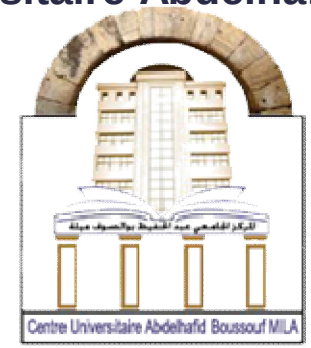
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre Universitaire-Abdelhafid Boussouf Mila



Réseaux et Informatique Mobiles

Chap 3: Réseaux locaux sans fil (WiFi - IEEE 802.11)

Master 1 STIC

Plan

I. Introduction

II. Architecture: modes de fonctionnement réseau sans fil

III. Modèle OSI 802.11 : couches physique & liaison

IV. Sécurité

Développé depuis 1990 (premier réseau WiFi est publié en 2001)

- **Relie des équipements sans fils (ordinateur, PDA, périphériques sans fils, etc.)**
- **Un rayon allant jusqu'à des centaines de mètres.**
- **Norme IEEE 802.11 :standard international décrivant les caractéristiques d'un WLAN**
- **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.

Plan

I. Introduction

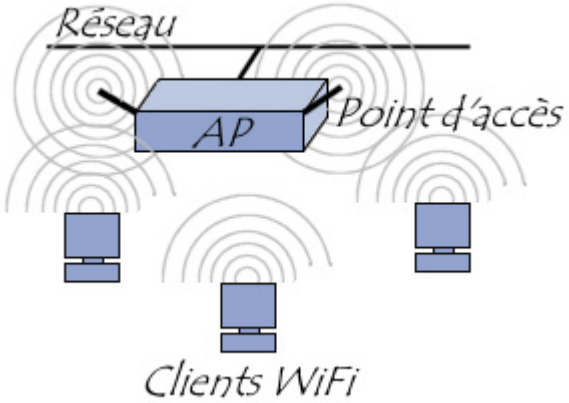
II. Architecture: modes de fonctionnement réseau sans fil

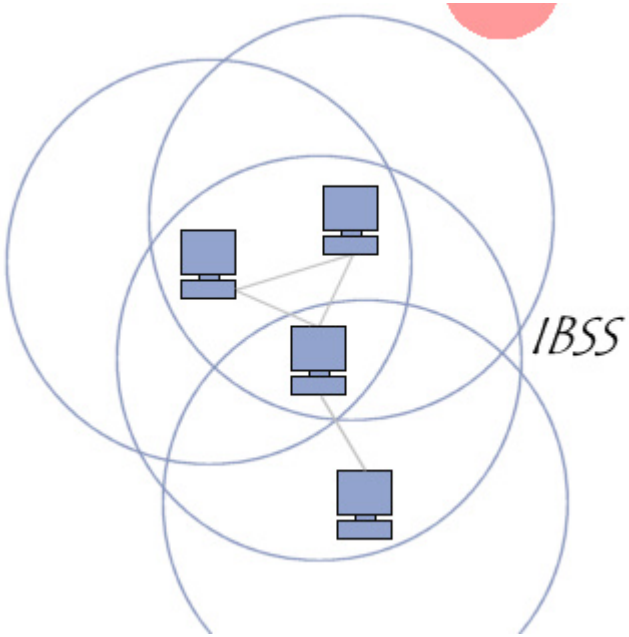
III. Modèle OSI 802.11 : couches physique & liaison

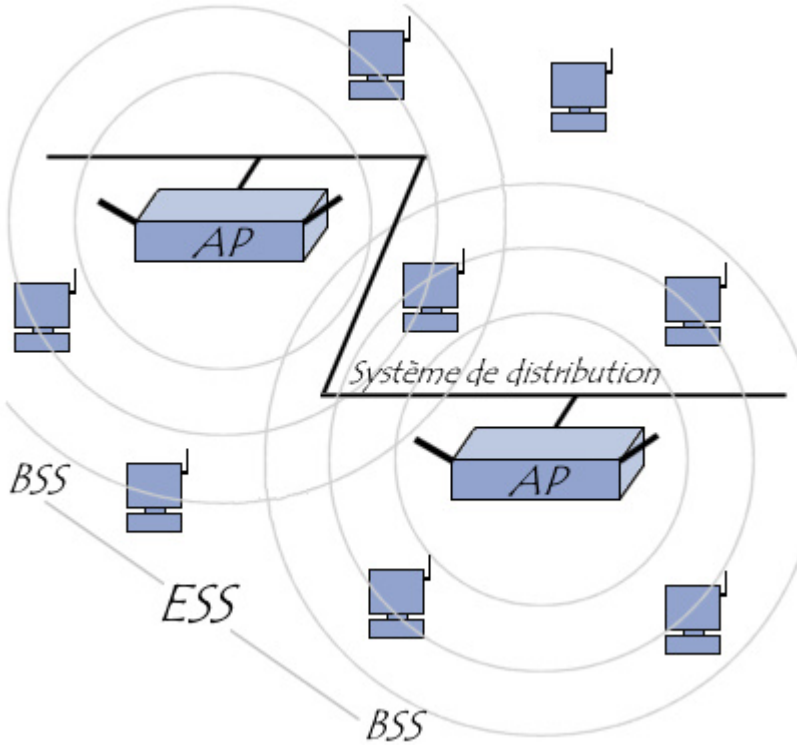
IV. Sécurité

- Le standard **802.11** définit deux modes :
  - ❑ **Avec infrastructure**
    1. ***BSS*** **(***basic service set*)
    2. ***ESS*** (*extended service set*)
  - ❑ **Sans infrastructure (Ad-hoc)**

    IBSS *(*independant basic service







Plan

I. Introduction

II. Architecture: modes de fonctionnement réseau sans fil

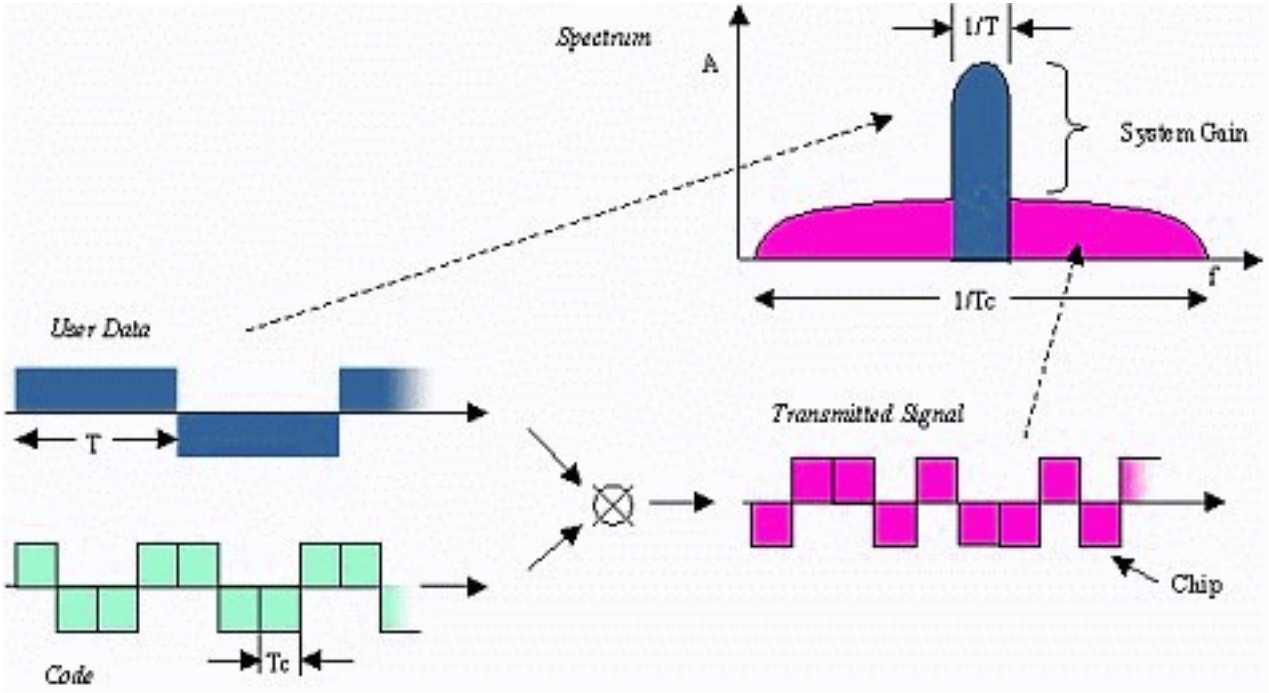
III. Modèle OSI 802.11 : Couches Physique & Liaison

IV. Sécurité

<table>
<tr><td rowspan="2">Couche liaison de données</td><td colspan="4">LLC 802.2</td></tr>
<tr><td colspan="4">MAC 802.11, sécurité, etc …</td></tr>
<tr><td>Couche physique</td><td>FHSS</td><td>DSSS</td><td>IR</td><td>OFDM</td></tr>
</table>

- **FHSS** : **étalement** de spectre par **saut de fréquence**
- **DSSS** : étalement de spectre en séquence directe
- IR : InfraRouge
- OFDM : Multiplexage en fréquences

- **Différentes bandes de fréquences (sans licence)**
  - **La bande (ISM) 2,4 GHz** : 802.11, 802.11b, 802.11g
  - **La bande (5U-NII) 5GHz:** 802.11a et 802.11n
- **DSSS** (Direct Sequence Spread Spectrum) étalement du spectre (***modulation***)



Idée: découper le spectre en « **canaux** » dont certains ne se **superposant** pas peuvent être utilisés simultanément.

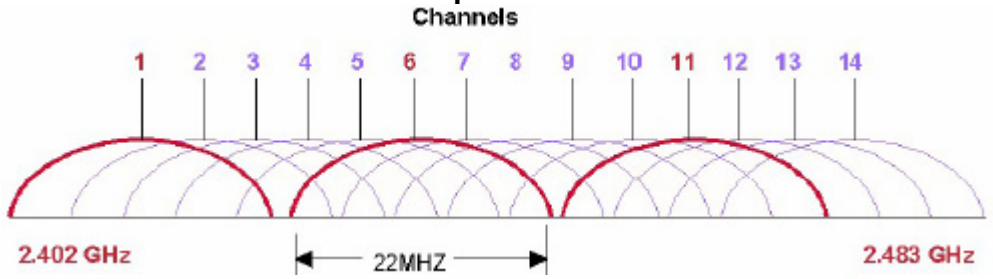
1-La fréquence 2,4 GHz - Bande ISM (*Industrial, Scientific and Medical)*

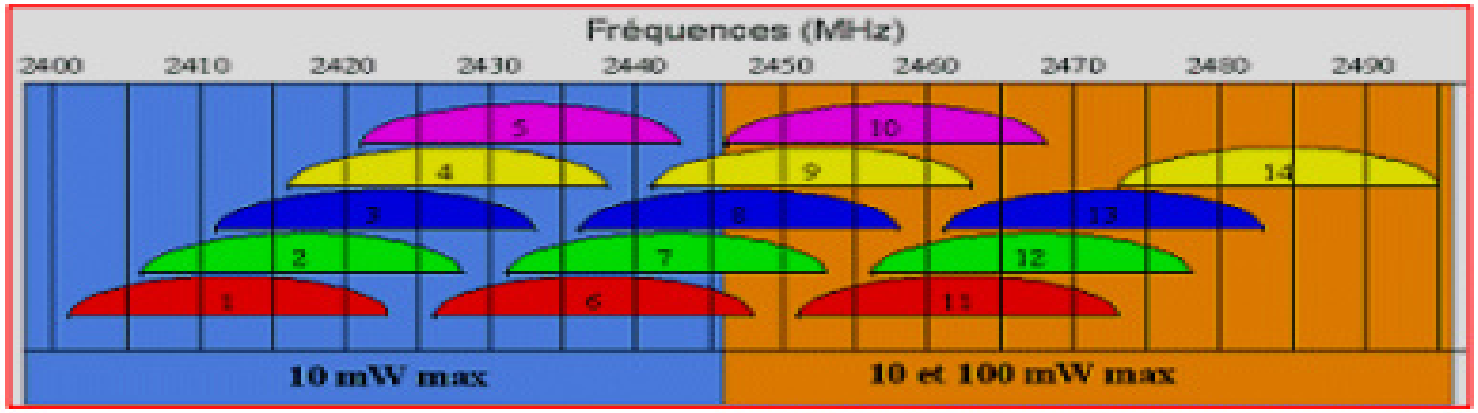
– Largeur de bande **83** MHZ (de 2,400 GHz à 2,483 GHz)

– Bande divisée en **14** canaux de 22 MHz

– Superposition de 3 réseaux au sein d'un même espace

– Problème de recouvrement





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

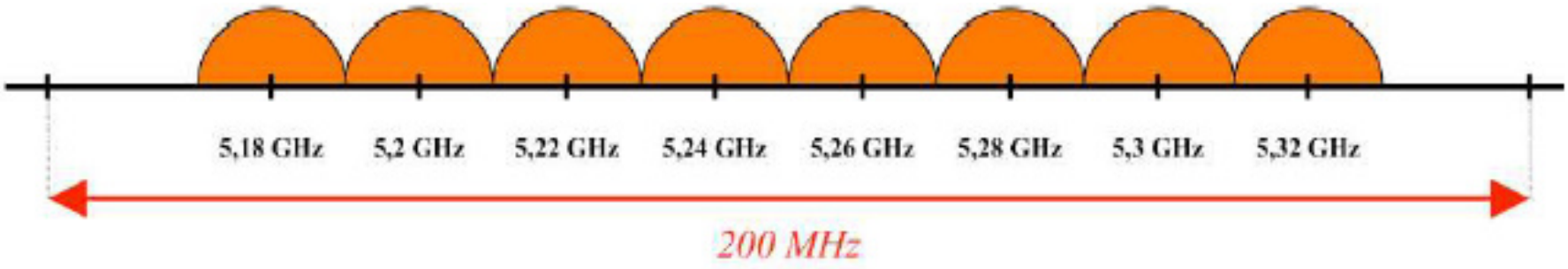
2-La fréquence 5 GHz - Bande UN-II

– 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

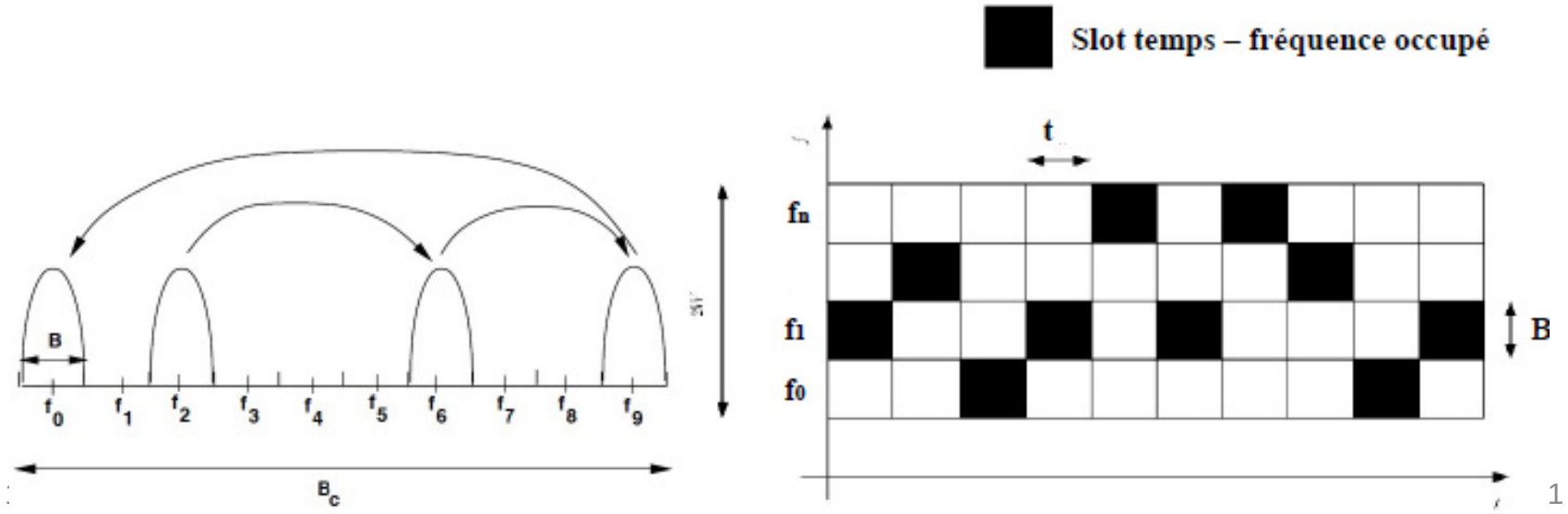


Canal	36	40	44	48	52	56	60	64
Fréquence (GHz)	5,18	5,20	5,22	5,24	5,26	5,28	5,30	5,32

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 ISM** 2,4 GHz)
  - saute d'une fréquence à une autre chaque **300** ms selon une règle pseudo-aléatoire
  - L'émetteur et le récepteur sont d'accord sur l'ordre des sauts
- Intérêts : simple, résistance aux interférences, sécurité.



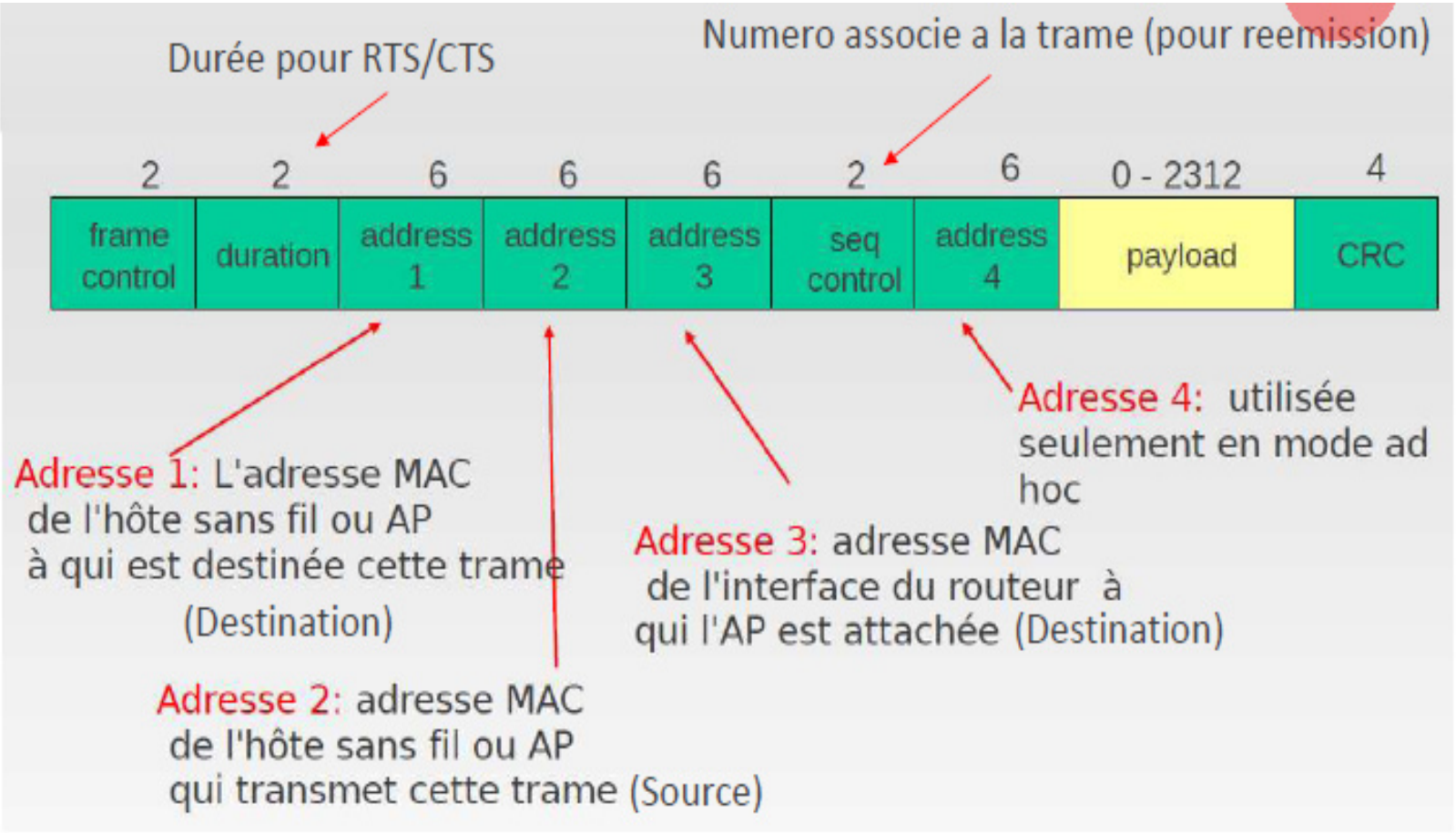
- La couche Liaison est divisée en deux sous couches: **MAC** et **LLC**

- La sous couche MAC définit deux **méthodes d'accès** différentes :

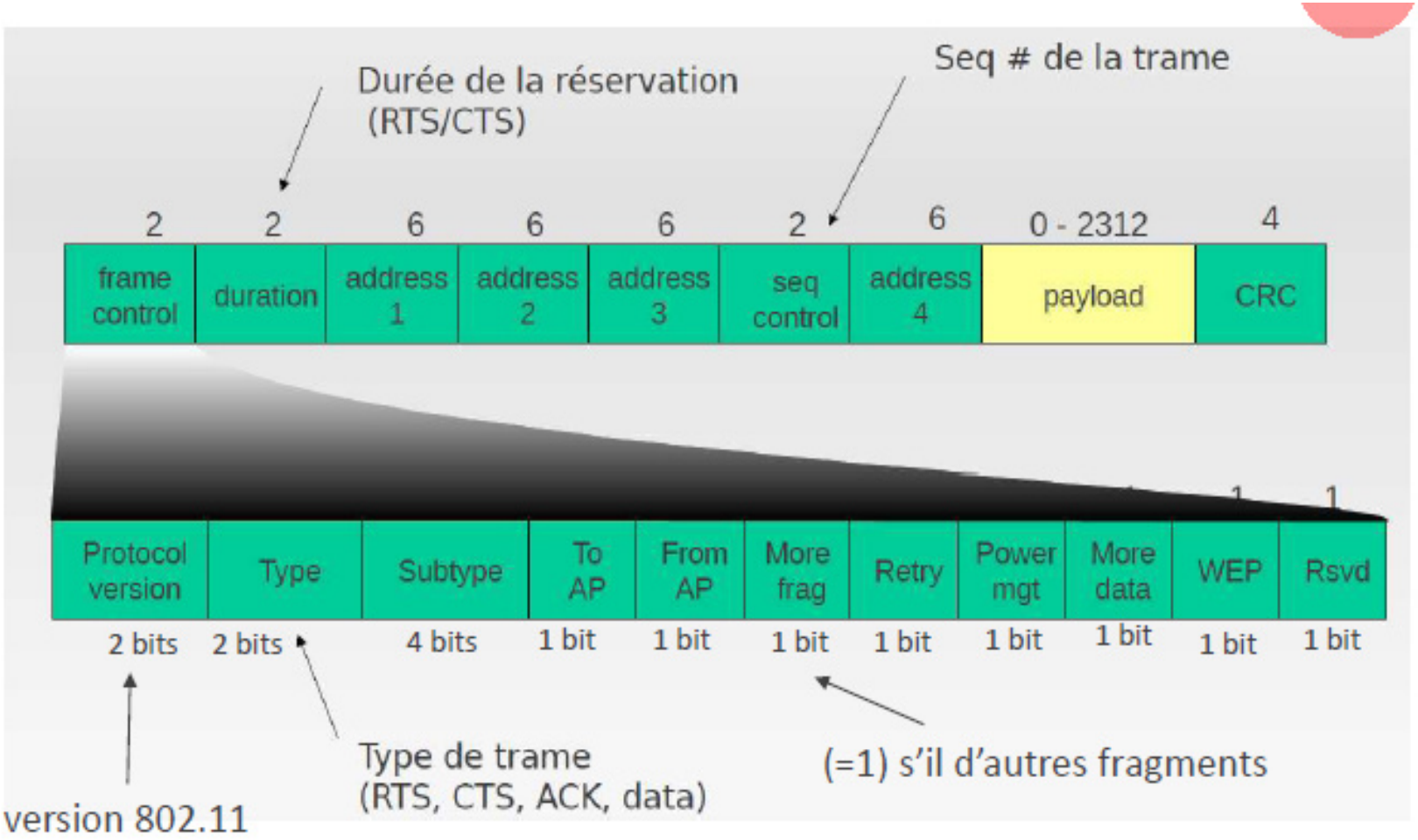
- **Le Distributed Coordination Function (DCF):**
  - Accès aléatoire et égalitaire, mais non garanti.
  - Utilise la méthode **CSMA/CA** (avec contention).
  - Pas d'entité de contrôle centralisé (possibilité de collisions).

- **Le Point Coordination Function (PCF) :**
  - 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: « polling »
  - Conçue pour la transmission de données sensibles (Applications temps réel: voix, etc.)

TRAME


Durée pour RTS/CTS
Numero associe a la trame (pour reemission)
2
2
6
6
6
2
6
0 - 2312
4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
Adresse 1: L'adresse MAC de l'hôte sans fil ou AP à qui est destinée cette trame (Destination)
Adresse 2: adresse MAC de l'hôte sans fil ou AP qui transmet cette trame (Source)
Adresse 3: adresse MAC de l'interface du routeur à qui l'AP est attachée (Destination)
Adresse 4: utilisée seulement en mode ad hoc

TRAME


Durée de la réservation
(RTS/CTS)
Seq # de la trame
2 2 6 6 6 2 6 0 - 2312 4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
1 1
Protocol version
Type
Subtype
To AP
From AP
More frag
Retry
Power mgt
More data
WEP
Rsvd
2 bits 2 bits 4 bits 1 bit 1 bit 1 bit 1 bit 1 bit 1 bit 1 bit 1 bit
version 802.11
Type de trame
(RTS, CTS, ACK, data)
(=1) s'il d'autres fragments

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)

Contrôle

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

Données

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

24

Trames de gestion

- Etablir et de maintenir des communications.
- Les principales trames de gestion 802.11 sont les suivantes :

1 -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

2-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.

3-Trame de réponse de sonde

– Répondre à une trame de demande de sonde

– Contenir des informations de capacités, débits supportés, etc.

4- Trame de dés-authentification

– Envoyée par une station souhaitant terminer ses communications.

5- 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 réponds 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.

6-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.

7-Trames de réassociation (requête et réponse)

– Pour se réassocier à un autre AP ayant un signal plus fort.

8-Trame de désassociation

– Pour demander à une autre station de terminer l'association.

Trame de Contrôle:

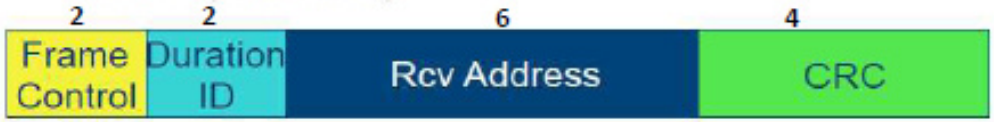
• Exemple**. RTS, CTS, ACK.**

• Utilisés pour aider à la livraison des trames de données entre les stations.

• Utilisées dans le protocole **CSMA/CA**.

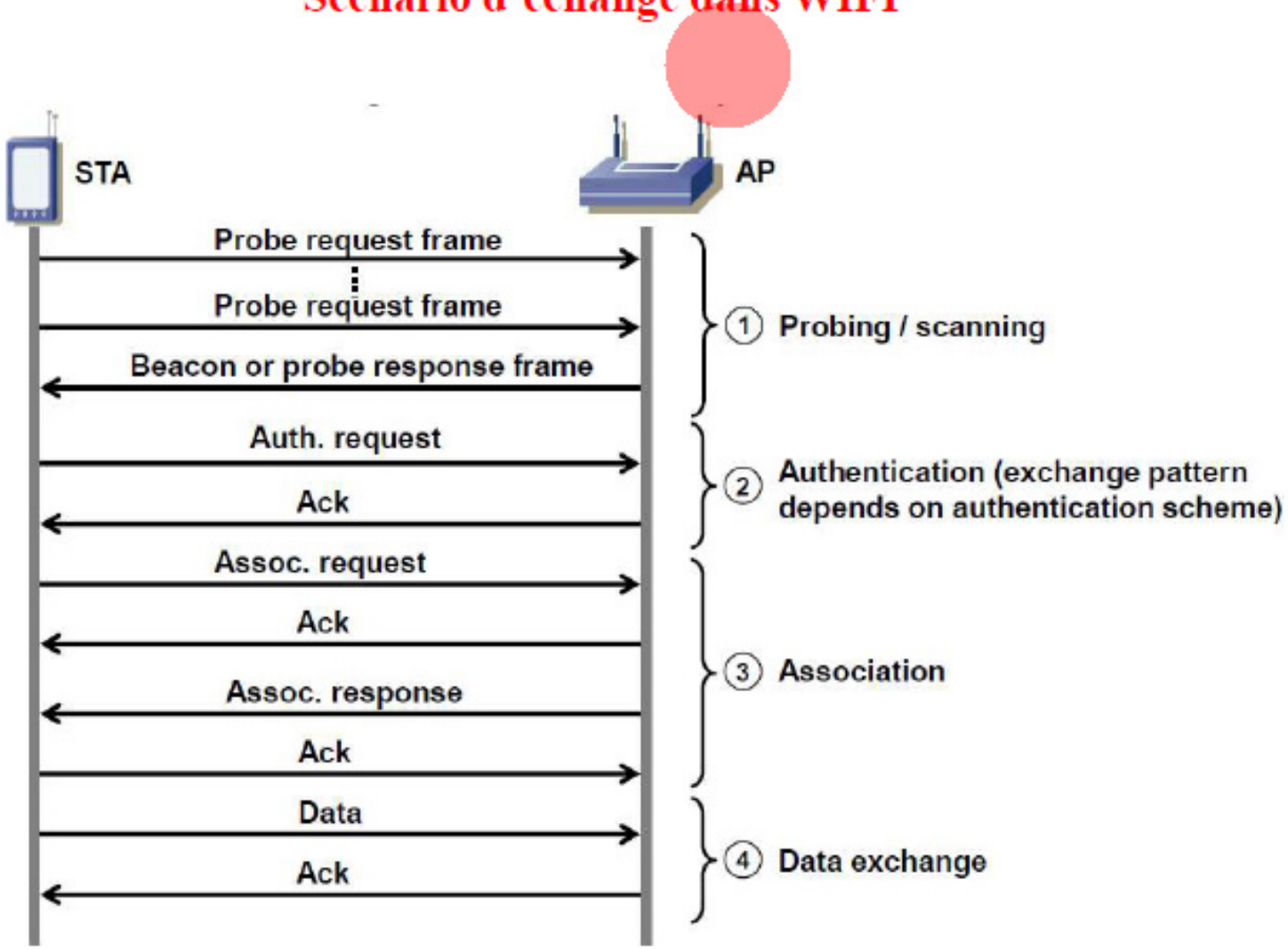
– RTS (160 bits)

– CTS (112 bits)



– ACK (112 bits)

Scénario d'échange dans WIFI



Plan

I. Introduction

II. Architecture: modes de fonctionnement réseau sans fil

III. Modèle OSI 802.11 : couches physique & liaison

IV. Sécurité

Sécurité

Le **problème de sécurité du sans fil** : le support de transmission est l'air
→Des "prises" du réseau sont à disposition pour toute personne à l'intérieur voire à l'extérieur du site (zone couverte par le réseau sans fil).

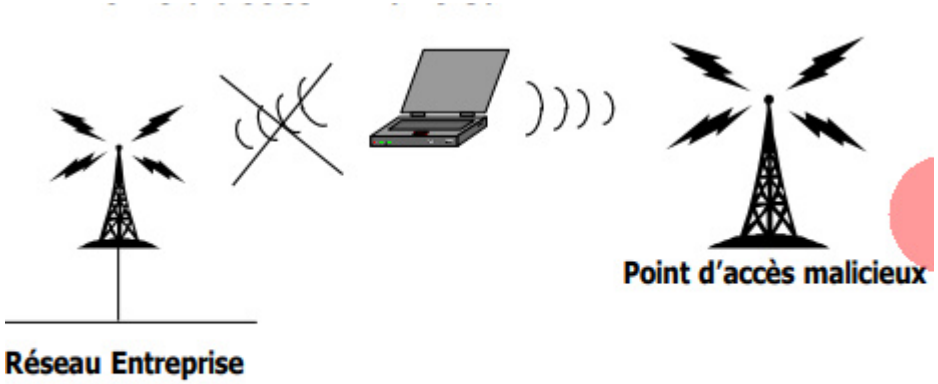
• Quatre types d'attaques :

– **Interception de données**, écoute clandestine

– **Le brouillage radio** : Création de système radio générant du bruit dans la bande des 2,4GHz. (système utilisant la même bande de fréquence : téléphone …)

– **Les dénis de services**: (deny of service)
  – Génération de trafic à travers le point d'accès vers un serveur.
  – Installation d'un point d'accès «malicieux» pour détourner le trafic.

– **Intrusion réseau**



Il suffit de connaître le SSID du réseau et le client s'associe au point d'accès «malicieux»

Sécurité

Conseilles pour sécurisé un réseau wifi:

– **Une infrastructure adaptée** : positionnement des points d’accès

– **Eviter les valeurs par défaut** (le mot de passe de l'administrateur, le nom SISD)

– **Le filtrage des adresses MAC**

– **WEP - Wired Equivalent Privacy** (protocol chiffrement de données)

– **Améliorer l'authentification:** gestion des comptes utilisateurs et les droits d'accès par RADUIS, AAA..

– **Mise en place d'un VPN**

Conclusion

- La norme *IEEE 802.11* (*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*).