Chapitre 3. Réseaux Local sans-fils (WLAN)

Technique OFDM pour le Wi-Fi 5

- ⇨ Wi-Fi 5 fonctionne dans la bande U-NII (5 GHz) et n'utilise pas les techniques à étalement de spectre mais l'OFDM qui est une technique plus performante ;
- ⇨ Comme le montre la figure (1), l'OFDM divise les deux premières sous-bandes de l'U-NII en 8 canaux de 20 MHz contenant chacun 52 sous-canaux de 300 KHz ;
- ⇨ La relation entre la fréquence centrale et le numéro de canal est donnée par l'équation suivante :

$$F_{centrale\ du\ canal} = 5000 + 5 \times n_{ch}\ (MHz),$$

Avec : $n_{ch} = 0, 1, 2, \ldots, 200.$

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

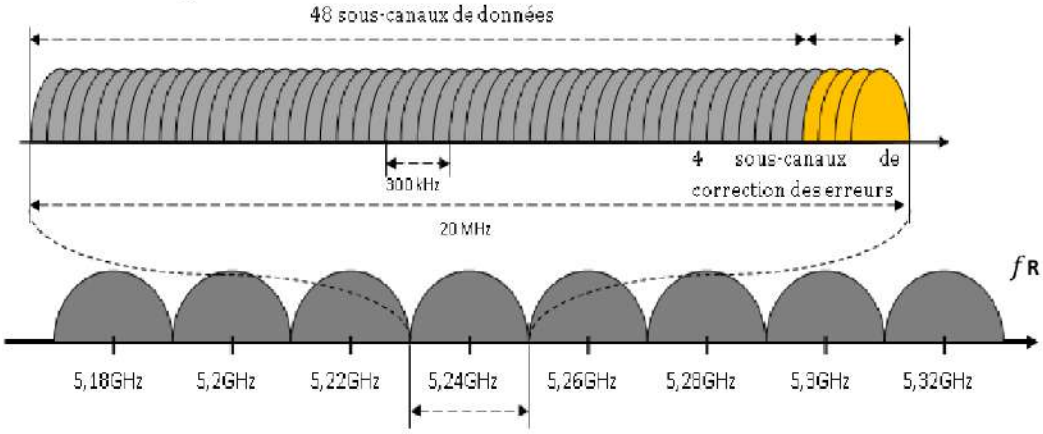


Figure.1. Division de la bande pour le Wi-Fi à base de technique OFDM

- ⇨ L'utilisation de tous les sous-canaux en parallèle pour la transmission permet un débit augmenté de 6 à 54 n_{ch}:
  - ➢ Modulation BPSK : 0,125 Mbits/s par sous-canal : total 6 Mbits/s ;
  - ➢ Modulation QAM64 : 1,125 Mbits/s par sous-canal : total 54 Mbits/s ;
- ⇨ La bande haute contient 4 canaux sur une largeur 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 (5150 MHz et 5350 MHz dans la figure (2)) des bandes basse et centrale ;
- ⇨ Les fréquences centrales des canaux situés aux extrémités de la bande haute doivent être espacées de 20 MHz des fréquences limites (5725 MHz et 5825 MHz dans la figure (2)).

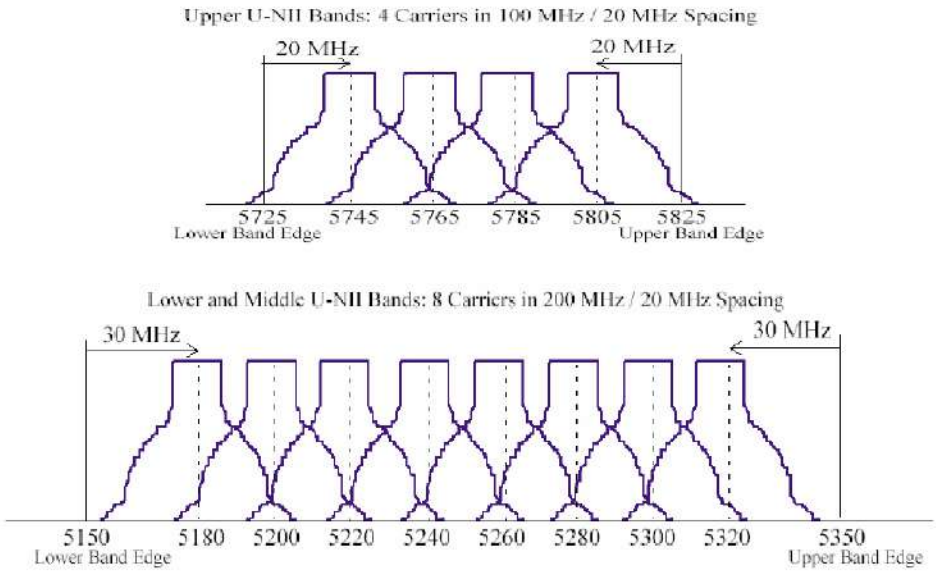


Figure.2. Bande U-NII supérieure et inférieure

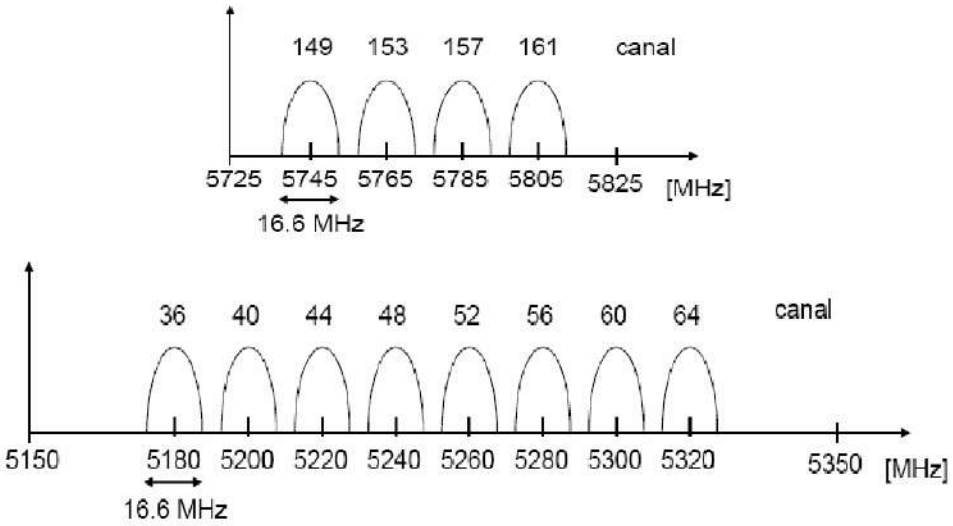


Figure.3. Fréquences centrales et numéros des canaux dans la Bande U-NII

- ⇨ Le Gabarit d'émission est montré sur la figure (4) ;
- ⇨ Comme le montre cette figure, le spectre du signal transmis doit 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 $30\ MHz$.

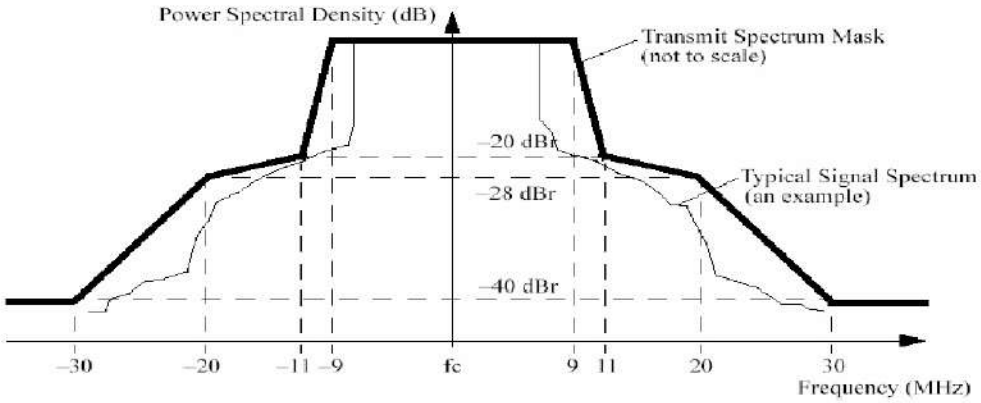


Figure.4. Masque de spectre d'émission

Quelques paramètres de dimensionnant de la couche physique IEEE 802.11a

- ⇨ La forme d'onde OFDM est basée sur une IFFT 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 sont utilisées comme pilotes. Il restera donc 48 porteuses utiles ;
- ⇨ Un intervalle de garde sous la forme d'un préfixe cyclique est ajouté afin de prendre en compte le problème des multitrajets dans canal ;
- ⇨ Ce préfixe cyclique a une durée égale à $0.8\,\mu s$ et le symbole OFDM émis, après insertion du préfixe cyclique, dure $4\,\mu s$.

Schémas de modulation pour l'OFDM

- ⇨ Les 48 symboles fournis toutes les 4 ms au bloc de l'IFFT peuvent provenir de différents schémas de modulation et codage. Le tableau ci-dessous donne un récapitulatif sur les différents schémas de modulation.

Tableau.1. Récapitulatif des modulations utilisées avec l'OFDM

Débit en Mbps	Modulation	Taux de codage	Bits codés par sous-porteuse	Bits de code par symbole OFDM	Bits de données par symbole OFDM
6	BPSK	½	1	48	24
9	BPSK	¾	1	48	36
12	QPSK	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

Utilisation de l'OFDMA et du MU-MIMO

⇨ Les dernières générations du Wi-Fi possèdent de nombreuses fonctionnalités améliorées. Deux d'entre elles sont des technologies multi-utilisateurs. Il s'agit de l'OFDMA et du MU-MIMO ;

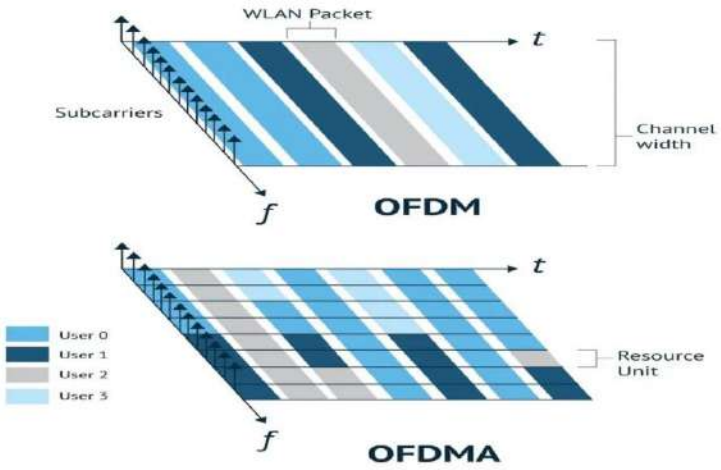


Figure.5. OFDMA versus OFDM

⇨ OFDMA signifie accès multiple par répartition orthogonale de la fréquence.
⇨ MU-MIMO signifie Multi-Utilisateurs Multiples Entrées Multiples Sorties. Également connu sous le nom de MIMO multi-utilisateurs ;
⇨ MU-MIMO représente une avancée significative par rapport au MIMO mono-utilisateur (SU-MIMO), généralement appelé MIMO ;

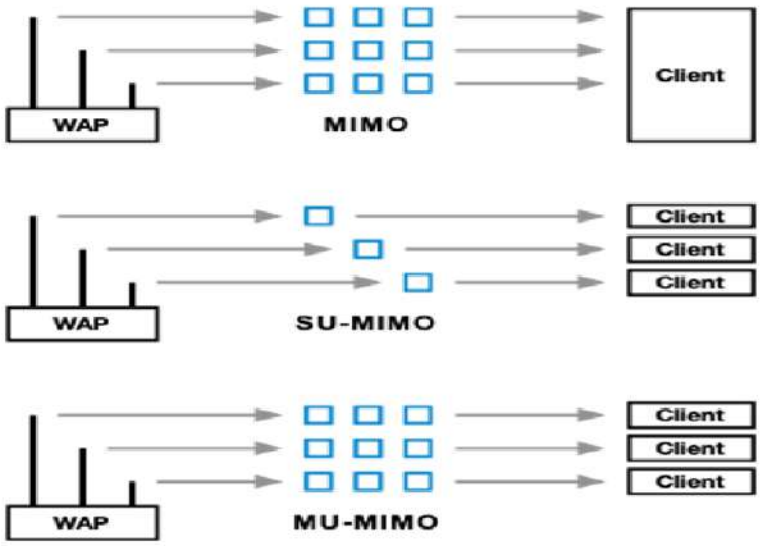


Figure.6. MIMO, SU-MIMO et MU-MIMO

⇨ Comme le montre la figure (7), SU-MIMO émet généralement des signaux comme un anneau du centre vers l'extérieur et communique avec les appareils à tour de rôle en fonction de la distance (pas le sens absolu de la distance, mais plus de qualité de signal, etc.). Lorsqu'il y a trop de périphériques d'accès, certains périphériques doivent attendre et le réseau sera en retard.

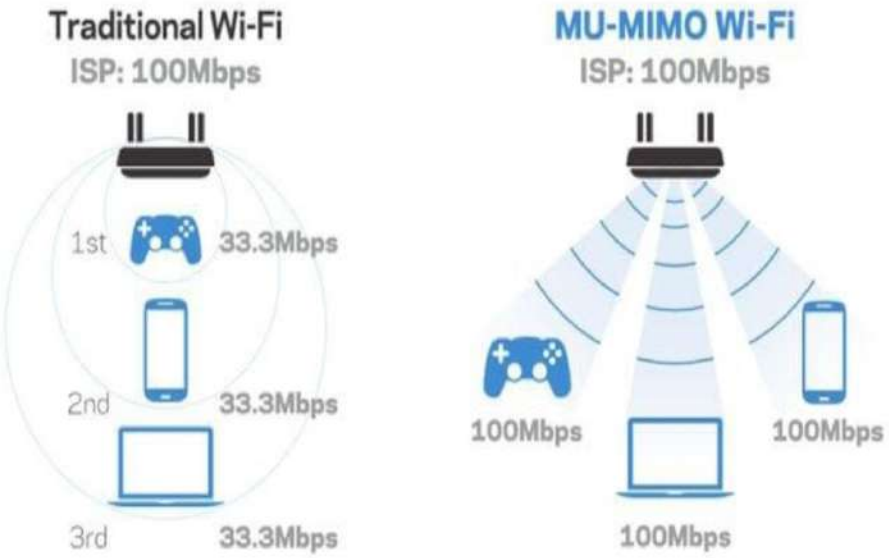


Figure. 7. SU-MIMO versus MU-MIMO

⇨ MU-MIMO est différent. En effet, ses signaux sont divisés en plusieurs parties dans les trois dimensions du domaine temporel, du domaine fréquentiel et du domaine spatial, ce qui revient à envoyer plusieurs signaux différents en même temps. Ainsi, le routeur MU-MIMO peut fonctionner avec plusieurs appareils simultanément. En particulier, comme plusieurs signaux n'interfèrent pas les uns avec les autres, les ressources sont maximisées ;

⇨ La technologie MU-MIMO a été créée pour aider à augmenter le nombre d'utilisateurs simultanés qu'un seul point d'accès peut prendre en charge ;

⇨ Ces deux technologies (OFDMA et MU-MIMO) multi-utilisateurs sont des améliorations techniques importantes fournies avec le Wi-Fi 6. Elles permettent d'accéder à une communication bidirectionnelle simultanée entre les appareils et le point d'accès ;

⇨ Chaque technologie peut être utilisée pour envoyer et recevoir des données vers/depuis plusieurs appareils en même temps ;

⇨ Bien que ces technologies soient similaires, elles présentent des différences essentielles données comme suit :

➢ L'OFDMA permet un accès multi-utilisateur en subdivisant un canal ;

➢ MU-MIMO permet un accès multi-utilisateur en utilisant différents flux spatiaux.

➢ En d'autres termes, OFDMA divise un canal et MU-MIMO utilise des canaux séparés.

Avantage de l'OFDMA

➢ L'OFDMA peut allouer l'ensemble du canal à un seul utilisateur. Il peut subdiviser un canal pour servir plusieurs utilisateurs en même temps ;

➢ L'OFDMA est une fonctionnalité intéressante pour les applications à faible bande passante, car il permet une meilleure réutilisation des fréquences, une latence réduite et une efficacité accrue dans les environnements denses ;

Avantage du MU-MIMO

➢ MU-MIMO complète l'OFDMA car il augmente la capacité et l'efficacité dans les applications à large bande passante ;

➢ MU-MIMO est également une technologie qui fournit un canal à plusieurs utilisateurs à la fois (jusqu'à 8 clients dans un groupe) ;

➢ Contrairement à l'OFDMA, MU-MIMO est idéal pour les jeux en ligne, les vidéoconférences ou les cours en ligne.

OFDMA versus MU-MIMO

⇨ Les technologies OFMDA et MU-MIMO se complètent pour augmenter les performances sur la liaison montante et la liaison descendante ;

⇨ L'OFDMA convient mieux aux applications à faible bande passante, tandis que le MU-MIMO sert mieux les applications à bande passante élevée ;

⇨ Avec le Wi-Fi 6, nous avons accès aux deux technologies. Les deux ont une approche gérée qui se traduit par un meilleur Wi-Fi.

La couche liaison de données pour la norme IEEE 802.11

⇨ Pour la norme IEEE 802.11, cette couche est composée de deux sous-couches (voir la figure (8)) :

➢ La sous-couche de *contrôle de la liaison logique* (*Logical Link Control*, notée **LLC**) ;

➢ La sous-couche de *contrôle d'accès au support* (*Media* Access Control, ou MAC).

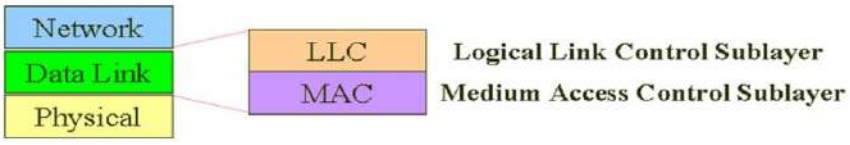


Figure.8. Couche liaison de données pour la norme IEEE 802.11

- La norme 802.11 utilise la même couche LLC du 802.2 ;
- Elle utilise également le même adressage 48 bits du LAN 802. Ceci permet en effet une simple interconnexion des réseaux sans fil aux réseaux câblés IEEE ;
- La couche MAC est unique au réseaux WLAN. Elle contrôle l'interaction des périphériques ;
- La sous-couche LLC traite de l'adressage et du multiplexage.

La couche MAC

- L'architecture de la sous-couche MAC comprend la fonction de coordination distribuée DCF (pour distributed coordination function en anglais) ;
- Elle comprend aussi la fonction de coordination ponctuelle PCF (pour point coordination function en anglais) ;
- La DCF et la PCF fonctionnent au sein du même BSS ;
- Les deux modes d'accès travaillent d'une façon alternée, avec une période sans contention CFP (Contention Free Period - فترة خالية من النزاعات) suivie d'une période de contention (CP فترة تنازع).

Fonction DCF

- La DCF est la méthode d'accès fondamentale du MAC IEEE 802.11 et est connue sous le nom CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance en anglais) ;
- L'accès au canal est de type compétitif (تنافسي) avec minimisation du nombre de collisions ;
- La méthode distribuée est mieux adaptée à un trafic déséquilibré entre les postes ;
- Elle est moins efficace pour les trafics de type "temps réel".

Fonction PCF

- C'est un mécanisme optionnel du standard IEEE 802.11 et est peu utilisé ;
- Dans les infrastructures avec points d'accès, l'accès peut être contrôlé de manière centralisée ;
- Le fonctionnement du PCF est essentiellement celui de l'interrogation, avec une station (coordinateur de point) jouant le rôle de maître d'interrogation ;
- Un accès par compétition règle les requêtes de transmission au point d'accès ;
- Celui-ci attribue ensuite de façon explicite les autorisations d'accès aux stations (Polling) ;
- La méthode centralisée est mieux adaptée aux flux de type "temps réel". Cependant, son efficacité diminue avec la mise en veille des postes et leur changement de cellule.

La méthode d'accès CSMA/CA

⇨ Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est la CSMA/CD (Carrier Sense Multiple Access with Collision Detect), pour laquelle chaque machine est libre de communiquer à n'importe quel moment ;

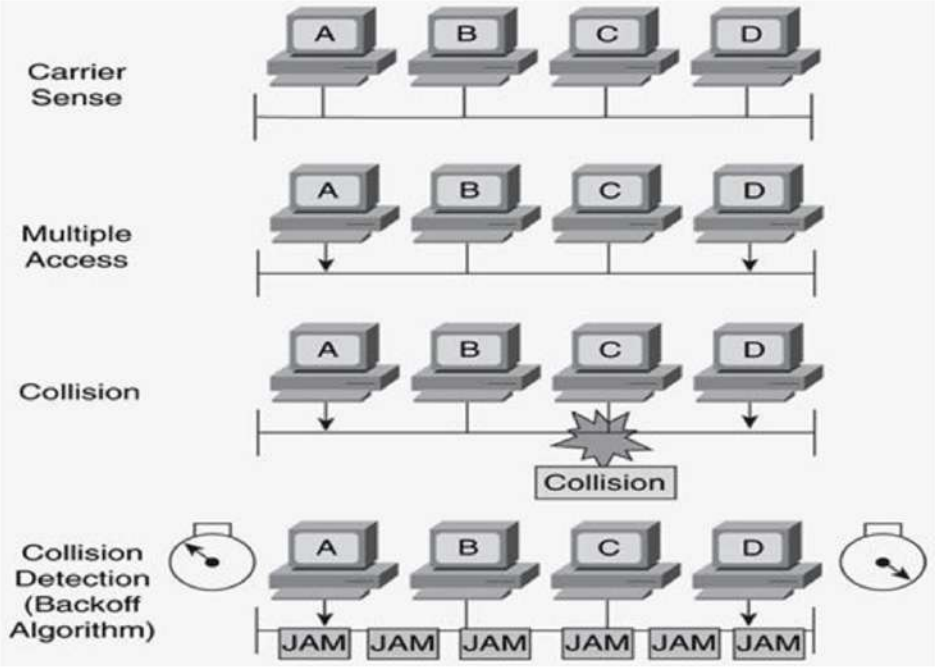


Figure.9. CSMA/CD

⇨ Chaque machine, voulant envoyer un message, vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine ;
⇨ Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre (Figure (9)) ;
⇨ Dans un environnement sans fil, ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée ;
⇨ Deux problèmes existent notamment le problème du terminal caché et le problème du terminal exposé ;

Exemple de terminal caché : comme le montre la figure (10), le terminal « A » communique avec le terminal « C ». Le terminal « B » ne sait pas que « A » communique avec « C » et il pense que « C » est inactif. En conséquence, « B » essaie également de communiquer avec « C » et provoque ainsi une collision en « C ». Par conséquent, « B » est un terminal caché par rapport à « A ».

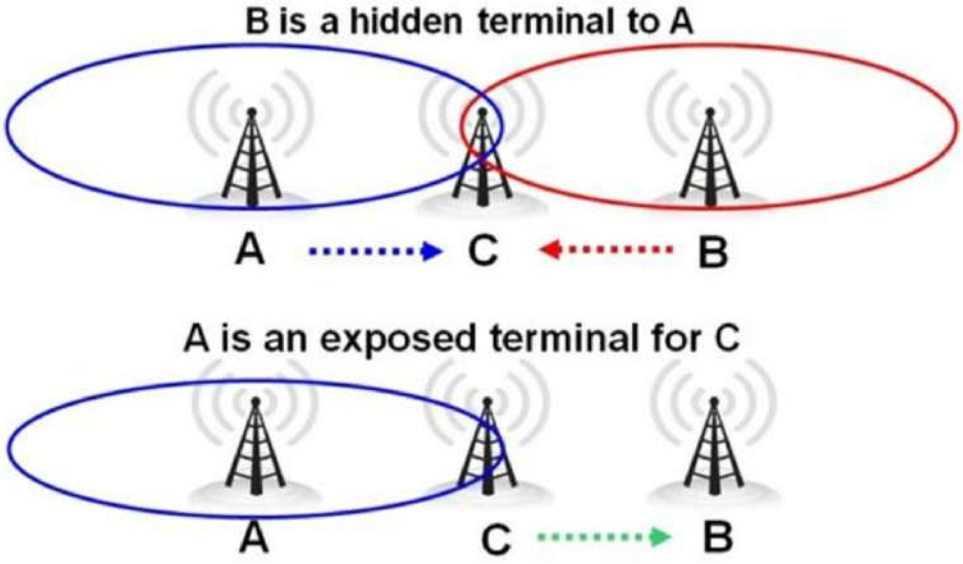


Figure.10. Terminal caché et terminal exposé

Exemple de terminal exposé : comme le montre la même figure (plan du dessous), le terminal « A » communique avec certains terminaux autres que « B » et « C ». Cependant, « C » se trouve dans la zone de couverture de « A » et il pense que le canal est occupé. Par conséquent, « C » ne peut pas communiquer avec « B » même si « C » et « B » sont inactifs. Par conséquent, « A » est un terminal exposé pour « C ».

- ⇨ Pour régler ces problèmes, la norme 802.11 propose un protocole similaire à celui de la CSMA/CD, appelé CSMA/CA ;
- ⇨ Le protocole CSMA/CA utilise un mécanisme d'évitement de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur ;
- ⇨ Le terme CSMA/CA est composé de trois composants individuels donnés comme suit :
  - ➢ **Carrier Sense (CA)** : Envoyer des données via le réseau uniquement dans le cas où le canal est libre ➔ Les données ne sont pas envoyées tant que le canal n'est pas disponible ;
  - ➢ **Multiple Access (MA)** : plusieurs appareils partagent un même canal de transmission. Pour que la communication soit efficace, il est essentiel qu'ils adhèrent à un protocole contraignant ;
  - ➢ **Collision Avoidance (CA)** : un mécanisme tente de s'assurer que deux participants ou plus ne démarrent pas une transmission en même temps. Cela permet donc d'éviter les collisions. S'il se produit néanmoins des chevauchements, ceux-ci sont détectés et la transmission est alors réessayée.

Principe de la méthode CSMA/CA

- ⇨ La méthode CSMA/CA tente de réduire la fréquence des collisions et fournit en même temps un plan et une structure sur la façon de procéder en cas de collision ;
- ⇨ Dans un réseau décentralisé, il est nécessaire que tous les participants suivent ensemble des règles communes et organisent ainsi la communication entre eux ;
- ⇨ L'idée de base de la CSMA/CA repose sur le principe de « *Listen before Talking* » (Écouter avant de parler) ;
- ⇨ Ceci signifie qu'il faut d'abord vérifier si le service est libre « idle » (inactif) avant que la station puisse commencer une transmission ;
- ⇨ La procédure de la CSMA/CA avec accusé de réception est montrée dans la figure (11).

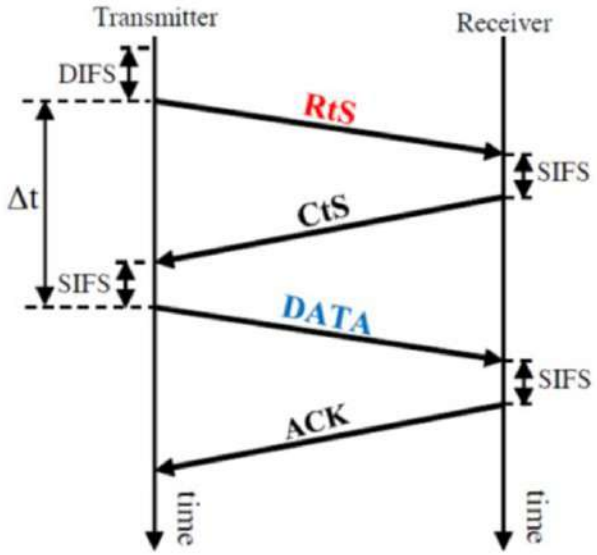


Figure.11. Procédure de la CSMA/CA

- ➢ La station voulant émettre écoute le réseau ;
- ➢ Si le réseau est encombré, la transmission est retardée ;
- ➢ Dans le cas contraire, si le média est libre, pendant un temps donné appelé DIFS (Distributed Inter Frame Space), alors la station peut émettre ;
- ➢ Comme le montre la figure (11), la station transmet alors un message appelé RTS (Ready To Send) signifiant « prêt à émettre ». Ce message contient des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission ;
- ➢ Le récepteur (généralement un point d'accès) répond par une message CTS (Clear To Send), signifiant « le champ est libre pour émettre » ;
- ➢ La station commence ensuite l'émission des données ;

- Après la réception de toutes les données émises par la station, le récepteur envoie un accusé de réception ACK (ACKnowledgment) ;
- Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

Structure temporelle de la CSMA/CA

- Dans la CSMA/CA, la technique DCF contrôle le temps d'attente d'une station avant d'initier une transmission sur un canal libre ;
- La DCF attribue aussi certaines durées du slot aux participants du réseau pour d'autres actions créant ainsi une structure temporelle contraignante ;
- Cette procédure est l'axe central de la prévention des collisions ;
- La structure temporelle complexe permet en effet d'éviter les collisions ;
- La DCF prend en compte divers intervalles, lors de la création de la structure temporelle. Ces derniers sont donnés comme suit :
  - **DCF Interframe Space (DIFS)** : dans un premier temps, les participants doivent surveiller le réseau pendant la durée d'un DIFS afin de déterminer si le réseau est bien libre. Pour la CSMA/CA, cela signifie qu'aucune station n'émet à portée au moment de la transmission. Le DIFS est compris entre 28 et 50 µs ;
  - **Contention Window (CW)** : si les participants déterminent que le canal est libre, ils attendent une période de temps aléatoire avant de commencer à transmettre. Cette durée correspond à la fenêtre de contention. Cette fenêtre temporelle double à chaque collision et correspond au BEB (*Binary Exponential Backoff*), comme dans la CSMA/CD ;
  - **Short Interframe Space (SIFS)** : après l'envoi du paquet de données, le nœud destinataire envoie une notification si la procédure RTS/CTS est aussi utilisée. Cependant, il doit attendre également une période de temps fixe avant la transmission. SIFS est le temps qu'il faut pour traiter un paquet de données. La durée dépend de la norme IEEE 802.11 utilisée et se situe entre 10 µs et 16 µs. Notons que DIFS est égal à SIFS + 2 fois la durée d'un slot ;
  - **Extended Interframe space (SIFS)** : L'espacement inter-trames étendu EIFS est une période d'attente utilisée dans la couche MAC de la norme IEEE 802.11. Il s'agit d'une période d'attente supplémentaire utilisée en plus du DISF obligatoire en cas de trames corrompues.

Algorithme Backoff

- Comme nous l'avons déjà vu plus haut, dans le réseau IEEE 802.11, avec le protocole MAC basé sur la CSMA/CA, chaque station ayant un paquet à transmettre écoute d'abord le canal pour savoir s'il est utilisé ;
- Si le canal est détecté comme inactif pendant un intervalle supérieur à DIFS, la station procède à la transmission ;

- ⇨ Si le canal est détecté comme occupé, la station reporte la transmission jusqu'à la fin de la transmission en cours ;
- ⇨ Dans ce cas, la station initialise un temporisateur d'attente (Backoff) avec un intervalle d'attente choisi aléatoirement et décrémente ce Backoff chaque fois qu'elle détecte que le canal est inactif ;
- ⇨ La décrémentation du Backoff est arrêtée lorsque le canal est occupé et elle est relancée lorsque le canal redevient inactif pour une durée DIFS ;
- ⇨ La station commence sa transmission lorsque le Backoff atteint la valeur zéro ;
- ⇨ La probabilité que deux ou plusieurs stations choisissent la même valeur de Backoff est faible, puisque ce dernier est choisi de manière aléatoire ;
- ⇨ La longueur de l'intervalle Backoff T_B est obtenue à partir de la formule suivante :

$T_B = Random(0, CW) \times T_S$.
T_S est le temps d'un time-slot.
$Random(0, CW)$ est un nombre tiré aléatoirement (distribution uniforme) sur l'intervalle $[0, CW]$;
Le paramètre de fenêtre de contention CW est un nombre entier appartenant à la plage de valeurs $[CW_{min}, CW_{max}]$;

L'ensemble des valeurs CW est constitué des puissances séquentiellement croissantes de 2, moins 1 (Voir la figure (12)). On commence par une valeur spécifique PHY CW_{min} et on termine par une valeur spécifique PHY CW_{max} ;

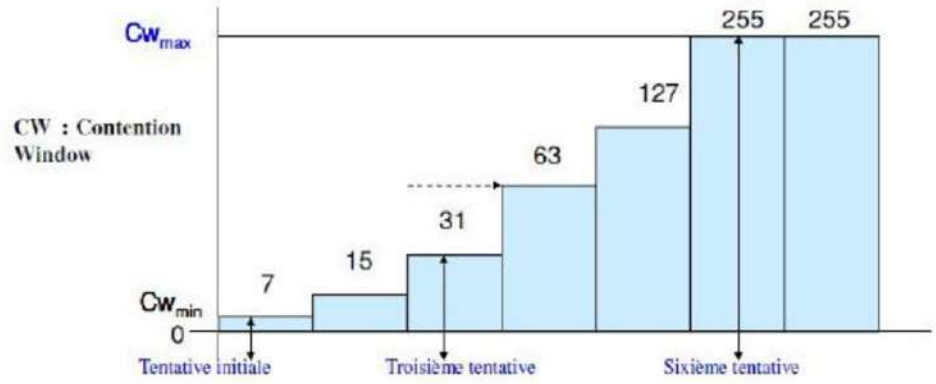


Figure.12. Valeurs de CW

- ⇨ Le CW doit prendre la valeur suivante (supérieure) dans la série (7, 15, 31, 63, ..., CW_{max}) chaque fois qu'une tentative infructueuse de transmission entraîne l'incrémentation du compteur de temporisateur de relance de la station, jusqu'à ce que le CW atteigne la valeur de CW_{max} ;
- ⇨ Dans le 802.11a et g, $CW_{min} = 15$ et $CW_{max} = 1023$;
- ⇨ Dans le 802.11b, $CW_{min} = 31$ et $CW_{max} = 1023$;

- ⇨ Une fois que CW atteint CW_{max}, il reste à la valeur de CW_{max} jusqu'à ce qu'il soit réinitialisé. Cela améliore la stabilité du protocole d'accès dans des conditions de charge élevée ;
- ⇨ L'opération de la DCF, basée sur l'algorithme Backoff, est montrée sur la figure (13).

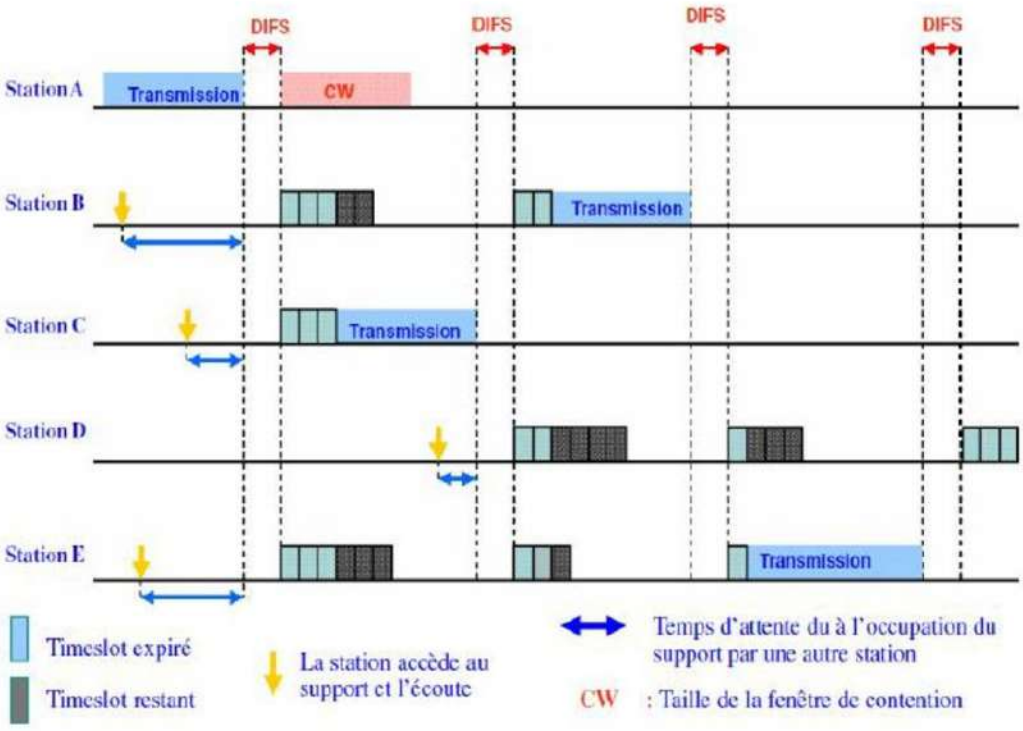


Figure.13. L'opération de la DCF utilisant le Backcoff.

Espaces de temps entre les trames

- ⇨ Comme le montre la figure (14), quatre intervalles de temps différents entre les trames sont définis ;

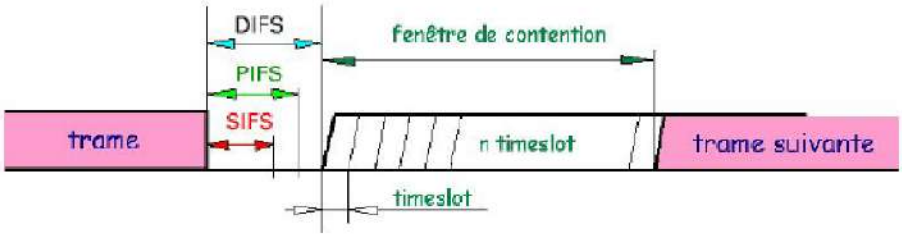


Figure.14. Espaces temps définis par le Wi-Fi

- ⇨ Ils fournissent des niveaux de priorité pour l'accès aux médias sans fil ;

- ⇨ Ils sont classés dans l'ordre, du plus court au plus long : SIFS - espace intertrame court, PIFS - espace intertrame PCF, DIFS - espace intertrame DCF, espace intertrame étendu EIFS ;
- ⇨ SIFS est utilisé lorsqu'une station occupe le canal et a besoin de le conserver pendant toute la durée de la séquence d'échange de trames ;
- ⇨ L'utilisation du plus petit intervalle entre les transmissions empêche les autres stations (qui doivent attendre que le support soit inactif pendant un intervalle plus long) de tenter d'utiliser le support ;
- ⇨ Le PIFS doit être utilisé uniquement par les stations actives pour obtenir un accès prioritaire au support au début du CFP.

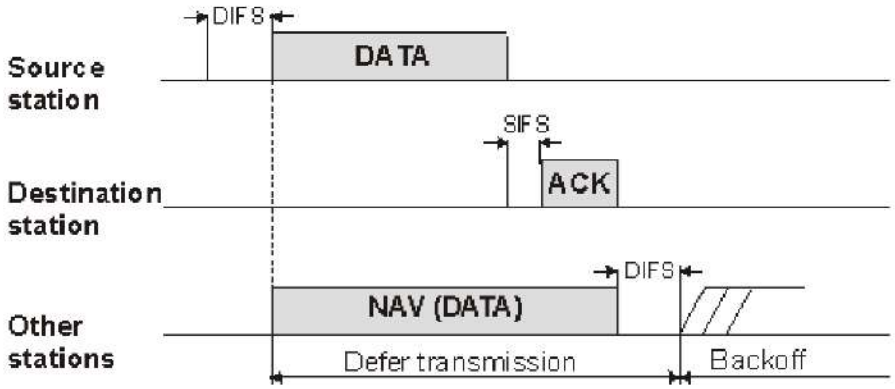


Figure.15. Mécanisme de détection (sensation) virtuelle de la porteuse

- ⇨ Chaque trame de données transmise contient un champ de durée, qui indique la période du canal réservée à sa transmission ;
- ⇨ Ces informations sont utilisées par les stations qui peuvent entendre l'émetteur pour mettre à jour leurs vecteurs d'allocation de réseau NAV (Network Allocation Vectors) ;
- ⇨ NAV est un mécanisme virtuel de détection de porteuse utilisé pour limiter le besoin de détection de porteuse physique afin d'économiser de l'énergie ;
- ⇨ C'est un temporisateur toujours décroissant si sa valeur est différente de zéro. Une station n'est pas autorisée à initier une transmission si son NAV est différent de zéro ;
- ⇨ Avant qu'un appareil du réseau ne commence une transmission, il envoie d'abord des informations (dans le champ *Duration* de la trame RTS) à tous les autres participants. La station indique combien de temps le réseau sera occupé par la transmission. Tout autre appareil saisit cette information dans son NAV personnel. Celle-ci est traitée pour spécifier le moment à partir duquel une nouvelle tentative de transmission sera possible ;
- ⇨ L'utilisation de NAV pour déterminer l'état occupé/inactif du canal est appelée mécanisme de détection (sensation) virtuelle de la porteuse (voir la figure (15)) ;

- ⇨ Un NAV peut augmenter la durée d'attente d'un maximum de 33 ms (32.767 μs). Il s'agit de la durée maximale pendant laquelle un expéditeur peut bloquer le support. Les appareils du réseau sont inactifs jusqu'à l'expiration du NAV. Cela permet d'économiser de l'énergie. Ce n'est que lorsque le compteur devient 0 que l'abonné redevient actif et vérifie donc le réseau ;
- ⇨ Le NAV n'est pas seulement ajusté par le RTS, mais il est aussi influencé par le CTS et ACK. Ce dernier est un signal émis pour que tous les participants réinitialisent leurs NAV à 0 : le support ou médium est donc à nouveau libre ;
- ⇨ Des accusés de réception positifs immédiats sont utilisés pour déterminer la réception réussie de chaque transmission de trame de données ;
- ⇨ Ceci est accompli par le récepteur, immédiatement après la réception de la trame de données, par la transmission d'une trame d'accusé de réception ACK après un intervalle de temps SIFS ;
- ⇨ Si la trame ACK n'est pas reçue, la trame de données est supposée perdue et une retransmission est programmée.

Comparaison entre CSMA/CA et CSMA/CD

- ⇨ La CSMA/CA est une adaptation de la procédure de traitement des collisions (CSMA/CD), utilisée dans les réseaux Ethernet semi-duplex, aux réseaux sans fil ;
- ⇨ CSMA/CD ne tente pas d'éviter directement les collisions. Au lieu de cela, ce protocole établit un mécanisme permettant aux participants du réseau de procéder, en cas de collision pour éviter notamment que celle-ci ne se reproduise lors d'une seconde tentative ;
- ⇨ Une période de temps aléatoire (déterminée par l'algorithme de *Backoff*) doit alors être respectée par les stations après l'échec d'une transmission afin que les deux participants ne recommencent pas à émettre de manière simultanée (ce qui est la cause de l'échec) ;
- ⇨ Un réseau sans fil ne peut pas être surveillé de manière aussi sûre qu'un réseau câblé ;
- ⇨ Les collisions peuvent être causées par un deuxième émetteur hors de portée du premier. En effet, ni l'un ni l'autre n'a le moyen de percevoir la tentative d'envoi de l'autre. Par conséquent, l'accent doit être mis sur la réduction de la probabilité de collisions ;
- ⇨ CSMA/CA tire la stratégie « *Backoff* » en amont du processus et l'utilise déjà avant le premier processus d'expédition. La probabilité que les participants du réseau lancent une transmission de manière simultanée, causant des collisions, est donc complétement réduite.

CSMA/CA avec Mécanismes RTS/CTS

- ⇨ Un échange réussi des trames RTS et CTS permet de réserver le canal pour la durée nécessaire au transfert de la trame de données ;

- ⇨ Le mécanisme RTS/CTS offre de meilleures performances réseau si des stations masquées sont présentes sur le réseau ;
- ⇨ Les règles de transmission d'une trame RTS sont les mêmes que celles de la trame de données. C'est-à-dire que l'émetteur émet une trame RTS après que le canal a été inactif pendant un intervalle de temps supérieur à DIFS. En effet, il indique clairement qu'il veut démarrer une transmission et occupera le support de transmission pendant un certain temps ;
- ⇨ Après réception d'une trame RTS, le récepteur répond par une trame CTS, après le temps SIFS. La trame CTS accuse réception de la réception réussie de la trame RTS ;
- ⇨ Comme pour la trame RTS, tous les autres participants sont informés que le support de transmission est actuellement occupé et que l'émetteur est activé pour la transmission. Ce n'est alors qu'à ce moment-là que l'appareil d'origine commence à transmettre les données. Maintenant, il n'est pas possible pour les participants à un réseau sans fil de détecter les collisions ou bien d'autres interférences pendant la transmission ;
- ⇨ Après l'échange réussi des trames RTS/CTS, la trame de données est envoyée par l'émetteur, après avoir attendu un intervalle de temps de SIFS ;
- ⇨ Dans le cas où la trame CTS n'est pas reçue dans l'intervalle de temps défini, le RTS est retransmis en suivant la procédure de Backoff spécifiée pour la DCF. En effet, dans ce cas, l'expéditeur des données suppose qu'une complication s'est produite. Il a par conséquent un droit prioritaire à utiliser le média. Il n'a pas besoin d'attendre jusqu'à ce que le canal soit libre ;
- ⇨ La méthode d'accès au canal utilisant des trames RTS/CTS est présentée à la figure (16).

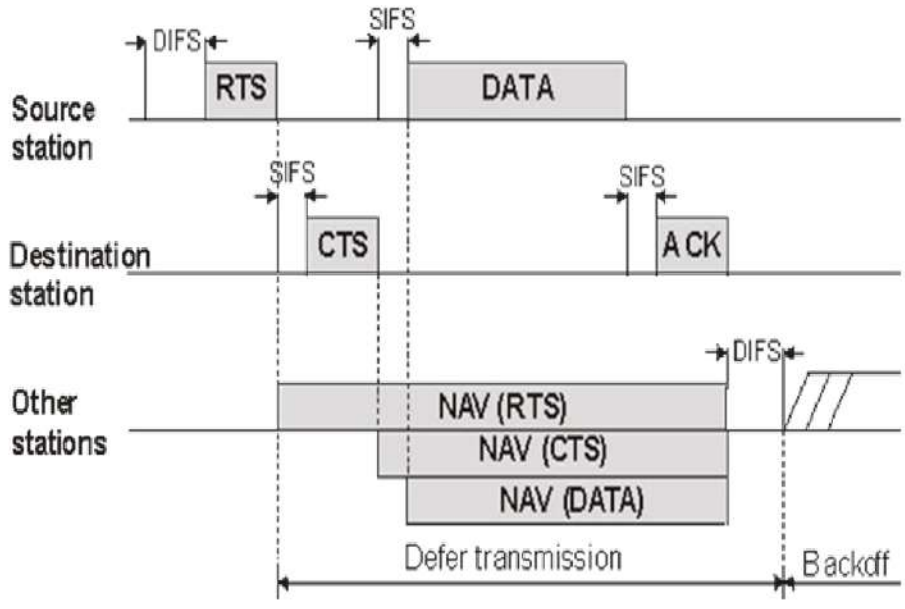


Figure.16. Accès au canal en utilisant le mécanisme RTS/CTS.

⇨ L'algorithme CSMA/CA+RTS/CTS est montré dans la figure (17).

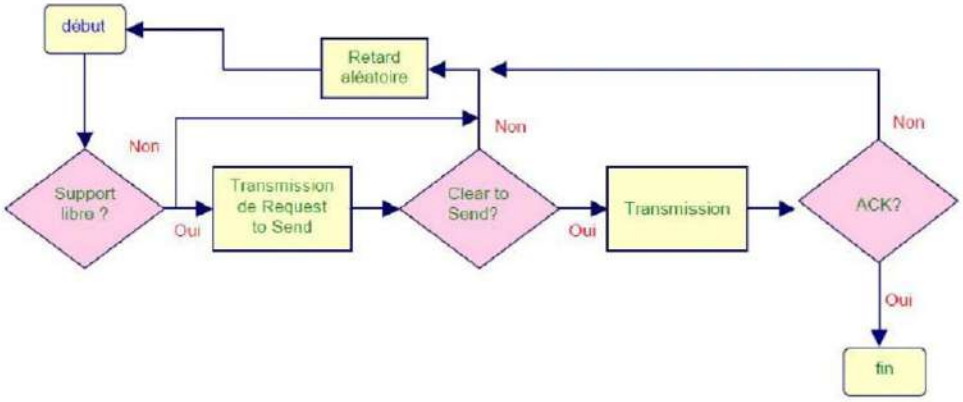


Figure.17. L'algorithme CSMA/CA+RTS/CTS

Processus d'authentification & d'association

⇨ Une fois qu'une station a trouvé un Point d'Accès et a décidé de rejoindre une cellule (BSS), le processus d'authentification s'enclenche. Celui-ci consiste en l'échange d'informations entre le Point d'Accès et la station, où chacun des deux partis prouve son identité par la connaissance d'un certain mot de passe ;

⇨ Une fois la station authentifiée, le processus d'association s'enclenche. Celui-ci consiste en un échange d'informations sur les différentes stations et les capacités de la cellule, et autorise le DSS (les Points d'Accès enregistre la position actuelle de la station) ;

⇨ Après le processus d'association, la station peut transmettre et recevoir des trames de données.

⇨ La procédure d'association d'une station au réseau sans fil suit les étapes suivantes (figure (18)) :

1. La station émet une demande d'enregistrement ;
2. Les points d'accès répondent à la requête ;
3. La station évalue les réponses et sélectionne le point d'accès présentant les conditions les plus favorables puis émet une trame de "demande d'authentification" ;
4. En retour, le point d'accès envoie un texte ;
5. La station chiffre ce texte avec la clé d'authentification du point d'accès ;
6. Le point d'accès confirme l'authentification de la station ;
7. La station envoie une demande d'association au point d'accès ;
8. Le point d'accès confirme l'association.

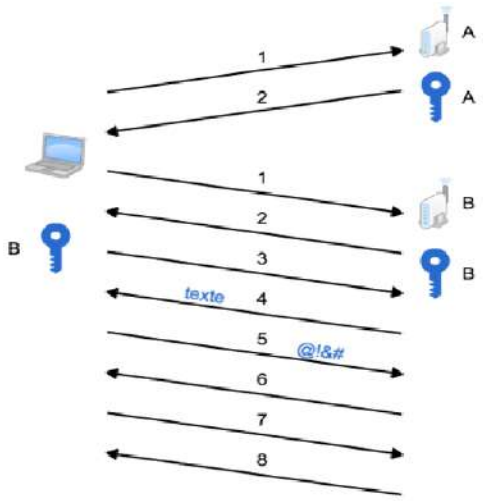


Figure.18. Processus d'association d'une station au réseau sans fil

Le Roaming

- ⇨ Le roaming est le processus de mouvement d'une cellule vers une autre sans fermer la connexion (Handover dans la téléphonie portable) ;
- ⇨ Sur un LAN (Transmission par paquets), la transition d'une cellule à une autre doit se faire entre deux transmissions de paquets (roaming plus facile) ;
- ⇨ Dans un système vocal, 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 comment le roaming est fait, mais en définit cependant les règles de base. Celles-ci comprennent l'écoute active ou passive, le processus de ré-association, où une station qui passe d'un Point d'Accès à un autre sera associée au nouveau Point d'Accès.

Synchronisation continue

- ⇨ Les stations doivent rester synchronisées. Pour se faire, sur une même cellule, la synchronisation des horloges des stations avec l'horloge du Point d'Accès est réalisée selon le mécanisme suivant :
  1- Le Point d'Accès transmet périodiquement des trames appelées « trames balise ». Ces trames contiennent la valeur de l'horloge du Point d'accès au moment de la transmission ;
  2- Les stations réceptrices vérifient les valeurs de leurs horloges au moment de la réception, et les corrigent pour rester synchronisées avec l'horloge du Point d'Accès (éviter des dérives d'horloge qui pourraient causer la perte de la synchronisation).

Sécurité

- ⇨ Concernant la sécurité (premier souci du WLAN), la norme 802.11 a apporté une solution à ce problème en élaborant un processus appelé WEP (Wired Equivalent Privacy) ;
- ⇨ Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 128 bits. Cette clé secrète doit être déclarée au niveau de chaque adaptateur sans fil du réseau, ainsi que le point d'accès dans le cas d'un réseau en mode infrastructure. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame ;
- ⇨ Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre le nombre pseudo-aléatoire et la trame ;
- ⇨ L'Ecoute clandestine est bloquée par l'utilisation de l'algorithme WEP.

Economie d'énergie

- ⇨ 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 ;
- ⇨ Le standard 802.11 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 Polling Request, 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 sont stockées par le Point d'Accès et transmises à certains moments (chaque DTIM) où toutes les stations en mode d'économie d'énergie qui veulent recevoir ce genre de trames devraient rester éveillées.

Types de trame

- ⇨ 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 constituées 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

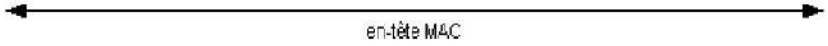
⇨ L'en-tête PCLP est toujours transmis à 1 Mbps et contient des informations logiques utilisées par la couche physique pour décoder la trame. Il s'agit de :

- **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

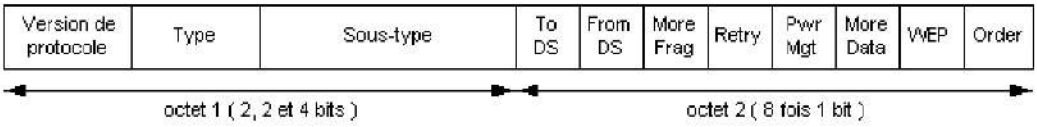
⇨ Le format général de la trame MAC est donné comme suit :

Contrôle de trame 2 octets	Durée / ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	Contrôle de séquence 2 octets	Adresse 4 6 octets	Corps de la trame 0-2312 octets	CRC 4 octets



Contrôle de trame

⇨ Le champ de contrôle de trame contient les informations suivantes :



- ⇨ **Version de protocole** : ce champ contient 2 bits qui peuvent être utilisés pour reconnaître les versions postérieures du standard 802.11. (0 pour la version courante) ;
- ⇨ **Type et sous-type** : Ils définissent le type et le sous-type des trames. Les détails sont donnés dans le tableau suivant :

Tableau.2. Détails du champs type et sous-type

Valeur du type (b3 b2)	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	1000	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 (sans 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 dans le but de 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 fonction du type de trame, ce champ à deux sens :

- 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

⇨ Selon le bit ToDS et FromDS (définit dans le champ de contrôle), une trame peut contenir jusqu'à 4 adresses. Ces dernières sont données 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 :

Tableau.3. 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

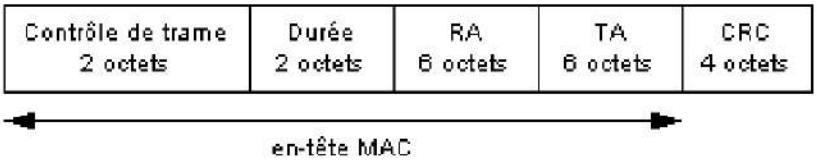
⇨ Le champ de contrôle de séquence est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame, et pour reconnaître les paquets dupliqués. Il consiste en deux sous-champs, le numéro de fragment et le numéro de séquence qui définissent le numéro de trame et le numéro du fragment dans la trame.

Cyclic Redundancy Check

⇨ Le CRC est sur 32 bits.

Format des trames RTS

⇨ Le format de cette trame est donné comme suit :



- RA est l'adresse du récepteur imsupportt 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.

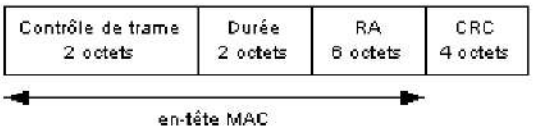
Format de la trame CTS

⇨ Le format de cette trame est donné comme suit :

- 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

⇨ Le format de cette trame est donné comme suit :



- 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.