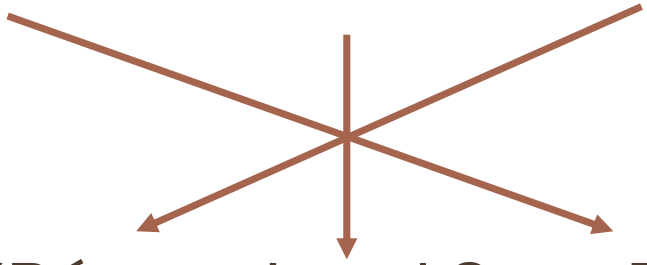
RÉSEAUX LOCAUX SANS FIL WIFI (IEEE 802.11) WLAN

Prof. M Bouziani

NOM GENERIQUE

WLAN

Wireless Local Area Network



(Réseau Local Sans Fils)

INTRODUCTION

- **WI-FI est une technologie de réseaux sans fil utilisant comme média les ondes hertziennes.**
- **Le Wi-Fi désigne la Wireless Fidelity, c'est un nom commercial donné à la norme IEEE 802.11**
- **Apparu au milieu des années 90 aux USA**

Introduction

- **La WECA (*Wireless Ethernet Compatibility Alliance*) est l'organisme chargé d'étudier l'interopérabilité des matériels de la norme 802.11. A l'origine le terme "WiFi" n'avait pas de signification. Il s'agissait d'un terme publicitaire. Par la suite ce terme a été justifié avec le slogan "*The standard for Wireless Fidelity*"**

Un réseau local sans fil

- C'est quoi ?
  - Un ensemble de stations fixes ou mobiles, interconnectées par un réseau local de communication radio
- Ca sert à quoi
  - Offrir un moyen de communications numériques entre ces stations
  - Facile à déployer (… sans fil !)

- 1990 : lancement du groupe de travail à l'IEEE
  - 1997 : IEEE 802.11 - "Wireless Local Area Network" (WLAN)

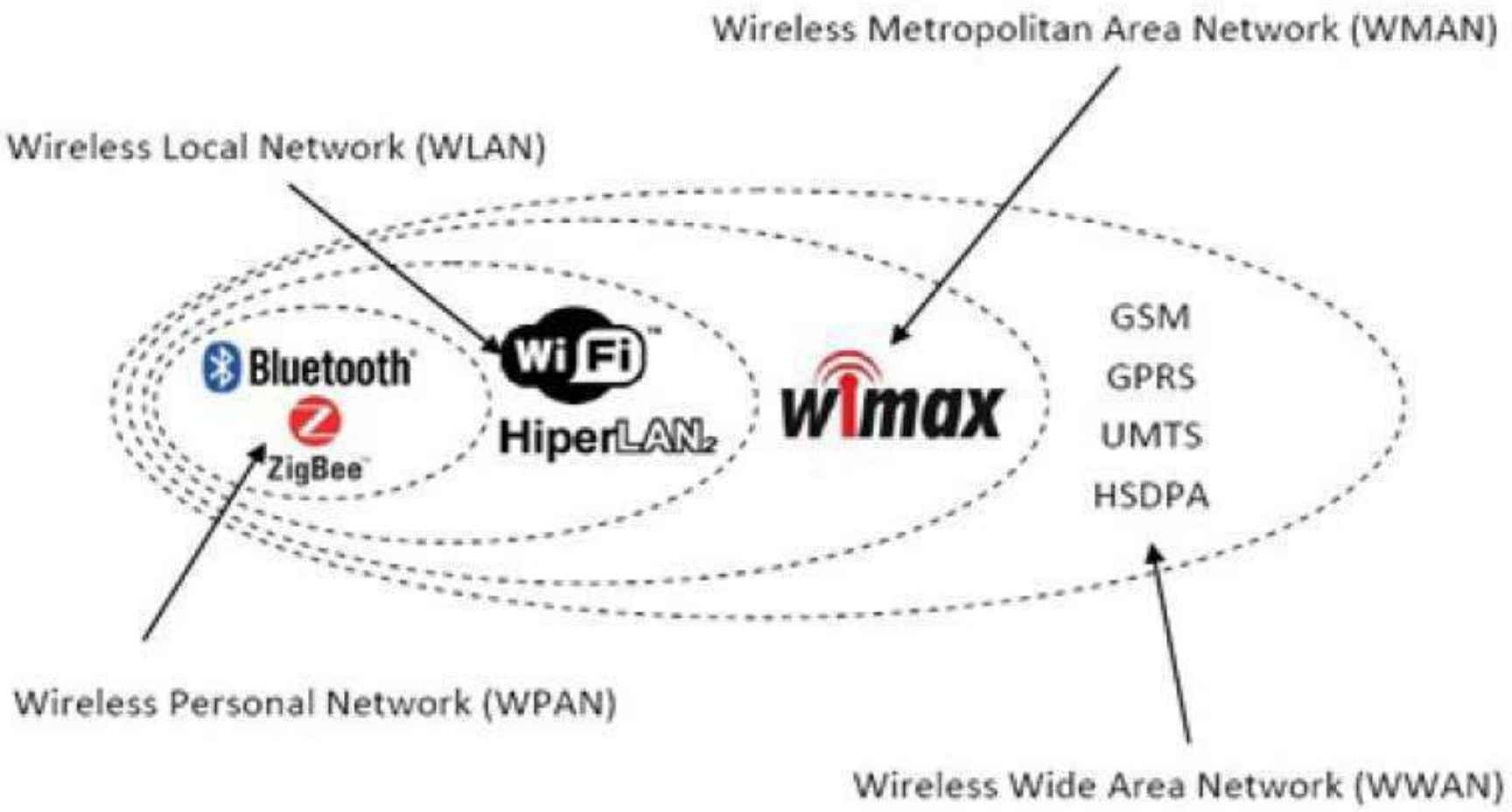
    "IEEE Standard for Information Technology-
    Telecommunications and Information Exchange Between Systems-
    Local and Metropolitan Area Networks- Specific Requirements-
    Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"

NORME

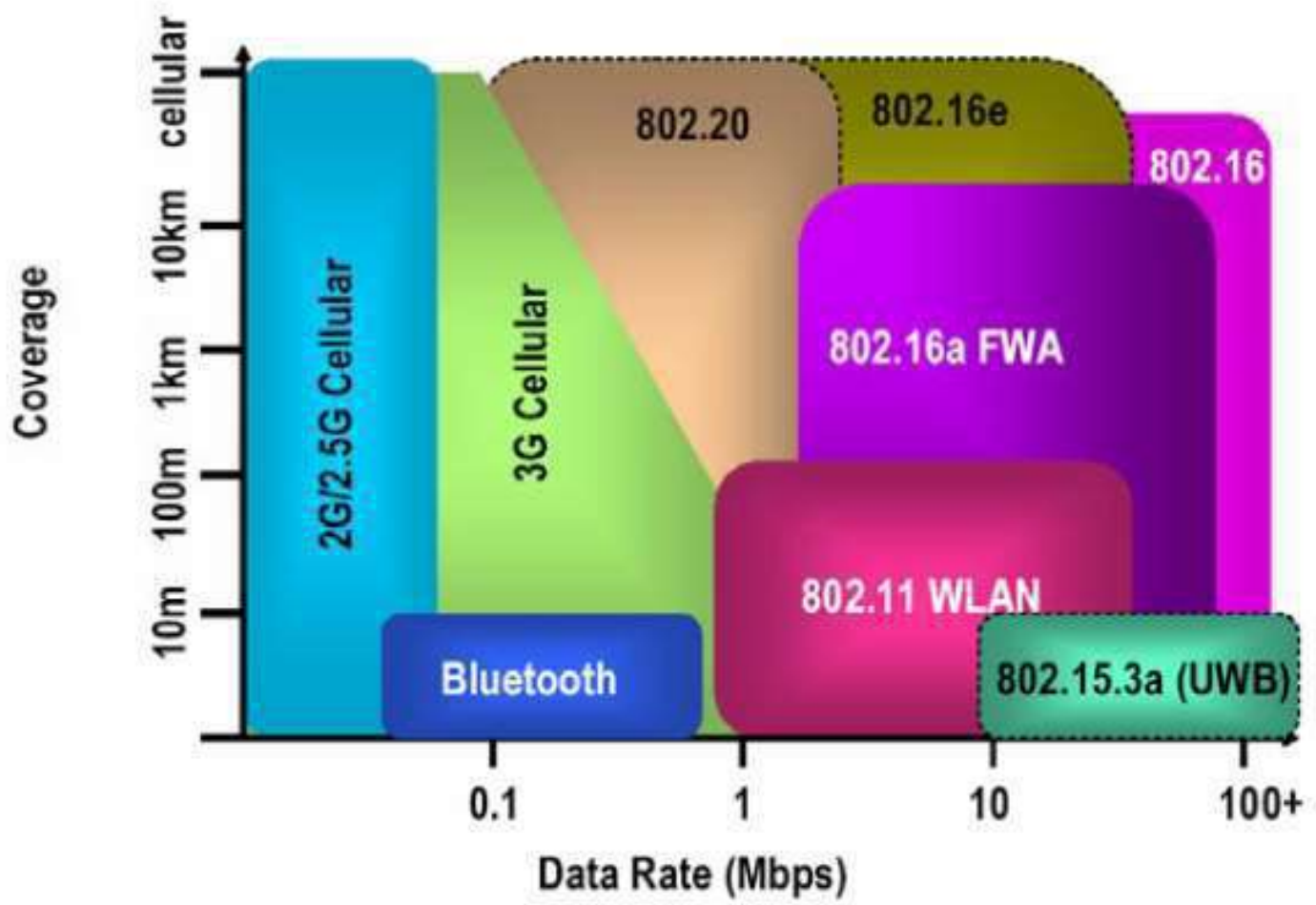
- **Elle est assurée essentiellement par le groupe 802.11 de l'I.E.E.E.**
- **La norme initiale 802.11 a connu de nombreuses révisions notées 802.11a, 802.11b, 802.11g pour les principales.**
- **Ces révisions visent essentiellement :**
  - **une amélioration du débit**

  et/ou
  - **une amélioration de la sécurité.**

CLASSIFICATION DES RÉSEAUX SANS FIL



Les réseaux sans fil



NORMES

- 1) WIFI : un réseau local radio.
  - Définition sur les deux niveaux physique et liaison.
- 2) WIFI : deux organisations architecturales.
  - Le mode infrastructure (centralisé).
  - Le mode ad 'hoc (distribué).
- 3) WIFI : deux protocoles différents d'accès au médium.
  - PCF 'Point Coordination Function' (en coopération).
  - DCF 'Distributed Coordination Function' (en compétition).
  - Pouvant être utilisés simultanément par une station.
- 4) WIFI : selon le débit, le codage, la bande de fréquences utilisée
  - 802.11, 802.11a , 802.11b , 802.11g, 802.11n, etc…

Caractéristiques de l'IEEE 802.11

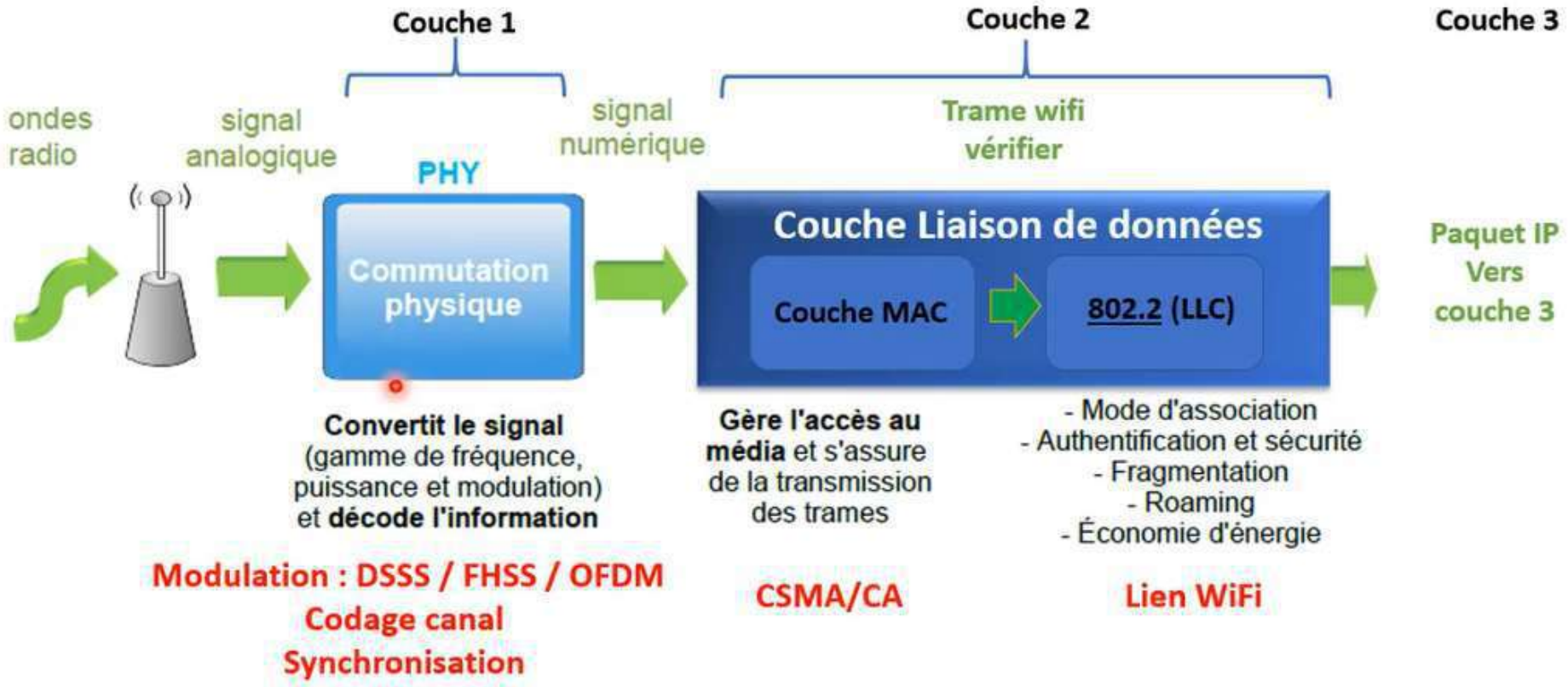
- Communications
  - Directes :
    - d'une station (fixe ou mobile) à une autre station (fixe ou mobile)
    - sans relayage
  - Indirectes :
    - En passant par une (ou des) station(s)
      - Station de base
      - Ou avec routage (réseau ad'hoc)
- Utilisation de bandes de fréquence
  - 2,4 Ghz (ISM : "Industrial, Scientific and Medical"), 5 GHz (U-NII : Unlicenced-National Information Infrastructure), ou Infrarouge
  - Sans licence d'exploitation
  - Libres dans de nombreux pays
- Débits variables
  - Adaptation aux conditions de l'environnement radio
  - Différents codages (FHSS, DSSS, OFDM, etc.)

Caractéristiques de l'IEEE 802.11

- Portée locale
  - Typiquement : 30 m en intérieur, 100 m en extérieur
- La technique d'accès au support partagé
  - "Medium Access Control"
  - Complexe :
    - S'adapte à une large gamme de fréquences
      - 2,4 GHz, 5 GHz, IR
    - Propose de nombreuses options
      - avec infrastructure ou adhoc, contrôle d'accès distribué ou centralisé, avec ou sans économie d'énergie, etc.
  - CSMA/CA
    - "Carrier Sense Multiple Access/Collision Avoidance"
    - Similaire mais différent du CSMA/CD d'Ethernet :
      - La détection de collision est impossible

Les réseaux WLAN

Principe de fonctionnement du module WiFi 802.11:



Normes principales

Norme	Débit nominal en Mb/s	Bande de fréquences	Commentaire
IEEE 802.11	1, 2	2.4 GHz	Première norme. Plus utilisée
IEEE 802.11b	1, 2, 5.5, 11	2.4 GHz	Compatible avec 802.11g. Peu utilisée
IEEE 802.11g	1 – 54 (plusieurs débits)	2.4 GHz	Très populaire aujourd'hui
IEEE 802.11a	6 – 54 (plusieurs débits)	5 GHz	Portée plus faible, mais moins d'interférences
IEEE 802.11n	Jusqu'à 600 (avec 2 canaux et 4 flux spatiaux)	2.4 GHz ou 5 GHz	Utilise MIMO (Multiple-input multiple-output), avec plusieurs flux spatiaux
Normes futures			
IEEE 802.11ac	Max 7 Gb/s	5-6 GHz	Ratifiée en janvier 2014
IEEE 802.11ad	Max 7 Gb/s	60 GHz	Courtes distances seulement

Architecture des systèmes IEEE 802.11x

Wi Fi Architecture

Wi Fi architecture cellulaire

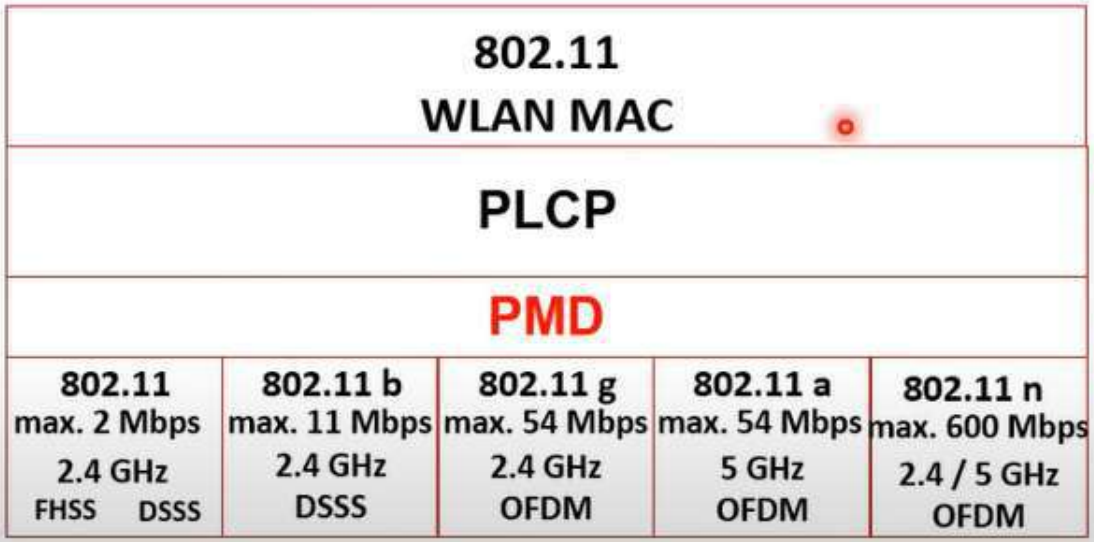
- similaire à la téléphonie mobile : téléphones + stations
- un ou plusieurs points d'accès : unifier le réseau et servir de pont
- → cellule

Wi Fi deux types de topologies

- mode infra-structure
  - BSS : Basic Service Set
  - ESS : Extended Service Set
- mode ad-hoc
  - IBSS Independent Basic Service Set

Les réseaux WLAN

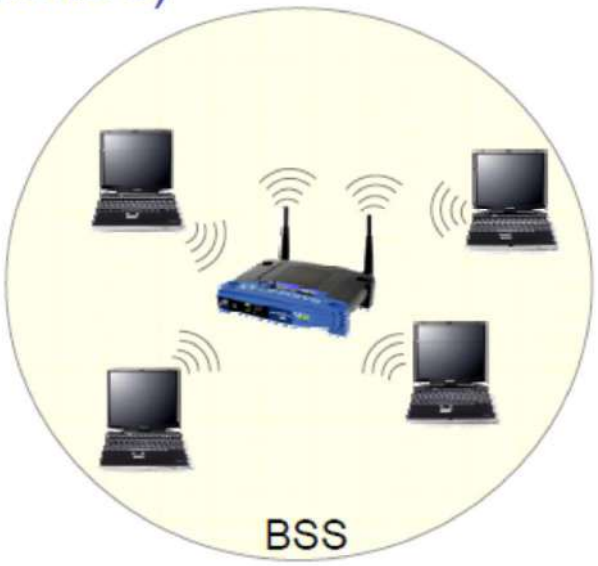
802.11 Physical Layer Overview



La couche physique est classée en deux sous-couches: Physical Layer Convergence Procedure (PLCP) et la procédure dépendant du support physique **Physical Medium Dependent (PMD).** PLCP mappe les trames MAC sur le support de transmission. PMD transporte les trames.

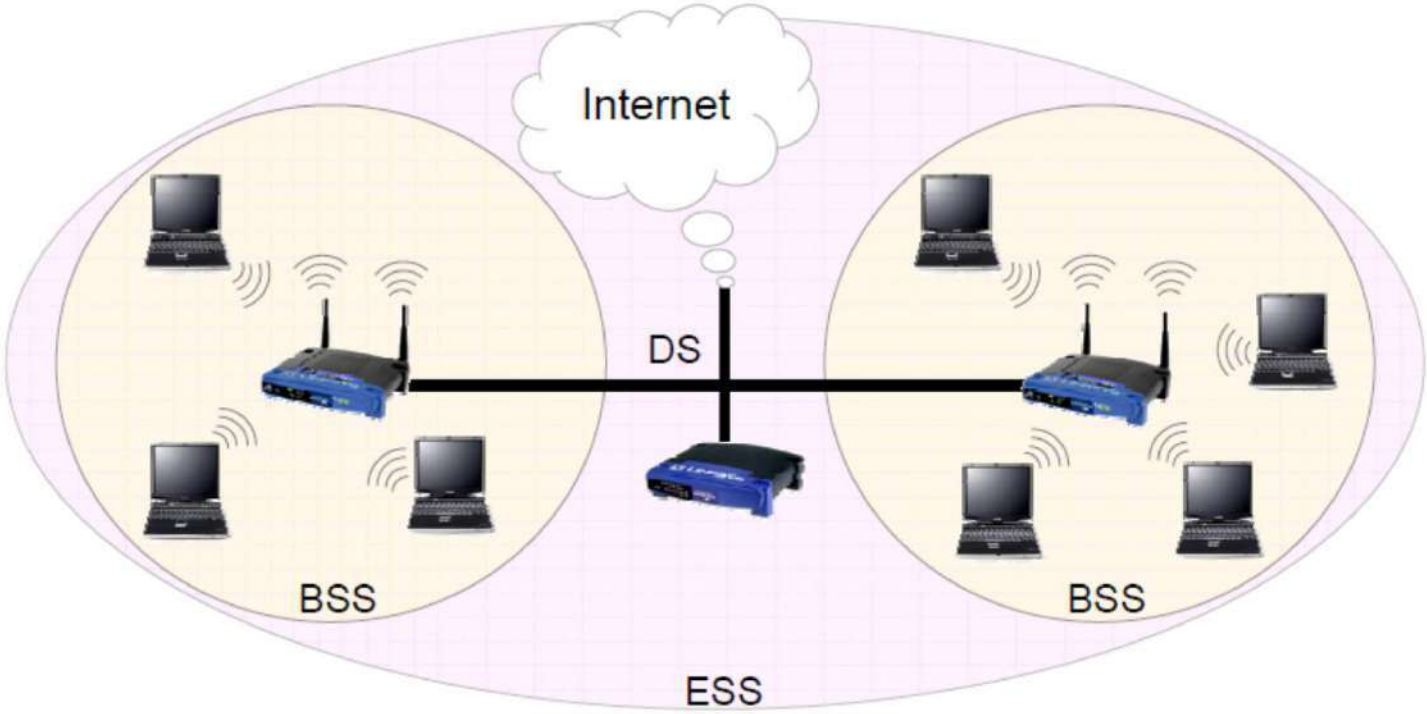
Le mode infra-structure : BSS

- Le mode infrastructure désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les stations ; l'infrastructure est le point d'accès
- 1 cellule = 1Basic Service Set (BSS) = 1 point d'accès
- 100 stations : support partagé entre toutes les stations, ainsi que le débit (11 Mbits/s)



Le mode infra-structure : ESS

- Extended Service Set : plusieurs points d'accès (BSS) connectés entre eux par un système de distribution (DS)
- DS : Ethernet ou un autre réseau WLAN
- Fourniture d'accès vers un autre réseau : Internet



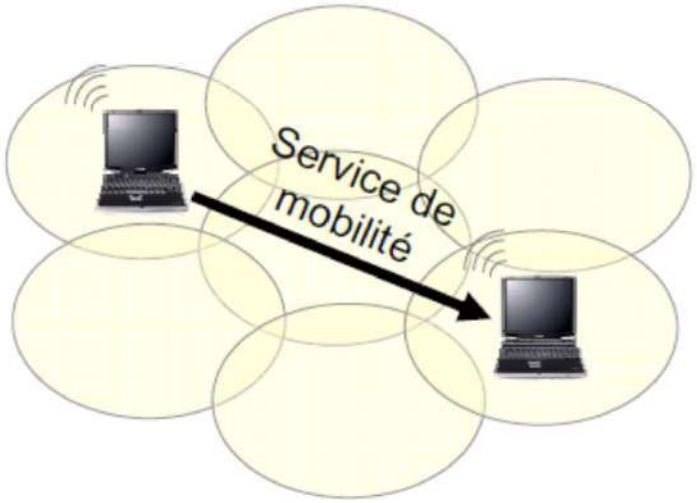
ARCHITECTURE

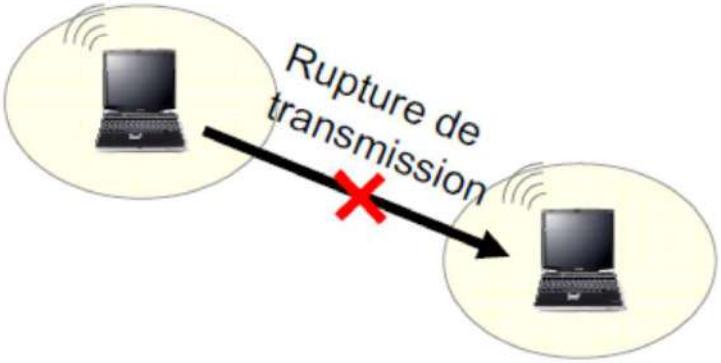
Le mode avec infrastructure

- Les points d'accès (AP) sont responsables :
  - des services spécifiques
    - contrôle d'accès, authentification, gestion de l'association
  - sur leur zone de couverture
  - ils jouent aussi le rôle de station (STA) dans un BSS
  - un BSS est identifié par son BSSID
- Le système de distribution (DS)
  - accroît le champ de communication au-delà de la couverture radio
  - offre aux usagers des STA l'accès à d'autres ressources
    - serveurs de fichiers, imprimantes, et au reste de l'Internet (dont d'autres réseaux mobiles avec d'autres types ou non)

Le mode infra-structure : ESS

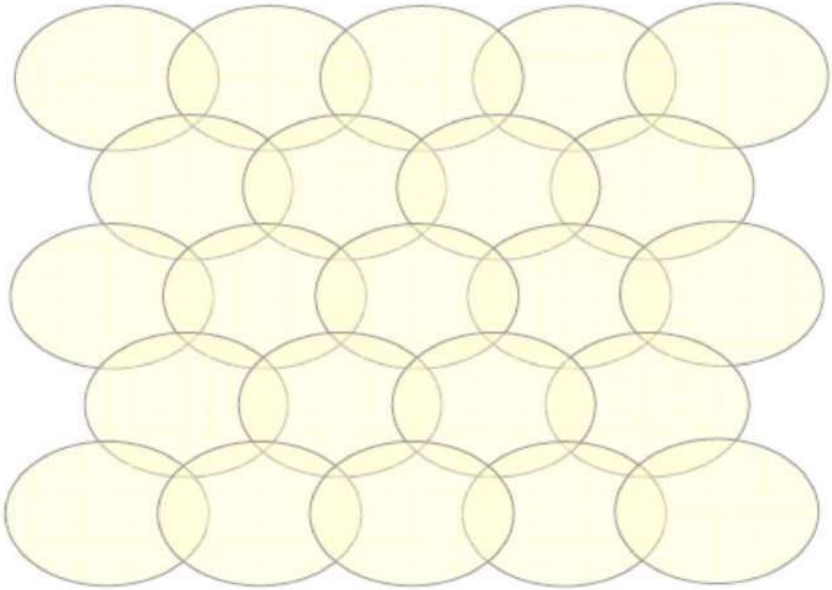
- Topologie ESS variable : cellules recouvrantes ou non
- les cellules recouvrantes permettent d'offrir service de mobilité (IEEE 802.11f) : pas de pertes de connexions
- plus grand nombre d'utilisateurs possibles sans dégradation trop importante des performances





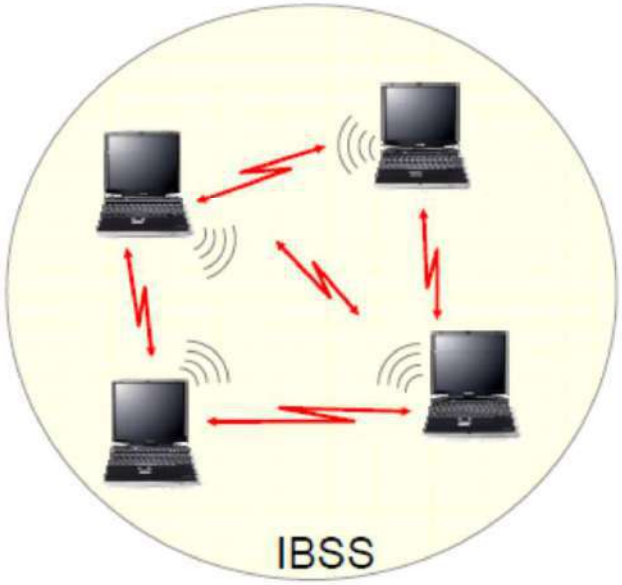
Réseau ambiant

- 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.)



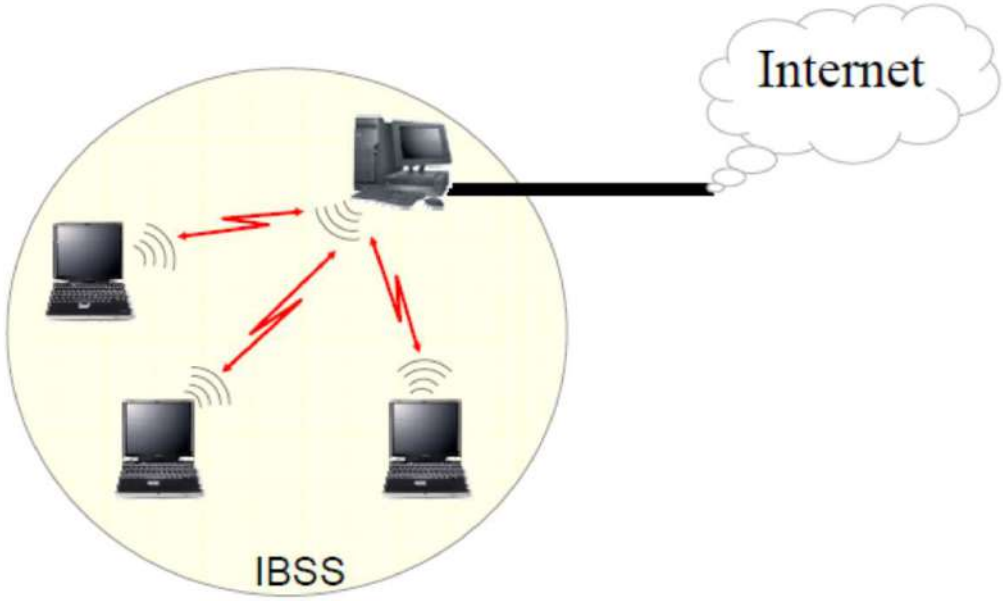
Le mode ad-hoc : IBSS

- Independent Basic Service Set : mode point à point
- Permet l'échange d'informations lorsque aucun point d'accès n'est disponible



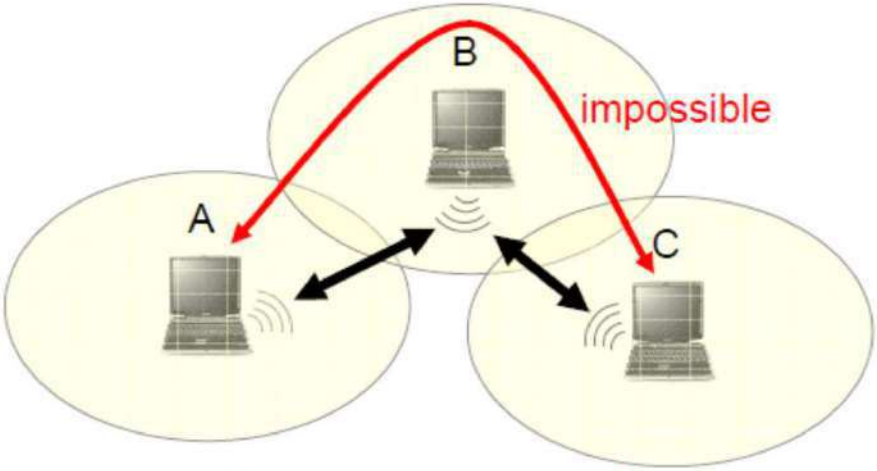
Le mode ad-hoc

une station peut partager un accès à Internet : le réseau fonctionne comme un BSS



Le mode ad-hoc

- 3 stations en mode ad-hoc : différent d'un réseau ad-hoc de trois stations
- il n'y a pas de protocole de routage : A ne peut pas envoyer de données à C car B ne peut effectuer le routage



3 stations en mode ad-hoc

Réseaux ad-hoc et routage

- Le logiciel de routage doit être présent dans chaque nœud
- Solution la plus simple : routage directe : toutes les stations peuvent se voir sans passer par un nœud intermédiaire
- Cas le plus classique : nœuds intermédiaires dotés de tables de routages optimisées
- Problèmes pour la construction des tables :
  - liaisons asymétriques
  - interférences
- Normalisation des réseaux ad-hoc :
  - protocoles réactifs
  - protocoles proactifs

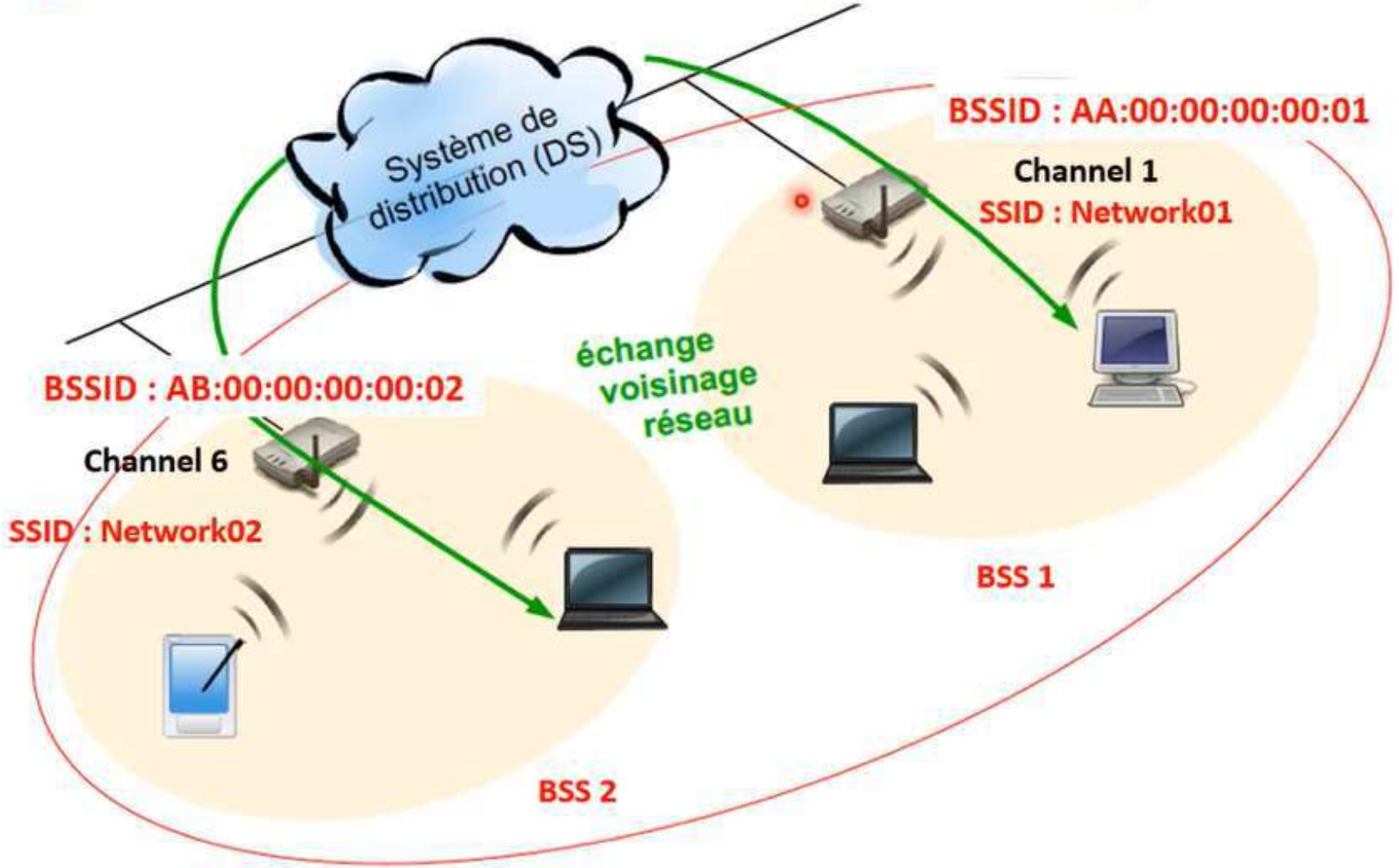
Protocoles réactifs

- Travaillent par inondation : détermination de la meilleure route lorsque les paquets sont prêts à être émis
- Pas d'échange de paquets de contrôle, sauf paquets de supervision (détermination du chemin)
- Le paquet de supervision diffusé vers les nœuds voisins est transmis par ceux-ci vers le nœud destination : plusieurs routes possibles si problèmes sur la route principale

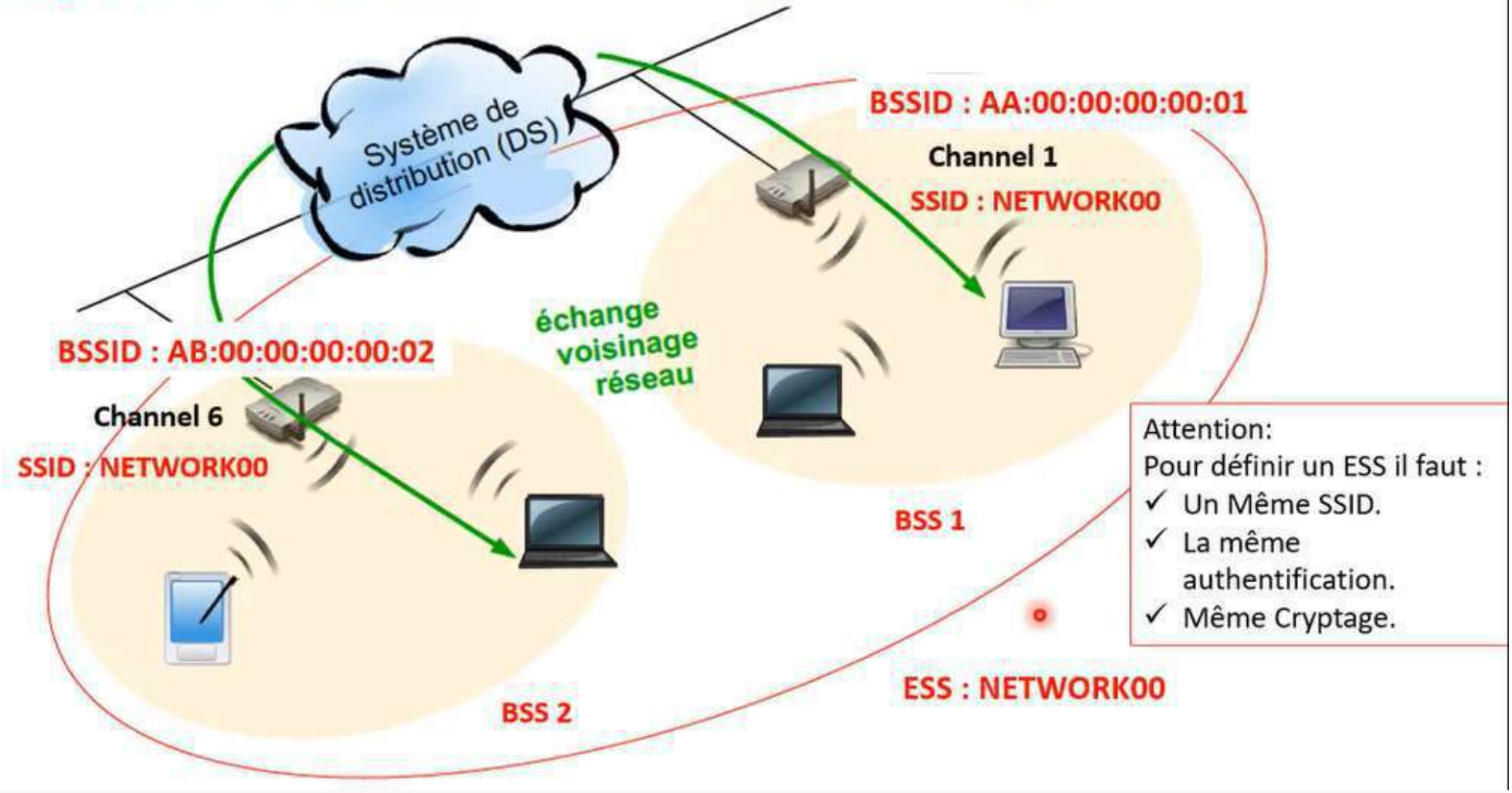
Protocoles proactifs

- Émission ininterrompu de paquets de supervision
- Maintien de la table de routage : rafraîchissement dynamique
- Chaque information de supervision influençant le comportement du réseau entraîne la modification des tables
- Difficulté : calcul des tables de routage pour qu'elles soient cohérentes

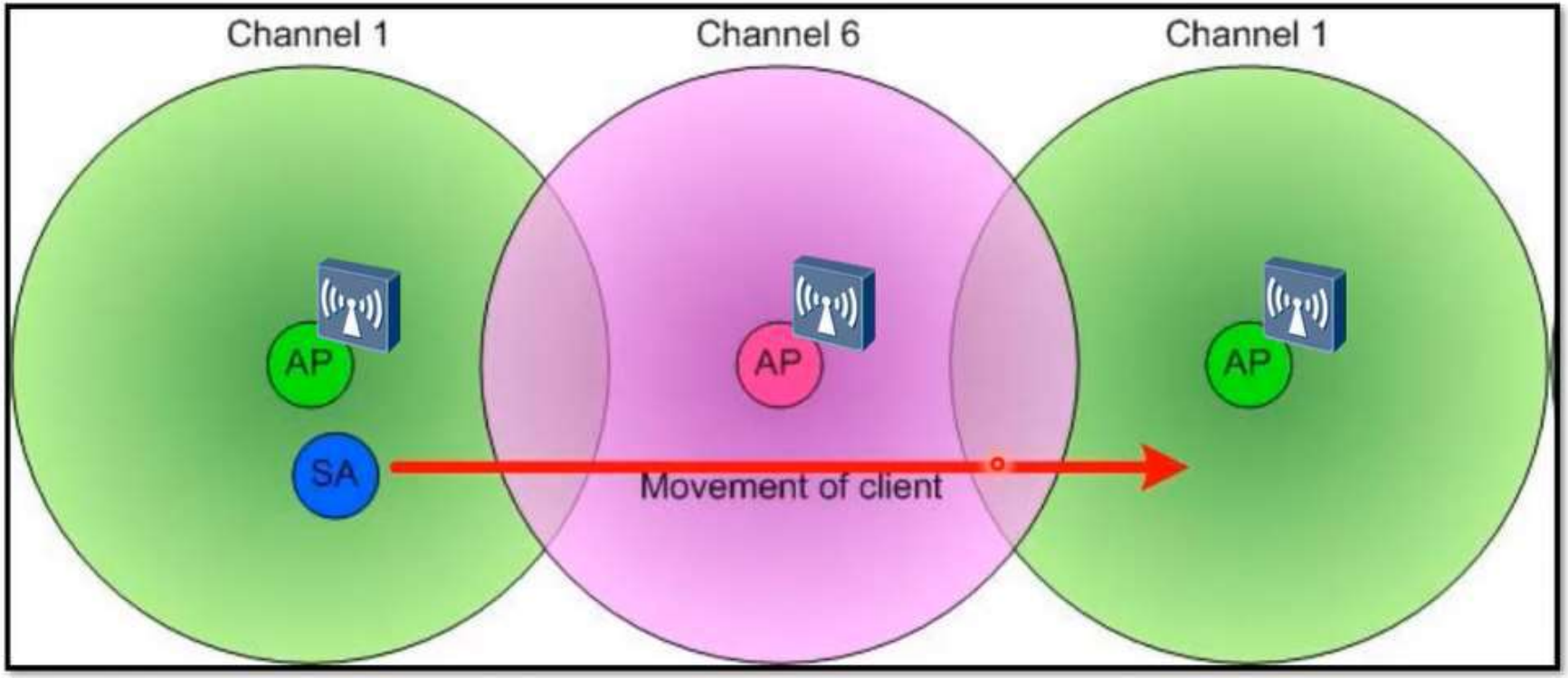
La topologie avec infrastructure et le concept de Roaming :



La topologie avec infrastructure et le concept de Roaming :



La topologie avec infrastructure et le concept de Roaming :



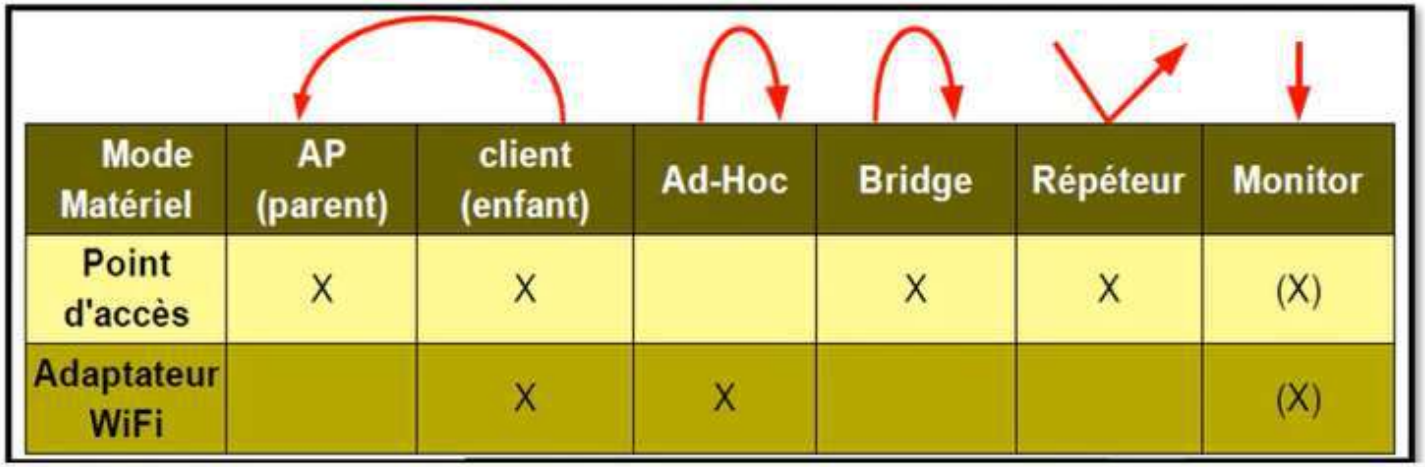
802.11f

ESS : NETWORK00

1) Les modes et Mécanismes d'association :

Le mode d'association configuré sur un module WiFi détermine ses possibilités de connexion avec les autres :

- **mode *AP* (access point)** : fonction d'association parent (diffuse un SSID, fonction switch et répartition de charge, gère la sécurité)
- **mode *client* ou *managed*** : fonction d'association enfant
- **mode *adhoc*** et **mode *bridge*** : pont réseau
- **mode *repeater*** : réémission des trames
- **mode *monitor*** : écoute et enregistrement des trames

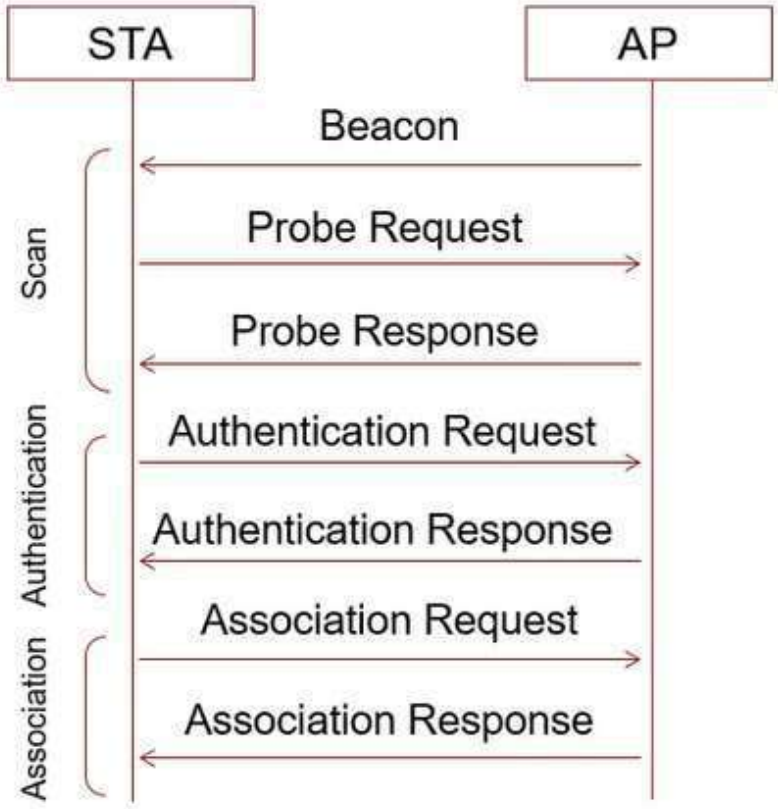


Mode Matériel	AP (parent)	client (enfant)	Ad-Hoc	Bridge	Répéteur	Monitor
Point d'accès	X	X		X	X	(X)
Adaptateur WiFi		X	X			(X)

1) Les modes et Mécanismes d'association :

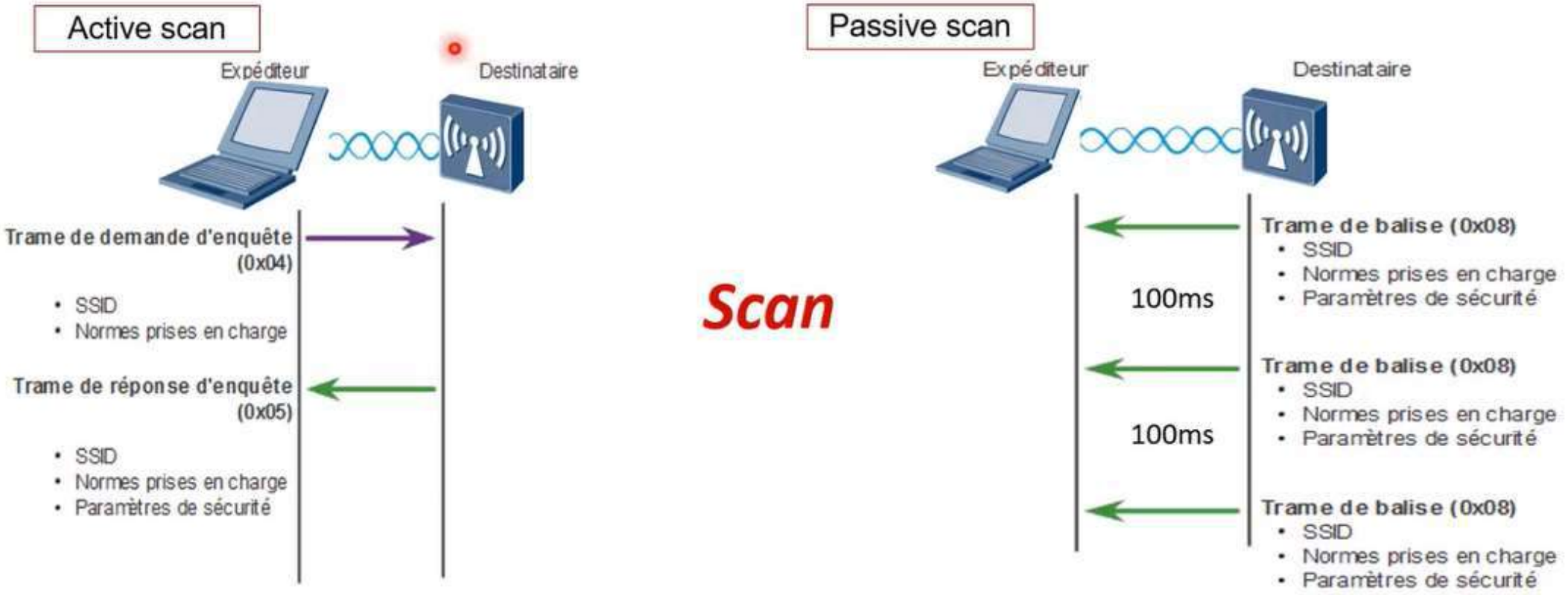
Mécanisme ou Processus d'accès au Réseau sans fil:

- Wireless users perform the following operations:
  - Scan for wireless services
  - Pass the authentication
  - Associate with an AP
- Access the WLAN



1) Les modes et Mécanismes d'association :

Mécanisme ou Processus d'accès au Réseau sans fil:



1) Les modes et Mécanismes d'association :

Mécanisme ou Processus d'accès au Réseau sans fil:

L'adaptateur client :

a) évalue la qualité du signal émis et la distance du PA

b) choisit le PA avec le meilleur débit et la plus faible charge en cas de propositions multiples

c) envoie une demande **d'authentification** puis **demande d'association au PA choisi**

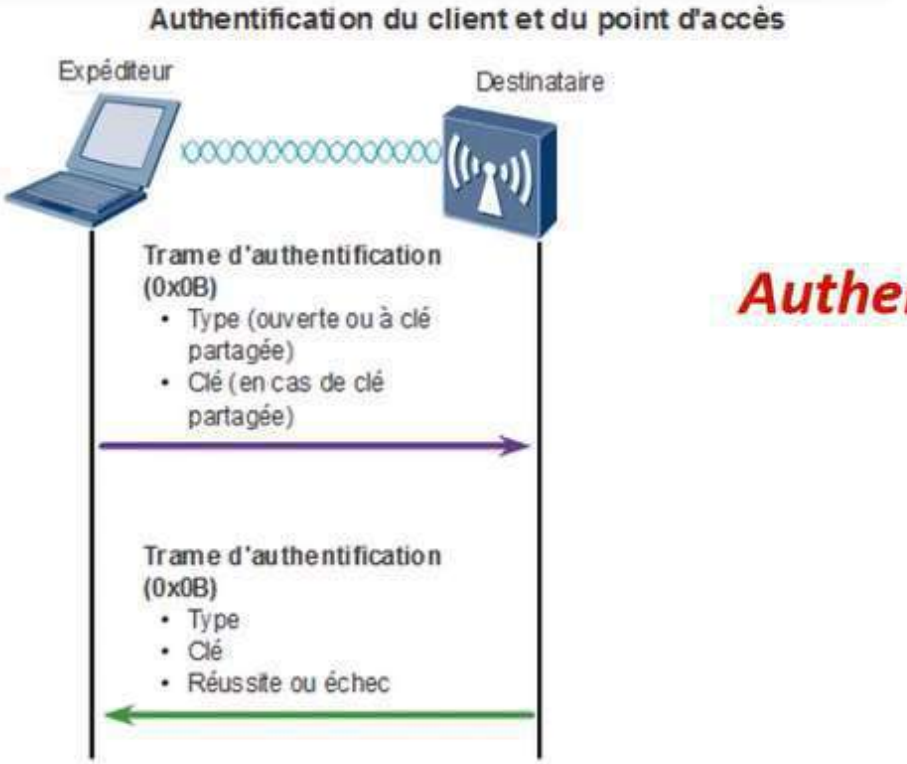
L'indicateur d'intensité du signal reçu (RSSI) et AP load

1) Les modes et Mécanismes d'association :

Mécanisme ou Processus d'accès au Réseau sans fil:

Authentication

- To ensure wireless network security, APs authenticate STAs. Only authenticated STAs can be associated with the APs. IEEE 802.11 defines two link authentication modes: **open system authentication and shared key authentication.**

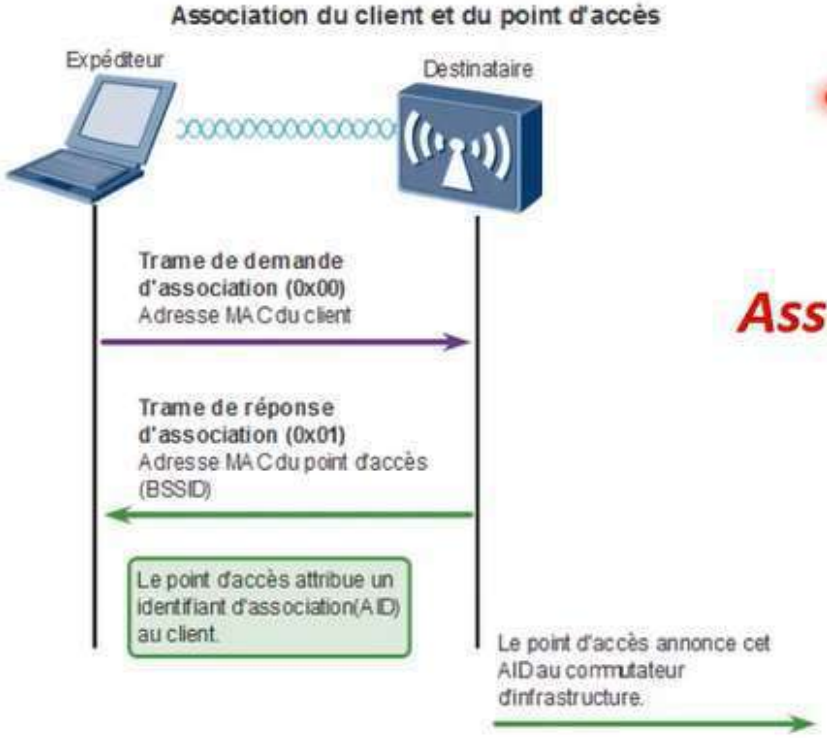


Authentication

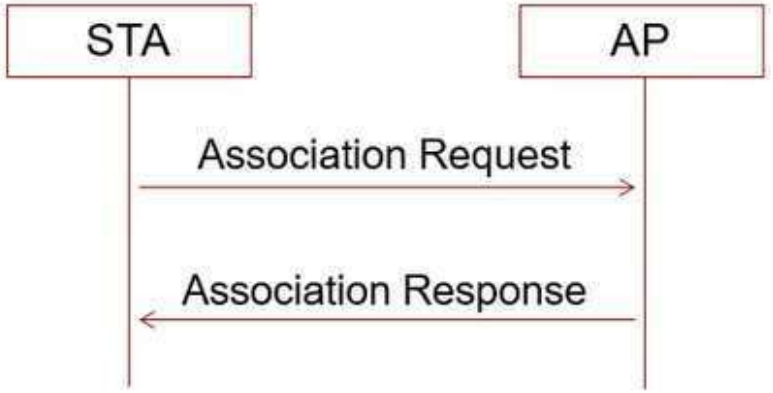
1) Les modes et Mécanismes d'association :

Mécanisme ou Processus d'accès au Réseau sans fil:

- Client association is a link negotiation process. After 802.11 link authentication is complete, the WLAN client initiates 802.11 link negotiation. During 802.11 link negotiation, association or re-association packets are exchanged between the client and server.

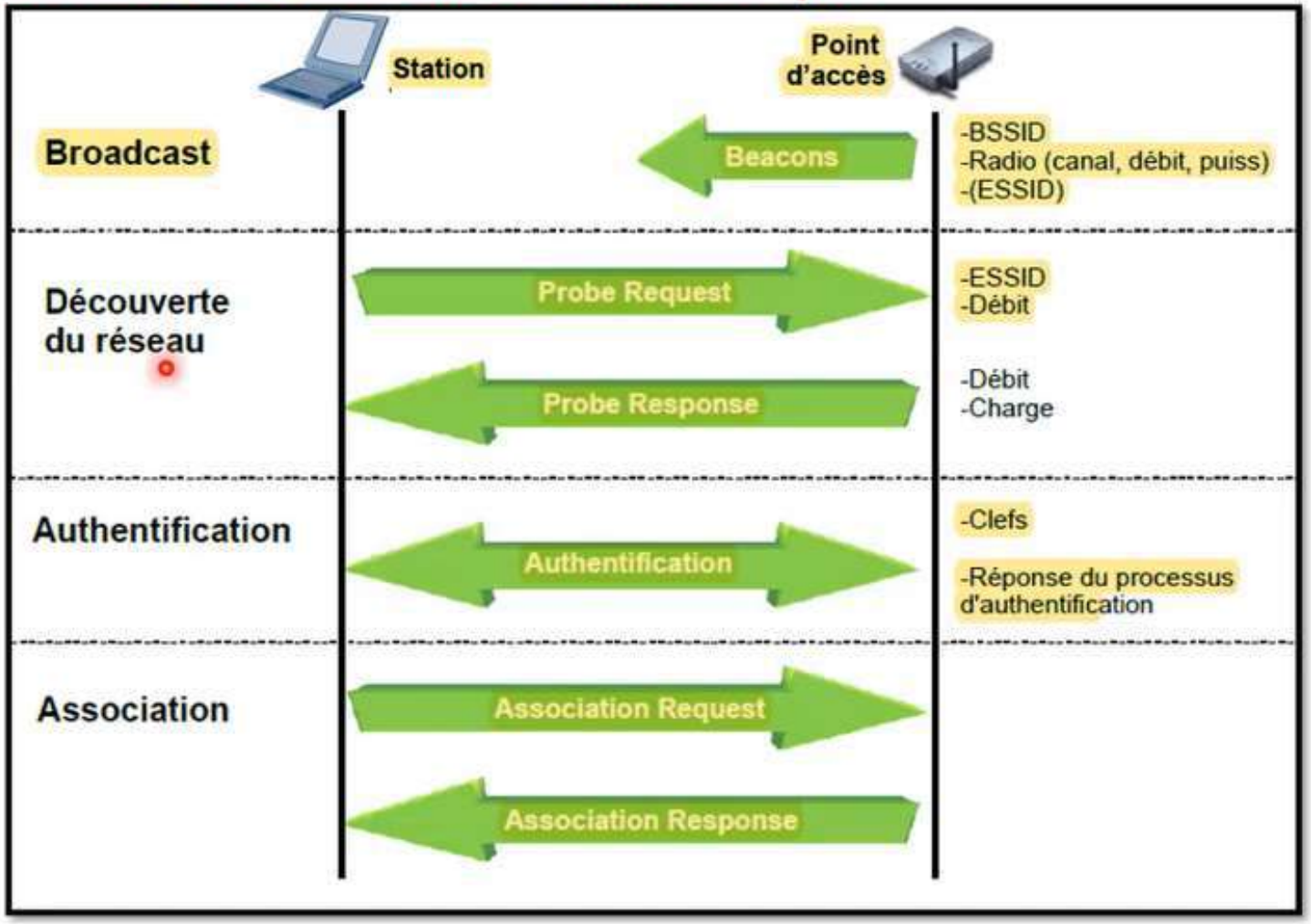


Association



1) Les modes et Mécanismes d'association :

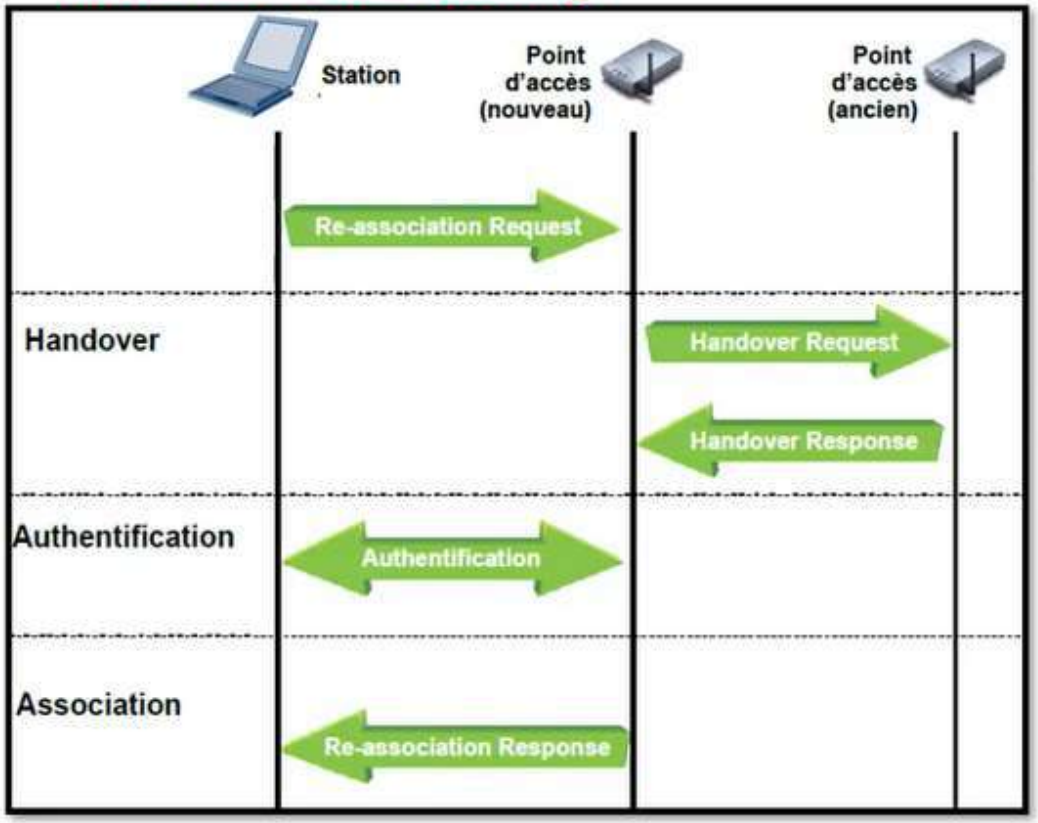
Mécanisme ou Processus d'accès au Réseau sans fil:

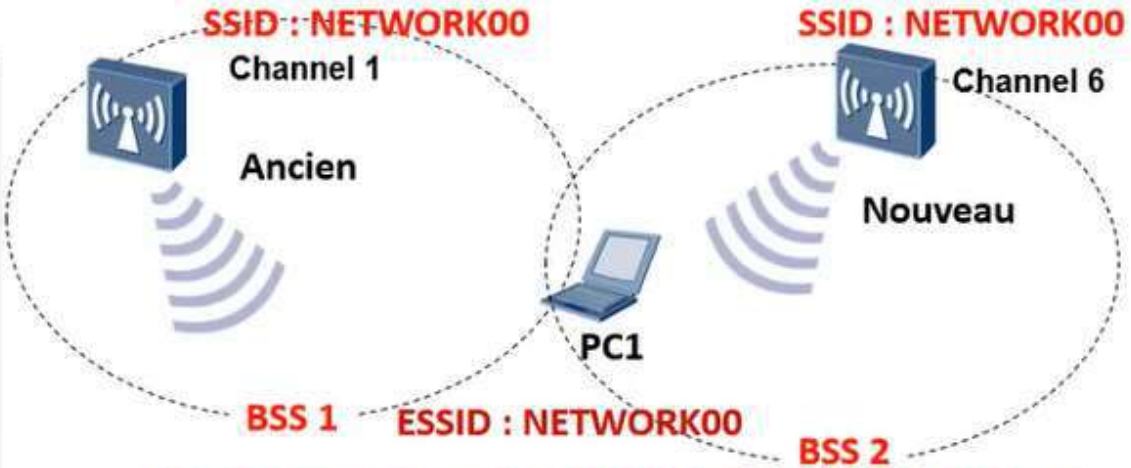


1) Les modes et Mécanismes d'association :

Mécanisme ou Processus d'accès au Réseau sans fil:

Mécanisme de roaming :





L'indicateur d'intensité du signal reçu (RSSI) et AP load

2) Le mécanisme de transfert de données :

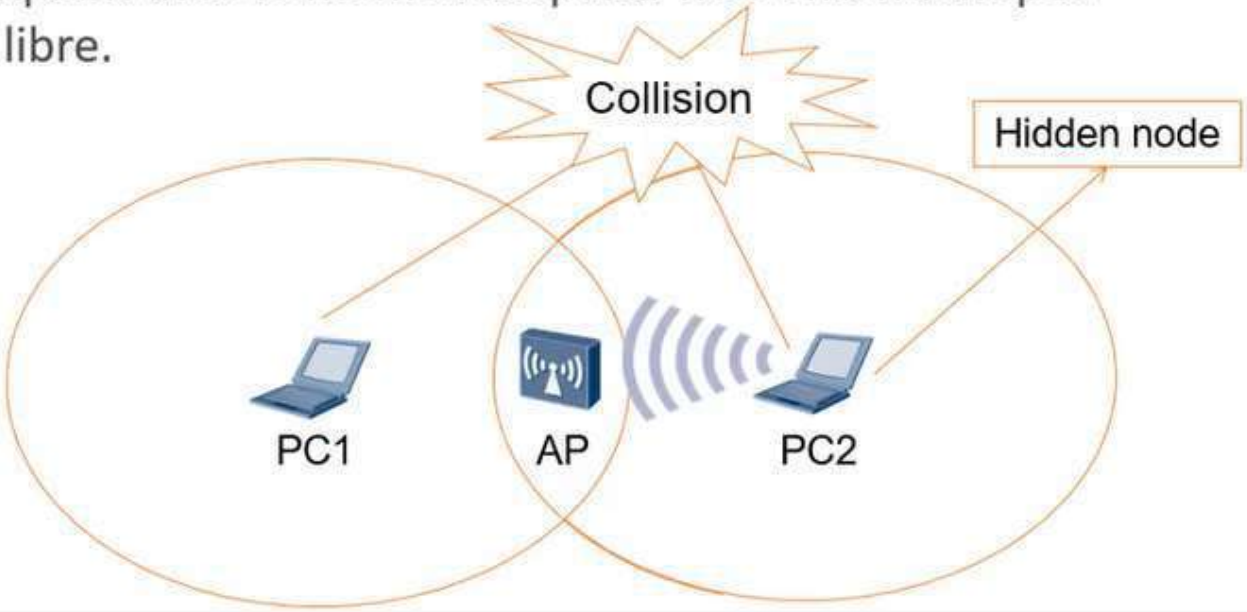
Inspiré du CSMA/CD de l'Ethernet :

Carrier Sense Multiple Access with Collision Detect

- ✓ Chaque machine est libre de communiquer à n'importe quel moment.
- ✓ Elle vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine.
- ✓ Autrement elles patientent pendant un temps aléatoire avant de recommencer à émettre.

Mais en WiFi, deux stations communiquant avec le même récepteur ne s'entendent pas forcément pour savoir si le media est libre.

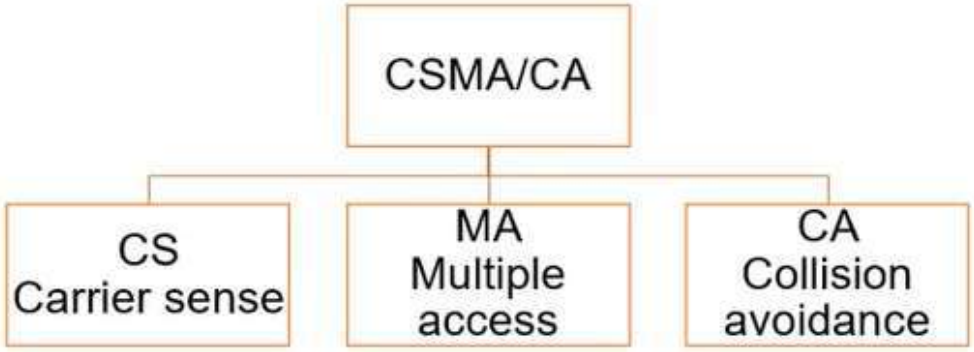
La solution :
CSMA/CA



2) Le mécanisme de transfert de données :

CSMA/CA :

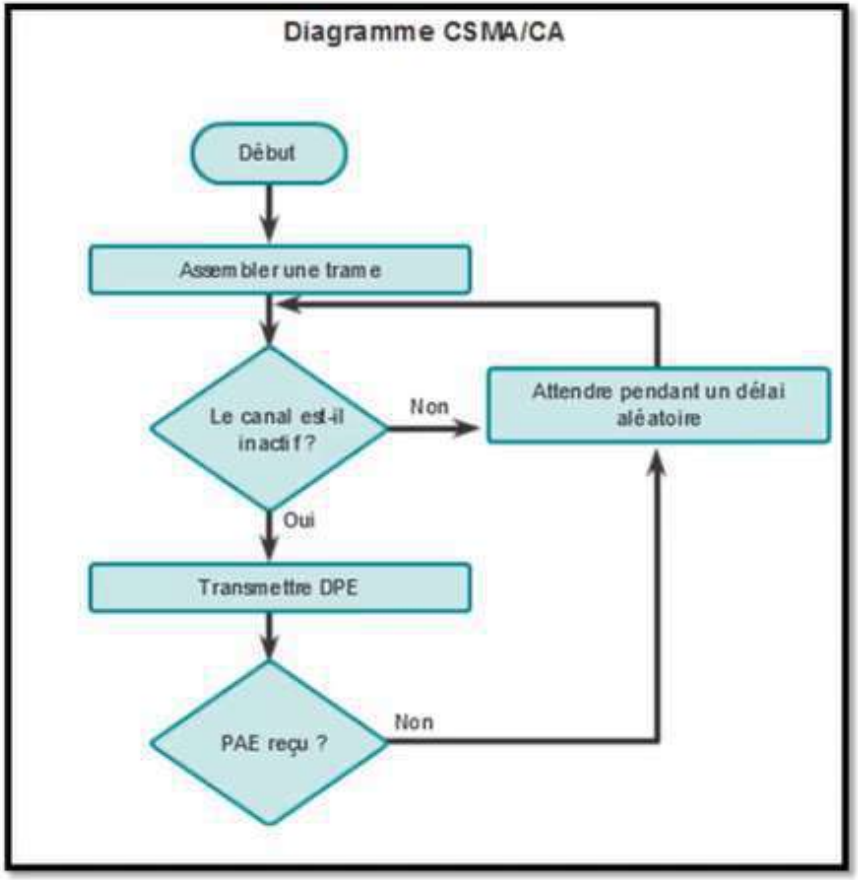
- ✓ Carrier Sense Multiple Access with Collision Avoidance incluse dans la fonction **DCF (Distributed Coordination Function)** de la couche MAC du 802.11
- ✓ Utilise un mécanisme d'esquive de collision basé sur l'accusé de réceptions réciproques entre l'émetteur et le récepteur.



2) Le mécanisme de transfert de données :

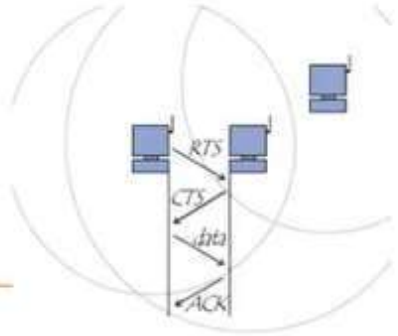
CSMA/CA

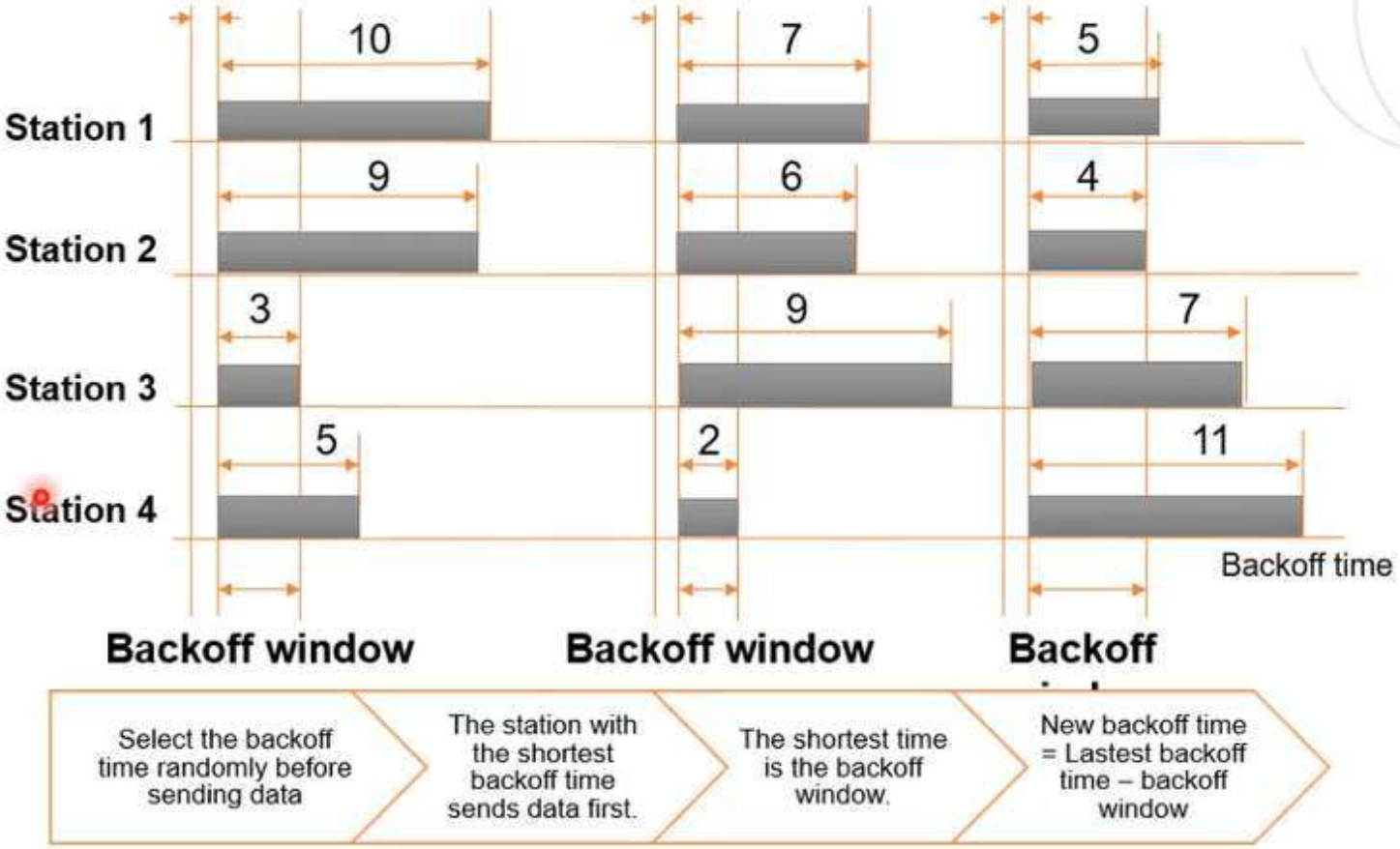
- La station voulant émettre écoute le réseau.
- Si le réseau est encombré, la transmission est différée.
- Si le média est libre, la station transmet **un message RTS (Ready To Send)** avec les informations sur le **volume de données et sa vitesse de transmission**.
- Le récepteur répond par un message **CTS (Clear To Send)** que reçoivent toutes les stations.
- La station effectue l'émission des données.
- A réception de toutes les données, le récepteur envoie un **ACK** (accusé de réception).
- Toutes les stations voisines patientent alors pendant le temps calculé à partir du CTS.



2) Le mécanisme de transfert de données :

CSMA/CA Working Mechanism:





Distributed Coordination Function

DCF

- méthode d'accès générale pour le transfert de données asynchrones, sans gestion de priorité
- repose sur le CSMA/CA

Le CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance

- accès aléatoire avec écoute de la porteuse : évite plusieurs transmissions simultanées, réduit le nombre de collisions
- impossible de détecter les collisions : il faut les éviter
  - écoute du support
  - back-off
  - réservation
  - trames d'acquittement positif

Distributed Coordination Function

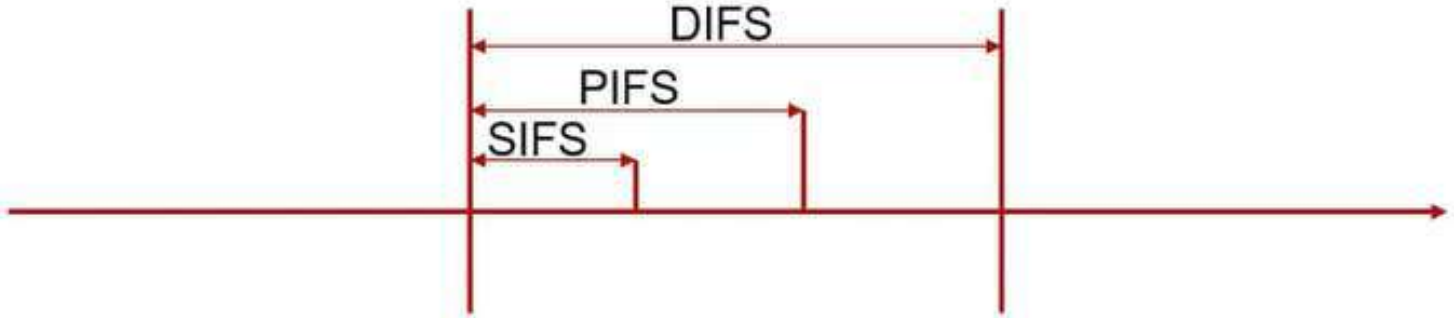
L'écoute du support

- Couche PHY : *Physical Carrier Sense* (PCS)
  - détecte et analyse les trames
  - fait appel au PLCP (Physical Layer Convergence Protocol)
- Couche MAC : *Virtual Carrier Sense* (VCS)
  - réserve le support via le PCS
  - deux types de mécanismes :
    - réservation par trames RTS/CTS
    - utilisation d'un timer (NAV : Network Allocation Vector) calculé par toutes les stations à l'écoute
  - utilisation optionnelle : trames RTS/CTS à 1 Mbits/s, font chuter le débit moyen de 11 Mbits/s à 6 Mbits/s

2) Le mécanisme de transfert de données :

InterFrame Space

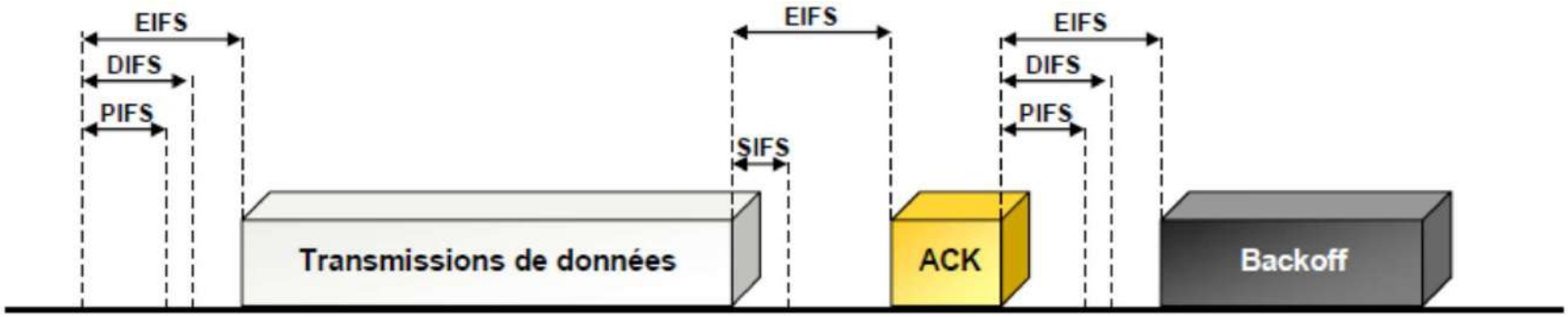
SIFS	PIFS	DIFS
Shortest waiting time, highest priority	Intermediate waiting time, intermediate priority	Longest waiting time, lowest priority



Distributed Coordination Function

L'accès au support

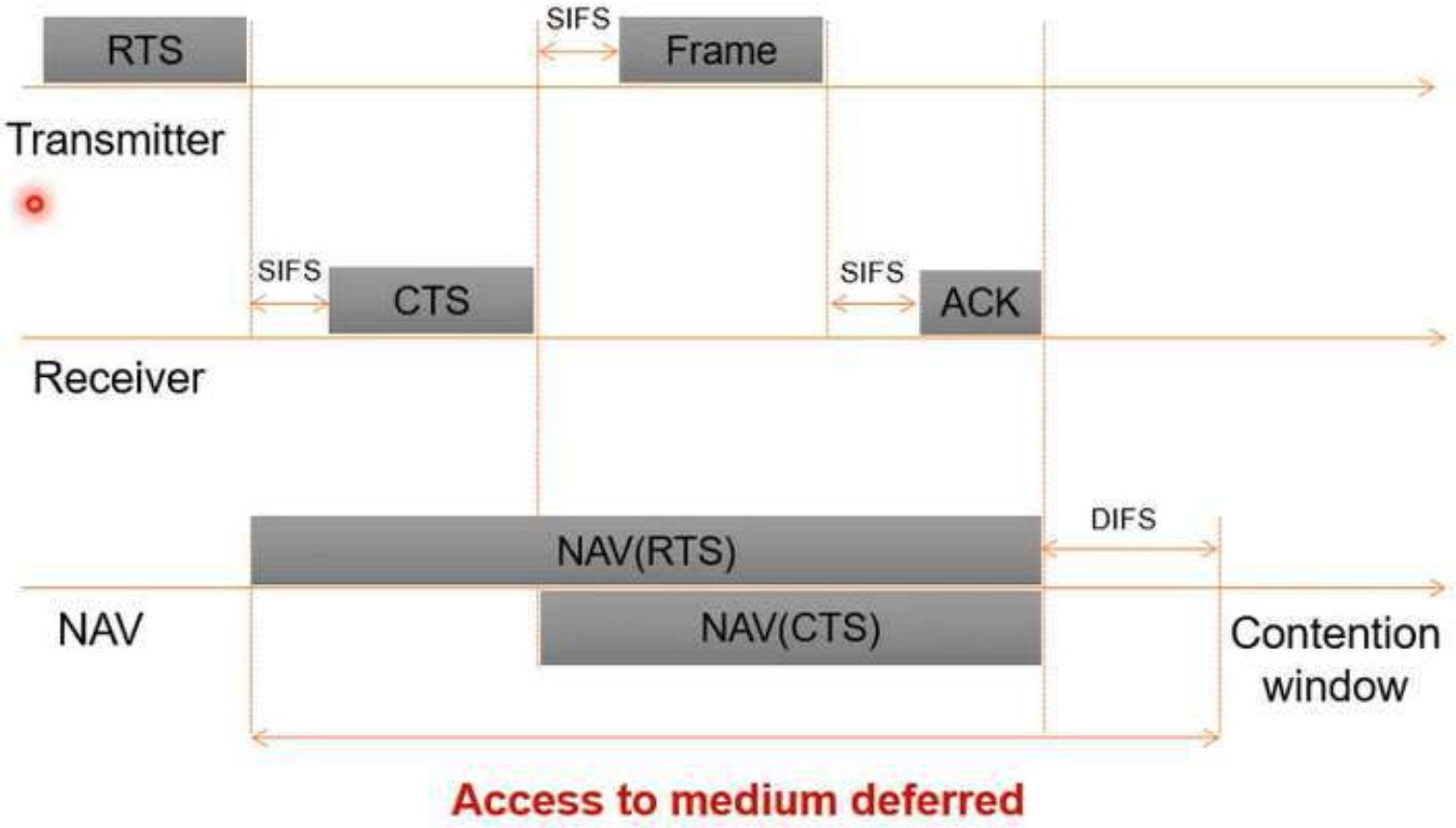
- mécanisme d'espacement entre deux trames : IFS
- 4 types d'*Inter-Frame Spacing* :
  - **SIFS : *Short IFS*** : sépare les différentes trames d'un même dialogue (données et ACK, RTS et CTS, différents fragments d'une trame segmentée, trame de polling en mode PCF)
  - **PIFS : PCF IFS** = SIFS + 1 timeslot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



2) Le mécanisme de transfert de données :

RTS/CTS with CSMA/CA

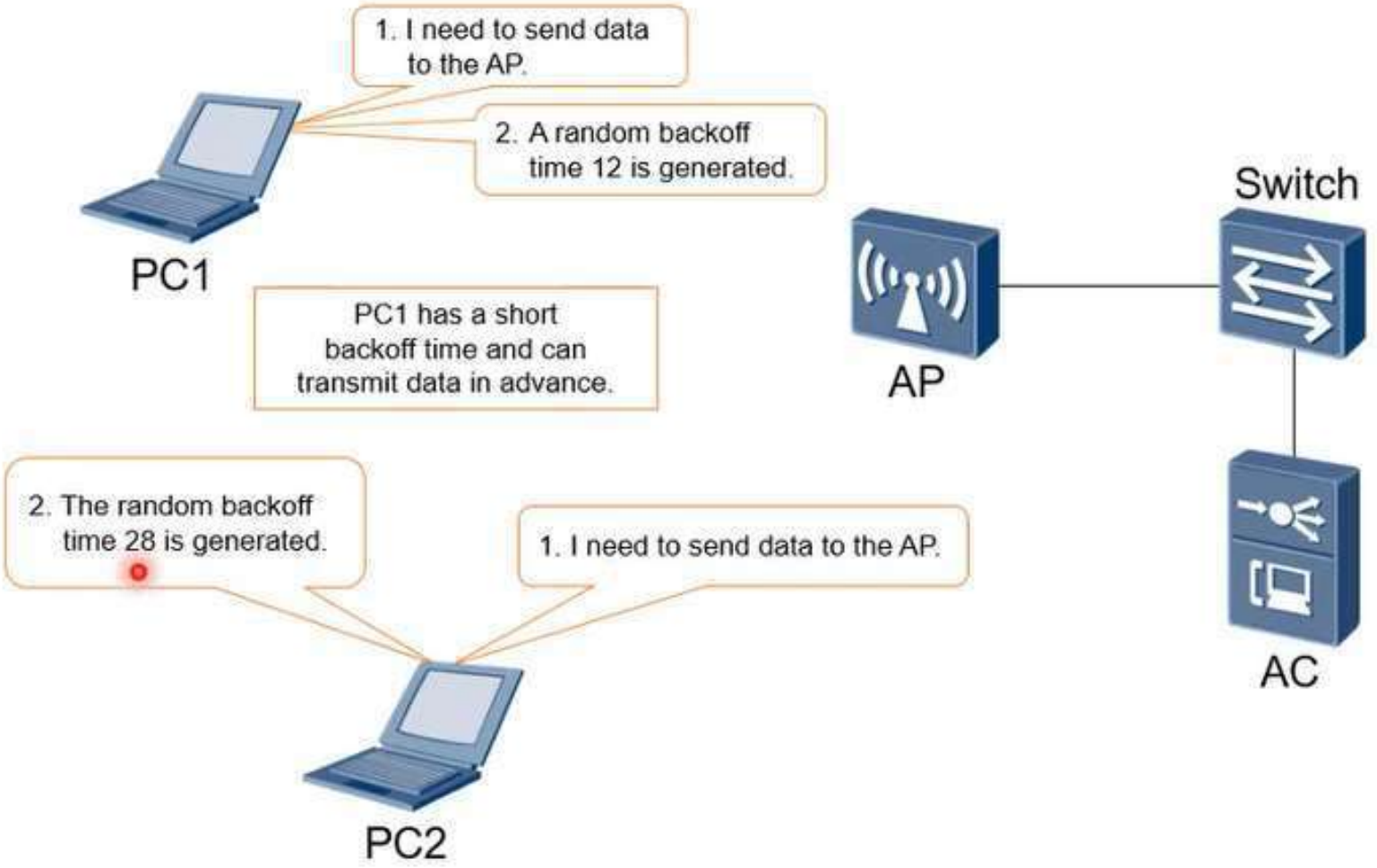
Network Allocation Vector (NAV)



Access to medium deferred

2) Le mécanisme de transfert de données :

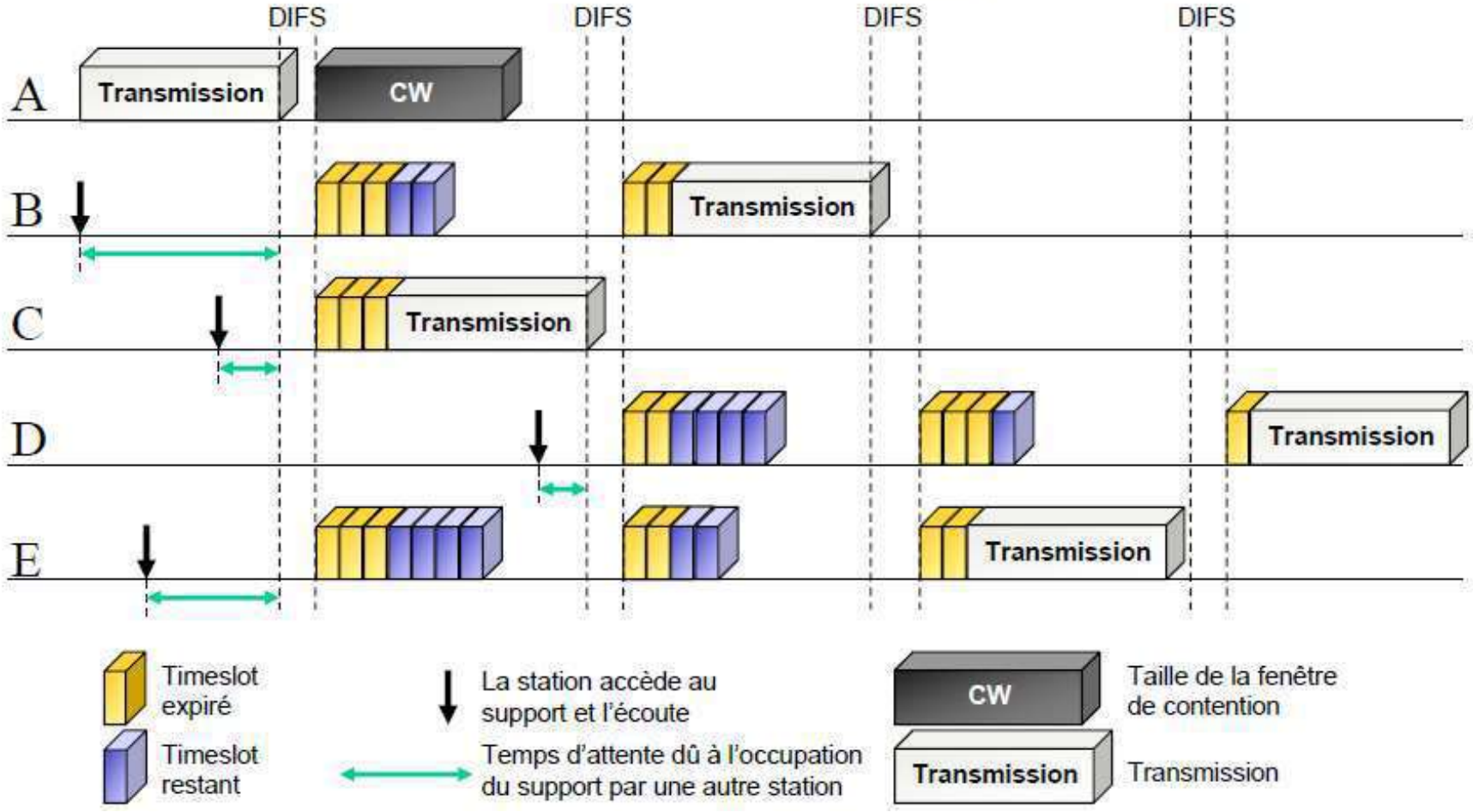
Exemple de transfert de trames



Distributed Coordination Function

Le *back-off*

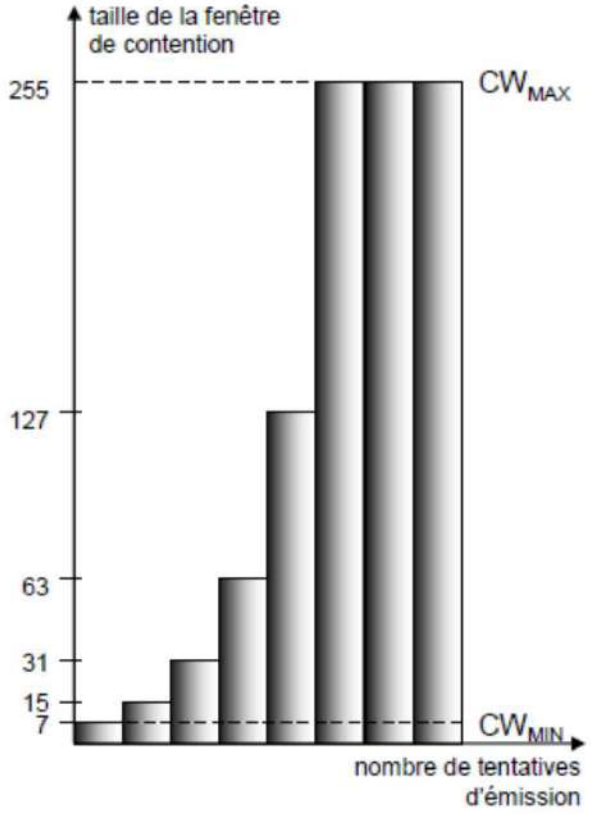
- fenêtre de contention CW, et un *timer* $T_{backoff}$=random(0,CW)×timeslot



Distributed Coordination Function

La contention

- en cas de collision la fenêtre de contention CW est doublée



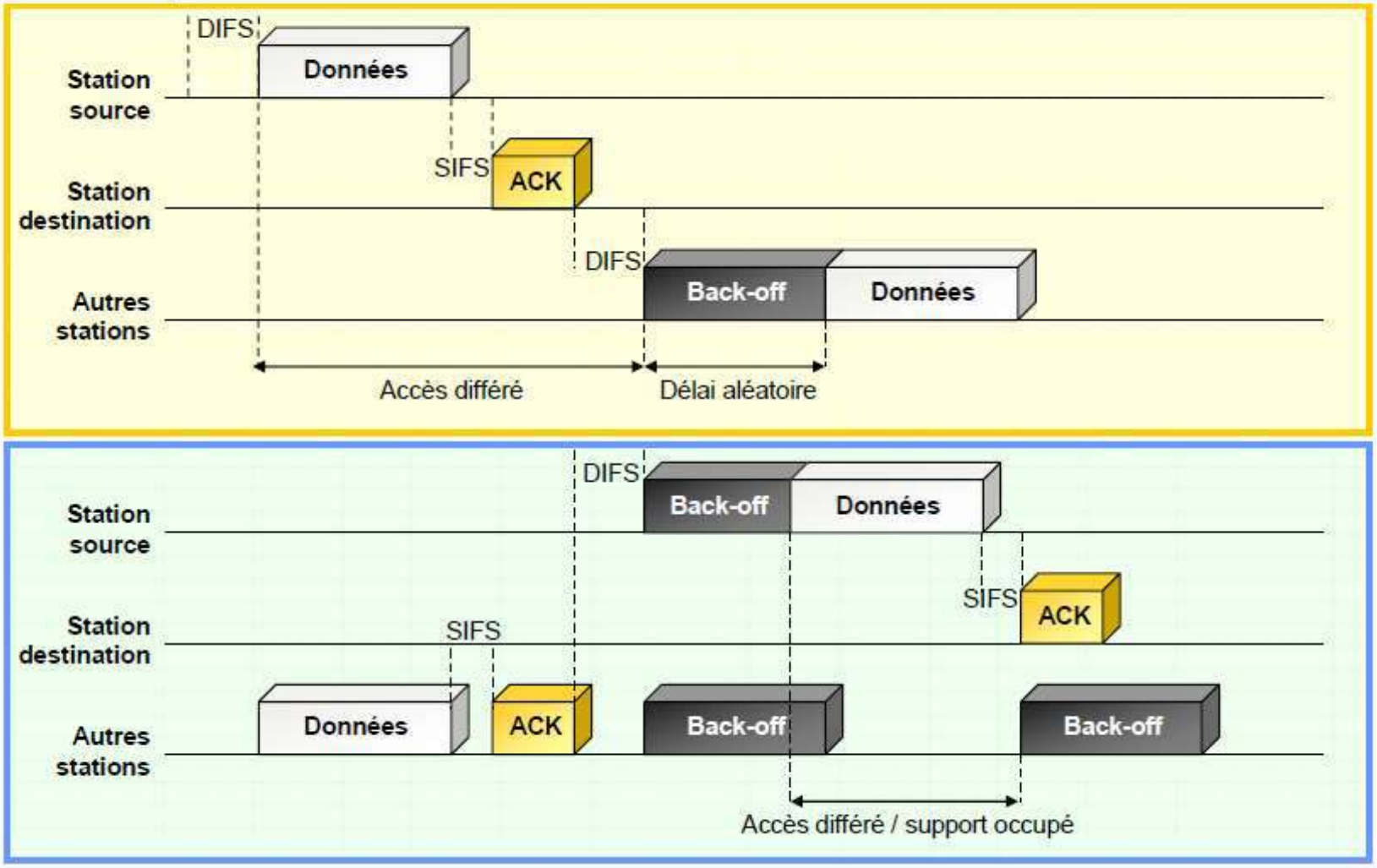
- le tirage au sort de la durée d'attente s'effectue sur un intervalle plus grand
- deux stations qui sont entrées en collision ont une probabilité plus faible mais non nulle d'entrer à nouveau en collision
- $n^{ième}$ tentative de transmission :

$$T_{backoff}(i) = random(0, CW_i) \times timeslot$$

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

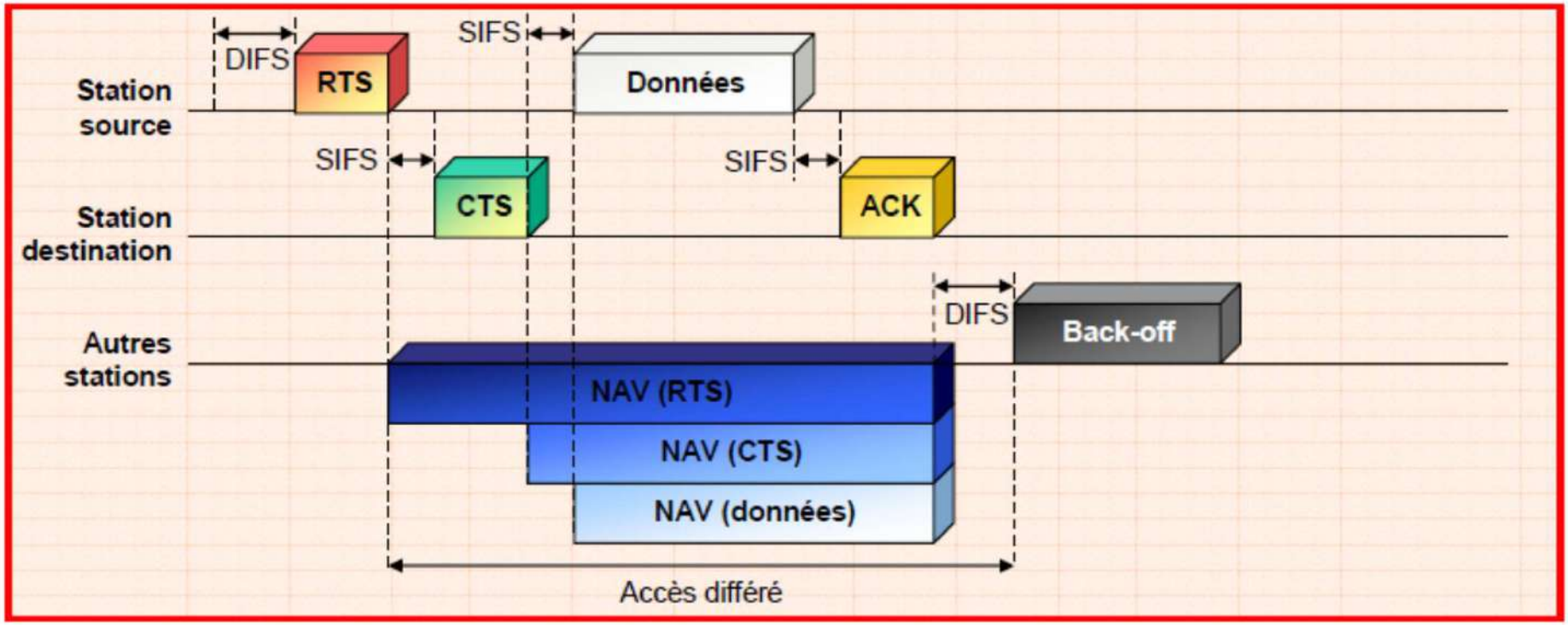
Distributed Coordination Function

Exemples de transmissions



Distributed Coordination Function

Exemples de transmissions avec réservation



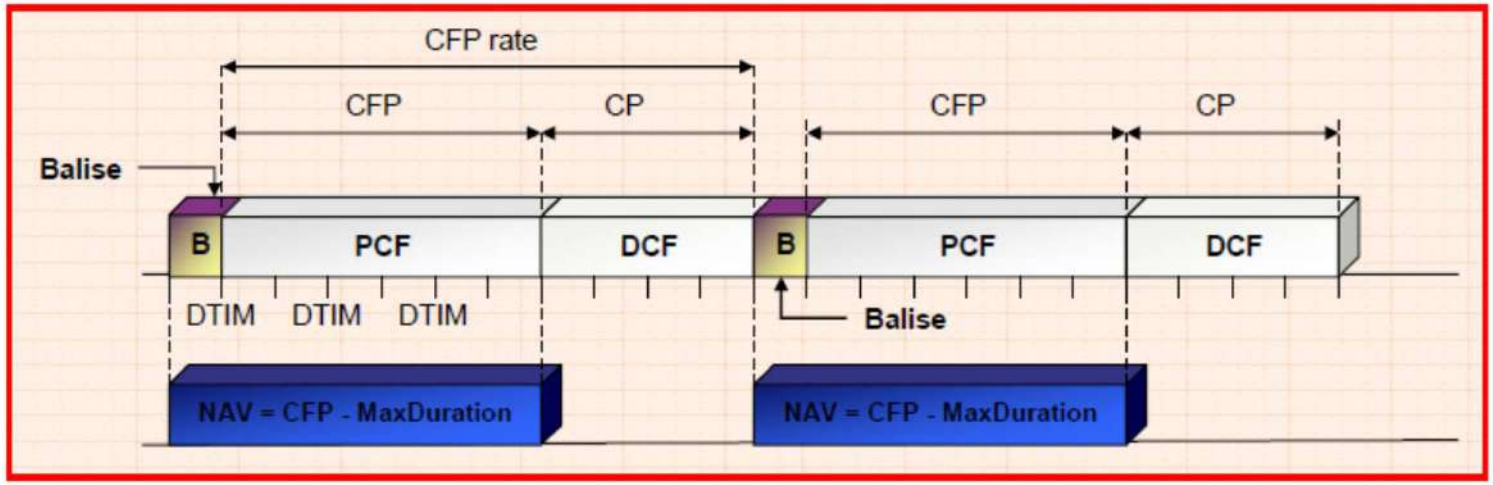
Point Coordination Function

PCF

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

Contention

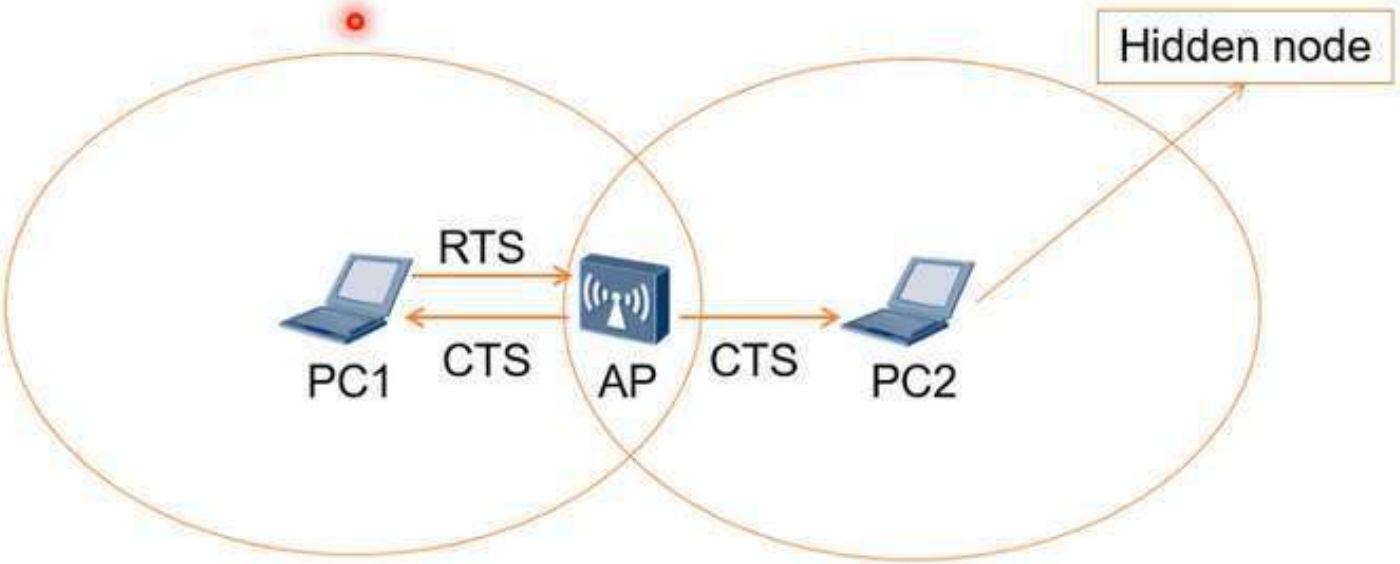
- l'AP définit un PC (Point Coordination) avec 2 périodes :
  - CP (*Contention Period*) : période de temps avec contention et DCF
  - CFP (*Contention Free Period*) : période de temps sans contention et PCF



2) Le mécanisme de transfert de données :

Hidden Node (RTS/CTS):

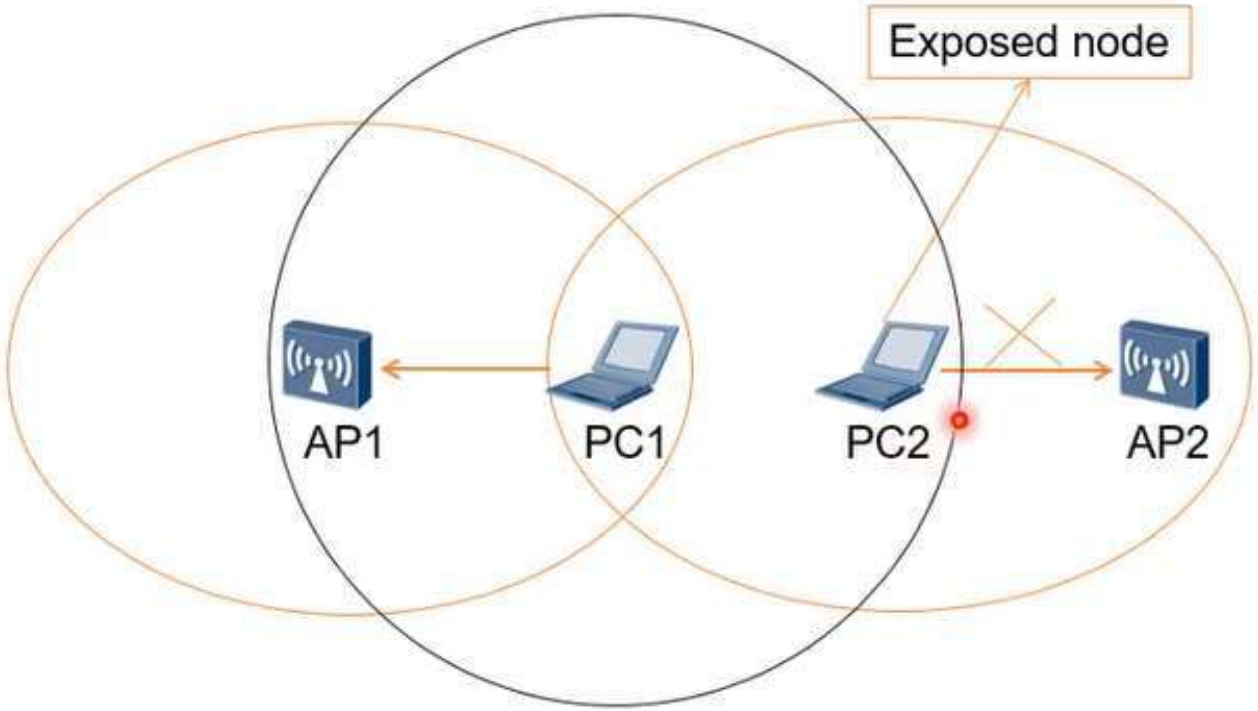
- A device can send RTS/CTS frames to reserve the transmission channel before sending data frames.



2) Le mécanisme de transfert de données :

Exposed Node :

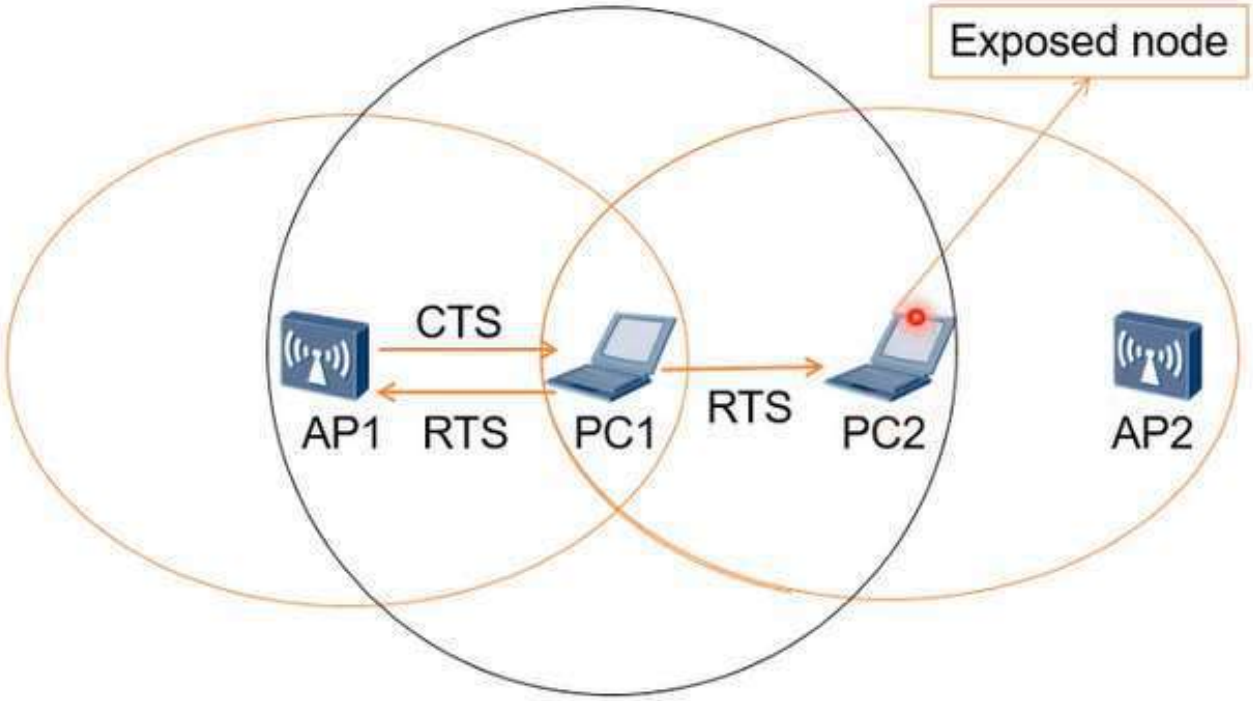
- An exposed node is within the communication range of the transmitter but out of the communication range of the receiver.



2) Le mécanisme de transfert de données :

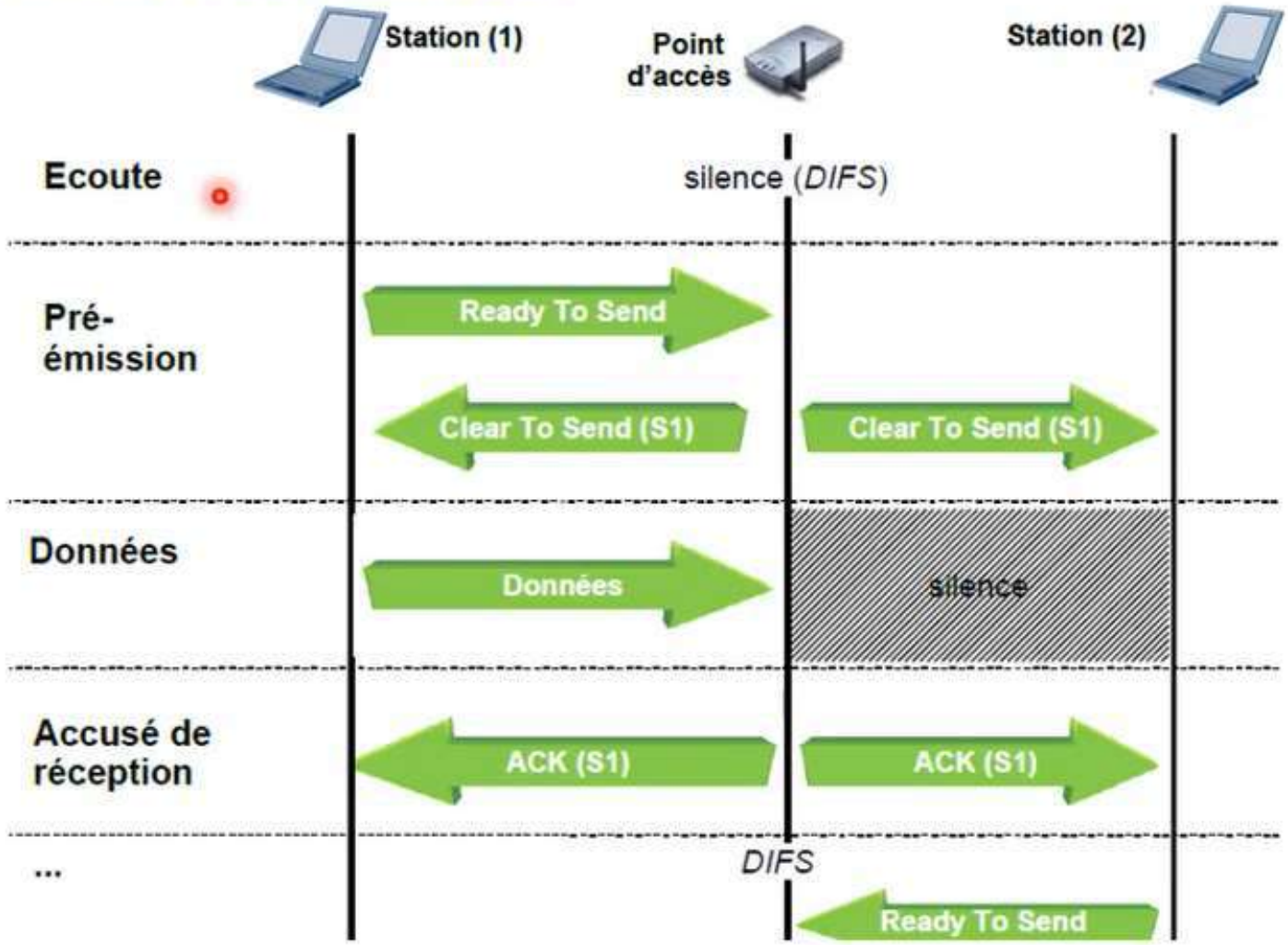
Exposed Node (RTS/CTS):

- A device can send RTS/CTS frames to prevent the collision before sending data frames.

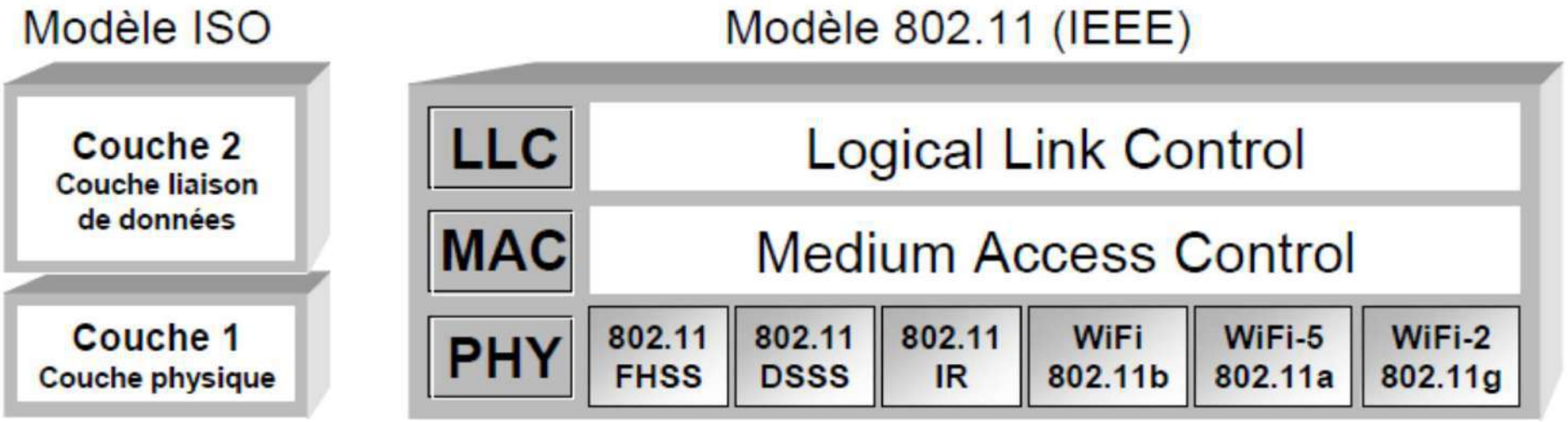


2) Le mécanisme de transfert de données :

Transfert de données



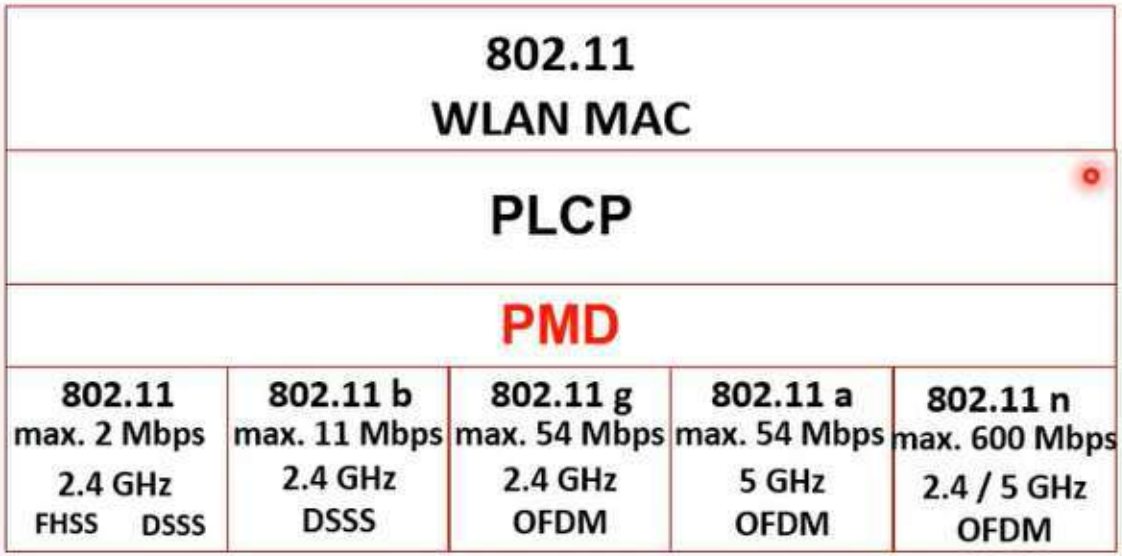
Architecture en couches



- Modèle IEEE : couche liaison de données subdivisée en deux sous-couche MAC et LLC
- Couche MAC commune à toutes les couches physiques

La couche physique : PHY

802.11 Physical Layer Overview

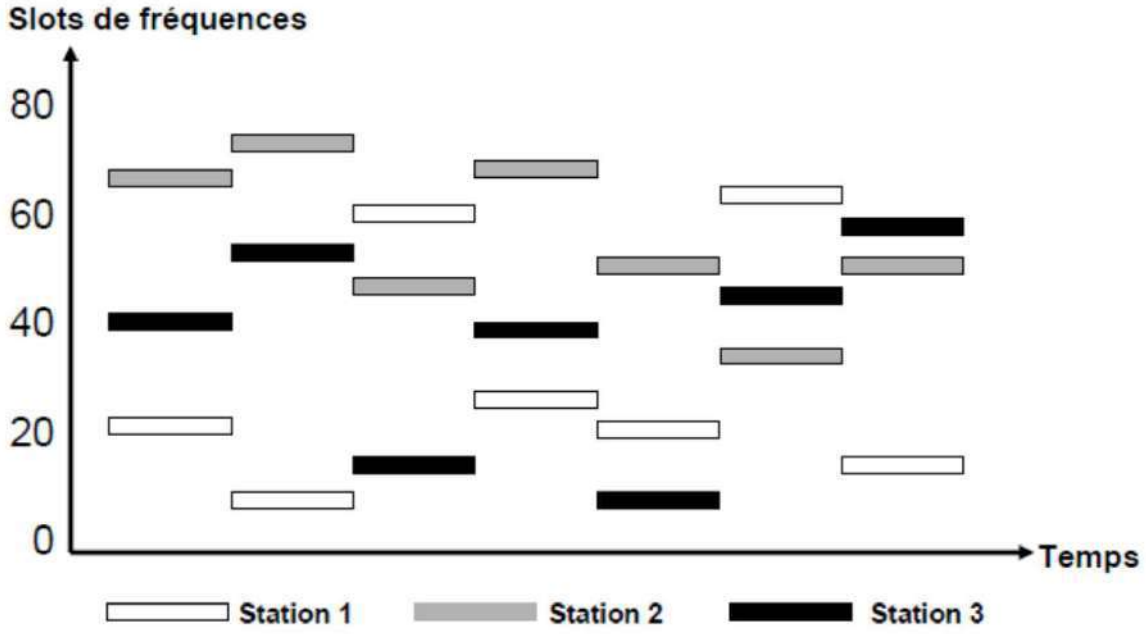


La couche physique est classée en deux sous-couches: **Physical Layer Convergence Procedure (PLCP)** et la procédure dépendant du support physique **Physical Medium Dependent (PMD).** PLCP mappe les trames MAC sur le support de transmission. PMD transporte les trames.

La couche physique : PHY

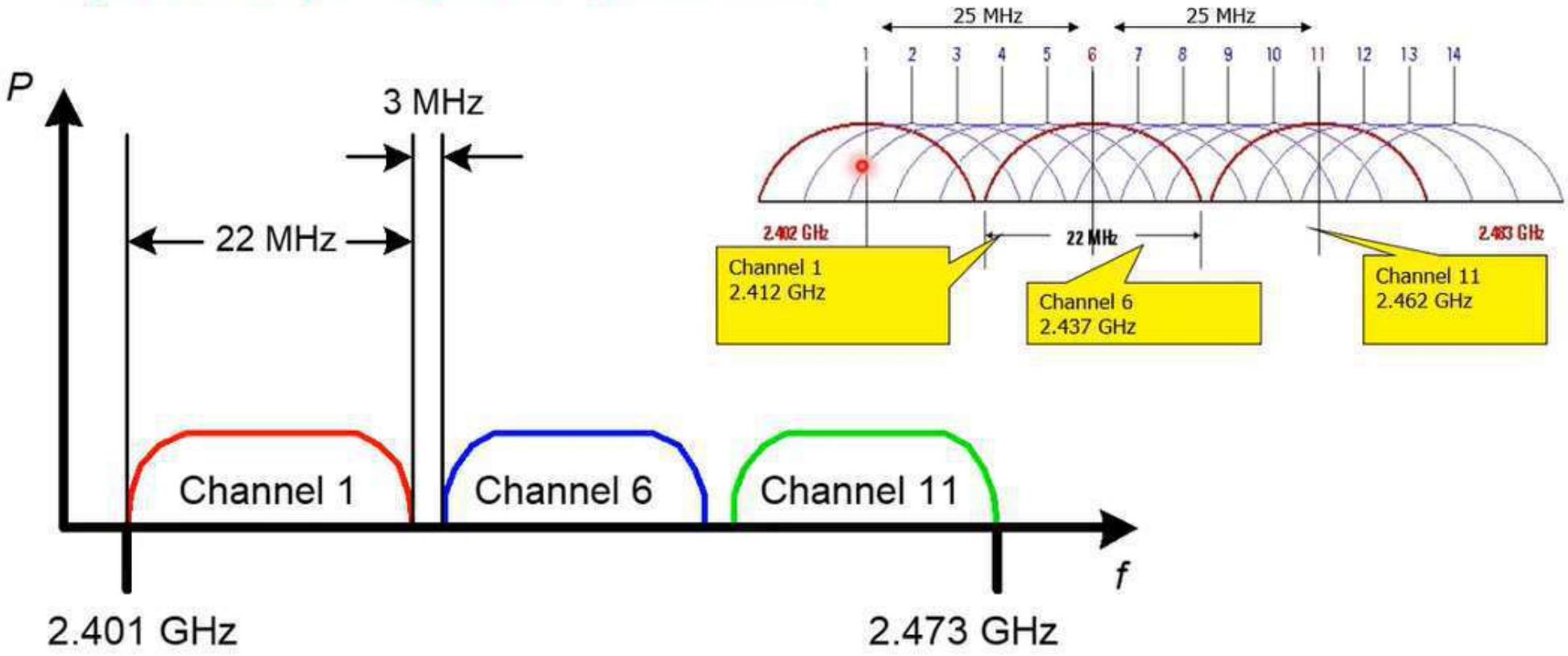
Frequency Hopping Spread Spectrum

- 79 canaux de 1 MHz de largeur de bande
- 3 ensembles de 26 séquences, soit 78 séquences de sauts possibles
- Exemple : 3 stations sur 7 intervalles de temps : émission simultanée mais pas sur le même canal



La couche physique : PHY

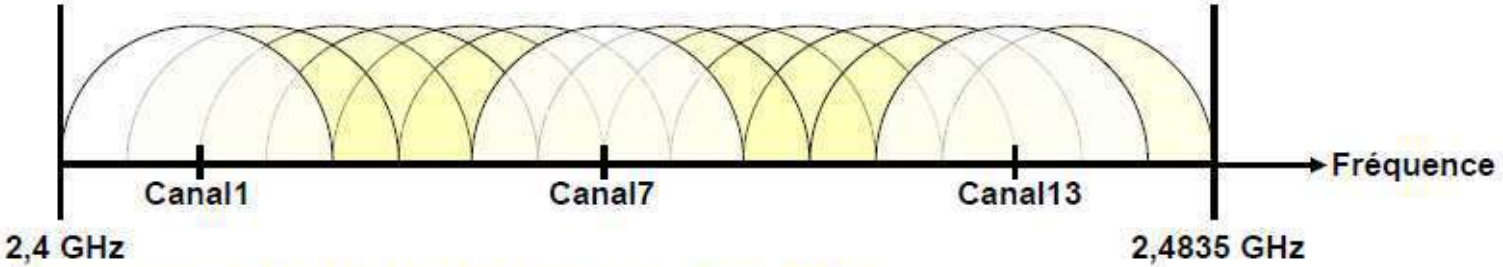
Physical Layer-Spread Spectrum :



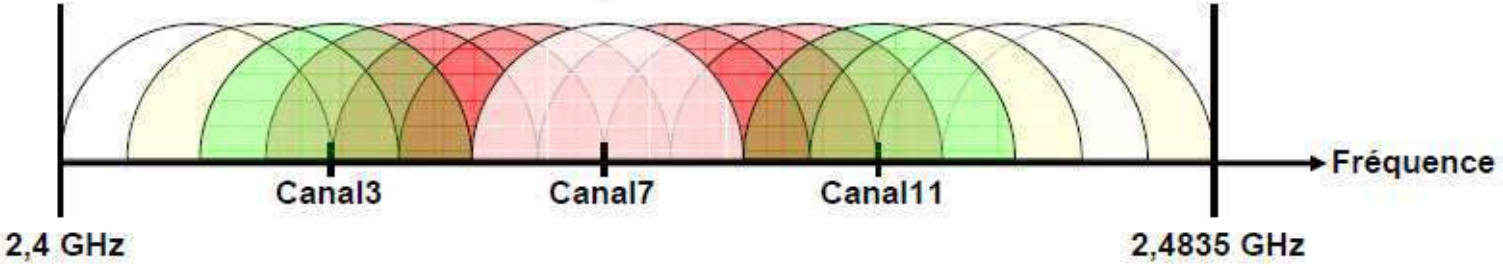
La couche physique : PHY

Direct Sequence Spread Spectrum

- Technique la plus répandue aujourd'hui : 802.11b
- 14 canaux de 20 MHz
- Fréquences crête espacées de 5 MHz
  - canal 1 = 2,412 GHz ; canal 14 = 2,477 GHz

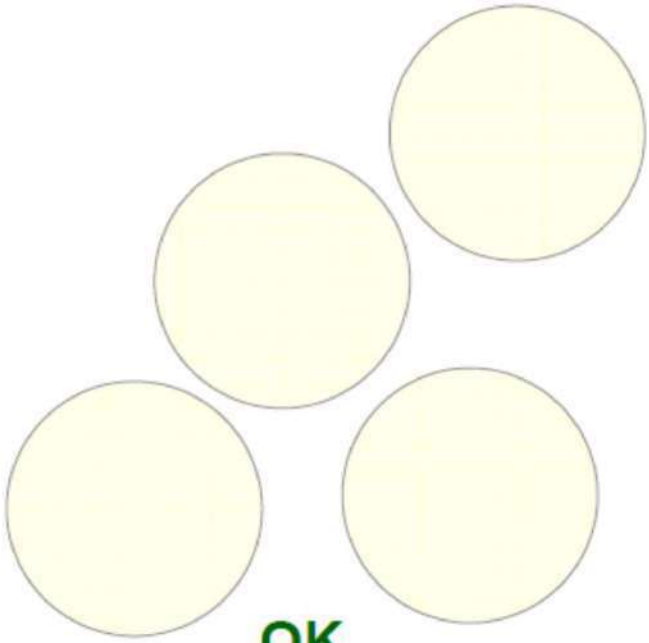


- Largeur totale de la bande = 83,5 MHz
- Canaux recouvrant : inexploitables simultanément

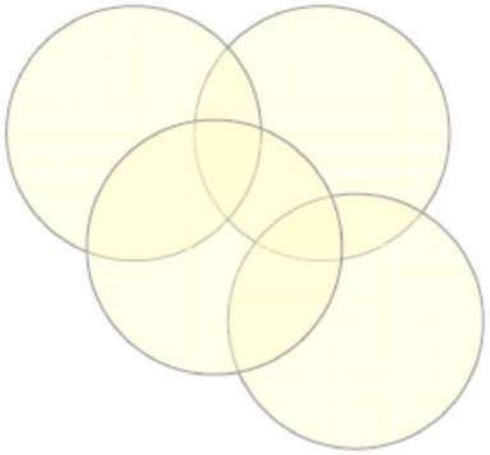


Affectation des canaux

- 14 canaux dans la bande ISM : 2,4 – 2,4835 GHz
- 4 canaux dans la bande 2,446 – 2,4835 GHz
- Affectation d'un canal unique ou de plusieurs canaux non recouvrant ne pose pas de problèmes



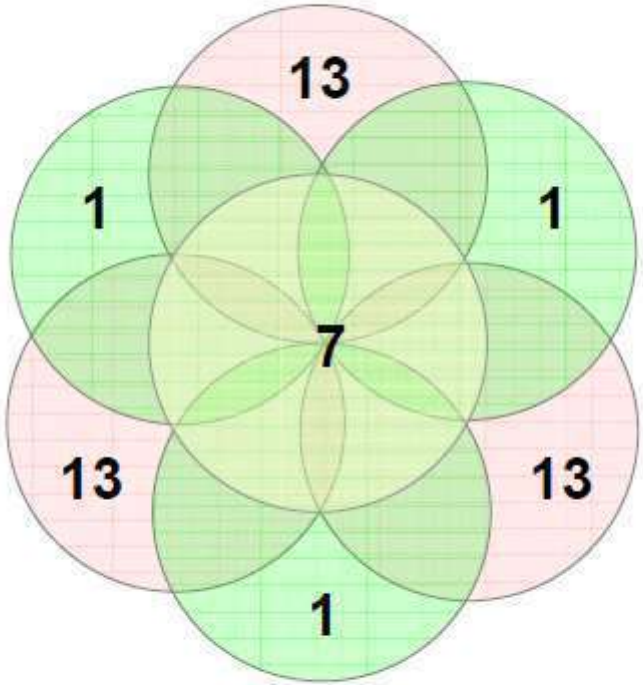
OK



Problème

Affectation des canaux

- Exemple d'affection à 7 points d'accès de 3 canaux qui ne se perturbent pas mutuellement :

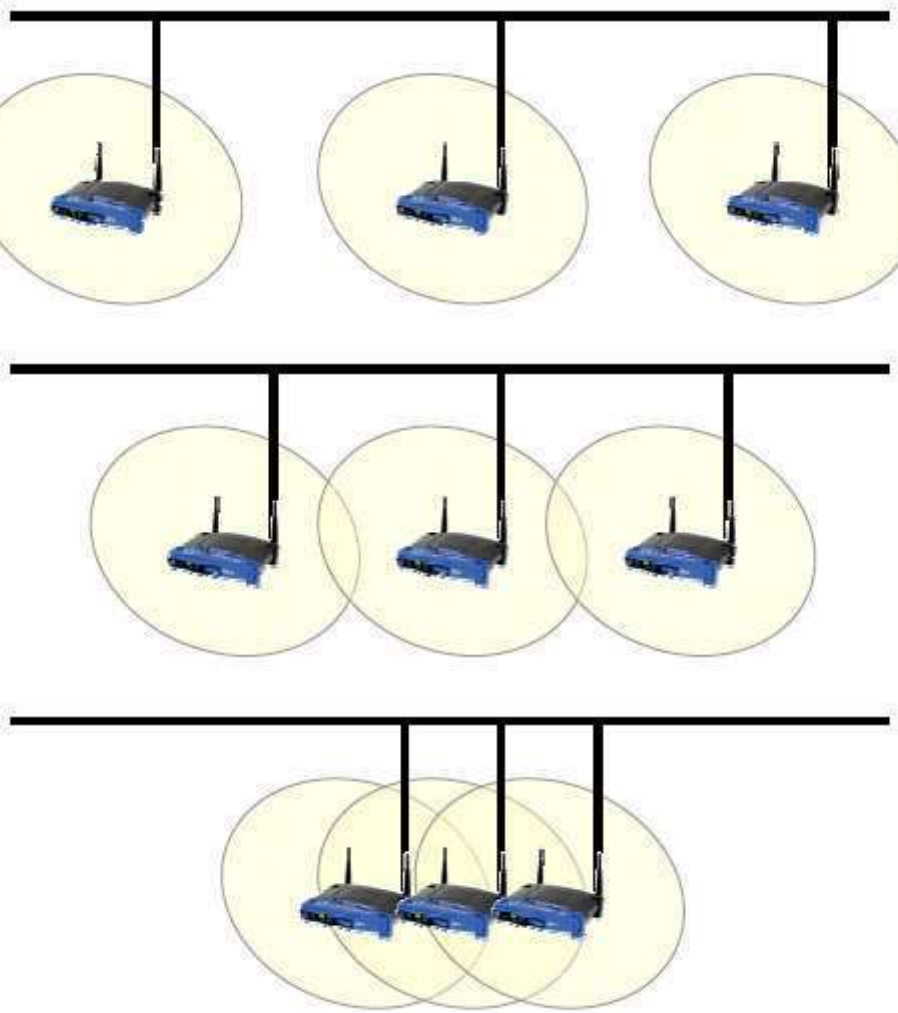


- Autre possibilité : 1, 6 et 11
- Même si on dispose de 14 canaux, seuls 3 peuvent être utilisés si on a plusieurs points d'accès

Affectation des canaux

- Puissance autorisée :
  - Totalité bande ISM : 10 mW ; taille cellule = 15 m
  - Canaux 10-13 : 100 mW ; taille cellule = 100 m
- Impossibilité de créer des réseaux WiFi important utilisant la topologie en « rosace »

Choix de la topologie



Wi Fi les cellules sont disjointes

- faible nombre de canaux
- pas d'interférence
- pas de mobilité

Wi Fi les cellules se recouvrent

- réseaux sans fils
- service de mobilité
- exploitation de l'espace
- gestion de l'affectation

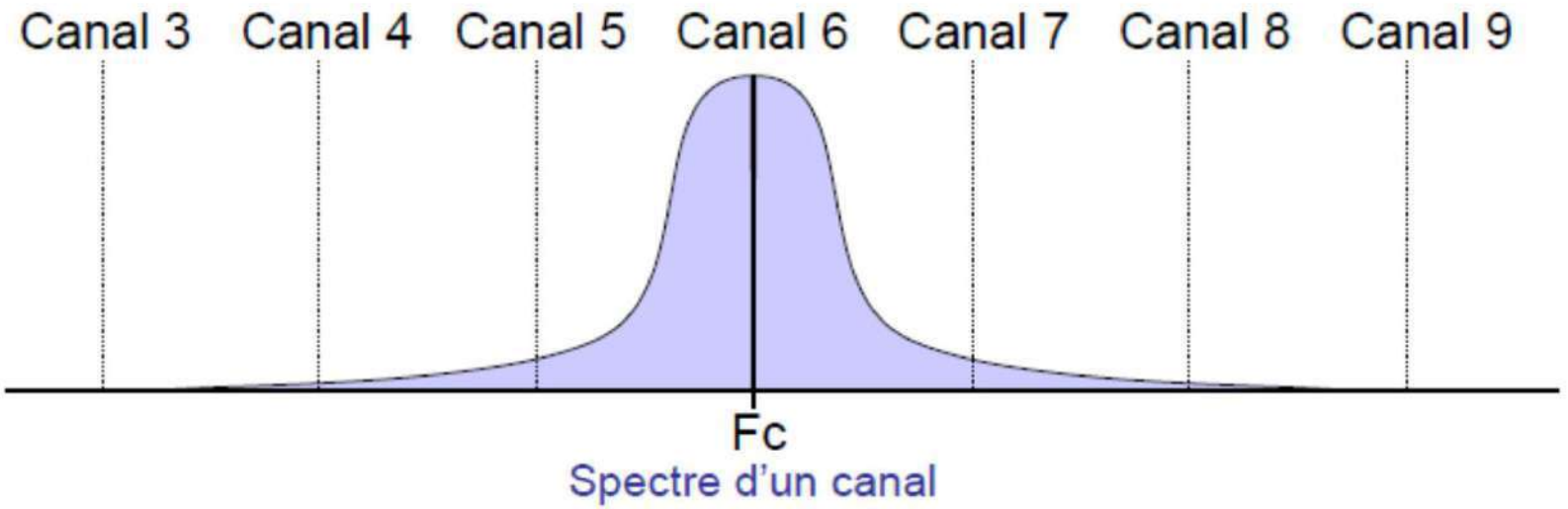
Wi Fi les cellules se recouvrent mutuellement

- configuration des canaux nécessaire
- nombre important d'utilisateurs

La couche physique : PHY

Direct Sequence Spread Spectrum

- Un seul canal utilisé par transmission : sensible aux interférences
- Plusieurs réseaux co-localisés doivent utiliser des canaux espacés de 25 à 30 MHz pour ne pas interférer



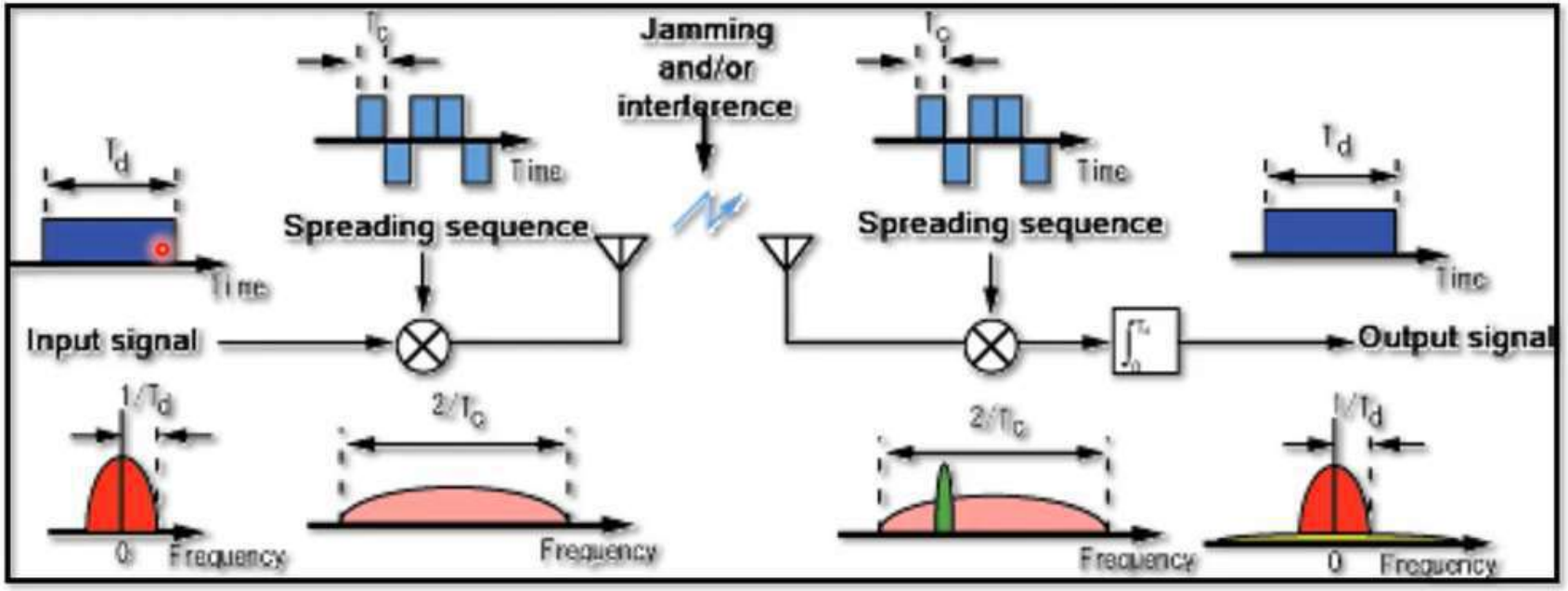
Spectre d'un canal

- La bande passante utilisée par un canal s'étale sur les canaux voisins

La couche physique : PHY

DSSS :

- DSSS: Direct Sequence Spread Spectrum
- DSSS spreads RF into a wide frequency band.



La couche physique : PHY

Méthode de Codage dans DSSS

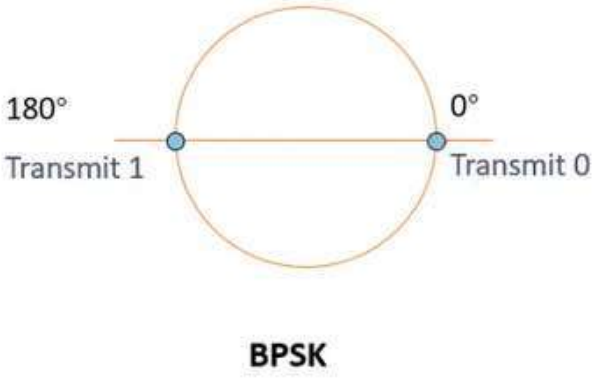
- DSSS utilise la séquence de Baker (11 chip)
- Le récepteur identifie l'information originale si au moins deux bits parmi 11 sont corrects,
- Tache : combattre les interférences
- Dans schéma suivant, la séquence transmise est 1010,

Transmitted data			
10110111000	01001000111	10110111000	01001000111
1	0	1	0

La couche physique : PHY

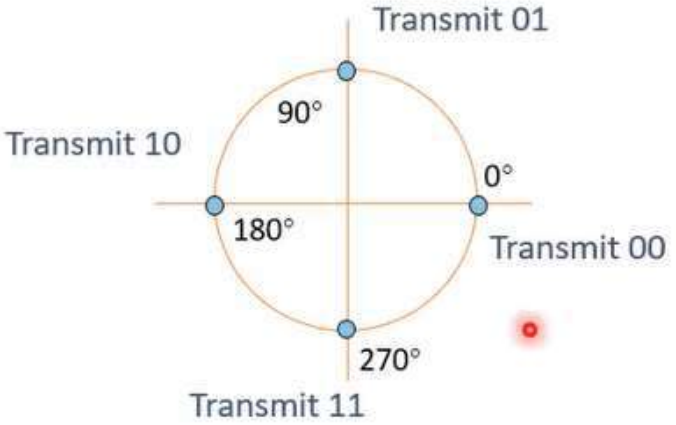
Modulation DSSS

- DSSS utilise deux types de modulation :



BPSK

Binary Phase Shift Keying



QPSK

Quadrature Phase Shift Keying

La couche physique : PHY

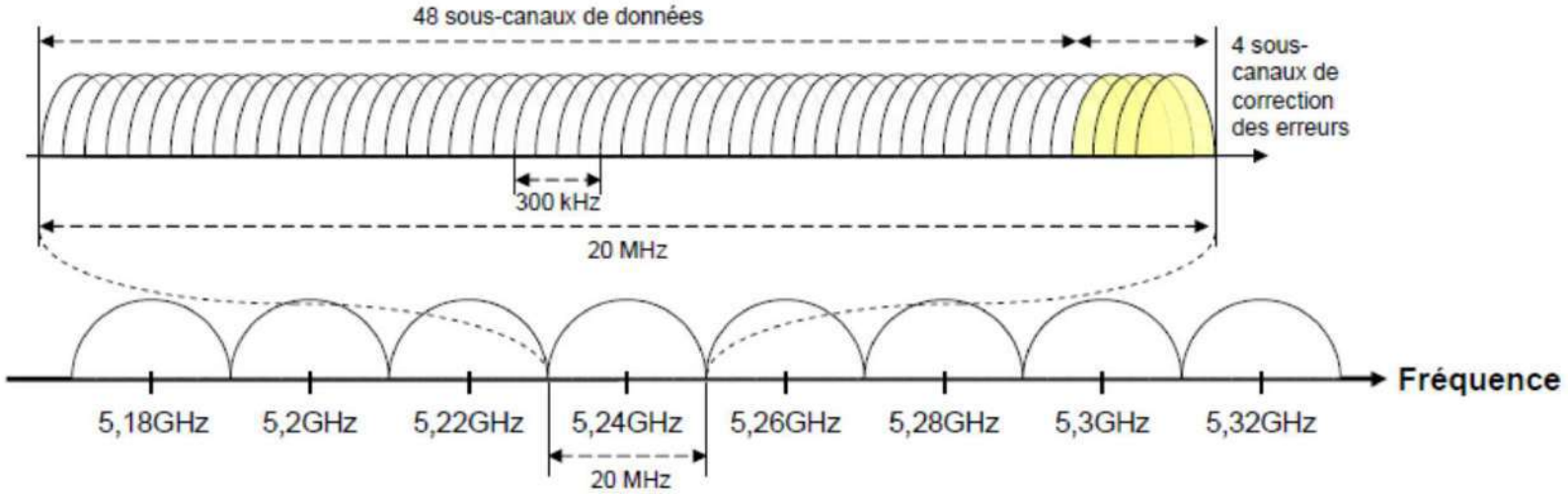
DSSS Coding

Data Rate	Coding Method	Modulation
1Mbps	Barker	BPSK
2Mbps	Barker	QPSK
5.5Mbps	4-bits CCK	QPSK
11Mbps	8-bits CCK	QPSK

La couche physique : PHY

Orthogonal Frequency Division Multiplexing

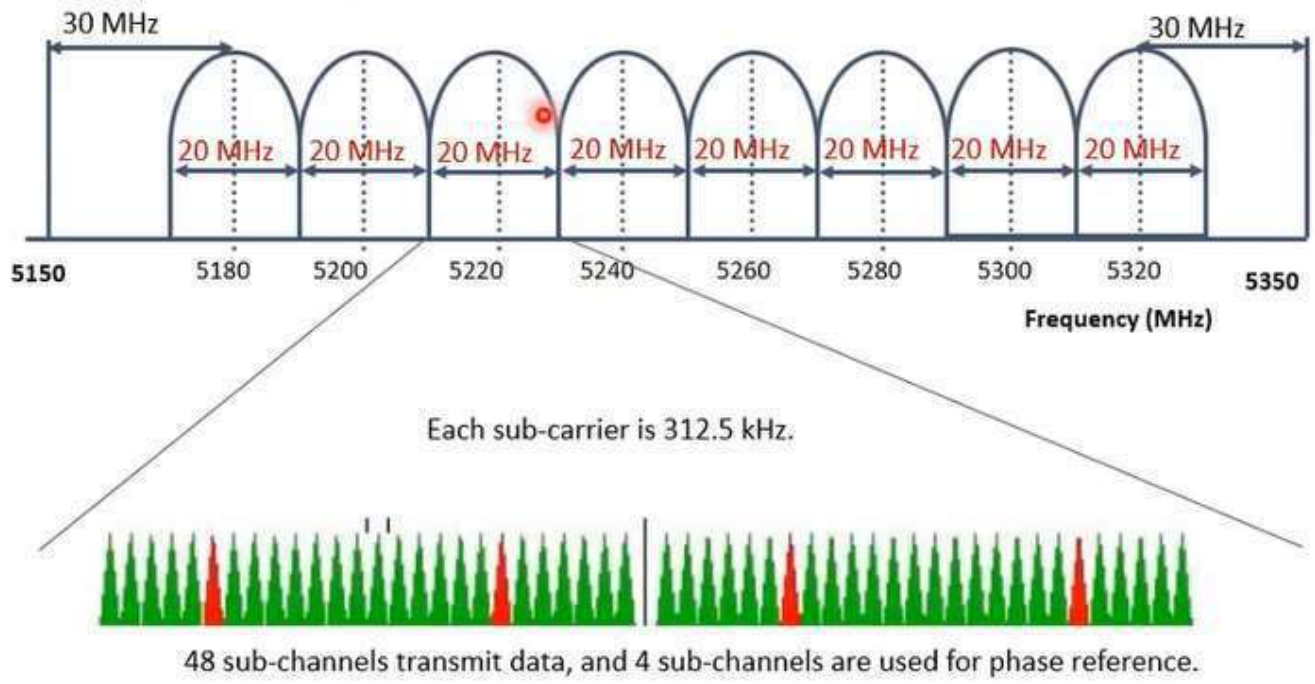
- bande U-NII (5 GHz)
- division des 2 premières sous-bandes en 8 canaux de 20 MHz
- chaque canal contient 52 sous-canaux de 300 kHz
- utilisation de tous les sous-canaux en parallèle pour la transmission
- débit de 6 à 54 Mbits/s :
  - modulation BPSK : 0,125 Mbits/s par sous-canal : total 6 Mbits/s
  - modulation QAM64 : 1,125 Mbits/s par sous-canal : total 54 Mbits/s



La couche physique : PHY

OFDM :

- OFDM 5 GHz channel:

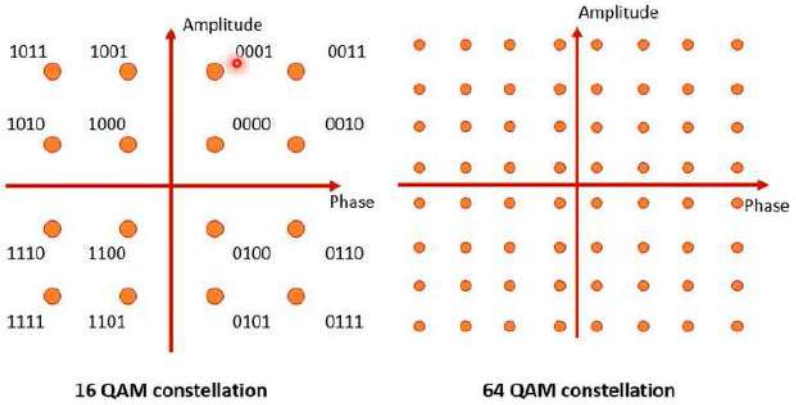


La couche physique : PHY

Sous-canaux et modulation OFDM

- OFDM modulation :
  - ❑ BPSK,
  - ❑ QPSK,
  - ❑ QAM
  - Combinée avec QAM, OFDM procure un débit pouvant atteindre 54 Mbit/s

802.11a Constellation



16 QAM constellation

64 QAM constellation

La couche physique : PHY

OFDM Modulation

Modulation Method	Data Rate (R)	Rate (Mbps)
BPSK	1/2	6
BPSK	3/4	9
QPSK	1/2	12
QPSK	3/4	18
16-QAM	1/2	24
16-QAM	3/4	36
64-QAM	2/3	48
64-QAM	3/4	54

La couche physique : PHY

Comparaison entre 802.11a/b/g/n

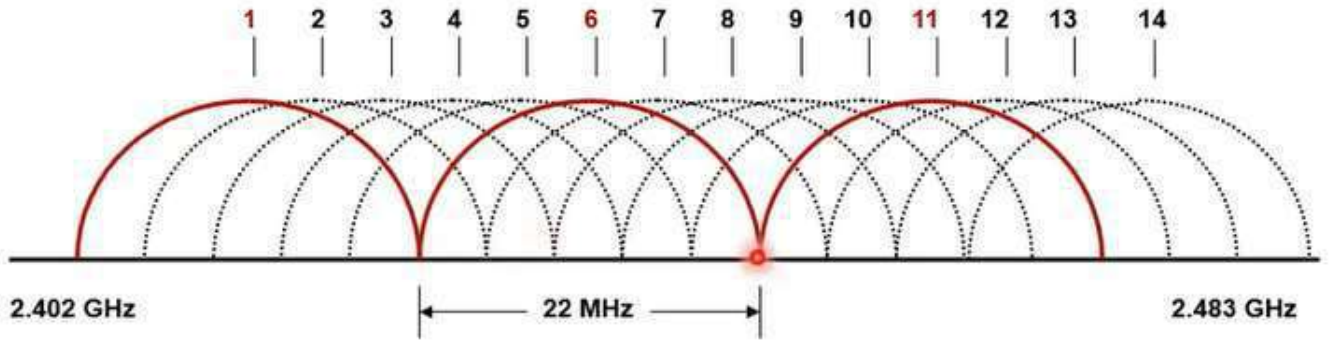
Standard	Frequency Band	Center Frequency Distance	Carrier Modulation	Highest Rate
802.11b	2.4-2.4835G	5M/Ch	DSSS	11 Mbps
802.11g	2.4-2.4835G	5M/Ch	DSSS OFDM	54 Mbps
802.11a	5.15-5.25G 5.25-5.35G 5.728-5.825G	5M/Ch	OFDM	54 Mbps
802.11n	2.4-2.4835G 5.15-5.25G 5.25-5.35G 5.728-5.825G	5M/Ch	MIMO& OFDM	600 Mbps

La couche physique : PHY

- La norme 802,11a :
  - Capacité : 54 Mbit/s,
    - Utilise OFDM,
    - Débit : 6, 9, 12, 18, 24, 36, 48 et 54 Mbit/s,
    - Bande 5 GHz (U-NII)
  - 23 canaux sans chevauchement

La couche physique : PHY

- La norme 802,11b :
  - ❑ Capacité : 11 Mbit/s,
    - ➢ Utilise DSSS,
    - ➢ Débit : 1, 2, 5.5 et 11 Mbit/s,
    - ➢ Bande 2,4 GHz (ISM)
  - ❑ 14 canaux :
    - ➢ 3 canaux sans chevauchement



La couche physique : PHY

- La norme 802,11g :
  - ❑ Capacité : 54 Mbit/s,
    - ➢ Utilise OFDM,
    - ➢ Débit : 6, 9, 12, 18, 24, 36, 48 et 54 Mbit/s et les débits supportés par 802,11b,
    - ➢ Compatible avec 802,11b,
    - ➢ Bande 2,4GHz (ISM),
  - ❑ 13 canaux :
  - ➢ 3 sans chevauchement,

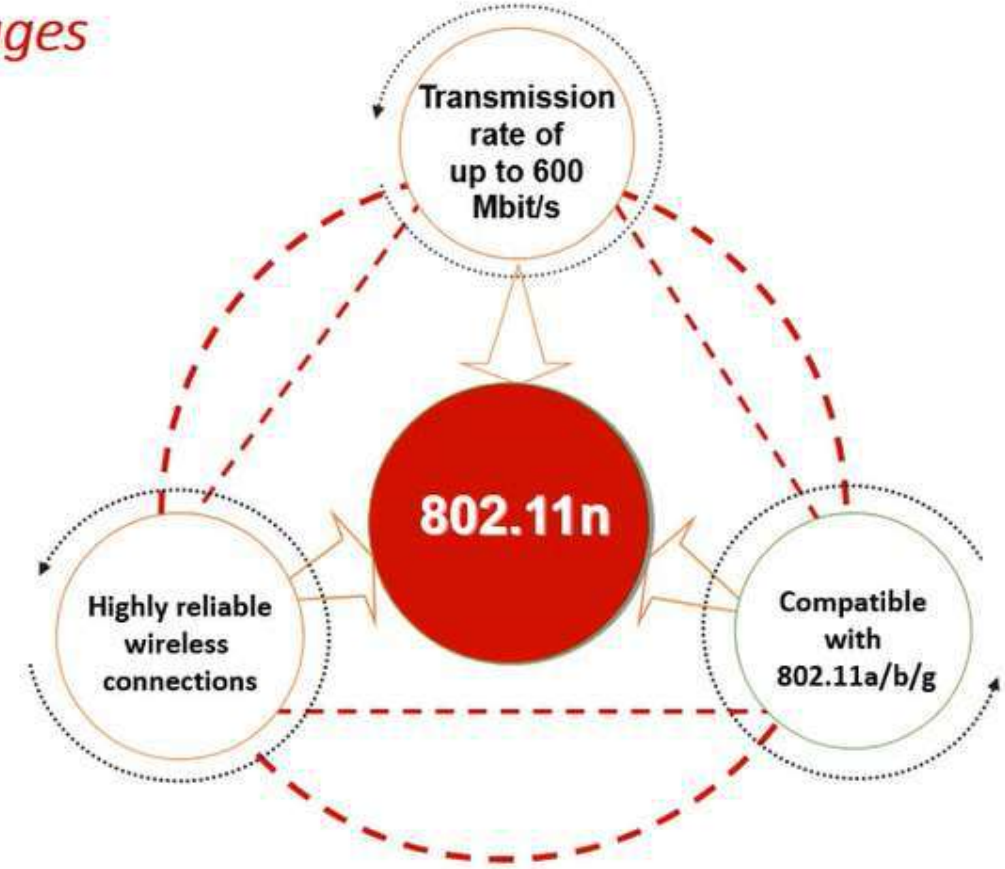
La couche physique : PHY

- La norme 802,11n :
  - ❑ Capacité : >600 Mbit/s,
    - ➢ Utilise MIMO et OFDM,
    - ➢ Portée plus importante,
    - ➢ Bandes 2,4GHz (ISM) et 5GHz ,

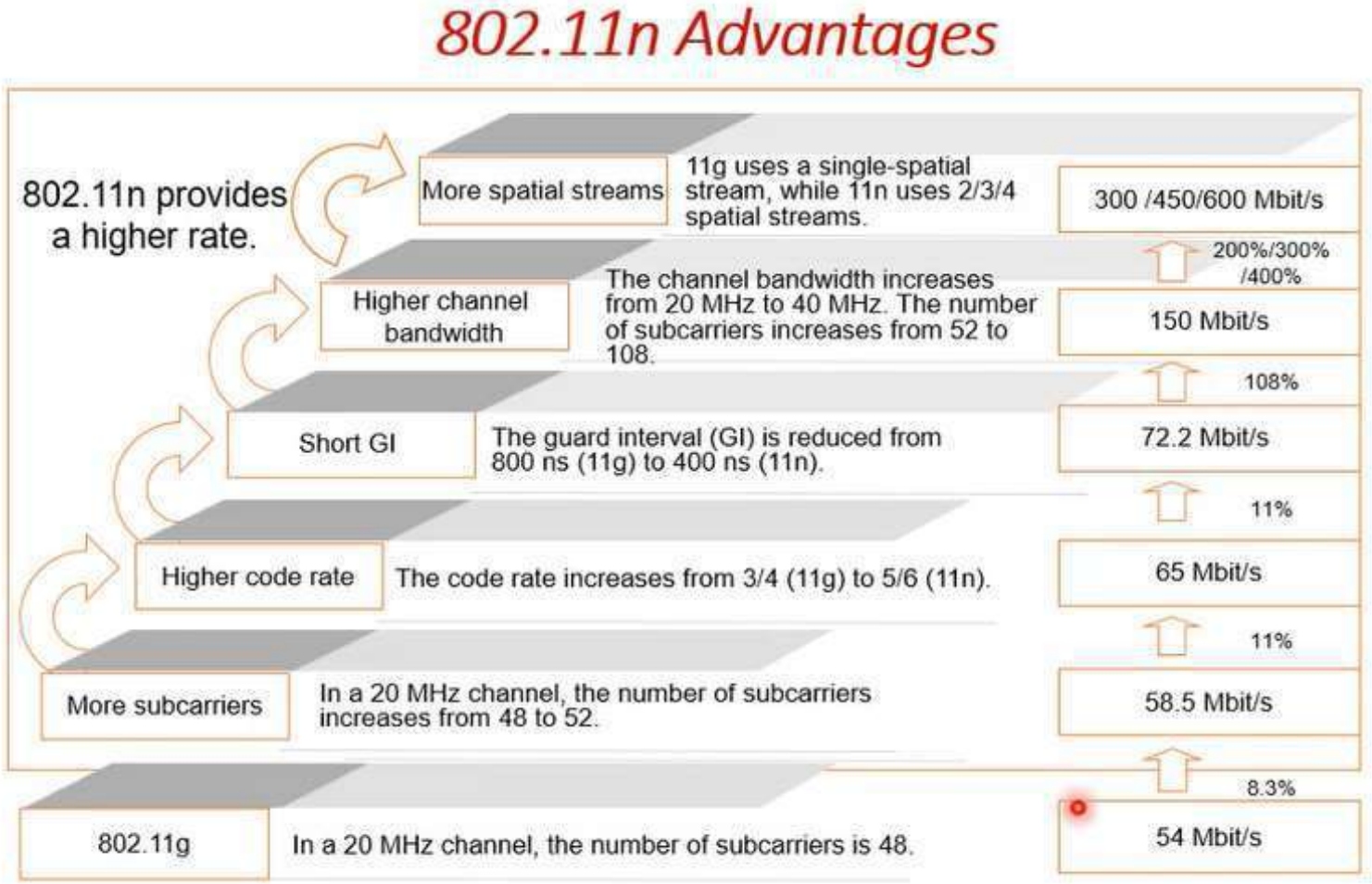
Huawei 802.11n
wireless AP

La couche physique : PHY

802.11n Advantages



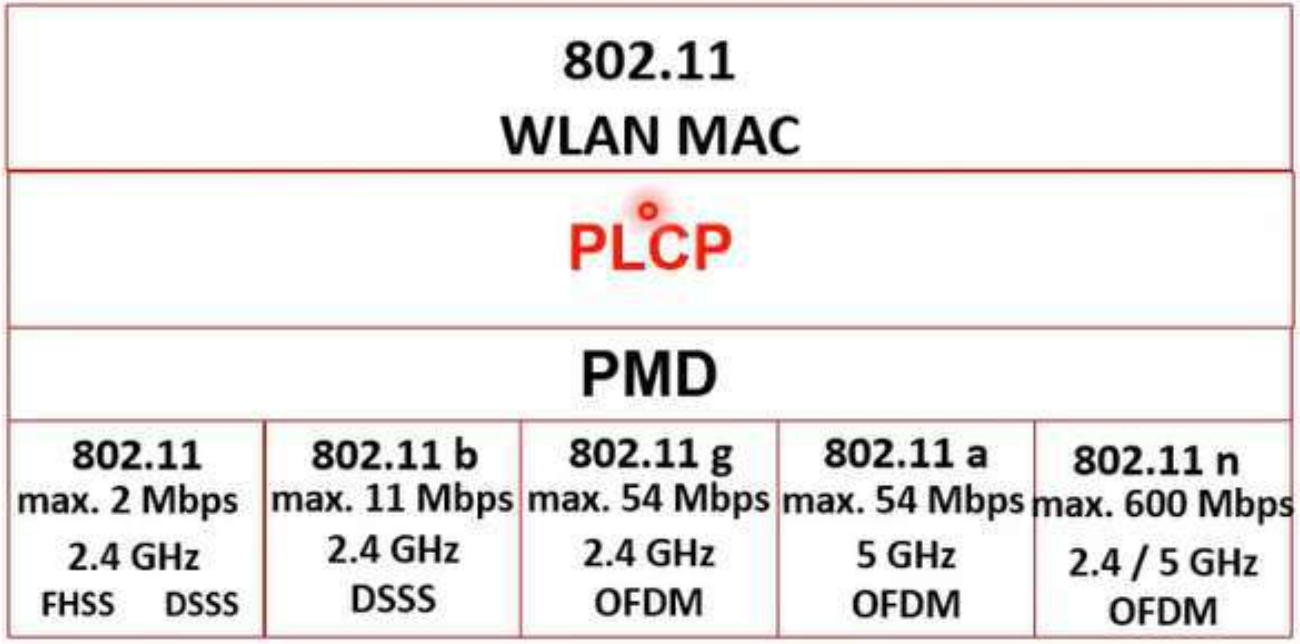
La couche physique : PHY



IEEE 802.11 : LA COUCHE PHYSIQUE

La sous Couche PLCP :

802.11 Physical Layer Overview



IEEE 802.11 : LA COUCHE PHYSIQUE

La sous Couche PLCP :

Les paquets de données, provenant de la couche réseau, sont encapsulés au **niveau 2 par un en-tête MAC, formant une MPDU (Mac Protocol Data Unit)**. Cette **MPDU** est **ensuite encapsulée dans une seconde trame** au **niveau 1 (physique)** pour permettre la transmission sur le média.

Cette encapsulation **niveau physique** consiste à **rajouter un préambule et un en-tête à la MPDU**, cet ensemble forme une **PLCP-PDU**. Le **préambule et l'en-tête différent suivant la couche physique utilisée**. Nous allons voir **les différentes trames du niveau physique (PLCP-PDU), puis celles du niveau liaison de données (MPDU).**

IEEE 802.11 : LA COUCHE PHYSIQUE

La sous Couche PLCP :

Le **préambule permet** la **détection du début de trame, la synchronisation de la trame**, il permet **la prise du canal pour l'émission ou CCA (Clear Channel Assesment).**

L'en-tête contient diverses informations, variable suivant l'interface physique utilisée (La technologie Wifi utilisée).

1) TRAME FHSS

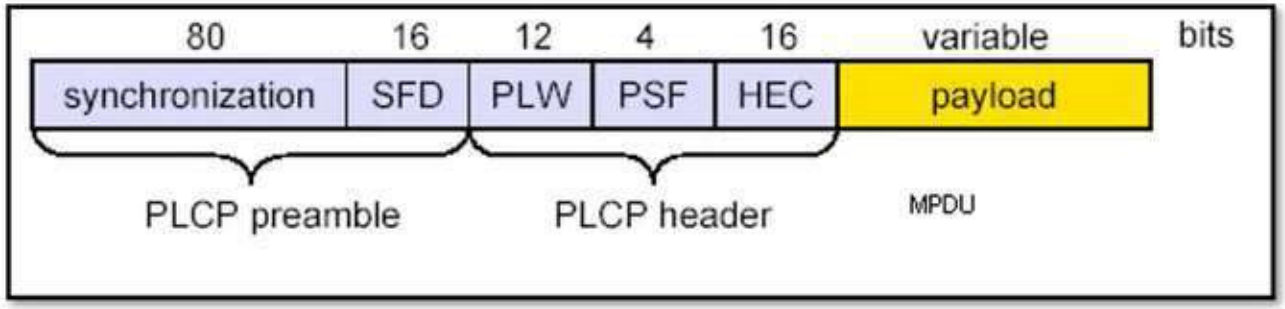
2) TRAME DSSS

3) TRAME OFDM

IEEE 802.11 : LA COUCHE PHYSIQUE

La sous Couche PLCP :

Trame FHSS : 802.11



Préambule (preamble) en deux parties :

-80 bits de synchronisation (alternance de 0 et de 1) permet de sélectionner le meilleur point d'accès et de se synchroniser avec (PA et STA).

-SFD (Start Frame Delimiter) de 16 bits (0000 1100 1011 1101): indique le début de la trame.

En-tête (header) en trois parties :

-PLW (PLCP-PDU Length Word) sur 12 bits: indique la longueur (en nombre d'octets) de la trame (PLCP-PDU), cela permet à la couche physique déterminer la fin de la trame.

-PSF (PLCP Signaling Field) sur 4 bits: indique le débit utilisé sur l'interface radio. (**1 ou 2 Mbits/s**) pour la transmission des données (MPDU).

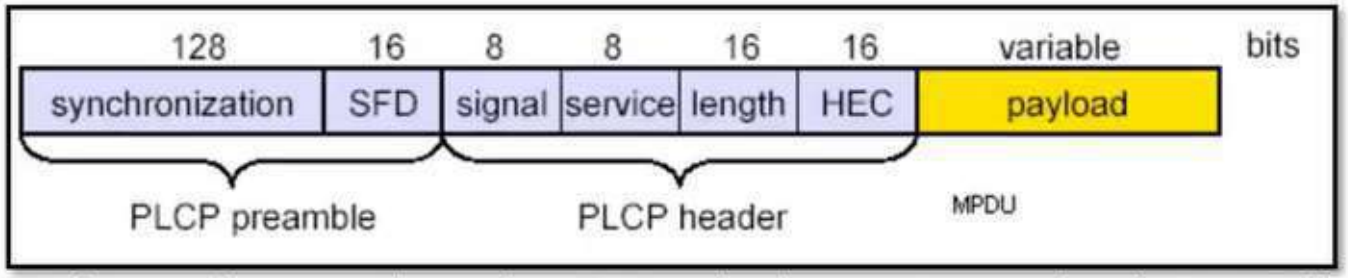
-HEC (Header Error Check) est un **CRC de 16 bits** permettant de détecter les erreurs des champs de l'en-tête (**PLW et PSF**).

Remarque : le préambule et l'en-tête sont toujours transmis à 1 Mbits/s.

IEEE 802.11 : LA COUCHE PHYSIQUE

La sous Couche PLCP :

La trame DSSS : 802.11 b



Préambule : identique à la trame FSSS, si ce n'est une longueur de synchronisation plus longue.et une valeur de 0xF3A0 (1111 0011 1010 0000) pour le SFD.

En-tête en quatre parties :

-Signal sur 8 bits : indique la vitesse sélectionnée pour la transmission des données (MPDU) :
0x0A pour 802.11 en mode BPSK (1Mbits/s)
0x14 pour 802.11 en mode QPSK (2Mbits/s)
0x37 pour 802.11b en mode QPSK (5,5Mbits/s)
0x6E pour 802.11b en mode QPSK (11Mbits/s)

-Service sur 8 bits : réservé pour un usage futur (valeur 0x00 : IEEE802.11)

-Lenght sur 16 bits : indique la longueur (en nombre d'octets) de la trame à suivre (MPDU), cela permet à la couche physique déterminer la fin de la trame.

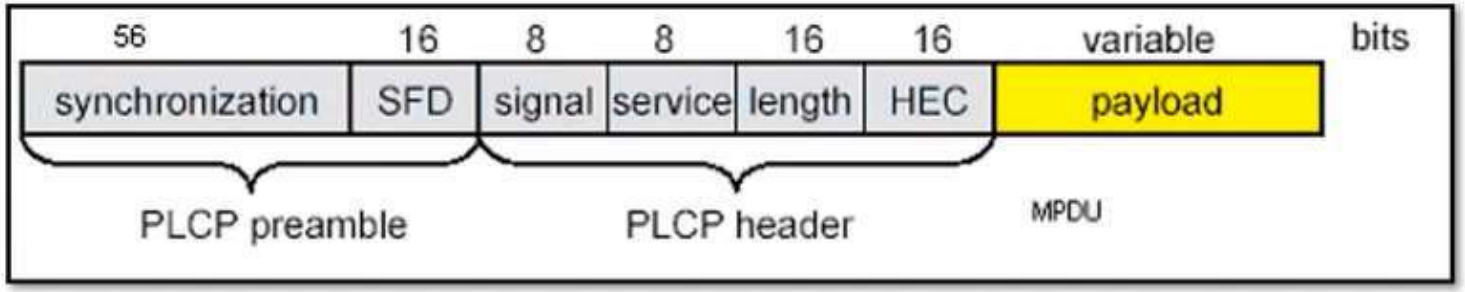
-HEC (Header Error Check) est un CRC de 16 bits permettant de détecter les erreurs des champs de l'en-tête (Signal, Service et Lenght).

IEEE 802.11 : LA COUCHE PHYSIQUE

La sous Couche PLCP :

La trame DSSS : 802.11 b

Remarque : le préambule et l'en-tête sont toujours transmis à 1 Mbits/s.
De plus pour la norme 802.11b il existe un deuxième type d'encapsulation dont le préambule est plus court (**72bits au lieu de 144bits**) :

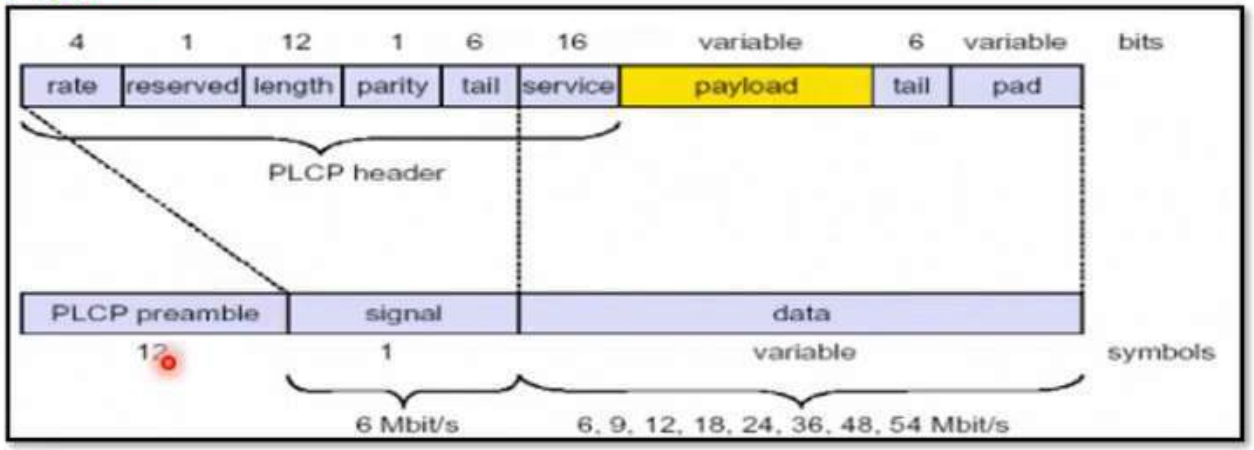


IEEE 802.11 : LA COUCHE PHYSIQUE

2) Présentation de la couche physique 802.11

La sous Couche PLCP :

La trame OFDM : 802.11 a / g /n :



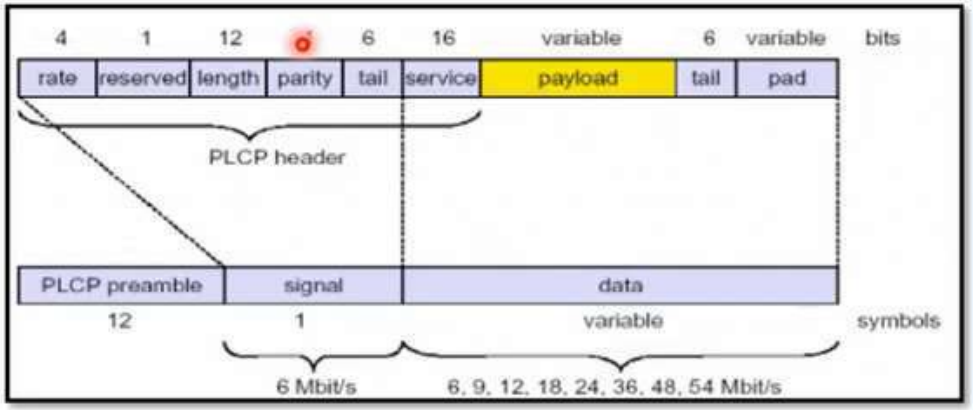
Préambule : réalisé grâce à **une séquence de douze symboles** permettant la détection du signal par le récepteur et le début de la trame.

IEEE 802.11 : LA COUCHE PHYSIQUE

2) Présentation de la couche physique 802.11

La sous Couche PLCP :

La trame OFDM : 802.11 a / g / n



En-tête en six champs :

-RATE : indique le débit de transmission

-1 bit réservé toujours à 0

-Lenght : indique le nombre d'octets dans la trame.

-1 bit de parité des trois champs précédents

-Tail (en-queue) : champs réservé, toujours à 0

- Service : champ réservé, toujours à 0

MPDU :

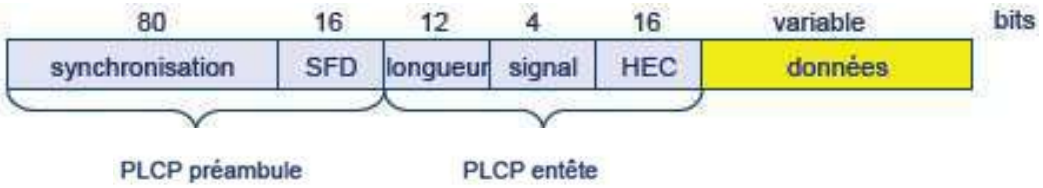
-Tail : champ réservé, toujours à 0

-Pad : champ de padding (remplissage) de 6 bits minimum permettant une structure se comptant en octets.

IEEE 802.11 : LA COUCHE PHYSIQUE

Format de la trame PLCP

FHSS Format des paquets PHY



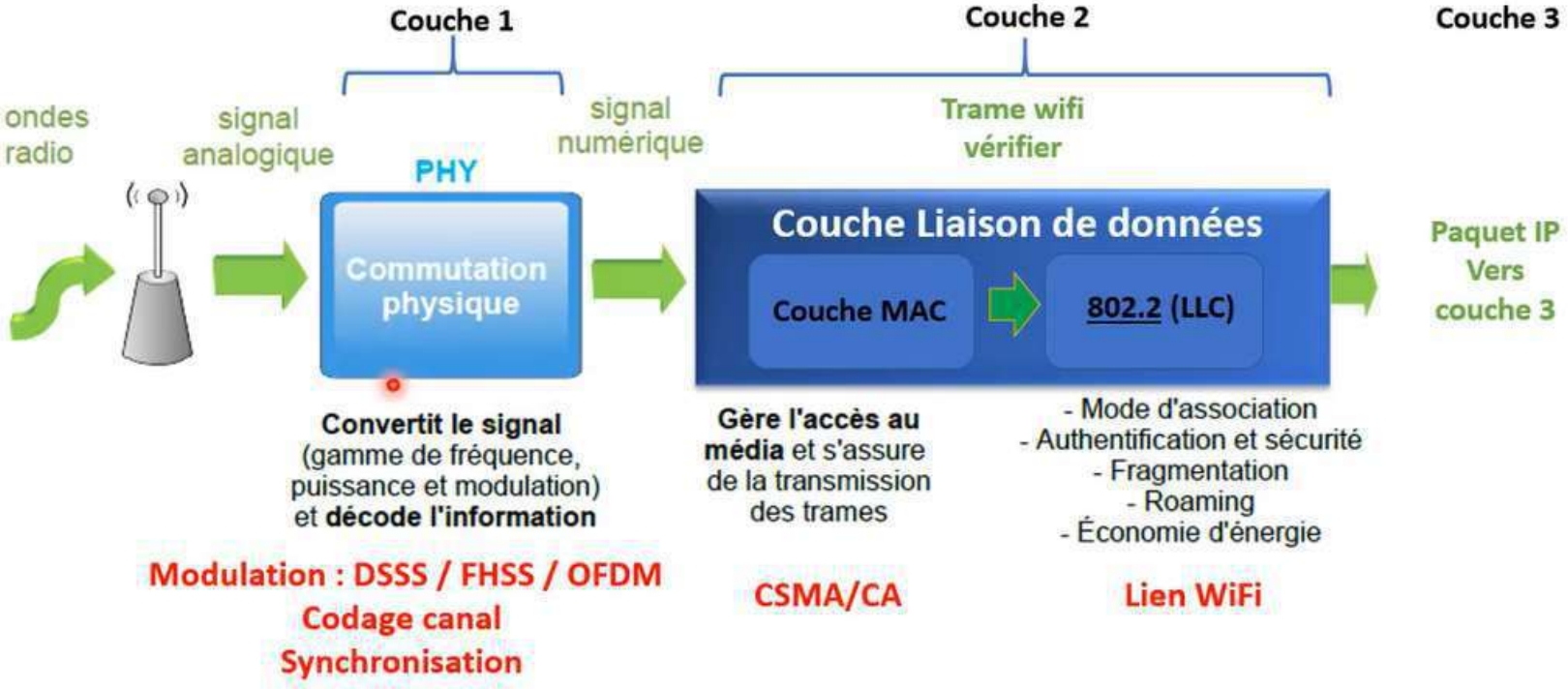
DSSS Format des paquets PHY

- Synchronisation
  - Une suite binaire de "0" et de "1" (12 symboles OFDM pour IEEE 802.11a)
  - Compensation de la fréquence
  - Détection de l'énergie
    - configuration du gain, choix du codage
- "Start Frame Delimiter"
  - "11110011 10100000"
- Signal
  - Débit de la transmission
    - 0x0A : 1 Mbit/s par DBPSK, 0x14 : 2 Mbit/s par DQPSK, 0x 37 : 5,5 Mbit/s, 0x6E : 11 Mbit/s
- Service
  - 00 : compatible 802.11
- "Length"
  - Longueur de champ de données (en ms)
- "Header Error Checksum"
  - CRC : x^16 + x^12 + x^5 + 1 (le CRC -16 d'HDLC !)

La couche liaison de données

Les réseaux WLAN

Principe de fonctionnement du module WiFi 802.11:



La couche liaison de données

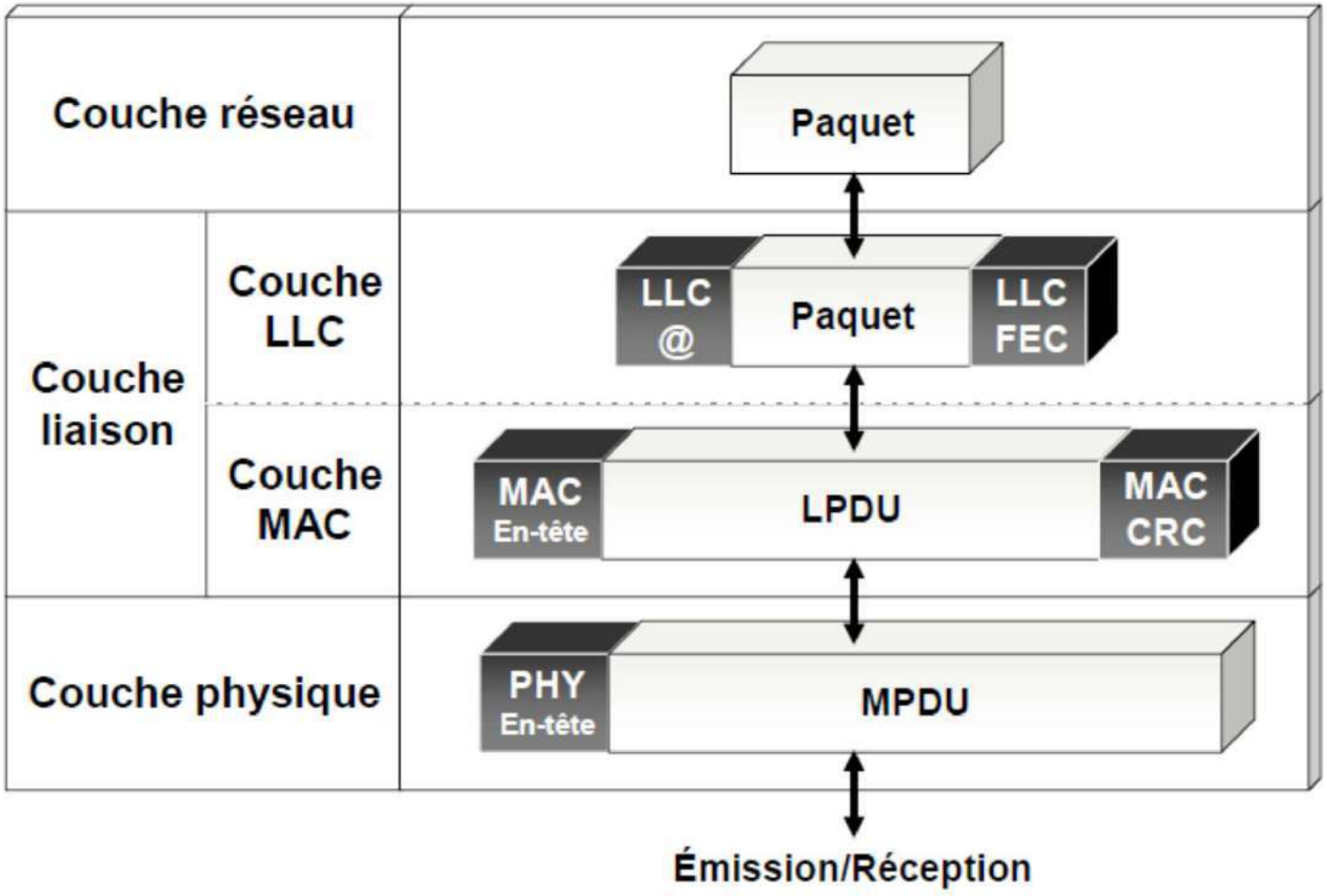
La couche LLC

- définie par le standard IEEE 802.2
- lien logique entre la couche MAC et la couche réseau (OSI 3) via le LSAP : *Logical Service Access Point*
- deux types de fonctionnalités :
  - système de contrôle de flux
  - système de reprise sur erreur
- Le LSAP permet de rendre interopérables des réseaux différents aux niveaux MAC ou physique, mais possédant la même LLC
- LDPU : *Logical Protocol Data Unit*

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

La couche liaison de données

La couche LLC



La couche liaison de données

La couche MAC

- similaire à la couche MAC d'Ethernet (IEEE 802.3)
- fonctionnalités :
  - contrôle d'accès au 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
- deux méthodes d'accès :
  - DCF (*Distributed Coordination Function*) : avec contention ; support de données asynchrones ; chances égales d'accès au support ; collisions
  - PCF (*Point Coordination Function*) : sans contention ; pas de collisions ; transmission de données isochrones (applications temps-réel, voix, vidéo)

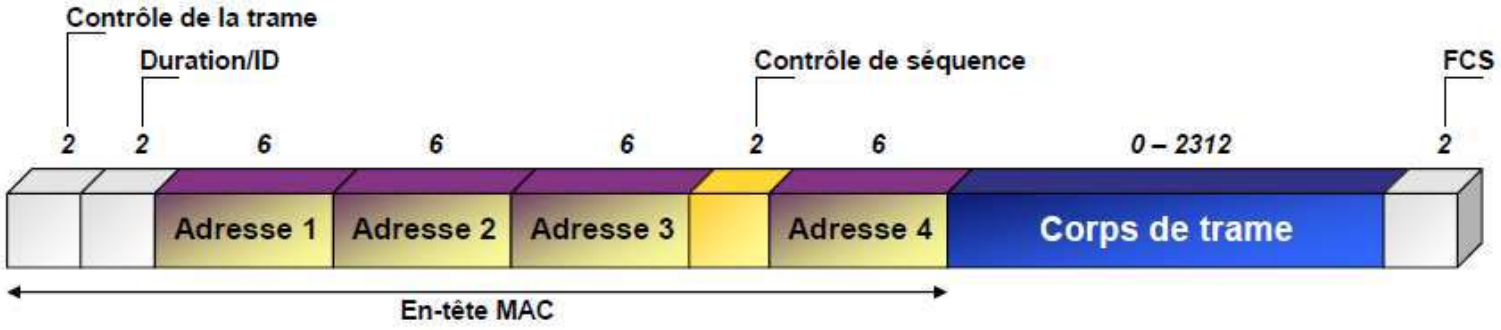
La couche liaison de données

Présentation de la trame MAC de 802.11 :

Trame 802.11 : La taille maximale de la trame est de 2346 octets. Le format général de la trame est comme suit :

Trois types de trames MAC :

- **trames de données** : transmission des données
- **trames de contrôle** : contrôle de l'accès au support (RTS, CTS, ACK, etc.)
- **trames de gestion** : association, réassociation, synchronisation, authentification

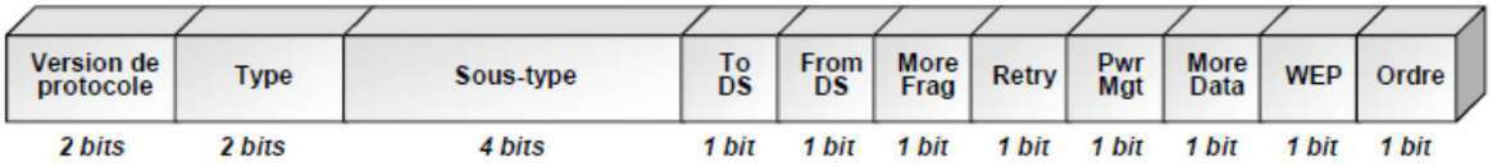


Les trames de niveau physique

- PLCP-PDU : *Physical Level Common Protoco – Protocol Data Unit*
- Constituées de trois parties :
  - **préambule** : détection du signal, synchronisation, détection du début de trame, prise du canal radio
  - **en-tête** : diverses informations comme le débit
  - **données** : informations provenant de la couche MAC : MPDU (*MAC Protoco Data Unit*)
- Ces informations varient en fonction de l'interface physique utilisée : FHSS, DSSS, IR, OFDM

Les trames MAC

Le champ « contrôle de trame »



- **Version de protocole** : actuellement fixé à 0
- **Type** et **sous-type** : 3 types de trames, plusieurs sous-types
- **To DS** et **From DS** : trame envoyée vers le ou provient du destinataire
- **More fragments**
  - =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 management** : mode économie d'énergie (=1) ou actif (=0)
- **More data** : trames présentes en mémoire tampon
- **WEP** : trame chiffrée ou non (trame donnée ou gestion/authentification)
- **Order** : classe de service strictement ordonnée (*Strictly Ordered Service Class*)

Les trames MAC

Le champ « duration/ID »

- deux sens différents :
  - certaines 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

Les champs « adresse »

- toutes de longueur 6 octets
- même format que les adresse IEEE 802 MAC
- composées de quatre parties :
  - ***Individual/Group*** (I/G) : premier bit : adresse individuelle ou de groupe
  - ***Universal/Local*** (U/L) : deuxième bit : adresse locale ou universelle
  - ***Organizationally Unique Identifier*** : 22 bits : assignés par l'IEEE
  - **Numéro de série** : 24 bits : généralement défini par le constructeur

Les trames MAC

- Les champs « adresse »
  - 2 types d'adresses 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) :
      - dans un BSS : adresse MAC
      - dans un IBSS : BSSID de l'IBSS
      - trames de gestion Probe Request : tous les bits à 1
    - DA (Destination Address) : destination de la trame ; indiv. ou de groupe
    - SA (Source Address) : source de la trame ; toujours individuelle
    - RA (Receiver Address) : destination des données ; indiv. ou de groupe
    - TA (Transmitter Address) : source des données ; toujours individuelle

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	Aucun
0	1	DA	BSSID	SA	Aucun
1	0	BSSID	SA	DA	Aucun
1	1	RA	TA	DA	SA

La couche liaison de données

Présentation de la trame 802.11 :

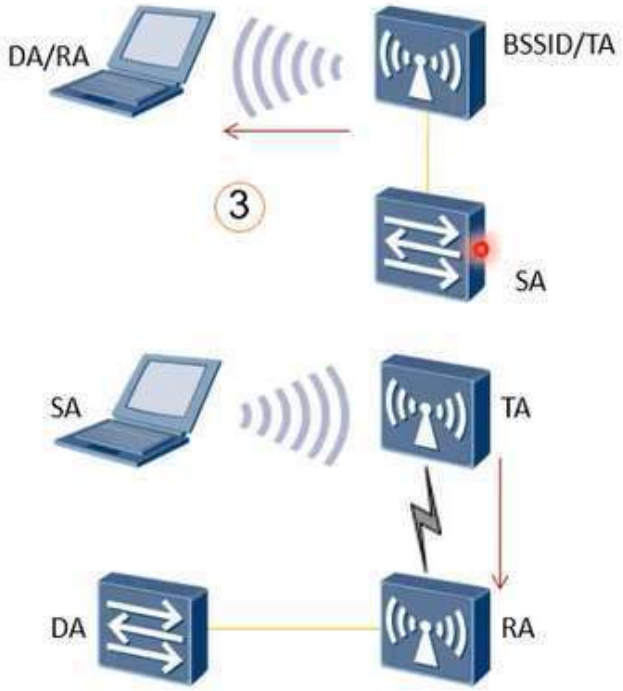
La signification d'Address dépend des champs To DS et From DS,

	Function	To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	IBSS	0	0	DA/RA	SA/TA	BSSID	Reserved
2	To AP	1	0	BSSID/RA	SA/TA	DA	Reserved
	From AP	0	1	DA/RA	BSSID/TA	SA	Reserved
	WDS	1	1	BSSID/RA	BSSID/TA	DA	SA

La couche liaison de données

Présentation de la trame 802.11 :

La signification d'Address dépend des champs To DS et From DS,



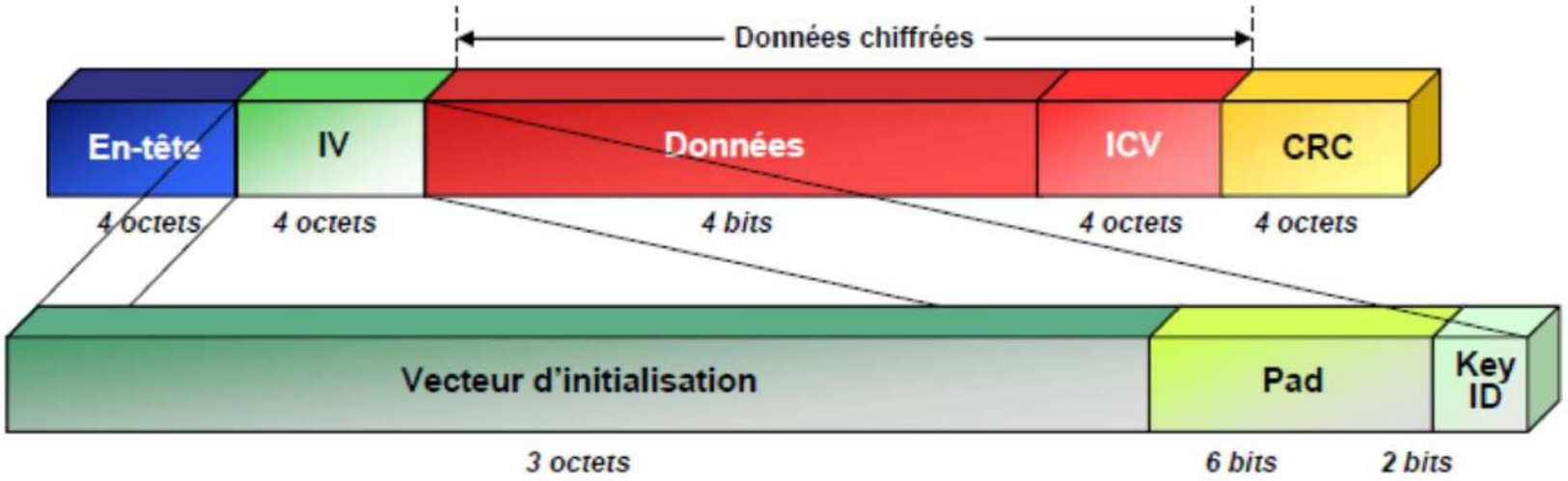
	Function	To DS	From DS	Address 1	Address 2	Address 3	Address 4
	IBSS	0	0	DA/RA	SA/TA	BSSID	Reserved
	To AP	1	0	BSSID/RA	SA/TA	DA	Reserved
3	From AP	0	1	DA/RA	BSSID/TA	SA	Reserved
4	WDS	1	1	BSSID/RA	BSSID/TA	DA	SA

Les trames MAC

- Le champ « contrôle de séquence »
  - **numéro de séquence** (12 bits) : attribué à chaque trame ; initialisé à 0 puis incrémenté pour chaque nouvelle trame
  - **numéro de fragment** (4 bits) : initialisé à 0 puis incrémenté pour chaque nouveau fragment
- Les données et le corps de la trame
  - taille minimale nulle (trames de gestion ou de contrôle)
  - taille maximale 1500 octets
  - taille plus importante si chiffrée par WEP
  - *Initialization Vector* (IV)
  - *Integrity Check Value* (ICV)
- Le champ FCS *(Frame Check Sequence)*
  - CRC sur 32 bits pour contrôler l'intégrité des trames

Les trames MAC Chiffrées

Une trame n'est chiffrée que partiellement :



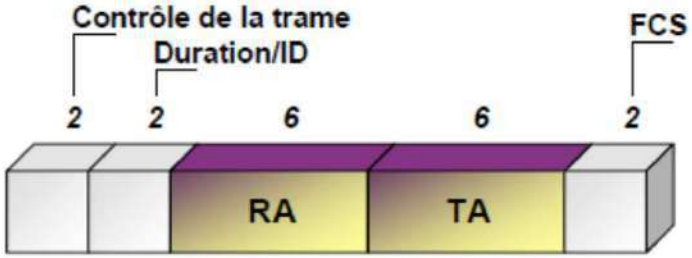
- **IV** : vecteur d'initialisation défini dans le WEP
- **Pad** : ne contient que des 0
- **Key ID** : valeur d'une des 4 clefs permettant de déchiffrer la trame

Les trames de contrôle

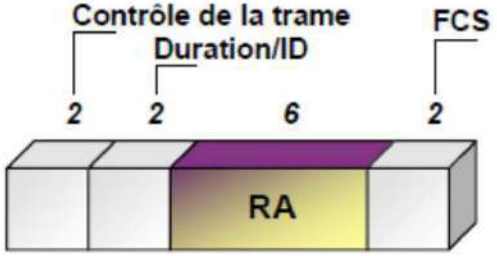
Trame de contrôle :

Version de protocole	Type	Sous-type	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Ordre
			0	*0*	*0*	*0*	*0/1*	*0*	*0*	*0*

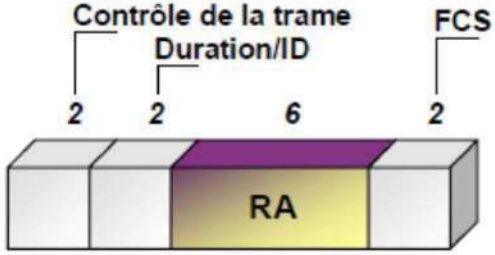
Trame RTS :



Trame CTS :

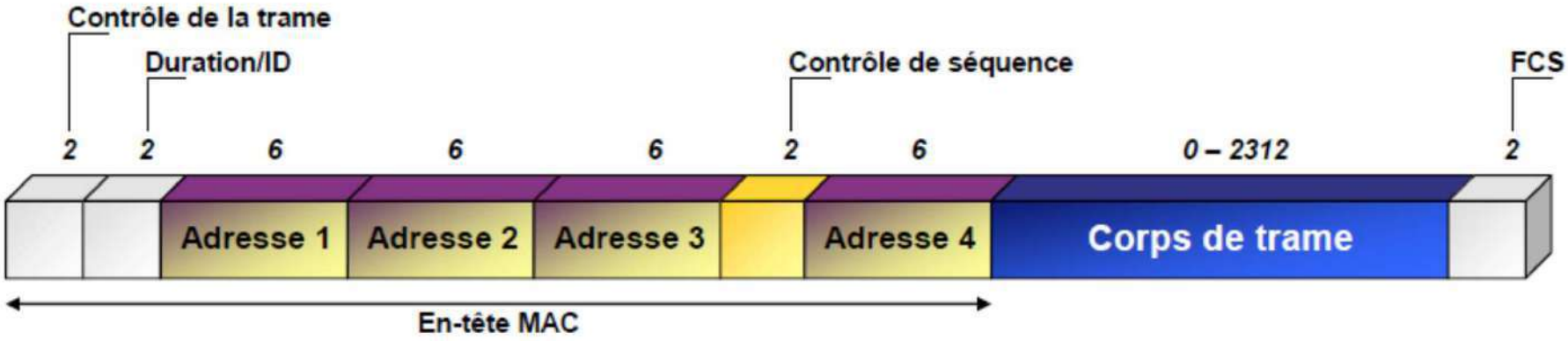


Trame ACK :

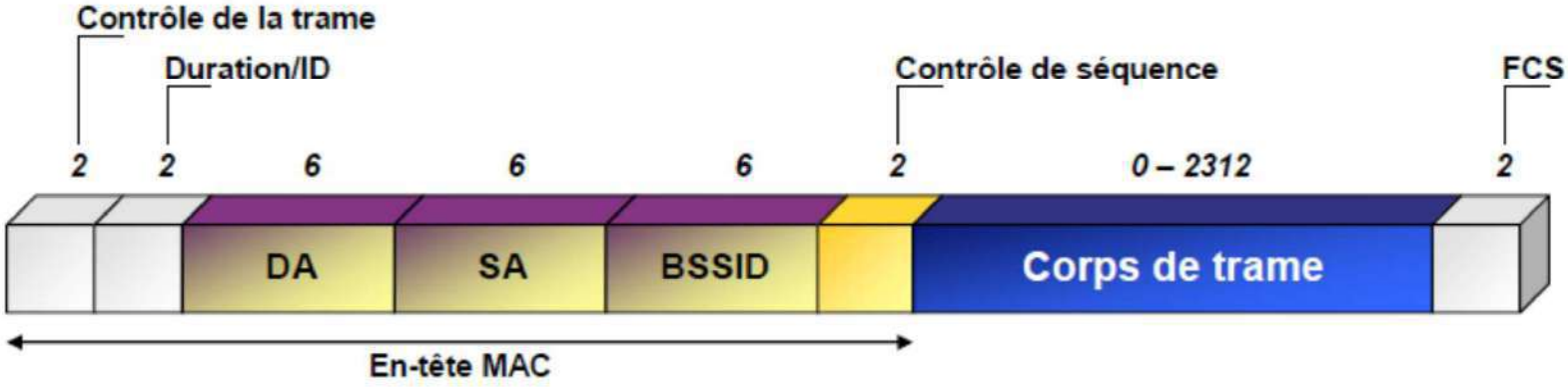


Les trames de gestion de données

Trame de gestion :



Trame de donnée :

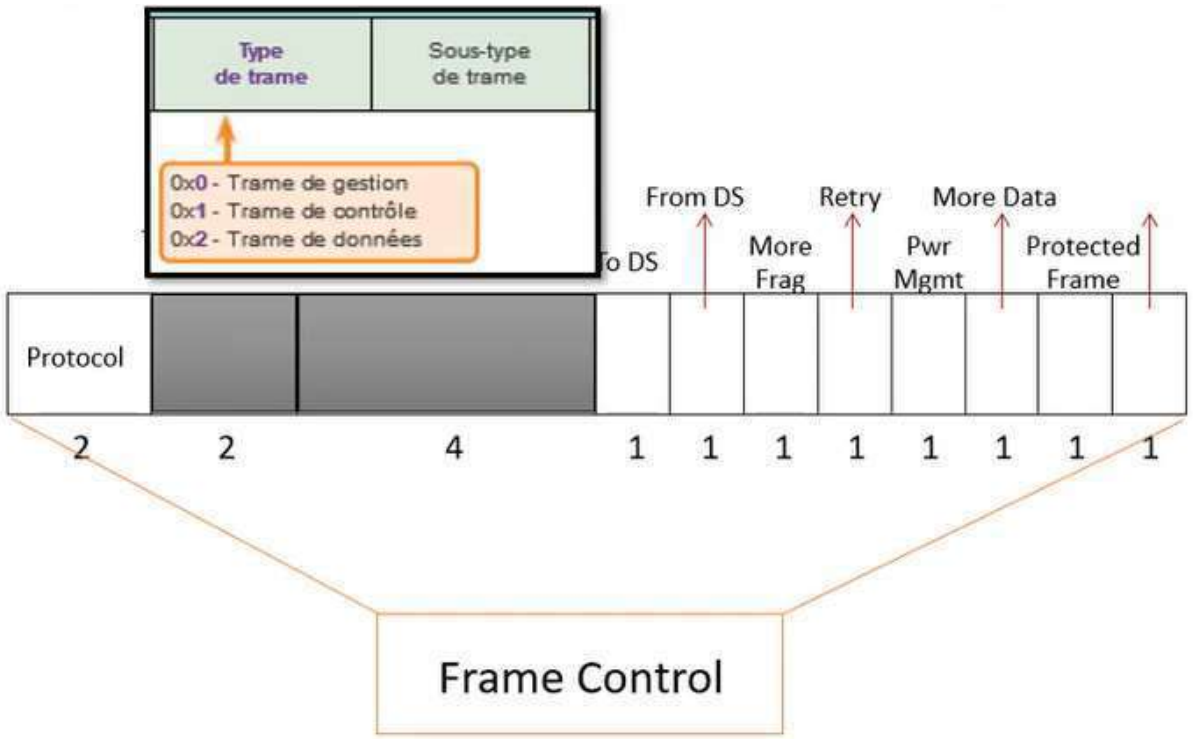


La couche liaison de données

Présentation de la trame 802.11 :

Le Champ Frame Control :

- ***Type values :***
  - **Management frame: 00**
  - **Control frame: 01**
  - **Data frame: 10**
  - **The value 11 is reserved.**
- Subtype is the specific type of frames



Sous-type :

- RTS,
- CTS,
- ACK,
- ,,,,

FONCTIONNALITÉS

Fragmentation et réassemblage

Variation du débit

Gestion de la mobilité

Qualité de service

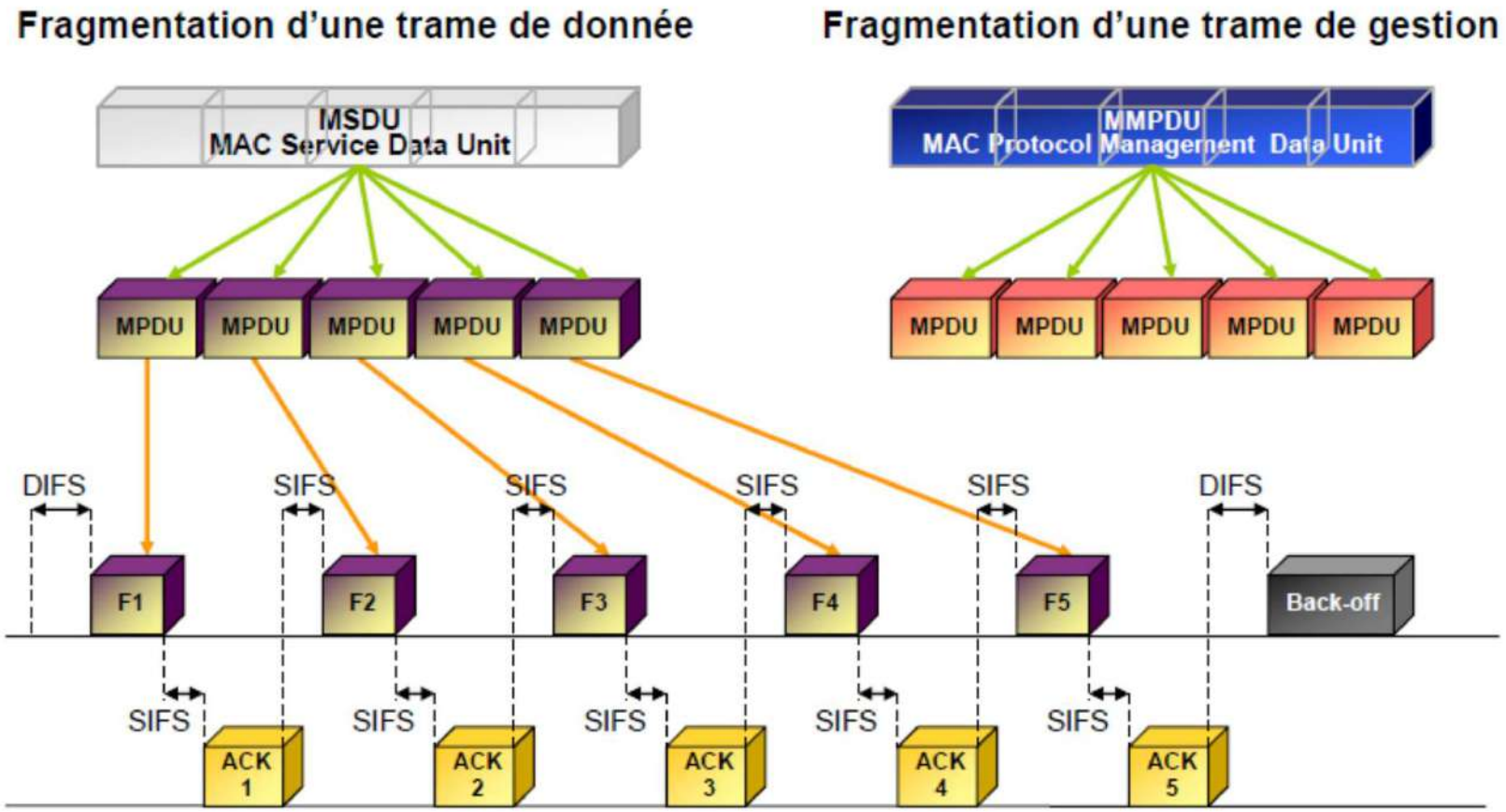
Économie d'énergie

Fragmentation et réassemblage

- Taux d'erreur pour liaison sans fil très supérieur à celui des liaisons filaires : nécessité de transmettre de petits paquets
- Fragmentation d'une :
  - trame de donnée MSDU (*MAC Service Data Unit*)
  - trame de gestion MMPDU (*MAC Management Protocol Data Unit*)
  - en plusieurs trames MPDU (*MAC Protocol Data Unit*)
- Fragmentation si taille > valeur seuil
  - fragments envoyés de manière séquentielle
  - destination acquitte de 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 lors à chaque nouveau fragment

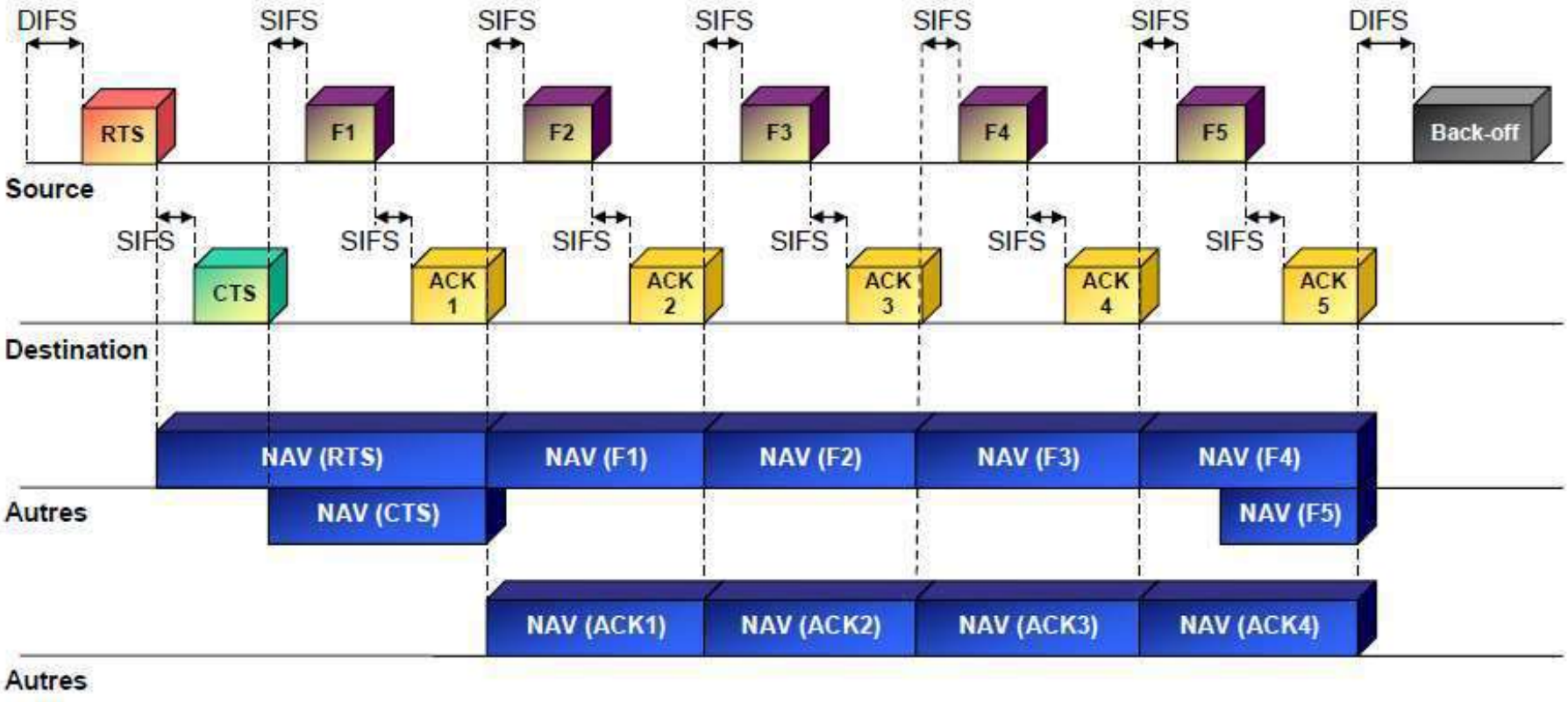
Fragmentation et réassemblage

Mécanisme d'émission d'une trame fragmentée



Fragmentation et réassemblage

Émission d'une trame fragmentée avec réservation du support

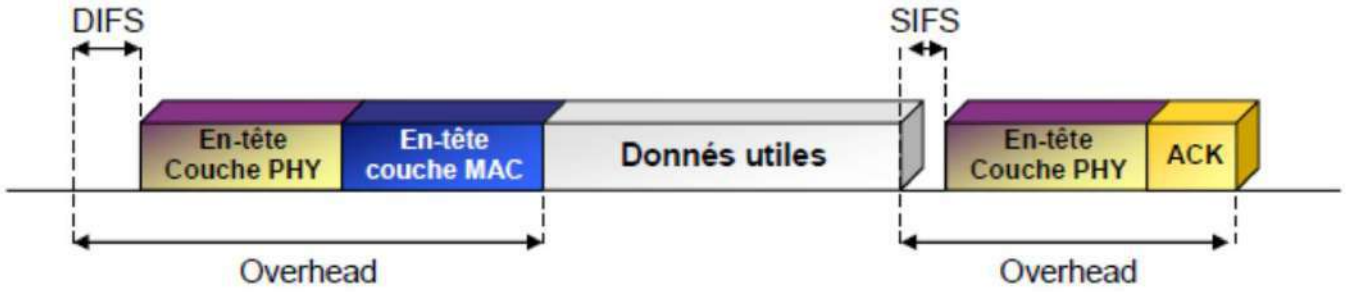


Fragmentation et réassemblage

- Deux champs permettent le réassemblage des fragments par la station destination :
  - ***Sequence control*** : permet le réassemblage de la trame grâce à
    - ***Sequence number*** : chaque fragment issu d'une même trame possède le même numéro de séquence
    - ***Fragment number*** : chaque fragment d'une même trame se voit attribuer un numéro de fragment, à partir de zéro, incrémenté pour chaque nouveau fragment
  - ***More fragment*** : permet d'indiquer si d'autres fragments suivent ; égale zéro si le fragment en cours est le dernier fragment

Fragmentation et réassemblage

- 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
  - un part importante du débit sert à la gestion de la transmission



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

Variation du débit

Wi Fi *Variable Rate Shifting* :

- 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 (Mbits/s)	Portée à l'intérieur	Portée à l'extérieur
11	50 m	200 m
5,5	75 m	300 m
2	100 m	400 m
1	150 m	500 m

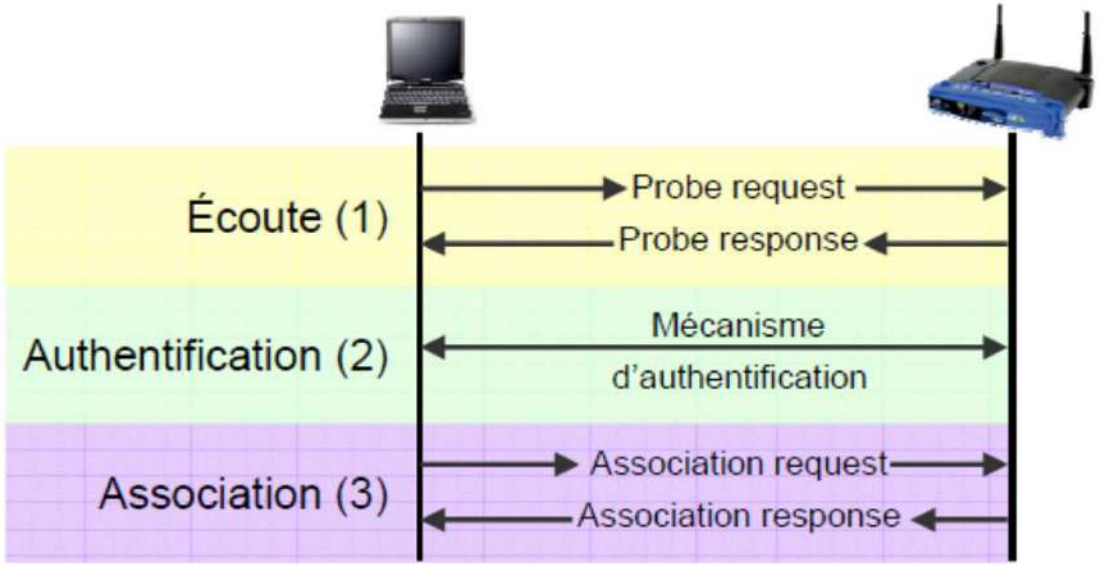
Gestion de la mobilité

- Des trames balises permettent aux stations mobiles de rester synchronisées
- Procédure d'association-réassociation :
  - choix du point d'accès : puissance du signal, taux d'erreur, charge
  - écoute du support
    - **passive** : attente d'une trame balise
    - **active** : envoie d'une trame de requête (*Probe Request Frame*) et attente de la réponse contenant les caractéristiques du point d'accès
  - authentification : deux mécanismes
    - ***open system authentication*** : mode par défaut ; ne constitue pas un réelle authentification
    - ***shared key authentication*** : véritable mécanisme d'authentification, repose sur le WEP (*Wired Equivalent Privacy*) ; repose sur une clef secrète partagée
- Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)

Gestion de la mobilité

Association

- utilisation d'un identifiant : SSID (*Service Set ID*) qui définit le réseau
- SSID émis régulièrement en clair par l'AP dans une trame balise : constitue une faille de sécurité



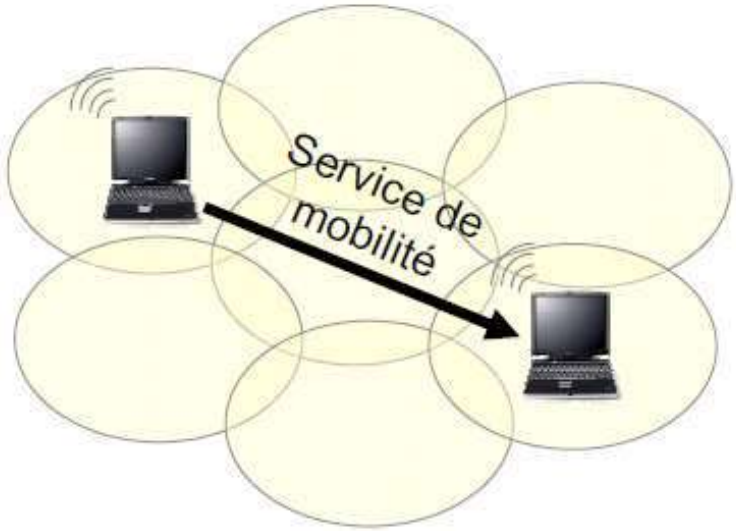
Réassociation

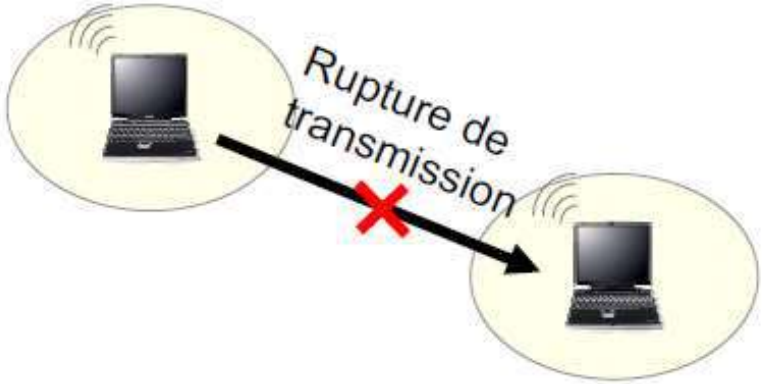
- similaire à l'association, effectuée lors de changements des caractéristiques de l'environnement (déplacement, trafic élevé)

Gestion de la mobilité

Les handovers

- mécanisme permettant à un dispositif mobile de changer de cellule sans que la transmission en cours ne soit interrompue
- possible que si les cellules voisines se recouvrent
- non défini dans la norme IEEE 802.11 ni 802.11b (WiFi)



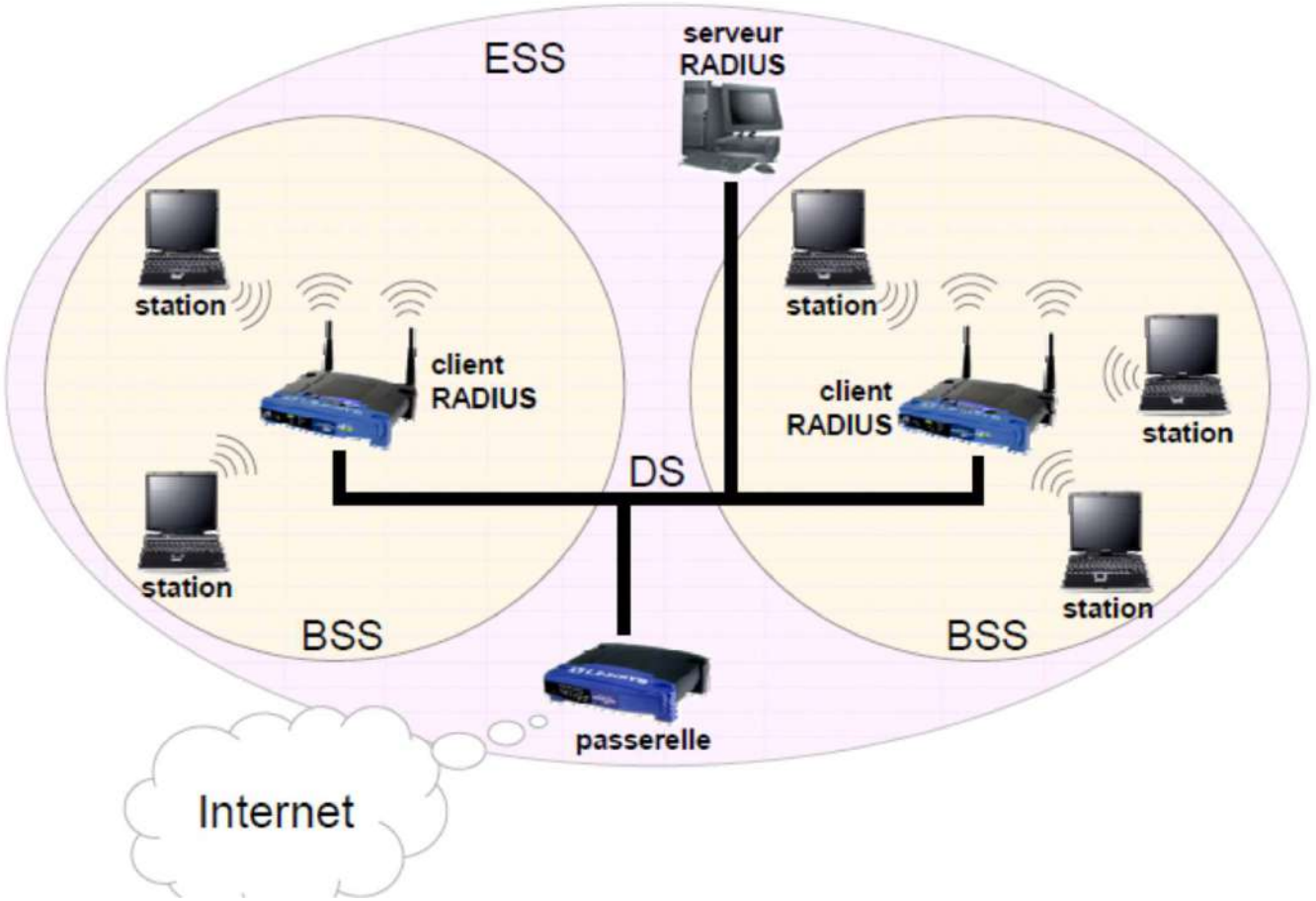


Gestion de la mobilité

- Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)
  - défini à l'origine par Lucent puis intégré à la norme 802.11
  - protocole de niveau transport (couche 4) qui se place au-dessus de UDP (*User Datagram Protocol*) : protocole sans connexion
  - utilise le protocole RADIUS pour permettre des handovers sécurisés (RADIUS : *Remote Authentication Dial-In User Server*)
  - serveur centralisé ayant une vue globale du réseau : il connaît la correspondance entre adresses IP et MAC

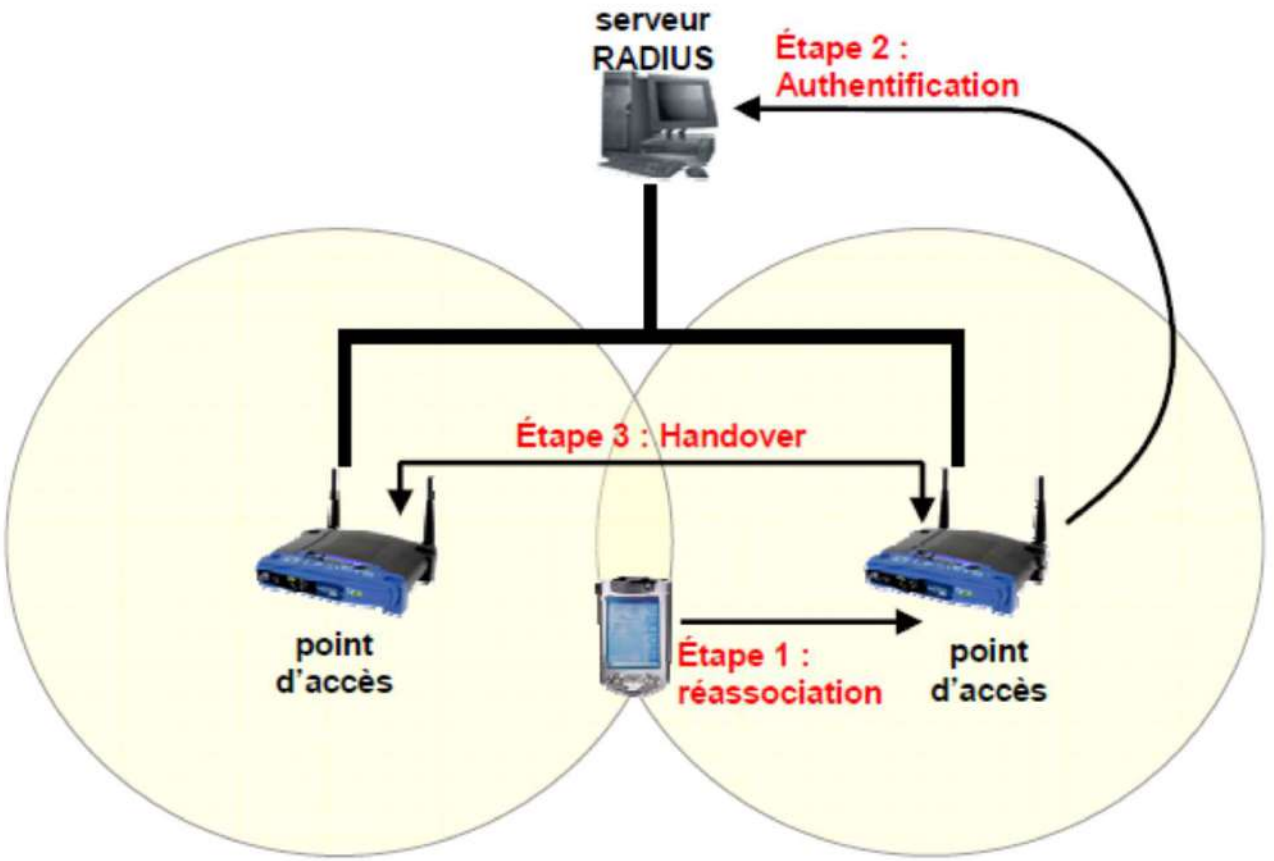
Gestion de la mobilité

Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)



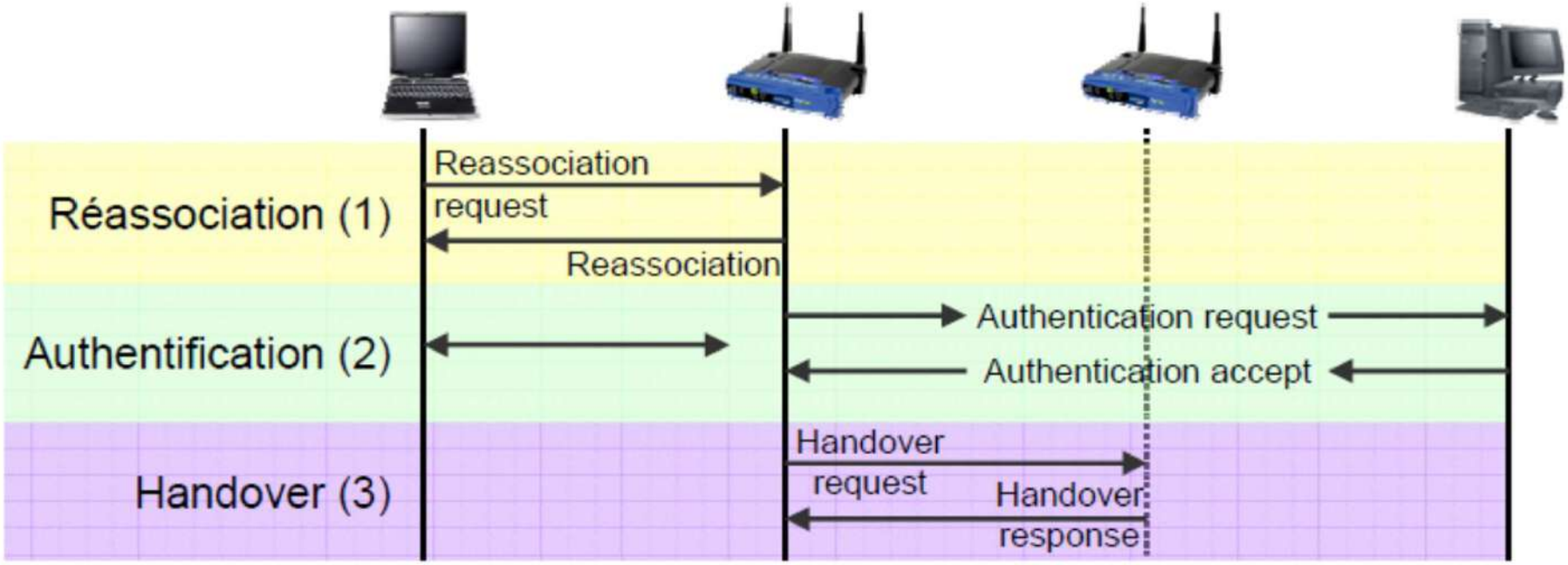
Gestion de la mobilité

Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)



Gestion de la mobilité

Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)



Economie d'Energie

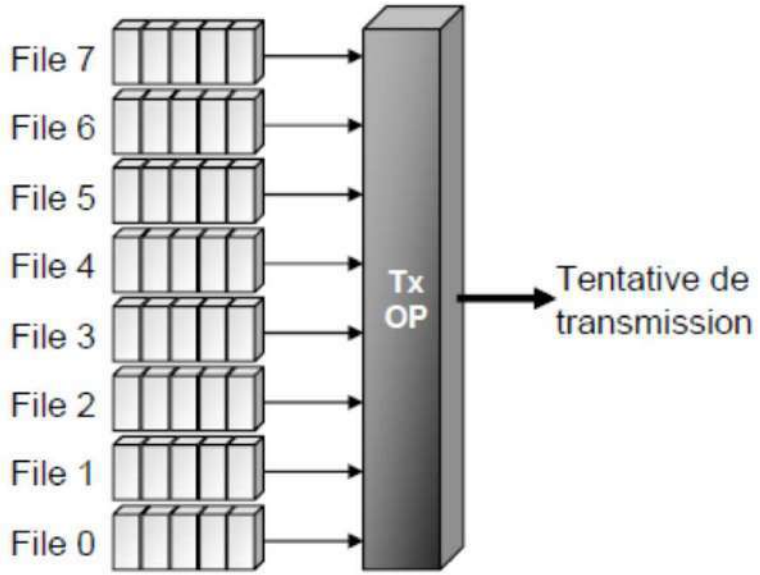
Stations mobiles : optimiser l'utilisation de l'énergie disponible :

- ***continuous aware mode*** : mode par défaut, pas d'économie d'énergie
- ***power save polling mode*** : mode économie d'énergie
  - le point d'accès tient un enregistrement de toutes les stations en mode économie d'énergie
  - il stocke toutes les données qui leur sont adressées
  - régulièrement, les stations s'éveillent pour recevoir un trame balise indiquant si oui ou non des données leur sont adressées
  - si oui, les stations récupèrent leurs données puis retournent en mode veille jusqu'à la prochaine trame balise

Qualité de Service

Gestion des priorités : accès EDCF (*Extended DCF*)

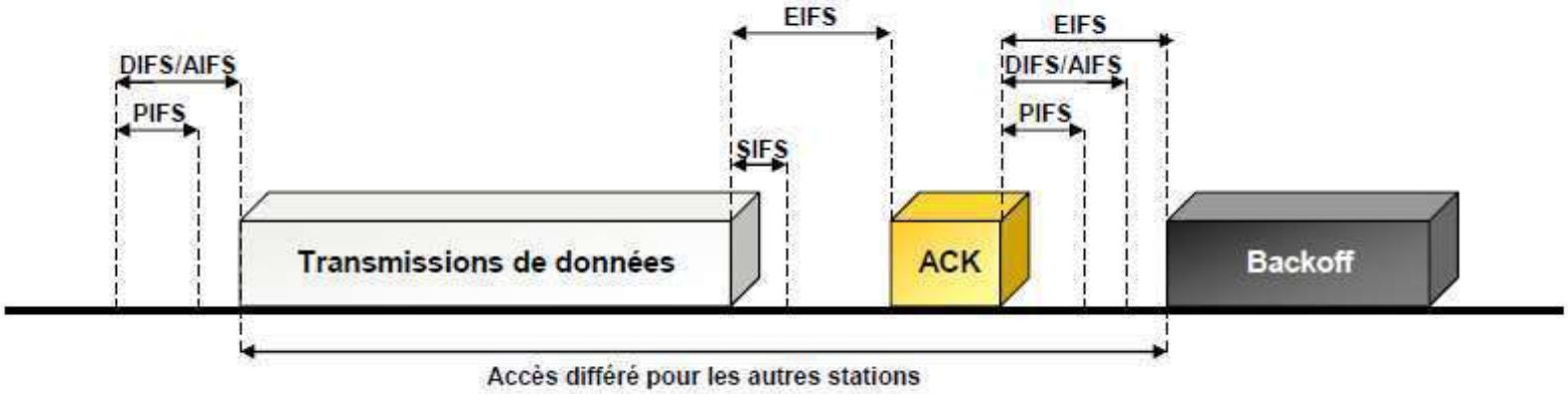
- méthode PCF jamais utilisée car non implantée par les fabricants
- EDCF : évolution du DCF, introduite dans IEEE 802.11e
- accès au support selon le niveau de priorité de la trame
- 8 niveaux de priorité : 8 files d'attente de transmission
- mécanisme TxOP : *Transmission Opportunities*



Qualité de Service

AIFS : *Arbitration IFS*

- utilisé de la même manière que le DIFS
- valeur dynamique : varie en fonction du niveau de priorité requis
- valeur supérieure ou égale au DIFS
- diminue les risques de collision



L'algorithme de back-off

- sa valeur est dynamique également
- variation fonction de la taille de la fenêtre de contention : si la taille est petite, la station attend moins longtemps

Qualité de Service

Accès HCF (*Hybrid coordination function*)

- méthode hybride entre l'EDCF et le PCF
- introduite dans IEEE 802.11e
- définit un HC (Hybrid Coordinator) qui génère des bursts de CFP au lieu d'un simple CFP dans le PCF
- système plus centralisé que le PCF

LA SÉCURITÉ

Accès au réseau et chiffrement

Chiffrement des données

Déchiffrement des données

Authentification

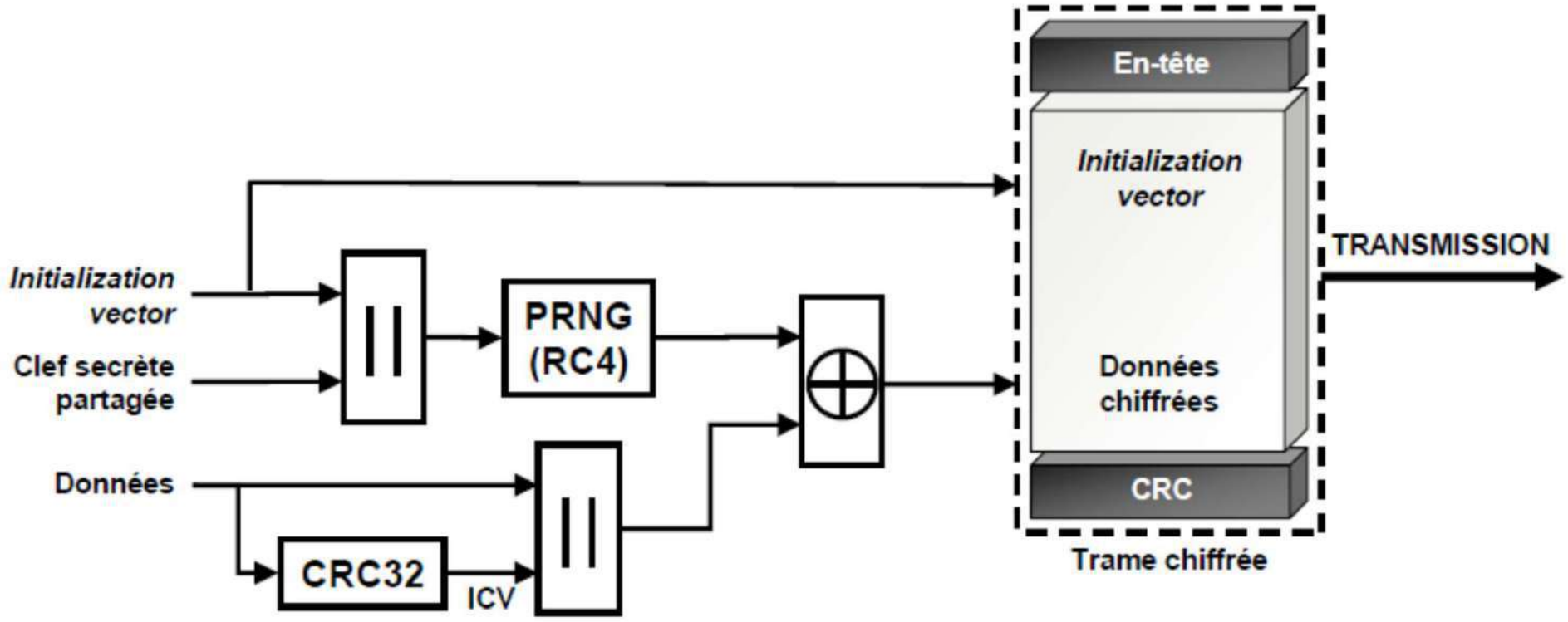
Les failles de sécurité

Accès au réseau et chiffrement

- SSID : seul mécanisme de sécurité obligatoire
- 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
- WEP : *Wired Equivalent Privacy*
  - repose sur RC4 :
    - key scheduling algorithm : clé composée d'une clef secrète partagée concaténée à un *Initialization Vector* (IV) : permet de générer une table d'état
    - séquence pseudo-aléatoire : la table précédente est placée dans un générateur pseudo-aléatoire

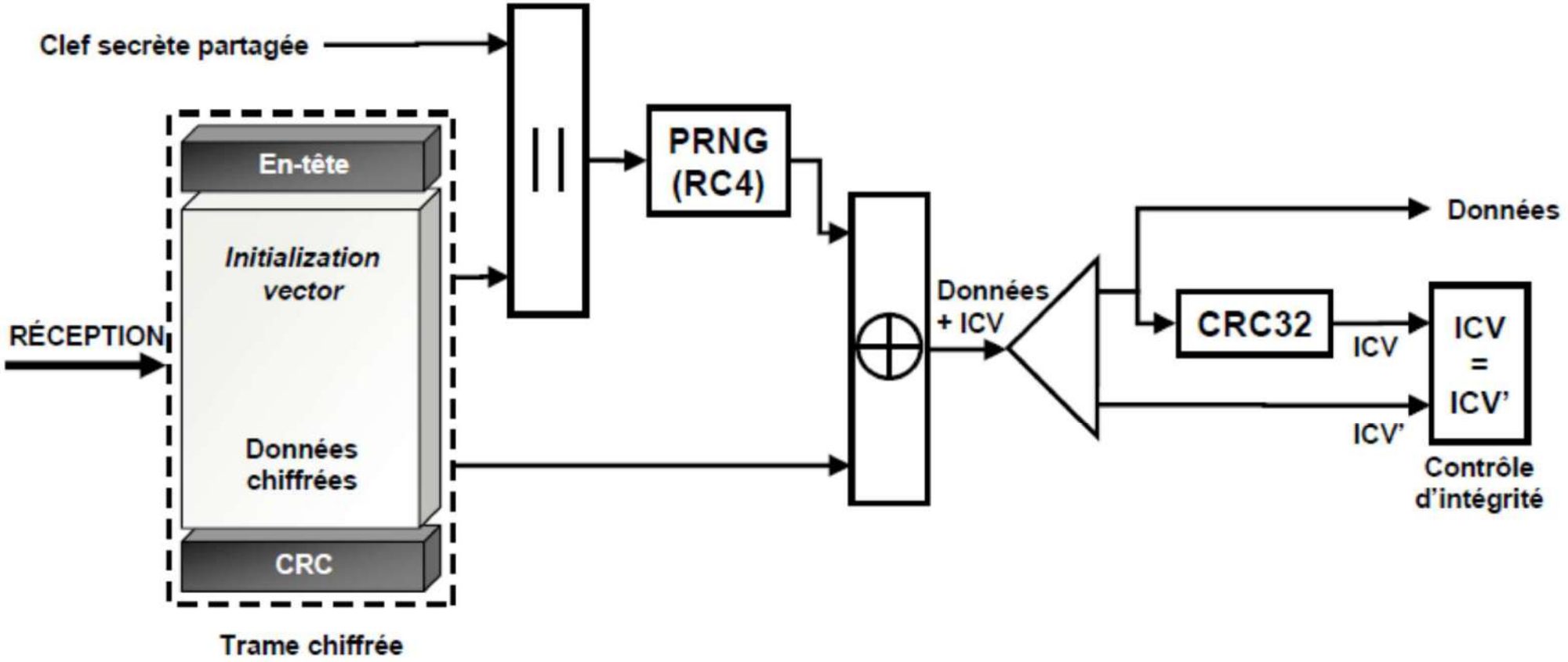
Chiffrement des données

Processus de chiffrement



Déchiffrement des données

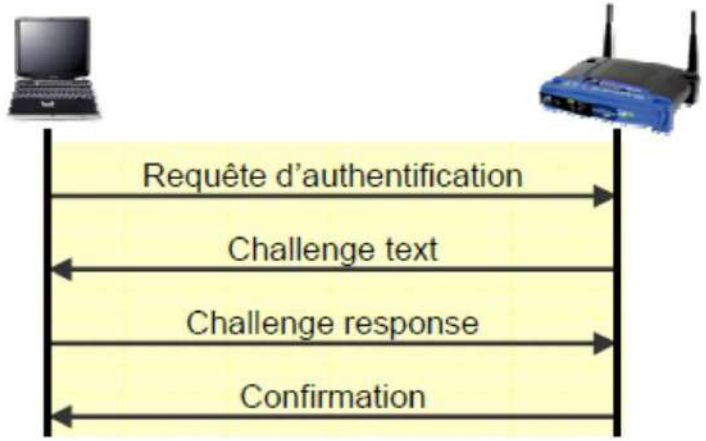
Processus de déchiffrement



Authentification

- 2 mécanismes :
  - ***Open system Authentication*** : mécanisme par défaut

  - ***Shared Key Authentication*** :



Les failles de sécurité

- WiFi comporte de nombreuses failles dans toutes ses composantes « *sécurité* » :
  - SSID (*Service Set ID*) :
    - transmis en clair par l'AP
    - le mécanisme *closed network* interdit sa transmission dans les balises
    - en mode ad-hoc, le SSID est systématiquement transmis en clair
    - même en mode fermé, le SSID est transmis en clair pendant l'association
    - utilisation du SSID par défaut, configuré par les constructeurs
  - 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
  - WEP
    - algorithme de chiffrement robuste : clef différente pour chaque paquet
    - faiblesse du WEP : système de génération de la clef : le vecteur d'initialisation est souvent réinitialisé à zéro à chaque nouvelle transmission

Les failles de sécurité

Réponses futures

- RC4 Fast Packet Keying (WEP+) : clef de chiffrement unique pour chaque trame
- IEEE 802.11i : introduction de l'AES ; plus gourmand en ressources

Solutions actuelles : serveurs d'authentification + tunnels

- IEEE 802.1x : contrôleur + serveur d'authentification
- réseaux privés virtuels (VPN)
- RADIUS
- gestion dynamique des clefs : modifier la clef périodiquement

Conclusion

- Les techniques de transmission sans fil
  - IEEE 802.11 (wifi)
  - Couche Physique
    - Techniques de modulation adaptés à un environnement variable
  - Couche Liaison de Données
    - Gestion de l'accès au CSMA/CD
    - Résolution du problème de la station cachée
    - Deux mode opératoires DCF, PCF
    - Mode d'économie d'énergie
  - De nombreuses variantes et extensions
    - Plus de débit => IEEE 802.11g
    - Gestion de la QoS
    - Meilleure gestion de la sécurité du canal radio
    - Gestion du "roaming"
    - Etc.

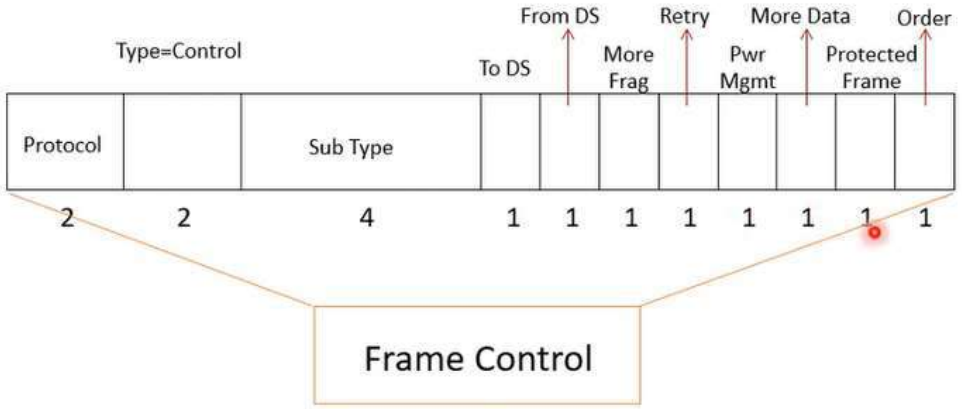
ANNEXE

La couche liaison de données

Présentation de la trame 802.11 :

Le Champ Frame Control :

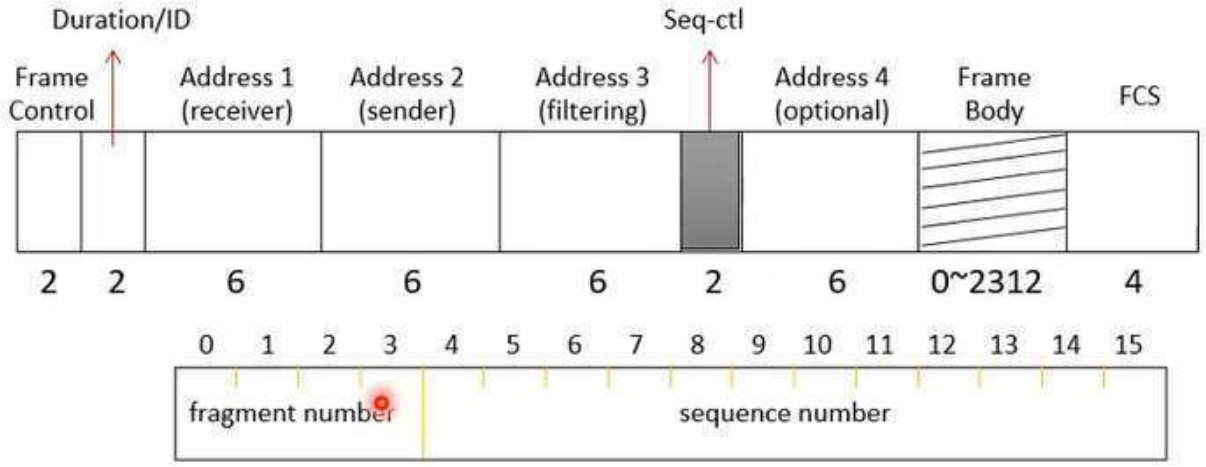
- To DS : Trame destinée au Système de Distribution,
- From DS : Trame provient du Système de Distribution,
- More Frag : Indique au récepteur si d'autres fragments de la trame sont attendus,
- Retry : Si erreur de réception, le système peut demander le re-transfert de la trame,
- Pwr Mgmt : indique si le mode économie d'énergie est activé,
- More Data : D'autres données sont enregistrées dans le point d'accès
- Protected Frame : Indique si la trame est protégée (Cas des trames de données ou de gestion).
- Order : si à 1 indique les trames doivent être traitées dans l'ordre,



La couche liaison de données

Présentation de la trame 802.11 :

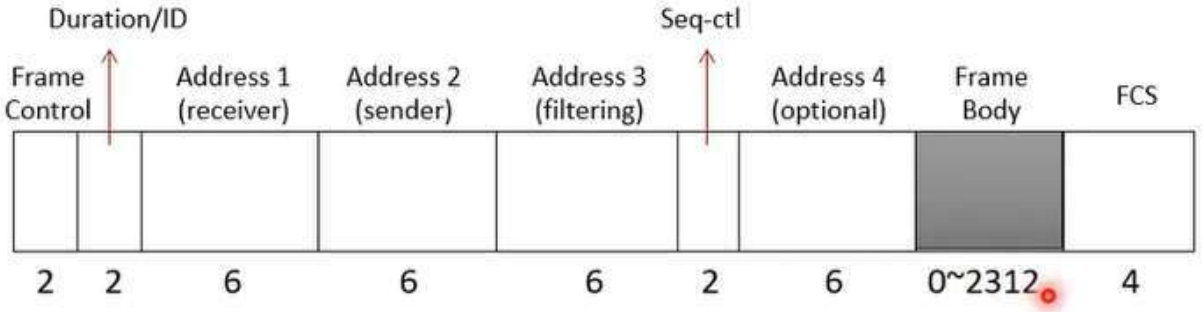
Seq-ctr contient 16 bits utilisé pour réassembler les trames fragmentées et récupérer les fragments perdus. Il composé de 4 bits pour le nombre de fragments et 12 bits pour le numéro du séquence.



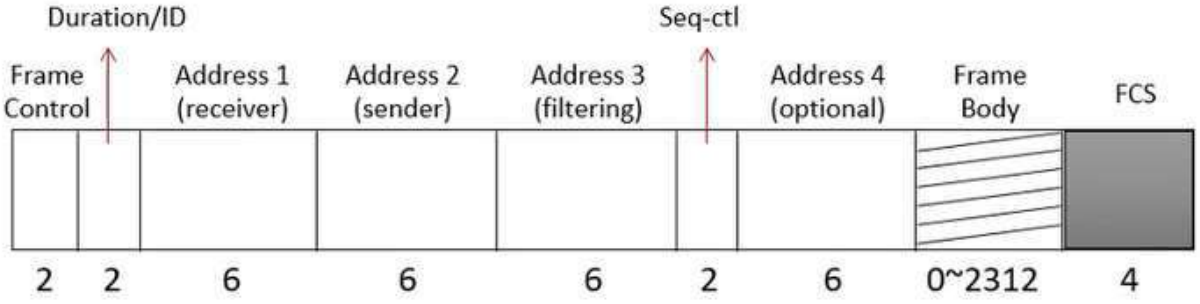
La couche liaison de données

Présentation de la trame 802.11 :

Le champ Body est aussi appelé bits de données. Il transmet les données de la couche supérieure entre stations. Il peut contenir jusqu'à 2312 groupes de données (Octets)



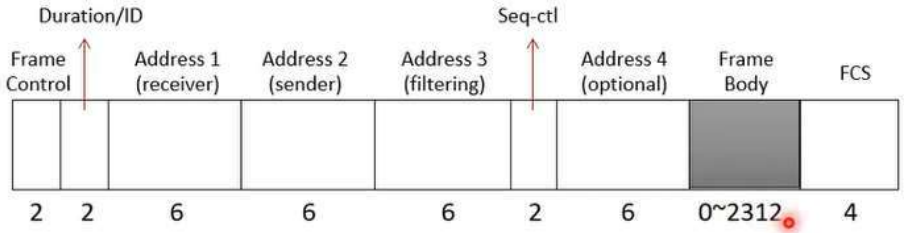
La trame 802.11 se termine avec un champ FCS pour s'assurer que la trame reçue est bien complète.



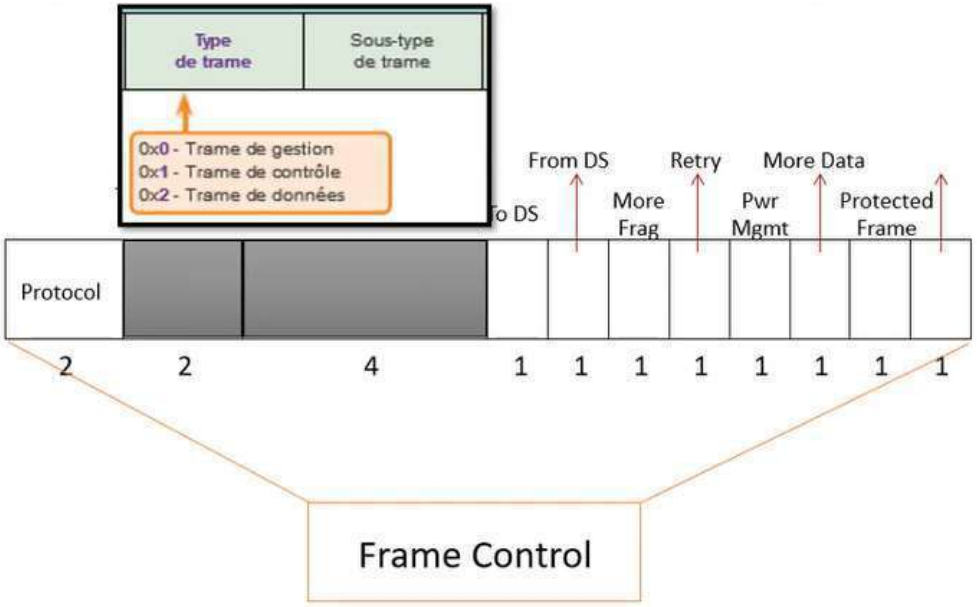
La couche liaison de données

Présentation de la trame 802.11 :

Le format de la trame change en fonction du type de la trame. Elle garde le format suivant si elle est de données :



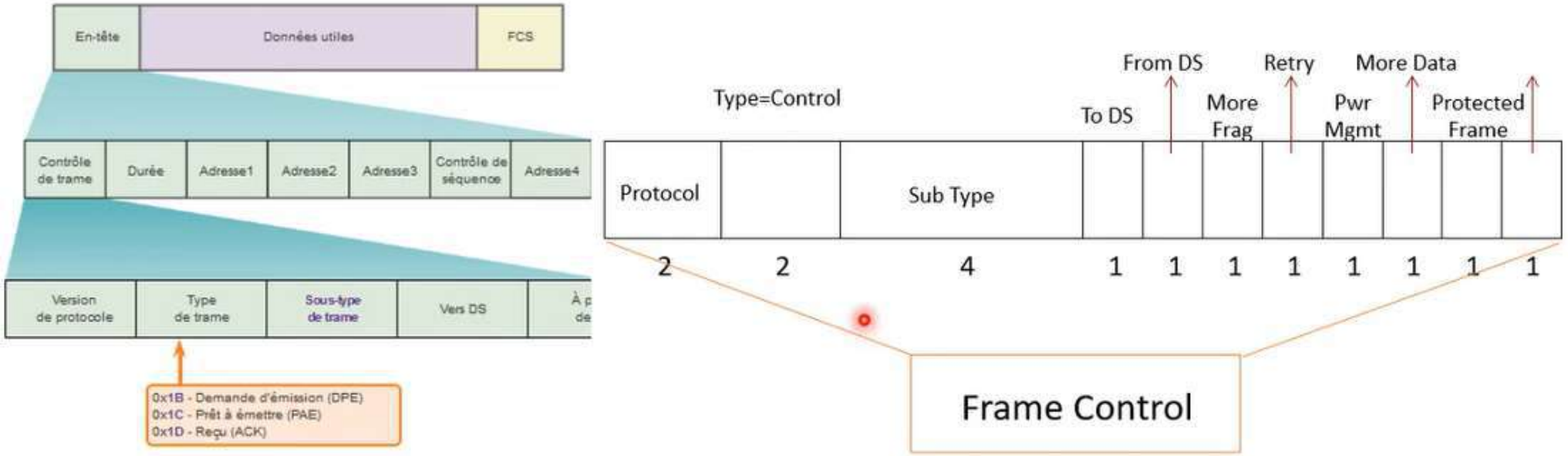
- ***Type values :***
  - **Management frame: 00**
  - **Control frame: 01**
  - **Data frame: 10**
  - **The value 11 is reserved.**
- Subtype is the specific type of frames



La couche liaison de données

Présentation de la trame 802.11 :

Si le type est une trame de contrôle, le format change. Le champ de contrôle est toujours le même.



Les trames de contrôle sont utilisées pour gérer les échanges d'informations entre un client sans fil et un point d'accès. Elles aident à éviter les collisions sur le support sans fil.

La couche liaison de données

Présentation de la trame 802.11 :

*802.11 Frame : **Control Frame : (Trame de controle) :***

Les trames de contrôle sont utilisées pour gérer les échanges d'informations entre un client sans fil et un point d'accès. Elles aident à éviter les collisions sur le support sans fil.

•**Trame DPE (RTS) (demande pour émettre)** : les trames DPE et PAE offrent un modèle facultatif de diminution des collisions pour les points d'accès présentant des clients sans fil masqués. Le client sans fil envoie une trame DPE comme première étape d'une connexion en deux étapes, ceci étant obligatoire pour l'envoi de trames de données.

•**Trame PAE (CTS) (prêt à émettre)** : un point d'accès sans fil répond à la trame DPE par une trame PAE. Celle-ci autorise le client sans fil demandeur à envoyer une trame de données. La trame PAE contribue à la gestion du contrôle des collisions en incluant une valeur temporelle. Ce délai réduit les risques que d'autres clients sans fil transmettent des données en même temps que le client demandeur.

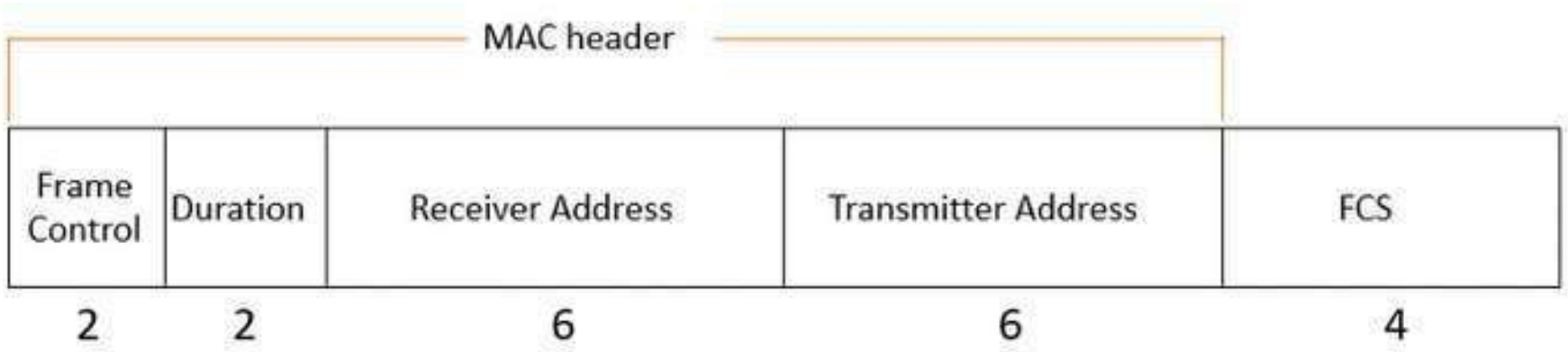
•**Trame ACK (Acknowledgment, reçu)** : après réception d'une trame de données, le client sans fil destinataire envoie une trame au client expéditeur si aucune erreur n'est détectée. Si l'expéditeur ne reçoit pas de trame ACK dans la durée impartie, il envoie à nouveau la trame.

Les trames de contrôle font partie intégrante de la transmission sans fil et jouent un rôle important dans le processus de gestion des conflits de supports sans fil, appelé méthode CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

La couche liaison de données

Présentation de la trame 802.11 : Trame de Contrôle

- Trame type RTS (DPE) : Lorsqu'un point d'accès veut transmettre des données vers une STA , il envoi un paquet RTS vers toutes les stations. Aucune station n'est donc autorisée à transmettre des données pendant une certaine période. Le format de la trame RTS est le suivant :

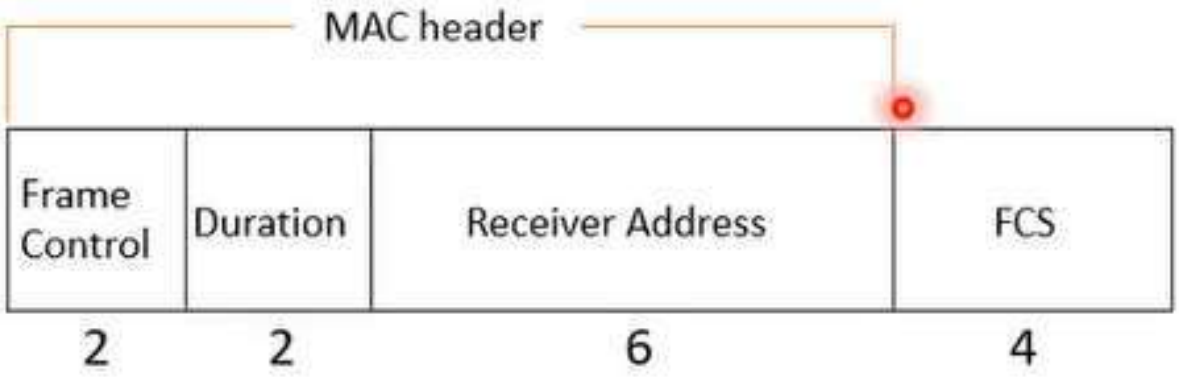


Trame RTS

La couche liaison de données

Présentation de la trame 802.11 : Trame de Contrôle

- Une fois qu'une station reçoit un paquet RTS. Elle répond par un paquet CTS. De même que précédemment, une fois un paquet CTS reçu par toutes les stations du réseau, aucune n'est autorisée à transmettre des données pendant une certaine durée (NV).

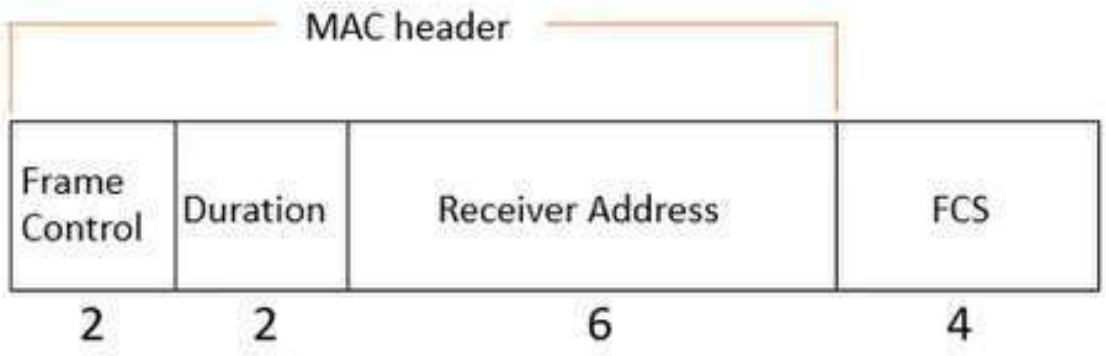


Trame CTS

La couche liaison de données

Présentation de la trame 802.11 : Trame de Contrôle

- Une station renvoie une trame ACK pour confirmer la réception d'un paquet unicast transmis par un émetteur.



Trame ACK

La couche liaison de données

Présentation de la trame 802.11 : Trame de Contrôle

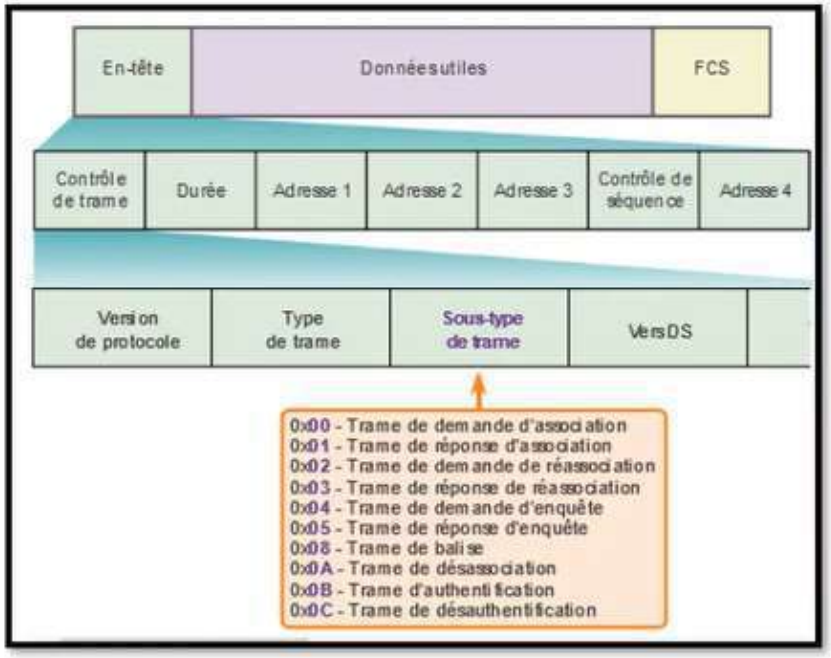
- Quand un nœud du réseau se réveille de son mode économique, il envoie une trame PS-Poll au point d'accès pour récupérer les trames dans le buffer. La trame du PS-Poll est comme suit :

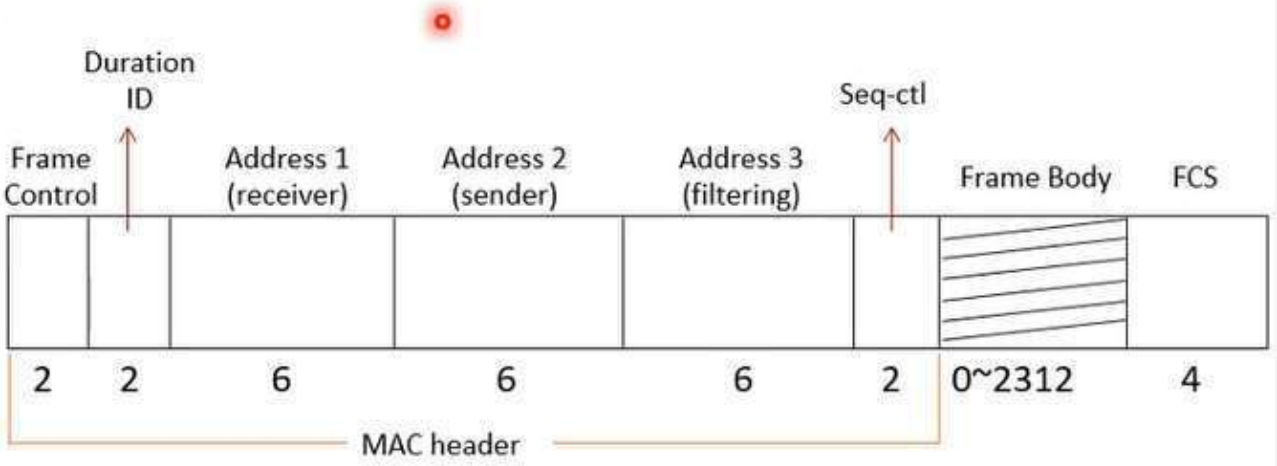
Trame PS-Poll

La couche liaison de données

Présentation de la trame 802.11 : Trame de gestion

- Les trames de gestion sont utilisées exclusivement pour la recherche, l'authentification et l'association avec un point d'accès.





La couche liaison de données

Présentation de la trame 802.11 : Trame de gestion

Les trames de gestion sont utilisées exclusivement pour la recherche, l'authentification et l'association avec un point d'accès.
La Figure 1 indique la valeur de champ des trames de gestion les plus courantes, telles que :

- **Trame de demande d'association** (0x00) : envoyée par un client sans fil, elle permet au point d'accès d'attribuer des ressources et d'effectuer une synchronisation. Cette trame contient des informations sur la connexion sans fil, notamment les débits de données pris en charge et l'identifiant SSID du réseau du client sans fil demandant l'association. Si la demande est acceptée, le point d'accès réserve de la mémoire et établit un ID d'association pour le périphérique.
- **Trame de réponse d'association** (0x01) : envoyée par un point d'accès à un client sans fil, elle indique si la demande d'association a été acceptée ou refusée. Dans le cas d'une acceptation, la trame contient différentes informations, telles que l'ID d'association et les débits de données pris en charge.
- **Trame de demande de réassociation** (0x02) : un périphérique envoie une demande de réassociation lorsqu'il se déconnecte du point d'accès déjà configuré et trouve un autre point d'accès au signal plus fort. Le nouveau point d'accès coordonne le transfert des éventuelles informations encore stockées dans la mémoire tampon du point d'accès précédent.
- **Trame de réponse de réassociation** (0x03) : envoyée par un point d'accès, elle indique si la demande de réassociation d'un périphérique a été acceptée ou refusée. Cette trame contient les informations nécessaires pour effectuer l'association, notamment l'ID d'association et les débits de données pris en charge.

La couche liaison de données

Présentation de la trame 802.11 : Trame de gestion

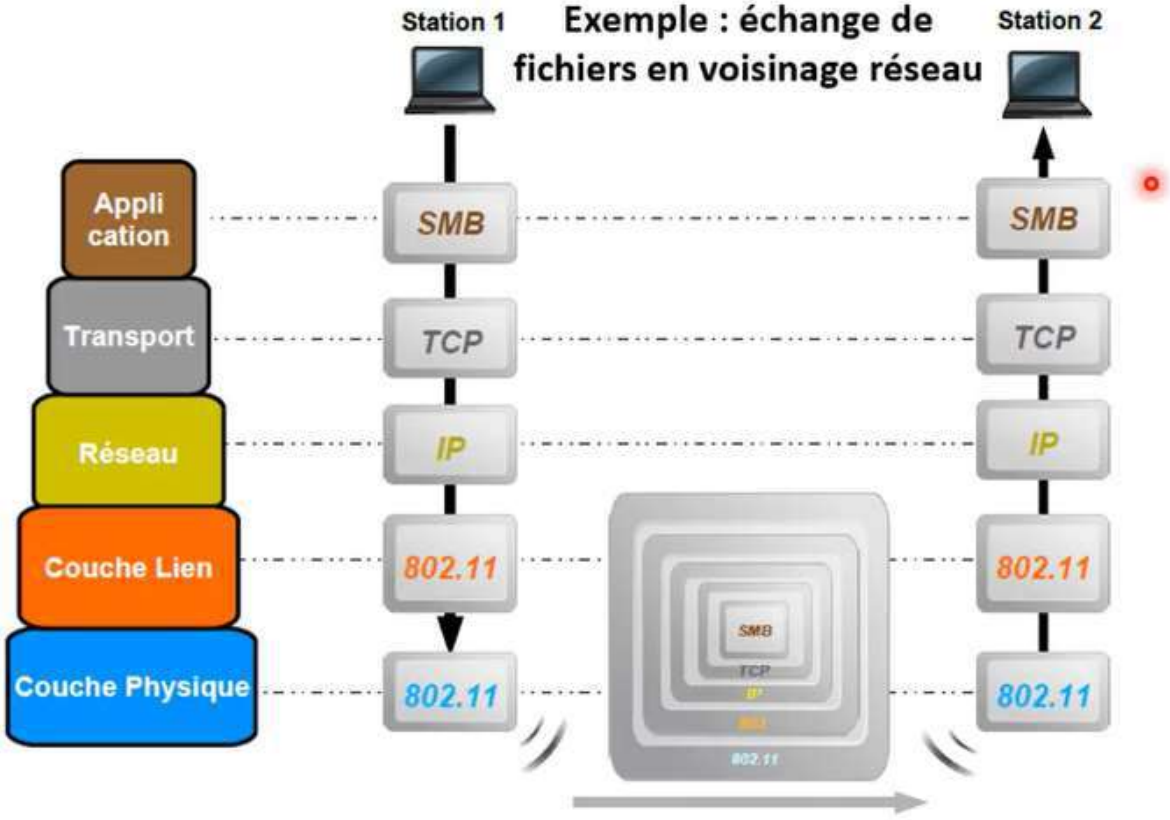
- **Trame de demande d'enquête** (0x04) : envoyée par un client sans fil demandant des informations à un autre client sans fil.
- **Trame de réponse d'enquête** (0x05) : envoyée par un point d'accès, elle contient des informations de fonctionnalité, telles que les débits de données pris en charge, renvoyées après une demande d'enquête.
- **Trame de balise** (0x08) : envoyée périodiquement par un point d'accès pour annoncer sa présence, elle fournit l'identifiant SSID, ainsi que d'autres paramètres préconfigurés.
- **Trame de désassociation** (0x0A) : envoyée par un périphérique qui souhaite interrompre une connexion. Cette trame permet au point d'accès d'annuler l'allocation de mémoire et de retirer le périphérique de la table d'association.
- **Trame d'authentification** (0x0B) : le périphérique d'origine envoie une trame d'authentification au point d'accès, en indiquant son identité.
- **Trame de désauthentification** (0x0C) : envoyée par un client sans fil qui souhaite annuler sa connexion à un autre client sans fil.

Les balises sont les seules trames de gestion pouvant être diffusées régulièrement par un point d'accès. Toutes les trames d'enquête, d'authentification et d'association sont utilisées exclusivement durant le processus d'association (ou de réassociation).

La couche liaison de données

Modèle TCP/IP en couches pour les réseaux Wifi :

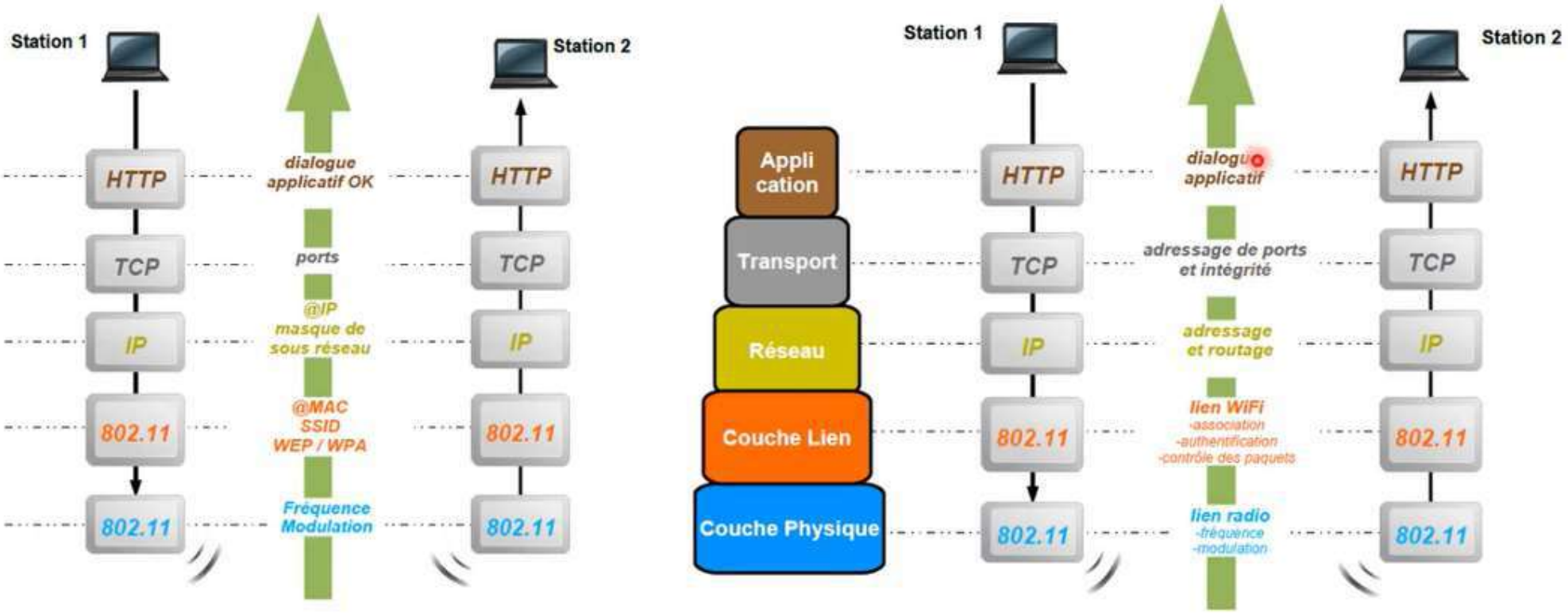
Communications entre deux stations en mode Adhoc : IBSS



La couche liaison de données

Modèle TCP/IP en couches pour les réseaux Wifi :

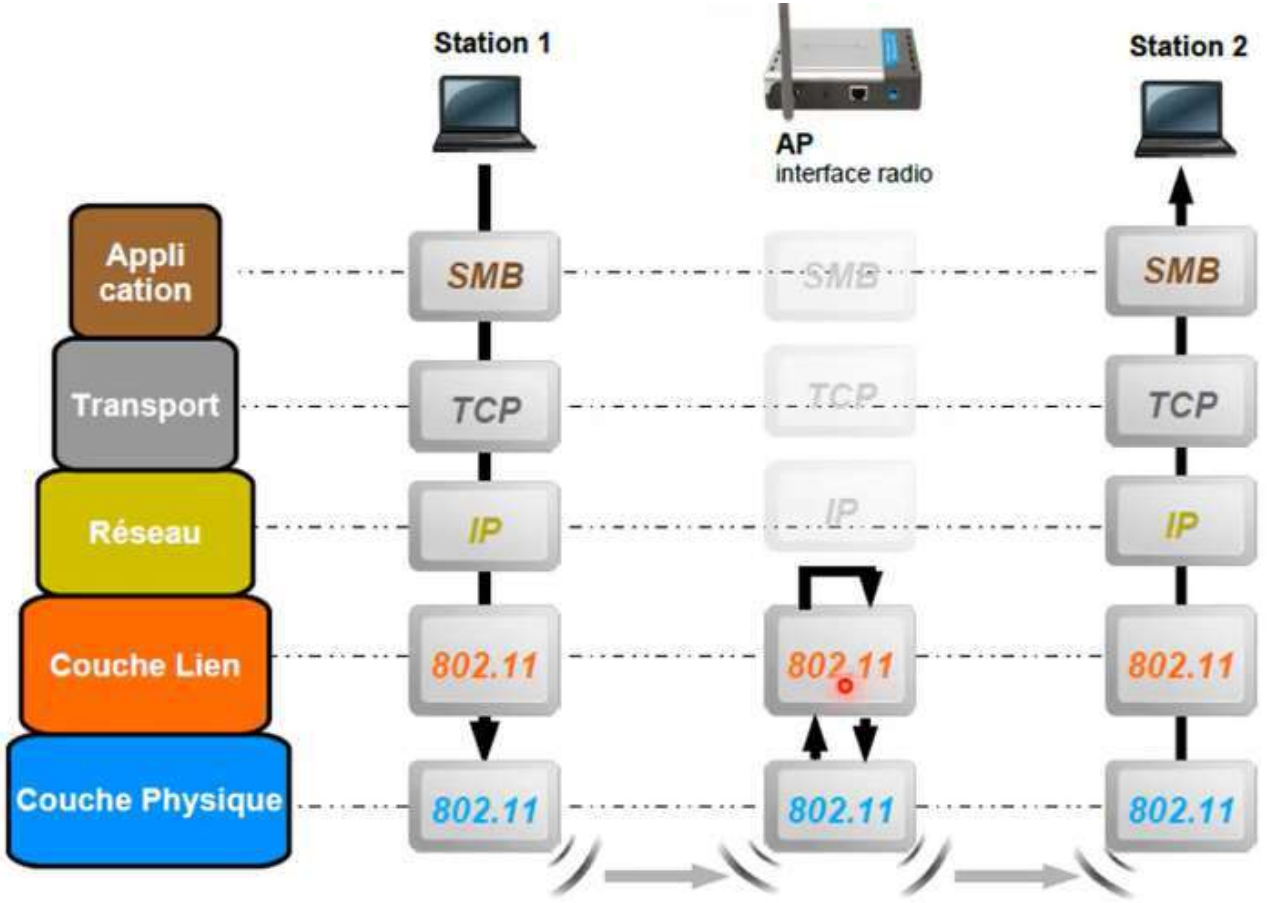
Communications entre deux stations en mode Adhoc : IBSS



La couche liaison de données

Modèle TCP/IP en couches pour les réseaux Wifi :

Communications entre deux stations en mode Infrastructure :



La couche liaison de données

Modèle TCP/IP en couches pour les réseaux Wifi :

Communications entre deux stations en mode Infrastructure :