**I. Réseaux Wi-Fi :**

Le **Wi-Fi**[] est une technologie permettant de relier sans fil plusieurs [appareils informatiques](http://fr.wikipedia.org/wiki/Appareil_informatique%22%20%5Co%20%22Appareil%20informatique) ([ordinateur](http://fr.wikipedia.org/wiki/Ordinateur%22%20%5Co%20%22Ordinateur), [routeur](http://fr.wikipedia.org/wiki/Routeur%22%20%5Co%20%22Routeur), Internet, etc.) au sein d'un [réseau informatique](http://fr.wikipedia.org/wiki/R%C3%83%C2%A9seau_informatique%22%20%5Co%20%22R%C3%A9seau%20informatique). Cette technologie est régie par le groupe de normes [IEEE 802.11](http://fr.wikipedia.org/wiki/IEEE_802.11%22%20%5Co%20%22IEEE%20802.11), qui a donner lieu à plusieurs sous-normes suivant les besoins de débit et de porté:

* IEEE 802.11 (1990, version initiale): Elle propose un débit théorique de 1à 2 Mbit/s avec une portée pouvant aller jusqu’à 50m. La plage de fréquences utilisée est la bande des 2,4 GHz.
* IEEE 802.11b (1998, wi-fi): est la plus utilisée actuellement. Elle propose un débit théorique de 11 Mbit/s (6 Mbit/s réels) avec une portée pouvant aller jusqu’à 100m. La plage de fréquences utilisée est la bande des 2,4 GHz.
* La norme 802.11a (baptisée *Wi-Fi 5*) permet d’obtenir un haut débit (dans un rayon de 10 mètres : 54 Mbit/s théoriques, 27 Mbit/s réels). La norme 802.11a spécifie 52 canaux de sous-porteuses radio dans la bande de fréquences des 5 GHz
* La norme 802.11g est la plus répandue dans le commerce actuellement. Elle offre un haut débit (54 Mbit/s théoriques, 25 Mbit/s réels) sur la bande de fréquences des 2,4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b.
* La norme *802.11n* est disponible depuis le 11 septembre [2009](http://fr.wikipedia.org/wiki/2009%22%20%5Co%20%222009). Le débit théorique atteint les 300 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 100 mètres). En [avril](http://fr.wikipedia.org/wiki/Avril_2006%22%20%5Co%20%22Avril%202006) [2006](http://fr.wikipedia.org/wiki/2006%22%20%5Co%20%222006), [des périphériques à la norme 802.11n commencent à apparaître](http://www-fr.linksys.com/servlet/Satellite?c=L_News_C2&childpagename=FR%2FLayout&cid=1145389519039&pagename=Linksys%2FCommon%2FVisitorWrapper). Le *802.11n* a été conçu pour pouvoir utiliser les fréquences 2,4 GHz ou 5 GHz. Les premiers adaptateurs 802.11n actuellement disponibles sont généralement simple-bande à 2,4 GHz, mais des adaptateurs double-bande (2,4 GHz ou 5 GHz, au choix) ou même double-radio (2,4 GHz et 5 GHz simultanément) sont également disponibles. Compatible avec 802.11b et g.

**II. Architecture Wi-Fi :** La norme IEEE 802.11 offre 2 modes de fonctionnement :

**Mode Infrastructure :** ou les terminaux mobiles communiquent à l’aide d’un point d’accès (station de base) et forment en conséquence un BSS (Basic Set Service : cellule de base). Lorsque le réseau est composé de plusieurs BSS, chacun d’eux est relié à un système de distribution (DS : Distribution System), par l’intermédiaire de leur point d’accès (AP) respectif. DS correspond souvent à un réseau Ethernet filaire (T-Ring, FDDI ou sans fil : réseau mesh). Cet ensemble de BSS forme un ESS (Extended Set Service).

**Mode Ad Hoc (sans infrastructure) :** un réseau Ad Hoc est un ensemble de terminaux mobiles indépendant de toute infrastructure (point d’accès ou une connexion au DS) , communicant entre eux par onde radio, formant un IBSS (Independent BSS), ou chacun de ces terminaux offre un service de relais (routeur) consistant à accepter un message qui ne lui est pas destiné afin de le réémettre vers un autre terminal qui est hors de portée de l’émetteur initial. Le service de relais est le point fondamental de l’Ad Hoc.





Carte réseau Wi-Fi + borne Wi-Fi (AP)

**III. Avantages et Inconvénients:**

Les **avantages** principaux par rapport au filaire sont les suivants :

* + - **flexibilité** de la topologie
		- **mobilité** génératrice de gains de productivité, avec un accès en temps réel aux informations, quel que soit le lieu où se situe l'utilisateur, pour une prise de décision plus rapide et plus efficace .
		- **installation** plus **simple** et plus **économique** dans les endroits difficiles à câbler, bâtiments anciens et structures en béton armé ou en cas de catastrophes naturelles, désert, montagnes, foret pour militaires.
		- **adapté** aux environnements dynamiques nécessitant des transformations fréquentes grâce au coût minime du câblage et de l'installation
		- **libération** de l'utilisateur de sa dépendance à l'égard des accès câblés au backbone en lui offrant un accès permanent et **omniprésent** :

Exemple : pour un accès immédiat entre le lit d'hôpital et les informations concernant le patient pour les médecins et le personnel hospitalier

* + - **accès** **étendu** aux bases de données pour les chefs de service nomades, …
		- **recours** **minime** au personnel informatique pour les installation temporaires telles que stands de foire, d'exposition ou salles des conférence
		- **accès** **omniprésent** au réseau pour les administrateurs, pour le support et le dépannage

Les **inconvénients** qu’il est possible de noter sont :

* **limitations** de propagation : varie en fonction des interactions avec les murs, de la puissance du signal
* **débits** sont encore inférieurs à ceux des réseaux filaires
* risques **d'interférences** possibles (problème si plusieurs réseaux sans fil proche)
* **Batteries** : les réseaux sans fil doivent incorporer des mécanismes d’économie d’énergie (particulièrement pour une utilisation avec des ordinateurs portables)
* **Sécurité** : support (ondes radio) ouvert, de nombreuses failles existent encore
* **Santé** : puissance du signale (10 mW en Europe) peut causer des maux de tête ;En Allemagne et en France arrêt de l’utilisation de réseau WIFI dans des bibliothèques (plaintes du personnels suite à des troubles (malaises, maux de têtes...)

**IV. Applications :**

Exemples d’utilisation :

* actuellement dans des applications verticales comme usines, entrepôts et magasins de détail.
* de plus en plus dans les activités de santé, les institutions éducatives et les bureaux des grandes entreprises, les salles de conférence, les zones publiques et les agences locales.

**V. Wi-Fi en couches :**

La norme 802.11 s’attache à définir les couches basses du [modèle OSI](http://fr.wikipedia.org/wiki/Mod%C3%83%C2%A8le_OSI%22%20%5Co%20%22Mod%C3%A8le%20OSI) pour une liaison sans fil utilisant des [ondes électromagnétiques](http://fr.wikipedia.org/wiki/Rayonnement_%C3%83%C2%A9lectromagn%C3%83%C2%A9tique%22%20%5Co%20%22Rayonnement%20%C3%A9lectromagn%C3%A9tique), c’est-à-dire :

* la [couche physique](http://fr.wikipedia.org/wiki/Couche_physique%22%20%5Co%20%22Couche%20physique) (notée parfois couche PHY) : définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données.
* la [couche liaison](http://fr.wikipedia.org/wiki/Couche_de_liaison%22%20%5Co%20%22Couche%20de%20liaison) de données (carte réseau), définit l’interface entre le bus de la machine et la couche physique, constituée de deux sous-couches :
	+ le contrôle de la liaison logique ([Logical Link Control](http://fr.wikipedia.org/wiki/Contr%C3%83%C2%B4le_de_la_liaison_logique%22%20%5Co%20%22Contr%C3%B4le%20de%20la%20liaison%20logique), ou LLC) ;
	+ le contrôle d’accès au support ([Media Access Control](http://fr.wikipedia.org/wiki/Mod%C3%83%C2%A8le_OSI%22%20%5Co%20%22Contr%C3%B4le%20d%27acc%C3%A8s%20au%20support), ou MAC).



**V.1 Fonctionnalités de la Couche MAC 802.11 :** ressemble à la couche MAC de l’Ethernet :

* Adressage et formatage des trames
* Détection d’erreur par CRC
* Fragmentation et réassemblage
* *Contrôle d’accès au support CSMA/CA*
* *Gestion de la mobilité (IEEE 802.11f)*
* *Gestion de l’énergie, gestion de QoS (IEEE 802.11e)*
* *Sécurité (IEEE 802.11i)*

**V.2 Trame MAC 802.11 :**

Il y a trois principaux types de trames :

* les trames de données, utilisées pour la transmission des données
* les trames de contrôle, par exemple RTS, CTS et ACK
* les trames de gestion : association, synchronisation, authentification.

L’entête varie suivant le type définit dans les 2 premiers octets (champ contrôle de trame).





**V.3 Techniques d’accès sans fil :**

La couche MAC définit 2 méthodes d'accès différentes

* la DCF (Distributed Coordination Function), basée sur le principe d’égalité des chances d’accès au support de transmission pour tous les utilisateurs (méthode probabiliste, données asynchrones)
* la PCF (Point coordination Function), basé sur une méthode de polling gérée par le point d’accès (méthode déterministe, voix et vidéo)

La DCF est basée sur la politique CSMA/CA (Carrier Multiple Acces with Collision Avoidance).

Contrairement à CSMA/CD (Carrier Sense Multiple Access with Collision Detection) dans laquelle chaque utilisateur écoute le média pendant l'émission pour **détecter** une éventuelle collision, la méthode CSMA/CA met en avant le principe d’évitement des collision dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée (impossible de détecter les collisions). Au lieu d’un contrôle des collisions à posteriori, on adopte une politique de contrôle à priori.

**CSMA/CA** est basé sur :

* L’écoute du support : Mécanisme de réservation du support (Ready To Send /Clear To Send : **RTS** et **RTC**)
* Les temporisateurs d’espacement inter trames IFS (Inter Frame Spacing), correspondent à un intervalle de temps entre l’émission de deux trames. Il en existe trois types selon 802.11 :

 **SIFS** (Short IFS), utilisé pour séparer les transmissions d’un même dialogue (RTS, RTC, ACK et fragments)

 **PIFS** (PCF IFS), utilisé par le point d’accès pour effectuer le polling dans la

 méthode PCF.

 **DIFS** (DCF IFS), utilisé en DCF (c’est à dire en CSMA/CA) lorsque une station

 veut initier une communication

 **EIFS** (Extended IFS) : le plus long, utilisé pour l’attente de l’ACK.

* Le temporisation d’émission, appelé NAV (Network Allocation Vector) permet d’éviter les collisions en retardant les émissions de toutes les stations qui détectent que le support est occupé.
* L’algorithme de **Backoff** : calculer une durée aléatoire, dans le but de gérer les collisions éventuelles et garantir la même probabilité d’accès pour chaque station au support.
* L’utilisation d’acquittement positif (ACK)



**Fig : Nœud caché et Nœud exposé**



 **Suite de l’exemple :** A veut transmettre vers B, D est à portée de A, C est à portée de B mais pas de A

 A envoie RTS *(Request To Send)* à B

 B envoie CTS *(****C****lear To Send)* à A pour signifier son accord

 A envoie sa trame et arme un décompteur EIFS.

 B acquitte la trame en répondant ACK à A, Si le compteur EIFS expire avant l’arrivée de ACK, le scénario est réexecuté.



**Emission d’une trame fragmentée avec réservation de support**



 **Point de vue de C et D :**

-D reçoit RTS envoyé par A et en déduit la longueur de l’échange demandé par A (Trame + ACK), Il arme un compteur : NAV *(****N****etwork* ***A****llocation* ***V****ector)* correspondant au temps d’occupation d’un canal virtuel

-C ne reçoit pas RTS mais CTS et procède alors comme D.

**Le point négatif de cette politique d’accès est qu’elle est probabiliste : il n’est pas possible de garantir un délai minimal avant l’accès au support, ce qui est problématique pour certaines applications (voix, vidéo, …)**

**IV. FONCTIONNEMENT : COMMENT UNE STATION REJOINT-ELLE UN BSS ?**

**1. Synchronisation**

Quand une station veut accéder à un BSS ou à un IBSS, soit après démarrage ou après un

passage en mode de veille, la station a besoin d’informations de synchronisation de la part du point d’accès (ou des autres stations dans le cas d’un réseau ad-hoc). Les stations doivent obligatoirement rester synchronisées afin de garder la synchronisation pour certaines fonctions comme l’économie d’énergie.

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

**Ecoute active** : dans ce cas, la station envoie au point d’accès (choisie suivant la puissance de signal, taux d’erreur et la charge) une trame de demande de synchronisation (Probe Request Frame) et attend une trame "balise" (Beacon Frame) de la part du point d’accès contenant les info de synchronisation ; son horloge.

**Ecoute passive** : dans ce cas, la station attend simplement de recevoir une trame "balise" (Beacon Frame), celle-ci étant envoyée périodiquement par le point d’accès toutes les 100ms par exemple. Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrige pour rester synchronisées avec l’horloge du point d’accès.

La *première* technique est utilisée lorsque la station veut se connecter à un BSS pour la

première fois (ou pour se reconnecter). La *deuxième* est utilisée pour garder la synchronisation avec le point d’accès une fois que la station a déjà été associée au BSS.

**2. L’authentification : vérification de l’identité de la station**

Une fois qu’une station a trouvé un point d’accès et une cellule (BSS) associée, le processus d’authentification s’enclenche.



**3. L’association**

Une fois la station authentifiée, le processus d’association s’enclenche. Celui-ci consiste en un échange d’informations concernant les différentes stations, les capacités de la cellule et enfin l’enregistrement de la position actuelle de la station par le point d’accès.

C’est seulement après la fin du processus d’association que la station peut transmettre et

recevoir des trames de données.

Etant associée à une cellule, la station reste synchronisée avec le point d’accès par écoute *passive*. Le point d’accès transmet régulièrement les trames "balises", qui contiennent la valeur de son horloge interne et qui permettent aux stations de synchroniser leur horloge.



**3. Réassociation** : similaire à l’association, elle se déclenche à la suite d’un déplacement.

## 4. Le roaming (Mobilité)

Le fait qu’un terminal peut se déplacer et donc passer d’une cellule à une autre a conduit à la mise en place d’une technique de handover.

Au contraire des réseaux de mobiles pour lesquels le handover se fait au milieu d’une conversation, dans le monde 802.11, la handover se fait entre deux transmissions de données. D’autre part le roaming n’est possible que si ces points d’accès sont configurés avec le même "Network ID" (le nom du réseau). Ce service n’est pas défini dans les normes 802.11 et 802.11b. toutefois, il est défini dans la norme 802.11f : IAPP (Inter-Access Point Protocol) ; utilise le serveur RADIUS pour permettre des handover sécurisés. RADIUS est un serveur centralisé ayant une vue globale du réseau.





