- **Chapitre 02:** Réseaux locaux sans fil
- Les réseaux sans fil
- 802.11
- Architecture 802.11
- liaison de données 802.11

Chapitre 02:
Réseaux locaux sans fil

I. Les Réseaux sans Fil

Définition
Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer
entre eux grâce à des signaux radioélectriques.

Avantages :

- *Mobilité :* les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.
- *Facilité et souplesse :* un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- *Coût :* si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.
- *Évolutivité :* les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins

Inconvénients :

- *Qualité et continuité du signal :* ces notions ne sont pas garanties du fait des problèmes
  pouvant venir des interférences, du matériel et de l'environnement.
- *Sécurité :* la sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette
  technologie est novatrice.

Catégories des réseaux sans fil :

Les réseaux sans fil sont répartis en plusieurs catégories, selon le périmètre géographique offrant la connectivité, appelé zone de couverture.

Les réseaux individuels sans fil (*Wireless Personal Area Network,* WPAN)

La portée d'unréseau WPAN ne dépasse pas quelque dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques comme une imprimante, un téléphone portable, un assistant personnel (PDA), relier une télécommande à un poste télévisé, etc. La principale technologie utilisée avec cette catégorie de réseaux sans fil est le standard IEEE 802.15.1 (Bluetooth) lancé par Ericsson en 1994 avec un débit de 1 Mbp/s et ayant une couverture qui ne dépasse pas une trentaine de mètres. Il est connu pour sa grande consommation d'énergie.

Le standard IEEE 802.15.4 (ZigBee) à faible consommation d'énergie et les liaisons infrarouges représentent d'autres exemples de réseaux sans fil pouvant transmettre des données sur quelques dizaines de mètres.

Les réseaux locaux sans fil (*Wireless Local Area Network*, WLAN)

La portée d'un réseau WLAN est de quelques centaines de mètres (300 mètres) et il est utilisé souvent dans les entreprises pour former un réseau local sans fil afin de connecter des ordinateurs et des imprimantes. Un exemple très connu de ce type de réseau est le fameux Wi-Fi (Wireless Fidelity) dont le débit peut atteindre 54 Mbp/s et la portée plusieurs centaines de mètres. Un autre exemple de WLAN est HiperLAN2 qui est une norme européenne proposant un débit équivalent au Wi-Fi (avec 54 Mb/s et une portée de 300 mètres).

Les réseaux métropolitains sans fil (Wireless Metropolitan Area Network, WMAN)

Ce type de réseau vise une couverture plus large que ses précédents tout en offrant un débit de 1 à 10 Mbp/s et une portée de 4 à 10 Km. Avec ce type de réseau, l'onde radio permet à plusieurs entreprises d'être interconnectées ou de relier différents bâtiment dans un même quartier, etc. Un exemple de ce réseau est la norme IEEE 802.16, WiMAX)

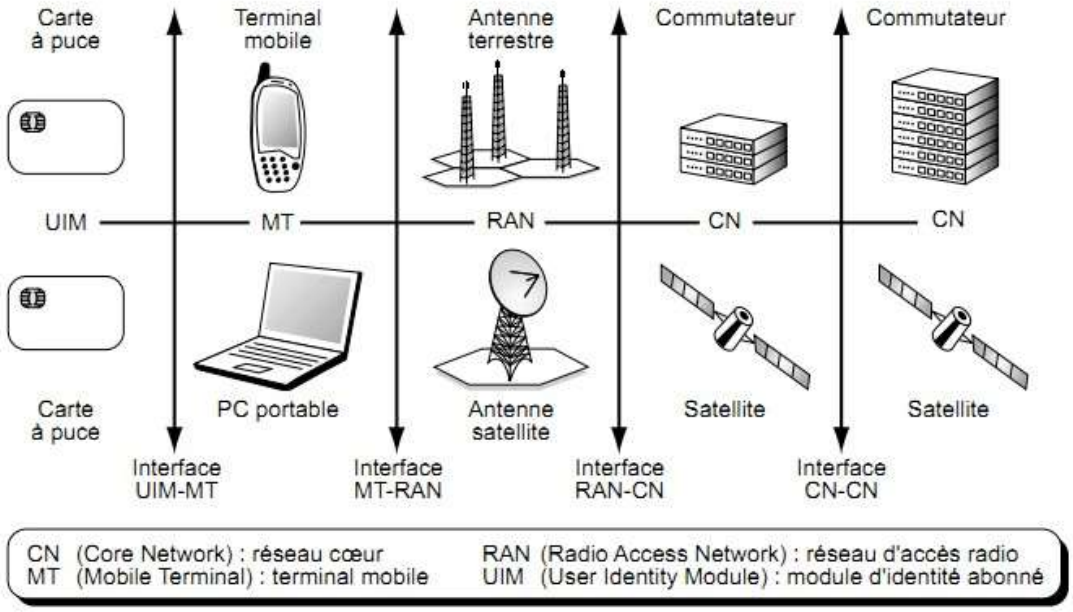
Les réseaux mobiles

Les réseaux cellulaires mobiles couvrent des zones étendues. Ce type de réseau est utilisé par les compagnies de la téléphonie cellulaire. Plusieurs systèmes très connus aujourd'hui utilisent ce type de réseaux, citons : le Global System for Mobile Communication (GSM) , le General Packet Radio Service (GPRS), l'Universal Mobile Telecommunication System (UMTS) , le Long Term Evolution (LTE) et le LTE Advanced (LTE-A)

Schémas d'architecture des réseaux de mobiles:

Les différents systèmes de réseaux mobiles peuvent être définis a partir des équipements qui les composent et des interfaces mises en place entre ces équipements (interface air, partie fixe, boucle locale, etc.)

L'ensemble équipements-interfaces caractérise un système mobile et s'illustre dans un schéma d'architecture.



L'interface UIM-MT ou SIM-MT

- MT peut correspondre avec différents types de réseaux
- Rôle de l'interface : sécuriser la communication qui s'établie a partir du mobile
- Une carte à puce est insérée dans le MT

L'interface MT-RAN

- Relie le MT à l'antenne ou à un autre terminal
- Concerne la traversée de la partie air du réseau
- Définit comment un terminal accède à l'antenne et réciproquement
- Représente souvent le point le plus sensible du réseau

L'interface RAN-CN

- Concerne la transmission de l'antenne au premier commutateur du CN
- Regroupe plusieurs antennes, de sorte à pouvoir gérer ces dernières collectivement
- Assure la gestion des appels
- Gere la mobilité

L'interface CN-CN

- Interface entre deux nœuds
- Partie fixe d'un réseau mobile
- Définit la technologie réseau utilisée pour acheminer les informations

La boucle locale radio

Dans le cadre du réseau fixe, l'opérateur est tenu de proposer un moyen de communication à chaque abonné. Souvent, le support physique de transport est installé depuis un

commutateur du réseau vers une résidence ou un lieu de travail. Ce maillage s'appelle la boucle locale.

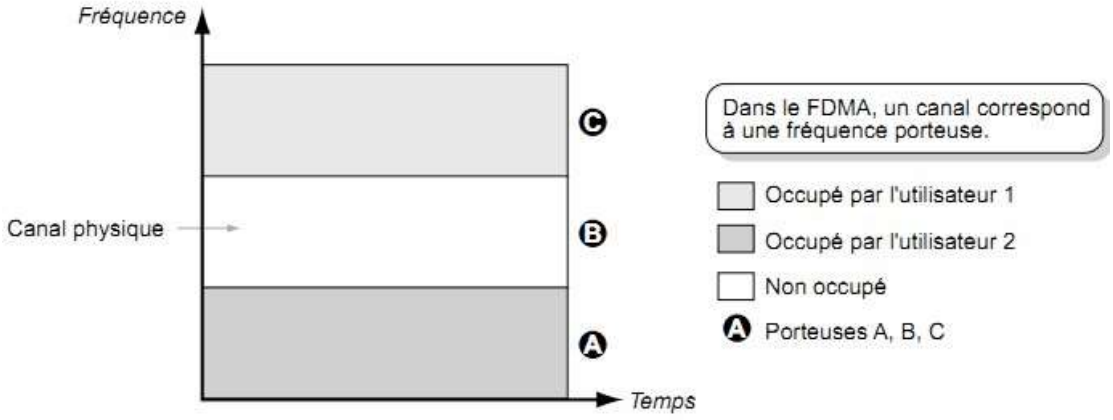
L'émergence des supports de transport sans fil a donné naissance au concept de boucle locale radio, qui présente le double avantage de réduire sensiblement les coûts d'installation tout en ouvrant le marché de la communication à la concurrence. Dans ce système, une antenne est fixée à proximité des zones d'habitation pour diffuser l'information vers des antennes plus petites, installées au sommet des immeubles, tout comme des antennes de télévision. Certains pays présentent des infrastructures de télécommunications insuffisantes pour offrir de nouveaux services à haut débit sur une boucle locale fixe. Dans de telles situations, la boucle radio offre, à coût réduit, le moyen d'assurer l'accès aux nouveaux services réseau (vidéo, multimédia), qui requièrent des débits élevés.

Les méthodes d'accès aux réseaux :

Dans les réseaux de mobiles, la transmission radio passe par l'interface radio, que se partagent les utilisateurs d'une même cellule. Plusieurs méthodes permettent aux mobiles d'accéder à la ressource radio. Ces méthodes ont toutes pour principe de diviser la bande de fréquences, généralement très limitée, en plusieurs canaux physiques assurant la communication tout en respectant les contraintes permettant d'éviter les interférences. Les trois principales méthodes d'accès utilisées par les réseaux de mobiles sont FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access) et CDMA (Code Division Multiple Access).

FDMA :

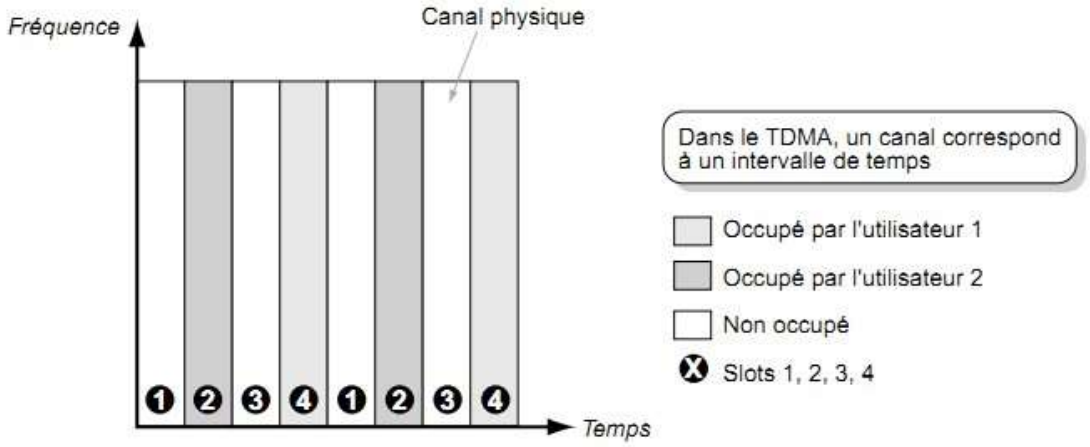
L'accès multiple par répartition en fréquence (*Frequency Division Multiple Access* ou *FDMA*) est un mode de multiplexage destiné à la téléphonie mobile. Il s'agit d'un découpage en bande de fréquences de manière à attribuer une partie du spectre à chaque utilisateur. De cette manière, chaque utilisateur se voit attribuer une bande de fréquences distincte.



TDMA :

Le Time division multiple access (TDMA) est un mode de multiplexage permettant de transmettre plusieurs signaux sur un seul canal. Il s'agit du multiplexage temporel, dont le principe est de découper le temps disponible entre les différentes connexions (utilisateurs). Par ce moyen, une fréquence peut être utilisée par plusieurs abonnés simultanément. Cette technologie est par exemple utilisée dans la norme GSM, où chaque porteuse (*canal*

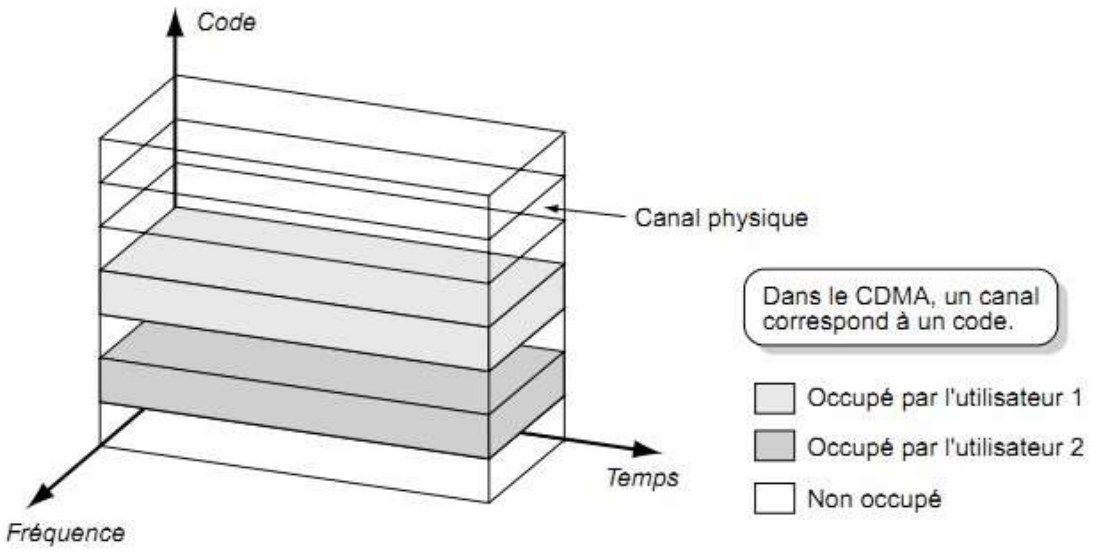
physique) supporte huit intervalles de temps (*time slot*) attribués à huit communications simultanées.



CDMA :

Troisième méthode, le CDMA, ou accès multiple par division de codes, autorise l'allocation de la totalité de la bande de fréquences, de manière simultanée, à tous les utilisateurs d'une même cellule. Pour ce faire, un code binaire spécifique est octroyé à chaque utilisateur. L'utilisateur se sert de son code pour transmettre l'information qu'il désire communiquer en format binaire d'une manière orthogonale, c'est-à-dire sans interférence entre les signaux, aux autres communications.

En CDMA, chaque utilisateur dispose de toute la largeur de la bande passante. L'attribution de différents codes permet une réutilisation de la même fréquence dans les cellules adjacentes.
Cela offre un avantage considérable à cette méthode par rapport aux deux autres, le TDMA et le FDMA. Toutefois, les codes étant seulement quasi orthogonaux à la réception, un problème d'autointerférence entre en jeu, qui s'intensifie au fur et à mesure que le nombre de communications simultanées augmente. Excédant le nombre maximal de codes attribués, la surcharge de la cellule affecte en outre tous les autres utilisateurs par l'interférence provoquée sur leurs canaux, alors que, en comparaison, un seul utilisateur est brouillé en TDMA.



4. Les Types des réseaux sans fil

Réseaux sans fil à stations de base

Les réseaux utilisés couramment de nos jours sont des réseaux sans fil à stations de base : GSM, GPRS, UMTS, Wi-Fi.

Caractéristiques :

– cout de déploiement important

– nécessité d'une infrastructure fixe, interconnectée de manière filaire.

– cout des licences, notamment pour l'UMTS

Réseaux sans fil Peer To Peer (ad hoc)

Le pair à pair ou pair-à-pair (*peer-to-peer*, souvent abrégé « P2P ») est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur. Le pair à pair peut être centralisé (les connexions passant par un serveur intermédiaire) ou décentralisé (les connexions se faisant directement). Il peut servir au partage de fichiers en pair à pair, au calcul scientifique ou à la communication.

II. LE STANDARD IEEE 802.11 : WI-FI

C'est un des standards qui permet de déployer un réseau sans fil en faisant communiquer plusieurs appareils (ordinateur, PDA, cellulaire, etc.) ensemble, à travers l'onde radioélectrique et à une liaison haut débit sur un rayon de couverture pratiquement égal à quelques dizaines de mètres.

La norme IEEE 802.11 offrait un débit entre 1 et 2 Mbp/s.

Pour des raisons d'amélioration de la performance (portée, débit, etc.), cette norme a subi plusieurs évolutions à travers l'apparition de différentes versions.

1. Les différentes normes WiFi

La norme *IEEE 802.11* est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Nom du standard	Nom	Description
802.11a	Wi-Fi	Cette norme offre un débit théorique de 54 Mbps (30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wi-Fi	802.11b est la norme Wi-Fi la plus répandue actuellement. Son débit théorique est de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres et spécifie 3 canaux radio dans la bande de fréquence des 2.4 GHz.
802.11d	Internationalisation	La norme 802.11d introduit les règlementations de chaque pays
802.11e	Amélioration de la qualité de service	La norme 802.11e améliore la qualité de service en fonction de la bande passante et du délai de transmission ce qui permet une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f permet une meilleure interopérabilité des produits, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Elle accélère les transitions entre points d'accès en redéfinissant le protocole de négociation de clés de sécurité
802.11g	intègre la modulation OFDM	La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence 2.4 GHz.
802.11h	service de gestion du spectre	La norme 802.11h est conforme avec la réglementation européenne en ce qui concerne la bande de fréquence.
802.11i	Authentification et chiffrement	La norme 802.11i s'appuie sur l'Advanced Encryption Standard (AES) pour améliorer la sécurité.

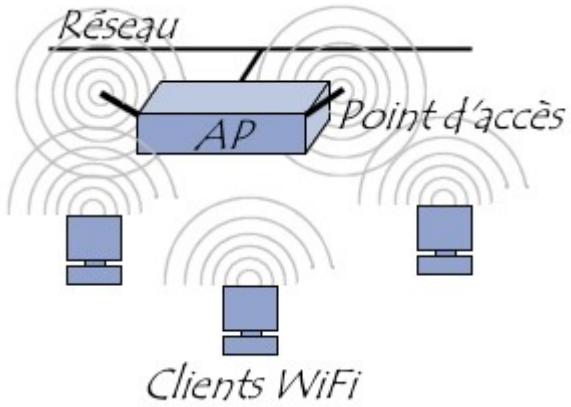
2. Les modes de fonctionnement du Wifi (802.11 ou Wi-Fi)

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wifi :

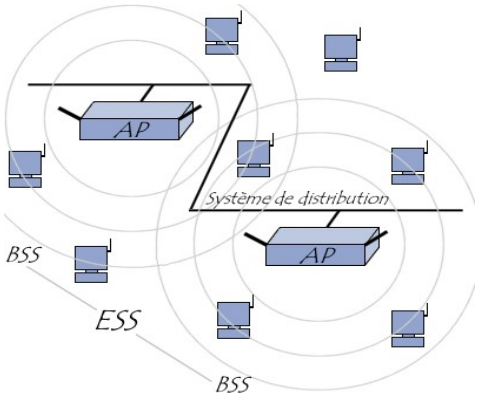
- Les **adaptateurs sans fils** ou **cartes d'accès** (en anglais *wireless adapters* ou *network interface controller*, noté *NIC*) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs WiFi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte CompactFlash, ...). On appelle **station** tout équipement possédant une telle carte.
- Les **points d'accès** (notés **AP** pour *Access point*, parfois appelés *bornes sans fils*) permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes wifi.
  Le standard 802.11 définit deux modes opératoires :
- Le mode infrastructure dans lequel les clients sans fils sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.

Le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

2.1. Le mode infrastructure :



En **mode infrastructure** chaque ordinateur station (notée **STA**) se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé *ensemble de services de base* (en anglais *basic service set*, noté **BSS**) et constitue une cellule. Chaque *BSS* est identifié par un *BSSID*, un identifiant de 6 octets (48 bits). Dans le mode *infrastructure*, le *BSSID* correspond à l'adresse MAC du point d'accès. Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs *BSS*) par une liaison appelée *système de distribution* (notée **DS** pour *Distribution System*) afin de constituer un *ensemble de services étendu* (*extended service set* ou *ESS*). Le système de distribution (*DS*) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil.



Un *ESS* est repéré par un **ESSID** (*Service Set Identifier*), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'*ESSID*, souvent abrégé en **SSID**, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du **SSID** est nécessaire pour qu'une station se connecte au réseau étendu.
Lorsqu'un utilisateur nomade passe d'un *BSS* à un autre lors de son déplacement au sein de l'*ESS*, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé *itinérance* (en anglais **roaming**).

2.2. La communication avec le point d'accès

Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal une requête de sondage (*probe request*) contenant l'*ESSID* pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun *ESSID* n'est configuré, la station écoute le réseau à la recherche d'un *SSID*.
En effet chaque point d'accès diffuse régulièrement (à raison d'un envoi toutes les 0.1 secondes environ) une **trame balise** (nommée **beacon** en anglais) donnant des informations sur son *BSSID*, ses caractéristiques et éventuellement son *ESSID*. L'*ESSID* est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option.

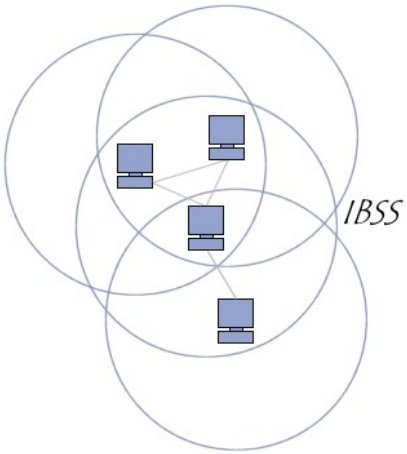
A chaque requête de sondage reçue, le point d'accès vérifie l'*ESSID* et la demande de débit présents dans la *trame balise*. Si l'*ESSID* correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe. En effet d'une manière générale, plus un point d'accès est proche, meilleur est le débit.

Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même *SSID*) pourra ainsi **choisir** le point d'accès offrant le meilleur compromis de débit et de charge.

2.3. Le mode ad hoc

En **mode ad hoc** les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point (*peer to peer* en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès L'ensemble formé par les différentes stations est appelé *ensemble de services de base indépendants* (en anglais **independant basic service set**, abrégé en *IBSS*).
Un *IBSS* est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'*IBSS* constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un *SSID*, comme l'est un *ESS* en mode infrastructure.

Dans un réseau ad hoc, la portée du *BSS indépendant* est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations. En effet, contrairement au mode infrastructure, le mode *ad hoc* ne propose pas de *système de distribution* capable de transmettre les trames d'une station à une autre. Ainsi un *IBSS* est par définition un réseau sans fil restreint.



III. L’architecture en couches du IEEE 802.11

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.

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.

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.

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.
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.

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 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.
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.
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.

LA COUCHE LIAISON DE DONNEES

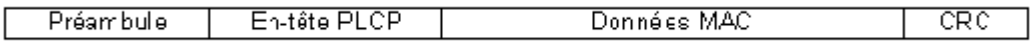
La couche de liaison de données de 802.11 se compose de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC). Le standard 802.11 utilise la LLC 802.2 et l'adressage sur 48 bits, tout comme les autres LAN 802, simplifiant ainsi le pontage entre les réseaux sans fil et filaires. Le contrôle d'accès au support est en revanche propre aux WLAN.
Le 802.11 MAC est conçu pour supporter de multiples utilisateurs sur un support partagé en faisant détecter le support par l'expéditeur avant d'y accéder.
Pour les LAN Ethernet (802.3), le protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) régule l'accès des stations Ethernet au câble ; il détecte et gère également les collisions qui se produisent lorsque deux périphériques ou plus tentent de communiquer simultanément sur le LAN.
Dans un WLAN 802.11, la détection des collisions est impossible du fait de ce qu'on appelle le problème "near/far". Pour détecter une collision, une station doit être capable de

transmettre et d'écouter en même temps. Or, dans les systèmes radio, il ne peut y avoir transmission et écoute simultanées.
Pour prendre en compte cette différence, le standard 802.11 fait appel à un protocole légèrement modifié, baptisé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), ou à la fonction DCF (Distributed Coordination Function), qui est une variante améliorée de la méthode d'accès CSMA/CA.
Autre problème de la couche MAC, spécifique au sans fil, celui du "nœud caché", où deux stations situées de chaque côté d'un point d'accès peuvent entendre toutes les deux une activité du point d'accès, mais pas de l'autre station, problème généralement lié aux distances ou à la présence d'un obstacle. Pour résoudre ce problème, le standard 802.11 définit sur la couche MAC un protocole optionnel de type RTS/CTS (Request to Send/Clear to Send). Lorsque cette fonction est utilisée, une station émettrice transmet un RTS et attend que le point d'accès réponde par un CTS. Toutes les stations du réseau peuvent entendre le point d'accès, aussi le CTS leur permet de retarder toute transmission prévue, la station émettrice pouvant alors transmettre et recevoir son accusé de réception sans aucun risque de collision. Du fait que le protocole RTS/CTS ajoute à la charge du réseau en réservant temporairement le support, il est généralement réservé aux plus gros paquets, dont la retransmission s'avérerait lourde du point de vue de la bande passante.
Enfin, la couche MAC 802.11 offre deux autres caractéristiques de robustesse : les sommes de contrôle CRC et la fragmentation des paquets. Pour chaque paquet, une somme de contrôle est calculée et rattachée afin d'assurer que les données n'ont pas été corrompues durant leur transit.
Cette technique diffère d'Ethernet où les protocoles de niveau supérieur tels que TCP gèrent le contrôle d'erreur. La fragmentation des paquets permet de casser les gros paquets en unités de plus petite taille lorsqu'ils sont transmis par radio, ce qui s'avère particulièrement utile dans les environnements très congestionnés ou lorsque les interférences posent problème, puisque les gros paquets courent plus de risque d'être corrompus. Cette technique limite le risque de devoir retransmettre un paquet et améliore donc globalement les performances du réseau sans fil. La couche MAC est responsable de la reconstitution des fragments reçus, le traitement étant ainsi transparent pour les protocoles de niveau supérieur.

Analyse des types de trames utilisés pour le protocole 802.11

Il y a trois principaux types de trames :
o Les trames de données, utilisées pour la transmission des données
o Les trames de contrôle, utilisées pour contrôler l'accès au support (eg. RTS, CTS, ACK)
o 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.

Format des trames



Toutes les trames 802.11 sont composées des composants suivants :

Préambule

Il est dépendant de la couche physique et comprend :
o Sync : 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).
o SFD : Le Start Frame Delimiter consiste en la suite de 16 bits 0000 1100 1011 1101, utilisée

pour définir le début de la trame.

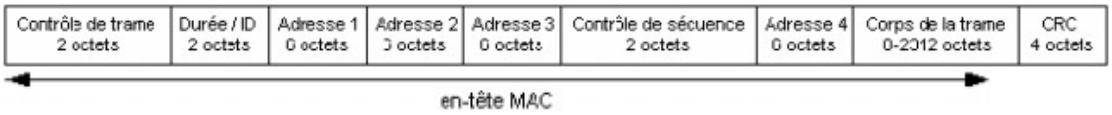
En-tête PCLP (Trame 802.11)

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

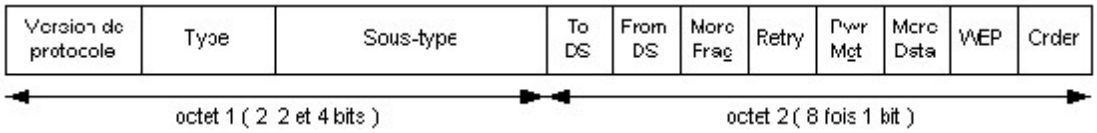
- Longueur de mot du PLCP_PDU : il représente le nombre d'octets que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.
- Fanion de signalisation PLCP : il contient seulement l'information de taux
- Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC.

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
- 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 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.

Contrôle de séquence (en-tête MAC)

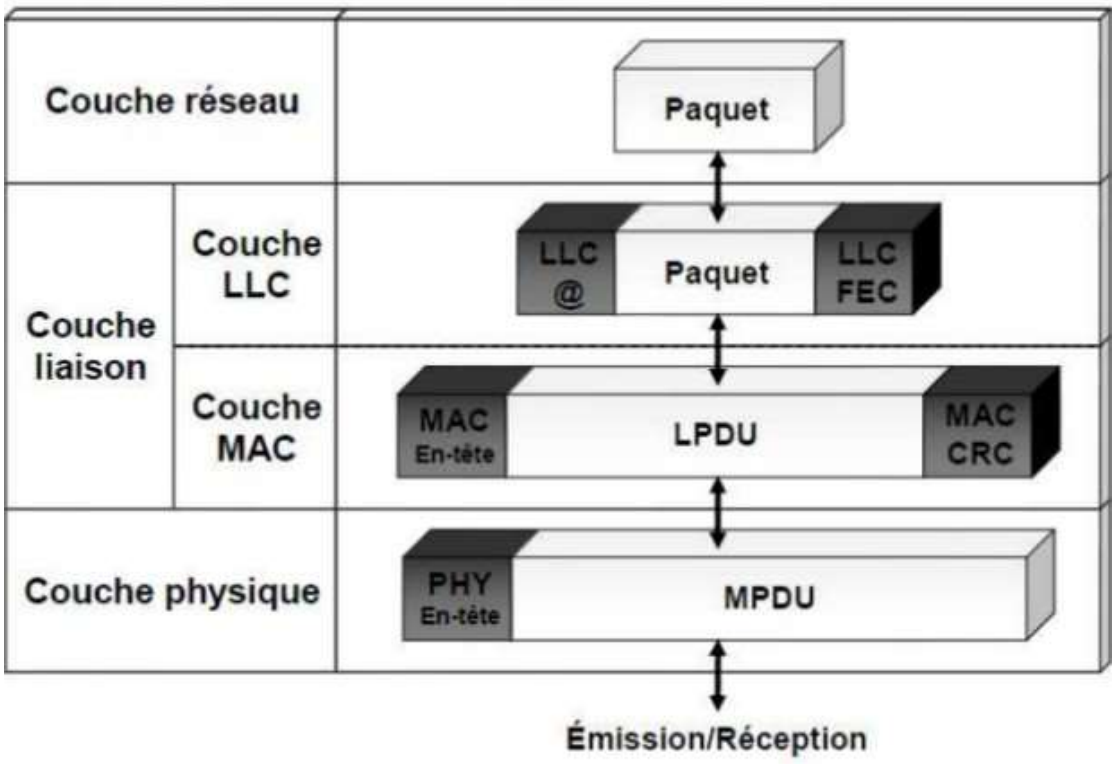
Le champ de contrôle de séquence est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame, et pour reconnaître les paquets dupliqués. Il consiste en deux sous champs, le numéro de fragment et le numéro de séquence qui définissent le numéro de trame et le numéro du fragment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

IV. Liaison de données 802.11

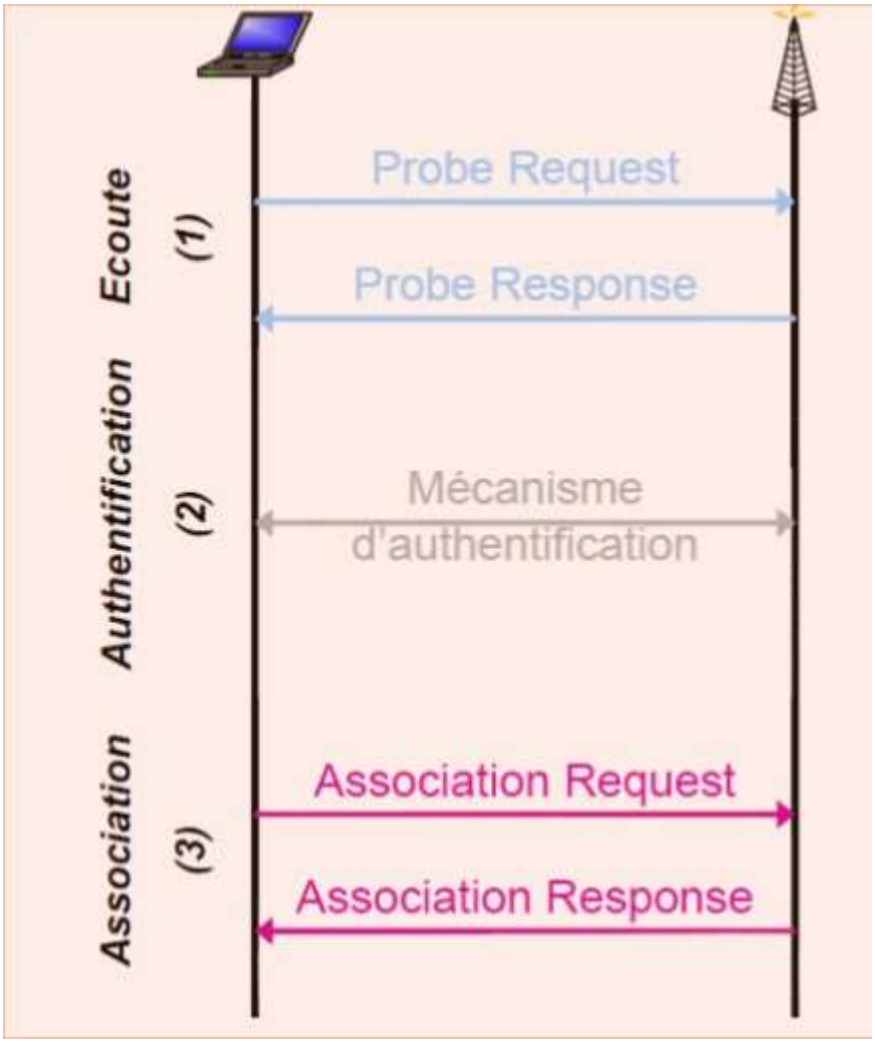
La couche de liaison de données de 802.11 se compose de deux sous-couches :
le contrôle de la liaison logique (Logical Link Control, ou LLC) : Définie par le standard IEEE802.2 et,
le contrôle d'accès au support (Media Access Control, ou MAC) :Assez similaire à la couche MAC 802.3 du réseau Ethernet terrestre

La couche LLC

● Lien logique entre la couche MAC et la couche réseau via le LSAP : Logical service Access Point
● Le LSAP permet de rendre interopérable des réseaux différents au niveau MAC ou physique, mais possédant la même LLC
● Cacher à la couche réseau les différences topologiques physiques
● Fournir une garantie de livraison des messages, la détection et la reprise sur erreur
● Deux fonctionnalités :
o Système de contrôle de flux
o Système de détection et reprise sur erreur



Connexion au réseau



La couche MAC

● Fonctionnalités
o Contrôle d'accès au support
o Formatage des trames et adressage
o Contrôle d'erreur par CRC
o Fragmentation et réassemblage
o Qualité de service
o Gestion d'énergie
o Gestion de la mobilité
o Sécurité

MAC : Problèmes à résoudre

● Résoudre le problème du média
➢ non guidé e.g. air
➢ énorme affaiblissement du signal, trajets multiples
● Résoudre le problème des interférences inter-symboles
➢ entête de synchronisation
➢ séquences d'apprentissage pour une équalisation du signal
● Résoudre le problème du taux d'erreur
➢ pas de vue atomique du réseau

➢ réutilisation spatiale

➢ noeuds cachés (hidden node)

- ● Résoudre le problème de la diffusion fiable
  ➢ dans un réseau radio, la diffusion n'existe pas
  ➢ e.g. ARP :
  - requête en diffusion portant l'adresse IP cible
  - réponse en point à point à la source
  ● Résoudre le problème de la détection de collision
  ➢ En Radio: du fait de l'affaiblissement, impossible de détecter la réception d'un autre signal pendant la transmission de son propre signal
  ➢ en quelque sorte aveuglé par son propre signal émis
  ➔ la détection de collision concomitante avec la transmission n'est pas possible
  ● Deux méthodes d'accès
  o Distribution Coordination Function (DCF), méthode d'accès avec collision. Utilisée par le mode ad-hoc et infrastructure :
  ● avec contention
  ● support de données asynchrones
  ● chances égales d'accès au support
  ● collisions
- Point Coordination Function (PCF), méthode d'accès sans collision. Utilisée par le mode infrastructure
  ● sans contention
  ● pas de collisions
  ● transmission de données isochrones
  ● (applications temps-réel, voix, vidéo)
  Distributed Coordination Function (DCF)
  ● méthode d'accès générale pour le transfert de données asynchrones
  ● sans gestion de priorité
  ● repose sur le CSMA/CA
  ● obligatoirement implémentée par les AP mais pas forcément seule
  Qu'est-ce que le CSMA/CA ?
  Carrier Sense Multiple Access with Collision Avoidance
  ● similitudes avec la technique CSMA/CD
  ● avec le même type de MAC adresse puisque compatible LLC
  ● avec acquittement positif
  ● Exemple: une station qui veut transmettre écoute le support de transmission:
  ● s'il est occupé, la transmission est reportée
  ● chaque station devra attendre :
  ● jusqu'à ce que la transmission s'arrête lorsque le récepteur envoie le ACK
  ● + un moment égal à la valeur d'un temporisateur: IFS (Initial Interframe Space)
  ● + un nombre aléatoire de time slots pour la prochaine transmission afin d'éviter des collisions
  ● sinon (le canal est à inactif) la station peut transmettre
  ● NB: Ceci exige que chaque station "entende" toutes les autres stations. Ce n'est pas toujours vrai (hidden node problem).
  CSMA/CA

● CSMA/CA implique des nouveaux mécanismes...
● accès aléatoire avec écoute de la porteuse :
➢ évite plusieurs transmissions simultanées,
➢ réduit le nombre de collisions
➢ impossible de détecter les collisions
● mettre en place des mécanismes pour les éviter:
➢ écoute du support
➢ accès au support
➢ backoff (période d'inactivité programmée: contention)
➢ réservation
➢ trames d'acquittement positif (positive ACK)

L'écoute du support

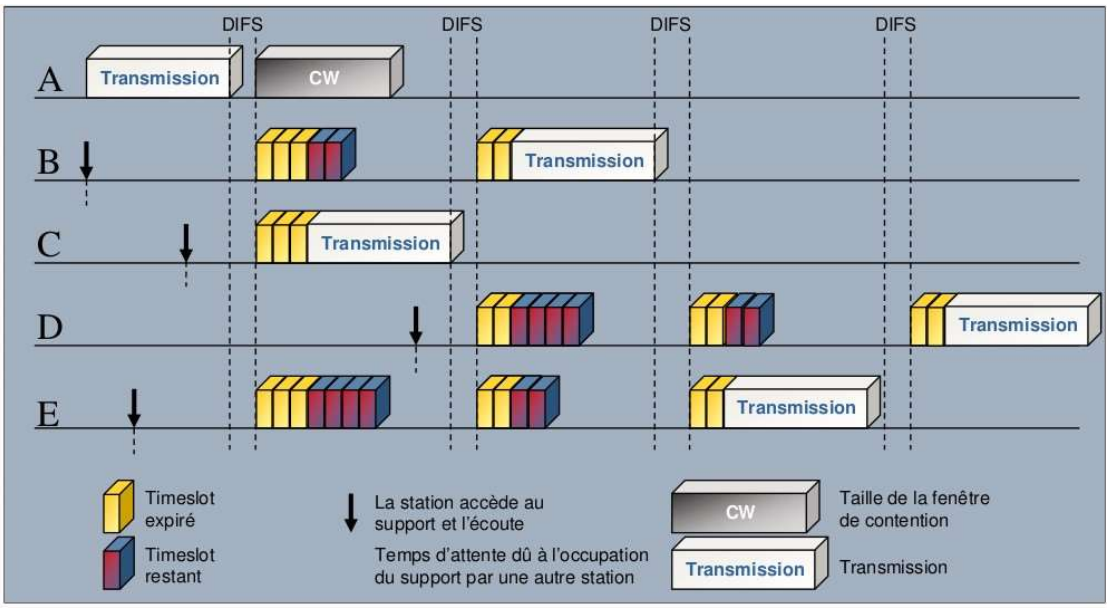
● Couche PHY : Physical Carrier Sense (PCS) :
● détecte et analyse les trames
● fait appel au PLCP (Physical Layer Convergence Protocol)
● Couche MAC : Virtual Carrier Sense (VCS) :
● réserve le support via le PCS
● deux types de mécanismes :
● réservation par trames RTS/CTS
● utilisation d'un timer (NAV : Network Allocation Vector) calculé par toutes les stations à l'écoute
● horloges bien synchronisées (beacons)

L'accès au support

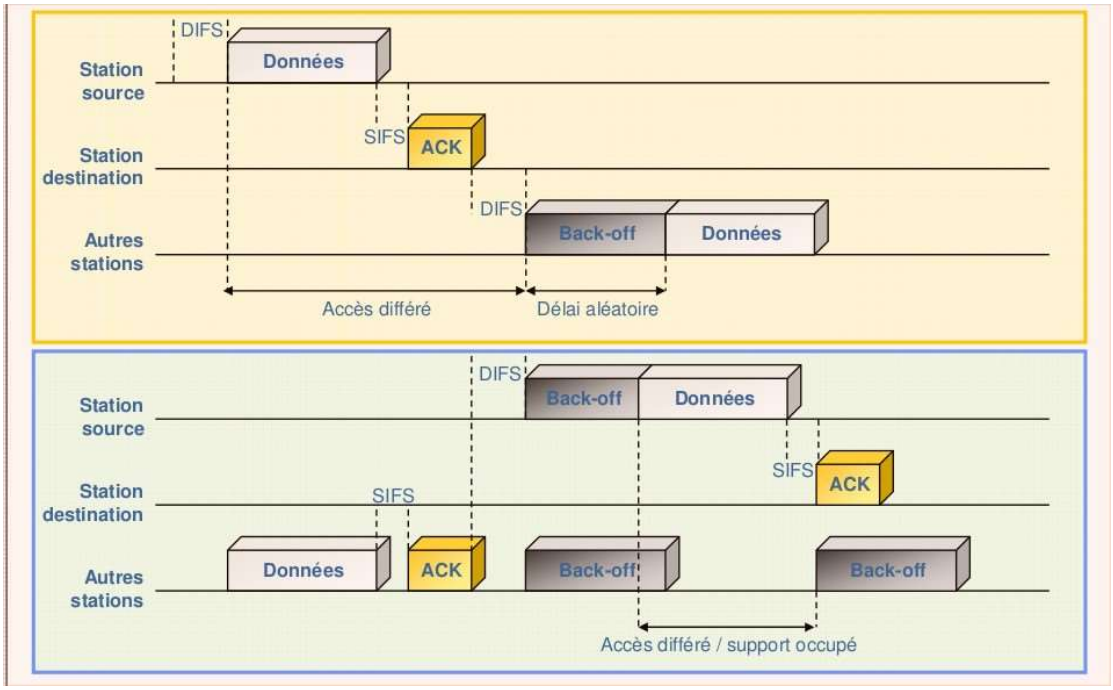
● mécanisme d'espacement entre deux trames : IFS
● 4 types d'Inter-Frame Spacing :
● SIFS : Short IFS : sépare les différentes trames d'un même dialogue (données et ACK, RTS et CTS, différents fragments d'une trame segmentée, trame de polling en mode PCF)
● PIFS : PCF IFS = SIFS + 1 timeslot : accès prioritaire, mode PCF
● DIFS : DCF IFS = SIFS + 2 timeslots : mode DCF
● (EIFS : Extended IFS : le plus long, uniquement en mode DCF)

Backoff

● fenêtre de contention CW
● timer Tbackoff=random(0,CW)×timeslot



Exemples de transmissions en DCF



Problème de la station cachée

● Deux stations situées chacune à l'opposé de l'AP ou d'une autre station :

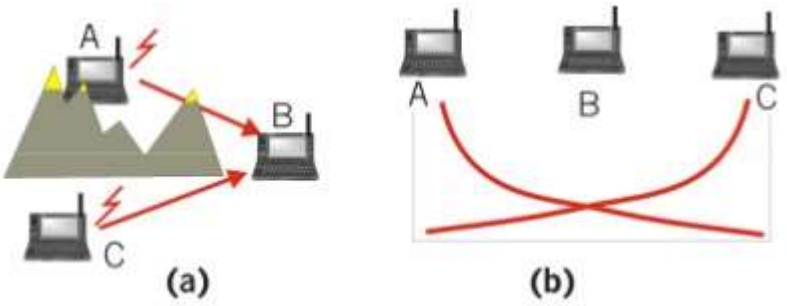
● Ne peuvent pas s'entendre mutuellement pour cause de distance ou de présence d'obstacles

● Effectuent des transmissions : Bande passante perdue

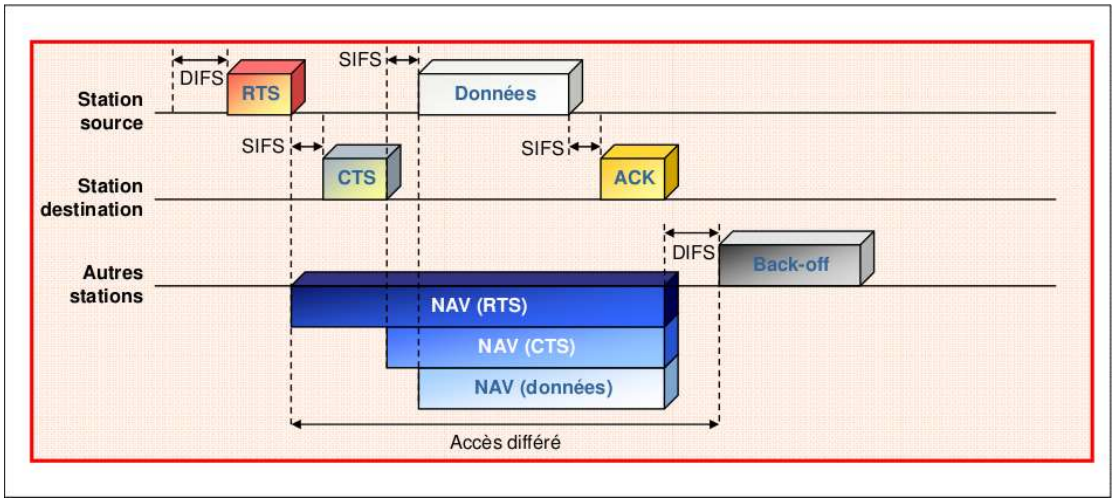
● Solution :

● Réservation du support : trames RTS/CTS

● Etat du support : NAV (network allocation vector)



Exemples de transmissions avec réservation



Point Coordination Function (PCF)

● transfert temps-réel (voix, vidéo), services de priorité

● le point d'accès prend le contrôle du support et choisit les stations qui peuvent transmettre : polling

● pas nécessairement implémentée par les AP (mais forcément en complémentarité de DCF)

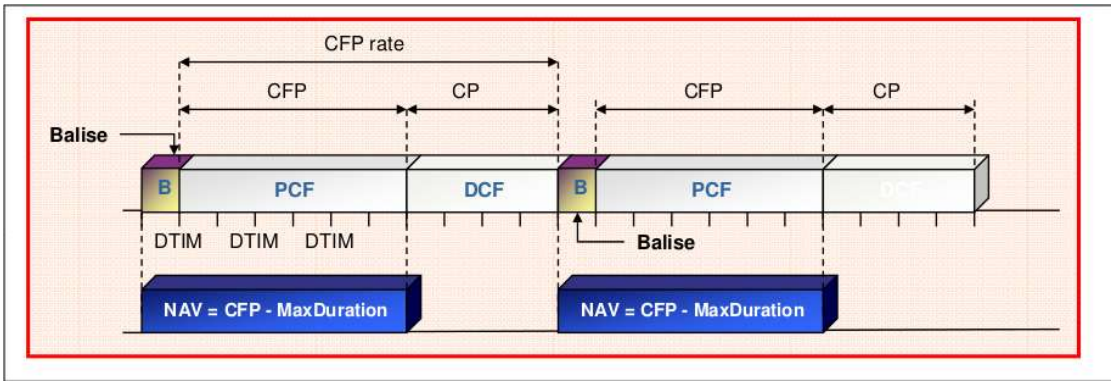
● PCF utilise un système de trame de controle (CF Poll frame) pour réguler l'accès des stations au média. Le coordinateur de Points d'Accès envoie cette trame (CF Poll frame) à tour de rôle à chacun des Point d'Accès , pour signifier l'octroi de l'autorisation de transmettre à station une trame unique pour n'importe quelle destination.

● Si le Point d'Accès interrogé n'a pas de trame à envoyer, il faut envoyer une trame de données nulle. Si le Point d'Accès émetteur ne reçoit pas d'accusé de réception de trame, il ne peut pas retransmettre la trame à moins que le coordinateur de Points d'Accès l'y autorise de nouveau. Le PCF balaie ainsi l'ensemble des stations pour qu'elles puissent accéder de façon équitable au média.

● Le service sans contention n'est pas disponible en permanence. Des périodes sans contention arbitrées par le coordinateur de points alternent avec le service DCF normal. La taille relative de la période sans contention peut être configurée.

Contention :

le point d'accès définit un PC (Point Coordination) avec deux périodes :

- CP (Contention Period) : période de temps avec contention et DCF
- CFP (Contention Free Period) : période de temps sans contention et PCF

Exemples de transmissions en PCF