ii. La modulation :

- **PSK (Phase Shift Keying):**

Cette technique est utilisée par la norme 802.11b. Chaque bit produit une rotation de phase. Une rotation de 180° permet de transmettre des débits peu élevés (technique appelée BPSK) tandis qu'une série de quatre rotations de 90° (technique appelée QPSK) permet des débits deux fois plus élevés grâce à l'optimisation de l'utilisation de la bande radio. [20]

- **OFDM (Orthogonal Frequency Division Multiplexing):**

OFDM est une méthode de codage appliquée aux normes 802.11a et g qui permet d'obtenir une meilleure bande passante. De ce fait, OFDM divise la bande de fréquence en bandes secondaires qui transmettent simultanément des fractions de données. Plus le nombre de canaux est élevé, plus les données transmises en parallèle sont nombreuses, plus la bande passante est élevée. Selon les conditions de bande passante, OFDM peut utiliser des méthodes de modulation de phase et d'amplitude.

OFDM est plus efficace que DSSS à savoir : en fonctionnant avec une même bande de fréquences (2,4000 - 2,4835 GHz), 802.11g a une bande passante de 54 Mbps avec OFDM, alors que 802.11b monte seulement jusqu'à 11 Mbps avec DSSS.

Le tableau suivant présente les différentes méthodes de codage pour le 802.11 a, b et g :

Paramètres	Standards		
	802.11a	802.11b	802.11g
Bande de fréquence (GHz)	5.15-5.35 5.725-5.825	2.4000-2.4835	2.4000-2.4835
Méthode d'encodage	OFDM	DSSS	OFDM (et DSSS pour une compatibilité avec 802.11b)
Bande passante maximale	54 Mbps	11 Mbps	54 Mbps

Tableau 2.3: Méthodes de codages pour le 802.11 a, b et g

II.4.2 La couche liaison de données :

La couche Liaison de données de la norme 802.11 est composée de deux sous-couches : la couche de contrôle de la liaison logique (LLC) et la couche de contrôle d'accès au support (MAC) [22]

En plus des fonctions habituellement rendues par la couche MAC, la couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme :

- la fragmentation et le réassemblage des trames
- le contrôle d'accès au support

- l'adressage et le formatage des trames.
- le contrôle d'erreur sur la trame, à partir d'un CRC (Cyclic Redundancy Chek)
- **la qualité de service**
- la gestion de l'énergie
- la gestion de la mobilité
- la sécurité

Le contrôle d'accès au support est une fonctionnalité qui nous intéresse ici particulièrement, se fait suivant deux méthodes (DCF et PCF) qui seront étudiées ultérieurement.

i. La trame MAC 802.11 : [22]

La norme a défini 3 types de trames MAC :

- Les trames de données : pour véhiculer les données à transmettre.
- Les trames de contrôle : utiles dans la procédure d'accès au canal (RTS, CTS, ACK).
- Les trames de gestion : contiennent des informations de gestion et ne sont pas remontées au niveau OSI supérieur (trames Beacon contenant les informations de synchronisation).

- **La trame de données MAC 802.11 :**

Comme l'illustre la figure ci dessous, une trame de données MAC 802.11 est constituée de trois parties :

- Entête MAC.
- Données MAC : Données reçues des couches supérieures et à encapsuler.
- CRC: champ de 32 bits contenant la somme de contrôle de la trame.

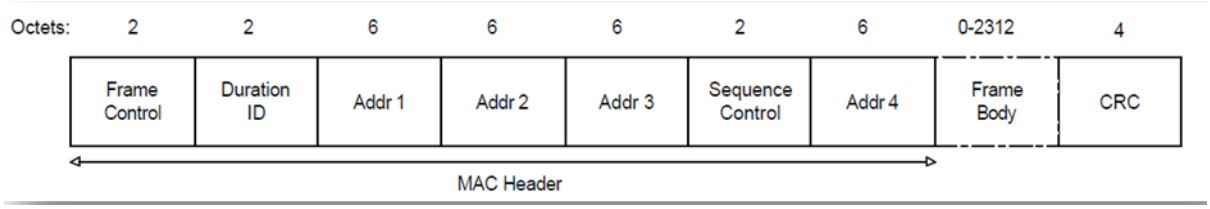

Figure 2.12 : Format de la trame MAC 802.11

L'entête MAC comporte les 7 champs suivants :

- ***Frame Control*** (2 octets) : renferme des informations de contrôle concernant la trame : version utilisée, type de la trame, mode de gestion de puissance, type de cryptage …

Ce champ contient en particulier les sous-champs FromDS qui indique nt si la trame est reçue de la part d'un DS (système de distribution), et ToDS qui indique nt si la trame est destinée à un DS.

- ***Duration ID*** (2 octets) : Indique la durée calculée pour le NAV (Network Allocation Vector).
- ***Adresse 1*** (6 octets) : Adresse de la station réceptrice. Si ToDS =1, alors c'est l'adresse de l'AP correspondant.
- ***Adresse 2*** (6 octets) : Adresse de l'émetteur. Si FromDS =1, c'est l'adresse du point d'accès
- ***Adresse 3*** (6 octets) : Adresse perdue, par exemple si FromDS = 1, Adresse 2 contient l'adresse du point d'accès et Adresse 3 celle de la station source d'origine
- ***Sequence Control*** (2 octets) : représente l'ordre des différents fragments d'une même trame. Ce champ permet aussi de reconnaître la duplication des paquets. Il est constitué de deux sous champs : *Fragment Number* et *Sequence Number* pour respectivement la trame et l'indice du fragment dans cette trame.
- ***Adresse 4*** (6 octets) : Utilisée dans des cas spéciaux tels que la transmission entre points d'accès, quand les ToDS et FromDS sont à 1.

- **Les trames de contrôle MAC 802.11**

La norme a prévu d'autres formats pour les trames de contrôle, en particulier les trames RTS,CTS et ACK.

- Les trames RTS et CTS sont utilisées pour la réservation virtuelle des ressources dans le cadre de la procédure d'accès au support physique.
- La trame ACK est utilisée pour acquitter les transmissions réussies. Elle est envoyée par une station réceptrice, ayant correctement reçu une trame de données, à la station source.

Les trames RTS, CTS et ACK sont constituées chacune par un et un entête MAC. L'entête MAC comporte quelques différences suivant qu'il s'agisse de trames RTS, CTS ou ACK :

- L'entête de la trame RTS comprend les champs suivant :
  - Frame Control : analogue au champ de la trame de données MAC.
  - Duration : Durée à réserver.
  - RA : Adresse de la station réceptrice.

- TA : Adresse de la station émettrice.

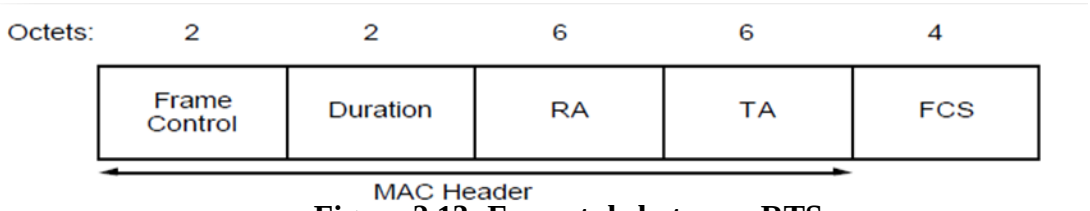

Figure 2.13: Format de la trame RTS

- L'entête de la trame CTS comprend les même champs que celui de RTS, hormis le champ TA. Le champ RA étant recopié à partir du champ TA de la trame RTS reçue.

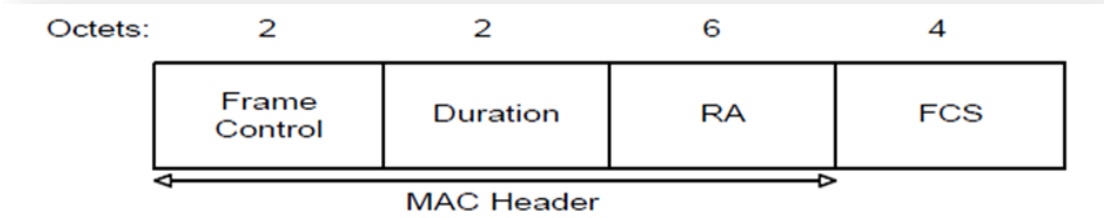

Figure 2.14: Format de la trame CTS

- L'entête de la trame ACK possède un format similaire à celui de CTS. L'adresse RA est recopiée à partir du champ Adresse 2 de la trame MAC à acquitter.

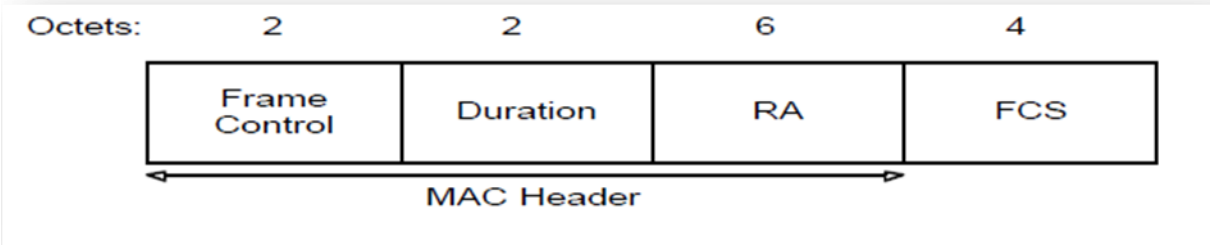

Figure 2.15 : Format de la trame ACK

iii. Protocoles d'accès au médium sans fil pour la norme IEEE 802.11 :

Comme mentionné plus haut, la principale fonctionnalité de la couche MAC 802.11 est de définir les mécanismes d'accès au support physique.

Le standard définit deux méthodes d'accès au support: DCF et PCF.

- **Le Distributed Coordination Function (DCF) : [13], [19], [22], [24]**

La technique DCF est basée sur le mécanisme CSMA/CA ou méthode d'accès multiple à détection de porteuse et évitement de collision. Cet algorithme distribué est exécuté localement sur chaque station afin de déterminer les périodes d'accès au médium.

- **Pourquoi CSMA/CA ?**

Les réseaux locaux sans fils adoptent la méthode d'accès CSMA/CA au lieu de la méthode CSMA/CD généralement utilisée dans les réseaux LANs classiques.

La méthode CSMA/CD consiste, pour une station désirant transmettre des données, à écouter le canal. Si le canal est libre alors la station peut transmettre. Sinon, elle attend que le canal redevienne libre. La station doit pouvoir détecter d'éventuelles collisions. Elle avortera dans ce cas la transmission et tentera de réémettre ultérieurement.

L'utilisation de cette méthode s'avère très coûteuse pour des réseaux sans fils. En effet, pour pouvoir implémenter la méthode CSMA/CD on doit disposer d'un circuit full duplex pour la détection de collision.

Ainsi, la méthode CSMA/CA a été retenue pour les WLANs puisque le canal varie au cours du temps. Cette méthode abandonne la détection de collisions, tout en renforçant les mécanismes pour les éviter. Dans un environnement radio-mobile, ce n'est pas possible d'appliquer le CSMA/CD.

- **Description générale du mécanisme DCF :**

Avant chaque émission, la station désirant émettre écoute le support. S'il est libre pendant une certaine durée DIFS (démontrer plus bas), la transmission est possible. Si le support est occupé, une procédure de *Backoff* est enclenchée.

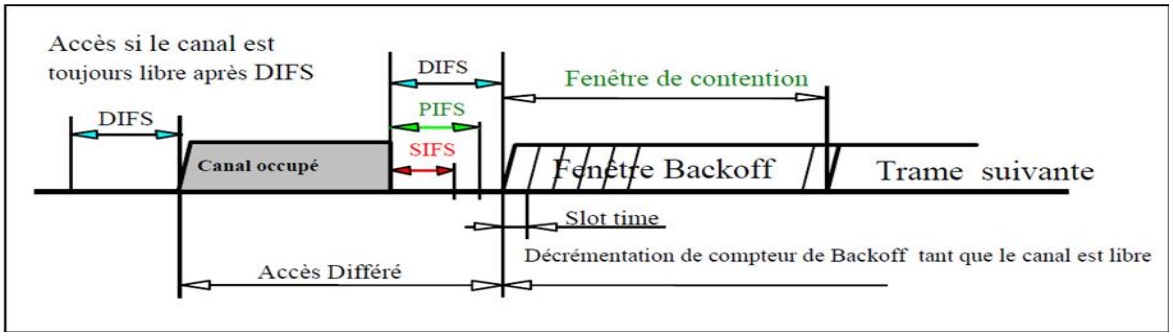

Figure 2.16: Accès au médium en mode DCF

Une station ayant correctement reçu un paquet, renvoie un accusé de réception (ACK) à la station émettrice. L'ACK indique à l'émetteur qu'aucune collision n'a eu lieu. Par contre, si l'émetteur ne reçoit pas d'acquittement au bout d'un certain temps, le fragment est retransmis jusqu'à réception d'un acquittement par le récepteur.

Enfin, si après un nombre défini de retransmissions, aucun accusé de réception n'est reçu, l'émission est abandonnée.

- **IFS (Inter-Frame Space) :**

Un espace inter-trames IFS est la durée pendant laquelle une station doit attendre avant de transmettre sur le canal. Pour définir les différentes sortes d'IFS, la norme a tout d'abord introduit la notion de Time Slot comme étant l'intervalle de temps qui

permet à une station de savoir si une autre station a accédé au canal au début du slot précédent. La valeur d'un Time Slot dépend de la couche physique utilisée. Pour la couche PMD à étalement de spectre à séquence directe, cette valeur est 20 µs.

A partir de la notion de Time Slot, la norme a ensuite introduit 4 types d'espaces inter trames, définis comme suit :

- **Short Inter-Frame Spacing (SIFS):**

Est le plus court des IFS. Il est utilisé pour séparer les différentes trames transmises au sein d'un même dialogue comme par exemple, entre des données et leurs acquittements ou entre différents fragments d'une même trame ou pour toute autre transmission relative à un même dialogue (question-réponse).

- **DCF Inter-Frame Spacing (DIFS) :**

Est le temps que doivent attendre les autres stations avant d'émettre un paquet en mode DCF. La valeur du DIFS est égale à celle d'un SIFS augmentée de deux times slot.

- **PCF Inter-Frame Spacing (PIFS) :**

Est le temps que doit attendre les autres stations avant d'émettre un paquet en mode PCF. La valeur est inférieure au DIFS, pour permettre de favoriser ce mode. Le mode PCF est expliqué dans la partie suivante.

- **Extended Inter-Frame Spacing (EIFS) :**

Est le plus long des IFS. Lorsqu'une station reçoit une trame erronée, elle doit attendre pendant un EIFS l'acquittement de cette trame.

- **L'algorithme de Backoff :**

La procédure de Backoff est un mécanisme simple, basé sur le calcul d'un temporisateur gérant les transmissions et les retransmissions. Il permet de réduire la probabilité de collision sur le canal en essayant de minimiser les chances d'avoir plusieurs stations qui accèdent au support en même temps.

- **Déroulement :**

Une station S désirant envoyer des données attend pendant une période DIFS. Si après cette durée le canal est libre, la station accède directement au canal. Dans le cas contraire, la station déclenche le mécanisme de Backoff qui se déroule en 3 étapes :

✓ La station calcule son temporisateur Backoff_Timer :

Backoff_Timer _Random ( ) x TS

Avec :

Random ( ) : nombre pseudo-aléatoire choisi ente 0 et CW-1 ; où CW est la taille de la fenêtre de contention qui sera détaillée plus loin.

TS : durée d'un time-slot définie comme étant l'intervalle de temps nécessaire pour une station pour savoir si une autre a accédé au canal au début du time-slot précédant.

- ✓ Quand le canal devient libre, et après un DIFS, la station commence à décrémenter son temporisateur time-slot par time-slot.
- ✓ Lorsque la valeur de Backoff_Timer est égale à 0, la station peut alors envoyer. Si par contre au cours de la phase de décrémentation, une autre station S' termine de décrémenter son temporisateur, la station S bloque son temporisateur. Elle pourra continuer de le décrémenter une fois la transmission de la station S' finie.

- **Fenêtre de contention :**

La taille de la fenêtre de contention CW a pour valeur initiale CWmin. Deux cas de figures peuvent se présenter :

- ✓ *Transmission réussie :* dans ce cas, CW est réinitialisée à CW_{min}.
- ✓ *Transmission échouée :* c'est-à-dire que la station émettrice ne reçoit pas d'acquittement au bout d'un certain temps. CW est alors incrémenté de la façon suivante:

$$CW_{new} \_ 2*CW_{old} +1$$

La station suppose dans ce cas qu'il y a eu collision lors de la transmission, et incrémente la taille de sa fenêtre de contention afin de diminuer les chances de collisions lors des prochaines retransmissions. Une valeur limite CWmax est cependant définie.

Si pour CW = CWmax la transmission échoue toujours, la valeur n'est plus incrémentée et est maintenue à CWmax.

La figure 2.18 montre un diagramme de variations de la taille de la fenêtre de contention en fonction du nombre de tentatives de transmissions.

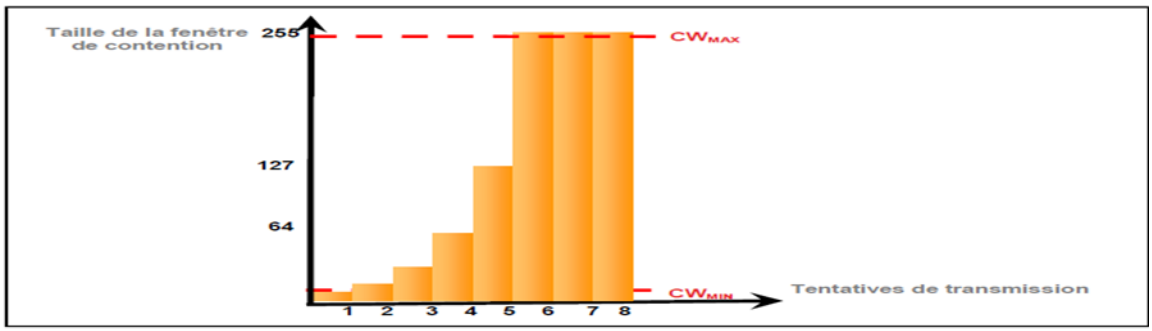

Figure 2.17: Exemple typique de la variation de la taille de la fenêtre de contention

iv. Diagramme de fonctionnement

La figure 2.19 résume le fonctionnement de la procédure CSMA/CA et de l'algorithme de Backoff.

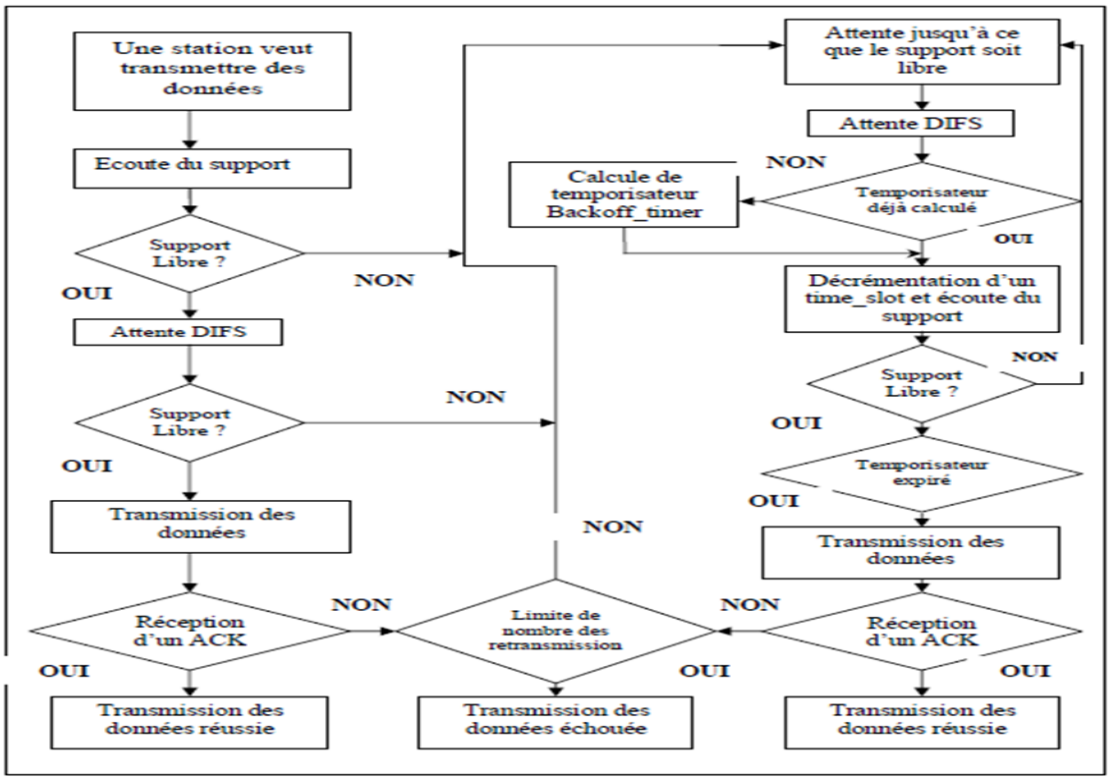

Figure 2.18: Procédure CSMA/CA

v. Le mécanisme de Virtual carrier Sense VCS :

Dans le but de résoudre le problème des stations cachées, le standard 802.11 définit sur sa couche MAC un mécanisme optionnel de type RTS/CTS appelé mécanisme VCS. Lorsque cette fonction est utilisée, une station émettrice transmet un RTS et attend en réponse un CTS. Toutes les stations du réseau recevant soit RTS soit le CTS, déclencheront pour une durée fixée leur indicateur NAV pour retarder toutes transmissions prévues. La station émettrice peut alors transmettre et recevoir son accusé de réception sans aucun risque de collision.

vi. Description générale du mécanisme PCF:

Le **PC** normalement installé sur l'AP, contrôle l'accès au médium par la méthode du Polling. Il faut noter que **PCF** est optionnel, et peut donc être implémenté avec **DCF**.

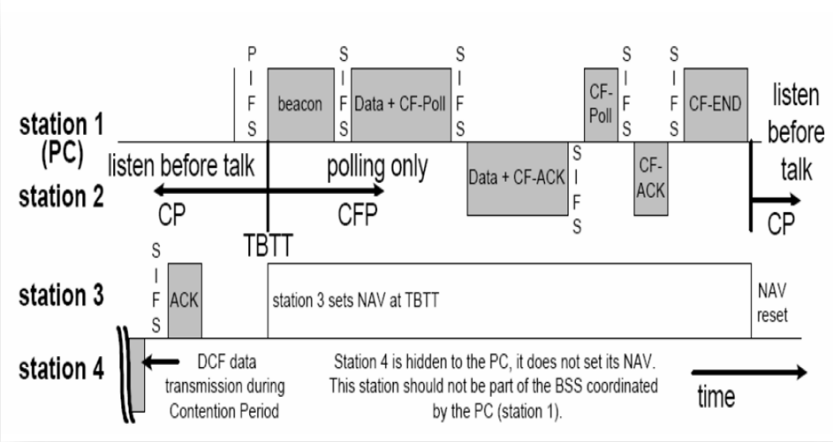

Figure2.19 : principe du fonctionnement du PCF

Le **PC** après un temps **PIFS** pendant lequel le canal est libre envoie la balise " **Beacon** " qui marque le début de la super trame, divisée en deux parties: la CFP et la CP. Initialement la durée maximale de la CFP CFPMaxDuration, ainsi que sa fréquence sont données; mais cette dernière n'est pas respectée la plupart du temps car le beacon peut être retardé, à cause d'une longue transmission d'une trame à la fin de la CP. Ce problème ne permet pas d'avoir une séquence rigoureusement périodique de la balise. Comme PCF a été développé au dessus de DCF toutes les stations doivent activer leur NAV au début de la CFP à la valeur CFPMaxDuration pour bloquer toute transmission parasite (contention) pendant la durée CFP, car aucune station n'a le droit d'émettre que si on le lui demande pendant la CFP.

Pendant la durée du CFP le PC attend une durée SIFS après le beacon avant d'envoyer une trame de données ou le CF-Poll ou faire du piggybacking (une trame de données qui contient aussi un message de polling). Le PC va séquentiellement faire du polling, pendant la durée CFP, pour toutes les stations déjà enregistrées dans sa liste. La station concernée va répondre au PC ou à une autre station dans le réseau par des trames de données ou un ACK séparés par SIFS. Si une station ne répond pas, le PC passe à la suivante après PIFS. Si le PC ou les stations n'ont plus de trames a transmettre, la CFP se termine par l'envoi de la trame CF-end par le PC. Toutes les stations vont alors remettre a zéro leur NAV, et la CP va débuter, et on repasse alors au mode DCF. Il faut noter qu'aucune station n'a le droit d'émettre que si on le lui demande pendant la CFP.

Si le PCF est utilisé pour les applications à contraintes temporelles, le PC doit établir une liste de polling. Chaque station doit être votée au moins une fois par CFP. Les stations peuvent demander une place dans la liste de polling avec des trames de gestion d'associations. Le PC peut avoir un modèle de priorité pour les différentes stations.

III. Conclusion :

Afin de gérer la priorité d'accès au support et garantir la qualité de service pour les trafics multimédia, le groupe IEEE 802.11 a développé de nouveaux mécanismes dans le but de garantir une certaine qualité de service.

Ce standard repose sur deux mécanismes d'accès : EDCF qui fonctionne durant la période CP et HCF qui fonctionne durant les deux périodes.

Le chapitre suivant a pour objectif d étudier ces deux mécanismes ainsi que tous les autres aspects liés a la Qualité de service.