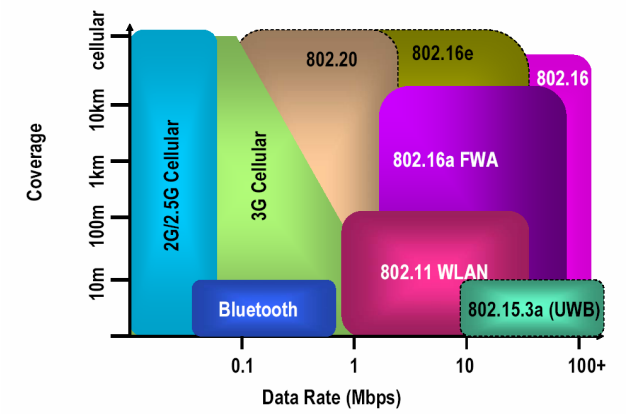
Conservatoire National des Arts et Métiers

WiFi

Le Standard 802.11
Couche physique et couche MAC

Version 1.1



Mars 2007

Michel Terré
terre@cnam.fr
www.cnam.fr/elau

TABLES DES MATIERES

1 INTRODUCTION

Le groupe **802.11** a été initié en 1990, et le standard **IEEE 802.11** définissant les réseaux locaux sans fil a vu le jour en 1997. Le standard d'origine a défini trois couches physiques pour une même couche MAC, correspondant à trois types de produits 802.11 :

- IEEE 802.11 FHSS (Frequency Hopping Spread Spectrum), qui utilise la technique d'étalement de spectre basé sur le saut de fréquence.
- IEEE 802.11 DSSS (Direct Sequence Spread Spectrum), qui utilise aussi la technique d'étalement de spectre mais sur une séquence directe.
- IEEE 802.11 IR (InfraRed), de type infrarouge.

Les réseaux IEEE 802.11 FHSS et IEEE 802.11 DSSS sont des réseaux radio sans fil émettant dans la bande ISM.
Etant donné leurs caractéristiques, ces trois types de produits ne sont pas directement compatibles entre eux. Même s'ils offrent une certaine opérabilité au niveau LLC, celle-ci ne se retrouve pas au ni niveau physique. Ainsi, une carte IEEE 802.11 FHSS ne peut pas dialoguer avec une carte IEEE 802.11 DSSS, et réciproquement. De même, IEEE 802.11 IR ne peut dialoguer avec un réseau IEEE 802.11 FHSS ni IEEE 802.11 DSSS. Pour obtenir cette opérabilité, il faudrait des produits multistandards, ce qui n'est pas le cas des produits existants.

Le standard IEEE 802.11 n'est pas resté figé, et de nombreuses améliorations ont été apportées au standard d'origine. Ces améliorations continuent actuellement..
Trois nouvelles couches physiques ont été ajoutées avec les standards IEEE 802.11b, IEEE 802.11a et IEEE 802.11g :

- IEEE 802.11b ou **Wi-Fi** utilise la même bande ISM que IEEE 802.11 mais avec des débits pouvant atteindre 11 Mbit/s. IEEE 802.11b est en réalité une amélioration de IEEE 802.11 DSSS. Ainsi, une caractéristique de IEEE 802.11b est de rester compatible avec IEEE 802.11 DSSS.
- IEEE 802.11a ou **Wi-Fi 5**, utilise une nouvelle bande, appelée bande U-NII, située autour de 5 GHz. Le débit de IEEE 802.11a peut atteindre 54 Mbit/s, mais en perdant la compatibilité avec 802.11 DSSS et FHSS et 802.11b, du fait de l'utilisation d'une bande différente.
- IEEE 802.11g utilise la bande ISM mais avec un débit pouvant atteindre 20 Mbit/s. Ce standard utilise en fait la forme d'onde OFDM de 802.11a. Mais, contrairement à IEEE 802.11a, IEEE 802.11g est compatible avec 802.11 DSSS et IEEE 802.11b.
- IEEE 802.11n, et une évolution de 802.11g qui intègre la "dimension" MIMO.

2 L'ARCHITECTURE EN COUCHES

La norme IEEE 802.11 définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Cette dernière est elle-même subdivisée en deux sous-couches, la sous-couche LLC (Logical Link Control) et la couche MAC (Medium Access Control).
La figure suivante illustre l'architecture du modèle proposé par le groupe de travail 802.11 comparée à celle du modèle OSI.

<table>
<tr><td rowspan="2">OSI Layer 2
Data Link Layer</td><td colspan="6">802.11 Logical Link Control (LLC)</td></tr>
<tr><td colspan="6">802.11 Medium Access Control (MAC)</td></tr>
<tr><td>OSI Layer 1
Physical Layer (PHY)</td><td>FHSS</td><td>DSSS</td><td>IR</td><td>Wi-Fi
802.11b</td><td>Wi-Fi
802.11g</td><td>Wi-Fi5
802.11a</td></tr>
</table>

Figure 1 : modèle en couches de l'IEEE 802.11

L'une des particularités de cette norme est qu'elle offre plusieurs variantes au niveau physique, tandis que la partie liaison est unifiée.
Bien que la norme 802.11 d'origine n'ai défini que trois couches physiques, les couches FHSS, DSSS, et IR, l'ajout ultérieur de Wi-Fi, de Wi-Fi 5 et de IEEE 802.11g n'a pas entraîné de changements radicaux dans la structure de la couche MAC.

On rappelle que la couche physique de la norme IEEE 802.11 est l'interface située entre la couche MAC et le support qui permet d'envoyer et de recevoir des trames.

Chaque couche physique 802.11/a/b/g est divisée en deux sous-couches :

- la sous-couche PMD (Physical Medium Dependent) qui gère l'encodage des données et effectue la modulation
- la sous-couche PLCP (Physical Layer Convergence Protocol) qui s'occupe de l'écoute du support et fournit un CCA (Clear Channel Assessment) à la couche MAC pour lui signaler que le canal est libre.

3 LES BANDES DE FREQUENCES

Les cinq couches radio du standard IEEE 802.11/a/b/g utilisent des fréquences situées dans des bandes dites sans licence. Il s'agit de bandes libres, qui ne nécessitent pas d'autorisation de la part d'un organisme de réglementation. Les deux bandes sans licence utilisées dans 802.11/a/b/g sont :

- la bande ISM (Industrial, Scientific and Medical)
- la bande U-NII (Unlicenced-National Information Infrastructure).

3.1 La bande ISM

La bande ISM utilisée dans 802.11/b/g correspond à une bande de fréquence située autour de 2.4 GHz, avec une largeur de bande de 83.5 MHz (2.4 MHz – 2.483 5 MHz). Cette bande ISM est reconnue par les principaux organismes de réglementation, tels que la FCC au Etats-Unis, l'ETSI en Europe, l'ART en France. La largeur de bande libérée pour les RLAN varie cependant suivant les pays (voir tableau suivant).

Pays	***Bande de fréquences***
Etats-Unis (FCC)	2.400-2.485 GHz
Europe (ETSI)	2.400-2.4835 GHz
Japon (MKK)	2.471-2.497 GHz
France (ART)	2.4465-2.4835 GHz

Tableau 1 - Allocation des bandes de fréquences ISM selon les pays

En France, la largeur de bande ISM autorisée pour 802.11/a/b/g dépend de la puissance maximale utilisée, comme le montre les tableaux suivants.

3.2 La bande U-NII

La bande sans licence U-NII est située autour de 5 GHz. Elle offre une largeur de bande de 300 MHz (plus importante que celle de la bande ISM qui est égale à 83.5 MHz). Cette bande n'est pas continue mais elle est divisée en trois sous-bandes distinctes de 100 MHz. Dans chaque sous bande la puissance d'émission autorisée est différente. La première et la deuxième sous bande concernent des transmissions en intérieur. La troisième sous-bande concerne des transmissions en extérieur. Comme pour la bande ISM, la disponibilité de ces trois bandes dépend de la zone géographique. Les Etats-Unis utilisent la totalité des sous-bandes, l'Europe n'utilise que les deux premières et le Japon la première. Les organismes chargés de réguler l'utilisation des fréquences radio sont : l'ETSI (European Telecommunications Standards Institute) en Europe, la FCC (Federal Communications Commission) aux Etats-Unis, le MKK (Kensa-kentei Kyokai) au Japon

3.3 Règlementation française

Cf http://www.art-telecom.fr

Métropole

	Intérieur	Extérieur
2400 2454	100 mW	100 mW
2483,5		10 mW

Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte

	Intérieur	Extérieur
2400 2483,5	100 mW	100 mW

Réunion et Guyane

	Intérieur	Extérieur :
2400 2420	100 mW	100 mW
2483,5		

Tableau des puissances dans la bande 5 GHz

	Intérieur	Extérieur
5150 5250	200 mW	impossible
5350	200 mW avec DFS/TPC ou équivalent ou 100mW avec DFS uniquement	

***Note**: La réglementation (compliquée) spécifique à la bande U-NII autour de 5 GHz*

La décision ECC du 09 Juillet 2004 précise les conditions d'utilisation coordonnée des bandes de fréquences 5 GHz pour la mise en oeuvre des systèmes d'accès hertzien, y compris les réseaux RLAN (WAS/RLANs) (ECC/DEC/(04)08); l'utilisation de ces équipements doit être conforme au standard harmonisé EN 301 893. Cette décision est entrée en vigueur le 12 novembre 2004.

Les stations WAS/RLANs fonctionnant dans les bandes 5.250-5.350 MHz et 5.470-5.725 MHz emploient la sélection dynamique de fréquences, DFS (dynamic frequency selection) conformément à la recommandation ITU-R M. 1652 afin d'éviter les brouillages cocanals avec les systèmes radiolocalisations. Le mécanisme DFS devra s'assurer que la probabilité de sélectionner un certain canal sera la même pour tous les canaux disponible, ceci afin de permettre un étalement spectral quasi uniforme.

Selon la Décision n°02-1091 de l'Autorité de régulation des télécommunications en date du 3 décembre 2002 attribuant des fréquences aux installations radioélectriques à haute performance dans la bande 5.150-5.350 MHz, la bande de fréquence 5.150-5.350 MHz est attribuée, en France, aux installations radioélectriques à haute performance avec une puissance isotrope rayonnée équivalente (PIRE) maximale de 200 mW pour une utilisation limitée à l'intérieur d'un bâtiment. Les équipements ne doivent en aucun cas émettre sur des canaux occupés par un autre système, notamment par un système de radiolocalisation utilisé par le Ministère de la Défense. Les équipements doivent utiliser, de manière aléatoire, la totalité des canaux disponibles de la bande concernée.

Pour ce faire, les équipements disposeront d'une fonctionnalité de sélection dynamique de fréquence (DFS) telle que décrite dans le projet de norme harmonisée pr-EN 301 893, puis telle qu'elle sera décrite dans la norme harmonisée correspondante quand cette dernière aura été publiée, ou d'une fonctionnalité reconnue équivalente et garantissant au minimum, pour les autres applications autorisées dans la bande concernée, un degré de protection identique à celui apporté par la norme harmonisée. En l'absence d'une fonction de contrôle de la puissance d'émission (TPC) permettant une atténuation de la puissance moyenne émise de 3 dB minimum, la puissance PIRE maximale est limitée à 100 mW.

4 LES COUCHES PHYSIQUES DU STANDARD IEEE 802.11/A/B/G

Comme il a été indiqué précédemment, le standard 802.11 d'origine a défini trois couches physiques de base, FHSS, DSSS, IR, auxquelles ont été rajoutées trois nouvelles couches physiques Wi-Fi (avec deux variantes au sein de la solution 802.11b) et Wi-Fi5 (802.11a/g).

4.1 FHSS (Frequency Hopping Spread Spectrum)

FHSS désigne une technique d'étalement de bande fondée sur le saut de fréquence, dans laquelle la bande ISM des 2.4 GHz est divisée en 79 canaux ayant chacun 1 MHz de largeur de bande. Pour transmettre des données, l'émetteur et le récepteur s'accordent sur une séquence de sauts précise qui sera effectuée sur ces 79 sous-canaux. La couche FHSS définit trois ensembles de 26 séquences, soit au total 78 séquences de sauts possibles.
La transmission de donnée se fait par l'intermédiaire de sauts d'un sous-canal à un autre, sauts qui se produisent toutes les 300 ms, selon une séquence prédéfinie. Celle-ci est définie de manière optimale de façon à minimiser les probabilités de collision entre plusieurs transmissions simultanées. Si une station ne connaît pas la séquence de sauts des canaux, elle ne peut pas récupérer ses données.
Cette technique était utilisée auparavant dans les transmissions militaires pour sécuriser leurs transmissions. Lors de la libération de la bande ISM, en 1985, ils ont également rendu libre l'usage de FHSS.
La bande ISM n'étant pas allouée de la même manière selon les pays, il existe des disparités dans le nombre de canaux utilisés (tableau 3).

Pays	Etats-Unis	Europe	Japon
Nombre de canaux utilisés	79	79	23

Tableau 3 - nombre de sous canaux utilisés pour le FHSS

En mode FHSS les données sont émises au moyen d'une modulation GMSK. Le débit est compris entre 1 et à 2 Mbit/s.
L'un des avantages du FHSS est qu'il permet, théoriquement, de faire fonctionner simultanément 26 réseaux 802.11 FHSS (correspondant aux 26 séquences) dans une même zone, chaque réseau utilisant une des séquences prédéfinies
Un autre avantage du FHSS est sa résistance face aux interférences, comme le système saute toutes les 300 ms d'un canal à un autre sur la totalité de la bande, si des interférences surviennent sur une partie de la bande ISM (un ou plusieurs canaux), cela n'engendre pas de trop importantes pertes de performances

Le principal inconvénient du FHSS vient de son débit qui est limité à 2 Mbit/s. Cette limitation est due au fait que la bande passante des canaux égale à 1 MHz.

Le FHSS est aussi utilisé dans Bluetooth. La seule différence entre FHSS de Bluetooth et celui de 802.11 vient des séquences de sauts, qui ne sont pas les mêmes de façon à éviter les interférences entre les deux systèmes.
On notera enfin que le mode FHSS est aujourd'hui totalement supplanté dans les équipements WiFi par les solutions 802.11b/a/g.

4.2 DSSS (Direct-Sequence Spread Spectrum)

Comme le FHSS, le DSSS divise la bande ISM en sous bandes. Cependant la division se fait ici en 14 canaux de 20 MHz chacun. La transmission ne se fait que sur un canal donné. La largeur de la bande ISM étant égale à 83.5 MHz, il est impossible d'y placer 14 canaux adjacents de 20 MHz. Les canaux se recouvrent donc, comme illustré à la figure suivante.

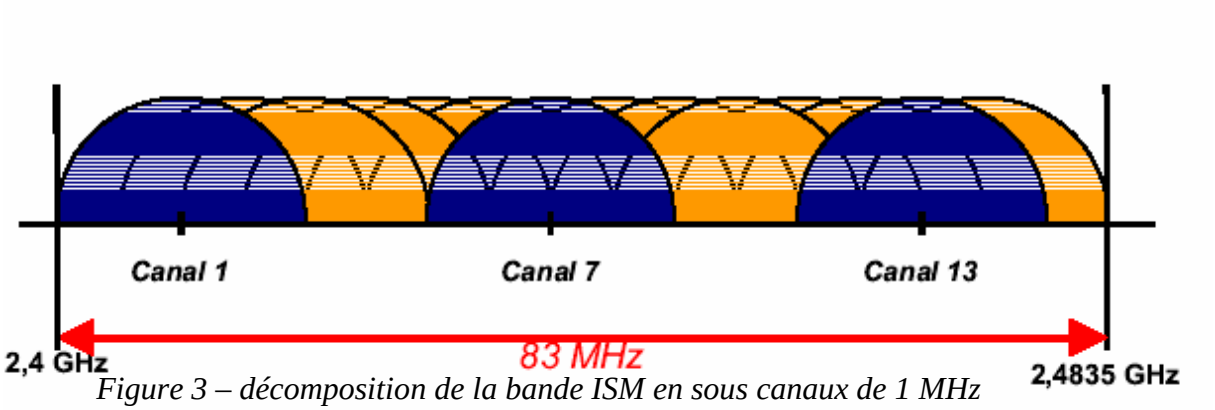


Figure 3 – décomposition de la bande ISM en sous canaux de 1 MHz

Comme le montre le tableau suivant, les fréquences centrales de chaque sous-canal sont espacées de 5 MHz.

Canal	Fréquence centrale (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442

Canal	Fréquence centrale (GHz)
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.477

Tableau 4 – Fréquences centrales des sous canaux du mode DSSS

Comme la transmission ne se fait que sur un canal, les systèmes DSSS sont plus sensibles aux interférences que les systèmes FHSS, qui utilisent toute la largeur de bande.

L'utilisation d'un seul canal pour la transmission est un inconvénient si différents réseaux 802.11 DSSS se superposent.

Lorsqu'un canal est sélectionné, le spectre du signal occupe une bande comprise entre 10 et 15 MHz de chaque coté de la fréquence centrale. La valeur 15 MHz provient de la décroissance non idéale des lobes secondaires de la modulation utilisée. Il n'est donc pas possible d'utiliser dans la même zone géographique les canaux adjacents à ce canal.

Pour permettre à plusieurs réseaux d'émettre sur une même cellule, il faut allouer à chacun d'eux des canaux appropriés, qui ne se recouvrent pas. Par exemple, considérons deux réseaux utilisant DSSS. Si l'un d'eux utilise le canal 6, le canal 5 et 7 ne peut pas être utilisé par le deuxième réseau, car trop proche. Il en va de malheureusement de même pour les canaux 2, 3, 4, 8, 9 et 10, qui ne peuvent non plus être alloués du fait de l'étalement de la bande passante du canal 6. Les canaux qui peuvent être utilisés sont les canaux 1, 11, 12, 13 et 14.

Sachant que la largeur de bande n'est que de 83.5 MHz, il ne peut donc y avoir au maximum que trois réseaux 802.11 DSSS émettant sur une même cellule sans risque d'interférences.

Comme pour le FHSS, les caractéristiques du DSSS varient selon chaque pays, notamment pour ce qui concerne le nombre de sous canaux utilisés, ce qui peut remettre en cause la superposition de réseaux. Comme le montre le tableau 5, en Europe et aux Etats Unis, le nombre de réseaux peut atteindre trois, tandis qu'il est limité à un au Japon. Pour la France, tout dépend de la largeur de bande utilisée et donc de la puissance du signal (la puissance autorisée dépend de la sous-bande utilisée). Dans le cas de la bande 2.446 5-2.483 5 GHz, même si quatre canaux sont disponibles, ils ne suffisent pas pour permettre le fonctionnement de deux réseaux simultanément sur une même cellule. Il faut que la totalité de la bande ISM soit utilisée pour que trois réseaux puissent fonctionner en même temps sur une même cellule.

Pays	Etats-Unis	Europe	Japon
Nombre de canaux utilisés	1 à 11	1 à 13	14

Tableau 4 – Nombre de canaux disponibles pour le DSSS en fonction du pays

L'étalement du spectre est réalisé en utilisant une séquence de 11 *chips*, appelée code de **Barker** (1-111-1111-1-1-1). Pour chaque bit de données transmis est multiplié par cette séquence de 11 chips.

Cette approche introduit un étalement de spectre rendant le signal à transmettre plus insensible aux interférences bande étroite. En effet, si le bruit n'affecte qu'une zone de la bande, il sera possible de restaurer le signal et de récupérer les bits d'information.

Deux schémas de modulation peuvent être utilisés :

- DBPSK (Differential Binary Phase Shift Keying), conduisant à un débit égal à 1 Mbit/s
- DQPSK (Differential Quadrature Phase Shift Keying)), conduisant à un débit égal à 2 Mbit/s

4.3 IEEE.802.11b (WiFi)

En 1999, une nouvelle couche physique, 802.11b, plus communément appelée Wi-Fi, a été ajoutée au standard 802.11. Fonctionnant toujours dans la bande ISM, cette couche physique utilise une extension du DSSS, appelée HR/DSSS (High Rate DSSS).

Le HR/DSSS utilise le même système de canaux que le DSSS. Le problème du choix d'un canal permettant la colocalisation de différents réseaux reste donc entier. Comme ils s'appuient sur le DSSS, les réseaux Wi-Fi et 802.11 DSSS sont compatibles et peuvent communiquer entre eux, mais aux débits de 802.11 DSSS, compris entre 1 à 2 Mbit/s.

Le HR/DSSS possède une meilleure efficacité spectrale que le DSSS et il permet d'offrir deux débits : 5.5 Mbit/s ou 11 Mbit/s.

Le codage CCK

Le signal émis est constitué de huit chips complexes que l'on appelle un mot de code ***c*** et qui est défini à partir de 4 valeurs de phase $\varphi_1, \varphi_2, \varphi_3, \varphi_4$.

Le mot émis ***c*** s'écrit de la manière suivante :

$$c = \left(e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)} \quad e^{j(\varphi_1+\varphi_3+\varphi_4)} \quad e^{j(\varphi_1+\varphi_2+\varphi_4)} \quad -e^{j(\varphi_1+\varphi_4)} \quad e^{j(\varphi_1+\varphi_2+\varphi_3)} \quad e^{j(\varphi_1+\varphi_3)} \quad -e^{j(\varphi_1+\varphi_2)} \quad e^{j(\varphi_1)} \right)$$

Son émission occupe un canal de 20 MHz avec d'importants lobes secondaires en dehors de ces 20 MHz comme il a été précisé précédemment.

CCK à 5.5 Mbit/s

Dans ce cas, le mot de code ***c*** représente 4 bits que l'on notera d_0, d_1, d_2, d_3.

Les 4 phases $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ sont constituées à partir des 4 bits de la manière suivante:

La phase φ_1 va coder de manière différentielle[1] les deux premiers bits. En fait on va conserver sa valeur, d'un mot de code au suivant et, en fonction des valeurs des deux premiers bits d_0, d_1, on va ajouter un incrément à cette phase. Cet incrément ne sera pas le même selon qu'il s'agira d'un mot de code pair ou impair.

bits d_0, d_1	***incrément de phase (symboles pairs)***	***incrément de phase (symboles impairs)***
00	0	π
01	π/2	3π/2
11	π	0
10	3π/2	π/2

[1] On parle de modulation différentielle DQPSK pour préciser que la démodulation se fait de manière différentielle et que la modulation est effectuée par une intégration de phase.

Les termes de phase $\varphi_2, \varphi_3, \varphi_4$ vont coder les bits d_2, d_3 :

$$\varphi_2 = d_2\pi + \frac{\pi}{2}$$

$$\varphi_3 = 0$$

$$\varphi_4 = d_3\pi$$

CCK à 11 Mbit/s

Dans ce cas, le mot de code ***c*** représente 8 bits que l'on notera : $d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7$.

Les deux premiers bits codent la phase φ_1 exactement comme il a été indiqué pour le codage CCK à 5.5 Mbit/s.

Les 3 phases $\varphi_2, \varphi_3, \varphi_4$ bits codent alors simplement les 6 bits $d_2, d_3, d_4, d_5, d_6, d_7$ au moyen de la table suivante :

bits : $d_{2i}d_{2i+1}$	***Phase*** φ_{i+1} ***correspondante***
00	0
01	$\pi/2$
10	π
11	$3\pi/2$

Une des particularités de Wi-Fi est la variation dynamique du débit (Variable Rate Shifting). Ce mécanisme permet d'ajuster le débit (en ajustant le codage et la modulation) en fonction des variations de l'environnement radio. Si l'environnement est optimal, le débit est de 11 Mbit/s. Dès que l'environnement commence à se dégrader, pour causes d'interférences, de réflexion, de sensibilité du matériel, d'éloignement du point d'accès, etc…, le débit descend automatiquement.

4.4 Wi-Fi5 (IEEE.802.11a)

Contrairement à Wi-Fi, Wi-Fi5 n'utilise pas la bande ISM mais la bande U-NII située autour de 5 GHz. Cette bande offre une largeur égale à 300 MHz (au lieu des 83.5 MHz de la bande ISM).
La forme d'onde utilisée en IEEE 802.11a est similaire à une norme ETSI appelée HiperlanII. Utilisant une approche OFDM, cette couche physique représente une avancée importante par rapport aux formes d'ondes précédemment décrites dans ce document.

La norme 802.11a permet d'obtenir un haut débit (54 Mbit/s théoriques). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.

Canaux

La relation entre la fréquence centrale le numéro de canal est donnée par l'équation suivante :

$$\mathbf{F_{centrale\ du\ canal} = 5000 + 5 \times n_{ch}\ (MHz)}, \text{ avec } n_{ch} = 0, 1, \ldots..200.$$

Cette définition offre un système de numérotation unique pour tous les canaux espacés de 5 MHz entre 5 GHz et 6 GHz.

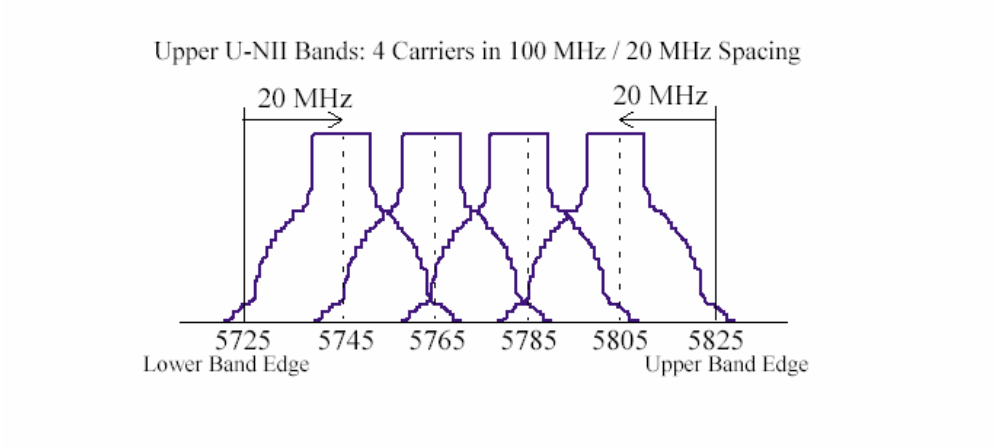
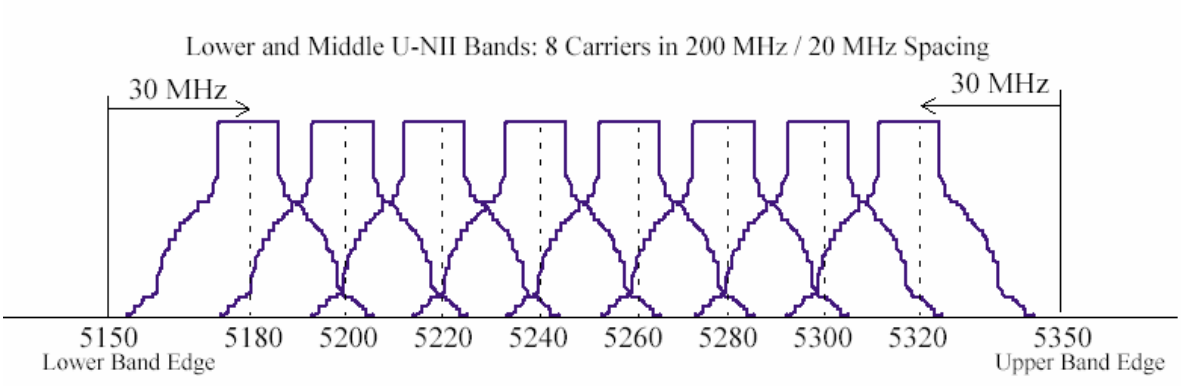
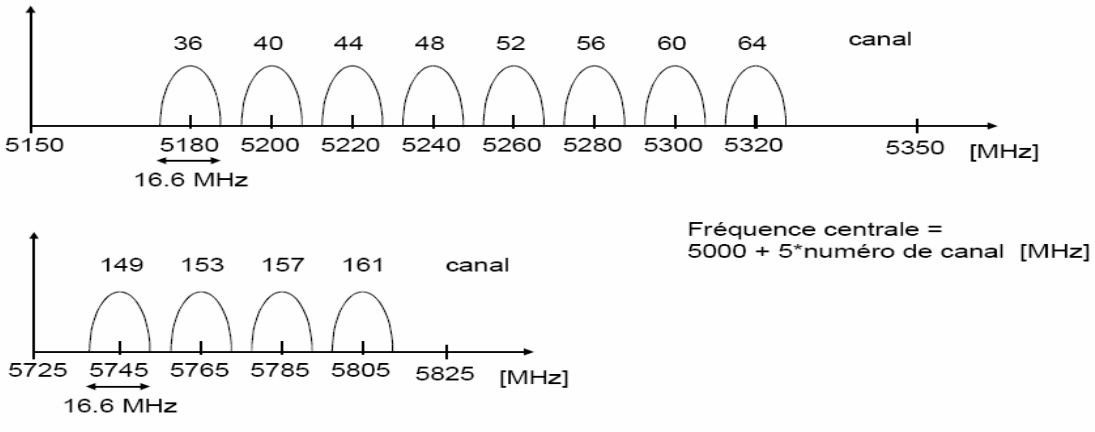


Figure 119—OFDM PHY frequency channel plan for the United States



Les bandes basse et centrale contiennent 8 canaux sur une bande passante totale de 200 MHz tandis que la bande haute contient 4 canaux sur une bande totale de 100 MHz. Les fréquences centrales des canaux situés aux extrémités des bandes basse et centrale doivent être espacées de 30 MHz des fréquences limites des bandes basse t centrale et de 20 MHz des fréquences limites de la bande haute.



Gabarit d'émission

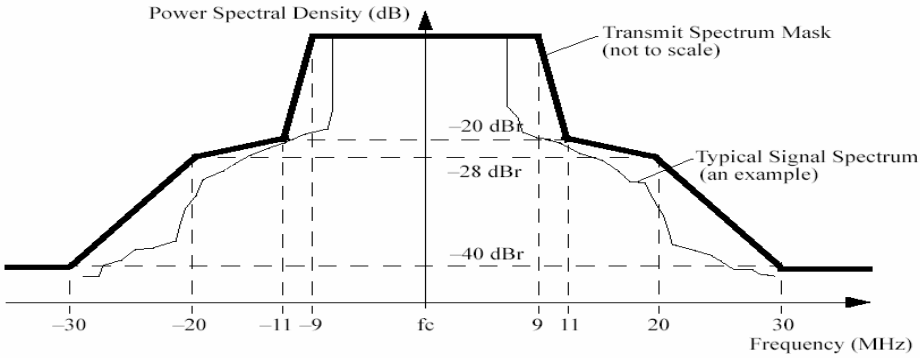


Figure 120—Transmit spectrum mask

Le spectre du signal transmis devra avoir 0dBr (dB relatif au maximum de la densité spectrale du signal) si la bande passante est inférieure à 18 MHz, - 20 dBr si l'offset de fréquence est de 11 MHz, - 28 dBr si l'offset de fréquence est de 20 MHz et de – 40 dBr si l'offset de fréquence est supérieure ou égale à 30 MHz.

Quelques paramètres dimensionnant de la couche physique IEEE 802.11a

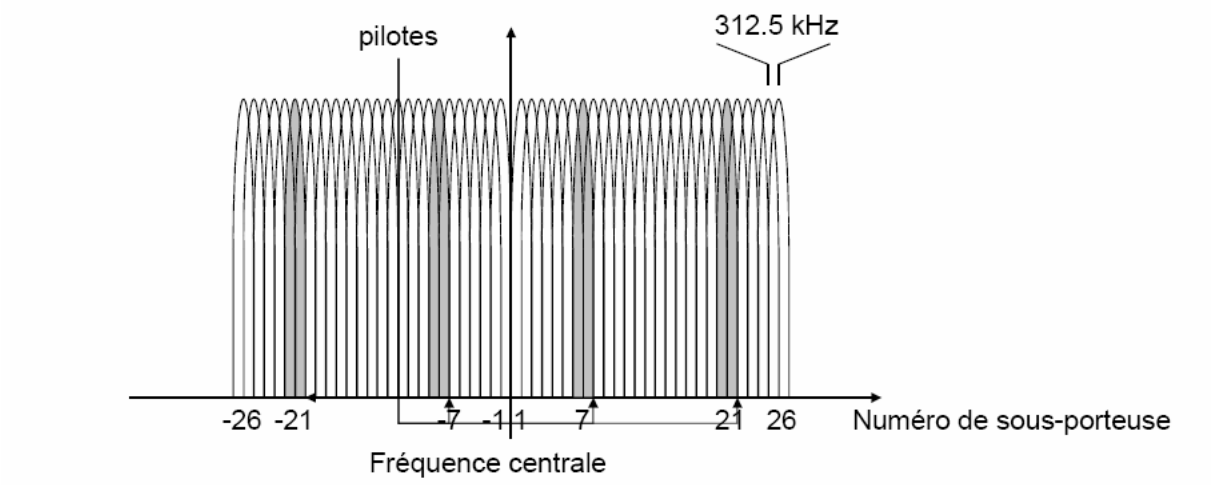
La forme d'onde OFDM est basée sur une IFFT (Transformée de Fourier Inverse) de taille 64. Pour éviter les lobes secondaires en extrémités de la bande, seules 52 porteuses parmi 64 sont utilisées. Les autres porteuses sont mises à zéro. C'est-à-dire que l'on présente une valeur nulle devant les entrées correspondantes de l'IFFT.
Parmi les 52 porteuses utilisées, 4 d'entre elles vont servir à véhiculer des signaux connus appelés pilotes.
En définitive il restera 48 porteuses utiles. On adjoint un intervalle de garde sous la forme d'un préfixe cyclique afin de prendre en compte simplement les multitrajets du canal. Ceci au moyen d'un simple égaliseur fréquentiel. Ce préfixe cyclique a une durée égale à 0.8 µs et le symbole OFDM émis, après insertion du préfixe cyclique, dure 4 µs.

Paramètres	Valeurs
N_{SD}:nombre de sous-porteuses de données	48
N_{SP}:nombre de sous-porteuses pilote	4
N_{ST}:nombre de sous-porteuses au total	52 (N_{SD} + N_{SP})
Δ_F:espacement en fréquence des sous-porteuses	0.3125 MHz (= 20 MHz 64)
T_{FFT}:Période IFFT/FFT	3.2 µs ($1/\Delta_F$)
T_{SIGNAL}:durée de symbole OFDM	4.0 µs (T_{GI} + T_{FFT})
T_{GI}: durée de l'intervalle de garde	0.8 µs (T_{FFT}/4)
Bande passante occupée	16;6 MHz
Largeur des canaux	20 MHz

Les 48 symboles fournis toutes les 4 µs à l'IFFT peuvent provenir de différents schémas de modulation et codage. Le tableau ci-dessous en dresse le récapitulatif.

Débit (Mbit/s)	Modulation	Taux de codage	Bits codés par sous-porteuse	Bits de code par symbole OFDM	Bits données par symbole OFDM
6	BPSK	½	1	48	24
9	BPSK	¾	1	48	36
12	QPK	½	2	96	48
18	QPSK	¾	2	96	72
24	16QAM	½	4	192	96
36	16QAM	¾	4	192	144
48	64QAM	2/3	6	288	192
54	64QAM	¾	6	288	216

La figure ci-dessous représente la localisation des porteuses pilotes :



Schémas simplifiés du modulateur et du démodulateur

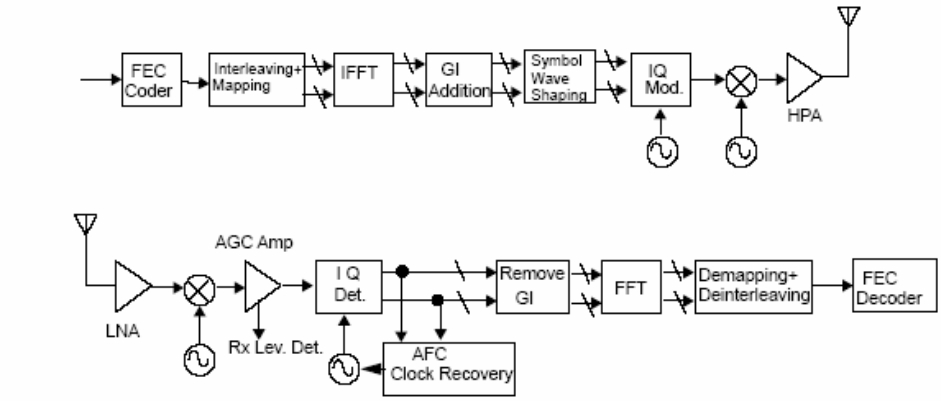


Figure 118—Transmitter and receiver block diagram for the OFDM PHY

Remarque sur le DFS

Le mécanisme de sélection DFS devrait pouvoir détecter des signaux brouilleurs dont la valeur moyenne calculée sur 1 µs est supérieure à un seuil de détection DFS minimal de –62 dBm pour les dispositifs dont la valeur maximale de p.i.r.e. est inférieure à 200 mW, et de –64

dBm pour les dispositifs dont la valeur maximale de p.i.r.e. est comprise entre 200 mW et 1 W.

4.5 IEEE 802.11g

La solution IEEE802.11g est une simple transposition de la forme d'onde IEEE802.11a de la bande U NII vers la bande ISM. A l'exception de cette différence de valeur de porteuse, la couche physique est rigoureusement identique à celle de IEEE802.11a.

5 COUCHE MAC

5.1 Rappel sur le CSMA/CD d'Ethernet

5.1.1 Généralités

En CSMA/CD (Carrier Sense Multiple Access with Collision Detection), avant toute tentative de transmission, une station s'assure que le canal n'est pas déjà utilisé (détection de porteuse), auquel cas la transmission est remise à un instant ultérieur. Quand le canal est détecté libre, après une durée aléatoire, si le canal est resté libre, la station envoie son paquet. Mais cette détection de porteuse ne suffit pas pour s'assurer que le paquet est reçu correctement. En effet, une ou plusieurs stations peuvent effectuer cette procédure et envoyer leurs messages simultanément et causent une collision, notamment quand le réseau est chargé.

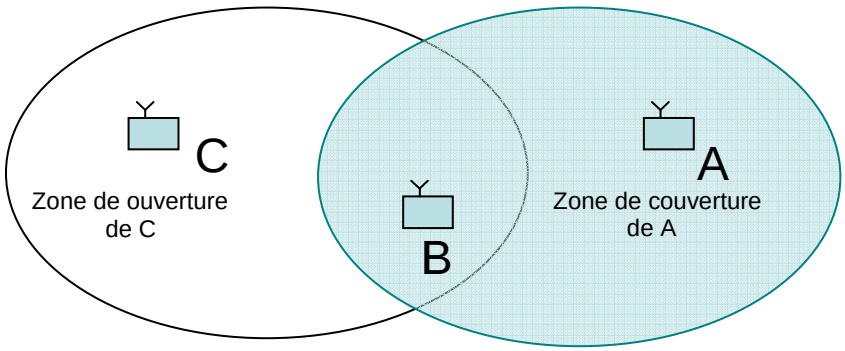
Les collisions sont détectées sur les réseaux filaires en se basant sur la nature de la propagation électromagnétique sur un câble, où, sur des distances modérées, l'amortissement du signal reste faible. En cas de transmission simultanée, le seuil de la puissance est violé et une violation du codage utilisé lors de la transmission peut être détectée. Les stations arrêtent alors de transmettre et tentent de retransmettre en répétant le même processus après des durées aléatoires.

5.1.2 Problème du CSMA dans le cas des réseaux sans fil

Si les mécanismes de détection de collisions s'avèrent adapté pour un réseau local câblé, ils ne le sont pas, en général, pour les réseaux radio. Plusieurs raisons pour cela :

- Dans un environnement sans fil, on ne peut pas être sûr que toutes les stations s'entendent 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.

- Le problème des stations cachées : Ce problème se produit quand deux stations ne peuvent pas s'entendre l'une et l'autre du fait que la distance qui les sépare est trop grande ou qu'un obstacle les empêchent de communiquer entre elles mais elles ont des zones de couverture qui se recoupent. Si les stations A et C ne font que la détection de porteuse en écoutant le canal, n'étant pas en mesure de s'entendre l'une l'autre, elles vont s'autoriser à émettre des paquets même temps à une station B située dans l'intersection des zones de couverture, il va y avoir collision entre les paquets et donc B ne pourra recevoir aucune des communications. On dit que les stations A et C sont cachées l'une par rapport à l'autre.



- Le problème des stations exposées : ce problème arrive dans le cas où une station B transmet des données à une station A. Si une station C écoute le canal radio, elle peut entendre une communication en cours. Elle conclut qu'elle ne peut pas transmettre des paquets à une station D, or si C transmettait, cela créerait des collisions seulement dans la région entre B et C et non dans les régions où D et A se situent.

Pour combler ces problèmes, 802.11 utilise le mécanisme d'**esquive de collision (Collision Avoidance) appelé CSMA/CA**.

5.2 Le CSMA/CA

5.2.1 Principe de l'accusé de réception ACK

Une station voulant transmettre écoute le support, et s'il est occupé, la transmission est différée. Si le support est libre pour un temps spécifique (appelé DIFS, Distributed Inter Frame Space, dans le standard), alors la station est autorisée à transmettre après une durée tirée aléatoirement en se basant sur l'algorithme de Backoff exponentiel (voir partie suivante). La station réceptrice va vérifier le CRC du paquet reçu et renvoie un accusé de réception (ACK). La réception de l'ACK indiquera à l'émetteur qu'aucune collision n'a eu lieu. Si l'émetteur ne reçoit pas l'accusé de réception, alors il retransmet le fragment jusqu'à ce qu'il l'obtienne ou abandonne au bout d'un certain nombre de retransmissions.

Remarque : c'est la couche MAC qui est informée des collisions par l'attente d'un accusé de réception (ACK) pour chaque fragment transmis. Dans le cas de non réception d'un ACK, la couche MAC retransmet le paquet sans avoir à passer par les couches supérieures, ce qui engendrait des délais significatifs.

La différence majeure entre CSMA/CA et CSMA/CD est la possibilité de détection de collisions. Dans la technique CSMA/CD, la collision est détectée à l'émission car les stations ont la possibilité de continuer à écouter leurs transmissions en cours. En revanche, cette collision ne pourra pas être détectée qu'au niveau du récepteur dans le cas du mécanisme CSMA/CA.

Afin de surveiller l'activité du réseau, la sous couche MAC travaille en collaboration avec la couche physique qui utilise l'algorithme CCA (Clear Channel Detection) pour évaluer la disponibilité du canal. Pour savoir si le canal est libre, la couche physique mesure la puissance reçue par l'antenne appelée RSSI (Received Signal Strength Indicator). La couche physique détermine donc si le canal est libre en comparant la valeur du RSSI à un certain seuil et transmet par la suite à la couche MAC un indicateur de canal libre. Dans le cas contraire, la transmission est différée.

5.2.2 Espace entre deux trames

La norme 802.11 définit quatre types d'espace entre deux trames **IFS (Inter Frame Space)**. Ils sont classés du plus court au plus long :

Le premier, le SIFS (Short IFS) est le plus court de tous. Il est utilisé pour la transmission des trames ACK, CTS, réponse à un polling…et des rafales de trames issues d'une même station. Le second PIFS (PCF IFS) est utilisé en mode PCF. Il permet aux transmissions PCF de gagner l'accès au médium par l'utilisation d'un IFS plus petit que celui utilisé pour la

transmission des trames en DCF. Le troisième DIFS (DCF IFS) est le plus couramment utilisé (avec le SIFS). Il est utilisé en mode DCF comme temps minimal d'attente avant transmission. Enfin, le quatrième et plus long EIFS (Extended IFS) est utilisé lorsqu'il y a détection de collision. Ce temps relativement long par rapport aux autres IFS est utilisé comme inhibiteur pour éviter des collisions en série.

Les valeurs des différents PIFS et DIFS sont calculées de la manière suivante :

$$PIFS=SIFS+Slot\ Time$$
$$DIFS= SIFS+ 2 * Slot\ Time$$

où *Slot Time* =durée minimale pour déterminer l'état du canal + temps aller-retour + temps de propagation.
La valeur de SIFS est fixée par la couche physique et est calculée de telle façon que la station émettrice sera capable de commuter en mode réception pour pouvoir décoder le paquet entrant.

La figure suivante illustre la relation entre les IFS. Le slot time est l'unité du canal. Il correspond à l'intervalle minimal entre deux opérations de détection physique de porteuse. Cette valeur est dépendante des caractéristiques de la couche physique considérée. C'est une constante spécifiée par le standard pour une couche physique donnée.

Ces IFS permettent de définir des degrés de priorité. Lorsque plusieurs stations souhaitent émettre simultanément, la station souhaitant émettre les trames les plus prioritaires comme les acquittements pourra les envoyer en premier. Puis seront transmises d'autres trames jugées prioritaires comme celles liées à l'administration réseau ou au trafic qui a des contraintes de délai. Enfin, les informations les moins importantes concernant le trafic asynchrone seront émises après un temps d'attente plus long.

5.2.3 Algorithme de backoff exponentiel BEB (Binary Exponenttiel Backoff)

Le backoff est une méthode bien connue pour résoudre les différents entre plusieurs stations voulant avoir accès au support. Cette méthode demande que chaque station choisisse un délai d'attente aléatoire compris entre 0 et la taille d'une fenêtre de contention de valeur CW qui est égale à un certain nombre de slots, et d'attendre ce nombre de slots avant de transmettre, toujours en vérifiant qu'une autre station n'a pas accédé au support avant elle.

La durée d'un slot (Slot Time) est définie de telle sorte que la station sera toujours capable de déterminer si une autre station a accédé au support au début du slot précédent. Cela divise la probabilité de collision par deux.

Le backoff exponentiel signifie qu'à chaque fois qu'une station choisit un slot et provoque une collision, la durée d'attente aléatoire est augmentée exponentiellement (doublée à la tentative de transmission suivante).

Le standard 802.11définit l'algorithme de backoff exponentiel comme devant être exécuté dans les cas suivant :
- Quand la station écoute le support avant la première transmission d'un paquet et que le support est occupé,
- Après chaque retransmission,
- Après une transmission réussie.

Le seul cas où ce mécanisme n'est pas utilisé est quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS.

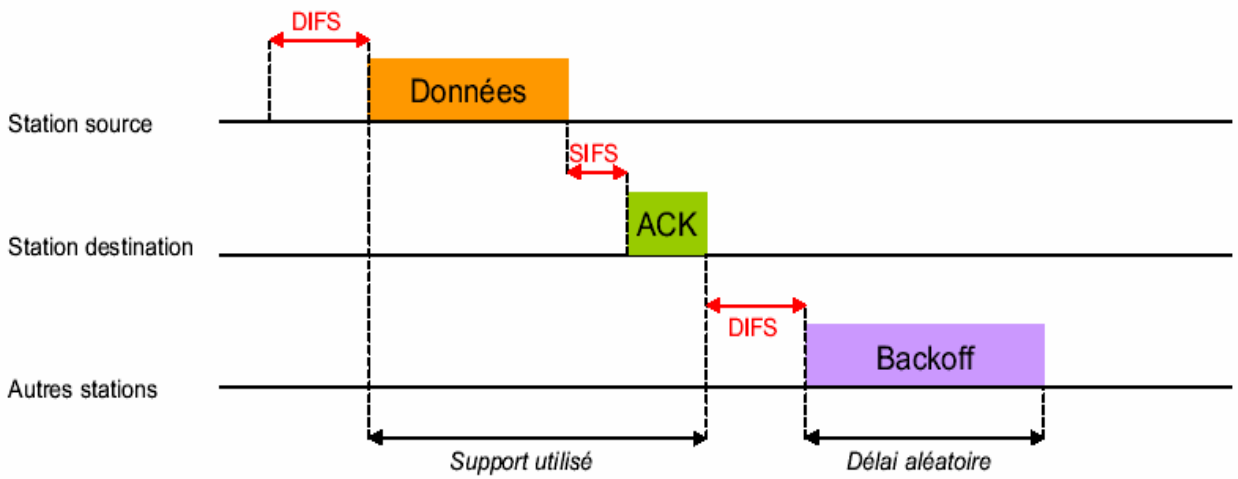
La durée d'attente aléatoire (DAA) du backoff est calculée de la manière suivante :

DAA= CW* random(0,CW)*SlotTime
random(0,CW) est une variable aléatoire uniforme comprise entre 0 et CW-1
CW est la taille de la fenêtre de contention, CW = [CWmin CWmax]
Lors de la première tentative de transmission, CW = CWmin; et à la fois suivante (en cas de collision) CW est doublée jusqu'à ce qu'elle atteigne CWmax.

Exemple wifi :

SlotTime= 20 µs
CWmin= 31
CWmax=1023

La figure suivante montre un exemple de transmission.



La figure suivante montre l'algorithme de la méthode d'accès DCF

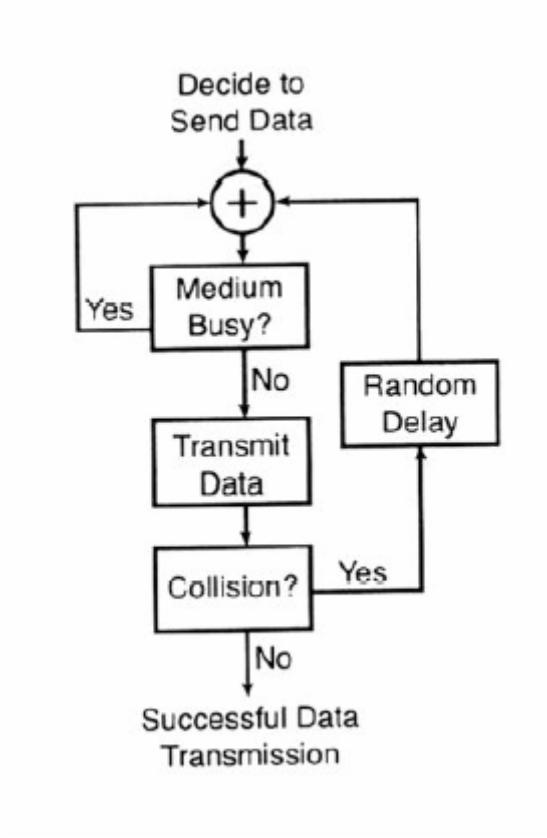


Figure : Algorithme de la méthode d'accès DCF

5.2.4 Mécanisme CSMA/CA avec échange de messages courts RTS et CTS

Il peut tout de même survenir des collisions malgré l'algorithme de reprise après collision BEB et l'acquittement des trames. Pour éviter surtout les problèmes des stations cachées et des trames longues (où les retransmissions coûtent du temps et la ressource spectrale), le standard définit un mécanisme **optionnel** qui permet de faire des réservations de canal. Ce mécanisme est appelé écoute virtuelle de porteuse.

Une station voulant émettre transmet d'abord un petit paquet de contrôle appelé RTS (Request To Send), qui comprend la source, la destination, et la durée de transmission (c'est à direl la durée totale de la transmission du paquet et de son accusé de réception) la station destination répond (si le canal est libre) avec un paquet de contrôle de réponse appelé CTS (Clear To Send) qui inclura les même informations sur la durée.

Toutes les stations écoutant soit la trame comprenant la demande de canal RTS, soit la trame de réponse de réservation CTS, déclencheront leur indicateur de l'écoute virtuelle (Virtual Carrier Sense) appelé NAV pour Network Allocation vector pour une certaine durée, et utilseront cette information avec la procédure d'écoute de support.

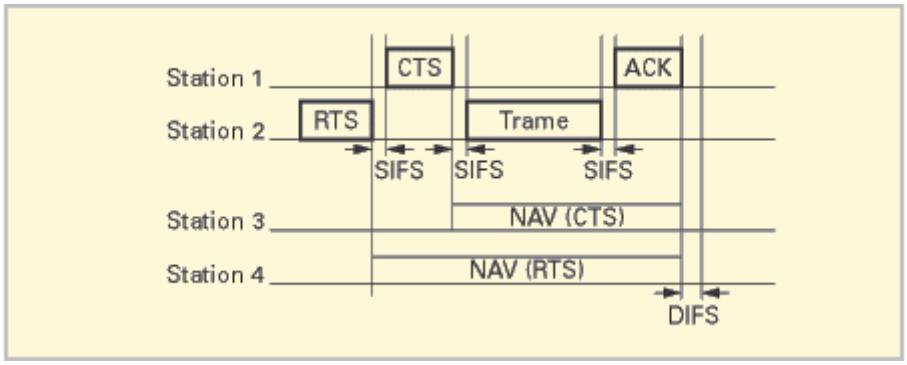
Grâce à l’envoi de la trame RTS, toutes les stations situées dans la couverture radio de la source sont informées d’une transmission imminente et de sa durée éventuelle. Elles peuvent ainsi mettre à jour leur NAV et passer en mode économie d’énergie pour la dite durée. Le CTS a le même rôle d’annonce mais cette fois autour du récepteur. Ces deux trames sont courtes (20 octets pour RTS et 14 octets pour CTS) et rencontrent donc une faible probabilité de collisions.

Ce mécanisme quoique efficace entraîne un surcoût important occasionné par la transmission sur la voie radio des trames de signalisation RTS/CTS. Ce surcoût correspond à autant de

bande passante qui n'est pas utilisée pour transmettre des données. C'est pourquoi à ce mécanisme est associé un seuil de déclenchement qui en limite l'usage lorsque le surcoût devient trop important. Si la longueur des données à transmettre est inférieure à ce seuil, la transmission se fera sans utilisation des trames RTS/CTS. Si le seuil est dépassé alors le mécanisme est utilisé pour la transmission.

Ce mécanisme demeure inopérant pour la transmission de trames diffusées à tous les membres dites trames broadcast. En effet, le destinataire n'étant pas unique, on ne peut avoir de réponse en retour (CTS) et par conséquent des collisions sur les trames diffusées sont toujours possibles.

La figure suivante illustre l'usage du RTS/CTS et du NAV.



5.2.5 Mode PCF (Point Coordination Function)

La **PCF** est une méthode optionnelle et donc peu ou pas implémentée dans les matériels 802.11. La PCF consiste en une gestion centralisée des ressources. C'est le point d'accès qui ordonne les transmissions et distribue le droit à la parole. C'est par l'intermédiaire de trames d'administration définies à cet effet qu'une sollicitation explicite est effectuée auprès d'une station (mécanisme de *polling*) pour lui attribuer le droit à émettre.

5.2.6 Analyse des types de trames utilisés pour le protocole 802.11

Il y a trois principaux types de trames :
- Les trames de **données**, utilisées pour la transmission des données
- Les trames de **contrôle**, utilisées pour contrôler l'accès au support (eg. RTS, CTS, ACK)
- Les trames de **gestion**, transmises de la même façon que les trames de données pour l'échange d'informations de gestion, mais qui ne sont pas transmises aux couches supérieures.

Chacun de ces trois types est subdivisé en différents sous-types, selon leurs fonctions spécifiques.

Format des trames

Toutes les trames 802.11 sont composées des composants suivants :

Préambule	En-tête PLCP	Données MAC	CRC

Préambule

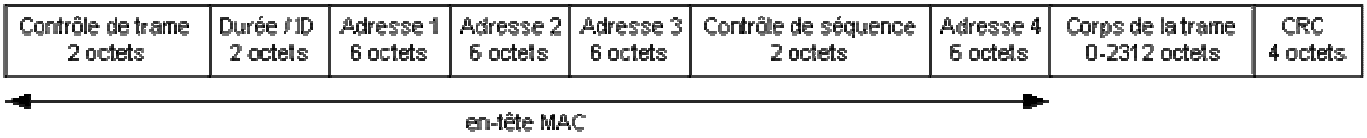
Il est dépendant de la couche physique et comprend :
- Synch : c'est une séquence de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne appropriée (si plusieurs sont utilisées), et pour corriger l'offset de fréquence et de synchronisation.
- SFD : Le Start Frame Delimiter consiste en la suite de 16 bits 0000 1100 1011 1101, utilisée pour définir le début de la trame.

En-tête PCLP (Trame 802.11)

L'en-tête PCLP est toujours transmis à 1 Mbps et contient des informations logiques utilisées par la couche physique pour décoder la trame :
- Longueur de mot du PLCP_PDU : il représente le nombre d'octets que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.
- Fanion de signalisation PLCP : il contient seulement l'information de taux, encodé à 0,5 Mbps, incrémenté de 1 Mbps à 4,5 Mbps
- Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC 16 bits.

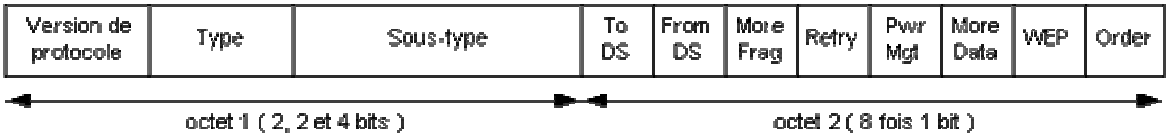
Données MAC (Trame 802.11)

La figure suivante montre le format général de la trame MAC, certains champs sont seulement présents dans une partie des trames, comme décrit ultérieurement.



Contrôle de trame (en-tête MAC)

Le champ de contrôle de trame contient les informations suivantes :



- Version de protocole : ce champ contient 2 bits qui pourront être utilisés pour reconnaître des versions futures possibles du standard 802.11. Dans la version courante, la valeur est fixée à 0.

- Type et sous-type : les 6 bits définissent le type et le sous-type des trames :

Valeur du type	Description du type	Valeur du sous-type (b7 b6 b5 b4)	Description du sous type
00	Gestion	0000	Requête d'association
00	Gestion	0001	Réponse d'association
00	Gestion	0010	Requête de ré-association
00	Gestion	0011	Réponse de ré-association
00	Gestion	0100	Demande d'enquête
00	Gestion	0101	Réponse d'enquête

00	Gestion	0110-0111	Réservés
00	Gestion	100	Balise
00	Gestion	1001	ATIM
00	Gestion	1010	Désassociation
00	Gestion	1011	Authentification
00	Gestion	1100	Désauthentification
00	Gestion	1101-1111	Réservés
01	Contrôle	0000-1001	Réservés
01	Contrôle	1010	PS-Poll
01	Contrôle	1011	RTS
01	Contrôle	1100	CTS
01	Contrôle	1101	ACK
01	Contrôle	1110	CF End
01	Contrôle	1111	CF End et CF-ACK
10	Données	0000	Données
10	Données	0001	Données et CF-ACK
10	Données	0010	Données et CF-Poll
10	Données	0011	Données, CF-ACK et CF-Poll
10	Données	0100	Fonction nulle (sans données)
10	Données	0101	CF-ACK (sans données)
10	Données	0110	CF-Poll (dans données)
10	Données	0111	CF-ACK et CF-Poll (sans données)
10	Données	1000-1111	Réservés
11	Réservé	0000-1111	Réservés

- ToDS (pour le système de distribution) : ce bit est mis à 1 lorsque la trame est adressée au Point d'Accès pour qu'il l'a fasse suivre au DS (Distribution System). Ceci inclut le cas où le destinataire est dans la même cellule et que le Point d'Accès doit relayer la trame. Le bit est à 0 dans toutes les autres trames.

- FromDS (venant du système de distribution) : ce bit est mis à 1 quand la trame vient du DS.

- More Fragments (d'autres fragments) : ce bit est mis à 1 quand il y a d'autres fragments qui suivent le fragment en cours.

- Retry (retransmission) : ce bit indique que le fragment est une retransmission d'un fragment précédemment transmis. Ceci sera utilisé par la station réceptrice pour reconnaître des transmissions doublées de trames, ce qui peut arriver si un paquet d'accusé de réception se perd.

- Power Management (gestion d'énergie) : ce bit indique que la station sera en mode de gestion d'énergie après la transmission de cette trame. Ceci est utilisé par les stations changeant d'état, passant du mode d'économie d'énergie au mode active ou le contraire.

- More Data (d'autres données) : ce bit est également utilisé pour la gestion de l'énergie. Il est utilisé par le Point d'Accès pour indiquer que d'autres trames sont stockées pour cette station. La station peut alors décider d'utiliser cette information pour demander les autres trames ou pour passer en mode actif.

- WEP (sécurité) : ce bit indique que le corps de la trame est chiffré suivant l'algorithme WEP.

- Order (ordre) : ce bit indique que cette trame est envoyée en utilisant la classe de service strictement ordonné (Strictly-Ordered service class). Cette classe est définit pour les utilisateurs qui ne peuvent pas accepter de changement d'ordre entre les trames unicast et multicast.

Durée / ID (en-tête MAC)

Ce champ à deux sens, dépendant du type de trame :
- pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station
- dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

Les champs adresses (en-tête MAC)

Une trame peu contenir jusqu'à 4 adresses, selon le bit ToDS et FromDS définit dans le champ de contrôle, comme suit :

Adresse 1 est toujours l'adresse du récepteur (ie. la station de la cellule qui est le récepteur imsupportt du paquet). Si ToDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station.

Adresse 2 est toujours l'adresse de l'émetteur (ie. celui qui, physiquement, transmet le paquet). Si FromDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice.

Adresse 3 est l'adresse de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, Adresse 3 est l'adresse destination.

Adresse 4 est utilisé dans un cas spécial, quand le système de distribution sans fil (Wireless Distribution System) est utilisé et qu'une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, ToDS et FromDS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire.

La table suivante résume l'utilisation des différentes adresses selon les bits FromDS et ToDS :

ToDS	FromDS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Contrôle de séquence (en-tête MAC)

Le champ de contrôle de séquence est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame, et pour reconnaître les paquets dupliqués. Il consiste en deux

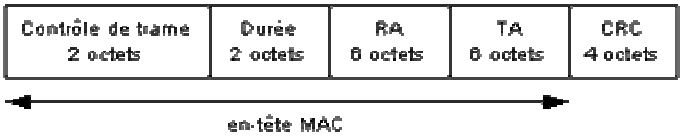
sous-champs, le numéro de fragment et le numéro de séquence qui définissent le numéro de trame et le numéro du fragment dans la trame.

Cyclic Redundancy Check (Trame 802.11)

Le CRC est sur 32 bits.

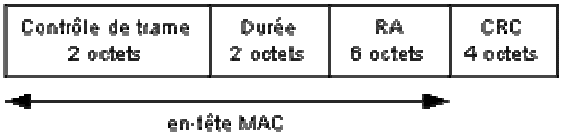
Format des trames les plus courantes

Format des trames RTS



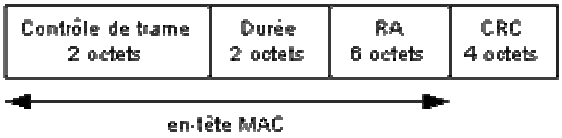
RA est l'adresse du récepteur ??? de la prochaine trame de données ou de gestion.
TA est l'adresse de la station qui transmet la trame RTS.
La valeur de la durée est le temps, en microsecondes, nécessaire à la transmission de la trame de gestion ou de données suivante, plus une trame CTS, plus une trame ACK, plus 3 intervalles SIFS.

Format de la trame CTS



RA est l'adresse du récepteur de la trame CTS, directement copiée du champ TA de la trame RTS.
La valeur de la durée est la valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame CTS et d'un intervalle SIFS.

Format de la trame ACK



RA est le champ directement copié du champ Adresse 2 de la trame précédent cette trame ACK.
Si le bit More Fragment était à 0 dans le champ de contrôle de trame de la trame précédente, la valeur de la durée est mise à 0. Sinon, c'est la valeur du champ durée précédent, moins le temps, en microsecondes, demandé pour transmettre la trame ACK et l'intervalle SIFS.

Annexe

Formules de propagation

Dans la bande ISM, on considère en général une formule de perte du type :

$$L = 40{,}2 + \begin{cases} 20\log(d) & d \le d_{ref} \\ 20\log(d_{ref}) + 33\log\left(\frac{d}{d_{ref}}\right) & d \ge d_{ref} \end{cases}$$

L représente l'affaiblissement en dB et *d* la distance en mètres

Bibliographie :

Livres :

- Wi-Fi par la pratique. Davor MALES, Guy PUJOLLE. Ed EYROLLES.
- 802.11 et les réseaux locaux sans fil, Paul Muhlethaler. Ed EYROLLES.
- De Bluetooth à Wi-Fi, Houda Labiod et Hossam Afifi.

Sites internet :
http://www.wi-fi.org/

Normes

IEEE Std 802.11b-1999 : Wireless LAN Medium Access Control (MAC) and physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band