

Cours Réseau et IoT

Réseaux sans fil WIFI – Standard 802.11



Département Informatique et Technologies du Numérique ITN
Master 1 Informatique
Parcours : Informatique & Big Data

Y. Y. Touati
capaok@gmail.com

Objectifs du cours

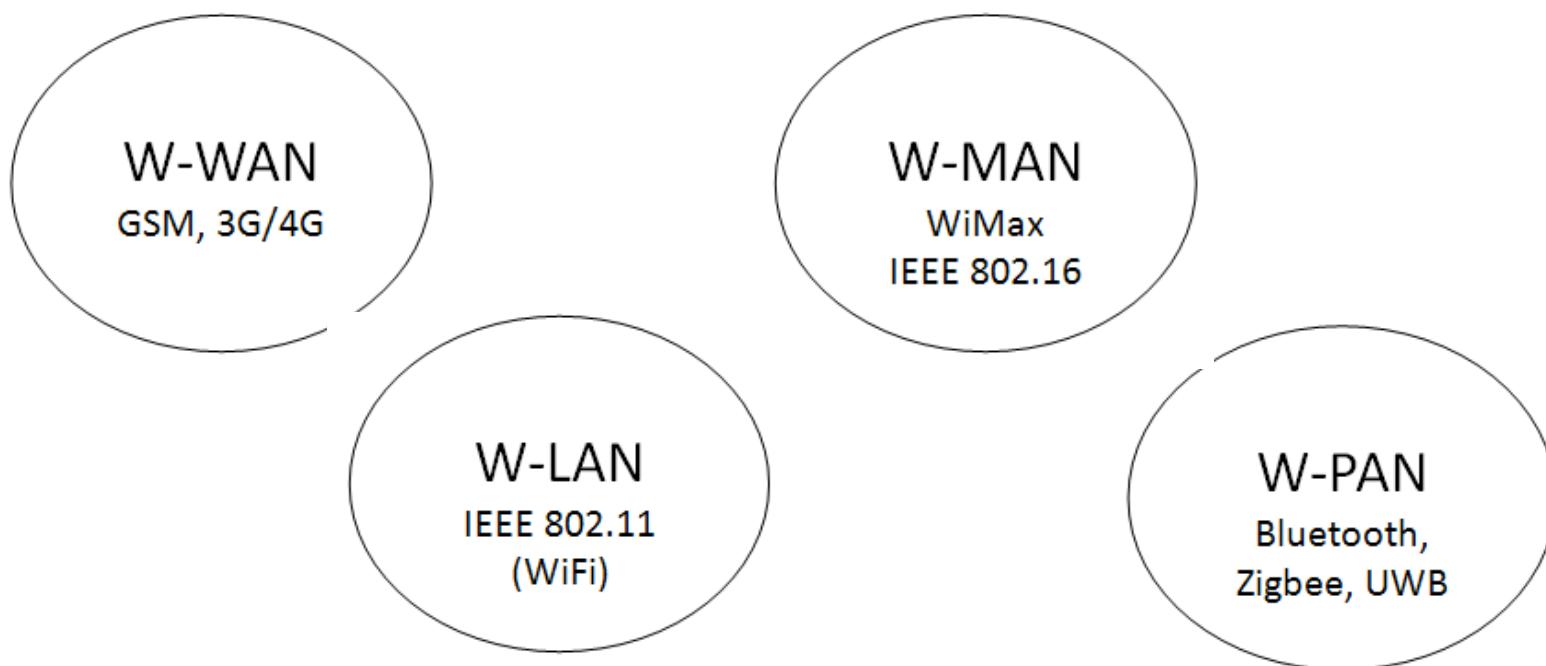
- Assimiler la notion des réseaux sans-fil et mobiles
- Illustrer via des exemples de technologies actuelles :
 - Notions d'architectures (station de base, cellule...)
 - Mécanismes d'échanges d'informations et de HANDOVER
 - Contraintes de sécurisation...
- Etudier le standard 802.11 (WiFi)
- Comprendre les réseaux de capteurs sans fil RCSF et leurs mises en œuvre dans les différentes applications (surveillance des forêts et des frontières, suivi médicalisé, Brain Computer Interfaces,)
- Mise en œuvre pratique

Réseaux sans fil

- Définitions
 - Réseau de machines interconnectées avec des liaisons non câblés (optimisation du câblage)
 - Applications nomades (accès à internet via des systèmes embarqués mobiles)
- Classification en fonction des usages et caractéristiques
 - Vitesse et débit de transmission
 - Coût de l'infrastructure et des équipements connectés
 - Sécurité, souplesse d'installation et d'usage
 - Consommation électrique et autonomie....

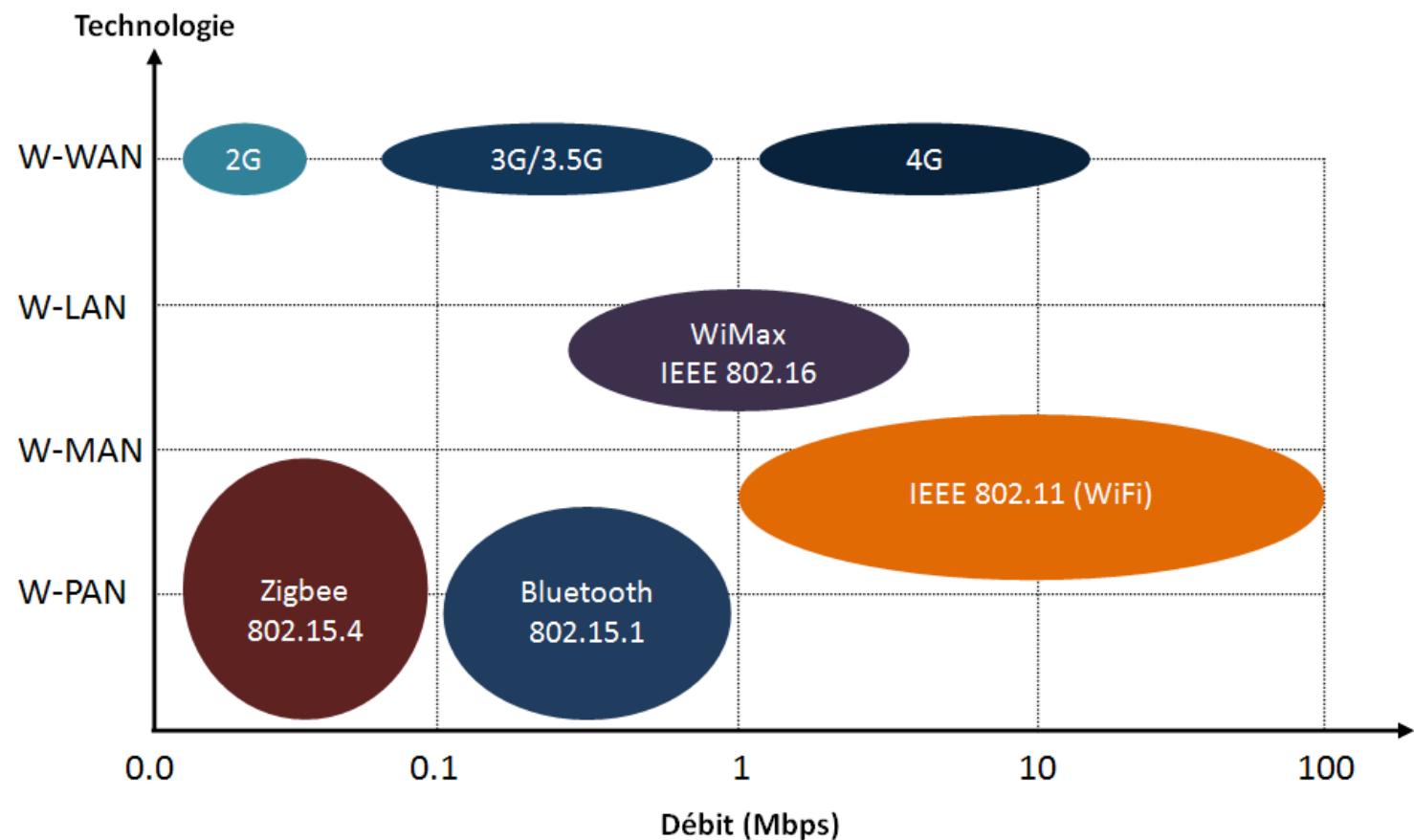
Technologies sans fil

- Plusieurs classes.
- Supports : radio, infrarouge, optique.
- Zone de couverture et portée des communications.



Classification des technologies sans fil

- En fonction du débit



Classification des technologies sans fil

Cat.	Portée max	Débit	Usages	Normes
WPAN	Qqs m	1 Mbit/s	Réseau particulier	IEEE 802.15 (Bluetooth), NFC, ETSI HyperPan
WLAN	500 m	+ de 50 Mbit/s	Réseaux internes, propres à un bâtiment (soit comme réseau d'entreprise, soit comme réseau domestique).	IEEE 802.11 (a,b,c,...) ETSI HyperLan
WMAN	4 à 10 kilomètres	de 1 à 10 Mbit/s	Ville, Campus, ... Interconnecte plusieurs WLAN	IEEE 802.16 WiMax ETSI HyperMan
WWAN	Plusieurs centaines de kms	de 1 à 10 Mbit/s	Régional, National Interconnecte plusieurs villes	Basé sur des technologies cellulaires

Organisme de réglementation

- FCC Federal Communication Commission (USA)
- ETSI European Telecommunications Standards Institute (Europe)
- ART Autorité de Régulation des Télécommunications (France)
- MKK (Japon)

HiperLan 1 : Débit 10-20 Mbit/s
HiperLan 2 : Débit de 54 Mbit/s

IEEE (USA) (Institut of Electrical and Electronics Engineers) : Standard
IEEE 802.11 et ses extensions (802.11b, 802.11a...)
(Utilisation aussi de la bande ISM et U-NII)

U-NII - Unlicensed National Information Infrastructure

Wireless LAN (WLAN)

Et le standard 802.11 dans tout cela!

Impact important dans la vie
quotidienne

Wireless LAN (WLAN)

- Définition
 - Réseau de machines interconnectées avec des liaisons sans fil offrant des fonctionnalités similaires que les réseaux LAN traditionnels (Ethernet)
- Pratiquement ?
 - Interconnexion de plusieurs machines et périphériques via une liaison haut débit de 11Mbit/s à plus de 540Mbit/s sur un rayon de plusieurs dizaines de mètres en intérieur à quelques centaines de mètres en extérieur



En fonction du standard

Publication du standard 802.11

- Année 90 : lancement du projet de création d'un WLAN (Wireless Local Area Network)

Objectif :

Offrir une connectivité sans fil à des stations fixes ou mobiles qui demandent un déploiement rapide au sein d'une zone locale en utilisant différentes bandes de fréquences

- Année 2000 : Publication du premier standard international pour les WLAN (IEEE 802.11)
 - Nombreuses normes : 802.11a, 802.11b, 802.11g, 802.11i ...
 - Amélioration par exemple du débit et/ou la sécurité

Label WiFi

- **Wireless Fidelity** : Label commercial décerné par un groupe de constructeurs WECA en 1999
 - Redevenue Wi-Fi Alliance depuis 2003



- Objectif :

Garantir l'interopérabilité inter-systèmes

Normes WiFi

Normes	Débit max	Fréquence	Date	Description
802.11	1 à 2 Mb/s	2,4 Ghz	1997	Première norme WiFi
802.11a	54 Mb/s	5 GHz	1999	<ul style="list-style-type: none"> - haut-débit sur 8 canaux - de 50Mbps jusqu'à 10m à 6Mbps jusqu'à 70m
802.11b	11 Mb/s	2,4 GHz	1999	<ul style="list-style-type: none"> - fixe un débit moyen maximum à 11 Mb/s théorique - portée de 50m en intérieur à 300 mètres en extérieur - spécifie 3 canaux radio (1, 6 et 11)
802.11g	54 Mb/s	2,4 GHz	2001	<ul style="list-style-type: none"> - fixe un débit moyen maximum à 54 Mbits/s théorique une - portée de 25m en intérieur à 75 mètres en extérieur - spécifie 3 canaux radio (1, 6 et 11)
802.11i			2004	- améliore la sécurité (authentification, cryptage et distribution des clés) en s'appuyant sur la norme Advanced Encryption Standard.
802.11n	270 Mb/s	2,4 GHz ou 5 GHz	2009	<ul style="list-style-type: none"> - regroupement des canaux - agrégation des paquets de données
802.11s	1 G/s	5 GHz	2012	<ul style="list-style-type: none"> - en cours de normalisation - améliore 802.11n

Paramètres de mise en œuvre

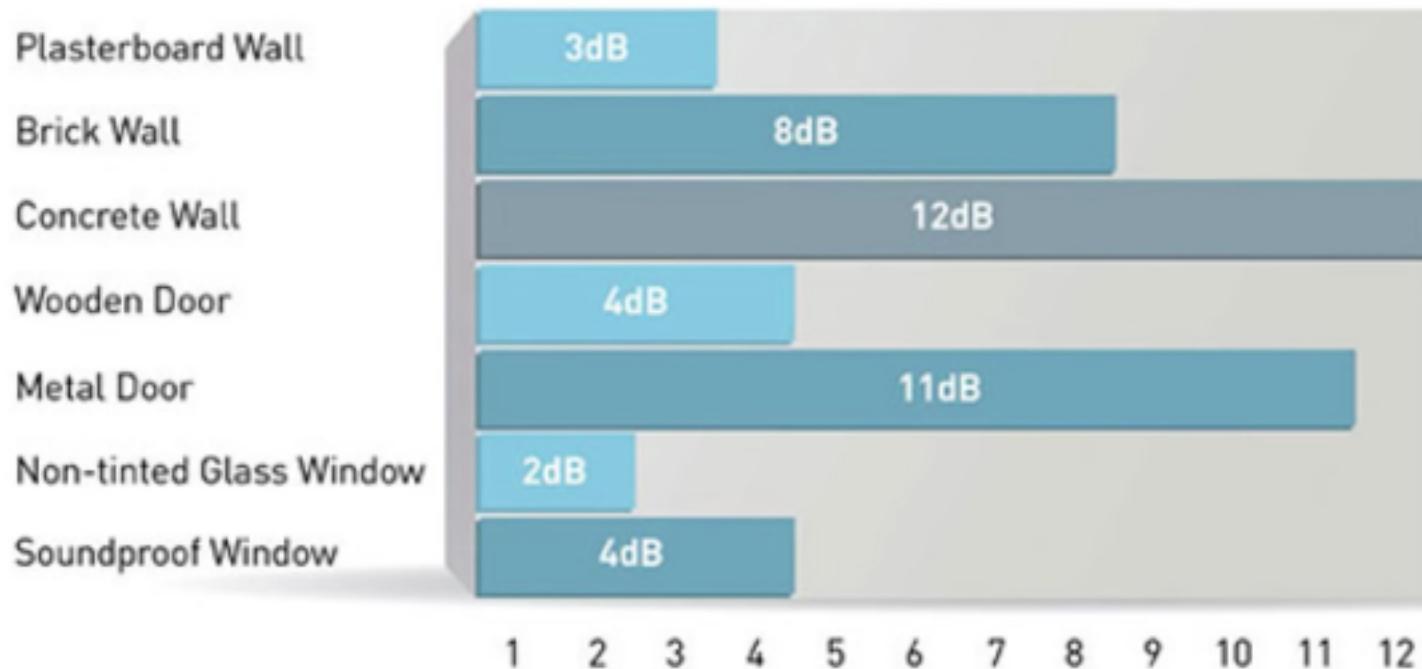
Débit et distance

- Technologie dépendante de l'environnement
 - Type de construction (cloisons, murs, matériaux)
 - Implantation des antennes
 - Interférences (Bluetooth, micro-ondes, autres réseau wifi)

Norme	débit théorique	portée en usage intérieur	
802.11a	54 Mbit/s	25 mètres	Accès au haut débit mais à courte portée.
802.11b	11 Mbit/s	35 mètres	Norme assez courante, utile pour le surf sur Internet. A éviter pour le streaming de vidéos ou le jeu en ligne.
802.11g	54 Mbit/s	25 mètres	Norme la plus répandue. Permet de jouer et de regarder des vidéos sur le Net avec un certain confort. Le transfert de fichiers volumineux reste long.
802.11n	540 Mbit/s	50 mètres	La norme à venir. Le très haut débit sans fil.

Source: Benchmark group

Environnement vs. Signal WiFi



Nouvelles normes WiFi

	802.11ac	802.11ax
BANDS	5 GHz	2.4 GHz and 5 GHz
CHANNEL BANDWIDTH	20 MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz	20 MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz
FFT SIZES	64, 128, 256, 512	256, 512, 1024, 2048
SUBCARRIER SPACING	312.5 kHz	78.125 kHz
OFDM SYMBOL DURATION	3.2 us + 0.8/0.4 us CP	12.8 us + 0.8/1.6/3.2 us CP
HIGHEST MODULATION	256-QAM	1024-QAM
DATA RATES	433 Mbps (80 MHz, 1 SS) 6933 Mbps (160 MHz, 8 SS)	600.4 Mbps (80 MHz, 1 SS) 9607.8 Mbps (160 MHz, 8 SS)

Densité de la couverture WiFi



Supports matériels

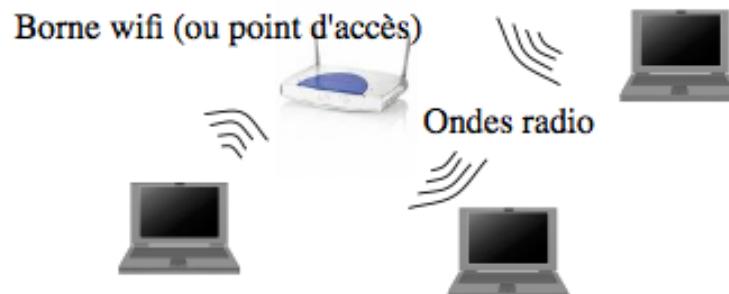
- **Carte WiFi et adaptateurs :**

Fonctionnant en mode client (dialogue avec une borne WiFi) ou point à point (dialogue avec une carte WiFi)



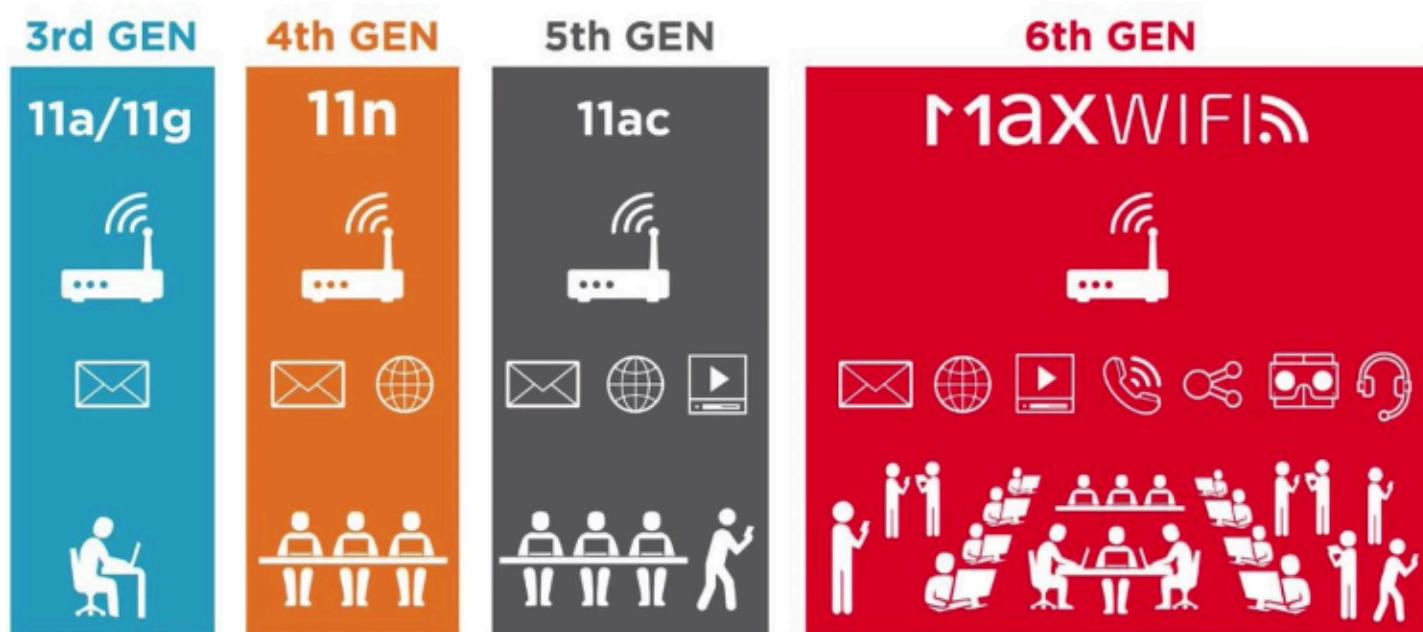
- **Point d'accès (Borne WiFi) :**

Similaire à un SWITCH où tous les paquets transitent (Pont vers d'autres types de réseaux)



Ordinateur possédant une carte WiFi

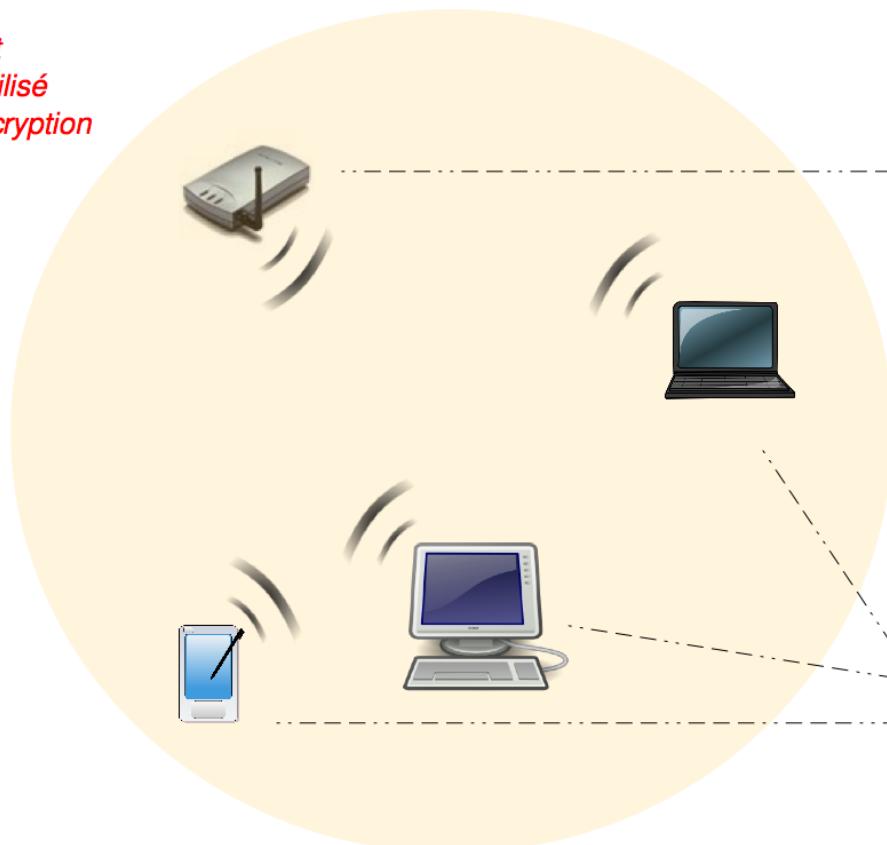
Evolution du réseau WiFi



Architecture cellulaire

Cellule (zone de couverture)

- ID
- Débit
- Canal utilisé
- Mode d'encryption



Point d'accès
module WiFi
&
module Ethernet

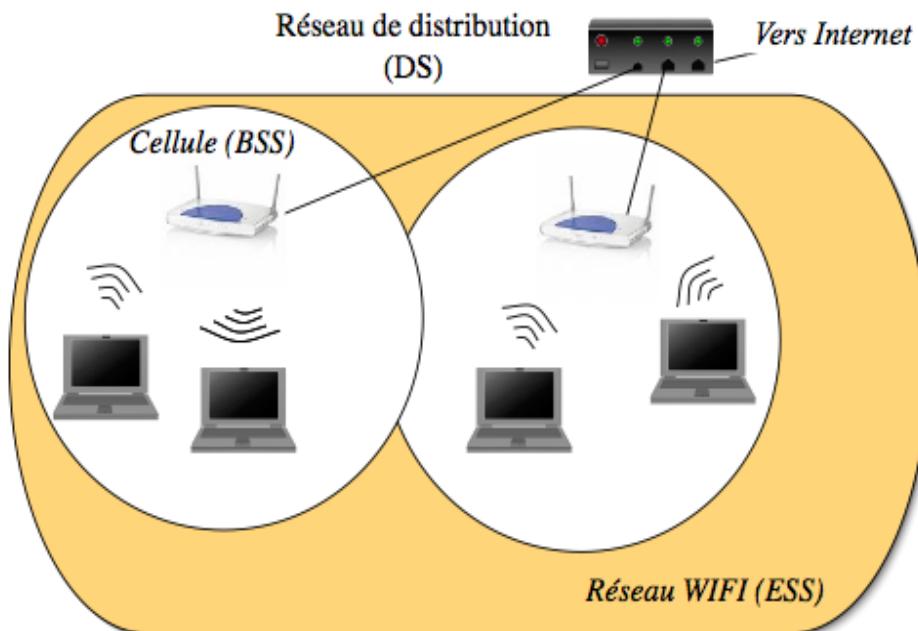
Un équipement
Wi-Fi
= 2 interfaces

Adaptateur WiFi
module WiFi
&
module PCI, PCMCIA,
CompactFlash ou USB

Topologies WiFi

- Mode infrastructure
 - Utilisation de PA comme SWITCH pour interconnecter les cellules
 - Généralement une antenne omnidirectionnelle
- Mode Ad Hoc ou Point-à-Point
 - Sans PA (configuration particulière de la carte WIFI)
 - Possibilité d'antennes directionnelles

Mode infrastructure (1/3)



BSS (Basic Service Set)

Ensemble de stations mobiles qui communiquent avec un PA. Chaque BSS dispose d'un identifiant **BSSID** correspondant à l'@ MAC du PA.

ESS (Extended Service Set)

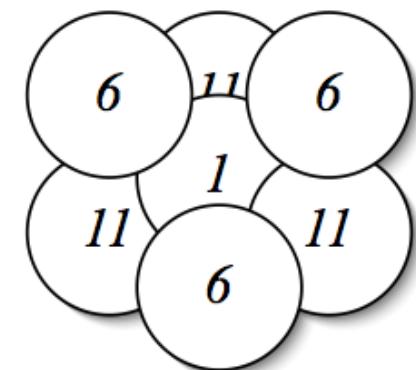
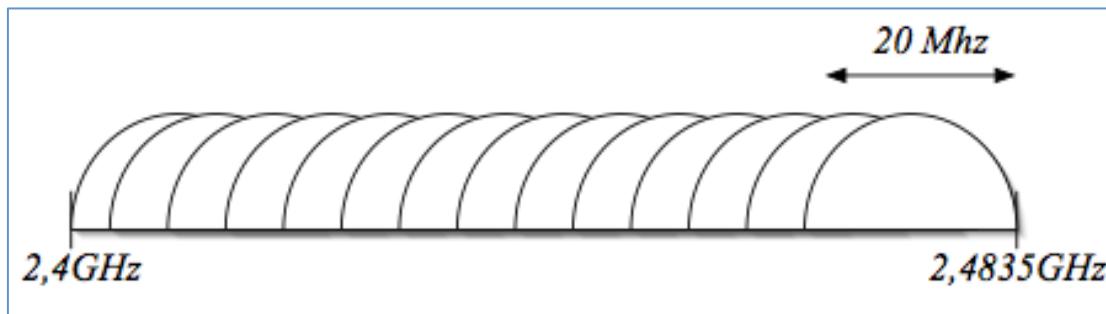
Interconnexion de plusieurs BSS entre eux et identifié par un nom **ESSID** sur 32 caractères ASCII (nom du réseau apparaissant dans la liste des réseaux wifi disponibles souvent abrégé en **SSID**).

DS (Distribution System)

Réseau de connexion des PA peut être filaire comme Ethernet ou Sans fil comme le WDS (Wireless DS).

Mode infrastructure (2/3)

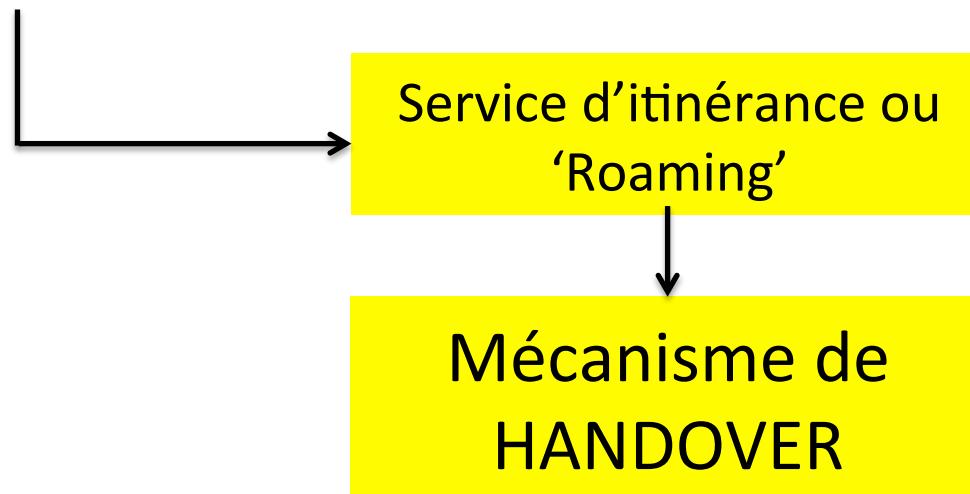
- Recouvrement des cellules utilisant des plages de fréquence différentes
- 802.11b : 14 canaux de 20Mhz entre 2.4 et 2.4835 (13 utilisés en Europe)
- Affectation de 3 canaux non recouvrant 1,6 et 11, avec au moins 5 canaux de différence pour éviter les interférences



- Choix du canal s'effectue en fonction des réseaux existants

Mode infrastructure (3/3)

- SI recouvrement : Possibilité de changer de cellule sans perte de connexion



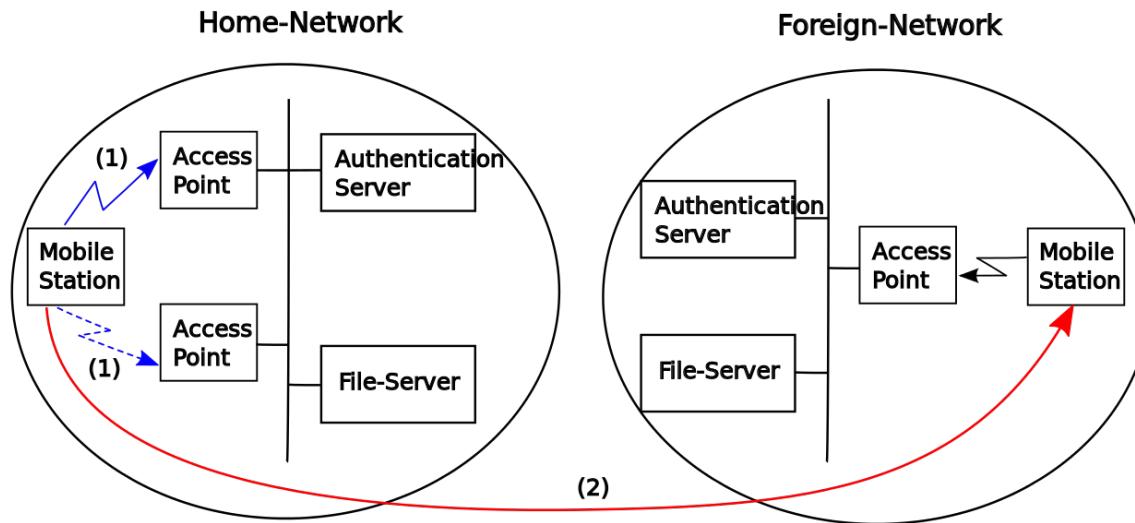
Roaming (1/7)

- **Définition**
 - Changement d'un PA par pour une station sans perte de connectivité réseau.
 - Mécanisme de niveau 2 (et 3) correspondant au modèle OSI associé au protocole 802.11.f en 2003.
- **Applications**
 - Beaucoup d'applications peuvent supporter de perdre/récupérer la connexion Internet mais certaines doivent la conserver (Exemples : VoIP, streaming, ...).

Roaming (2/7)

- Classification

- **Roaming intra-ESS (*Internal Roaming*)** : le mobile passe d'un PA à un autre PA au sein du même réseau sans fil
An authentication server (RADIUS) for re-authentication of MS via 802.1x (Use of EAP).
- **Roaming inter-ESS (*External Roaming*)** : le mobile se déplace dans le WLAN d'un autre fournisseur de service internet sans fil ou Wireless Internet Service Provider (WISP)



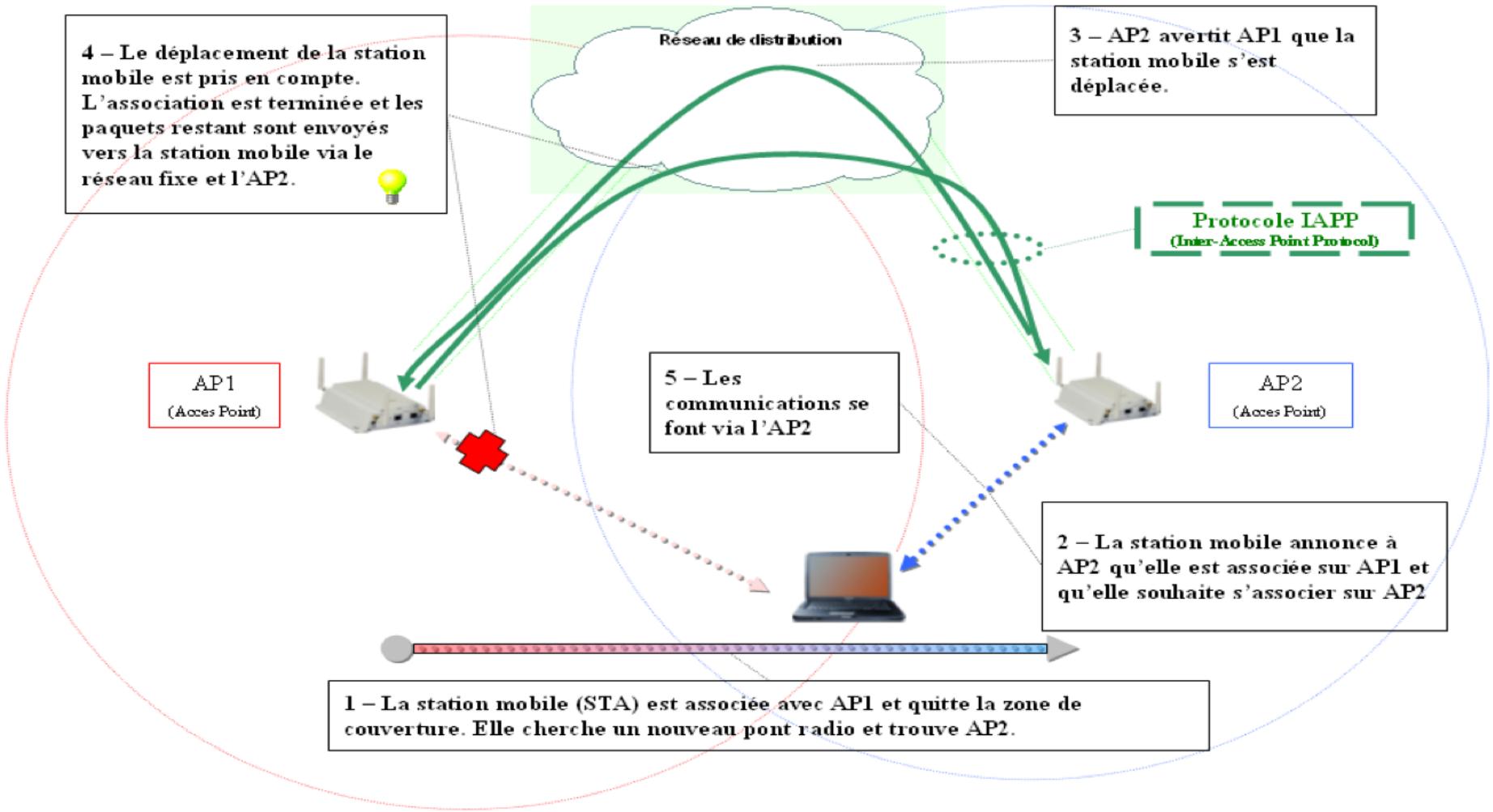
Roaming (3/7)

- Classification
 - **Roaming intra-ESS (*Internal Roaming*) :**
La station mobile passe d'un PA à un autre au sein du même réseau sans fil
 - **Roaming inter-ESS (*External Roaming*) :**
La station mobile se déplace dans le WLAN d'un autre fournisseur de service internet sans fil ou Wireless Internet Service Provider (WISP)

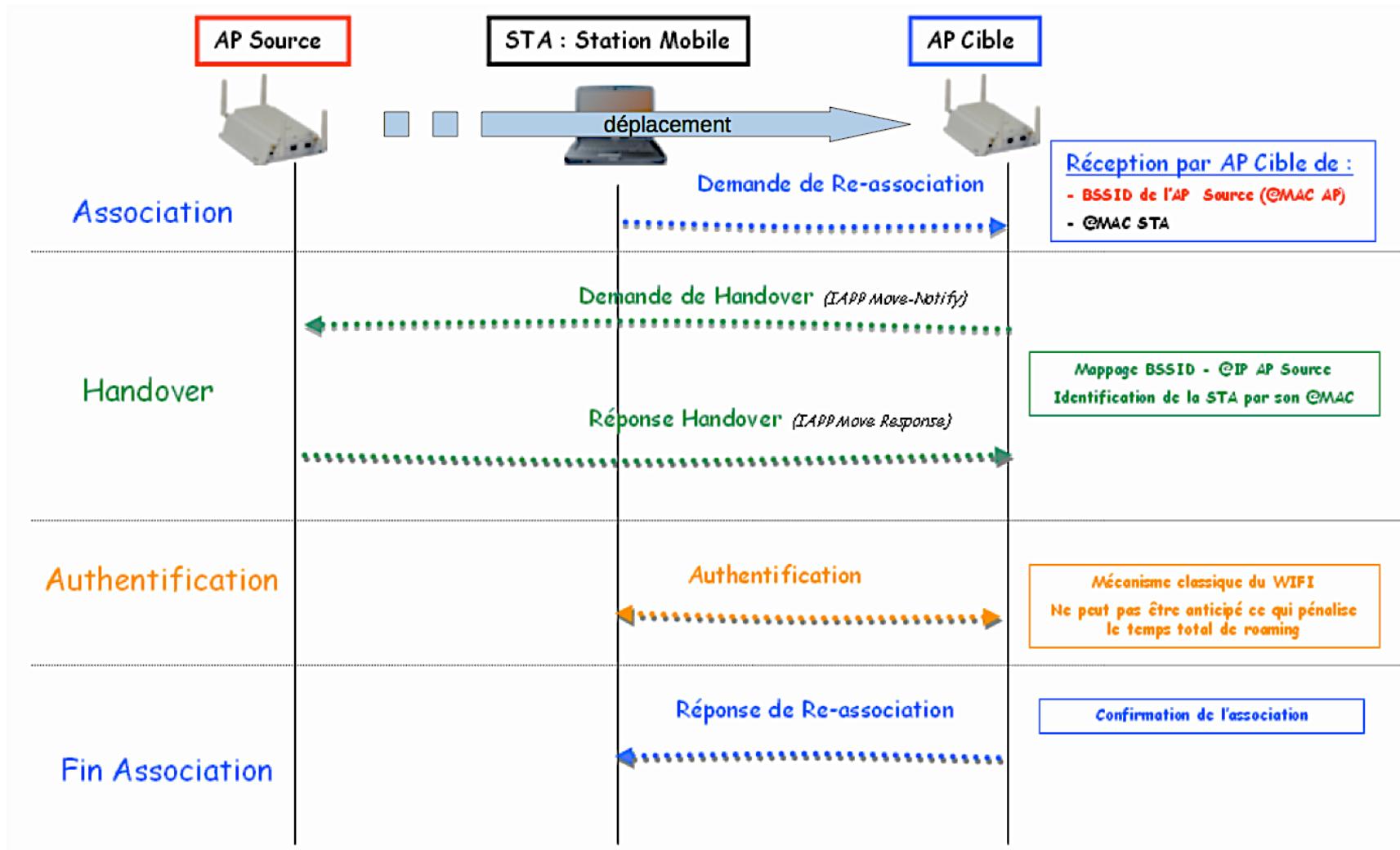
Roaming (4/7)

- **Association – désassociation**
 - Une station qui souhaite utiliser le réseau doit s'associer avec le point d'accès. Grâce à cette association, la station fait partie du BSS du point d'accès. Elle peut alors, utiliser les services du point d'accès. L'attachement entre la station mobile et le PA est rompu grâce à la désassociation
- **Distribution**
 - Service qui aiguille les trames. Il permet à une station mobile d'envoyer des trames à travers le système de distribution (DS) d'un BSS ou d'un ESS
- **Intégration**
 - Le service d'intégration permet aux différents PA de communiquer par un canal différent de 802.11, le plus souvent il s'agit d'un réseau local

Roaming (5/7)



Roaming (6/7)



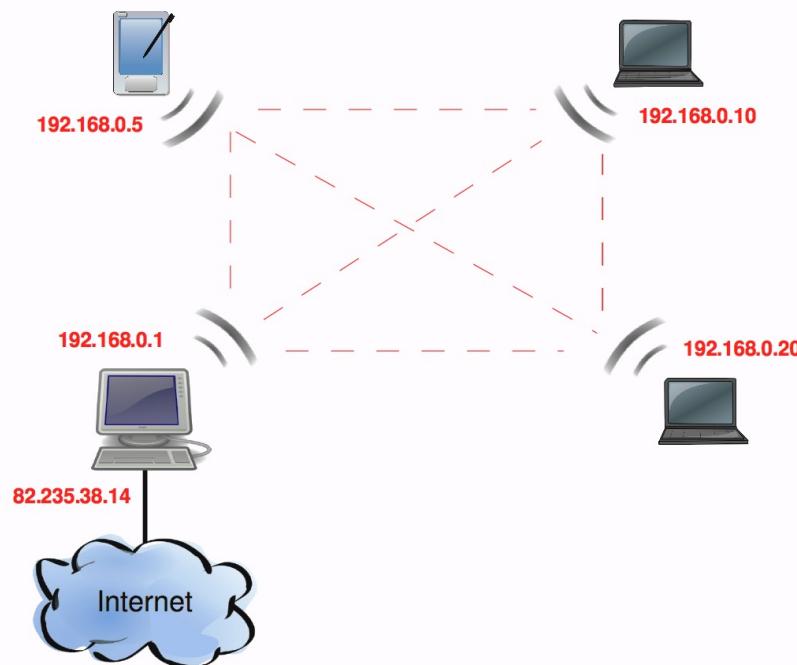
Roaming (7/7)

- Performances
 - Très lent pour la Voix sur IP (VoIP) → principalement du à la lenteur du mécanisme d'authentification
 - Les normes additionnelles pour améliorer le Roaming n'ont pas été finalisées
 - Désintérêt de la part des acteurs du marché
 - Echec de la norme 802.11f qui a été retirée en 2006 par l'IEEE
- Evolution du Roaming WiFi
 - Evolution de la norme 802.11i (authentification par WAP2)
 - Afin de palier au problème du Roaming avec la VoIP, l'IEEE se penche sur l'utilisation du réseau GSM associé au Wifi

Wi-Fi Protected Access

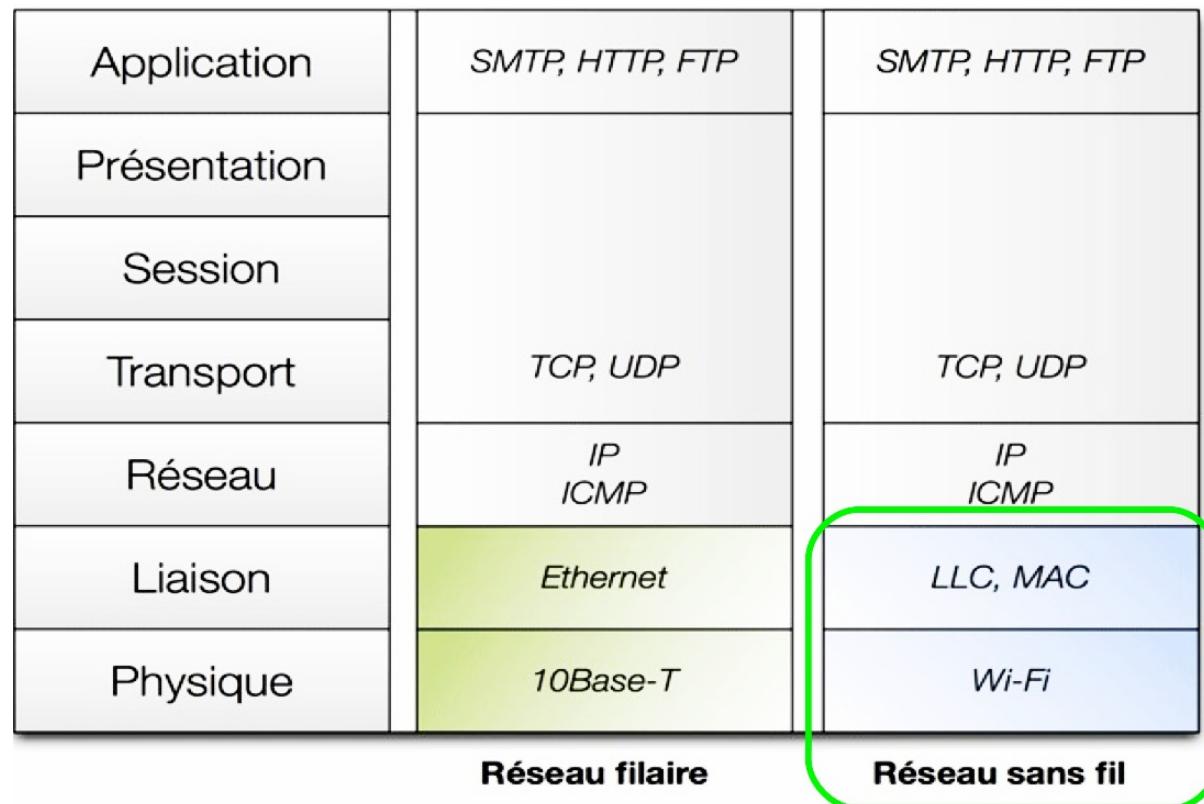
Mode Ad Hoc

- Les machines utilisateurs servent de routeurs entre elles (besoin d'algorithmes de routage particuliers)
- Infrastructure du réseau dynamique
- On parle de IBSS: Independent Basic Service Set



Le WiFi dans le Modèle OSI (1/3)

- Associé aux niveaux 1 et 2 du modèle OSI



Le WiFi dans le Modèle OSI (2/3)

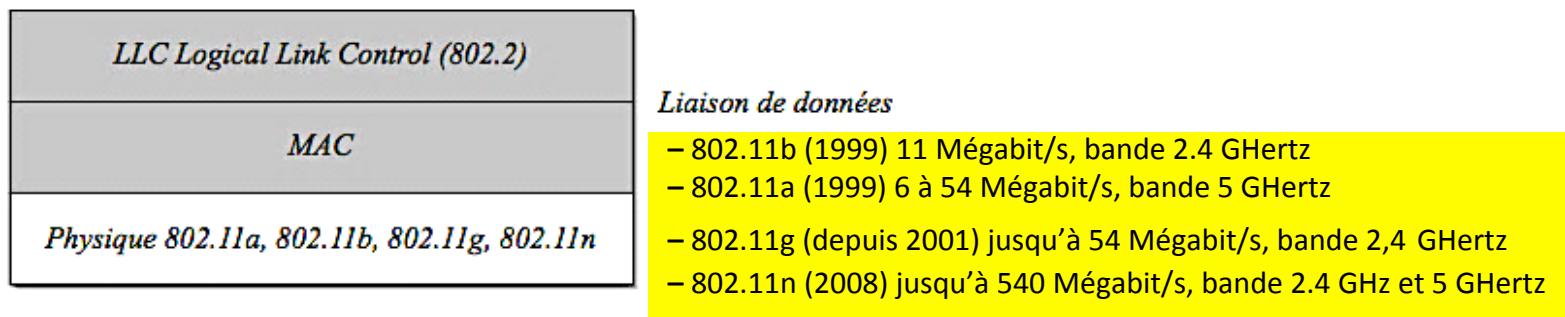
- **Couche physique**

- On retrouve les différentes normes utilisant la bande de fréquence ISM
- Différentes techniques de transmission pour éviter les problèmes d'interférences

Technique d'étalement de spectre à saut de fréquence FHSS

Technique d'étalement de spectre à séquence directe DSSS

Technologie infrarouge



ISM : Industrie, Science et Médecine

DSSS Direct Sequence Spread Spectrum 802.11 b et g

HFSS Frequency Hopping Spread Spectrum

Le WiFi dans le Modèle OSI (3/3)

- Couche liaison
 - Sous-couche LLC : Plusieurs fonctionnalités possibles dans LLC
 - Simple aiguillage vers les protocoles supérieurs grâce aux SAP (Point d'accès source et destination)
 - Connexion, contrôle de flux
 - Acquittement
 - Sous-couche MAC : Commune à l'ensemble des normes de la couche physique
 - Contrôle d'accès au support CSMA/CA
 - Adressage et formatage des trames
 - Détection d'erreur par CRC
 - Fragmentation et réassemblage
 - QoS, gestion de la mobilité et sécurité

Modes d'accès au médium

Mécanisme CSMA/CA

DCF (Distributed Coordination Function)

1. Basé sur le mécanisme CSMA/CA et l'acquittement positif
2. Employé en mode Ad hoc et AP

PCF (Point Coordination Function)

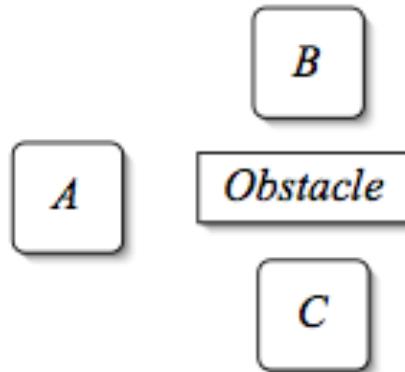
1. Utilise l'interrogation (Polling)
2. Mode AP uniquement

Remarque : Les deux mécanismes peuvent coexister dans une même cellule

Contrôle d'accès au support CSMA/CA_(1/2)

- Problématique

- Dans un réseau filaire, chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre
- Dans un réseau sans fil, ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée
- Possibilité de collisions due aux stations cachées (obstacle aux ondes radio ou éloignement)

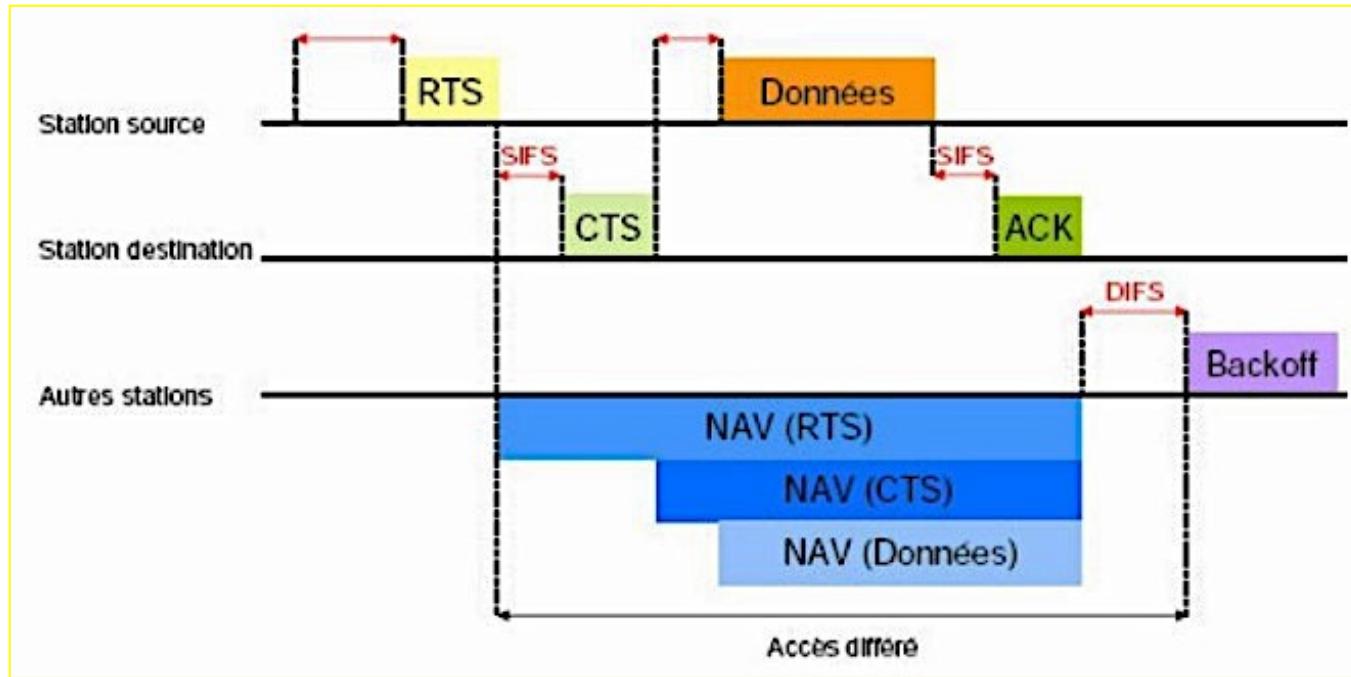


A VOIT B et C MAIS B et C NE SE VOIENT PAS

Contrôle d'accès au support CSMA/CA_(2/2)

- Une alternative
 - Mécanisme CSMA/CA
 - Mécanisme d'esquive de collision basé sur un principe d'accusé de réception réciproque Emetteur-Récepteur
 - Utilisation de paquets spéciaux :
 - RTS** (Request To Send)
L'émetteur demande une émission et précise la durée de l'émission
 - CTS** (Clear To Send)
Le récepteur PA accepte la transmission (toutes les stations reçoivent ce paquet - stations cachées)
 - Les autres émetteurs qui reçoivent le CTS, se mettent en attente de la durée indiquée
 - NAV** (Timer)

Accès au support via CSMA/CA et RTS/CTS



$$DIFS = SIFS + (2 * \text{Durée d'un slot})$$

SIFS : Short Inter-Frame Spacing
DIFS : DCF Inter-Frame Spacing

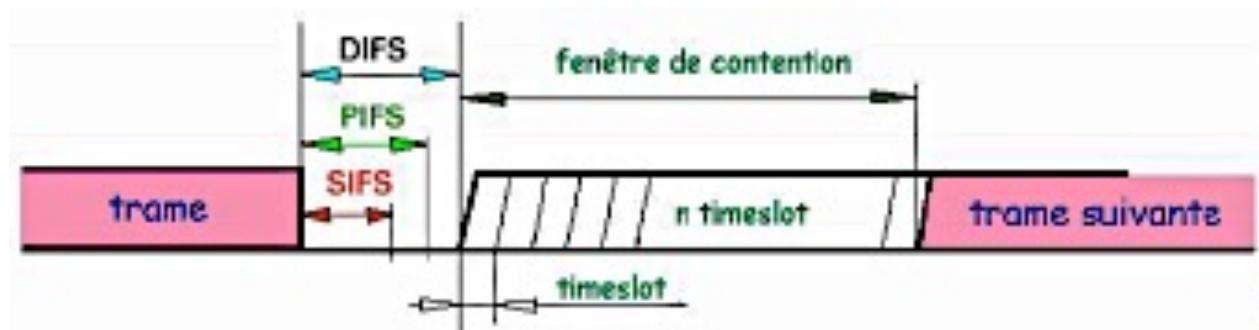
DCF : Distributed Coordination Function (mode d'accès par compétition)

PIFS : Point Coordination Function (mode d'accès contrôlé)

paramètre	DS	FH	IR	802.11b
Slot time	20 µs	50 µs	6 µs	20 µs
SIFS	10 µs	28 µs	7 µs	10 µs
DIFS	50 µs	128 µs	19 µs	50 µs

Espace inter-trames

- **SIFS (Short Inter Frame Space)** de $28\mu\text{s}$
Plus petit écart entre deux trames appartenant à un même dialogue (Exemple Fragment DATA-ACK).
- **PIFS (Point Coordination IFS)** de $78\mu\text{s}$
Utilisé par le PA pour obtenir l'accès au support avant n'importe quelle autre station.
- **DIFS (Distributed IFS)** de $128\mu\text{s}$
Intervalle utilisé par une station voulant initier une nouvelle transmission.



Algorithme Backoff (1/3)

- Résolution du problème d'accès au support (accès multiple et simultané)
 - Temps découpé en tranches ou timeslots, utilisé pour définir les intervalles IFS
1. Au début, chaque station détermine une valeur de temporisation, i.e., $\text{Backoff} \in (0, 7)$.
 2. Si le support est libre, chaque station décrémente son temporisateur jusqu'à ce que le support de communication soit occupé **OU** que le Backoff atteigne la valeur 0.
 3. Si le temporisateur n'atteint pas la valeur 0 et que le support est de nouveau occupé par une autre station, alors la station concernée bloque son temporisateur.

Et ainsi de suite, dès que la temporisation atteint la valeur 0, la station transmet sa trame via le support de communication.

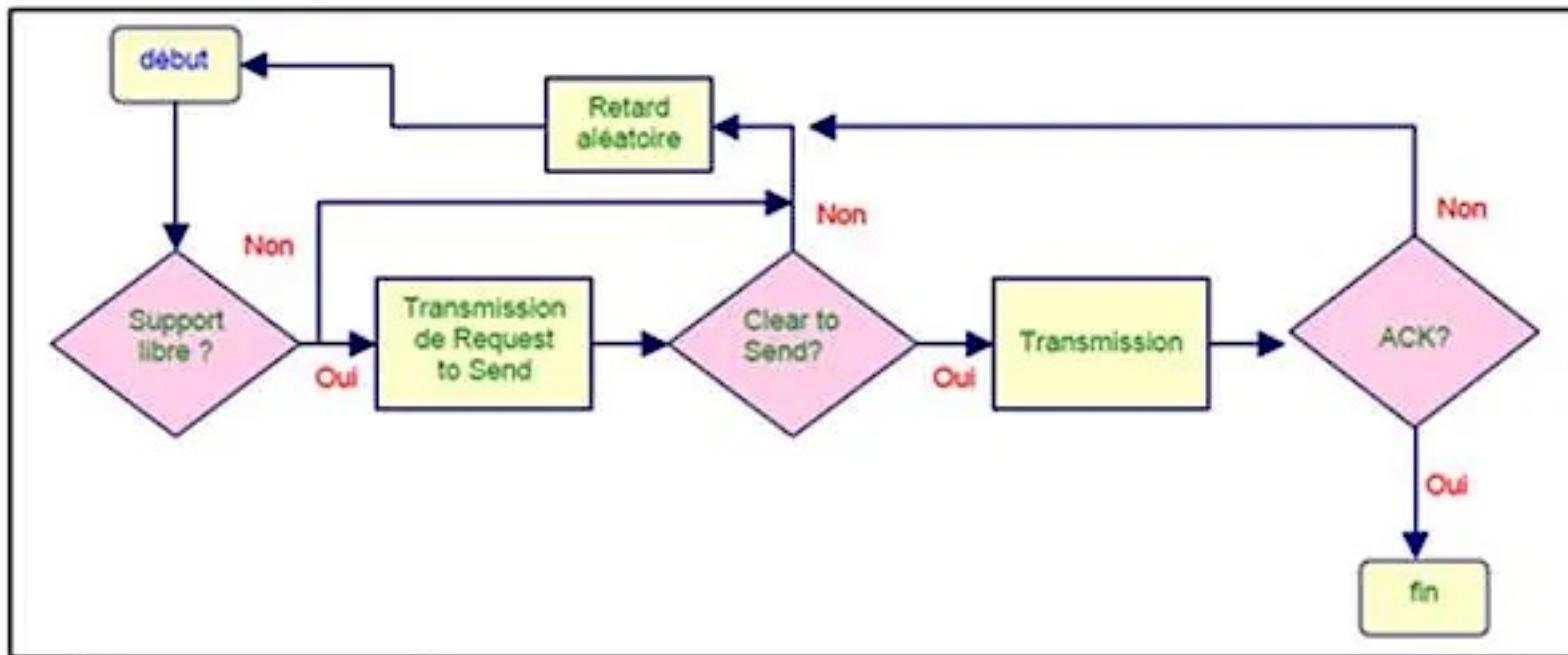
Dans le cas où plusieurs stations dispose de la même valeur de temporisation, i.e., 0, à un instant donné, le phénomène de collision se produit et chaque station devra régénérer un nouveau temporisateur $\in (0, 15)$.

A chaque tentative de retransmission, le temporisateur croît de manière exponentielle comme suite : $\text{rand}(2^c-1) \cdot \text{TimeSlot}$

c : Nombre de collisions que rencontre la station

TimeSlot : Nombre d'unités temporaires déterminées aléatoirement dans l'intervalle $0, 2^c-1$

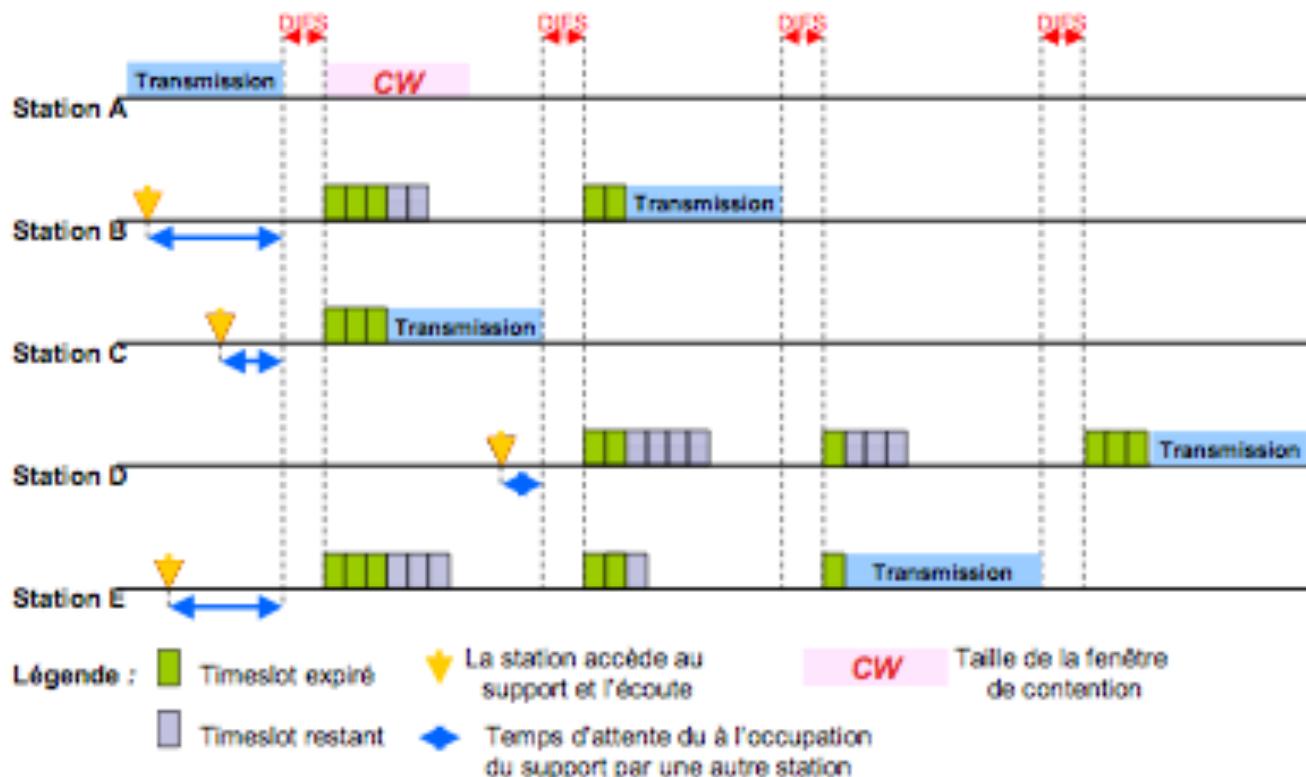
Algorithme Backoff (2/3)



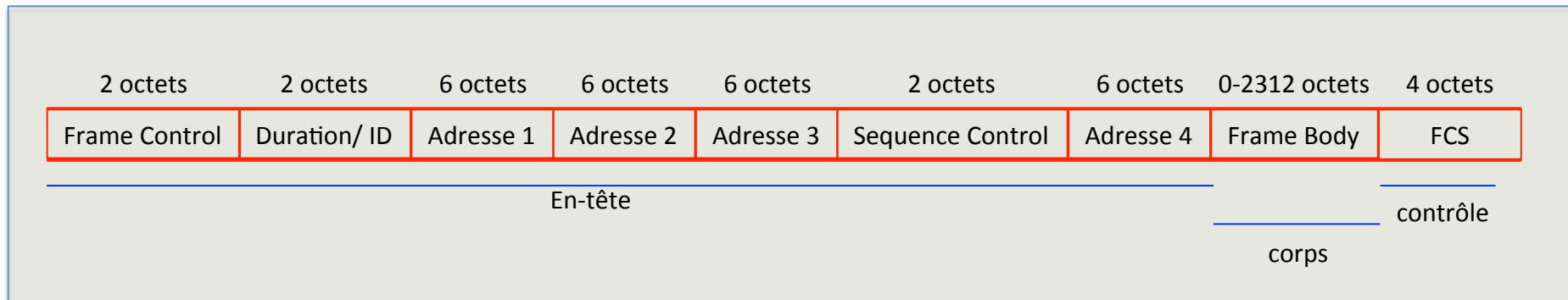
Algorithme Backoff

(3/3)

- Les stations ont la même probabilité d'accéder au support car chaque station doit, après chaque retransmission, réutiliser le même algorithme
- Inconvénient : pas de garantie de délai minimal
 - Complique la prise en charge d'applications temps réel telles que la voix ou la vidéo



Trame WiFi (1/4)



Champs optionnels (pas toujours)

Adresse 3

Adresse 4

Séquence de control

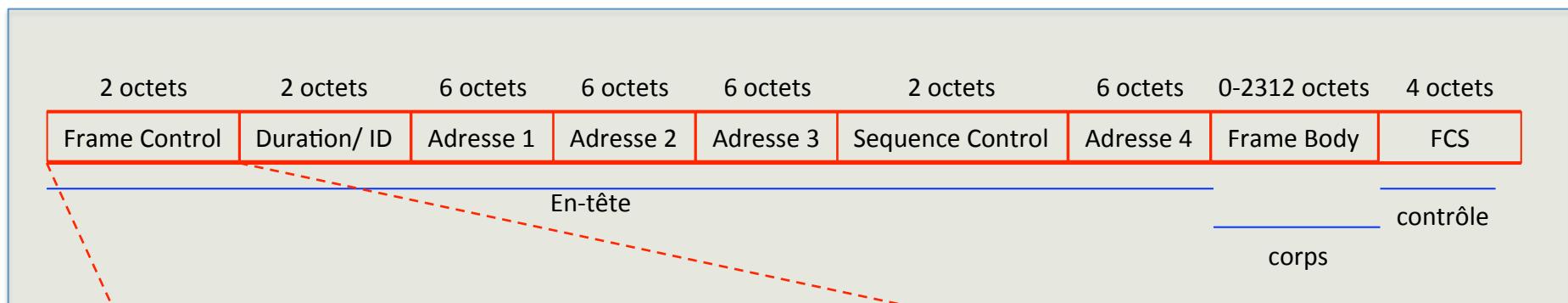
Frame Body

Frame Control

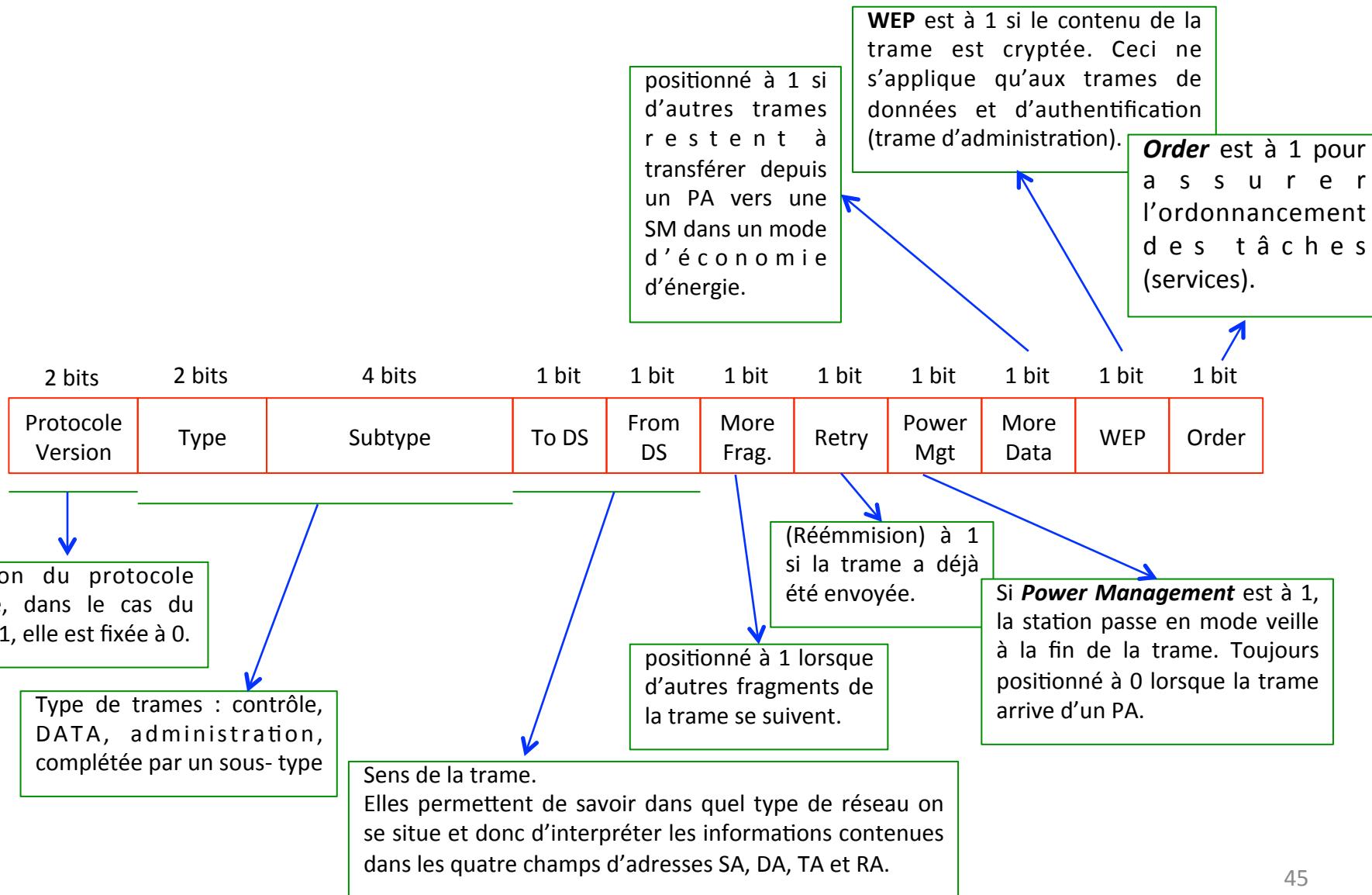
Champ de contrôle de la trame.

Trame WiFi (2/4)

Frame Control : Champ de contrôle de la trame

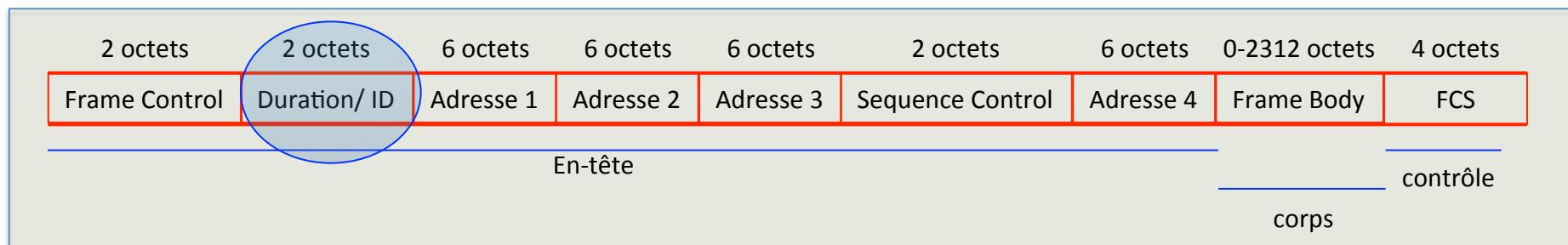


Trame WiFi (2/4)



Trame WiFi (3/4)

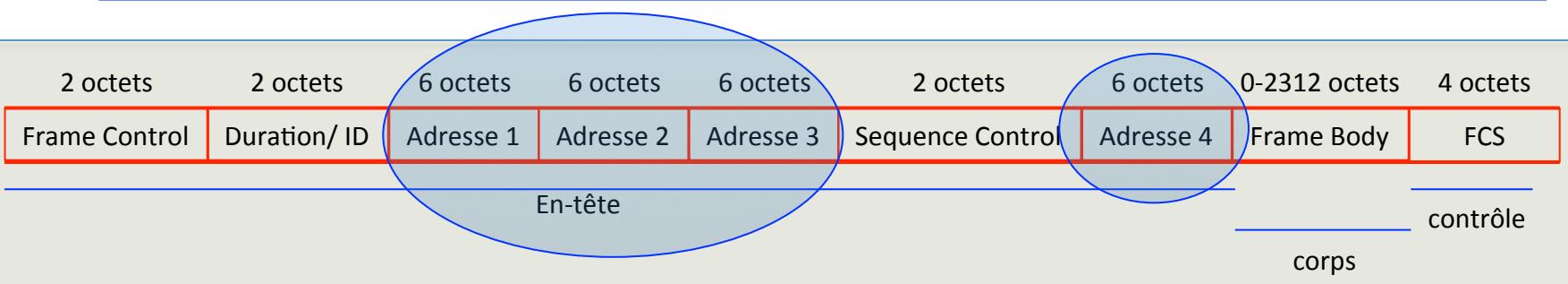
La valeur est codée sur 2 octets et correspond soit à la mise à jour du NAV (en μ s), et dans ce cas la valeur est inférieure à 32767, soit la valeur correspond à l'ID d'une SM par rapport au PA (déterminé au moment de l'association).



Trame WiFi (3/4)

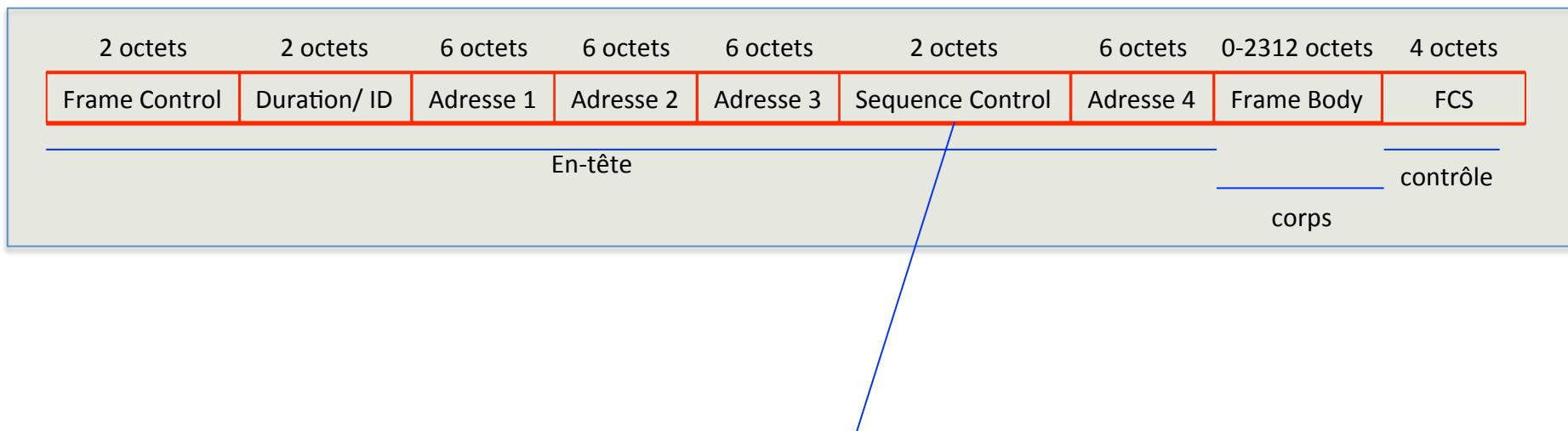
La mise en place des adresses dépend fortement des champs déjà souscrits dans le **Frame Control**.

1. SA est l'@ MAC source qui envoie le message. Elle peut être l'adresse du PA (BSSID).
2. DA est l'@ MAC destination à qui est destiné le message.
3. TA est l'@ MAC qui se réfère à la station ayant mis le message sur le réseau sans fil.
4. RA est l'@ MAC qui se réfère à la station recevant le message du réseau sans fil.



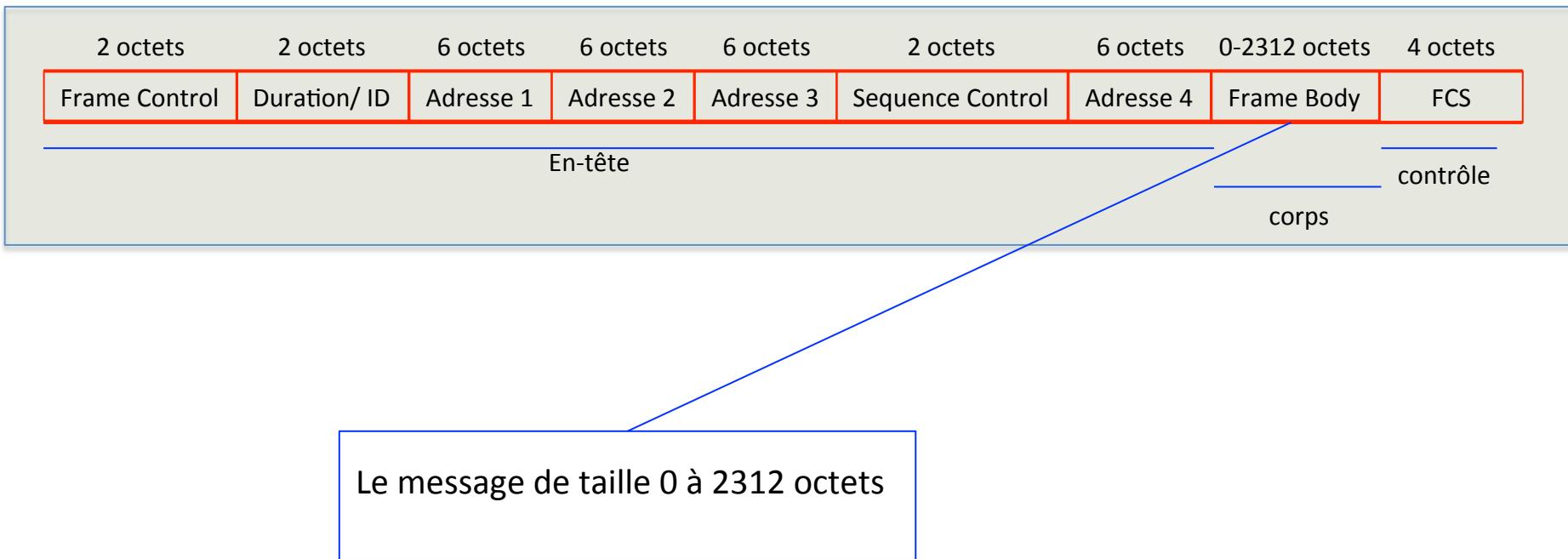
To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	BSSID	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

Trame WiFi (4/4)

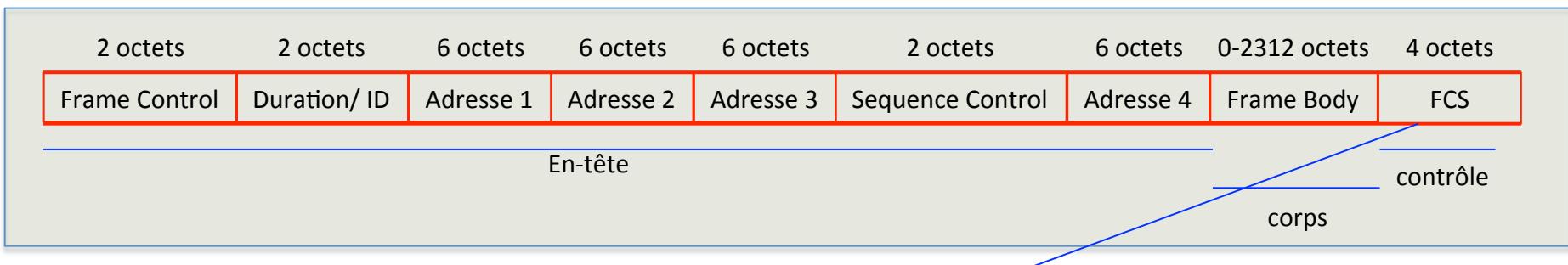


Utilisée dans le cas d'envoi de trames fragmentées et est codée sur 16 bits.
Cette valeur comprend la séquence (sur 12 bits), c'est à dire le numéro de la trame envoyé, et le numéro du fragment (sur 4 bits).

Trame WiFi (4/4)



Trame WiFi (4/4)

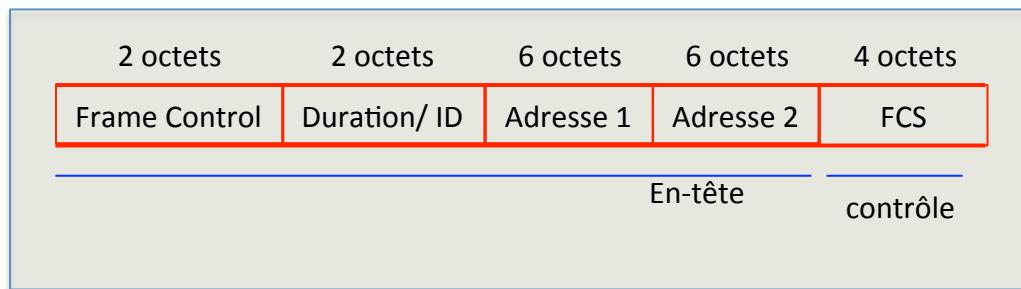


Champ de contrôle de 32 bits dont la valeur est calculée suivant une formule polynomiale.

Une station qui reçoit une trame recalcule le FCS pour vérifier qu'il n'y a pas eu de problème durant la transmission.

Trames WiFi spécifiques (1/3)

RTS

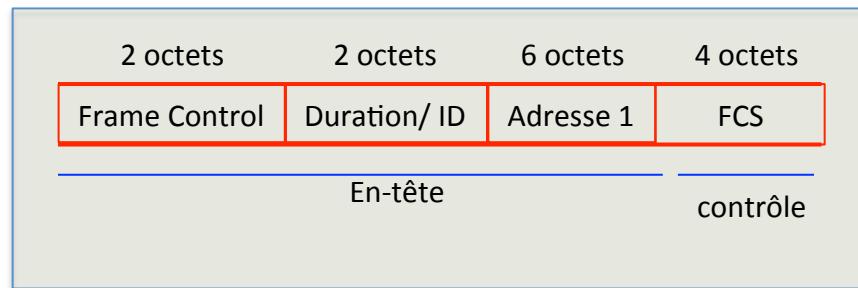


Dans cette trame on positionne l'adresse de la station sans fil qui recevra la trame et qui participe au processus du RTS/CTS (adresse RA) dans l'adresse 1.

Et dans l'adresse 2, on positionne l'adresse de la station du réseau sans fil qui émet la trame (adresse TA).

Trames WiFi spécifiques (2/3)

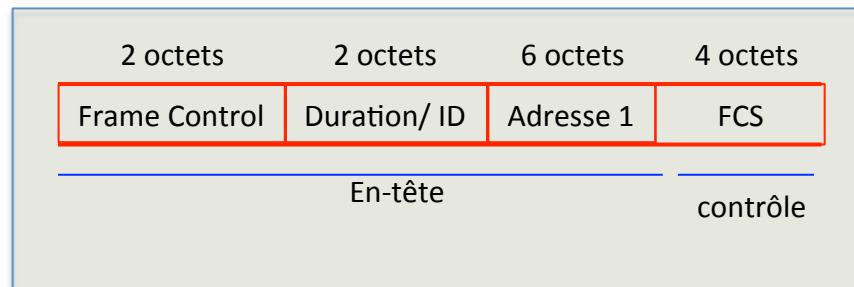
CTS



L'adresse 1 prend pour valeur l'adresse de la station sans fil qui recevra la trame (adresse RA), c'est la même adresse que l'adresse 2 de la trame RTS.

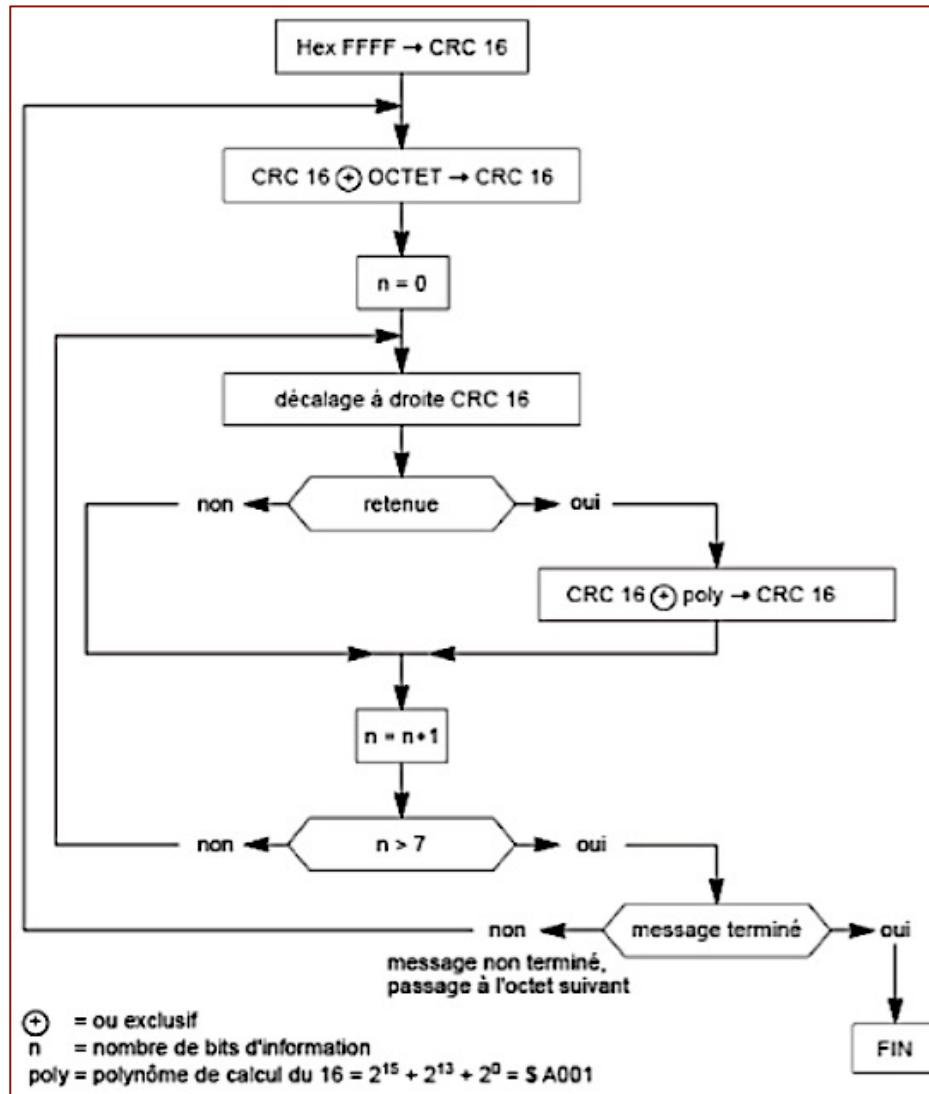
Trames WiFi spécifiques (3/3)

ACK



L'adresse 1 prend la valeur de l'adresse qui recevra cette trame (adresse RA).

Calcul du FCS



Pour le WiFi, le polynôme générateur est d'ordre 32