Réseaux : RCA - Code RSX103

Chapitre III

RÉSEAUX LOCAUX SANS FILS

(Wirelss LAN)

IEEE 802.11 'WiFi' (Wi-Fi : Wireless Fidelity)

- Généralités – Modèle OSI
- Niveau liaison
- Niveau physique
- Architecture des réseaux sans fil

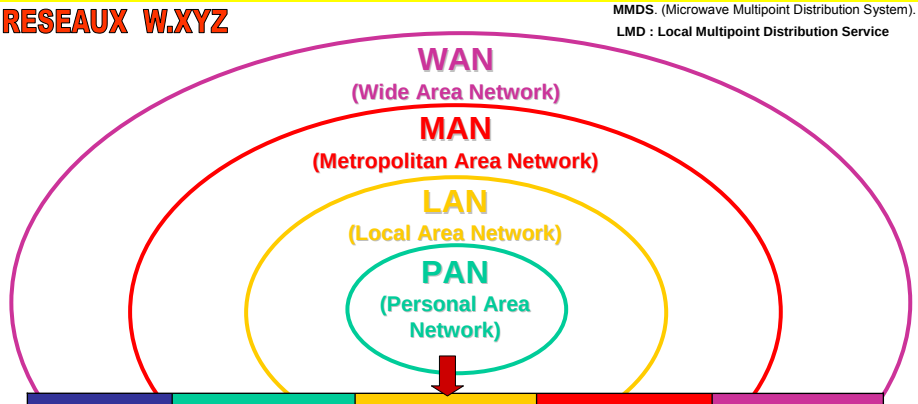
GENERALITES

- **Ce Chapitre est dédié aux réseaux locaux sans fil.**
  - Le terme réseau locaux sans fil est une traduction immédiate de l'anglais de Wirless LAN (Wirless Local Airea NetWork)
- **Les réseaux locaux sans fil sont à étudier dans le domaine des réseaux locaux partagés,**
  - puisque leur protocole est destiné au partage d'une voie commune qui est une bande de fréquence radio
- **Dans le domaine des réseaux locaux sans file, le standard IEEE 802.11 est un peu près le seul le plus connu),**
  - ici nous ne traiterons que cet exemple
- **Les réseaux locaux 802.11 ont reçu la domination commercial WIFI (Wirelss Fidelity).**
  - WIFI est donc totalement équivalent à IEEE 802.11.

Généralités – Catégories des réseaux locaux sans fils -1-

RESEAUX W.XYZ

MMDS. (Microwave Multipoint Distribution System).
LMD : Local Multipoint Distribution Service



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g WI-FI /HIPERLAN 2..	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Vitesse	< 1 Mbps	2 à 54+ Mbps	22+ Mbps	10 to 384 Kbps
Portée	Courte	Moyenne	Moyenne-Longue	Longue
Applications	Peer-to-Peer Device-to-Device	Réseaux d'entreprises et particulier	Fixe, dernier kilomètre	PDAs, Téléphones Mobiles Phones, cellular access

Généralités – Catégories des réseaux locaux sans fils -2-

❑ **Différentes catégories des systèmes de communication sans fils**

- **Une façon courante de présenter les technologies de communication sans fil consiste à les classer sur un schéma indiquant le débit en fonction de la portée de transmission :**

1. **Réseaux personnels sans fils (WPAN)**
   - **Bluetooth (IEEE 802.15.1),**
   - **HomeRF,**
   - **ZigBee IEEE (802.15.4),**
   - **Infrarouges**
2. **Réseaux locaux sans fils (WLAN)**
   - **WiFi IEEE 802.11,**
   - **HiperLAN,**
   - **DECT**
3. **Réseaux métropolitains sans fils (WMAN)**
   - **Norme IEEE 802.16 (boucle locale radio), Wimax**
4. **Réseaux étendus sans fils (WWAN)**
   - **GSM (Global System for Mobile),**
   - **GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunication System).**

Généralités – Catégories des réseaux locaux sans fils –2.1-

1. **Réseaux personnels sans fils (WPAN)**

- **Sont d'une portée très faible : de quelques mètres à quelques dizaines de mètres.**
- **L'objectif est de relier des systèmes informatiques très peu distantes à l'intérieure d'une même pièce :**
  - **il peut s'agir d'ordinateurs, de périphériques d'ordinateurs, d'imprimantes ..de téléphones portables ou encore des appareils domestiques.**
- **On utilisé aussi ces réseaux dans le domaine industriel pour connecter un système de diagnostic et un système informatique embarqué.**

Généralités – Catégories des réseaux locaux sans fils –2.2-

- **Exemples :**

A. : Bluetooth

- **développé par Ericsson et normalisé en IEEE 802.15.1 pour connecter un téléphone portable et une périphérie très proche comme une oreillette,**
- **il a été, ensuite repris par de nombreux industriels.**
- **Le débit visé est de 1Mbits/s et la distance autorisée est d'une trentaine de mètres.**
- **La consommation est donc très fiable en rapport avec la faible portée.**
- **Ce réseau est en développement depuis 1994 et déjà très utilisé.**

B. Home RF : Home Radio Frequencey

- **est soutenu par un consortium de constructeurs depuis 1998**
- **Remplacé par WIFI car d'objectifs très similaires**

Généralités – Catégories des réseaux locaux sans fils –2.3-

- **Exemples - suite:**

  C. **Zigbee / IEEE 802.15.4 :**

  - **a été développé pour des réseaux sans fils à très bas prix et avec de très faible consommations comme des petits appareils « par exemple des jouets ».**

  D. **Citons pour mémoire, la communication à infra rouges utilisé dans les télécommandes et qui sont aussi dans le domaine des réseaux sans fils.**

Généralités – Catégories des réseaux locaux sans fils –2.4-

2. **Réseaux Locaux sans fils (WLAN)**

   - **Sont destinés à remplacer un réseau local filaire, pour cela, il faut qu'ils aient :**
     - Une portée d'une centaine de mètre
     - et un débit d'un dizaine de Mbits/S.
     - WIFI, que nous allons étudier dans ce chapitre est le standard par excellence, avec son débit maximum de 54 Mbits/s et une portée mesurant une centaine de mètres.

   - **Hiper LAN :**
     - est un acronyme de Hygh Performance Radio LAN
     - C'est une proposition européen pour un réseau sans fil local du type voisin du WIFI
     - S'est complètement effacé devant le développement de WIFI

   - **DECT : est un acronyme de Digital Enhanced Cordless Telecommunications:**
     - Est un standard pour le téléphone sans fil domestique. Cette nome est citée ici car elle a été utilisée pour construire des réseaux locaux sans fils dans les entreprises.

Généralités – Catégories des réseaux locaux sans fils –2.5-

3. Réseaux Métropolitains Sans fils (WMAN : Wirless Metroplitain Area Network) :

- Sont utilisé pour connecter des réseaux locaux sans fils sur une aire géographique à l'échelle d'une agglomération (⇔ quelques Km, voir une dizaine de km).
- On parle encore de boucle local radio (BLR : Wirless Local Boucle) dans la mesure ou ce type de réseaux peut remplacer les boucles locale filaires du réseau téléphonique.
- C'est une donc une technologie qui est utilisée par des constructeurs qui veulent connecter de nouveaux abonnés à leurs réseaux sans recourir aux frais de la boucle locale classique.
- **Exemples :**
  - La principale norme dans ce domaine est IEEE 802.16 avec un débit de 10 Mbits/s et une portée de 10 Km.
  - Citons aussi la proposition WIMAX, un standard développé par un consortium de constructeurs avec Intel et Nokia et d'autres, le débit de WIMAX et de 70 Mbits/s sur 50 Km de distance

Généralités – Catégories des réseaux locaux sans fils –2.6-

4. Réseaux Etendus Sans fils (WWAN : Wirless Wide Area NetWork) :

- On parle le plus souvent de réseaux cellulaires ou réseaux mobiles.
- Il s'agit des réseaux sans fils à distance quelconque, proposés par les opérateurs de télécommunications mobiles.
- On parle beaucoup des trois générations associées aux trois standards, à savoir :
  A. GSM : Global System for Mobile
  B. GPRS : General Packet Radio Service
  C. UMTS : Universal Mobile Telecommunication System

Remarque :

- Ces transparents montre à quel point le domaine des réseaux sans fils este en pleins bouillonnement, car, il faut se dire que chacune des architectures est en soit-même une architecture de réseau et présente une complexité énorme.

Généralités – WIFI -1-

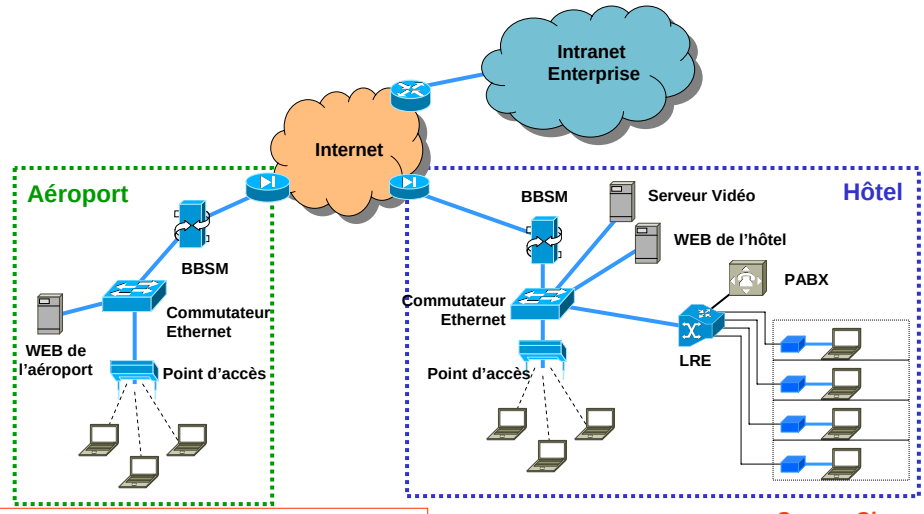
- Recherches sur les réseaux locaux sans fils depuis le début des années 1970.
- Normalisation wifi: fin des années 1990.

1. Avantages du sans fil :
   1. Les réseaux WIFI constitue un excellent compléments des réseaux locaux existant, car on un avantage considérable à ne pas avoir à câbler un bâtiment pour y mettre des machines réseaux.
   2. D'autre part, les communications sans fils offrent « à priori » plus de souplesse et de mobilité aux utilisateurs que les réseaux filaires.
2. Déploiement des réseaux Wifi
   - **Réseaux domestiques.**

Généralités – WIFI -2-

- **En terme de pénétration industrielle,**
  - les réseaux locaux WIFI sont déjà assez largement utilisés dans la communication à l'intérieur d'une maison
  - Ces réseaux sont également utilisés dans domaine des réseaux d'accès,
    - le point de départ est un lieu de fort passage « en anglais Hotspot » tel que les gares ou les aéroports,
    - les opérateurs, appelés WISP : Wirless Internet Service Provider » commencent à déployer des réseaux sans fils,
    - l'installation **des points d'accès WIFI** permet à des utilisateurs un accès à Internet et d'autres services via un accès 802.11

Architectures Wireless LAN « *HotSpot* » *Privé*

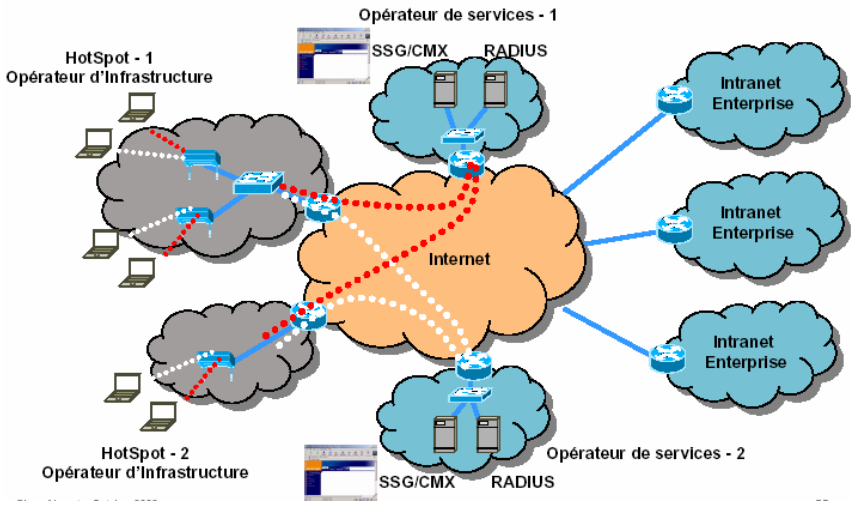


BBSM : Building Broadband Service Manager

Source Cisco

http://www.cisco.com/global/FR/documents/pdfs/datasheet/switching/Cat2950ST-LRE_fr_v3.pdf

Architectures Wireless LAN « *HotSpot* » *Public*



Source Cisco

Généralités WIFI: Quelques éléments d'architecture –1-

1. **WIFI : Est un réseau local radio.**

   - **Le réseaux WIFI définit une architecture de réseau local sans fils radio, c'est-à-dire un réseau local à medium partagé qui est une bande de fréquence.**

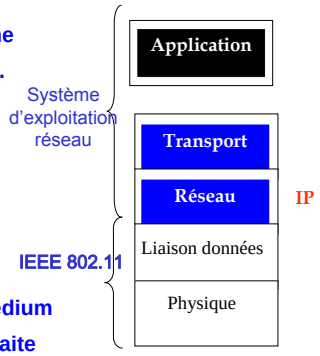
   - **Pour construire de tel réseau, il faut donc définir une couche physique et une couche liaison de données.**

1. **La couche physique :**

- **s'occupera de codage, de la modulation de la synchronisation des signaux.**

1. **La couche liaison de données :**

- **définit principalement les protocoles d'accès au medium qui est réalisé par une bande de fréquences, on y traite aussi les problèmes de qualité de service, de la fragmentation, ..etc. et de contrôle des erreurs.**



Généralités WIFI: Quelques éléments d'architecture –2-

2. **WIFI : Deux organisations architecturales.**

- **Le niveau liaison de WIFI présente deux organisations architecturales très différentes :**

1. **Le mode Infrastructure :**

   - **est un mode de fonctionnement centralisé avec lequel, un point d'accès central peut relayer les trames vers un autre réseau**

2. **Le mode ad'hoc :**

   - **est un mode de fonctionnement complètement distribué, dans lequel, deux stations peuvent communiquer à tout instant et ne suppose pas l'existence de point d'accès central qui joue un rôle particulier.**

Généralités WIFI: Quelques éléments d'architecture –3-

3. **WIFI : deux protocoles différents d'accès au médium.**

- Le niveau liaison WIFI peut fonctionner selon deux protocoles d'accès très différents

A. **Le protocole PCF : « Point Coordination Function » :**

- fonctionne en coopération selon une méthode d'arbitrage centralisé, c'est donc un protocole de pooling «scrutation »

B. **Le protocole DCF : « Distributed Coordination Function » :**

- fonctionne en compétition, il rentre dans la classe des protocoles Ethernet , mais il est très différent d'Ethernet.

⇨ Pouvant être utilisés simultanément par une station

Généralités WIFI: Quelques éléments d'architecture –4-

4. **WIFI : Différents niveaux physiques :**

- Le niveau physique de WIFI fait apparaître un grand nombre de standards
- Si on regard de plus près, on constate que les choses ne sont pas si compliqué que cela :
  - Le 802.11b : correspond à un débit de 11 Mbits/s
  - 802.11g : à un débit de 54Mbits/s.
  - La norme 802.11a : semble distancé par la norme 802.11g car il utilise le même débit.
  - 802.11n : correspond à une norme qui est en cours d'élaboration qui devrait permettre des débits beaucoup plus importants (maintenant dispo.)

Généralités WIFI: Quelques éléments d'architecture –5-

5. **Le WIFI :**

- **Est soutenu par un consortium qui est destiné à promouvoir aussi bien les normes WIFI que la diffusion des matériels associés.**
- **Avant, le WIFI Alliance s'appelait WECA : Wirless Ethernet Compatibility Alliance :**
  - **Cette référence à Ethernet est abandonnée; car cette référence est jugée plus nécessaire pour attirer les utilisateurs vers les nouveaux standards. Le sigle WIFI est, maintenant, connu aussi bien qu'Ethernet.**

Réseaux Locaux Partagés WIFI : Le modèle de référence

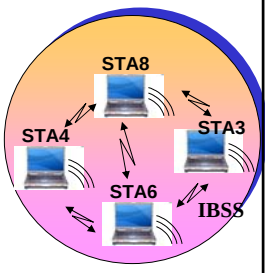
Architectures des Réseaux Locaux WIFI

Réseaux Locaux Partagés WIFI : Le modèle de référence

- La nonne IEEE 802.11 dispose de deux modes de fonctionnement distincts, qui correspondent à des architectures différentes:
  - ⇨ Deux types de topologies :
    1. Le mode réseau ad-hoc :
       - IBSS : Independent Basic Service Set
    2. Le mode infrastructure avec point d'accès :
       - **BSS : Basic Service Set**
       - **ESS : Extended Service Set**

Réseaux Locaux Partagés WIFI : Mode ad-hoc "Distribué"

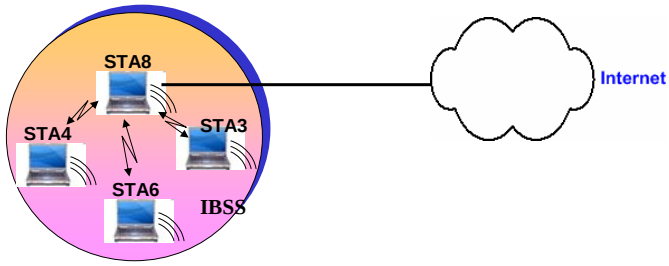
- **Dans le mode ad'hoc, il n'y a pas d'équipement qui joue un rôle particulier, comme par exemple, des contrôleurs centraux.**
- **C'est une approche complètement répartie dans laquelle, toutes les stations communiquent sur une base égalitaire.**
- **Les liaisons radios établies entre les stations radios sont des coupleurs sans fils (on parle aussi d'adaptateur sans fils:**
  - ➢ **Wirless adapter ou (Wirless Network Interface Adapter). Il existe de nombreux formats de cartes existent : PCI, PCMCIA, USB , …etc.**



- **Le mode ad'hoc peut être utilisée à condition que les stations soient suffisamment proches pour communiquer par radio, et que ces stations utilisent la même bande de fréquence.**
  - **Les stations ainsi associées forment ce que on appelle dans le jargon WIFI : IBSS : "Independent Basic Service Set"**

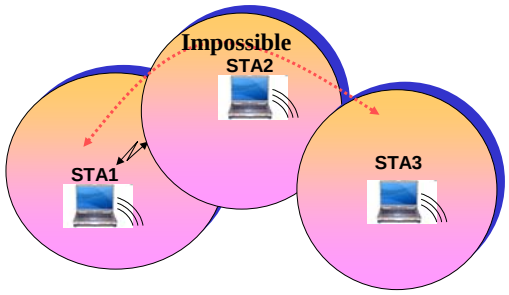
Réseaux Locaux Partagés WIFI : Mode ad-hoc “Distribué”

- **Un IBSS :**
  - **est une sorte de cellule d’entités communicantes sans fils.**
  - **Ce mode de fonctionnement complètement répartie traite un réseau sans fils sans besoin d’un équipement particulier, c’est pour quoi on l’appelle ad' hoc.**
- **Une station peut partager un accès à internet : le réseau fonctionne comme un BSS**



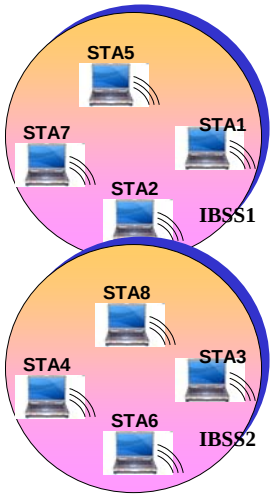
Réseaux Locaux Partagés WIFI : Mode ad-hoc “Distribué”

- **Remarque : Un IBSS :**
  - **3 stations en mode ad’hoc : différent d’un réseau ad’hoc de trois stations**
  - **Il n y a pas de protocole de routage : STA1 ne peut pas envoyer de données à STA3 car STA2 ne peut effectuer le routage**



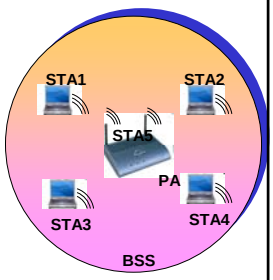
- **Bilan Mode peer-to peer (ad-hoc)**
  - Un réseau ad-hoc est un Groupe de terminaux formant un IBSS (Independent Basic Set Service)
  - Rôle : permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure telle qu'un point d'accès ou une connexion au système de distribution
  - Chaque station peut établir une communication avec n'importe quelle autre station dans l'IBSS
  - Pas de point d'accès : les stations n'intègrent qu'un certain nombre de fonctionnalités
  - Mode très utile pour mettre en place facilement un réseau sans fil lorsqu'une infrastructure sans fil ou fixe fait défaut

- Les stations en mode ad’hoc utilisent le protocole d’accès en mode distribué “DCF”
- Si tôt, les stations sont hors de portée radio l’unes des autres, comme les stations 5 et station 6 sur la figure, elles ne peuvent plus communiquer en utilisant seulement DCF.



Réseaux Locaux Partagés WIFI : Le Mode infrastructure « Centralisé »

- **Le mode infrastructure est un mode de fonctionnement centralisé, autour des dispositifs qui sont baptisés AP « Access Point » ou en français : Point d'Accès.**
  - **Il existe donc un certain nombre de stations de travail qui dialoguent avec l'AP via des coupleurs**
  - **Les PA qui sont des systèmes informatiques disposant d'une carte réseau WIFI et qui peuvent accéder au monde extérieur**



- **Ce point d'accès est généralement relié à un réseau filaire.**
  - **Il permet aux stations sans fil de communiquer avec des stations du réseau filaire.**
  - **Il permet également à une station sans fil de communiquer avec une autre station sans fil, qu' elle dépende ou non du même point d'accès**
  - **La norme désigne par BSS (Basic Service Set) l'ensemble des stations radio à portée radio du point d'accès**

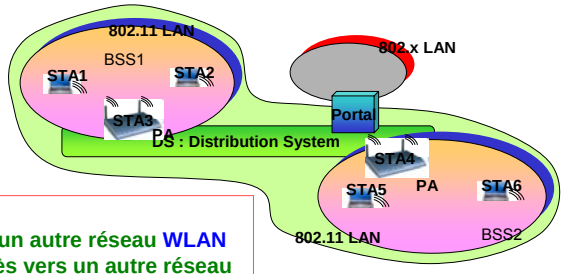
Réseaux Locaux Partagés WIFI : Le Mode infrastructure « Centralisé »

✓ Dans un BSS, il n'existe qu'un point d'accès :

- **tout le trafic passe obligatoirement par ce point d'accès.**
- **La zone de couverture est donc restreinte à la zone de portée radio autour de ce point d'accès.**
- **Le support est partagé entre toutes les stations d'un BSS, ainsi que le débit (11 Mbit/S)**

✓ Le PA d'un BSS peut jouer le rôle d'un communicateur avec un autre BSS via un autre réseau,

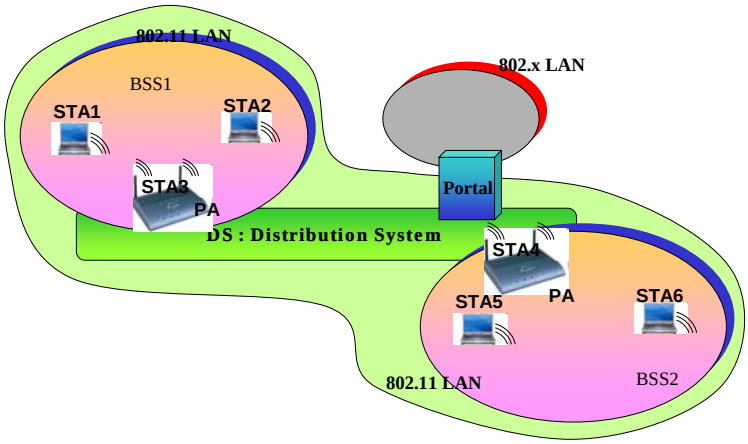
- **dans le jargon WIFI, cet autre réseau est baptisé un DS « Distributed System ou système de distribution »**



Un DS :
- **Est un réseau Ethernet ou un autre réseau WLAN**
- **Objectif : Fourniture d'accès vers un autre réseau**

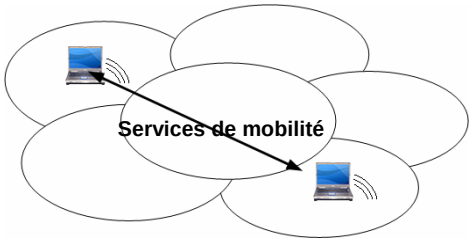
Réseaux Locaux Partagés WIFI : Le Mode infrastructure « Centralisé

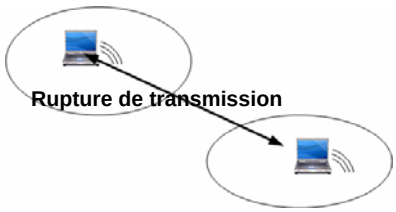
- **Un ESS : Extended Service Set :**
  - **Plusieurs points d'accès (BSS) connectés entre eux par un systèmes de distribution**



Réseaux Locaux Partagés WIFI : Le Mode infrastructure « Centralisé »

- Topologie ESS variable :cellules recouvrantes ou non
  - Les cellules recouvrantes permettent d'offrir un service de mobilité (IEEE 802.11f) : pas de pertes de connexions
  - Plus grand nombre d'utilisateurs possibles sans dégradation trop importante des performances





Lorsqu'une station mobile se déplace d'une cellule vers une autre(d'un BSS à un autre) : problème de changement de point d'accès (handover / roaming),

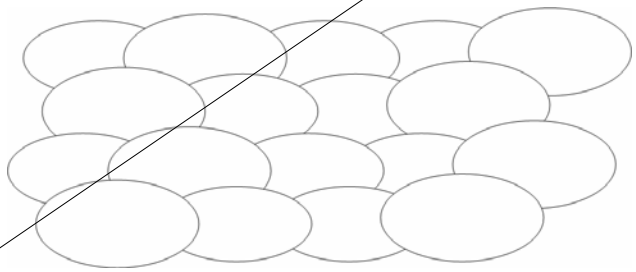
le changement est déterminé par la surveillance de la qualité de transmission des signaux sur les différents points d'accès dans l'environnement d'une station.

Le mobile WIFI peut passer de façon transparent d 'un point d'accès à un autre.

Les points d'accès peuvent échanger des informations d'entrée et de sortie dans leur BSS grâce à au système de distribution au moyen d'un protocole d'itinérance, on appelle ça le protocole de roaming.

Réseaux Locaux Partagés WIFI : Le Mode infrastructure « Centralisé »

- **Réseaux ambiant**
  - **Permet de se connecter à Internet de partout**
  - **Constitué de nombreuses cellules qui possèdent chacune un point d'accès**
  - **Les points d'accès sont reliés entre eux par un réseau d'infrastructure (Ethernet, GigE, IEEE 802.17, …etc.)**



Mode Infrastructure : Bilan –1-

- **Blian : Réseaux en Mode infrastructure :**
  - Fournit aux différentes stations des services spécifiques sur une **zone de couverture déterminée par la taille du réseau**
  - Réseaux d'infrastructure établis en utilisant des **points d'accès ou Access Points (AP)**, qui jouent le rôle de station de base pour un BSS
  - **Chaque BSS** est relié à un système de distribution ou **DS (Distribution System)** par l'intermédiaire de leur point d'accès (AP) respectif
  - **Système de distribution** : en général un réseau Ethernet utilisant du câble métallique
  - Groupe de BSS interconnectés par un DS = **ESS** (Extended Set Service)

Mode Infrastructure : Bilan –2 -

- **Bilan : Réseaux en Mode infrastructure :**
- **Rôle du DS**
  - ✓ Le système de distribution (DS) est responsable du transfert **des paquets entre** différents BSS d'un même ESS
  - ✓ DS implémenté de manière indépendante de la structure hertzienne de la partie sans fil
  - ✓ Le DS peut correspondre à un réseau Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface) ou un autre IEEE 802.11
- **• Rôle de l'ESS**
  - ✓ L'ESS peut aussi fournir aux différentes stations mobiles une passerelle d'accès vers un réseau fixe, tel qu'Internet
  - ✓ Passerelle : connexion du réseau 802.11 à un autre réseau

Réseaux Locaux Partagés WIFI : Le modèle de référence

IEEE 802.11 dans la hiérarchie OSI

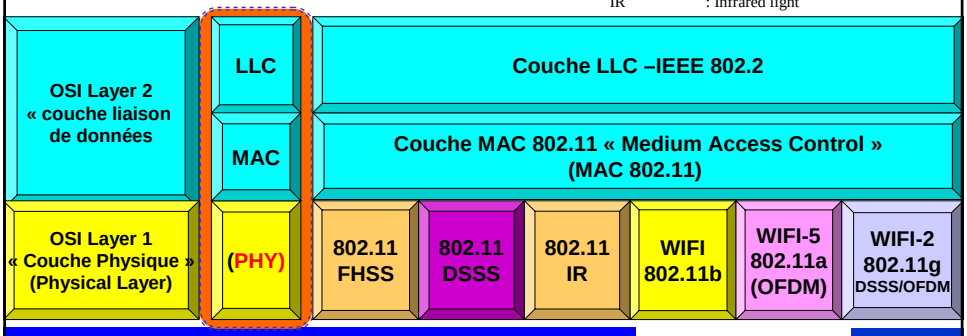
Sous-Couche Liaison de données

Sous-Couche MAC

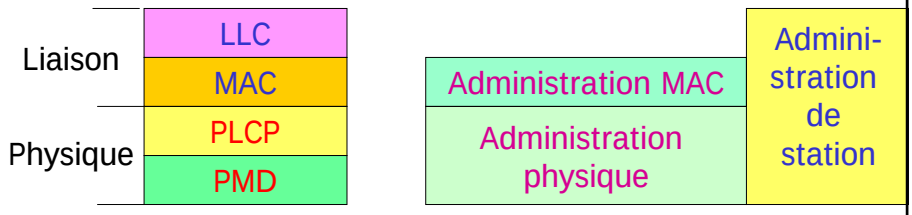
Architecture IEEE 802.11 : Le modèle de référence WIFI

- A l'instar des autres normes 802.*x*, 802.11 couvre les couches physique et liaison de données.
- Le schéma suivant présente les couches en question, positionnées par rapport au modèle de référence OSI de l'ISO :
- IEEE 802.11 définit :
  - ⇨ La couche liaison de données / subdivisée en deux sous-couches :
    1. liaison (LLC)
    2. et accès (MAC) pour les réseaux sans fils (commune à toutes les couches physiques)
  - ⇨ les couches physique

FHSS : Frequency hopping Spread spectrum
DSSS : Direct sequence Spread spectrum
IR : Infrared light



Architecture IEEE 802.11 : Modèle de référence WIFI

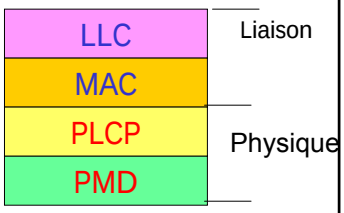


- Le modèle de référence (⇔ le modèle en couche) de WIFI ressemble à tous les modèle en couche des réseaux locaux récents.
- Sur la partie gauche du dessin,
  - Apparaît les aspects de transmission des donnés avec dans les niveau physique et liaison, deux sous-niveaux distincts
- Sur la partie droite sont représentées
  - Les fonctions d'administration du réseau. L'administration du réseaux et également structurée en couches mais de manière un peu différente.

Architecture IEEE 802.11 : Modèle de référence WIFI

I. <u>Pour ce qui est de la transmission de données</u>,

- Le niveau LLC : Logical Link Control
  - protocole de liaison point à point habituel,
  - ce niveau est commun à tous les réseaux locaux.



- Le niveau MAC : Medium Acces Control :

  → Est le niveau de partage de la voie commune avec les fonctions de contrôle d'erreur, de segmentation et de sécurité.

- Le niveau physique de convergence : PLCP : Physical Layer Convergence Protocol
  - réalise l'encapsulation des données de niveau physique :
    - ⇨ c'est-à-dire, **la traduction** d'une trame MAC en une trame du niveau physique

- Le niveau physique dépendant « PMD : Physical Medium Dependent » :
  - traite des **techniques de codage**, de **modulation** et de **synchronisation** et qui sont propres à un medium particulier (la bande de fréquence, la synchronisation, …etc.)

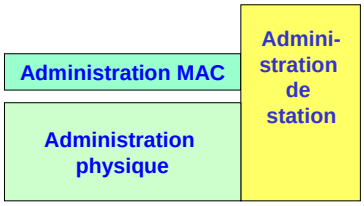
Architecture IEEE 802.11 : Modèle de référence WIFI

II. <u>Pour ce qui est de l'administration réseau : « Network Management » , on y trouve les</u>

1. couches administration de la couche physique (physical management »
   - ✓ fonctions de sélection des bandes de fréquences,
   - ✓ gestion de la MIB physique (⇔ de la base de données physique)
   - ✓ et de l'administration du niveau physique.

2. L'administration au niveau MAC « Administration MAC »
   - ✓ s'occupe de l'itinérance « en anglais le romaing » ou changement de cellules.
   - ✓ La gestion de l'économie d'énergie.
   - ✓ La gestion de MIB du niveau MAC (la gestion de la base des données des fonctions d'administration du niveau MAC)

3. La couche gestion station « station Management »
   - ✓ coordonner les différents fonctions d'administration au niveau d'une station



LE NIVEAU LIAISON DE DONNEES

Accès au médium

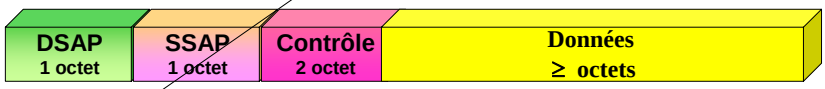
« MAC Medium Access »

- La couche liaison de données
  - **I. La couche LLC**
  - **II. La couche MAC**
    1. **Distributed Coordination Function : DCF**
       - **Le CSM/CA**
       - **L'écoute du support**
       - **L'accès Au support**
       - **Le back-Off**
       - **La contention**
       - **Exemple de transmission**
       - **Exemple de transmission avec réservation**
    2. **Point Coordination Function : PCF**
       - **Contention**

IEEE 802.11 : La couche liaison de données – 1 -

I. La couche LLC :

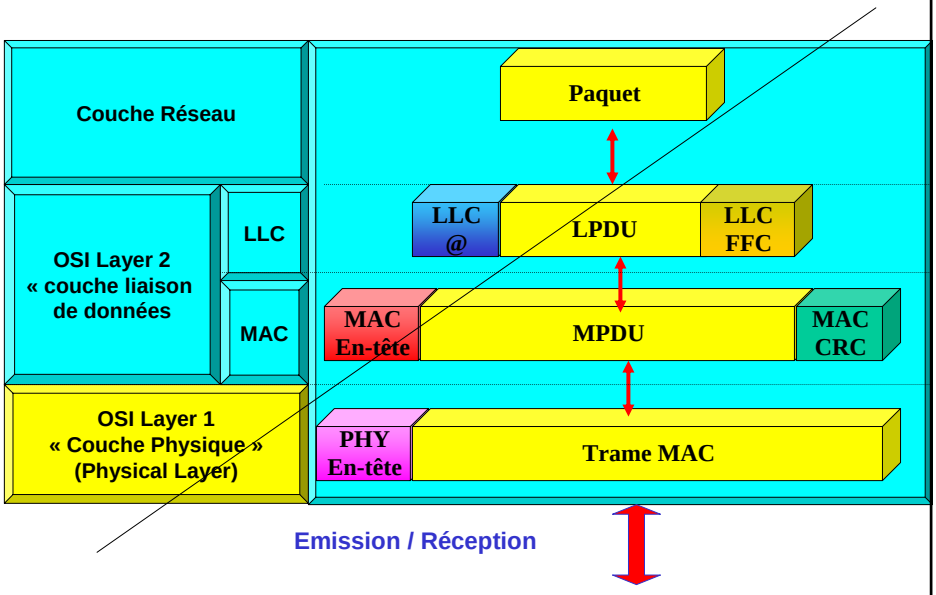
- Définie par le standard IEEE 802.2
- Lien logique entre la couche MAC et la couche réseaux (OSI 3) via le LSAP : Logical Service Access Point
- **Deux types de fonctionnalités :**
  1. Système de contrôle de flux
  2. Système de reprise sur erreur
- Le LSAP permet de rendre interopérables des réseaux différents aux niveaux MAC ou physique, mais possédant la même LLC
- LPDU : Logical Prtocol Data Unit



- DSAP : Destination Service Access Point
- SSAP : Source Service Access Point
- **Contrôle** : Type de LLC (avec / sans connexion avec / sans acquittement)

IEEE 802.11 : La couche liaison de données – 2 -

La couche LLC - suite



IEEE 802.11 : La couche liaison de données – 3 -

II. La couche MAC :

- **La couche MAC 802.11 est comparable à la couche MAC 802.3 :**
  - elle implante la politique d'accès.
- **Cette couche MAC est spécifique à l'IEEE 802.11 car elle offre d'avantages de fonctions par rapport à une couche MAC classique**
  - **Fonctionnalités :**
    - ⇨ **Contrôle d'accès au support (allocation du support)**
    - ⇨ **Adressage et formatage des trames**
    - ⇨ **Contrôle d'erreur par CRC**
    - ⇨ **Fragmentation et réassemblage**
    - ⇨ **Qualité de service**
    - ⇨ **Gestion de l'énergie**
    - ⇨ **Gestion de la mobilité**
    - ⇨ **Sécurité**
- **Remarque :**
  - Ces fonctions supplémentaires sont normalement **confiées aux protocoles supérieurs**, comme les sommes de contrôle de CRC, la fragmentation et le réassemblage (***très utile car le support radio a un taux d'erreur important***), les retransmissions de paquet et les accusés de réception.

IEEE 802.11 : La couche liaison de données – 4 -

❑ La couche MAC :

- **Deux modes sont définis**

1. DCF(Fonction de Coordination Distribuée)

- **Basée sur CSMA avec des extensions :**
  1. CSMA/CA: **C**arrier **S**ense **M**ultiple **A**cces / **C**ollision **A**voidance
  2. Réservation du canal avec **RTS / CTS**
- **Collisions possibles**
- **Appropriée à la transmission de données (sans QoS)**

2. PCF(Fonction de Coordination Centralisée)

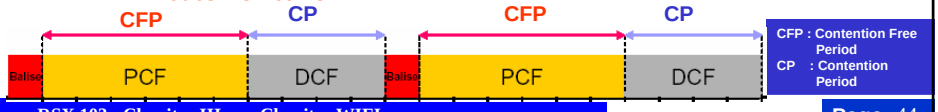
- **Basée sur l'interrogation périodique des stations par l'AP**
- **Sans collisions**
- **Appropriée au services temps réel**

➢ **Mode ad-hoc :**

- **Uniquement mode DCF**

➢ **Mode Infrastructure :**

- **Modes DCF et PCF**



DCF : Distributed Coordination Function –1.0-

❑ Principales caractéristique du mode DCF « Distributed Coordination Function »

1. Protocole en compétition avec écoute (CSMA) :

   a. Ce protocole du niveau MAC entre dans la catégorie des protocole en mode compétition. L'accès au medium en mode DCF est réalisée en compétition avec écoute (LBT : Listen Befor Talk)

      - Par contre, l'écoute n'est pas suffisante et nécessite un intervalle de vulnérabilité qui est du au temps de propagation des signaux.(Pendant cet intervalle, bien que les stations écoutent le medium, deux station peuvent commencer à transmettre leurs trames et produire une collision.

        ⇨ WIFI rentre comme Ethernet dans la catégorie des réseaux **CSMA** (Carrier Sense Multiple Access).

DCF : Distributed Coordination Function –1.1-

2. Ajournement non persistant.

   - Le mode DCF rentre dans la catégorie des réseaux locaux en compétition non persistant

     ☞ lorsqu'une station détecte par écoute que la voie est occupée, elle ne commence pas à émettre. Après la fin de la circulation des trames (la voie redevient libre), la station entre dans une phase d'attente d'une durée calculée par l'algorithme de retard binaire (binary backoff)

DCF : Distributed Coordination Function –1.2-

3. Détection de collisions par accusé de réception.

- La détection de collision dans WIFI n'est pas réalisée par l'écoute du medium, ceci n'est pas prévu.
- Dans WIFI, on a retenu le même principe qu' ALHOA : une détection de collision par accusé de réception positif
  - **chaque trame est associé à un code polynomial,**
  - **si le destinataire reçoit la trame correctement, il émet immédiatement une trame d'acquittement positif.**
  - **Si la trame n'est pas bien reçue, la trame est considérée comme en collision (en fait, elle peut être aussi perdue suite à une erreur sur ses données)**

DCF : Distributed Coordination Function –2.0-

4. Retransmission sur collision (binary backoff).

- **La retransmission en cas de collision est effectué après un temps d'attente réel défini par l'algorithme de retard binaire exponentielle (Exponantial Binary Backup)**

5. Gestion de la fragmentation.

- **A la différence d'Ethernet, WIFI dispose des mécanismes de fragmentation au niveau liaison (selon une politique liée au taux d'erreur sur la voie, permet de réduire la taille en fragments plus petites et diminuer ainsi le volume de retransmissions nécessaires.)**

6. Pas de gestion de connexion.

DCF : Distributed Coordination Function –2.1-

7. Pas de contrôle de flux.
   - Comme les débits visés ne sont pas très élevés, WIFI dans sa version de base ne propose aucun mécanisme de contrôle de flux

8. Pas de qualité de service (en version de base)
   - WIFI dans sa version de base ne propose pas de garantie de qualité de service : elle fonctionne donc au mieux (best effort)

DCF : Distributed Coordination Function –3-

9. Pas de garantie de livraison sans erreurs.
   a. **En matière de traitement des erreurs dues aux bruits : WIFI en mode DCF agit comme si c'était une collision :**
      ⇨ **le message en collision comme un message bruité, n'est pas acquitté, et en absence d'un acquittement positif, le message est retransmis.**
   b. la norme WIFI ne garantit pas formellement que la transmission soit sans erreur.
      - **WIFI renvoie à la couche supérieure la mise en place d'un protocole de détection et de correction des erreurs de transmission qui garantit un taux d'erreur acceptable**

DCF

« Ecoute et ajournement non persistant »

DCF : Ecoute et ajournement non persistant (1)

A. Ecoute et ajournement non persistant : Principe –Etapes

1. Ecouter la voie, transmettre si la voie est libre.
   - ⇨ Une station qui souhaite émettre, écoute la voie (qui est une bande de fréquence hertzienne)
   - ⇨ Elle transmet s'elle constate que la voie est libre ou moment ou elle veut transmettre.
     - ↳ Plus précisément, elle doit constater que une période de silence de durée prédéfinie.

DCF : Ecoute et ajournement non persistant (2)

2. Si la voie est occupée : choisir un intervalle d'attente aléatoire ('backoff') dans l'intervalle [0,CW] (⇔ CW : Contention Window ; défini au niveau physique).

   ⇔ Si la voie est occupée ou moment ou une station souhaite transmettre, on fait l'hypothèse que ceci indique l'existence d'une certaine charge,

   ⇔ Donc pour lisser le trafic, une station applique une stratégie **d'ajournement non persistant** en choisissant un **intervalle d'attente aléatoire** qui est le même qu'en cas de collision (« backoff time »).

      ↗ Cet intervalle est défini comme étant un nombre entier de tranches canal (slot time),

      ↗ la durée de tranche canal dépend du niveau physique utilisé à un moment donné par une station (exemple : dans la 802.11b la tranche canal dure 20 µs)

DCF : Ecoute et ajournement non persistant (3)

3. Quand le medium redevient libre : La station Décompte les intervalles de temps (tranche canal 'Slot Time).

   ⇔ Si le medium reste toujours libre pendant la durée d'une tranche de temps, la station continue à décrémenter son compteur d'attente

4. Le décompte est suspendu chaque fois le medium redevient occupé

   ⇔ chaque fois qu'une trame émise par une autre station est en cours de transmission, on arrête de décompter.

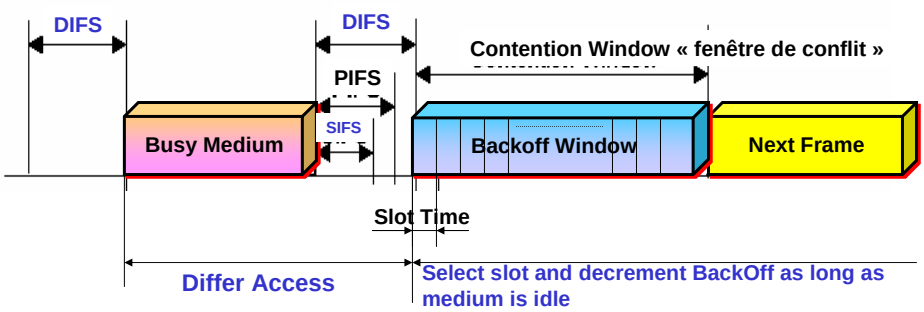
5. Quand l'intervalle d'attente devient nul et la voie est libre:

   ⇨ La station peut s'emparer du medium, et peut commencer à transmettre selon ses besoins ; une trame de données ou une trame de contrôle par exemple la trame RTS définie dans le protocole CSMA/CA

DCF : Diagramme d'écoute et d'ajournement

DCF : Distributed Coordination Function – 0 -

- Accès lorsque le medium est libre ≥ DIFS



-**Notions utilisées :**

-Silence inter trame (IFS Inter-Frame Spacing)

DIFS: Distributed IFS (50micros);

PIFS: Point IFS(30 micros);

SIFS: Short IFS (10micros)

- Fenêtre de collision CW ('Contention Window') :

-Tranche canal ('Slot Time') 20 micros

- Attente en nombre entier de tranches ('Backoff')

DCF : Distributed Coordination Function – 1 -

- **Remarque :**
- **la figure mentionne plusieurs silences inter-trames : SIFS, PIFS, DIFS :**
  - Dans un but pédagogique, la figure aurait pu mentionner seulement l'intervalle DIFS, puisque c'est celui qui est appliqué dans ce cas
  - Le silence SIFS : Short IFS est le plus court silence inter-trames, il sépare, par exemple une trame d'un acquittement positif.
  - Le silence PIFS « Point IFS) est un peu plus court que le silence DCF : est utilisé pour le protocole PCF.
    - Les trames PCF sont donc plus prioritaires que les trames DCF, par ce qu'elles prennent la voie plus tôt et force les trames DCF à passer en **mode d'ajournement.**
  - Donc, il y une hiérarchie de priorités qu'on établie entre les protocoles en établissant des délais croissants.
  - Exemple :
    - SIFS : 10 micro secondes
    - PIFS : 30 micro secondes
    - DIFS : 50 micro secondes

DCF : Distributed Coordination Function – 2 -

- Diagramme précédent – fonctionnement de l'écoute et de l'ajournement non persistant en mode DCF.

I. **Première phase :**

- **Le diagramme temporel, montre d'abord qu'une voie ne peut être acquise en mode DCF que s'elle est libre pendant un intervalle au moins égale à DIFS (Distributed Inter Frame Space).**
  - C'est comme en Ethernet, une silence inter-trames qui délimite deux trames successives. (En Ethernet, on appelle ça l'IFG : Inter Frame Gap et il y en a qu'un seul),
  - Par contre, en WIF, on joue beaucoup sur les silences inter trames. Ici, nous sommes en DCF, et le silence est caractéristique du mode DCF, ce silence s'appelle DIFS
  - Concrètement, si une station en mode DCF, tente d'envoyer une trame et si la voie est libre pendant un DIFS, l'émission peut commencer

DCF : Distributed Coordination Function –3 -

- La figure se place dans le cas ou la voie est occupée :

1. La station considérée va appliquer alors l'algorithme d'ajournement non persistant et commence par attendre que l'émission de la trame en cours se termine.
   - Sur cette figure, set intervalle s 'appelle intervalle de medium occupé (Busy Medium)
2. A l'issu de la circulation d'une trame émise par un autre station, on va attendre obligatoirement un intervalle de **silence entre-trame** et comme on est en mode DCF, on a donc une silence du durée **DIFS.**
3. La phase d'attente (Defer Access) se termine par un l'application d'un silence DIFS :

DCF : Distributed Coordination Function – 5 -

ii. <u>Seconde phase</u> : phase de sélection de nombre de slots et décrémentation (sur la figure cette phase s'appelle Decrement Backoff as long as medium is idle) :

- Sur le principe d l'ajournement non persistant, la station qui a trouvée la voie occupée, ne peut émettre directement, elle **va rentrer dans une phase d'attente aléatoire définie par l'algorithme de retard binaire.**
- La version de retard binaire présente dans WIFI reprend le même principe que celui d'Ethernet : on tire un nombre de tranches à attendre, la voie doit rester libre pendant ce temps pour que la station puisse commencer à émettre.
- **<u>N.B :</u>** Ce qui est mentionné sur la figure avec l'algorithme de retard binaire(BackOff Window ou contention window (CW) ou fenêtre de conflit) c'est le nombre de slots
- SI pendant la phase de décrémentation, une trame d'une autre station est transmise, alors :
  - ⇔ Passage en mode différence : Defer Access
  - ⇔ On interrompe la décrémentation et on reprend aussi tôt que la voie devienne libre (ceci permet d'éviter un phénomène <u>de file d'attente</u> : **dernier arrivé premier servie**)

DCF : Méthode CSMA - Bilan

- **Canal radio: détection de collision difficile**
  - **CSMA/CD n'est pas utilisable**
- **Principe de CSMA dans 802.11. Le CSMA est basé sur**
  1. **L'écoute du support : Une station écoute le canal avant de transmettre**
     - Si le canal est libre pendant un temps DIFS: transmission
     - Si le canal est occupé: remettre transmission à plus tard
       - Durée d'occupation est **signalée dans les trames**
  2. **L'algorithme de Backoff**
  3. **4 types de temporisateurs : SIFS, PIFS, DIFS, EIFS**
     - **IFS** : Période d'inactivité sur le support de transmission
       - **SIFS (Short IFS),** utilisé pour séparer les transmission d'un même dialogue
       - **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
       - Permet d'instaurer un système de priorité (+ le délai est petit + l'accès est prioritaire)
  4. **L'utilisation d'acquittements positifs**
     - Chaque trame doit être acquitté après chaque transmission
       - Intervalle SIFS (< DIFS) entre la réception de la trame et l'acquittement)

Transmission d'une trame en mode DCF

« Transmission Directe »

DCF : Méthode CSMA / Transmission Directe

- **Exemple :Transmission A ⇒ AP ⇒ B**

✓ **Chaque trajet est acquitté**

✓ **Le point d'accès n'a pas de priorité**

- **Il est possible qu'une autre station gagne l'accès au canal avant lui**
- **Dans ce cas, le point d'accès va transmettre la trame plus tard**

1. 802.11 CSMA : Emetteur :

- **Si (le canal est libre pendant DIFS sec) alors**

  transmission de la trame entière (pas de détection de collision)

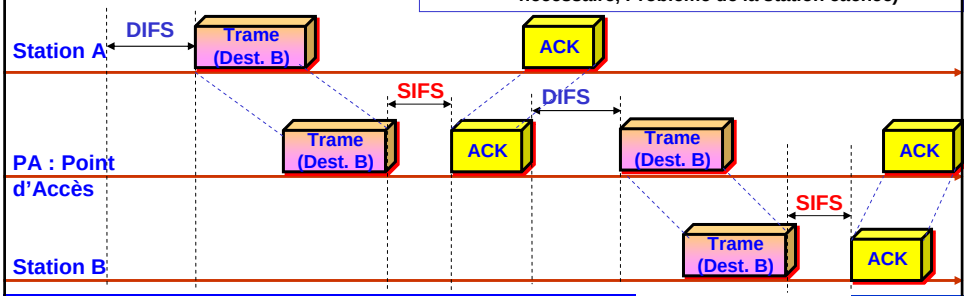
- **Si (le support est occupé) alors**

  Binary Backoff

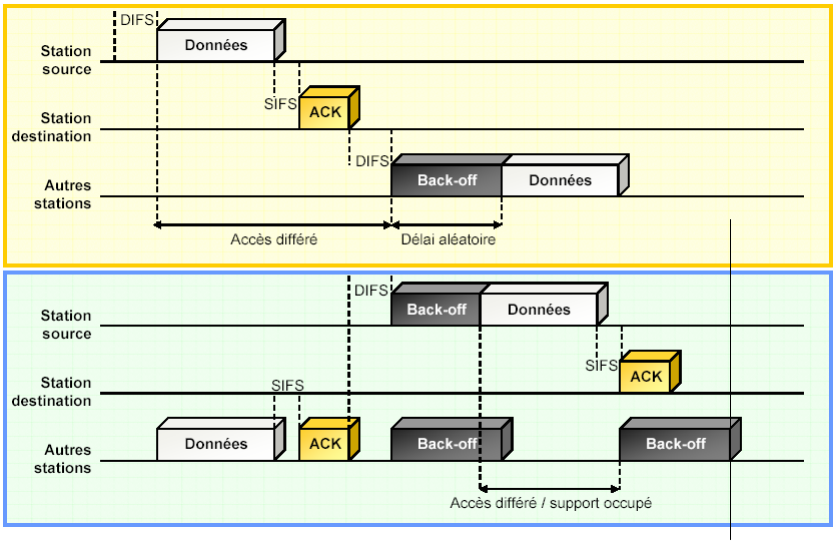
2. 802.11 CSMA : Récepteur

- **Si (la réception est correcte) alors**

  transmission d'un ACK après SIFS sec. (ACK nécessaire, Problème de la station cachée)



DCF : Quelques exemples de transmissions

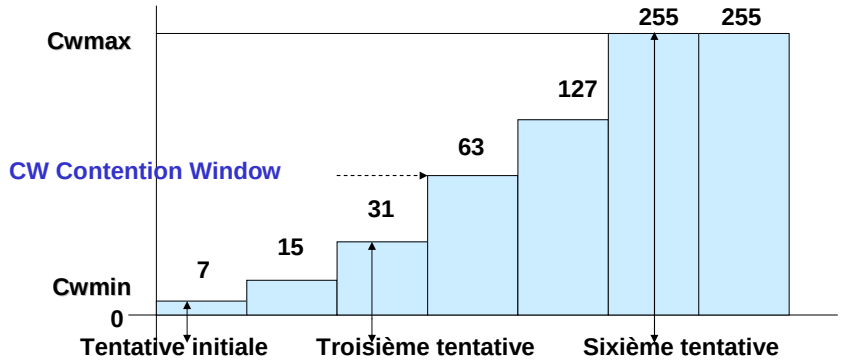


DCF : Algorithme de BackOff

Algorithme de BackOf f- objectif-

- Son but est de définir la durée d'attente aléatoire d'une station
  - ⇨ quand elle rencontre une collision.
  - ⇨ en plus que cette attente sert dans le cadre de l'ajournement non persistante lorsqu'une station constate que la voie est occupée
- Rappel :
  - **Le temps d'attente est mesuré en nombre entier de slots (slot time : sert à discrétiser le temps sur la voie de communication pour que une collision ne puisse prendre place à n'importe quel moment, mais seulement sur des instants qui sont des multiples entiers d'une valeur)**
  - **On a vu en Ethernet, qu'on augment ainsi considérablement l'efficacité de de protocole en compétition**

Algorithme de BackOff – 1 -



$$T_{backoff}(i) = random(0, CW_i).TimeSlot$$

$$CW_i = 2^{k+i} - 1$$

Attente = Random(0, CW) * ST (Backoff Time).

Random = Entier aléatoire uniformément distribué sur [0,CW].

CWi = Entier entre CWmin et CWmax qui double après chaque collision.

SlotTime = Valeur caractéristique du niveau physique (Slot Time).

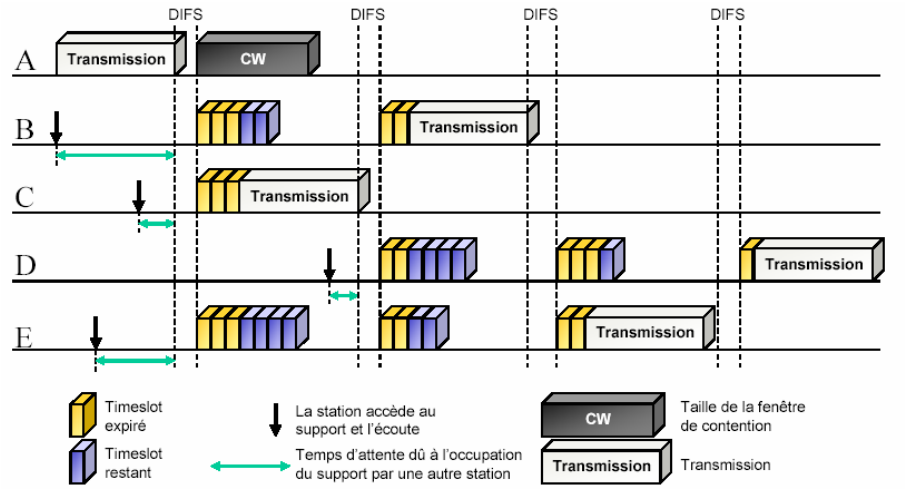
802.11a et g : CWmin =15, CWmax=1023; **802.11b** : CWmin n=31, CWmax =1023

DCF : Algorithme de BackOff - 2 -

- **But : Permet de résoudre le problème de l'accès au support physique lorsque plusieurs stations veulent transmettre des données en même temps :**
- **Fonctionnement :**
  1. **Temps découpé en TimeSlots**
  2. **Fenêtre de contention : CW (CWmin ≤ CW ≤ CWmax)**
  3. **Une station écoute le support avant toute tentative de transmission**
     - Si le support est libre après un **DIFS** : transmission
     - Sinon, calcul un temporisateur selon la formule : **TBackOff= TimeSlot * Random(0,CW)**
     - Chaque fois que le support est libre, **TbackOFF** est décrémenté de **1.**
     - Dès que **TBACKOFF** atteint la valeur **0**, la trame est émise
  4. **Il y a une collision lorsque :**
     - ↗ Deux stations ont **la même valeur** du temporisateur
     - ↗ Un **ACK** n'est pas reçu par l'émetteur
     - A chaque collision, la taille de la fenêtre de contention (CW est doublée)

DCF : Algorithme de BackOff

❑ **Exemple : Transmission Directe**



DCF : Algorithme de BackOff

- **Remarques:**
  1. **Similaire au Backoff exponentiel d'Ethernet**
  2. **• Mais: il est utilisé**
     1. **quand le canal est occupé lors de l'écoute**
     2. **après une transmission réussie**
     3. **après chaque retransmission**
        - Pas de garantie de délai minimal
        - Complique la prise en charge d'applications temps réel telles que la voix ou la vidéo.
  3. **• Résultat**
     1. **Évite les collisions quand le canal se libère**
     2. **Empêche une station de monopoliser le canal**
     3. **Toutes les stations ont la même priorité d'accéder le canal**
     4. **Pas de qualité de service**

Collision Avoidance (CA)

- **Problème de la station cachée (Faiblesses du CA)**
  - **Collisions toujours possibles**
    1. **Deux stations atteignent simultanément TemporisateurBack-off = 0**
    2. **Problème de la station cachée**

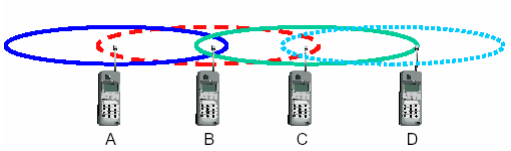
1. Terminal caché :

a. **A envoie à B, C ne peut pas recevoir A**

b. **C veut envoyer à B, C croit le support libre**

c. **collision à B, A n'entends pas la collision**

d. **A est "caché" pour C**



- **Conclusion : 2 stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station**
  - **peuvent entendre l'activité de cet AP**
  - **ne peuvent pas s'entendre l'une l'autre du fait que la distance entre les 2 est trop grande ou qu'un obstacle les empêche de communiquer entre elles**

Ecoute du support (1)

- **Solution : Réservation du canal peut**
  - **Éviter le problème de la station caché**
  - **Réduire la durée de collisions**
- **Mise en pratique par le mécanisme de RTS / CTS**
- **Ecoute du support :**
  - **Les terminaux d'un même BSS peuvent écouter l'activité de toute les stations se trouvant dans le même BSS**
  - **Lorsqu'une station envoie une trame**
    - les autres stations mettent à jour un timer appelée **NAV (Network Allocation Vector) (⇔ écoute virtuelle)**
    - Le NAV permet de retarder toutes les transmissions prévues
    - **NAV** calculé par rapport à l'information située dans le **champ durée de vie ou TTL contenu dans les trames envoyées**

Ecoute du support (2)

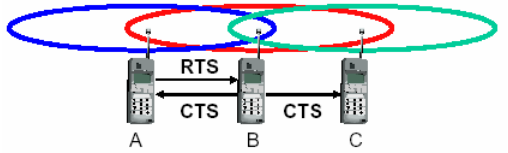
- **Ecoute du support ? :**
  - Couche physique avec PCS : Physical Carrier Sense
    - Le PCS détecte la présence d'autres stations 802.11
      - en analysant toutes les trames passant sur le support hertzien
      - en détectant l'activité sur le support grâce à la puissance relative du signal des autres stations
    - Couche MAC avec VCS
      - Virtual Carrier Sense (⇔ NAV)

Mécanisme de Réservation

- **La réservation avec RTS et CTS :**
  1. **Message RTS (*request-to-send*):**
     - Bref message envoyé par la source pour indiquer **l'intention d'émettre**
  2. **Message CTS (*clear-to-send*)**
     - Bref message envoyé par la destination comme réponse au message RTS
     - Reçu par tous les nœuds dans la couverture du récepteur
     - Indique la durée de **la 'réservation'**
  3. **Réception de RTS:**
     - Silence pendant la transmission de CTS + trame suivante
  4. **Réception de CTS:**
     - Silence pendant la transmission suivante
  5. **RTS / CTS paquets courts pour éviter au max des collisions**

Mécanisme de Réservation

- La réservation avec RTS et CTS permet de résoudre le problème des stations cachées
  - A→ B C →B
  - A envoie RTS
  - C attend après avoir entendu CTS de B



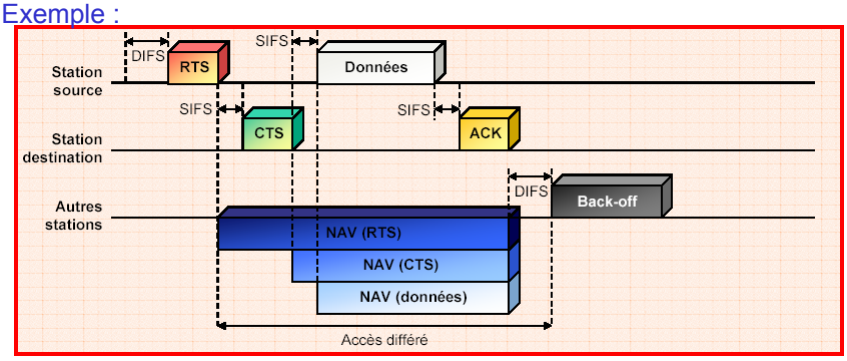
Transmission d'une trame en mode DCF

Echange RTS - CTS « protocole CSMA / CA »

« Protocole à évitement de collision »

Echange RTS - CTS « protocole CSMA / CA »

- Exemple :



-**Echange RTS/ CTS (Request To Send/Clear To Send) pour une trame données.**

-Envoi de RTS avec durée de réservation

-Acquis via CTS après SIFS (avec durée de réservation)

- **Utilisation des silences courts SIFS (l'échange est prioritaire)**
- **Acquittement positif ACK obligatoire.**
- **Mécanisme d'écoute virtuelle (indicateur NAV pour une autre station).**

-Les autres stations connaissent la durée distribuée via RTS and CTS

Protocole PCF (Point Coordination Function)

Le niveau liaison WIFI : PCF « Point Coordination Function »-0-

1. **Fonctionnement en scrutation (‘protocole du type polling’) par le PC (‘Point Coordinator’).**
2. **Une station émet si elle est autorisée par le PC**.
   - Pour les besoins du **protocole PCF,** une trame particulière est utilisée par cet arbitre, par exemple, une trame baptisée **BEACON** ouvre une période de fonctionnement en mode PCF.
   - Les trames de données émises par l’arbitre peuvent contenir des directives de scrutation POLL demandant à une station si elle a des informations à transmettre
3. **Le PC sélectionne une station en plaçant son adresse dans la trame.**
   - Le PC fonctionne comme un commutateur, c’est-à-dire pour émettre une trame d’une station vers une autre station, l’émetteur commence par cette trame au PC, puis le PC la retransmet à son destinataire
4. **Les trames sont acquittées. Si l’acquittement ne revient pas, le PC ou la station effectuent la retransmission.**
   - Le protocole PCF, utilise aussi un acquittement positif pour faire le contrôle d’erreur

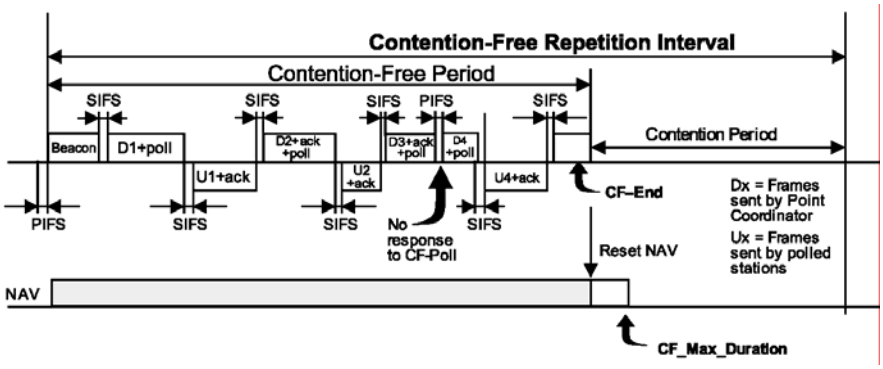
Le niveau liaison WIFI : PCF « Point Coordination Function » »-1-

5. **PCF a plutôt été destiné à des échanges à qualité de service**
   - PCF supporte le mode de scrutation, il est assez facile de lui faire supporter des échanges de qualité de service (échange en respectant des contraintes sur les temps de réponse ou sur les gigues, il suffit de régler les durées des cycles de scrutation et le temps de transmission attribué à chaque station.

Le niveau liaison WIFI : PCF « Point Coordination Function » -0-

❑ **Exemple de transfert en mode PCF**

- Intervalle de répétition: mode PCF (contention free) puis DCF.
- PIFS puis trame Beacon : ouverture d'un intervalle sans collision (mode PCF)
- CF-End fin de séquence Poll Ack sous contrôle du PC.



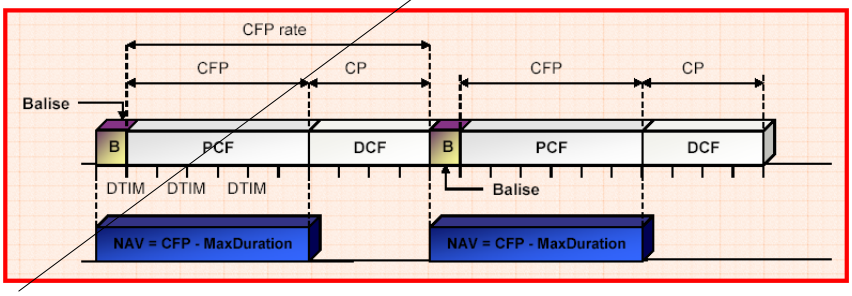
Le niveau liaison WIFI : PCF « Point Coordination Function »

❑ PCF

- **Transfert temps-réel (voix, vidéo), service de priorité**
- **l 'AP (Access Point : point d 'accès) prend le contrôle du support et choisit les stations qui peuvent transmettre : polling**

❑ **Contention**

- **l 'AP définit un PC (Point Coordination) avec 2 périodes :**
  - **➔CP (Contention Period) : période de temps avec contention et DCF**
  - **➔CFP (Contention Free Period) : période de temps sans contention et PCF**



La Couche Liaison : Autres fonctions

- Fragmentation – Réassembalge

Fragmentation et réassemblage –1-

- **Fragmentation?**
  - Découpage d'une trame longue en plusieurs fragments
    - Diminue les données à retransmettre en cas d'erreur bit
    - N. B : Taux d 'erreur pour liaison radio est supérieur à celui des liaisons filaires : nécessité de transmettre de petits paquets
- **Fragmentation, Qui ?:**
  - D'une trame de donnée MSDU (MAC service Data Unit)
  - Ou d 'une trame de gestion MMPDU (MAC Mangagement Protocol Data Unit) en plusieurs trames PDU (MAC Protocol Data Unit)
- **Fragmentation : Principe :**
  - Les fragments sont transmis de manière séquentielle
  - Le support est libéré après :
    - Soit à la fin de la transmission de tous les fragments
    - soit suite à une erreur de transmission d'un fragment
  - Après une erreur
    - La station regagne l'accès au canal
    - Retransmission à partir de la trame perdue

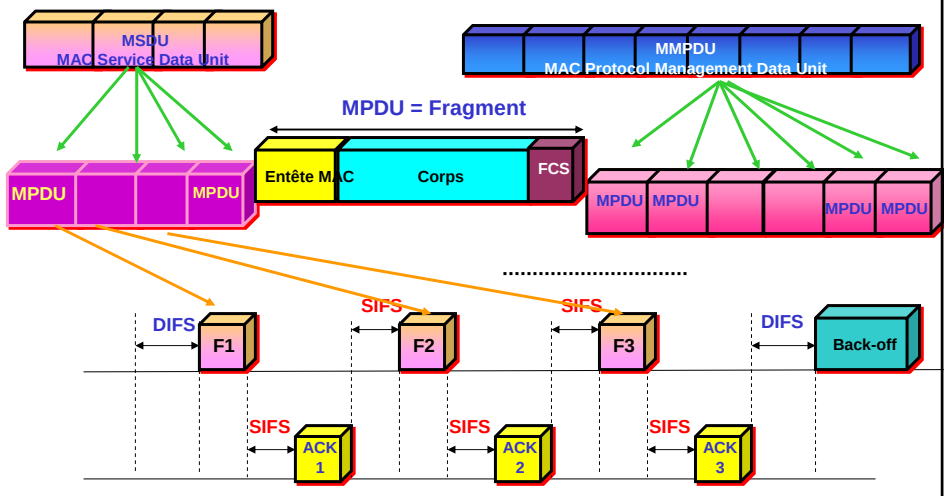
Fragmentation et réassemblage –2-

- **Fragmentation Quand :**
  - si taille > valeur seuil
    - fragments envoyés de manière séquentielle
    - La destination acquitte chaque fragment
    - Support libéré après transmission de tous les fragments
- **Utilisation du RTS/CTS**
  - Seul le premier fragment utilise les trames RTS/CTS
  - Le NAV doit être maintenu à jour alors à chaque nouveau fragment

Fragmentation et réassemblage – 3 -

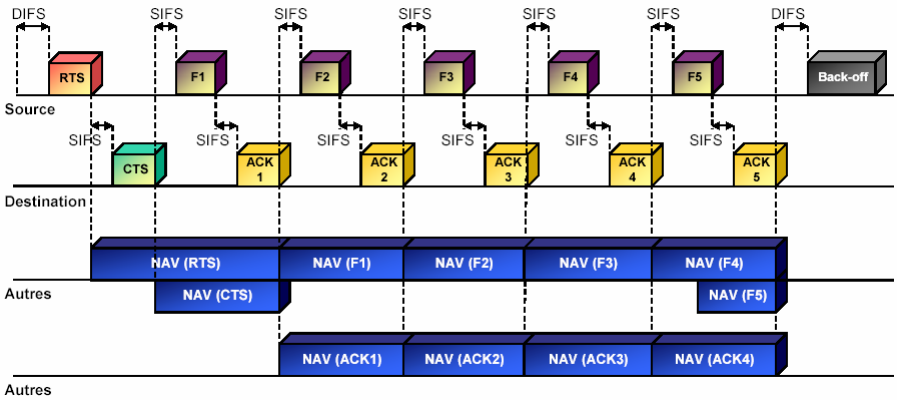
- Mécanisme d 'émission d 'une trame fragmentée

Fragmentation d'une trame de donnée **Fragmentation d'une trame de gestion**



Fragmentation et réassemblage –4-

- Exemple : Emission d 'une trame fragmentée avec réservation du support



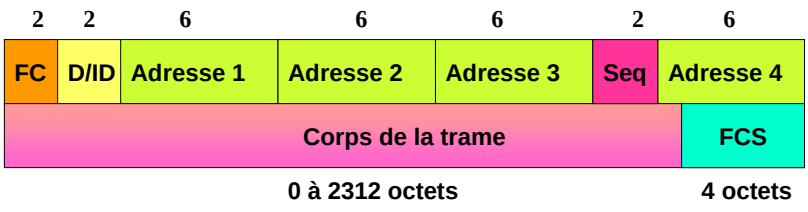
Fragmentation et réassemblage –5-

- Remarque :
  - **Dans la trame, plusieurs informations « dans deux champs » sont utilisées pour permettre le réassemblage des fragments par la station destination :**
    1. **Sequence Control : permet le réassemblage de la trame grâce à :**
       A. **Sequence number :**
          - **chaque fragment issu d 'une même trame possède le même numéro de séquence**
       B. **Fragment Number :**
          - **chaque fragment d 'une même trame se voit attribuer un numéro de fragment, à partir de zéro, incrémenté pour chaque nouveau fragment**
    2. **More Fragment : permet d 'indiquer si d 'autres fragments suivent : égale à zéro si le fragment en cours est le dernier fragment.**

Format de Trames 802.11

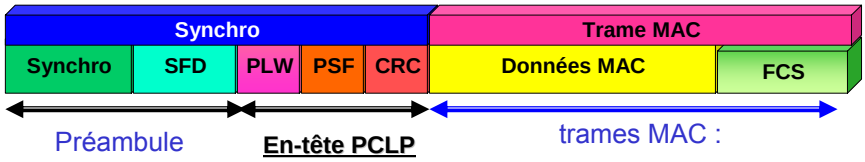
IEEE 802.11 : Les trames

- La norme dispose de trois types de trames MAC :
  1. Trames de données : transmission des données
  2. Trames de contrôles : contrôle d'accès su support (RTS, CTS, ACK, etc…)
  3. Trames de gestion : association, ré-association, synchronisation, authentification
- Une trame du niveau MAC possède la structure suivante :



IEEE 802.11 : Les trames MAC –1-

- **Cette trame MAC est encapsulée dans une trame « au niveau physique » qui a la structure suivante :**



A. Préambule :

- **C'est la première capsule de la : elle permet d'opérer la synchronisation physique du récepteur**

1. Synch :

- **Ce champ sert à la synchronisation du récepteur**
- **c'est une séquence 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.**

2. SFD : Start Frame Delimiter

- **Un délimiteur de début de la trame**
- **Permet au récepteur de localiser le début de la trame**
- **Ce champ est sur deux octets (16 bits)**

IEEE 802.11 : Les trames MAC –1-

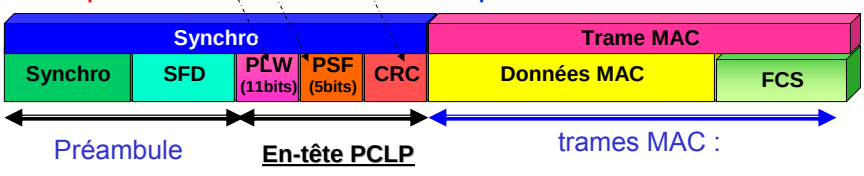
B. En-tête PCLP (Trame 802.11) : C'est la seconde capsule de la trame

- **« PLCP : infos logiques utilisées par la couche physique pour décoder la trame »**
- **Comme la norme possède plusieurs niveaux physique, cette seconde capsule permet d'adapter le niveau physique à la couche MAC:**

1. Longueur de mot du PLCP_PDU (PLW) : 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. (paramètre passé par la couche MAC)

2. Fanion de signalisation PLCP (PSF) : il contient seulement l'information de taux de débit (vitesse de transmission)

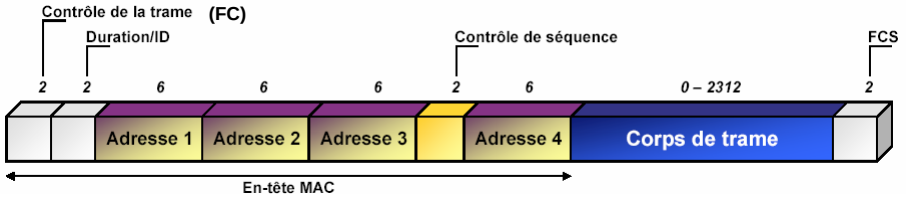
3. Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC 16 bits.



IEEE 802.11 : Les trames MAC –1-

C. Trame Données MAC (Trame 802.11)

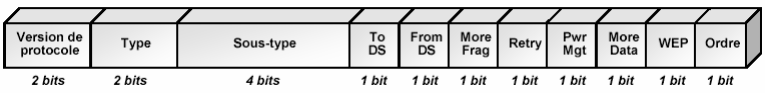
- **La figure suivante montre le format général de la trame MAC,**



1. **FC (Frame Control): version de protocole, type de trame …etc.**
2. **Durée / ID : Durée d'utilisation du canal de transmission.**
3. **Champs adresses : Une trame peut contenir jusqu'à 4 adresses (mode ad'hoc adresse 1 destination et adresse 2 source).**
4. **Contrôle de séquence : pour la fragmentation (numéro de fragment sur quatre bits et numéro de séquence de la trame sur douze bits).**
5. **Corps de la trame : charge utile d'au maximum 2312 octets.**
6. **FCS (Field Check Sequence): somme de contrôle de niveau MAC : x32+ x26+ x22+ x16+ x 2+ x11+ x10+ x8+ x7+ x5+ x4+ x2 + x+ 1**

IEEE 802.11 : Les trames MAC –2-

1. Le champ « contrôle de trame » : (détail des deux octets de contrôle) situé au début de la trame MAC



- Version de protocole : actuellement fixé à 0
- Type et sous-type : 3 types de trames, plusieurs sous-types
- ToDS et From DS : trame envoyée vers le ou provient le système de distribution « du destinataire »
- More Fragrments
  - = 1 si trame fragmentée et ce n'est pas le dernier fragment
  - = 0 si trame non fragmentée ou dernier fragment
- Retry =1 si retransmission
- Power mangement : mode économie d'énergie (=1) ou actif (=0)
- More data : trames présentes en mémoire tampon du point d'accès et ont en attente de délivrance
- WEP : trame chiffrée ou non (trame donnée ou gestion /authentification)
- Order : classe de service strictement ordonnée (Stricktly Ordered Service Class)

IEEE 802.11 : Les trames MAC –3-

2. Le champ « Duration ID » :

- **Deux sens différents :**
  - Certains trames de contrôle : identifiant de la station (AID : Association Identity)
  - Toutes les autres trames : valeur de durée de vie utilisée pour le calcul du NAV : varie de 0 à 32767 (µs)
- **Les champs « adresse »**
  - Toutes de longueur 6 octets
  - Même format que les adresses IEEE 802 MAC
  - Composée de quatre parties :
    - Individual/Group (I/G) : premier bit : adresse individuelle ou de groupe
    - Universal/Local (U/L) : deuxième bit : adresse locale ou universelle
    - Organizationaly Unique Identifier : 22 bits : assignés par l'IEEE
    - Numéro de série : 24 bits : généralement défini par le constructeur

IEEE 802.11 : Les trames MAC –4-

3. Le champ « contrôle de séquence »
   - Numéro de séquence (12 bits) :
     - attribué à chaque trame ; initialisé à 0 puis incrémenté pour chaque nouvelle
   - Numéro de fragment (4 bits) :
     - initialisé à 0 puis incrémenté pour chaque nouveau fragment

4. **Les données et le corps de la trame :**
   - Taille minimum nulle (trames de gestion ou de contrôle)
   - Taille maximale : 2312 (pas de taille min ⇔ La détection de collision ne le nécessite pas)
   - Taille plus importante si chiffrée par WEP
   - Initialization Vector (IV)
   - Integrity Check Value (ICV)

5. **Le champs FCS (Frame Check Sequence)**
   - **CRC sur 32 bits pour contrôler l'intégrité des trames**

Cas de transmission WIFI

rôles des zones adresse dans une trame WIFI

Cas de transmission WIFI

- **Cas 1 (mode ad'hoc):**
  - **Transmission directe entre deux stations (dans un IBSS). (⇔ deux adresses)**
- **Cas 2 (mode infrastructure) :**
  - **Transmission d'une station vers le point d'accès (qui doit ensuite relayer vers une station destinataire) (trois adresses sont nécessaires)**
- **Cas 3 (mode infrastructure) :**
  - **Transmission par un point d'accès d'une trame vers son destinataire.(trois adresses sont nécessaires)**
- **Cas 4 (mode infrastructure avec réseau de distribution sans fil):**
  - **Transmission intermédiaire d'une trame d'un point d'accès à un autre point d'accès. (quatre adresses sont nécessaires)**
  - **Relayage via les points d'accès**

Rôle des adresses MAC

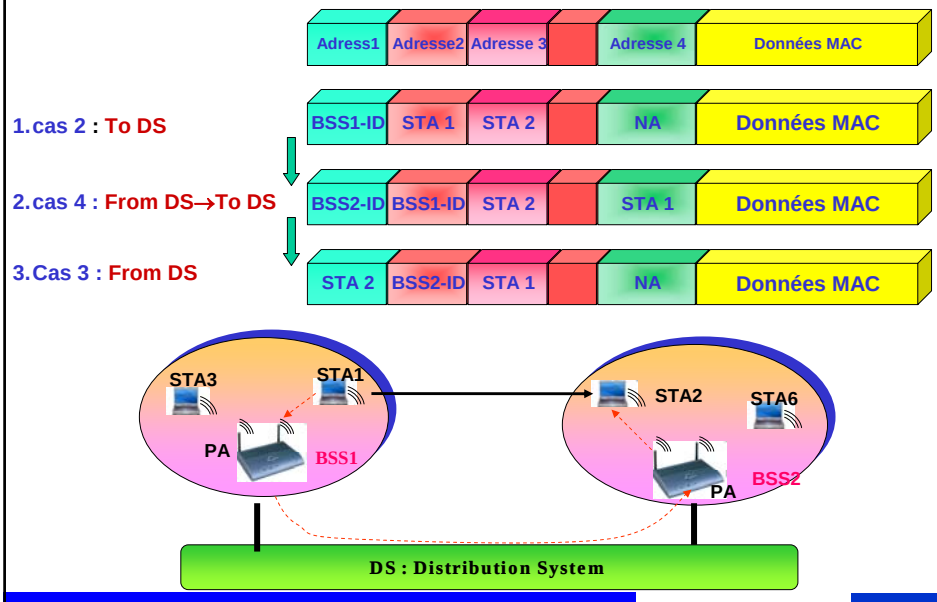
Rôle des adresses MAC « Les champs Adresses »

- **Deux types d'adresse de groupe :**
  - Adresse broadcast : l'ensemble des stations d'un réseau, 48 bits à 1
  - Adresse multicast : groupe de stations en nombre fini
- **5 types d'adresses :**
  - BSSID (Basic Service Set Identifier)
  - DA : (Destination Address) : : destination de la trame; indiv, ou groupe
  - SA (Source Address) : Source de la trame ; toujours individuelle
  - RA (Receiver Address) : Destination de données; indiv, ou groupe
  - TA (Transmitter Address) : source de données ; toujours individuelle)
  - N/A : Non applicable.

Cas	To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
1	0	0	DA	SA	BSSID	N/A
2	1	0	BSSID	SA	DA	N/A
3	0	1	DA	BSSID	SA	N/A
4	1	1	RA	TA	DA	SA

Rôle des adresses MAC

- **UN ECHANGE CLASSIQUE :**

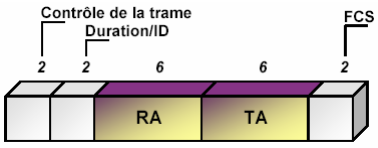


IEEE 802.11 : Les trames de contrôle

IEEE 802.11 : Les trames de contrôle –1-

- **Trame RTS**

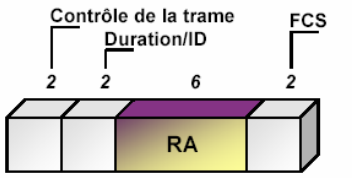
1. **RA est l'adresse du récepteur de la prochaine trame de données ou de gestion.**
2. **TA est l'adresse de la station qui transmet la trame RTS.**
3. **La valeur de la durée est :**
   - **le temps, en microsecondes, nécessaire à la transmission de la trame de gestion ou de données suivante,**
  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



IEEE 802.11 : Les trames de contrôle –2-

- **Trame CTS**

1. **RA est l'adresse du récepteur de la trame CTS, directement copiée du champ TA de la trame RTS.**

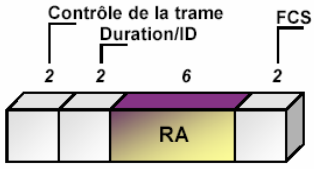


2. **La valeur de la durée est la valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame RTS et d'un intervalle SIFS.**

IEEE 802.11 : Les trames de contrôle –3-

- **Trame ACK :**

1. **RA est le champ directement copié du champ Adresse 2 de la trame précédent cette trame ACK.**

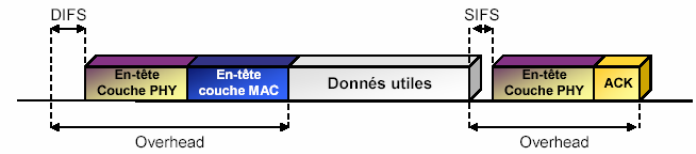


2. **Deux cas :**
   a. **Le bit More Fragment dans le champs de contrôle de la trame précédente = 0, la valeur de la durée est mise à 0.**
   b. **Sinon, c'est la valeur du champ durée précédent, moins le temps, en microsecondes, demandé pour transmettre la trame ACK et l'intervalle SIFS.**

Variation de débit

Variation du Débit –1-

- **Débit compris entre 1 et 11 Mbits/s**
  - **11 Mbits/s donne un débit utile de 6 Mbits/s soit 0,75 Mo/s**
  - **Différence due :**
    - ⇨ **aux en-têtes des trames utilisées**
    - ⇨ **à certains mécanismes de fiabilisation de la transmission**
    - ⇨ **une part importante du débit sert à la gestion de la transmission**



- **L 'Ovrhead engendré est plus important que les données elles-mêmes**

Variation du Débit –2-

- **Exemple : Débits effectifs pour un datagramme IP**

Standard	Débit max (fourni par la couche PHY)	Débit Max Effective	
		Paquet 64 Octet	Paquet 1500 Octets
IEEE 802.11 b	11 Mb/s	0.8 Mb/S	7.1 Mb/s
IEEE 802.11 g/a	54 Mb/S	1.4 Mb/S	20 Mb/s

- **Débit max util ≤ 50% débit nominal**
- **Exemple : IEEE 802.11g:**
  - **UDP ≤ 28 Mbit/s**
  - **TCP ≤ 23 Mbit/s**

Variation du Débit –3 -

- **Variable Rate Shiffting :**
  - ➔ **Permet de faire varier le débit d 'une station en fonction de la qualité de la liaison**
  - ➔ **permet à toutes les stations d 'avoir un accès, même minimal, au réseau**
  - ➔ **débits possibles : 11 / 5,5 / 2 / 1 Mbits/s**

Vitesse	Portée à l'intérieur (m)	Portée à l'extérieur (m)
11	50	200
5.5	75	300
2	100	400
1	150	500

Accès au réseau

Initialisation / Accès au Réseau

- **Phase 1 :**
  - **Allumer station → Phase de découverte**
    - Découvrir l'AP et / ou les autres stations
  - **Présence détectée → rejoindre le réseau**
    - Service Set ID (SSID) : détection du nom du réseau de connexion
    - Synchronisation
    - Récupération des paramètres de PHY
- **Phase 2 :**
  - **Négocier la connexion**
    1. Authentification (⇔ Requête d'authentification)
    2. Association (⇔ Requête d'association)

Phases de découverte du réseaux

- **Phase d'écoute**
  - Écoute passive / écoute active

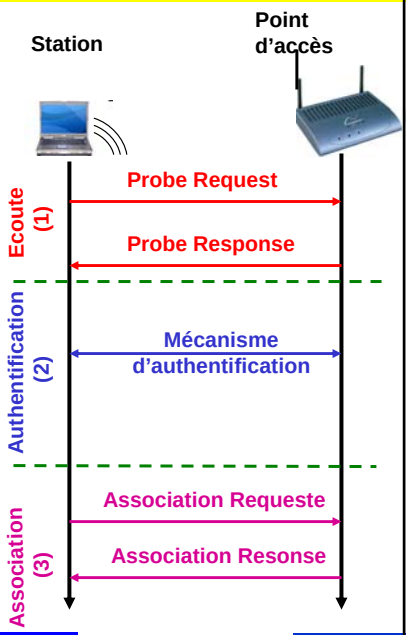
  → **Ecoute passive**
  - ✓ La station attend de recevoir une trame de balise (Beacon)
  - ✓ A la réception de Beacon, prendre les paramètres (SSID et les autres)

  → **Ecoute active**
  - ✓ La station envoie directement une requête d'association (Probe Request Frame)
  - ✓ Attendre la réponse de l'AP ou des autres stations

Service Set Identifier (SSID) : Sélection du réseau WLAN

Mécanisme d'Association

- **SSID : Seul mécanisme de sécurité obligatoire**
  - Définition du nom du réseau sur lequel on veut se connecter :
  - *authentification et association*
  - Le SSID n'est pas un mécanisme de sécurité
    - Transmie en clair dans les requêtes 'probe'.



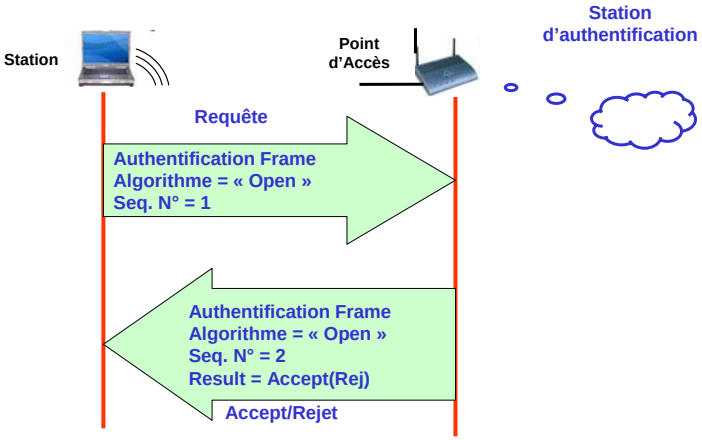
Authentification

- **Deux mécanismes d'authentification:**

1. Authentification ouverte « Open System Authentification » : mécanisme par défaut

Aucune authentification explicite

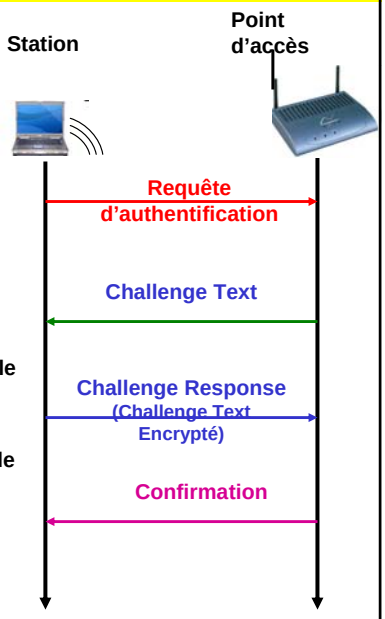
N.B : L'authentification Open System, permet à n'importe quels appareils sans fil de communiquer entre eux.



Authentification

2. Authentification à clé partagée « Shared Key Authentification » :

- **utilise la clé de réseau WEP (Wired Equivalent Privacy) pour authentifier le client**
- **Principe :**
  - ✓ **l'AP envoie au client sans fil un challenge en texte clair ;**
  - ✓ **Le client utilise la clé de réseau pour crypter le challenge puis le renvoie à l'AP.**
  - ✓ **Si le client utilise une clé incorrecte, ou pas de clé, l'AP refuse l'accès à l'utilisateur.**



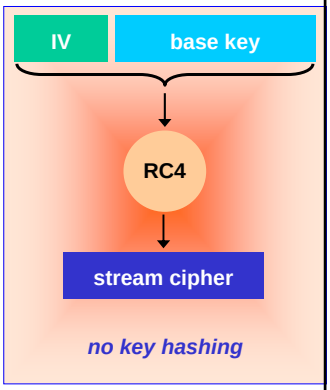
Sécurité Wireless LAN : Filtrage des adresse MAC

- **ACL (Access Control List) :**
  - **Liste maintenue par le point d'accès**
  - **Contient les adresses MAC autorisées à se connecter à cet AP**
  - **Optionnelle et peu utilisée car peu fiable**

- **Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC).**
- **Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil.**
- **En activant ce MAC Address Filtering (Filtrage des adresses MAC), même si cette précaution est un peu contraignante, cela permet de limiter l'accès au réseau à un certain nombre de machines.**
- **En contrepartie cela ne résout pas le problème de la confidentialité des échanges.**

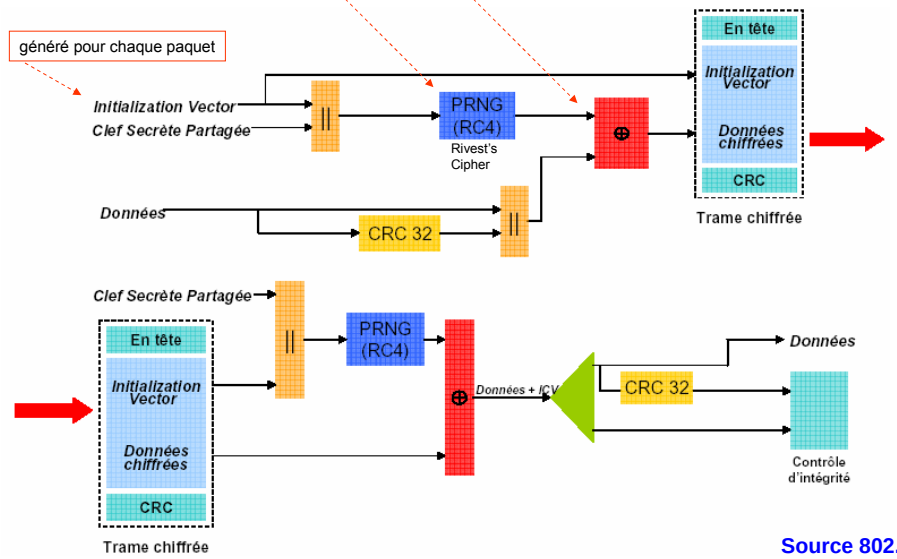
WEP : Wired Equivalent Privacy

- **Cryptage dans WEP : Solution de chiffrement choisie par le 802.11**
  - **SES OBJECTIFS :**
    - Confidentialité.
    - Contrôle d'accès.
    - Intégrité.
  - **L'UTILISATION DU WEP EST UNE OPTION DU 802.11.**
  - **Basé sur un algorythme RC4**
  - **Chiffrement 40 bits optionnel (plusieurs constructeurs offrent du 128 bits)**
    - Pour être conforme Wi-Fi™ il faut supporter le 40 bits
  - **Le groupe de travail 802.11i est en train de définir une amélioration du WEP pour répondre aux problèmes de sécurité rencontrés actuellement**
    - Interception de trames cryptées avec la même clé permettrait de deviner facilement le contenu



Cryptage dans WEP

Chiffrement WEP RC4(v, k) C=(P, c(P)) ⊕ RC4(v, k).



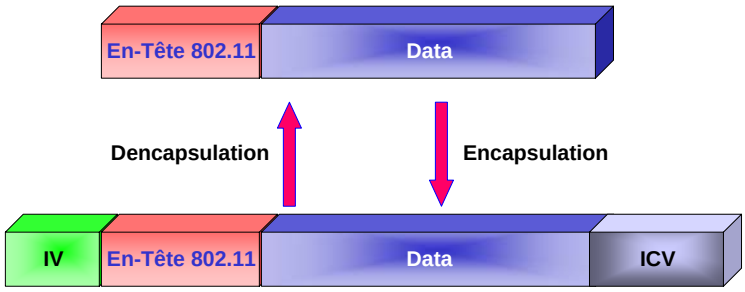
Source 802.11

Cryptage dans WEP

- ALGORITHMES UTILISES :
  - RC4 et CRC-32bit.
- PARAMETRES
  - Plaintext : P.
  - Ciphertext : C.
  - Clé partagée: k (40 bits) [Clé de cryptage]
  - Un vecteur d'initialisation :IV (généré pour chaque paquet): v(24bits)
- PROCESSUS
  - Calculer CRC(P): c(P)
  - Lier P et c(P)
  - Calculer RC4(v, k) :
    - Concaténation de la clé de cryptage et du vecteur d'initialisation
  - Résultat : C=(P, c(P)) ⊕ RC4(v, k).

WEP : Wired Equivalent Privacy

⇨ ENCAPSULATION WEP



ICV : Integrity Check Value

IV : Initialisation Vector : 1 pour chaque paquet

Faiblesses des solutions actuelles

■ **WIFI comporte de nombreuses failles dans toutes ses composantes :**

1.SSID (Service Set ID) :

- Transmis en clair par l'AP
- En mode ad-hoc, le SSID est systématiquement transmis en clair
- Le SSID est transmis en clair pendant l'association
- Utilisation du SSID par défaut, configuré par les constructeurs

2.ACL

- Optionnel, donc peu souvent utilisé
- Repose sur l'identification de l'adresse MAC
- Il **suffit de sniffer** le réseau puis copier une adresse MAC

Failles de sécurité de WEP

1. Gestion des clés (tous les utilisateurs ont la même clé).

- le WEP ne définit aucun moyen pour gérer les clés de chiffrement.
- C'est à l'administrateur de WLAN de créer les clés, de les distribuer, de les archiver/stocker d'une manière protégée,

2. Récupération de la clé secrète

- Comme les clés WEP sont partagées, la confidentialité de la communication n'est pas assurée.
  - **Système de génération de la clef :** le vecteur est souvent initialisé à zéro à chaque nouvelle transmission
  - **Le vecteur d'initialisation représente les premiers octets de la clé RC4**
    - Si l'on connaît les premiers octets de la clé RC4, on peut trouver le prochain octet à partir du premier octet de la séquence générée par RC4

1. **Le nombre de *keystream* est limité à 2^24 clés.** *Un pirate peut facilement générer des trames, enregistrer leur forme chiffrée puis déduire et stocker les KeyStream identifié par leur IV*

Failles de sécurité de WEP

1. **Modification clandestine du message crypté**
   - **Le code CRC**, prévu pour l'intégrité du message, est linéaire
   - Si l'intrus modifie le message crypté, **il peut calculer un CRC correct,** sans savoir déchiffrer le message

2. **Et beaucoup d'autres...**

Sécurité Wireless LAN : *Les solutions actuelles*

- **Attente du standard 802.11i**
- **Solutions pré-standard**
  - ⇨ Chiffrement WEP 128 bits
  - ⇨ Filtrage sur Adresses MAC
  - ⇨ Authentification par Login/Password : 802.1x / LEAP (radius)
- **WiFi Protected Acces (WPA)**
  - ⇨ Le successeur de WEP avec **génération dynamique des clés**
  - ⇨ Utilise TKIP (Temporal Key Integrity protocol) comme méthode de chiffrement
- **Centralized Security & Management (802.1x)**
  - ⇨ **Authentification radius EAP-MD5** avec support de 802.1x
  - ⇨ **Gestion des certificats** en utilisant un serveur radius **EAP (** Extensible Authentication Protocol) **–TLS** (Transport Layer Security)
- **802.11i WiFi Protected Access**
  - ⇨ Le standard de sécurité des réseaux radio
  - ⇨ Base sur WPA
  - ⇨ Utilise AES (Advanced Encryption Standard) comme méthode de chiffrement
- **Utilisation de réseaux VPN (Virtual Private Network)**

Sécurité Wireless LAN : *Résumé*

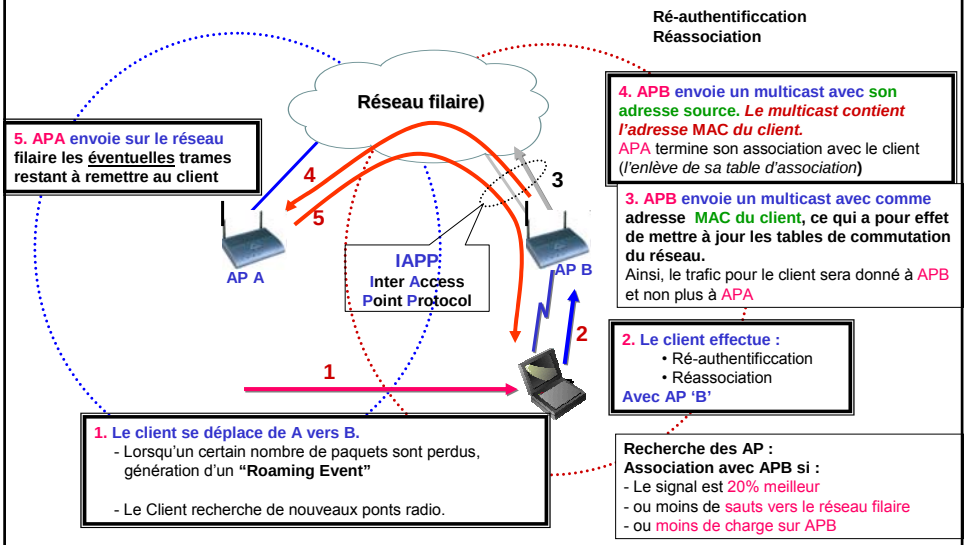
Aucune Sécurité	Sécurité Basic	Sécurité Avancée	Sécurité Maximale
Pas de WEP et mode broadcast	WEP Statique 40-bit, 128-bit @ MAC	Gestion dynamique des clés, Authentification mutuelle 802.1x / EAP (radius)	Sécurité VPN de bout en bout
			
Accès Public	PME Télétravailleurs	Grandes Entreprises	Utilisateurs mobiles Accès Publics

Gestion de mobilité « Roaming »

Les Handovers

- **Les Handovers**
  - Mécanisme permettant à un dispositif mobile de **changer de cellule** sans que la transmission en **cours soit interrompue**
  - Possible que si les cellules **voisines se recouvrent**
- **Phases :**
  - **Pas ou mauvaise connexion:**
  - **Scanning :**
    - Scanning de l'environnement
      - écoute passive (balises) / écoute active : envoi de probes
  - **Demande de réassociation**
    - station envoie une demande à une ou plusieurs AP(s)
  - **Réponse de réassociation**
    - **succès:** AP répond, Terminal parle avec l'AP
    - **échec:** continue scanning
  - **AP accepte la demande de réassociation** (IAPP : Inter Access Point Protocol)
    - L'AP signale la nouvelle station au **DS (Distribution System)**
    - La DS met sa base de données à jour **(i.e., adresses / routage)**
    - Typiquement, **le DS informe l'ancienne AP,** qui peut libérer ses ressources

Roaming



Qualité de service

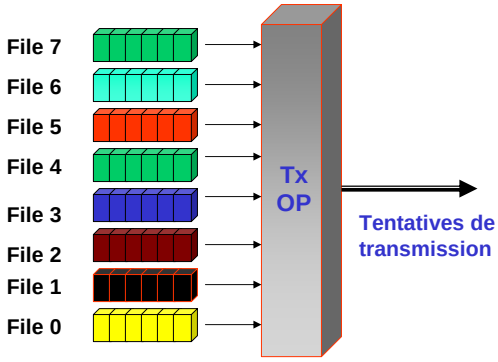
Qualité de service –1 -

- **Définition ?**
  - QoS : Garantir un délai, une gigue, une bande passante et taux de perte pour un flux donné
  - Exemple : Pour la voix, le délai maximum est de 300 ms

- **QoS dans WIFI**
  - **Pas de QoS dans Wi-Fi**
  - **802.11e**
    - Définir de nouvelles méthodes d'accès compatible avec les précédentes afin d'apporter de la QoS à Wi-Fi
    - EDCF (Extended DCF)
    - HCF (Hybrid Coordination Function)

Qualité de service –2-

1. **Accès distribué avec priorité « Gestion des priorités » : accès EDCF (Extended DCF)**
   - ➔ méthode PCF jamais utilisée car non implémentée par les fabricants
   - ➔ EDCF : évolution DCF, introduite dans l 'IEEE802.11e
   - ➔ accès au support selon le niveau de priorité de la trame
   - ➔ 8 niveaux de priorité : 8 files d 'attentes de transmission
2. **mécanisme d'accès sans contention : Transmission Opportunities « TxOP »**



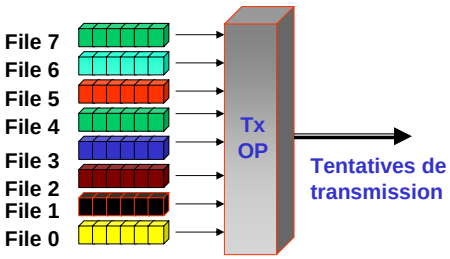
Qualité de service –3-

- **AIFS : Arbitrations IFS**
  - **utilisé de la même manière que le DIFS**
  - **valeur dynamique : varie en fonction du niveau de priorité requis**
  - **diminue les risque de collision**

- **L 'algorithme de back-off pour une statcion TCi**
  - sa valeur est dynamique également
  - Attente =random_uni(CWmin [TCi]) * Surée_Solt_Collision
  - random_uni(CWmin [TCi]) est un entier aléatoire dans l'intervalle [1, CW[TCi]+1]
- **La taille de la fenêtre de contention varie pour chaque classe de trafic**
  CWmin [TCi] ≤ CW[TCi] ≤ CWmax[TCi]
- **Calcul de CW après une collision**
  - Persistent Factor (PF)
    CWnew [TCi] =(PF x(CWold [TCi] +1)) –1
- **CWmin [TCi] , CWmax[TCi] PF[Tci] sont transmis par le point d'accès**

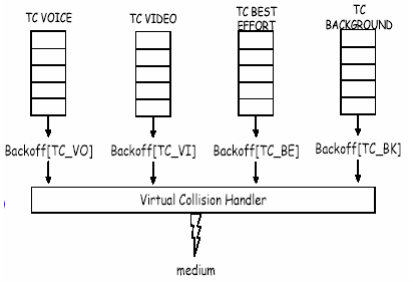
Qualité de service –4-

- **Mécanisme d'accès sans contention : Transmission Opportunities « TxOP »**
  - Le point d'accès envoie une trame du type CF_Poll à la fois dans la période sans contention et dans la période avec ocntention
  - Ces trames fournissent à la station intérrgée un créneau de transmission (TxOp : Transmission Opportunity)
  - Dans ce créneau, la station peut envoyer des trames ayant des contraintes de qualité de service



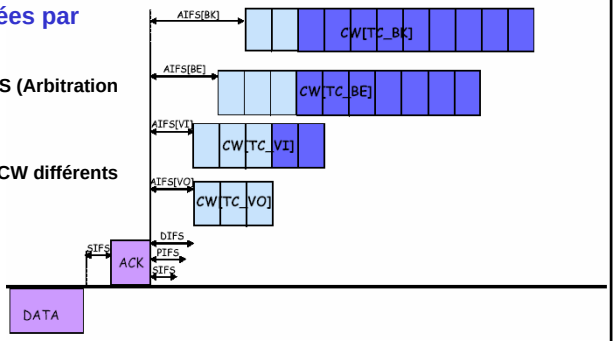
Quatre niveaux de priorité pour 4 types de trafics : TC (Traffic Categories)

1. ***TC-VO*** *pour des applications de type voix (le plus prioritaire : AIFS et CW petits)*
2. ***TC-VI*** *pour des applications vidéo,*
3. ***TC-BE*** *pour des trafics associés à une méthode d'accès de type « Best Effort »,*
4. ***TC-BK*** *pour des applications « Background » (les - prioritaires : donc l'AIFS le + grand !)*



Quatre FIFO différentes vidées par priorité croissantes

- **Le DIFS est remplacé par 4 AIFS (Arbitration IFS) de tailles croissantes**
- **- Les 4 AIFS sont associés à 4 CW différents**



ANNEXE

Réseaux Locaux Partagés WIFI
« Le niveau physique »

Normes IEEE 802.11

	802.11b	802.11a	802.11g
Bande de Fréquence	2.4 GHz	5 GHz	2.4 GHz
Disponibilité	Mondiale	US Partiellement Europe	Mondiale
Débit maximum	11 Mbps	54 Mbps	54 Mbps

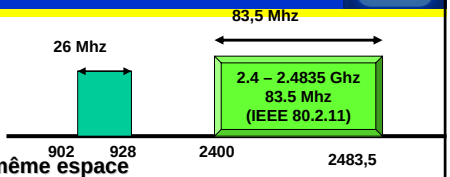
Les lois de la Radio :

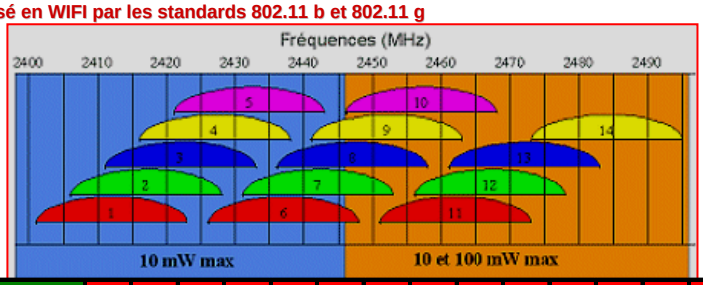
Débit = Fréquence x qualité de transmission (signal / bruit)

$$\text{Couverture} = \frac{\text{Puissance}}{\text{Fréquence}}$$

BANDE ISM (Industrial, Scientific and Medical)

- **Bande ISM**
  - Libréation de cette bande aux EU en 1985
  - Bande divisée en 14 canaux de 20 MHz
  - Problème de recouvrement
  - Superposition de 3 réseaux au sein d'un même espace
  - Largeur de bande 83 MHZ
  - Pb principal : interfernces entre produits de toutes natures qui utilisent cette bande
  - Utilisé en WIFI par les standards 802.11 b et 802.11 g



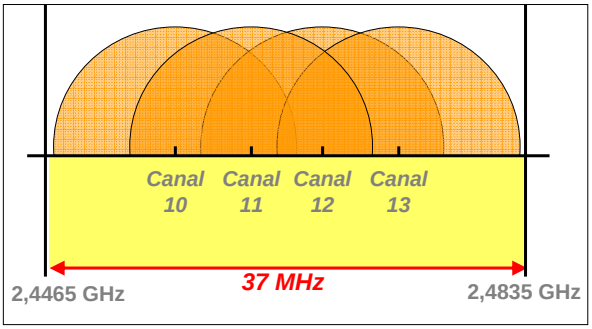


Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

BANDE ISM (Industrial, Scientific and Medical)

AFFECTATIONS DES CANNAUX

Pays	Etats-Unis	Europe	Japon	France
Nombres de sous canaux utilisés	1 à 11	1 à 13	14	10 à 13



BANDE ISM (Industrial, Scientific and Medical)

REGLEMENTATION BANDE ISM (Industrial, Scientific and Medical) DANS LE MONDE

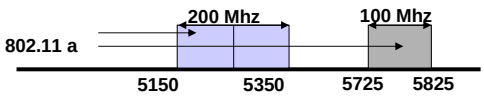
Pays	Bandes de fréquences
Etats-Unis *FCC*	2,400 – 2,485 GHz
Europe *ETSI*	2,400 – 2,4835 GHz
Japon *MKK*	2,471 – 2,497 GHz
France *ART*	2,4465 – 2,4835 GHz

EN FRANCE

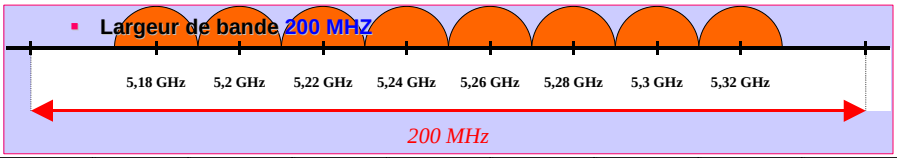
FREQUENCE en MHZ	Intérieur	Extérieur
2400 – 2454	100 mW	100 mW
2483,5		10 mW

BANDE UN-II (UNLICENCED NATIONAL INFORMATION INFRASTRUCTURE)

- Bande UN-II (5 GHZ) : Bandes libres
- Plus large et moins solide aux interfernces
- Deux partie : basse (200 MHz) et Haute (100 MHz)
  - Bande divisée en 8 canaux de 20 MHz
  - Pas de problème de recouvrement (atténuation du bruit)
  - Co-localisation de 8 réseaux au sein d'un même espace
  - Utilisé en WIFI par le standard 802.11 a



- Largeur de bande 200 MHZ

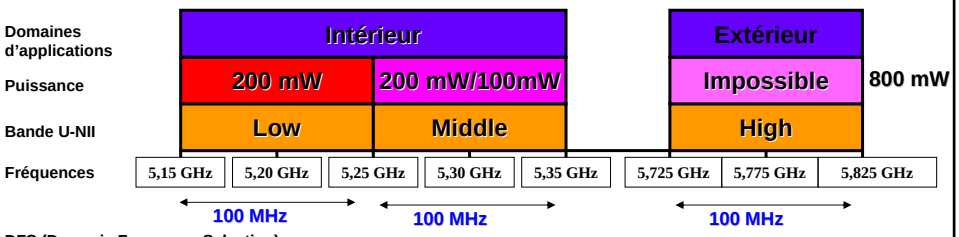


Canal	36	40	44	48	52	56	60	64
Fréquence (GHz)	5,18	5,20	5,22	5,24	5,26	5,28	5,30	5,32

BANDE UN-II (UNLICENCED NATIONAL INFORMATION INFRASTRUCTURE)

EN FRANCE

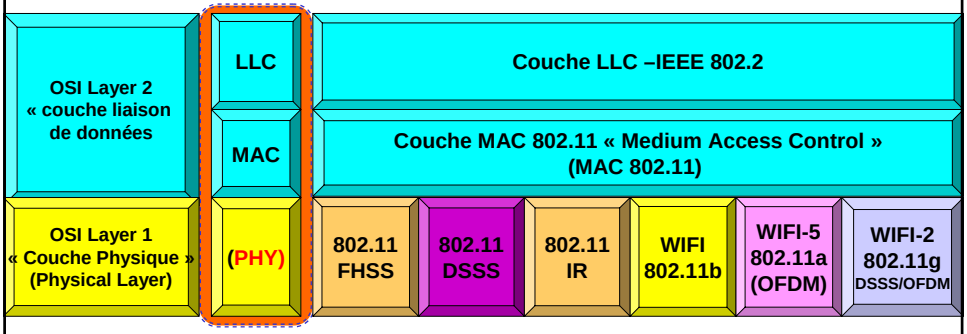
FREQUENCE en MHZ	Intérieur	Extérieur
5150 5250	200 mW	impossible
5350	200 mW avec DFS/TPC ou equivalent ou 100 mW avec DFS uniquement	impossible
5470 5725	impossible	impossible



DFS (Dynamic Frequency Selection)

TPC (Transmit Power Control).

Les couches Physiques

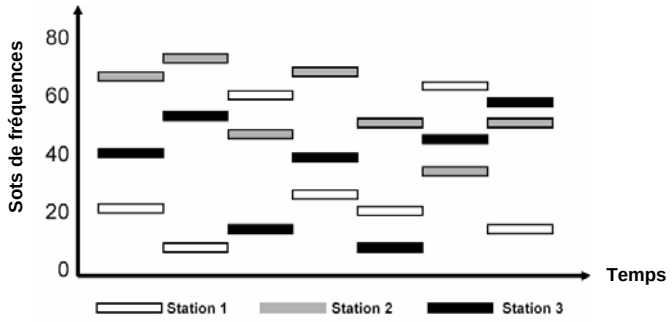


- **Principales caractéristiques :**
  - Le standard 802.11 définit un réseau sans fil dans lequel trois couches physiques peuvent être adoptées :
    1. IR (Infra rouge). (à modulation en impulsion , limité à une seul pièce)
    2. FHSS ('Frequency Hopping Spread Sequence') :
    3. DSSS ('Direct Sequence Spread Spectrum')

FHSS

COUCHE PHYSIQUE

- **FHSS : Frequency Hopping Spread Sequence**
  - 79 canaux de 1 MHz de largeur de bande
  - 3 ensembles de 26 séquences, soit 78 séquences de sauts possibles
  - **Saut de fréquence limite l'effet des interférences**
  - **Exemple : 3 stations sur 7 intervalles de temps : émission simultannée mais pas sur le même canal**
    - **Débit possible : de 1 à 2 Mbit/s**

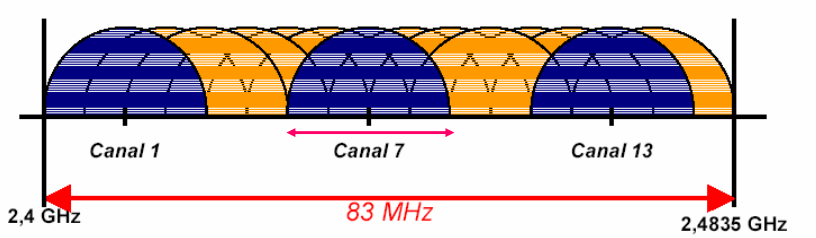


DSSS ('Direct Sequence Spread Spectrum')

COUCHE PHYSIQUE

DSSS : Etalement de spectre à séquence directe (division de la bande)

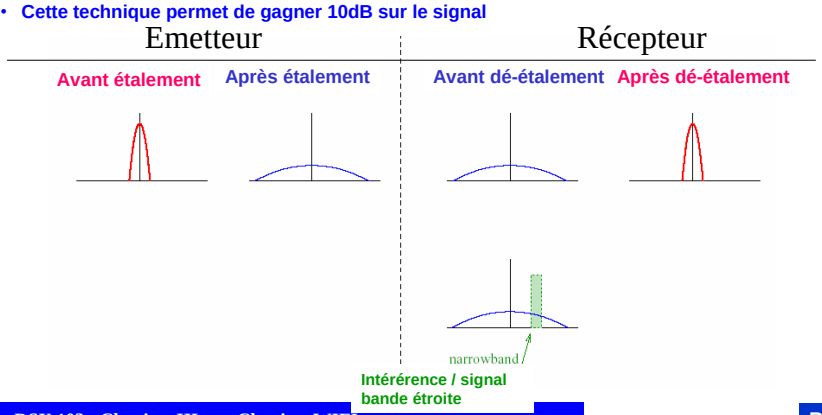
1. Technique la plus répandue aujourd'hui : 802.11b
2. Bande divisée en 14 canaux de 20 MHz (13 en France, 11 aux US)
3. Fréquence crête espacées de 5 Mhz / Canal 1 = 2.412 Ghz ; canal 14 = 2.477 Ghz
4. Débit théorique maximum de 11 / 54 Mbps
5. **3 canaux disjoints :** (1, 7, 13), (1, 6, 11), (3, 8, 13)
6. Une cellule peut utiliser jusqu'à **trois canaux simultanément**



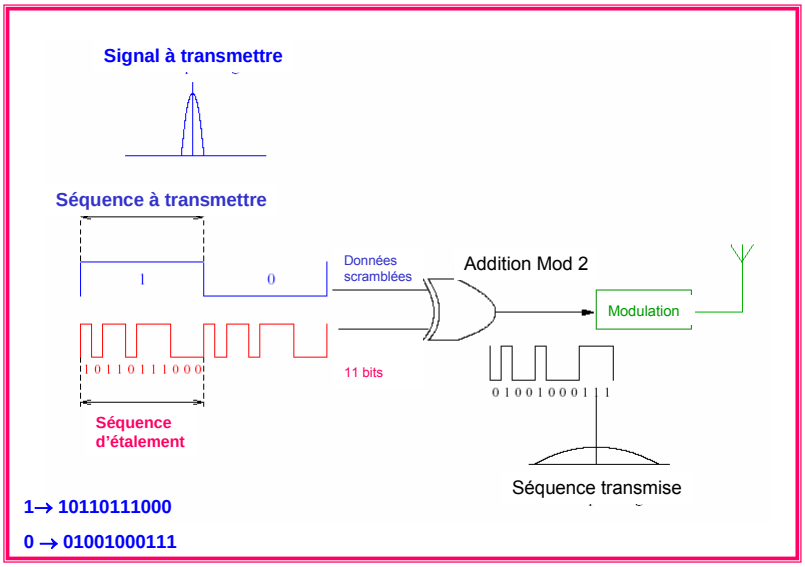
DSSS ('Direct Sequence Spread Spectrum')

Etalement de spectre à séquence directe : Principe :

- Le "spectre étalé" est une technique de transmission consistant a étaler l'énergie d'un signal de télécommunications sur une largeur de bande qui est beaucoup plus importante que le débit d'information.
- La plupart du temps, cet étalement se fait a l'aide d'un code pseudo-aléatoire (pseudo-noise code) indépendant des données.
- Cette technique permet de gagner 10dB sur le signal



DSSS ('Direct Sequence Spread Spectrum')



1→ 10110111000

0 → 01001000111

Étalement de spectre : Comparatif

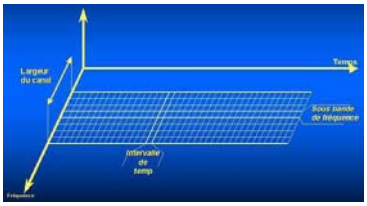
Caractéristiques	Saut de Fréquence FHSS	Séquence directe DSSS
Avantages	La + sûre Env. difficile	La + employée Env. peu perturbé
Débit théorique (Mb/s)	1	2
Débit effectif (Mb/s)	0.3 à 0.7	1.2 à 1.4
Sécurité	Séquence de saut	Code d'étalement
Taux d'erreur moyen	10^{-3}	10^{-8}
Distance maximale en intérieur	50 m	25 m
Distance maximale en extérieur	800 m	200 m
Cohabitation entre WLAN	simple	contraignant
Nb max de stations par AP	30 à 50	10 à 20
Remarques	Partage de la bande passante	Média monopolisé par émetteur

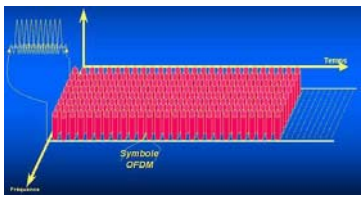
OFDM : *Orthogonal Frequency Division Multiplexing*

COUCHE PHYSIQUE — **TECHNIQUES DE MODULATION**

- **OFDM (Orthogonal Frequency Division Multiplex)**
  - Le principe de OFDM est :

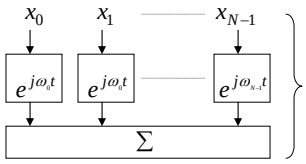
    De diviser le canal principal en **sous canaux** de fréquence plus faible.
    - Chacun de ces sous canaux est modulé par une **fréquence différente**,
    - L'espacement entre chaque fréquence restant constant.
  - Ces fréquences constituent une **base orthogonale** : le spectre du signal OFDM présente une occupation optimale de la bande allouée.
  - La répartition des canaux se fait par une FFT (Fast Fourier Transform).



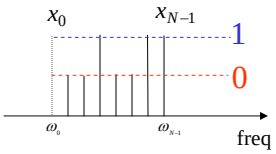


Orthogonal Frequency Division Multiplexing

Codage



Transformée de
Fourier inverse 64 points



$$x(n)=\frac{1}{N}\sum_{k=0}^{N-1}X(k)\exp(\frac{j2\pi kn}{N});\qquad 0\le n\le N-1$$

Décodage = Transformée de Fourier

Largeur de bande : 20 MHz

par exemple 8 canaux de 5150 à 5350 MHz

Dans chaque canal

48 sous-porteuses espacées de 300 kHz

+ 4 fréquences pilotes

Durée d'un symbole OFDM : **4ms**

Débit de 24 Mbit/s (de 6 à 54 Mbit/s)

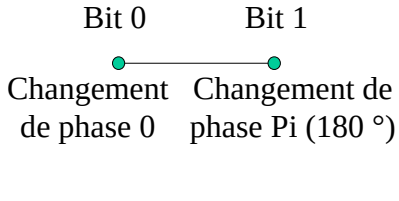
(⇔ soit 5 à 6 programmes pour un canal analogique actuel)

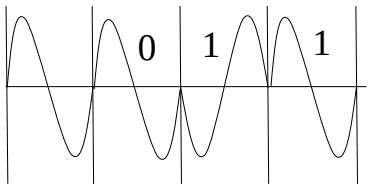
Constellations possibles

BPSK (2), QPSK (4), 16QAM, 64QAM

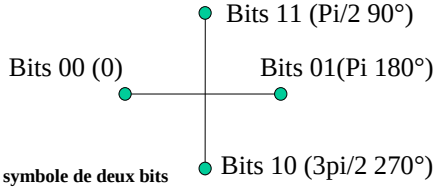
COUCHE PHYSIQUE

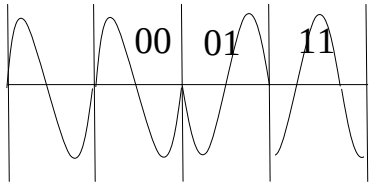
- **Modulation de phase différentielle** binaire (un bit par intervalle) ('**DBPSK** **D**ifferential **B**inary **P**hase **S**hift **K**eying')
  - **Débit 1 Mb/s**





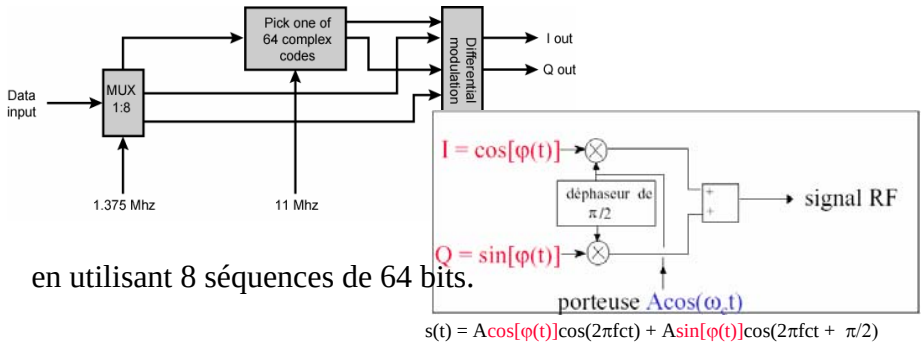
- Modulation de phase différentielle de porteuses en quadrature (deux bits par intervalle). **DQPSK** **D**ifferential **Q**uadrature **P**hase **S**hit **K**eying.
  - **Débit 2 Mb/s**





Debit : symbole de deux bits

- **CCK (Complementary code Keying)**
  - **Codage de plusieurs bits avec une seule puce (chip) en utilisant 8 séquence de 64 bits**
  - **En codant simultanément 4 bits → Débit de 5.5 Mbps**
  - **En codant simultanément 8 bits → Débit de 11 Mbps**
- **Exemple : schém d'un modulateur CCK pour transmission 11 Mbit/s**



en utilisant 8 séquences de 64 bits.

$s(t) = A\cos[\varphi(t)]\cos(2\pi fct) + A\sin[\varphi(t)]\cos(2\pi fct + \pi/2)$

OFDM : *Orthogonal Frequency Division Multiplexing*

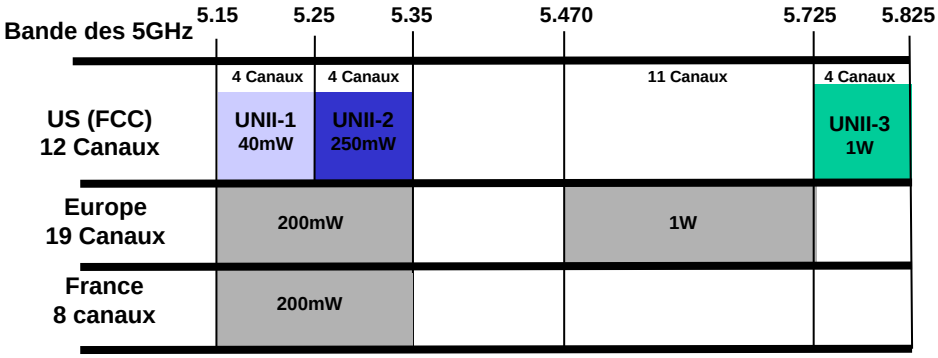
- **CCK (Complementary code Keying)**

Technologie	Codage	Type de modulation	Débit
802.11b	11 bits (Barker sequence)	PSK	1Mbps
802.11b	11 bits (Barker sequence)	QPSK	2Mbps
802.11b	CCK (4 bits)	QPSK	5.5Mbps
802.11b	CCK (8 bits)	QPSK	11Mbps
802.11a	CCK (8 bits)	OFDM	54Mbps
802.11g	CCK (8 bits)	OFDM	54Mbps

IEEE 802.11

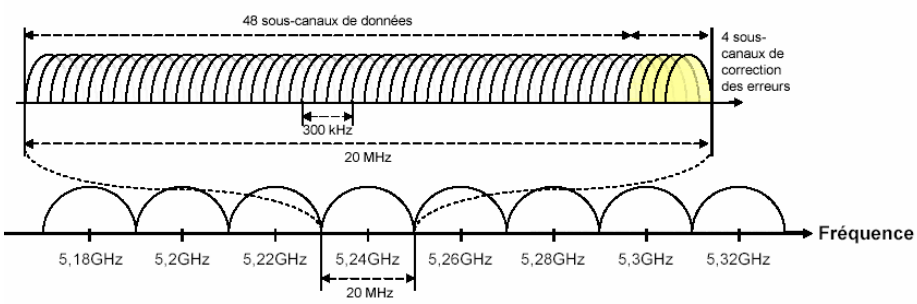
- **IEEE 802.11**
  - **Couche MAC + Tois couches physiques :**
  - **Deux couches utilisent la bande 2,4 GHz :**
    - **FHSS**
    - **DSSS**
  - **Une couche qui utilise la bande infra-rouge**
    - **IR**
  - **Débits offerts par les trois couches : 1 et 2 Mbps**

Généralités sur le 802.11a



- 8 canaux disjoints de 20 MHz en France
- Débits théoriques supportés : 6, 12, 24, 36, 48 et 54 Mbps
- Possibilité d'agréger plusieurs canaux avec plusieurs Points d'accès ou Ponts radio sur la même zone.

- Bande U-NII (5 Ghz) : Division des 2 premiers sous-bandes en 8 canaux de 20 Mhz
- Chaque canal contient 52 sous-canaux de 300 Khz
- Utilisation de tous les sous-canaux en parallèle pour la transmission



IEEE 802.11a

- Débit de 6 à 54 Mbits/s
- 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

à l'intérieur	
Débits Mbits/s	**Portée (en m)**
54 Mbits/s	10 m
48 Mbits/s	17 m
36 Mbits/s	25 m
24 Mbits/s	30 m
12 Mbits/s	50 m
6 Mbits/s	70 m

IEEE 802.11b

- **Amélioration des codages 802.11(baptisé HR/DSSS 'High Rate') pour atteindre des débits de 5.5 Mb/s et 11 Mb/s (Enhanced rates)**
- **Adaptation du débit (technique de codage) en fonction du rapport signal à bruit ('variable rate shifting').**
- **(plusieurs débits sont prévus, 1, 2, 5.5 et 11)**
  - **Si la transmission avec un débit est mauvais, le 802.11b se replie sur un débit inférieur**
  - **'Indication' des distances en intérieur à l'intérieur d'un bâtiment (débits possibles en fonction de la distance):**
    - 11 Mbit/s ⇔ (30 à 45 m) ;
    - 5,5 Mbit/s ⇔ (45 à 75 m) ;
    - 2 Mbit/s ⇔ (75 à 100 m) ;
    - 1 Mbit/s ⇔ (100 à 300 m).
- **: Utilisation de la bande ISM : 2,4 à 2,4835 Ghz.**

Niveau physique 802.11b : Codages et modulations

Débit en b/s	Nb bits codés par symbole	Longueur du symbole	Débit en symboles /s	Modulation
1 Mb/s	1 bit	11 bits code Barker	1 Méga symboles /s	DBPSK
2 Mb/s	2 bits	11 bits code Barker	1 Méga symboles /s	DQPSK
5,5 Mb/s	4 bits	8 signaux code CCK5,5	1,375 Méga symboles /s	QPSK
11 Mb/s	8 bits	8 signaux code CCK11	1,375 Méga symboles /s	QPSK

- DPSK : Differential Phase Shift Keying
- DQPSK : Differential Quadrature Phase Shift Keying QPSK Quadrature Phase Shift Keying (modulation Binaire)
- CCK : Complementary Code Keying (Optionnel PBCC Packet Binary Convolutional Coding)

IEEE 802.11g

Généralités sur le 802.11g

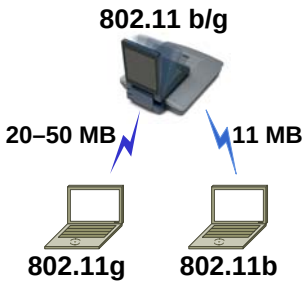
Standard IEEE depuis Juillet 2003

Objectif 54 Mbps @ 2.4 GHz (20 mbps aujourd'hui)

Compatible avec les 11 Mbps du 802.11b

Utilise les techniques développées dans 802.11a et 802.11b

- Permet d'atteindre un meilleur débit @ 2.4 GHz
- Vitesses proches du 802.11a
- Compatible avec les 11 Mbps du 802.11b
  - BPSK = 1Mbps
  - QPSK = 2Mbps
  - CCK = 5,5Mbps, 11Mbps
- • Même modulation que le 802.11a (OFDM)
  - OFDM = 12Mbps – 54Mbps



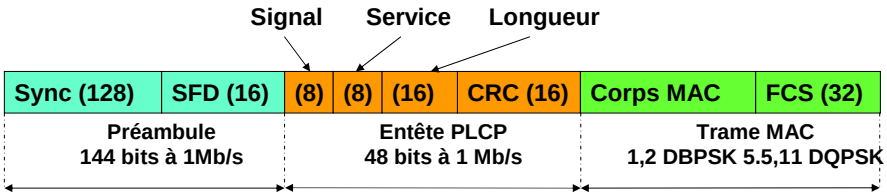
WIFI niveau physique : 802.11b

- Format des trames DSSS : /* utilisé dans 802.11b */
  - N.B : le format de la trmae du niveau physique dépend du codage et du médium utilisé

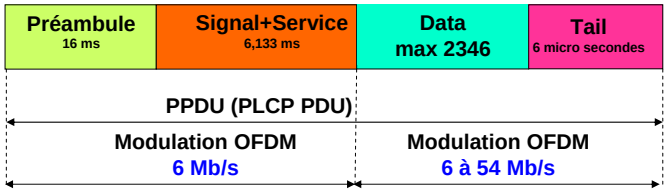
- **Préambule ' Preamble ' :**
  Synch (128 bits): Séquence 0101 … (128 bits entête normal, 56 bits entête court).
  SFD (16 bits Start Frame Delimiter): Délimiteur début F3A0 ou 1111 0011 1100 0000

- **PLCP ' Physical Layer Convergence Protocol ' .**
  Signal (8 bits): débit en centaine Kb/s hexa 0A, 14 (20d), 37, 6E pour 1, 2, 5,5, 11 Mb/s.
  Service (8 bits) : à 0.
  Longueur (16 bits): de la trame en octets (pour déterminer la fin).
  Header Error Check Field : CRC (16 bits) sur l'entête PLCP selon
  G(X)= X16 + X**12 + X**5 + 1**

- **Trame de niveau MAC avec code polynomial FCS.**

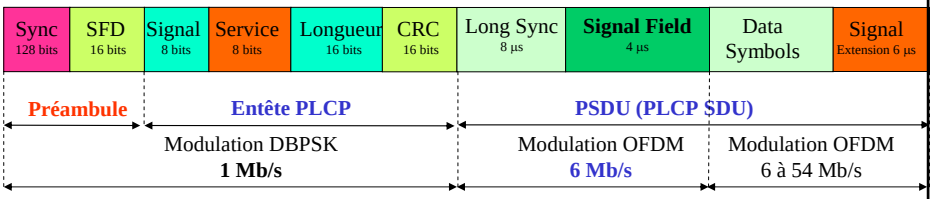


802.11g : Le format de trame DSSS-OFDM (pur 802.11g)



- **PPDU (PLCP PDU): Une unité de protocole de niveau physique.**
  - **L'entête PLCP est transmise à 6 Mb/s.**
  - **Préambule: Synchronisation pour une transmission OFDM.**
  - **Zone signal (24 bits): le débit de transmission utilisé pour la zone données et sa longueur (un symbole de 4 ms à 6 Mb/s).**
  - **La zone service est de 2/3 de symbole soient 16 bits (inutilisée).**
- **La zone de données contient une trame de niveau MAC d'une longueur maximum de 2346 octets.**
- **A la fin TAIL est une zone de silence de 6 micro secondes.**

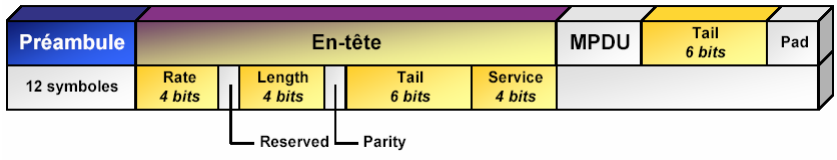
802.11g : Le format mixte d'une trame compatible 802.11b



- **PSDU (PLCP SDU) :**
  - **la charge utile d'une trame au niveau physique après le préambule et la zone PLCP comme en 802.11b à 1 Mb/s**
  - **(la partie signal de la zone PLCP, -il sert à coder les débits de 802.11b 1, 2, 5,5 et 11- codé par un débit à 3 Mb/s tous les débits OFDM : convention utilisée pour signifier à toute station réceptrice que la suite sera codée en OFDM).**
- **Les deux premières zones sont toujours émises à 6 Mb/s:**
  - **Long Sync (Long Training Sequence) est une séquence de synchronisation de deux fois 4 micro seconde plus un intervalle de garde.**
  - **OFDM Signal définit le débit et la longueur pour la partie OFDM Data Symbols.**
- **Data symbols: la partie MAC habituelle suivie de 6 ms de silence (signal extension).**

Niveau physique 802.11a - OFDM

Trame OFDM



- **Préambule Différent:**
  - **12 symboles**
- **En-tête :**
  - **OFDM**
  - **Reserved : réservé pour un usage future : ne contient que des 0**
  - **Length : nombre d'octets dans la trame, détermine la fin de trame**
  - **Parity : calcul de parité, détection d'erreur**
  - **Tail : « queue » , réservé pour un usage future, ne contient que des 0**
  - **Service : réservé pour un usage future, ne contient que des 0**

CONCLUSION

IEEE 802.11 Standard Activities

- 802.11a - 5GHz- ratifié en 1999
- 802.11b - 11Mbps 2.4 GHz- ratifié en 1999
- 802.11d - Domaines de régulation additionnels
- 802.11e - Qualité de Service
- 802.11f - Inter-Access Point Protocol (IAPP)
- 802.11g - 802.11b boosté (>20 Mbps) 2.4 GHz
- 802.11h - Sélection automatique du canal et de la puissance d'émission
- 802.11i - Authentification et sécurité

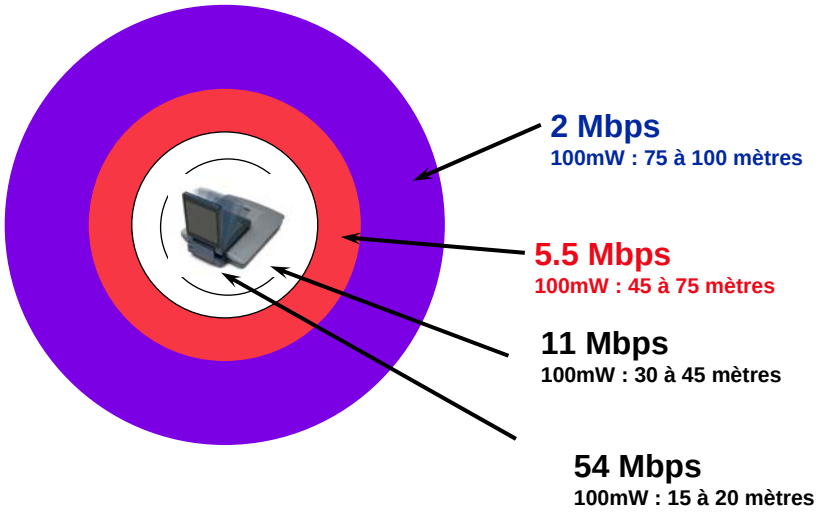
Normes IEEE 802.11

Choix de la bonne norme :

Norme	Caractéristiques	Avantages	Inconvénients
802.11b	▪ Débit jusqu'à 11 Mb/s Bande de 2.4 GHz ▪ 3 canaux séparés	▪ Utilisée par la plupart des équipements ▪ Prix faible ▪ Bonne portée	• Débit faible • Interférence avec d'autres équipements dans la bande de 2.4 GHz • Peu de canaux utilisables simultanément
802.11g	▪ Débit jusqu'à 54 Mb/s ▪ Bande de 2.4 GHz ▪ 3 canaux séparés	▪ Bonne porté ▪ Compatible avec 802.11b ▪ Débit élevé ▪ Prix moyen	▪ Interférence avec d'autres équipements dans la bande de 2.4 GHz ▪ Peu de canaux utilisables simultanément
802.11a	▪ Débit jusqu'à 54 Mb/s ▪ Bande de 5 GHz ▪ 19 canaux séparés	▪ Pas d'interférences avec d'autres équipements ▪ Débit élevé ▪ Beaucoup de canaux utilisables simultanément	▪ Porté plus faible ▪ Coût plus élevé ▪ Incompatible avec 802.11b

Normes IEEE 802.11

Couverture du 802.11b/g :



Normes IEEE 802.11

Technologie *Wireless LAN*
Fréquences & Réglementation Réseaux privés

802.11b / 802.11g En France (territoire métropolitain)	Intérieur	Extérieur
Canaux 1 à 7	100 mW	100 mW
Canaux 8 à 13	100 mW	10 mW et 100 mW sur propriétés privées avec accord défense

802.16 : WirelessMAN

- **Organisation de certification: WiMAX**
- **Fournit un accès réseau sans fil à large bande**
  - **Alternative à ADSL / Câblemodem**
  - **Vise principalement des utilisateurs fixes !**
    - **L'utilisation mobile sera considérée dans les normes futures**
    - **N'est pas optimisé quant à la consommation d'énergie**
- **État actuel**
  - **Les premières normes sont approuvées**
  - **Les premiers produits sont disponibles aux US**
  - **L'Europe (la Suisse) va allouer des fréquences en 2005**
  - **Quelques fréquences nécessiteront une licence de l'OFCOM (Office Fédéral de la COMmunication)**

Comparaison WLAN - WMAN

Norme	802.11	802.16
Utilisation principale	Ordinateurs mobiles	Ordinateurs fixes ou nomadiques
Portée	< 100 m	Typiquement : 3 – 10 km
Nombre D'utilisateurs	< 10	Des centaines de récepeteurs avec un nombre illimité d'utilisateurs
Débit	Jusqu'au 54 Mbits/s	Jusqu'au 75 Mbits/s
Support de QoS	IEEE 802.11e	QoS intégrée dans la couche MAC : approprié pour la transmission multi-média
Sécurité	WEP, WPA	Triple DES 128 bits RSA 1024 bits
Prix	Faible	Estimé à : 350 $ en 2005 100 $ en 2006

Les différentes normes WiMAX

	802.16	802.16a	802.16e
Approbation	Déc. 2001	Janv. 2003	Attendu pour 2005
Fréquences	10 – 66 GHz	2 – 11 GHz	2 – 6 GHz
Modulation	QPSK, QAM-16 QAM-64	OFDM avec 256 porteuse utilisant QPSK, QAM-16	QPSK, QAM-16 QAM-64
Débits	32- 134 Mb/s dans un canal de 28 MHz	Jusqu'à 75 Mb/s dans un canal de 20 MHz	Jusqu'à 15 Mb/s dans un canal de 5 MHz
Portée typique	2 – 5 Km	7 – 10 Km	2 – 5 Km
Utilisation	Fixe	Fixe	Mobile

WIFI : Conclusion

- Avantages :

1. Supprime les câblages (construction ‘ ad-hoc ’).
2. Débit acceptable pour un grand nombre d’applications.

- Inconvénients

1. Surcharges protocolaires (11 Mb/s => 6,38 Mb/s réels).
2. Problèmes des transmissions hertziennes.
   Distances assez faibles, Interférences
3. Problèmes de sécurité
4. Mise en œuvre de l’itinérance entre cellules (Roaming)
5. Qualité de service (téléphone sur wifi).