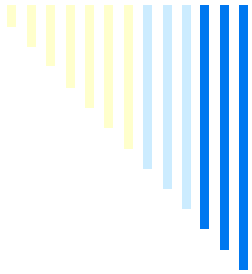
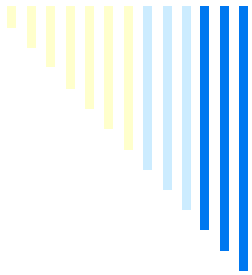


# Wi-Fi

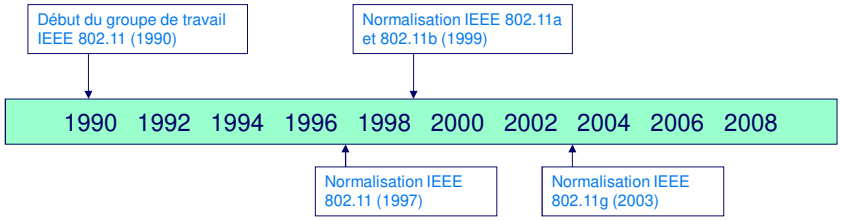
**Anthony Busson**



## Les différentes normes et l'historique.

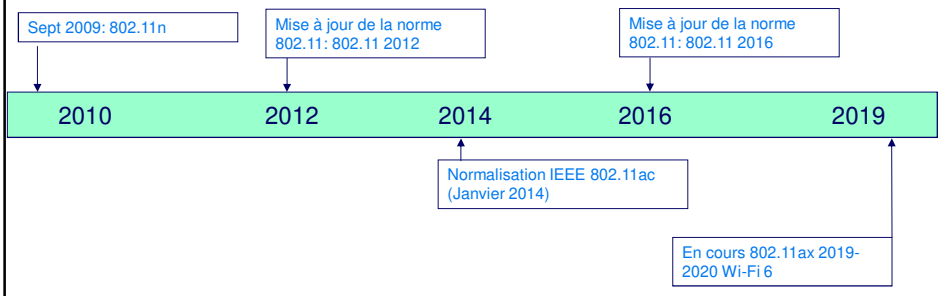
## Historique de la normalisation du 802.11

- Spécifications pour l'implémentation de réseaux numériques locaux à liaison sans fil (IEEE 802.11).
  - 802.11 norme initiale du WLAN débit max 2Mbps. Les autres sont des amendements à cette norme.
  - 802.11b WLAN débit max 11Mbps
  - 802.11g WLAN débit max 54Mbps
  - 802.11a WLAN débit max 54Mbps
  - 802.11f Gestion de l'itinérance (handover)
  - 802.11n amélioration de la couche physique (MIMO, etc.)
  - 802.11s Wireless Mesh Networks (en cours de normalisation)
  - 802.11e (qualité de service), 802.11i (sécurité), etc.




## Historique de la normalisation du 802.11

- Spécifications pour l'implémentation de réseaux numériques locaux à liaison sans fil (IEEE 802.11):
  - 802.11n (MIMO): de 54 à 600 Mbps
  - 802.11 mis à jour du standard initial 802. 11
  - 802.11ac

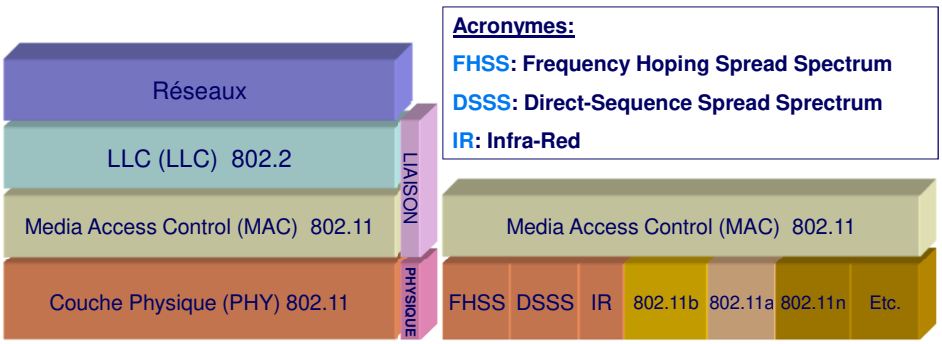


## IEEE 802.11 et Wi-Fi

- La norme IEEE 802.11 spécifie les caractéristiques d'un réseau local sans fil.
- Le Wi-Fi (Wireless-Fidelity) est la certification délivrée par la Wi-Fi alliance chargée de vérifier l'interopérabilité des matériels répondant à la norme 802.11.

## Définition

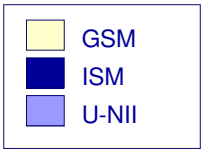
- La norme IEEE 802.11 (1997) spécifie 3 couches physique pour une même couche MAC.
- Les amendements 802.11b, 802.11g et 802.11a définissent leur propres couches physiques mais ne modifient pas la couche MAC.

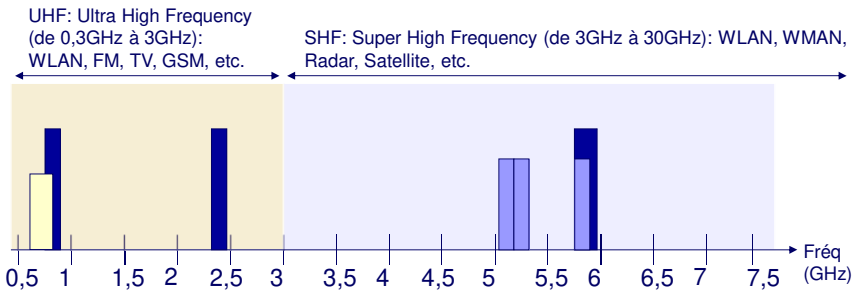


# La couche physique.

## Bande de fréquences

- Utilisation de bande libre (sans licence) ne nécessitant pas d'autorisation d'un organisme de régulation.
  - ISM: Industrial, Scientific and Medical.
  - U-NII: Unlicensed-National Information Infrastructure.



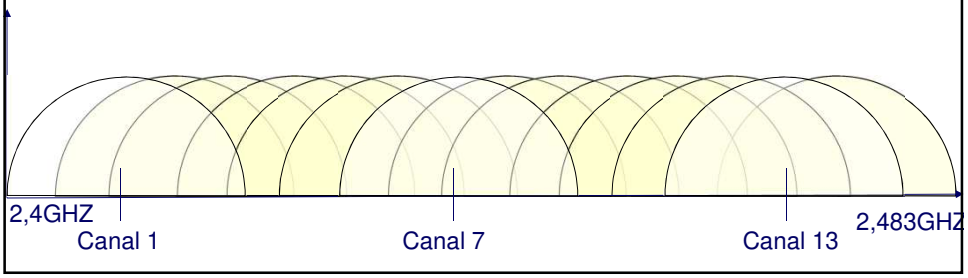



## DSSS: Direct-Sequence Spread Spectrum

- Utilisé par 802.11 et 802.11b
- Bande ISM [2,4GHz,2,483GHz] divisé en 14 canaux de 20MHz
- Ils n'existent que 3 canaux orthogonaux (1, 7 et 13).

| Canal | Fréquences (GHz) |
|---|---|
| 1 | 2,412 |
| 2 | 2,417 |
| 3 | 2,422 |
| 4 | 2,427 |
| 5 | 2,432 |
| 6 | 2,437 |
| 7 | 2,442 |
| 8 | 2,447 |
| 9 | 2,452 |

| Canal | Fréquences (GHz) |
|---|---|
| 10 | 2,457 |
| 11 | 2,462 |
| 12 | 2,467 |
| 13 | 2,472 |
| 14 | 2,477 |




## Exercice 1:

- Nous considérons un réseau Wi-Fi composé de 4 AP. 2 stations sont associées à chacun des APs. Faites un schéma avec les APs, les stations et indiquez quels sont les bandes et canaux utilisés entre chaque station et leur AP.

## Codage et modulation du 802.11 et 802.11b

- 802.11
  - Chaque bit est codé sur 11 bits (XOR avec le code de Barker) donnant 1 symbole.
    - 10110111000 pour un bit 1
    - 01001000111 pour un bit 0
  - Code approprié à la modulation d'onde radio.
  - Une phase est transmis à débit fixe de 1MS/s ou 2MS/s. Il s'agit ici des 11bits (1 symbole = 11bits)
  - La modulation varie suivant la qualité du signal
    - BPSK (Binary Phase Shift Keying): modulation de phase avec deux phases. Encode 1 bit par phase pour un débit de 1Mbps.
    - QPSK (Quadrature Phase Shift Keying): modulation de phase avec 4 phases (0°, 90°, 180° et 270°). Encode 2 bits par phase pour un débit de 2Mbps.
- 802.11b
  - Même principe que 802.11 HR/DSSS (High Rate DSSS).
    - Utilisation de code plus efficace (Complementary Code Keying) où on a soit 4bits soit 8bits pour un symbole,
    - et d'un débit symbole plus important (1,375MS/s).

## Exercice 2:

- Une liaison 802.11 a les propriétés suivantes:
  - le codage est donné par les deux tableaux suivants:

| Bits utiles | Code |
|---|---|
| 00 | 000 |
| 01 | 101 |
| 10 | 010 |
| 11 | 111 |

| Bits utiles | Code |
|---|---|
| 00 | 00 |
| 01 | 01 |
| 10 | 10 |
| 11 | 11 |

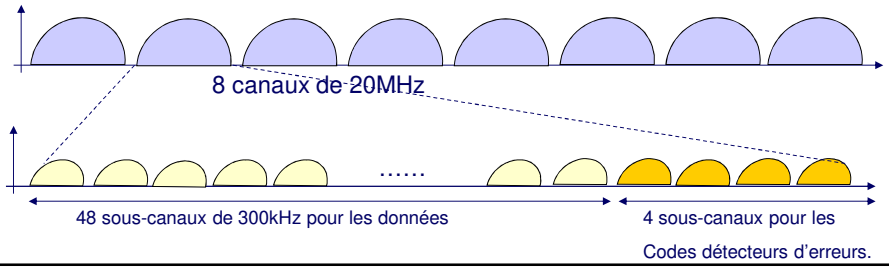
  - Les modulations possibles sont BPSK, QPSK, QAM-16 et QAM-64 avec 1M de motifs par seconde (baud).
- Faites un tableau représentant les débits utiles pour ces différentes valeurs.

## Codage et modulation du 802.11 et 802.11b (2)

| Débit (Mbps) | Longueur du code | Modulation | Nombre de bits par symbole | Débit (en MS/s) |
|---|---|---|---|---|
| 11 | CCK - 8 bits | QPSK | 8bits | 1,375MS/s |
| 5,5 | CCK - 8bits | QPSK | 4bits | 1,375MS/s |
| 2 | Code de Barker (11bits) | QPSK | 1bit | 2MS/s |
| 1 | Code de Barker (11 bits) | BPSK | 1bit | 1MS/s |

## OFDM: Orthogonal Frequency Division Multiplexing

- Exemple avec le 802.11a
- Division de la bande U-NII en 8 canaux de 20MHz
  - Utilisation d'une partie de la bande U-NII comprise entre 5,15GHz et 5,35GHz (sur un total de 300 MHz de large).
- Chaque canal est sous divisé en 52 sous canaux de 300KHz.
- La transmission a lieu en parallèle sur ces 52 canaux
  - 48 pour les données
  - 4 pour les codes détecteurs d'erreurs (FEC).



## Codage et modulation du 802.11a

Débit en MS/s (sur l'ensemble des sous canaux)=0,25MS/s.

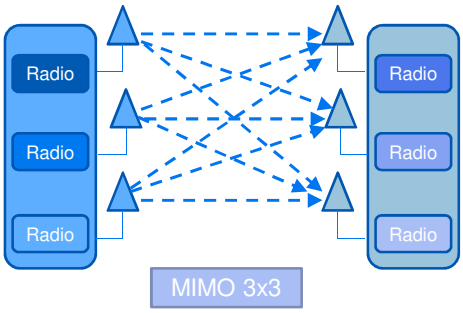
| Débit (Mbps) | Modulation | Taux de codage (« bits utiles »/ »taille du code ») | Bits par symbole d'un sous-canal | Bits utiles par symbole d'un sous-canal | Bits par symbole OFDM (ensemble des sous-canaux) | Bits utiles par symbole OFDM | Débit en Mbit/s par sous canal (non utile) | Débit en Mbit/s par sous-canal (utile) | Débit en Mbit/s sur l'ensemble des sous-canaux (non utile) |
|---|---|---|---|---|---|---|---|---|---|
| 6 | BPSK | ½ | 1 | ½ | 48 | 24 | 0,25 | 0,125 | 12 |
| 9 | BPSK | ¾ | 1 | ¾ | 48 | 36 | 0,25 | 0,1875 | 12 |
| 12 | QPSK | ½ | 2 | 1 | 96 | 48 | 0,5 | 0,250 | 24 |
| 18 | QPSK | ¾ | 2 | 3/2 | 96 | 72 | 0,5 | 0,375 | 24 |
| 24 | 16-QAM | ½ | 4 | 2 | 192 | 96 | 1 | 0,5 | 48 |
| 36 | 16-QAM | ¾ | 4 | 3 | 192 | 144 | 1 | 0,750 | 48 |
| 48 | 64-QAM | 2/3 | 6 | 4 | 288 | 192 | 1,5 | 1,0 | 72 |
| 54 | 64-QAM | ¾ | 6 | 9/2 | 288 | 216 | 1,5 | 1,125 | 72 |

## 802.11g

- Utilisation de la bande ISM
  - Problèmes d'interférences
  - Recouvrement des canaux
- Technique de codage CCK
- OFDM

## 802.11n (MIMO)

- Utilisation de plusieurs antennes en réception et/ou en émission
- Corrélation des signaux profitant de la diversité spatiale




- Meilleure décodage
- Débit: 288.8Mbit/s (20MHz) et 600Mbit/s (40MHz)

## 802.11ac

- Bande des 5GHz
- Basé sur le MIMO (jusqu'à 8 antennes)
- Modulation plus complexe
- Canaux plus large (80MHz ; 160MHz)
- Débit: 433 Mbits/s jusqu'à 6.77 Gbit/s

## Exercice 3

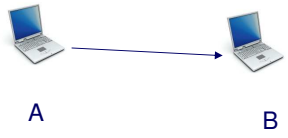
- Nous considérons un lien Wi-Fi 802.11a utilisant l'OFDM.
- Le codage est donné ci-dessous.
- Il y a 3 sous porteuses OFDM (pour simplifier)
- La modulation utilisé est BPSK (phase=0 pour un 0)
- Le nombre de motifs est de 2M « motifs » / sec
- Quel est le débit utile?
- On souhaite transmettre la chaîne binaire suivante 001011010:
  - En combien de temps sera-t-elle transmise?
  - Dessinez le signal correspondant à chaque sous porteuse

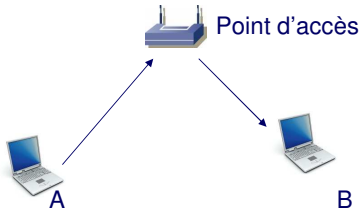
| Valeur binaire | Code | Valeur binaire | Code |
|---|---|---|---|
| 000 | 0000 | 100 | 1001 |
| 001 | 0101 | 101 | 0011 |
| 010 | 1010 | 110 | 1100 |
| 011 | 1000 | 111 | 1111 |

## La couche MAC

## Modes Wi-Fi/802.11

- Deux modes
  - Infrastructure
    - Chaque station doit être rattaché à un point d'accès
    - Toute communication transite par le point d'accès
  - Ad-Hoc
    - Les stations communiquent directement entre elles.




## Introduction de la problématique

- Nécessité de partager le support
  - Plusieurs transmissions en même temps interfèrent entre elles
  - Nécessité d'ordonnancer les transmissions de manière à ce qu'elles aient lieus à des moments différents
- Formater les trames
  - Identique à un réseau Ethernet:
    - Les données à transmettre sont encapsulées dans des trames
    - Le format de l'en-tête est différent de l'Ethernet

## Couche MAC

- Les fonctionnalités de la couche MAC 802.11 sont
  - Association
  - Accès au medium
  - Adressage et formatage des trames
  - Contrôle d'erreur
  - Fragmentation et réassemblage
  - Qualité de service
  - Gestion de l'énergie
  - Gestion de la mobilité
  - Sécurité.

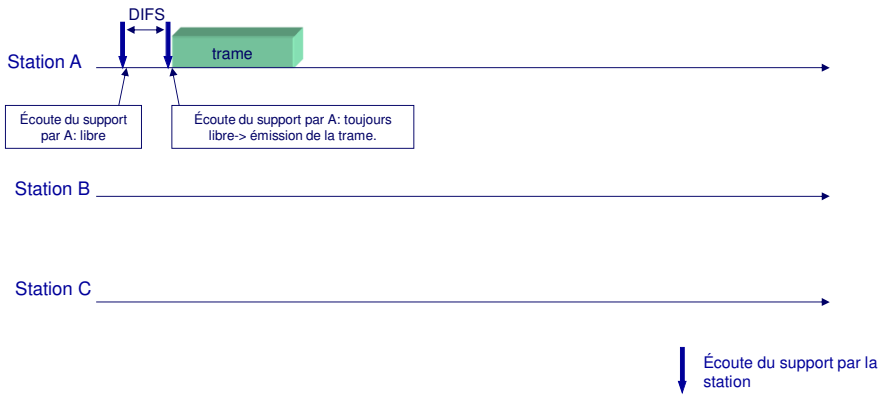
## Accès au medium

- Deux méthodes d'accès sont définies par la norme IEEE 802.11
  - DCF (Distributed Coordination Function). Permet le support de transmissions asynchrones tout en garantissant une chance égale d'accéder au medium. Possible collision.
  - PCF (Point Coordination Function). Système centré sur le point d'accès. Celui-ci gère les transmissions de données entre les stations du réseau. Pas de collision possible.

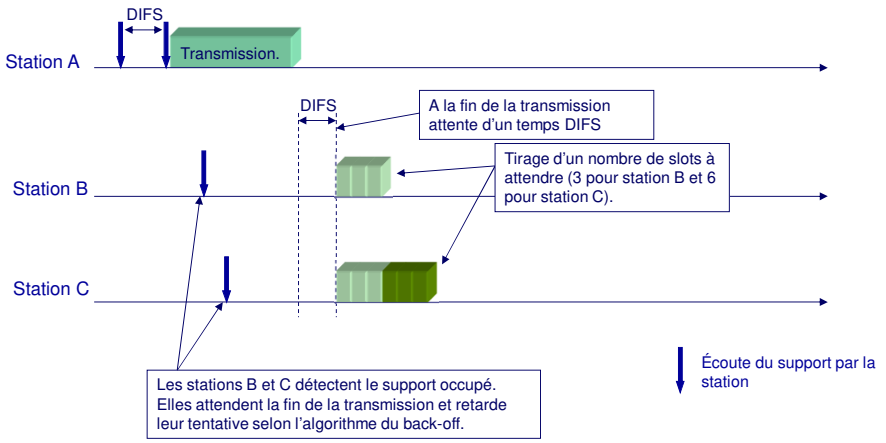
## DCF: Distributed Coordination Function CSMA/CA

- CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance
  - Chaque station souhaitant émettre une trame, écoute le support avant émission.
    - Si support libre, attente d'un temps constant (DIFS) et émission de la trame (si le support est toujours libre).
    - Si support occupé, on attend une durée NAV ou que le support devienne libre. On attend un DIFS et une durée aléatoire (back-off). On essaye alors de retransmettre.

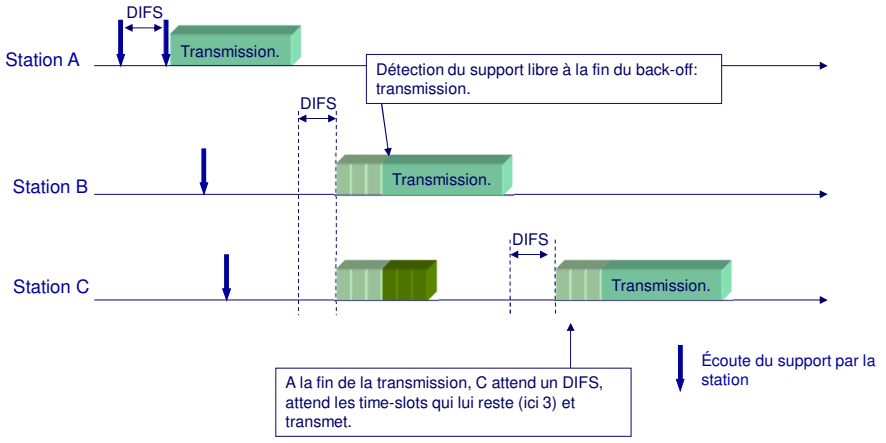
## DCF: Distributed Coordination Function CSMA/CA



# DCF: Distributed Coordination Function CSMA/CA

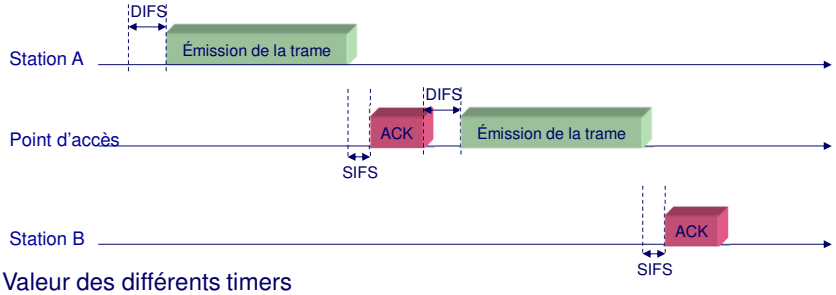



# DCF: Distributed Coordination Function CSMA/CA



# Déroulement d'une transmission.

- Émission de la station A à la station B (en mode infrastructure).
- Chaque trame doit être acquittée par le récepteur.
- Dans l'en-tête des trames, un champ *duration* permet aux stations à l'écoute de savoir combien de temps elles doivent attendre jusqu'à la fin de la transmission (trame+ack).

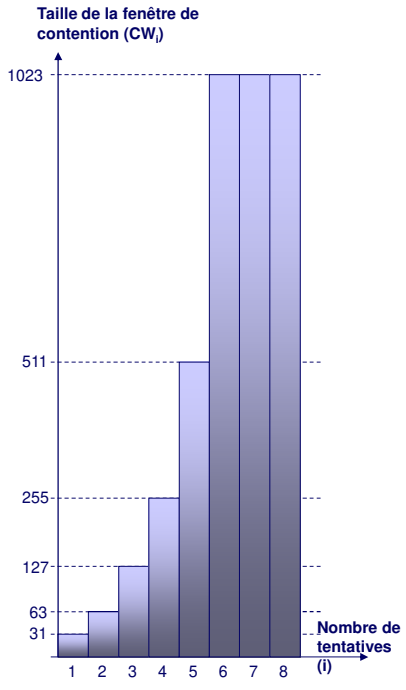



Valeur des différents timers

| | 802.11 | 802.11b | 802.11g |
|---|---|---|---|
| Timeslot (µs) | 50 | 20 | 9 |
| SIFS(µs) | 28 | 10 | 16 |
| DIFS(µs) | 128 | 50 | 25 |

# Calcul du back-off.

- Le back-off est pris au hasard (uniformément) dans une fenêtre [0,CW].
- $T_{BACKOFF}$=Random(0,$CW_i$)xtimeslot
- $CW_i$ = Min($2^{k+i}$-1,1023) avec
  - k: nombre lié à la valeur minimale de la fenêtre de contention (k=5). La taille de fenêtre minimale est $2^k$-1 ($CW_{Min}$=31).
  - i: nombre de tentative (nombre de collisions subies).
- A chaque tentative, le temps d'attente moyen est augmenté (croissance exponentielle).

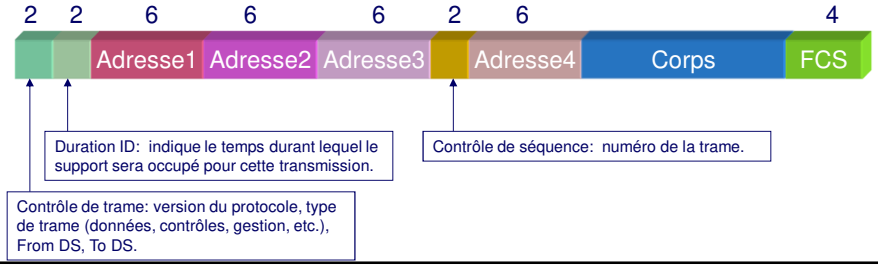


## Exercice 4: Accès au medium

- Dans cet exercice, on vous demande de dérouler l'algorithme d'accès au medium pour 4 stations qui essayent d'émettre 5 trames.
- La station A a une seule trame à émettre et elle commence à écouter le support au slot 1. La station B a une seule trame à émettre et elle commence à écouter le support au slot 4.2.
- La station C a deux trames à émettre consécutivement. Elle commence à écouter le support au slot 13.5.
- La station D a une seule trame à émettre et elle commence à écouter le support au slot 7.3.
- Les tirages aléatoires (en nombre de slots) effectués par les stations pour l'algorithme du back-off sont les suivants (A=12 ;11 - B=3 ; 4 - C=2 ; 5 - D=6 ; 3). La transmission d'une trame est de 3 slots.
- Celle d'un acquittement est de 1 slot (en réalité c'est plus long). DIFS=2 slots. SIFS=1 slot. On néglige les temps de propagation. Toutes les stations émettent au point d'accès.

## Adressage et formatage des trames

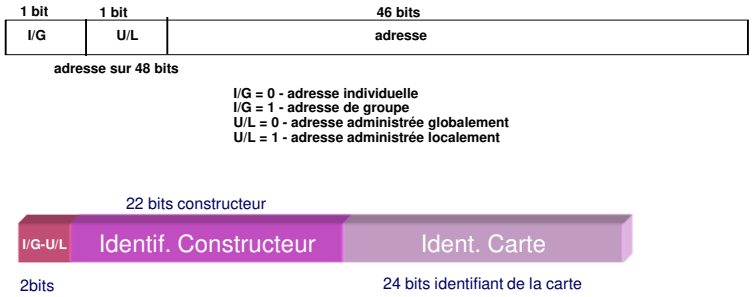
- 3 types de trames
  - Trames de données
  - Trames de contrôles (RTS, CTS, ACK, etc.)
  - Trames de gestion (beacon, association, etc.)
- Suivant le type de trames, le format ci-dessous varie.
- Les trames chiffrées ont un format différents.



## Adresse Ethernet ou adresse IEEE

Les adresses Wi-Fi ou Ethernet (EUI-48) ont été normalisé par l'IEEE.

Elles sont uniques pour chaque carte.





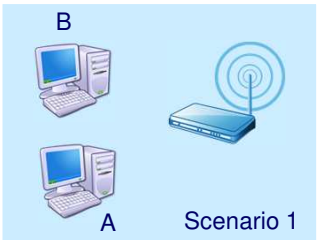


## Adresse et valeurs des bits « From DS » et « To DS »

- From DS: si égale à 1 indique que la trame provient du « Distribution Service » (de l'AP).
- To DS: si égale à 1 indique que la trame est à destination du « Distribution Service » (vers l'AP).
- Adresse 1: destinataire directe (adresse du prochain saut Wi-Fi)
- Adresse 2: source émettrice de la trame (le dernier émetteur)
- Adresse 3: celle qui manque.
- Adresse 4: La source qui a initialement initié le paquet.

## Exercice 5: les adresses

- Décrivez les adresses pour la transmission des trames de A -> B dans les scénarios ci-dessous.
- MAC de A: @MAC-A, etc.



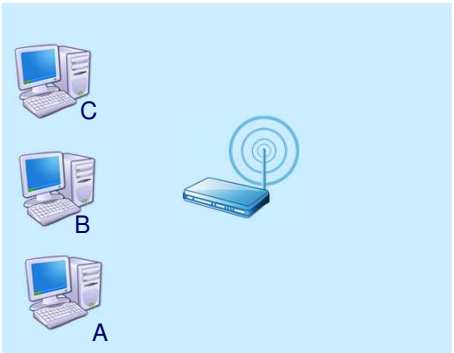
Scenario 1

Scenario 2

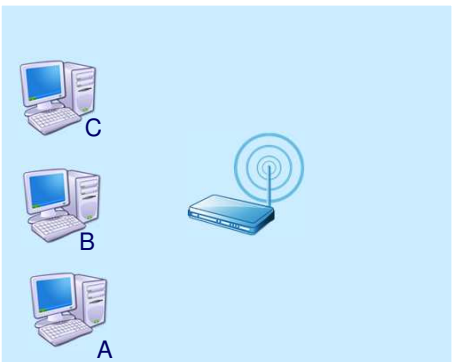
Scenario 3

## Exercice 5: adresses et acquittement

- Décrivez les adresses pour les 2 scenarios suivant (comme pour l'exercice précédent)
- Décrivez les acquittements



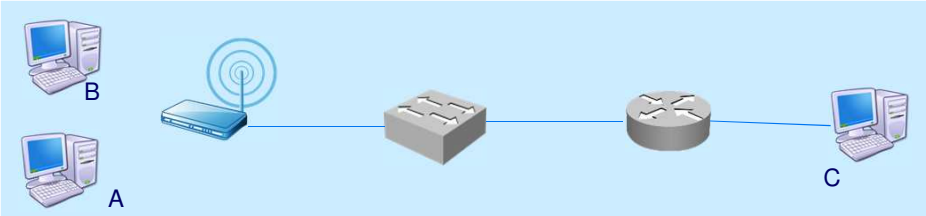
Scenario 1: trame de A vers B en unicast



Scenario 2: trame de A en broadcast

## Exercice 6: interaction Wi-Fi Ethernet IP

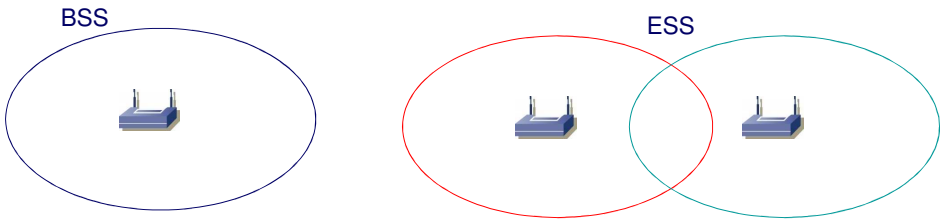
- A veut envoyer un paquet IP à C (sur un autre sous réseau)
- Une requête ARP est effectué par A au préalable
- Puis le paquet est envoyé
- Décrivez :
  - Toutes les trames envoyés/émises pour la requête et la réponse ARP avec les adresses au niveau Wi-Fi
  - Les tables de commutations sont elles à jour?
  - Même travail pour le paquet IP




## Opération de gestion

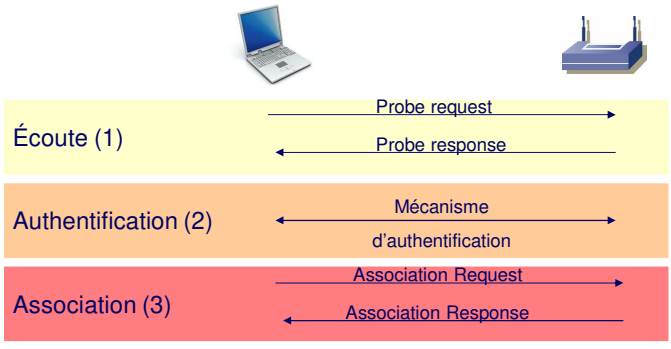
## Mode infrastructure: deux types de service

- BSS: Basic Service Set
  - Le réseau WLAN est constitué d'un seul point d'accès.
- ESS: Extended Service Set
  - Le réseau WLAN est constitué de plusieurs point d'accès.
  - Réseau constitué de cellule.
  - Les canaux des cellules adjacentes doivent être différentes.
- A chaque point d'accès est associé un SSID (Service Set ID). Celui identifie de manière unique le réseau Wi-Fi.
  - Un ESS est constitué d'un ensemble d'AP ayant le même SSID.



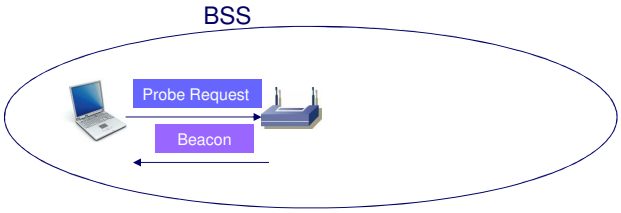

## Association à un point d'accès

- Chaque station doit s'associer à un point d'accès.
  - Découverte du point d'accès
  - Authentification
  - Association



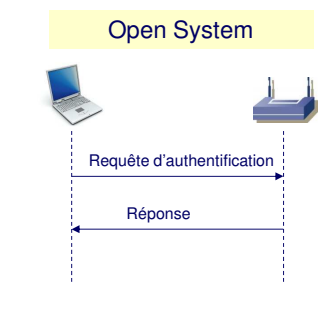
# Écoute

- Les AP diffusent régulièrement des messages *beacon frame* permettant de s'identifier et d'indiquer les paramètres du réseau.
- Au démarrage des cartes Wi-Fi, les stations scan toutes les fréquences pour écouter ces *beacon frames (écoute passive)*. Cela permet de lister et de connaître les paramètres des WLAN.
- Ces informations peuvent être obtenues plus rapidement par une station si elle émet un *probe request (écoute active)*.

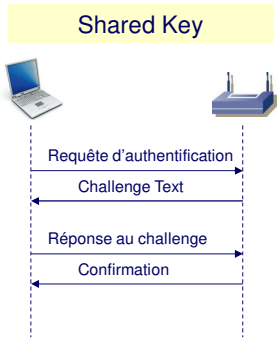



# Authentification

- Deux types
  - Open System Authentication
  - Shared Key Authentication



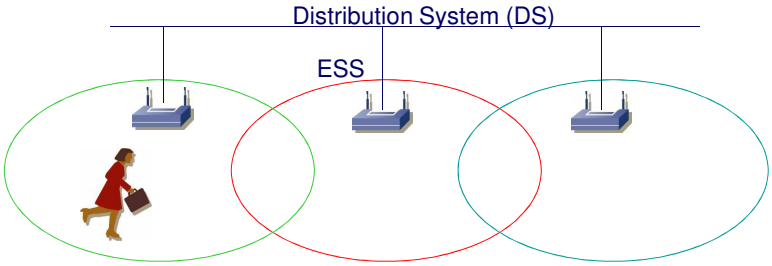

Pas véritablement d'authentification, toutes les stations sont acceptés.




Utilisé avec la clé secrète du WEP, le challenge est crypté avec la clé.

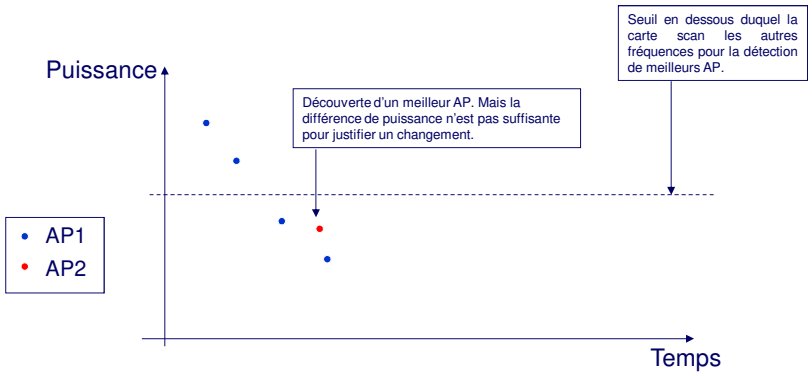
## Handovers.

- Dans un BSS, la station peut être mobile mais doit rester dans la cellule de l'AP.
- Dans un ESS, la station peut être mobile et passer d'une cellule à une autre sans perte de connectivité (handover de niveau 2).
- Les cartes des stations se désassocie de l'AP courant pour se réassocier à un AP offrant de meilleur conditions (signal).




## Exemple de mécanisme de handover (Lucent).

- Condition d'un passage d'un AP à un autre (dans le même ESS).



## Exemple de mécanisme de handover (Lucent).

- Condition d'un passage d'un AP à un autre (dans le même ESS).