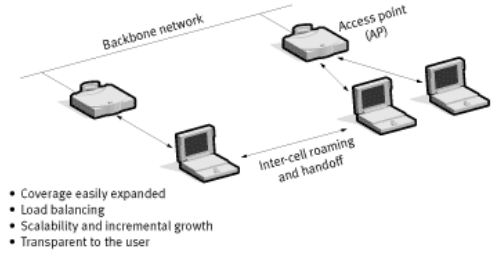


Figure 12 : Le roaming : passage d'un point d'accès à un autre

3. ANATOMIE D'UN LAN SANS-FIL 802.11B

3.1 LE MODELE OSI

Grâce au modèle de référence OSI de l'ISO, on peut facilement représenter ce que définit la norme 802.11. Comme tous les protocoles 802 de l'IEEE, le protocole 802.11 se situe dans les couches basses du modèle OSI. En l'occurrence, la norme 802.11 définit seulement les deux couches les plus basses du modèle OSI. Ainsi sont définies la couche physique PHY et la sous-couche MAC (Medium Access Control) de la couche liaison de données.

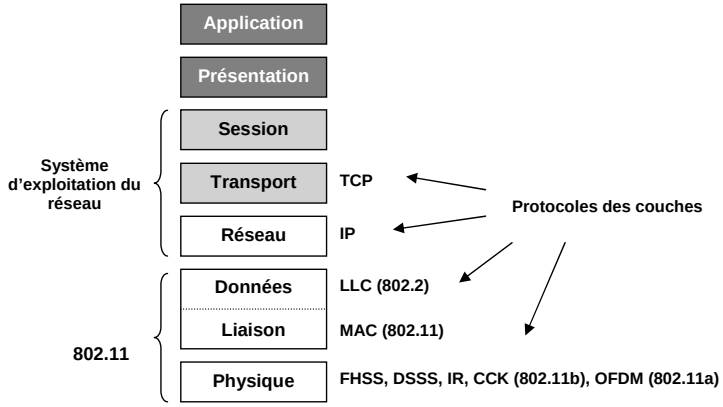


Figure 13 : 802.11 dans le modèle OSI

La **couche physique** gère essentiellement la transmission des bits sur le support de communication, les niveaux électriques et les modulations. Exemples de normes classiques pour la couche physique : protocole V24 (ou RS232C), protocole V11 (ou RS422)…
Notons ici que l'architecture de base, les caractéristiques et services du protocole **802.11b** sont définis par le protocole 802.11. Les spécifications du **802.11b** affectent seulement la couche physique en ajoutant un taux de transfert plus rapide et des connexions plus robustes.

La **couche liaison de données** gère la fiabilité du transfert des informations, le découpage en trames, la protection contre les erreurs, les trames d'acquittement et la régulation du trafic. Cette couche se compose de 2 sous-couches :

- La **sous-couche liaison logique LLC** (Logical Link Control) : elle gère les erreurs, le trafic, le flux, et la liaison au support. Dans le cas d'un LAN 802.11, cette sous-couche est la même que pour un LAN filaire. Elle est définie par le protocole 802.2 (adressage 48 bits). Elle est reprise simplement pour permettre le pontage entre les LANs sans fil et les LANs filaires de l'IEEE. Exemples de protocoles LLC : SDLC, HDLC, LAP, LLC…
- La **sous-couche d'accès au support MAC** (Medium Access Control) : elle gère le partage du support. En plus des fonctions habituellement rendues par la couche MAC, la couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme la fragmentation des données, les retransmissions de paquet et les accusés de réception. Exemples de protocoles MAC : ALOHA, 802.3 (CSMA/CD), CSMA/CA, 802.4 (bus à jeton), 802.5 (anneau à jeton)…

La **couche réseau** n'est pas gérée par 802.11. Détailler cette couche nous permet de voir ce que 802.11 n'intègre pas : la couche réseau gère l'acheminement des informations (routage, contrôle de flux), les adressages, l'interconnection de réseaux hétérogènes et l'établissement et la libération des connexions. Exemples de protocoles de la couche réseaux : IP (Internet Protocol), X25…

3.2 SYNOPTIQUE GENERAL : DES ONDES AU FIL

Pour mieux comprendre comment fonctionne chaque élément d'un LAN sans fil, il est utile de détailler chaque partie constitutive d'un système sans fil 802.11 dont le synoptique général est représenté ci-dessous en figure 6.

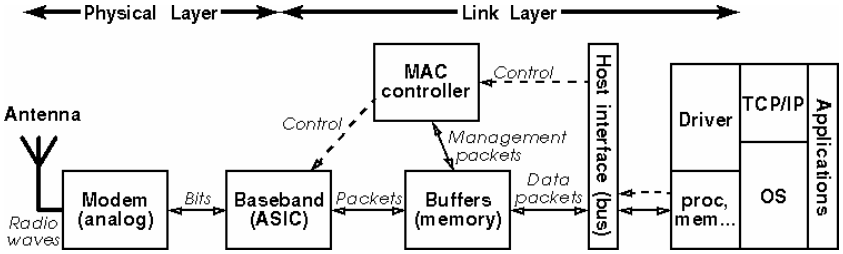


Fig. 14 : Synoptique général d'un système sans-fil 802.11

Nous allons décrire chaque partie séparément.

3.2.1 L'équipement radio

Un réseau radio est une multitude de nœuds appelés à communiquer en utilisant les ondes radioélectriques pour porter l'information grâce à des équipements radio. La plupart des équipements radio se présentent sous forme de carte (ISA, PCI ou PCMCIA) à brancher directement sur un PC.

Un équipement radio est composé de deux parties principales :

- le **modem** (modulateur/démodulateur) **radio**, qui constitue la partie devant transmettre à l'aide d'une modulation le signal sur la bonne fréquence et inversement recevoir l'information captée et donc effectuer la démodulation. Il est composé principalement de parties analogiques (antenne, amplificateurs, convertisseurs de fréquences, oscillateurs, filtres) et d'un démodulateur (généralement un ASIC). Tout ce petit monde est encapsulé dans un blindage métallique pour protéger le PC des radiations à haute fréquence. Les caractéristiques principales du modem sont : la bande de fréquence, le taux de transfert, la modulation et la puissance transmise.
- le **contrôleur MAC**. Le protocole MAC est principalement implémenté dans un ASIC et/ou un microcontrôleur sur la carte même, avec parfois certaines fonctionnalités gérées directement par le driver sur le PC. La carte contient aussi quelques blocs mémoire pour le contrôleur MAC afin de stocker les paquets entrants et sortants (buffers) et autres données (configuration, statistiques...). Les caractéristiques principales du contrôleur MAC sont le format des paquets (taille, en-têtes), la méthode d'accès au canal, et des fonctionnalités purement liées au management de réseau.

3.2.2 La "host interface"

On trouve ensuite la "host interface" qui fait le lien de la carte au PC par un de ses bus (ISA, PCI, Pcmcia...) ou de ses ports de transmission (séquentiel, parallèle, USB ou Ethernet). Cette

interface permet au logiciel (la plupart du temps le driver) de communiquer avec le contrôleur MAC et la majeure partie du temps directement avec la mémoire de la carte (le logiciel écrit des paquets à un emplacement spécifique, et le contrôleur les lit et les envoie). La caractéristique principale de l'interface est principalement la vitesse (E/S, mémoire partagée ou accès direct à la mémoire (DMA)) et la capacité de traiter des demandes en parallèle.

3.2.3 Le driver

Avec tous les systèmes d'exploitation modernes, l'application n'accède pas directement au matériel mais utilise un API standard. Le système d'exploitation a besoin d'un driver pour interfacer le matériel avec le protocole réseau (TCP/IP, NetBeui, IPX...). La fonction principale du driver est de gérer le matériel et de répondre à ses interruptions.

4. LA COUCHE PHYSIQUE : LE MODEM RADIO

Le standard définit actuellement une seule couche MAC qui interagit avec 3 couches physiques :

- FHSS Frequency Hopping Spread Spectrum
- DSSS Direct Sequence Spread Spectrum
- l'infrarouge

4.1.1 Le FHSS ou saut de fréquence

La bande des 2.4 GHz est divisée en 79 canaux de 1 MHz chacun. Cette technique est basée sur le saut de fréquence périodique de l'émetteur (toutes les 20 à 400ms), suivant un ordre cyclique prédéterminé. Le fait de ne jamais rester sur le même canal accroît fortement l'immunité au bruit. Dans le cas de canaux encombrés, cela permet d'avoir au final un bon moyennage et d'utiliser au mieux toute la bande passante allouée. Cette technique rend difficile l'interception de trames. L'avantage de cette technique est aussi que même en perdant quelques "sauts" (ou hop) suite à des interférences très localisées, on peut tout de même retrouver le signal. D'un autre côté, si le bruit de fond est plus puissant que le signal émis, il n'y a rien à faire. De plus, cette méthode de transmission est relativement simple mais elle est limitée par son débit maximum de 2 Mbits/s. Enfin, elle introduit une certaine complication au niveau MAC, ce qui se traduit en termes de multiplication d'en-têtes et donc de réduction de débit.

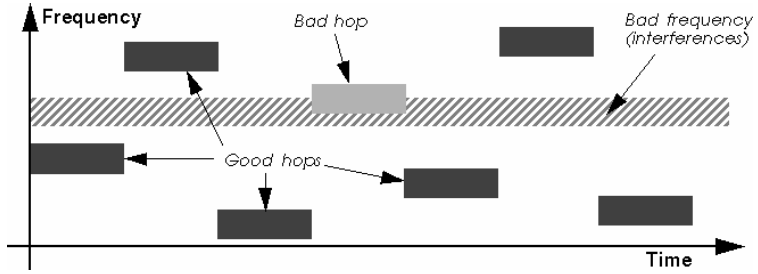


Figure 15 : FHSS

4.1.2 Le DSSS ou séquence directe

La technique de la séquence directe divise la bande des 2.4 GHz en 14 canaux de 22 MHz chacun. Les données sont envoyées uniquement sur l'un des 14 canaux. Pour minimiser le bruit de fond et les interférences locales, une technique dite de "chipping" est utilisée. Elle consiste à convertir les bits de données en une série de bits redondants. Le bit 1 sera remplacé par une succession de 11 bits 0 ou 1 (appelée code PN) pendant le même temps de transmission. Le bit 0 sera remplacé par le complémentaire de la succession de bits utilisée pour le bit 1 (voir ci-dessous).

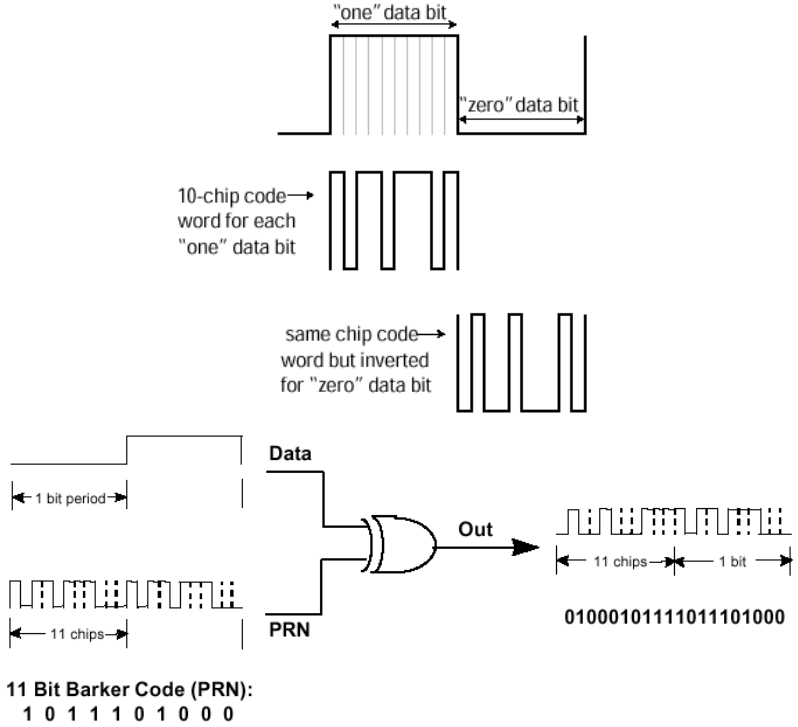
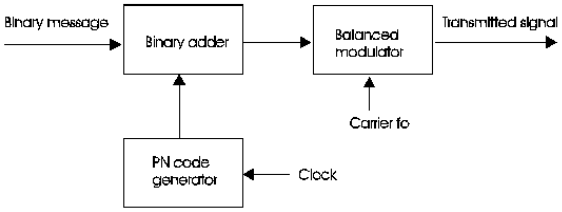


Figure 16 : code PN - chipping

On étale ainsi le signal sur une bande de fréquence plus large en sur-modulant chaque bit du paquet à transmettre par ce code PN répétitif. Au niveau du récepteur, le signal original est retrouvé en réceptionnant tout le canal étalé et en le démodulant avec le même code.



Direct-sequence transmitter

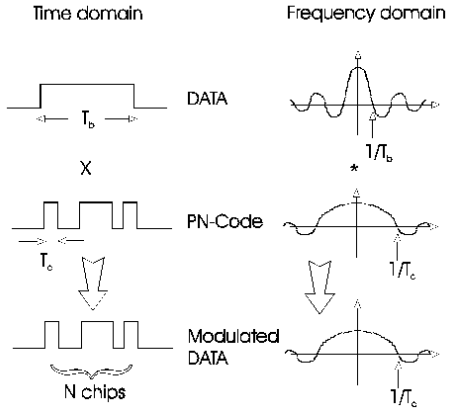
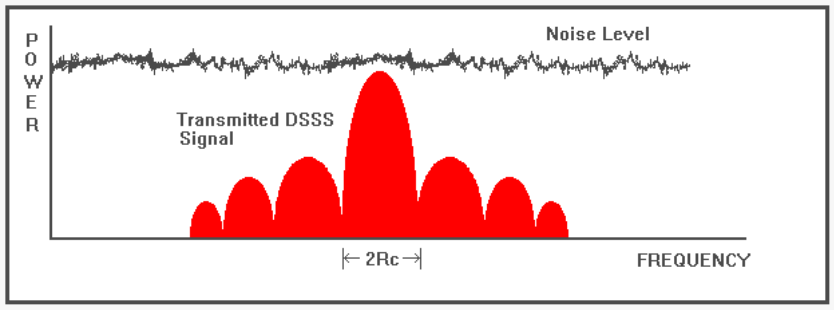


Figure 17 : code PN - étallement



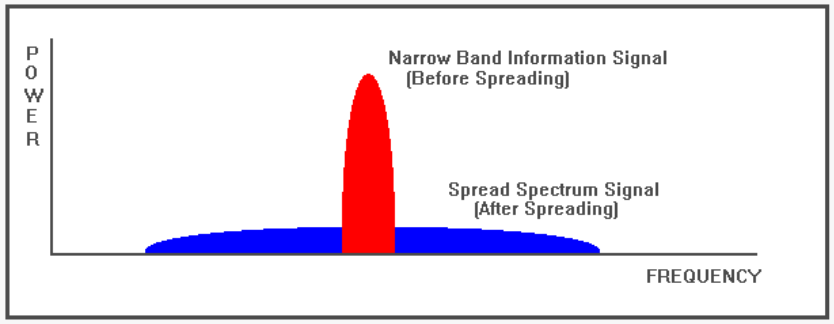


Figure 18 : DSSS

Le DSSS du protocole 802.11 spécifie donc un chipping de 11 bits appelé *Barker sequence*. Chaque séquence de 11 bits représente un bit (0 ou 1) de données. Elle est ensuite convertie en onde appelée *symbol* transmis à 1 MS/s (1 millions de Symboles par seconde). C'est la modulation utilisée qui permet d'avoir des débits différents. La BPSK (Binary Phase Shift Keying) pour un débit de 1 Mbit/s et la QPSK (Quadature Phase Shift Keying) pour un débit de 2 Mbit/s.
Dans le protocole 802.11b, pour pouvoir supporter les 2 nouveaux débits 5.5 Mbit/s et 11 Mbit/s, seul le DSSS est utilisé. En effet, le FHSS ne pourrait pas supporter ces nouveaux débits sans violer les règles actuelles du FCC (Federal Communication Commission).
Cette augmentation des débits est faite grâce aux techniques de modulation et de codage comme le CCK (Complementary Code Keying). Mais quelle que soit le débit employé, et c'est d'ailleurs pourquoi ces techniques ont été autorisées, le signal est toujours étalé sur 22 MHz *(=2*taille codage*vitesse de symbole).*

Le tableau suivant récapitule la situation :

Débits	Codage ?	Modulation	Vitesse de symbole	Nb de bits/symbole
1 Mbit/s	11 (Barker Sequence)	BPSK	1 MS/s	1
2 Mbit/s	11 (Barker Sequence)	QPSK	1 MS/s	2
5.5 Mbit/s	8 (CCK)	QPSK	1,375 MS/s	4
11 Mbit/s	8 (CCK)	QPSK	1,375 MS/s	8

Figure 19 : Tableau récapitulatif des différentes techniques.

Ainsi, toute interférence à bande étroite apparaîtra très faible, d'autant plus que le démodulateur utilise le même code que l'émetteur pour retrouver le signal étalé, ce qui minimise encore les signaux aléatoires.

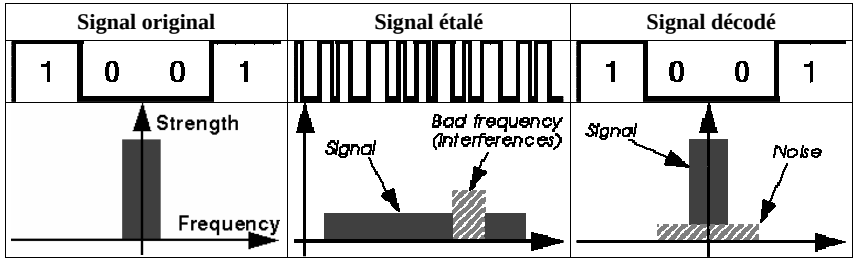


Figure 20 : Robustesse aux interférences

Mais par conséquent, dans cette technique où la bande passante de chaque canal est de 22MHz, ceci implique que seuls 3 canaux (sur les 14 prévus par la norme) peuvent être utilisés de manière adjacente si on veut totalement éviter le recouvrement de spectre. On pointe du doigt un problème latent en France qui limite l'intérêt du LAN sans fil : pour l'instant, seuls 4 canaux sont disponibles. On est donc contraint pour le moment à superposer plusieurs canaux, mais ceci tend à augmenter le bruit et diminuer ainsi les performances du système, car tous les produits opèrent avec le même code PN (et non un code par fréquence) !

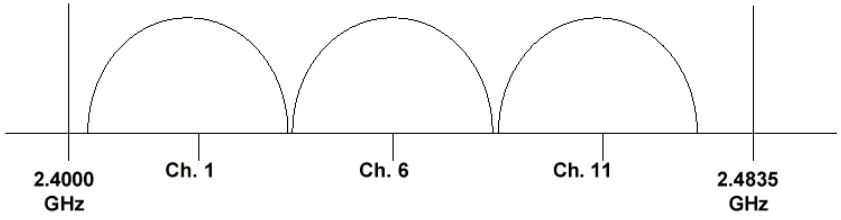


Figure 21 : Espacement des canaux adjacents pour limiter tout recouvrement spectral

Frequency Range	2400-2500 MHz[1]			
Channel ID	FCC	ETSI	France	Japan
1	2412	2412	-	2412
2	2417	2417	-	2417
3	**2422**	**2422**	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11	2462	2462	**2462**	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14	-	-	-	**2484**

Figure 22 : Fréquences des canaux alloués

4.1.3 Comparaison des deux techniques

Saut de fréquence	Séquence directe
• faible débit (2Mbps maxi) • + sûr du point de vue de la sécurité • + grande portée • cohabitation aisée entre LANs sans fil • 30 à 50 stations par point d'accès pour un débit intéressant (8 kO/s mini) à condition d'avoir un petit réseau (peu de points d'accès car pas de partage de la bande) • modulation plus simple • moins onéreux	• débit élevé (11Mbps, et bientôt 22Mbps) • + employé • 10 à 20 stations par point d'accès pour un débit intéressant (8 ko/s mini), quelle que soit la taille du réseau • moins d'interférences car pas de partage désordonné de la bande passante • protocole MAC plus simple

5. LA COUCHE MAC

La norme IEEE 802.11 utilise les retransmissions au niveau MAC, le RTS/CTS et la fragmentation de paquets. La sous-couche MAC définit deux normes d'exécution : le mode distribué CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), le plus utilisé, et le mode par point.

Au niveau de la sécurité, le protocole MAC du 802.11 inclue l'authentification facultative et le cryptage des données (utilisant le WEP, Wired Equivalent Privacy, qui est du RC4 à 40 bits ; quelques constructeurs offrent du RC4 à 128 bits). Pour plus de détails sur ces points, voir le chapitre sur la sécurité.

5.1 LE CSMA/CA

5.1.1 Le CSMA et les collisions

Dans les réseaux filaires, on utilise les protocoles CSMA comme mécanisme d'accès de canal, c'est à dire un mécanisme qui indique comment chaque nœud peut utiliser le support (le canal) : quand écouter, quand transmettre... Le principal avantage du CSMA est qu'il est approprié aux protocoles de réseau tels que le TCP/IP, qu'il s'adapte tout à fait bien avec l'état variable du trafic et qu'il est tout à fait robuste aux interférences.

Le protocole CSMA fonctionne ainsi : une station voulant transmettre sonde le support de transmission. S'il est occupé (une autre transmission est en cours), alors la station reporte sa transmission pour plus tard. S'il est libre, alors la station peut émettre.

Ce type de protocole est très efficace lorsque le support n'est pas surchargé, dans la mesure où il permet aux stations d'émettre avec un minimum d'attente, mais il existe toujours un risque pour que deux stations émettent en même temps après avoir détecté un support libre et créent ainsi une collision.

Il faut alors détecter ces collisions pour que la couche MAC puisse retransmettre la trame sans avoir à repasser par les couches supérieures, ce qui engendrerait des retards significatifs. Pour Ethernet, les collisions sont repérées par les stations émettrices qui effectuent alors un algorithme de retransmission appelé algorithme de retour aléatoire exponentiel ("Algorithme de Back-off aléatoire exponentiel").

Si ces mécanismes de détection de collision sont bons sur un réseau local câblé, ils ne peuvent pas être utilisés dans un environnement sans fil, ceci pour deux raisons principales :

- Implémenter un mécanisme de détection de collision demanderait l'implémentation d'une liaison radio full duplex, capable de transmettre et de recevoir simultanément, ce qui augmenterait le prix.
- Dans un environnement sans fil, on ne peut pas être sûr que toutes les stations ont un lien radio entre elles (ce qui est l'hypothèse de base du principe de détection de collision), et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcement dire que le support est libre autour du récepteur.

Pour pallier ces problèmes, 802.11 utilise un mécanisme d'évitement de collision associé à un système d'accusé de réception : le CSMA/CA.

5.1.2 Le mécanisme d'accès de canal du DCF ou CSMA/CA

La couche MAC définit deux méthodes d'accès de canal différentes, la Fonction de Coordination Distribuée (DCF : Distributed Coordination Function) et la Fonction de Coordination par Point (PCF : Point Coordination Function).

Le mécanisme d'accès de base, le DCF, est typiquement le mécanisme CSMA/CA, qui est le mécanisme d'accès de canal employé par la plupart des LANs sans fil dans les bandes ISM. CSMA/CA est dérivé de CSMA/CD (Collision Detection), qui est la base d'Ethernet. Nous reparlerons du PCF plus loin.

Détection physique de porteuse :

Le mécanisme de base est l'écoute du canal avant transmission. Ce mécanisme est appelé détection physique de porteuse.

La station voulant transmettre commence par écouter le canal de transmission :

- Si le canal est occupé (une autre transmission est en cours), l'émetteur attend la fin de transmission du paquet et émet au bout d'une période aléatoire. Si le canal est encore occupé à l'émission, il utilise toujours le même algorithme. Puisque le temps d'attente avant émission est un nombre aléatoire pour chaque paquet, chaque nœud à la même probabilité d'accès au canal.
- Si le canal est libre au moins pendant un temps spécifié, appelé DIFS (Distributed Inter Frame Space), il émet le paquet. Après fin de transmission du paquet, le destinataire vérifie le CRC du paquet et renvoie un accusé de réception à l'émetteur, ce qui signifie à l'émetteur qu'il n'y a pas eu collision. Les collisions ne sont donc pas détectées, mais s'il y a collision, les deux stations qui l'ont provoquée ne reçoivent pas l'accusé de réception du destinataire, donc tentent de ré-émettre chacune au bout d'un temps aléatoire. Le premier a ré-émettre peut alors transmettre son paquet. En pratique, avec les cartes Orinoco, lorsqu'un accusé de réception n'est pas reçu, l'émetteur ré-émet le paquet. Si au bout de plusieurs fois, il n'y a toujours pas de réponse, la station ré-émet à un débit moins important.

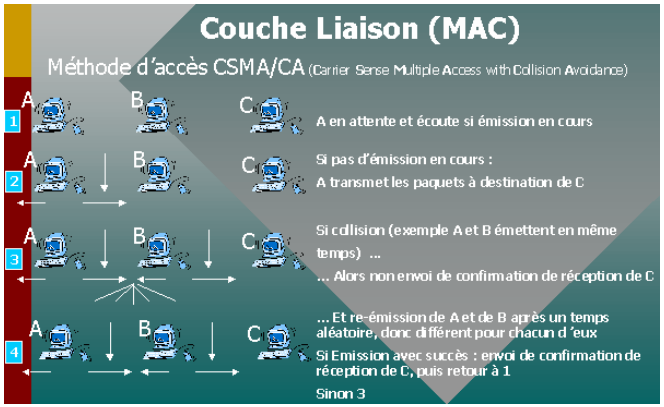


Figure 23 : Le mécanisme de détection physique de porteuse

Détection virtuelle de porteuse :

Pour réduire la probabilité de collision due au fait que deux stations sans fil appartenant au même réseau n'ont pas de liens radio entre-elles (elles sont trop éloignées), 802.11 utilise un mécanisme de détection virtuelle de porteuse. Nous allons nous servir de la figure 15 pour expliquer ce mécanisme.

Une station (A sur la figure) voulant transmettre commence par émettre un court message appelé RTS (Ready To Send), qui contient les adresses de l'émetteur et du destinataire et la durée du message. Si le canal est libre (donc après une non-détection physique de porteuse), le destinataire (B) émet alors un message CTS (Clear To Send) comportant les mêmes informations que le RTS, indiquant à l'émetteur que son paquet peut être envoyé.

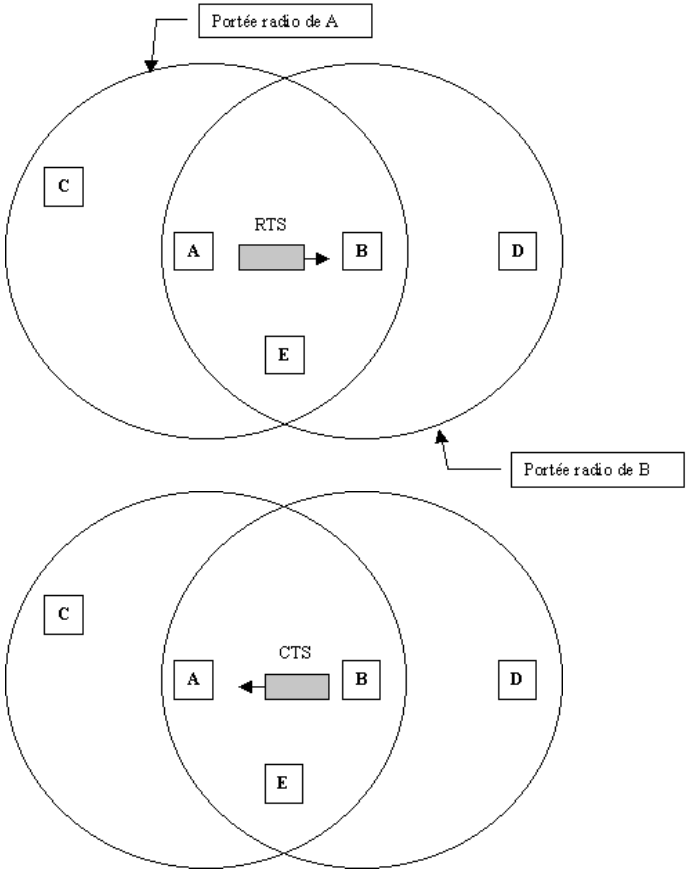


Figure 24 : Détection virtuelle de porteuse : le problème des stations "cachées"

Toutes les stations recevant ce message RTS ou/et CTS mettront à jour leur indicateur de détection virtuelle de porteuse (appelé NAV pour Network Allocation Vector : indique le temps minimal de report) pour la durée précisée dans ces messages et utiliseront ces informations en parallèle avec la détection physique de porteuse pendant le processus de détection avant d'émettre un message. Ainsi, sur la figure 16, la station C aura reçue le RTS, la station D le CTS et la station E le RTS et le CTS.
Ce mécanisme réduit la probabilité de collision par une station "cachée" de l'émetteur dans la zone du récepteur à la courte durée de transmission du RTS, parce que la station entend le CTS et considère le support comme occupé jusqu'à la fin de la transaction. L'information "durée d'occupation du canal" dans le RTS et le CTS protège la zone de l'émetteur des collisions pendant la transmission de l'accusé de réception (par les stations étant hors de portée de la station accusant réception).

Il est également important de noter que grâce au fait que le RTS et le CTS soient 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. Ceci est vrai si le paquet est beaucoup plus important que le RTS. Le standard autorise donc les paquets courts à être transmis sans l'échange de RTS/CTS, ceci étant contrôlé pour chaque station grâce au paramètre appelé *RTS Threshold*. (Voir documentation driver linux et tests sans RTS/CTS).

Le diagramme de la figure 17 résume les échanges entre les deux stations A et B et le vecteur NAV des stations voisines.

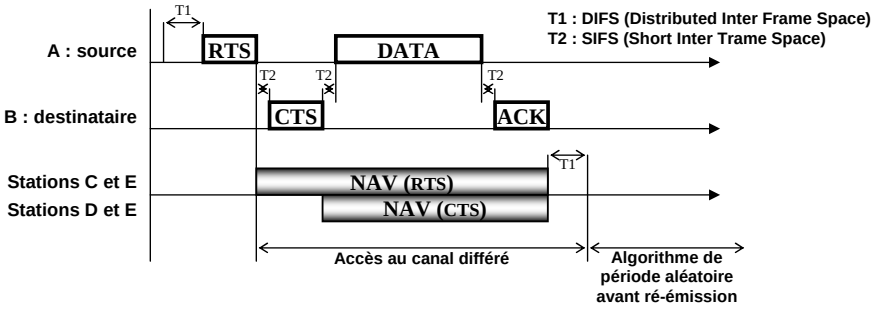


Figure 25 : Echanges entre 2 stations A et B et vecteur NAV des autres stations

5.1.3 La Fonction de Coordination par Point (PCF)

A l'opposé du DCF, où le contrôle d'accès au canal est distribué sur toutes les stations, le mode PCF définit le point d'accès comme seul contrôleur d'accès au canal.
Si le mode PCF est actif dans un BSS, le temps est partagé entre le mode PCF et le mode DCF pour permettre aux stations l'accès au canal. Dans le mode PCF, le point d'accès élit chaque station pour un temps déterminé et passe à la station suivante. Ainsi, chaque station n'est autorisée à transmettre ou à recevoir les données que si elle a été élue. Ce fonctionnement permet de garantir la qualité de service, mais sur un réseau important le fait de n'avoir qu'un seul point d'accès au canal et d'élire tour à tour chaque station peut-être un inconvénient. Notons que le PCF est très peu utilisé dans la couche MAC des LANs sans fil.

5.2 LA SECURITE

La sous-couche MAC définit un mécanisme de cryptage et de contrôle d'accès appelé WEP (Wired Equivalent Privacy) que nous allons décrire plus précisément dans le chapitre adéquat (sécurité).

5.2.1 L'accès aux ressources du réseau

L'accès aux ressources du réseau est obtenu en utilisant un mécanisme d'authentification où une station est obligée de prouver sa connaissance d'une clé, ce qui est similaire à la sécurité sur réseaux câblés, dans le sens où l'intrus doit entrer dans les lieux (en utilisant une clé physique) pour connecter son poste au réseau câblé.

5.2.2 L'écoute clandestine

L'écoute clandestine est bloquée par l'utilisation de l'algorithme WEP qui est un générateur de nombres pseudo-aléatoires initialisés par une clé secrète partagée par toutes les stations d'un LAN. L'algorithme WEP est un simple algorithme basé sur l'algorithme RC4 de RSA, qui a les propriétés suivantes :

- Plutôt performant : l'attaque par "force brutale" (essai de décodage par des clés aléatoires ou des listes de clés) de cet algorithme est difficile car chaque trame est envoyée avec un vecteur d'initialisation qui relance le générateur de nombres pseudo-aléatoires.
- Autosynchronisé : l'algorithme se resynchronise pour chaque message. Ceci est nécessaire pour travailler en mode non connecté, où les paquets peuvent être perdus, comme dans tout réseau local.

5.3 L'ECONOMIE D'ENERGIE

Les réseaux sans fil sont généralement en relation avec des applications mobiles, et dans ce genre d'application, l'énergie de la batterie est une ressource importante. C'est pour cette raison que le standard 802.11 donne lui-même des directives pour l'économie d'énergie et définit tout un mécanisme pour permettre aux stations de se mettre en veille pendant de longues périodes sans perdre d'information.
L'idée générale, derrière le mécanisme d'économie d'énergie, est que le point d'accès maintient un enregistrement à jour des stations travaillant en mode d'économie d'énergie, et garde les paquets adressés à ces stations jusqu'à ce que les stations les demandent avec une requête de polling, ou jusqu'à ce qu'elles changent de mode de fonctionnement.
Les points d'accès transmettent aussi périodiquement (dans les trames "balise") des informations spécifiant quelles stations ont des trames stockées par le point d'accès. Ces stations peuvent ainsi se réveiller pour récupérer ces trames balise, et si elles contiennent une indication sur une trame stockée en attente, la station peut rester éveillée pour demander à récupérer ces trames.
Les trames de multicast et de broadcast (trames destinées à toutes les stations du réseau) sont stockées par le point d'accès et transmises à certains moments (à chaque DTIM) où toutes les stations en mode d'économie d'énergie qui veulent recevoir ce genre de trames devraient rester éveillées.

Département Télécommunications
Année 2006-07

5.4 CONCLUSION SUR LES FONCTIONNALITES DE LA COUCHE MAC

Donc la couche MAC :

- Décrit comment les trames "balise" sont envoyées à intervalles réguliers (par ex 100 ms) des APs aux stations pour permettre à celles-ci de gérer la présence ou non de l'AP.
- Donne une batterie de trames de management qui permettent aux stations de scanner régulièrement leur environnement en quête d'autres APs sur chaque canal disponible.
- Définit des fonctionnalités spéciales pour la retransmission de paquets non reçus, la fragmentation des paquets, la réservation du « médium » via RTS/CTS (Request To Send/Clear To Send) etc…
- Dans le cas des réseaux ad hoc, il n'y a pas de point d'accès, et une partie de ses fonctionnalités sont reprises par les stations elles-mêmes (comme les trames "balise" pour la synchronisation). D'autres fonctions ne sont pas utilisables dans ce cas : le relayage des trames et le mode d'économie d'énergie).

On ne peut pas faire de changements énormes au niveau MAC, comme par exemple « upgrader » son WLAN 802.11b à 802.11a en changeant le protocole, et ceci pour la simple raison que la majorité du protocole MAC est embarqué dans la carte (sur le microcontrôleur ou voire même sur un ASIC ou un FPGA pour les couches basses du protocole MAC) et que seulement quelques fonctions sont prises en charge par le driver. De plus, les constructeurs ne disent en général pas comment reprogrammer le driver de leurs produits mais même s'ils le faisaient, cela ne suffirait pas pour créer des émetteurs/récepteurs radios universels qui puissent être re-configurables facilement et à volonté pour recevoir n'importe quel standard radio. Pour cela, il faudrait re-concevoir toute la carte avec un bloc conséquent de logique re-programmable sur laquelle on téléchargerait une nouvelle configuration pour le protocole que l'on désirerait utiliser, afin de pouvoir s'adapter à n'importe quel modulation ou taux de transfert. Ce serait alors un produit implémenté entièrement en numérique et non plus principalement analogique comme c'est le cas actuellement. Il faudrait tout d'abord numériser toute la bande passante du signal capté, avec un convertisseur analogique numérique très rapide, et « envoyer » le tout dans un DSP ou un FPGA (Field Programmable Gate Array). Le problème principal serait, d'une part le coût d'un tel produit, mais aussi et surtout de gérer tout ce que cela implique de travailler avec des fréquences de l'ordre du GigaHertz !