

*Centre universitaire de Mila, Algérie
Domaine : Mathématique et Informatique*

*1^{er} année master Informatique (STIC)
Module : Réseaux et informatique mobile*

Chapitre 03
Réseaux locaux sans fil



Plan

- ❑ Réseau Local Sans Fil – WLAN
- ❑ Eléments d'un réseau sans fil
- ❑ Architecture (Mode opératoire)
- ❑ Allocation du spectre de fréquence
- ❑ Standard WIFI (IEEE 802.11)
 - Variantes
 - Normalisation
 - Couche physique
 - Couche liaison
 - Scénario d'échange WIFI

Introduction

Réseau Local San Fil – WLAN

- Réseau informatique sans fil en sa plus petite forme.
- Relie des équipements sans fils (ordinateur, PDA, périphériques sans fils, etc.)
- Un rayon allant jusqu'à des centaines de mètres.
- Différentes normes: IEEE 802.11, HyperLAN, etc.



Éléments d'un réseau sans fil

Un réseau sans fil est composé d'un ou plusieurs **points d'accès qui connectent** plusieurs **stations mobiles**.

◆ Station sans fil (ou mobile):

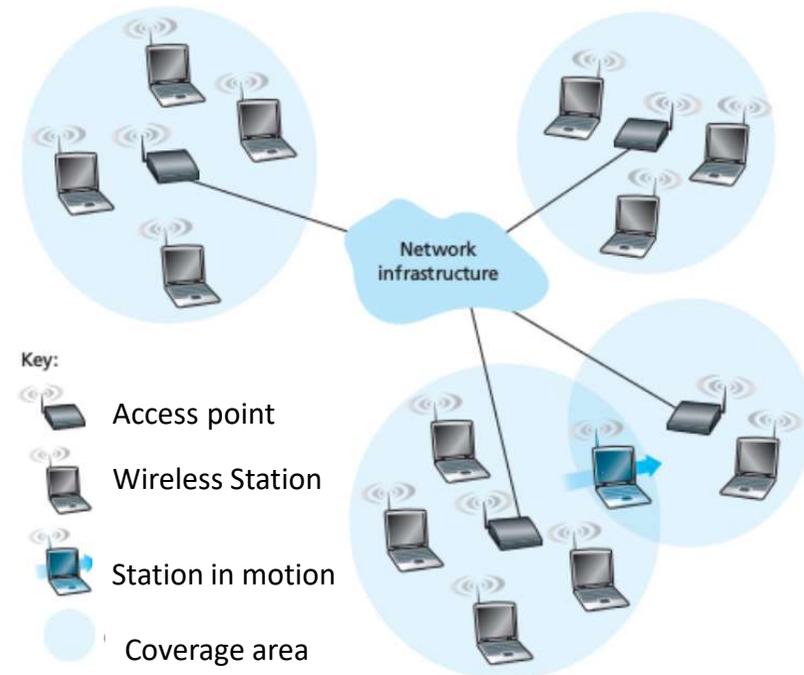
- Equipé d'une carte Wi-Fi (émetteur/récepteur)
- PC, PDA, Téléphone, etc.

◆ Point d'accès (Access Point – AP)

- station intégré au système de distribution
- couvre une zone permettant la connectivité des stations qui y appartiennent

◆ Zone de couverture (Cellule)

- Zone couverte par le signal du AP



N.B. Il a une **architecture cellulaire** où:

- Les stations mobiles utilisent les points d'accès pour communiquer entre eux.
- Sa taille dépend de la zone de couverture du point d'accès, aussi appelé **cellule**.

Architecture (Mode opératoire)

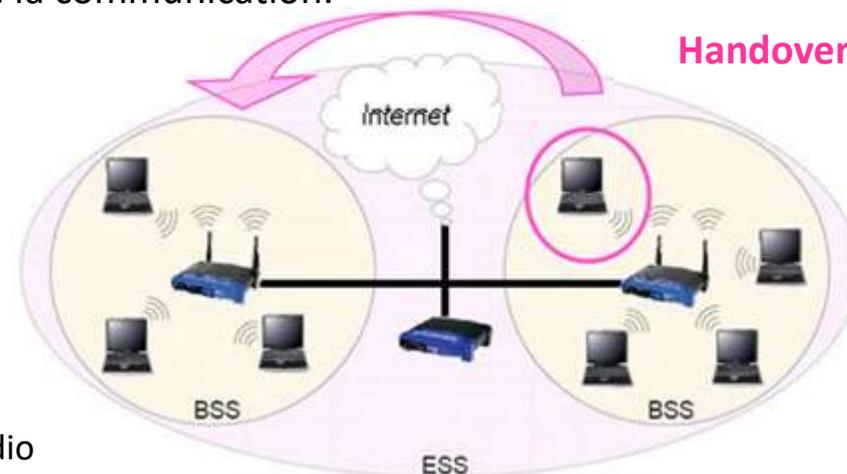
Deux types d'architecture :

◆ Mode avec infrastructure

- Les communications passent par une station de base : AP (Access Point), BTS (Base Transmission Station).
 - ✓ **Infrastructure avec BSS**
 - Un point d'accès.
 - ✓ **Infrastructure avec ESS**
 - Plusieurs points d'accès reliés entre eux par un DS (Distribution System).
 - Passer de l'un à l'autre en utilisant le mécanisme de **Handover**
 - Sans interruption de la communication.



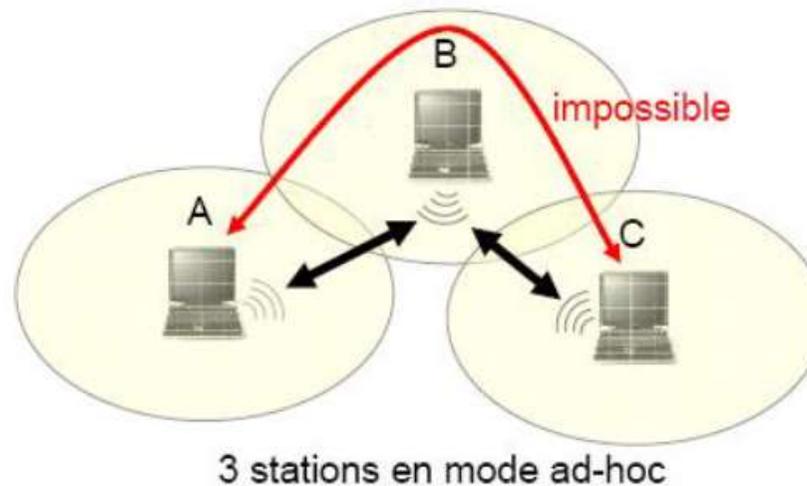
Groupe de stations utilisant la même fréquence radio



Architecture (Mode opératoire) - suite

◆ Mode ad-hoc (sans infrastructure)

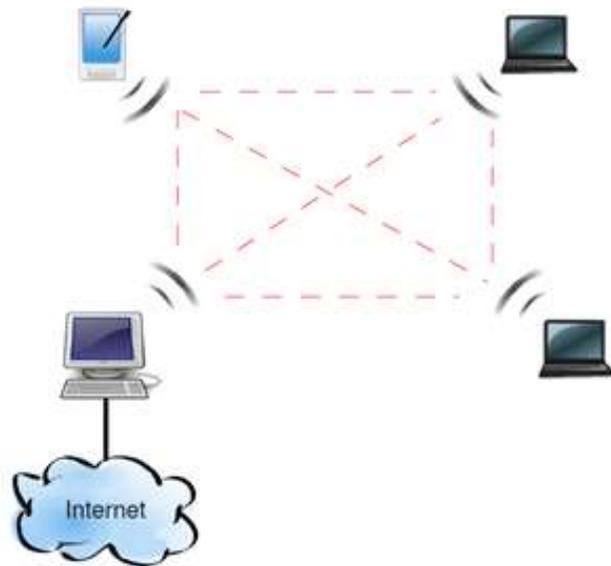
- ou **IBSS** : Independent Basic Service Set, c'est-à-dire **mode point à point**
- Pas de points d'accès (station de base)
- Une station peut seulement transmettre aux stations dans son rayon de couverture .
- Les stations s'organisent pour acheminer les données



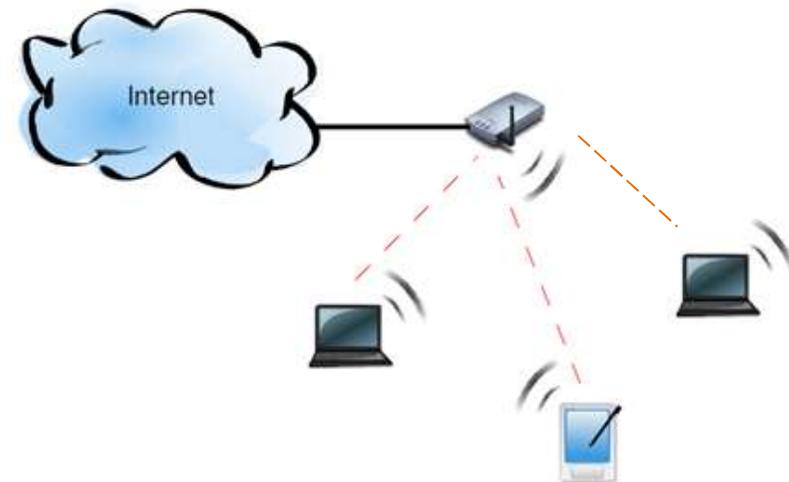
Réseau poste à poste (chaque poste peut communiquer avec chacun des autres postes)

Architecture (Mode opératoire) - suite

Quelque soit l'architecture du réseau sans fil, il se connecte à un réseau filaire (Internet)



Mode Ad hoc



Mode avec infrastructure

Allocation du spectre de fréquence

- Les ressources spectrales sont limitées.
 - ◆ Chaque pays a une agence qui contrôle et alloue les ressources spectrales.
 - ◆ Les ressources sont contrôlées par Agence Nationale des fréquences (ANF)



- Bandes de fréquences sans Licence (utilisés Gratuitement)

(ISM = Industrial, Scientific, and Medical)

900 MHz	ISM Band I (Cordless phones, 1G WLANs)	902-928 MHz
2.4 GHz	ISM Band II (Bluetooth, 802.11b WLANs)	2.4-2.4835 GHz
5.8 GHz	ISM Band III (Wireless PBX)	5.725-5.85 GHz
5 GHz	NII Band I (Indoor systems, 802.11a WLANs)	5.15-5.25 GHz
5 GHz	NII Band II (short outdoor and campus applications)	5.25-5.35 GHz
5.8 GHz	NII Band III (long outdoor and point-to-point links)	5.725-5.825 GHz

(U-NII = Unlicensed National Information Infrastructure)

Standard WIFI - IEEE 802.11

WI-FI - Wireless Fidelity

- C'est une norme WLAN.
- Réponds au standard **IEEE 802.11**.
- Développé depuis 1990 (premier réseau WiFi est publié en 2001)
- Plusieurs variantes : 802.11b, 802.11a, 802.11g, 802.11n

IEEE 802.11

- Opère sur 2,4 GHz.
- Débit de 2 Mb/s (modulation DSSS)
- Pas d'interopérabilité

IEEE 802.11b

- Opère sur 2,4 GHz
- Débit de 11 Mb/s
- Interopérable

IEEE 802.11a

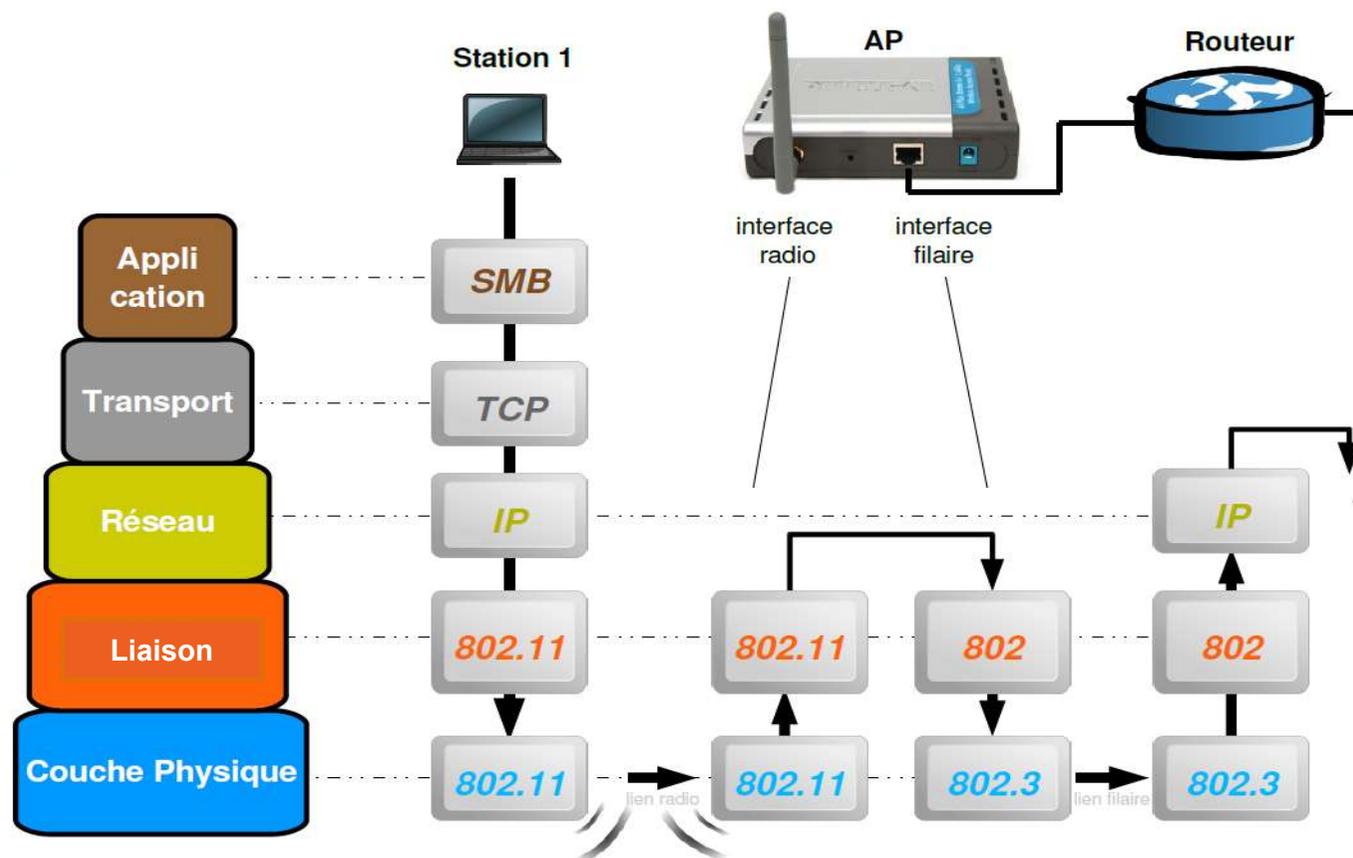
- Opère sur 5 GHz (WiFi 5)
- Haut débit de 54 Mb/s théoriques

IEEE 802.11g

- La norme la plus répandue
- Débit de 54 Mb/s
- Compatibilité ascendante avec la norme 802.11b.

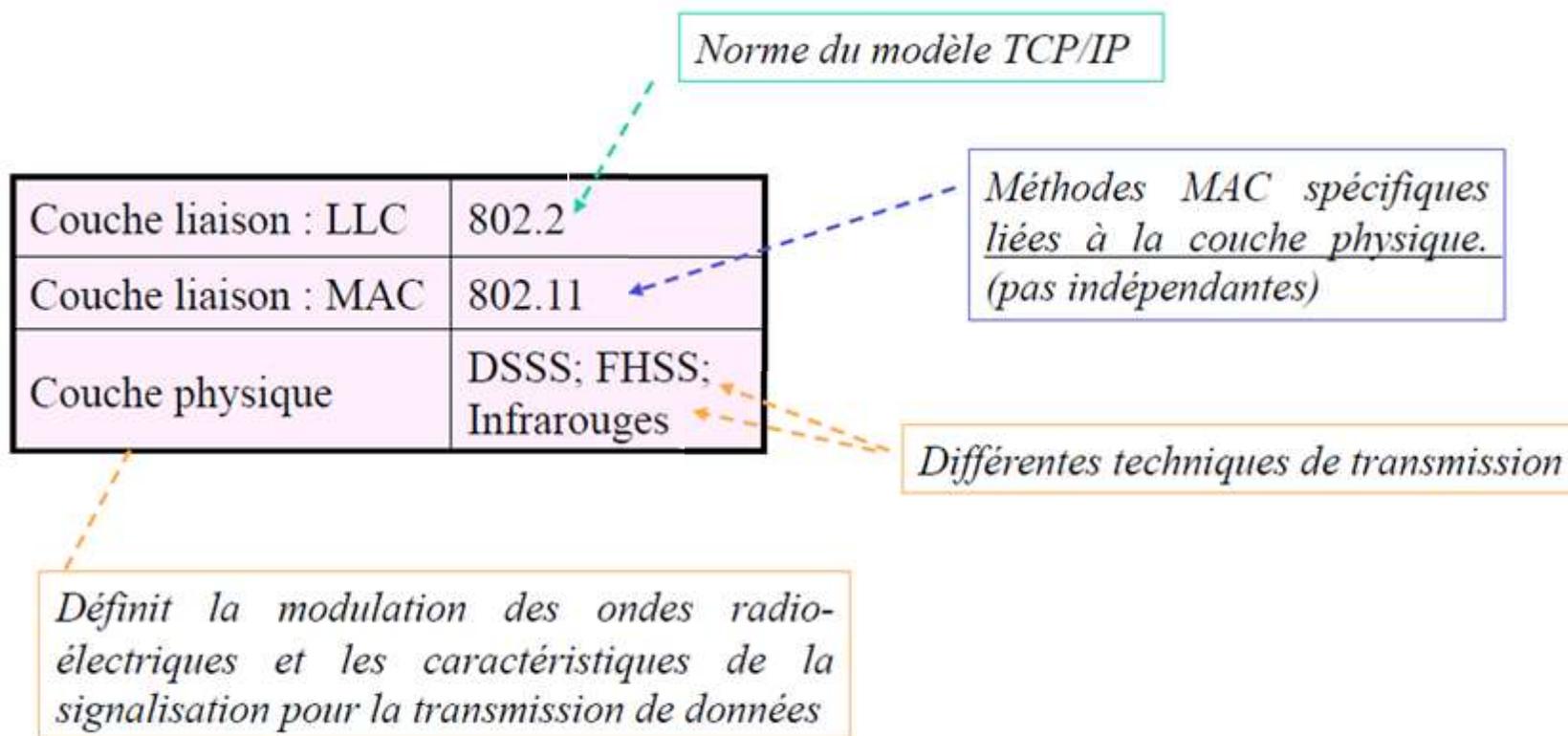
Standard WIFI - IEEE 802.11

Normalisation (couches)



Standard WIFI - IEEE 802.11

Normalisation (couches)



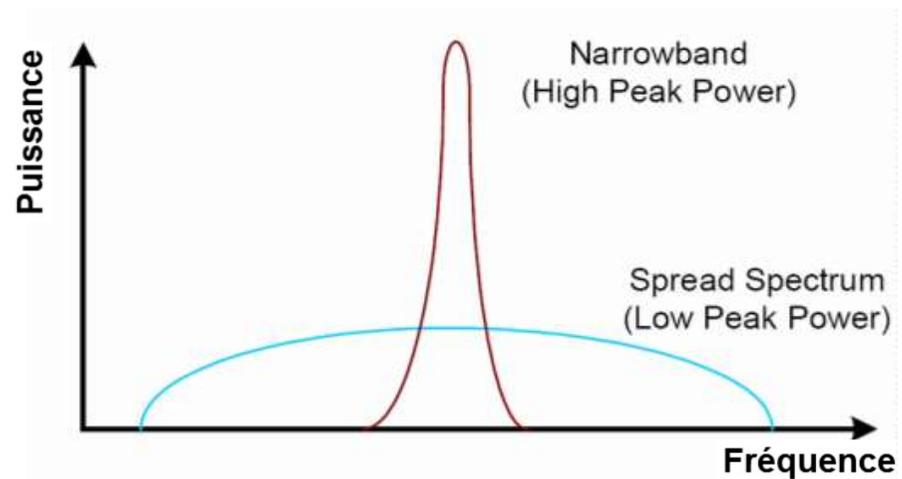
Standard WIFI - IEEE 802.11

Couche physique

- Différentes bandes de fréquences
 - ◆ La bande 2,4 GHz : 802.11, 802.11b, 802.11g
 - ◆ La bande 5GHz: 802.11a et 802.11n
- Transmission par étalement du spectre (modulation)

Etalement du spectre vs Bande étroite

- Transmission en bande étroite (Narrow Band)
 - Sensibilité :
 - ✓ Au bruit (S/N ratio)
 - ✓ Interférences
 - ➔ Débit faible.



Transmission par principe d'étalement du spectre ➔ **Transmission « Large Bande »**

Standard WIFI - IEEE 802.11

Couche physique

■ Etallement du spectre

- **Idée:** Au lieu de transmettre par un canal avec une bande passante étroite, on transmet par un canal avec la bande passante très large, mais à la puissance très petite.
 - ◆ Elle offre une bonne protection contre l'interférence entre symboles.
 - ◆ La technique est bien adaptée aux systèmes multiutilisateurs;
- Une technique de **modulation** où :
 - ◆ Le signal obtenu occupe une bande plus large que la bande du signal de données.
 - ◆ Le signal d'étalement est pseudo-aléatoire (le signal étalé ressemble à un bruit).
 - ◆ Le des-étalement à la réception est obtenue par la corrélation du signal reçu avec le code d'étalement utilisé.
- Deux techniques d'étalement du spectre existent:
 - ◆ Etallement du spectre par code directe (DSSS)
 - ◆ Etallement du spectre par (FHSS)

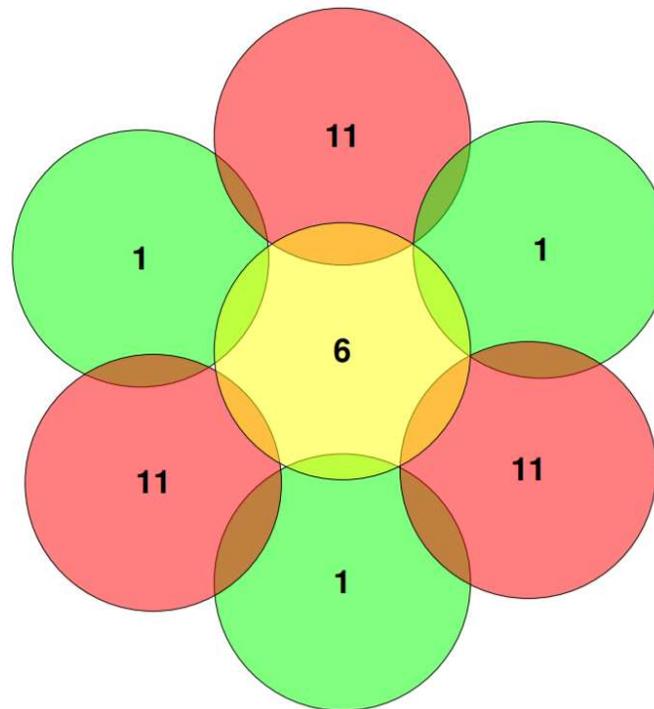
Standard WIFI - IEEE 802.11

Couche physique

DSSS (Direct Sequence Spread Spectrum)

- La transmission ne se fait que sur un seul canal
- Problème de recouvrement
- Superposition de 3 réseaux au sein d'un même espace

Affectation des canaux

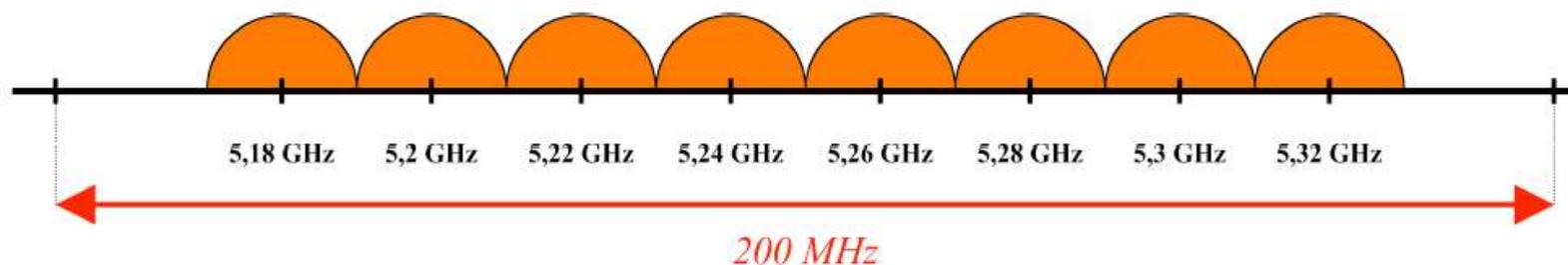


Standard WIFI - IEEE 802.11

Couche physique

DSSS (Direct Sequence Spread Spectrum)

- ◆ **La fréquence 5 GHz - Bande UN-II**
 - Largeur de bande 200 MHz
 - Bande divisée en 8 canaux de 20 MHz
 - Pas de problème de recouvrement (atténuation du bruit)
 - Co-localisation de 8 réseaux au sein d'un même espace



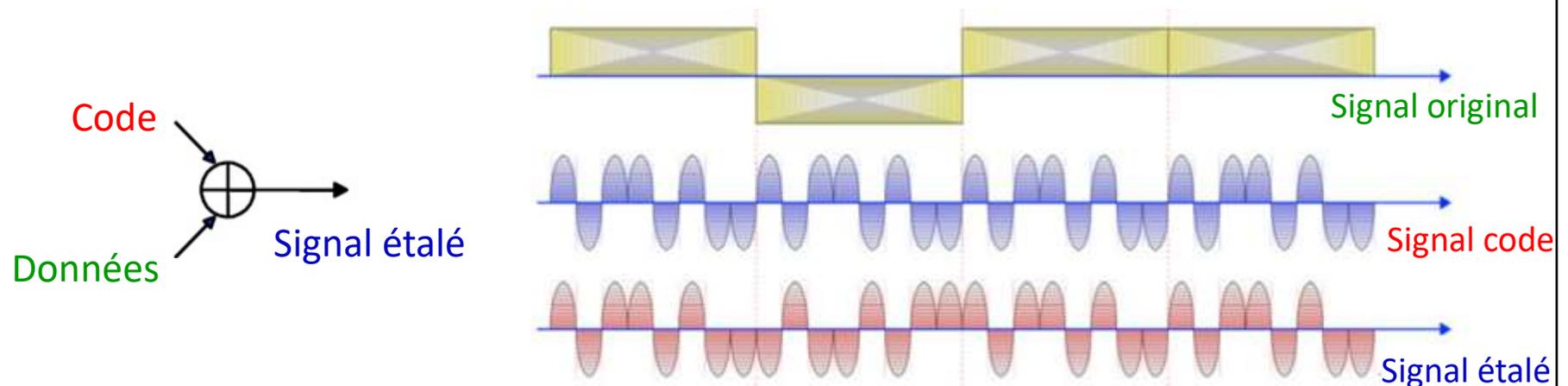
Canal	36	40	44	48	52	56	60	64
Fréquence (GHz)	5,18	5,20	5,22	5,24	5,26	5,28	5,30	5,32

Standard WIFI - IEEE 802.11

Couche physique

DSSS (Direct Sequence Spread Spectrum)

- L'étalement est effectué par la modulation du signal utile.
- Étalement le signal sur un même canal de 22 Mhz sans changement de fréquence.
- le signal utile est multiplié par un signal pseudo-aléatoire de bande large, appelé le **code d'étalement** ou la **séquence des chips**.
 - Code de Barker: séquence de "chips" à 11 bits



- Découper chaque bit de données en une série de combinaisons redondantes de bits, puis les transmet

Standard WIFI - IEEE 802.11

Couche physique

FHSS (Frequency Hopping Spread Spectrum)

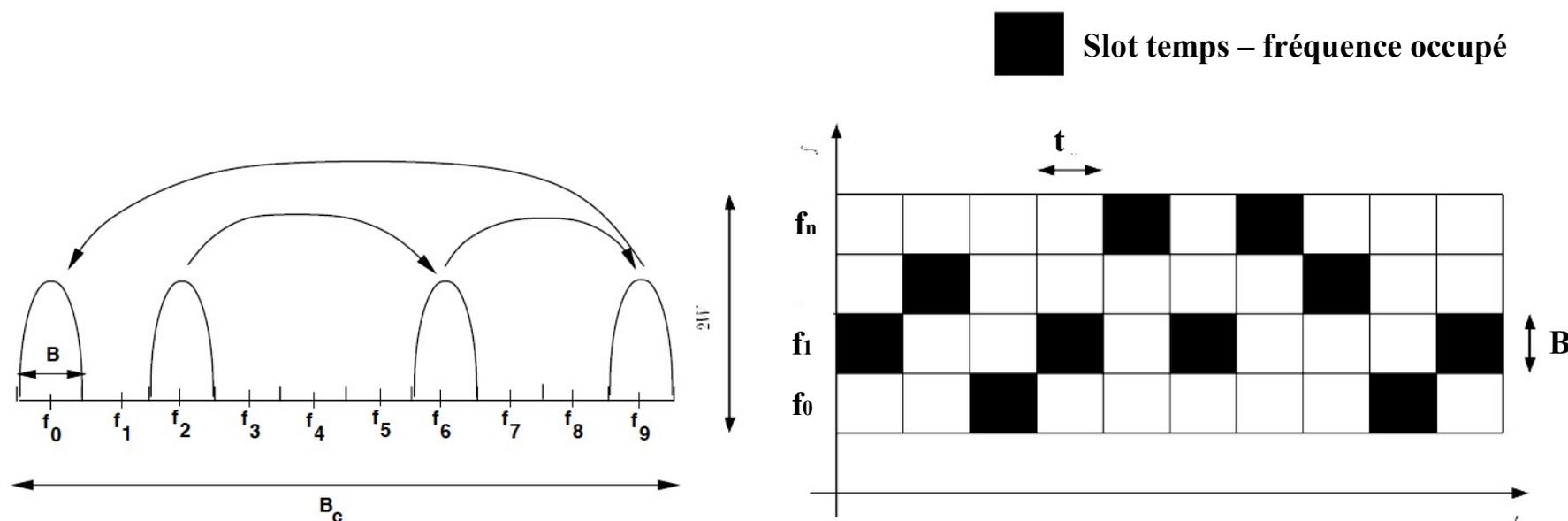
Idée: utiliser toutes les fréquences en sautant de l'une à l'autre dans un ordre pseudo aléatoire partagés entre 2 stations

- ◆ Utilisation d'une modulation à saut de fréquence, sur spectre étalé:
 - ✓ Divise le signal radio en 79 sous canaux de 1 MHz chacun (bande 2,4 GHz)
 - ✓ saute d'une fréquence à une autre chaque 300 ms.
 - ✓ Sauts selon une règle pseudo-aléatoire
 - ✓ L'émetteur et le récepteur sont d'accord sur l'ordre des sauts

Standard WIFI - IEEE 802.11

Couche physique

FHSS (Frequency Hopping Spread Spectrum)



- **Intérêts** : simple, résistance aux interférences, sécurité.
 - Faible interférence entre les différents couples émetteur - récepteurs.
 - car faible probabilité d'émission sur le même sous canal à un même instant.

Standard WIFI - IEEE 802.11

Couche physique

Caractéristiques des différentes variantes IEEE 802.11

- ◆ **IEEE 802.11b**
 - Bande ISM
 - Basé sur le DSSS
 - Débits compris entre 1 et 11 Mbits/s
 - Variation de débits selon l'environnement radio (murs, meubles, interférences, etc.)

- ◆ **IEEE 802.11a**
 - Bande UN-II (5GHz)
 - Largeur de la bande : 200 MHz
 - Basé sur OFDM
 - Débits compris entre 6 et 54 Mbits/s

- ◆ **IEEE 802.11g**
 - Bande ISM
 - Basé sur OFDM et DSSS
 - Débits compris entre 6 et 54 Mbits/s
 - Compatibilité ascendante avec 802.11b

N.B. La bande ISM est de plus en plus saturée (802.11b, 802.11g, Bluetooth, etc.)

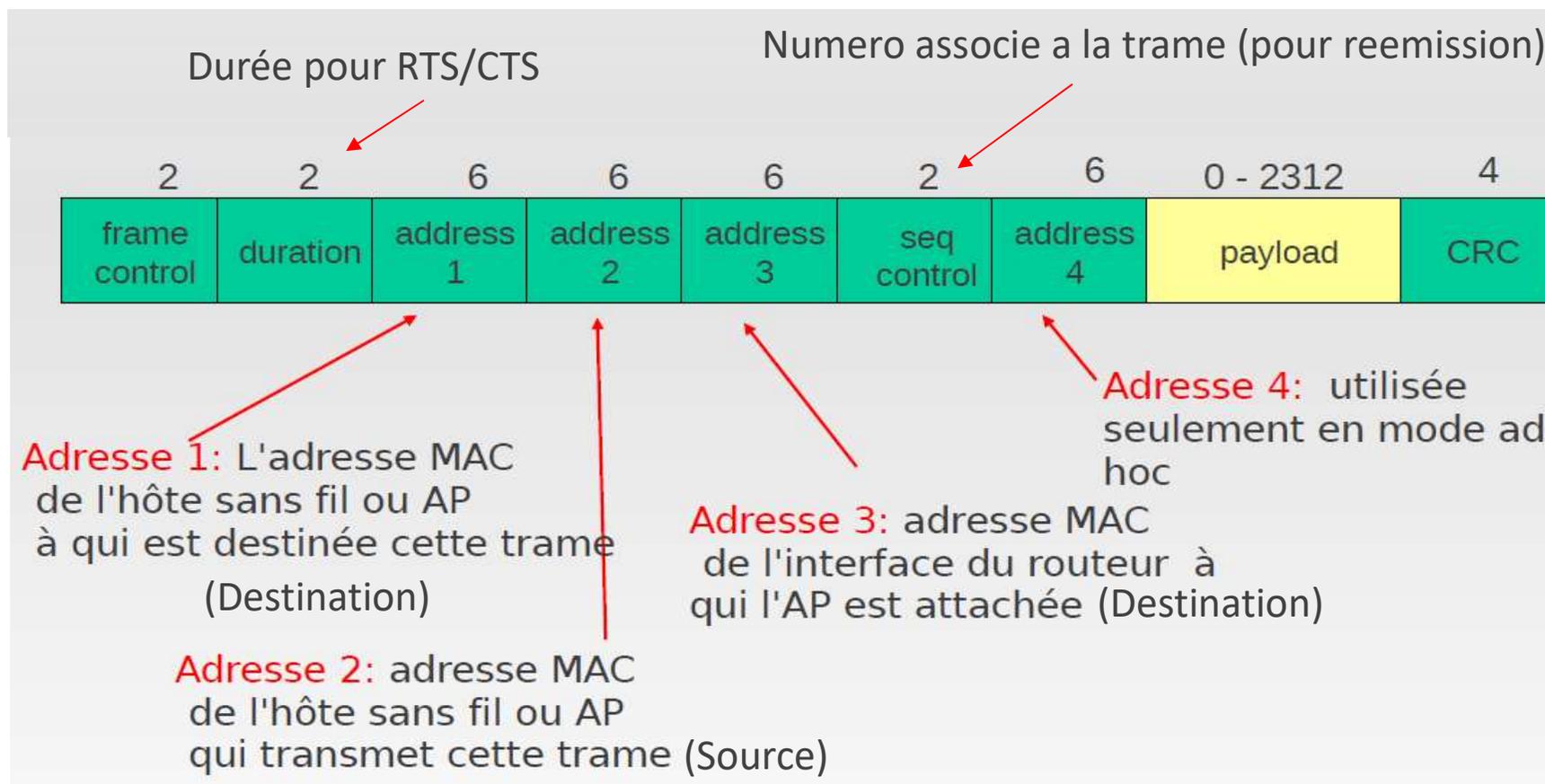
Standard WIFI - IEEE 802.11

Couche liaison

- La couche Liaison est divisée en deux sous couches: MAC et LLC
- La sous couche MAC définit deux méthodes d'accès différentes qui peuvent **cohabiter** :
 - ◆ **Le Distributed Coordination Function (DCF): - Obligatoire -**
 - ✓ accès aléatoire et égalitaire, mais non garanti.
 - ✓ utilise la méthode CSMA/CA (avec contention).
 - ✓ Pas d'entité de contrôle centralisé (possibilité de collisions).
 - ◆ **Le Point Coordination Function (PCF) : - facultative -**
 - ✓ accès assuré mais performance plus faible.
 - ✓ La transmission de données est centralisée (pas de collisions).
 - ✓ Le point d'accès donne l'accès à toutes les stations à tour de rôle.
 - L'AP diffuse une trame de signalisation Beacon frame contenant différents paramètres systèmes (ex. fréquences).
 - Les stations « s'enregistrent » auprès de l'AP et s'apparente à du « polling »
 - ✓ Conçue pour la transmission de données sensibles (Applications temps réel: voix, etc.)

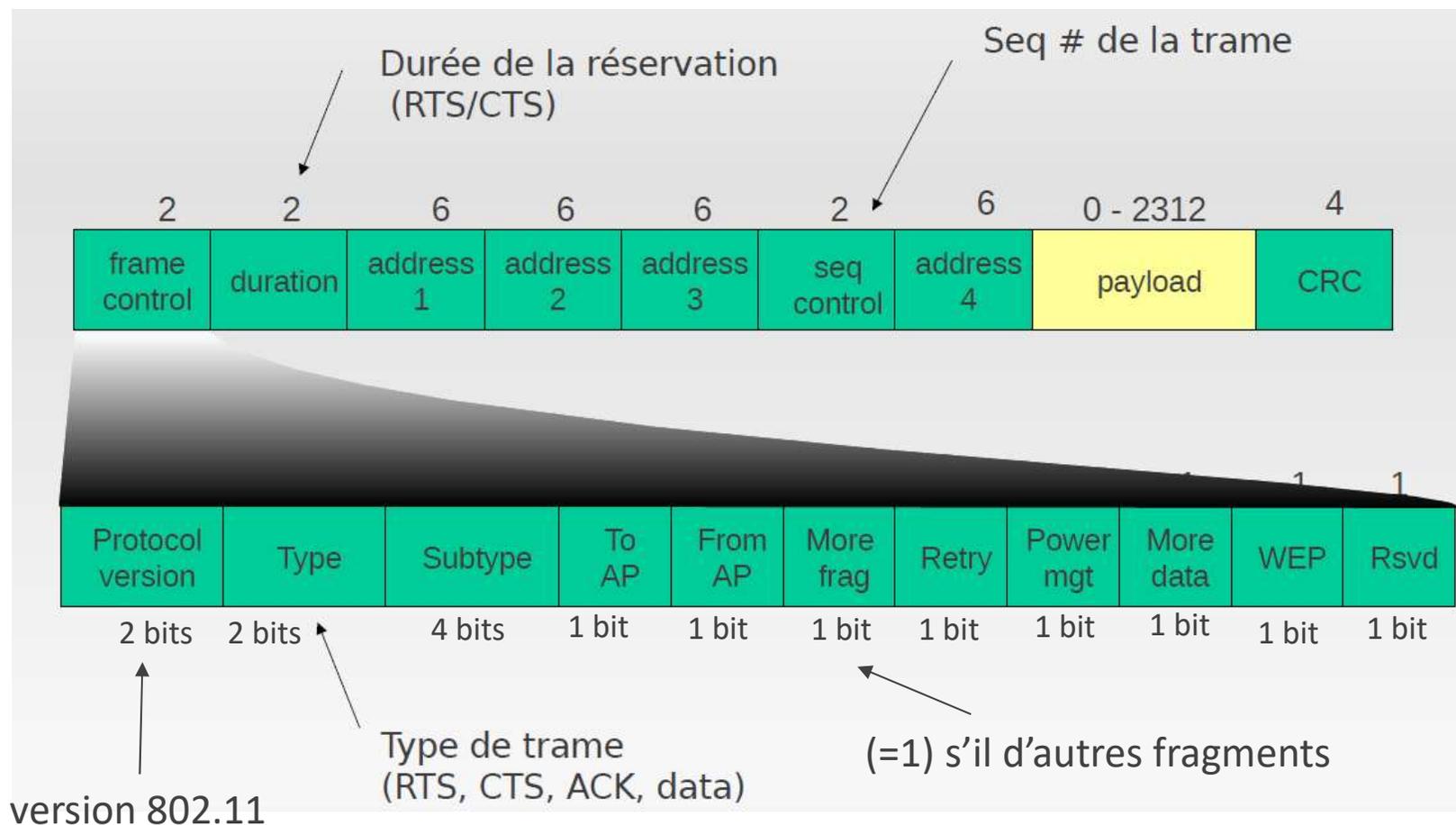
Standard WIFI - IEEE 802.11

Frame



Standard WIFI - IEEE 802.11

Trame



Standard WIFI - IEEE 802.11

Trame

Gestion

type	sous-type	Description du sous type
00	0000	Requête d'association
00	0001	Réponse d'association
00	0010	Requête de ré-association
00	0011	Réponse de ré-association
00	0100	Demande de sonde
00	0101	Réponse de sonde
00	0110-0111	Réservés
00	100	Balise (BEACON)

01	0000-1001	Réservés
01	1010	PS-Poll
01	1011	RTS
01	1100	CTS
01	1101	ACK
01	1110	CF End
01	1111	CF End et CF-ACK

Contrôle

10	0000	Données
10	0001	Données et CF-ACK
10	0010	Données et CF-Poll
10	0011	Données, CF-ACK et CF-Poll
10	0100	Fonction nulle (sans données)
10	0101	CF-ACK (sans données)
10	0110	CF-Poll (dans données)
10	0111	CF-ACK et CF-Poll (sans données)
10	1000-1111	Réservés

Données

Standard WIFI - IEEE 802.11

Trame

Trames de gestion

- ◆ Etablir et de maintenir des communications.
- ◆ Les principales trames de gestion 802.11 sont les suivantes :
 - Trame de “Beacon”
 - Envoyée périodiquement par un AP pour annoncer sa présence et relayer des paramètres (ex. SSID).
 - Les mobiles écoutent “continuellement” tous les canaux et entendent ces trames
 - Trame de requête de sonde
 - Envoyé par une station pour obtenir des informations d'une autre station.
 - Ex. déterminer quels sont les points d'accès à sa portée.
 - Trame de réponse de sonde
 - Répondre à une trame de demande de sonde
 - Contenir des informations de capacités, débits supportés, etc.

Standard WIFI - IEEE 802.11

Trame

Trames de gestion

○ Trame d'authentification

– Pour accepter ou rejeter l'identité d'un mobile par l'AP.

▪ système ouvert (par défaut)

- ✓ Le mobile envoie une trame d'authentification
- ✓ L'AP répond avec une trame d'authentification indiquant l'acceptation.

▪ facultative clé partagée

- ✓ le mobile envoie une première trame.
- ✓ L'AP répond en joignant son texte de défi.
- ✓ Le mobile renvoie une version chiffrée du texte de défi.
- ✓ Le point d'accès informe le mobile du résultat de l'authentification.

○ Trame de dés-authentification

– Envoyée par une station souhaitant terminer ses communications.

Standard WIFI - IEEE 802.11

Trame

Trames de gestion

- **Trames d'association**
 - Pour allouer des ressources (ex. espace mémoire) pour un mobile et de les synchroniser avec lui (identification d'association et débit supportés).
 - Envoyée par un mobile à un AP.
 - Contient les informations du mobile (ex. débits supportés) et le SSID du réseau avec qui il souhaite s'associer.
- **Trames de réassociation (requête et réponse)**
 - Pour se réassocier à un autre AP ayant un signal plus fort.
- **Trame de désassociation**
 - Pour demander à une autre station de terminer l'association.

Standard WIFI - IEEE 802.11

Frame

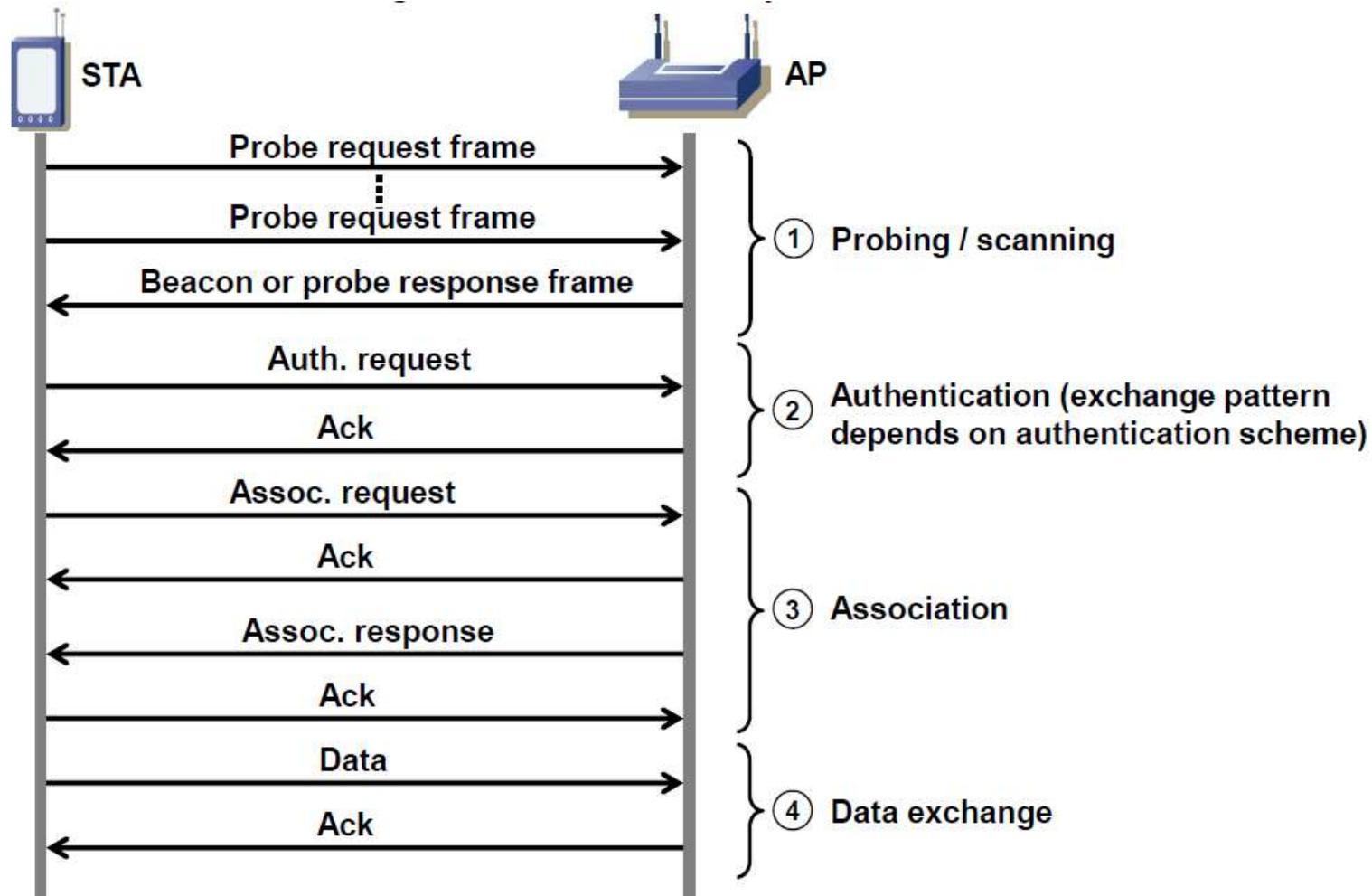
Trames de contrôle

- Exemple. RTS, CTS, ACK.
- utilisés pour aider à la livraison des trames de données entre les stations.
- utilisées dans le protocole CSMA/CA.



Standard WIFI - IEEE 802.11

Scénario d'échange dans WIFI

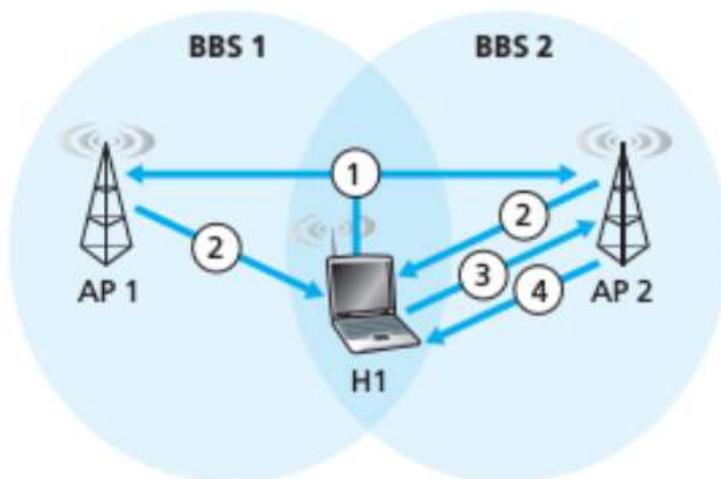


Standard WIFI - IEEE 802.11

Scénario d'échange dans WIFI

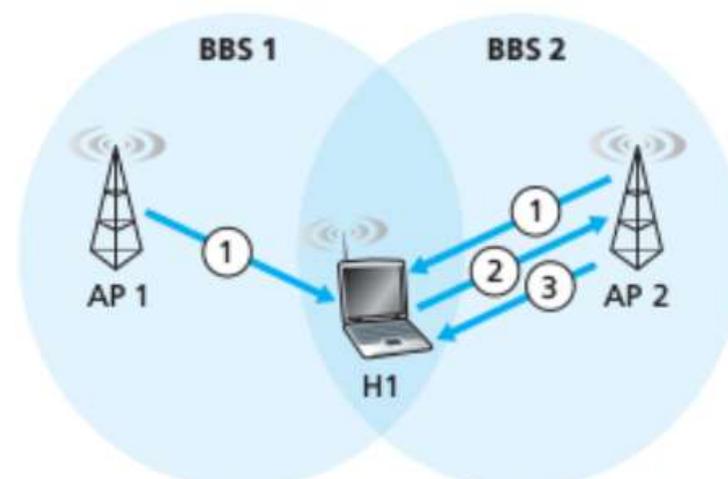
Etape 1. Probing / scanning

- ◆ La STA tente de trouver un point d'accès via:
 - ✓ Une Analyse active (Probe Request trame) (facultative).
 - ✓ Une Analyse passive (la STA attend les trames Beacon envoyées par AP à intervalles réguliers).
- ◆ L'utilisateur sélectionne ensuite le AP à associer en fonction du SSID (la Beacon contient le SSID).



Active scanning

1. Probe Request frame broadcast from H1
2. Probes Response frame sent from Aps
3. Association Request frame sent: H1 to selected AP
4. Association Reponse frame sent: Selected AP to H1



Passive scanning

1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
1. Association Response frame sent: Elected AP to H1

Standard WIFI - IEEE 802.11

Scénario d'échange dans WIFI

Etape 2. Authentification

- ◆ STA s'authentifie avec AP.
- ◆ Les schémas d'authentification possibles sont:
 - ✓ Open (no authentication).
 - ✓ Authentification avec clé (ex. PSK -Pre-Shared Key- with WEP).

Etape 3. Association

- ◆ STA entre dans le BSS contrôlé par le AP.
- ◆ STA informe AP des débits de données pris en charge.
- ◆ AP alloue des tampons et d'autres structures de données pour la communication avec le STA.

Etape 4. Send / receive data:

- ◆ STA commence à envoyer et recevoir des données (directement ou avec le mécanisme RTS / CTS).