

Cours  - *R.301*

RT - IUT Colmar – 2022 / 2023

*Jean Luc Biellmann
contact@alsatux.com*



Les technologies sans fil

Abréviaison	WPAN	WLAN	WMAN	WWAN / WRAN
<i>Nom complet</i>	Wireless Personal Area Network	Wireless Local Area Network	Wireless Metropolitan Area Network	Wireless Wide/Régional Area Network
<i>Portée</i>	1-100 m	1-300 m	1-10 km	10-100 km
<i>Normes</i>	IEEE 802.15 1 IEEE 802.15 3 IEEE 802.15 4	IEEE 802.11 b/a/g/ n/ac/ax/be, (HiperLAN)	IEEE 802.16 a/e	IEEE 802.20 IEEE 802.22
<i>PMax</i>	100 mW	100 mW à 500 mW	5-10 W	W-kW

Les technologies sans fil

WPAN 802.15	- 802.15.1 : Bluetooth - 802.15.3 : Haut-débit / UWB (Ultra Wideband) - 802.15.4 : Bas-débit / Zigbee - 802.15.7 : LiFi / VLC (Visible Light Communication)
WLAN 802.11	- WiFi (Wireless Fidelity)
WMAN 802.16	- Boucle Locale Radio (BLR) - WiMAX (Worldwide Interoperability for MicroWave Access)
WWAN / WRAN 802.20/22	- 2G : GSM (Global System for Mobile Communications) - 2,5G : GPRS (General Paquet Radio Service) - 2,75G : EDGE (Enhanced Data Rates for GSM Evolution) - 3G : UMTS (Universal Mobile Télécommunications System) - 3G+ : HSDPA (High Speed Downlink Packet Access) - 4G : LTE (Long Term Evolution) - 4G+ : LTE Advanced - 5G...

Organismes régulateurs

**Wi-Fi
Alliance**

Consortium industriel qui possède la marque WiFi.

WiFi 1,2,3,...

IEEE

Institut of Electrical and Electronics Engineers

IEEE
802.11b/g/n/...

FCC

Federal Communication Commission

ETSI

European Telecommunications Standards Institute

HiperLAN

- HiperLAN = HIgh PERformance radio LAN

Compatibilité descendante du WiFi

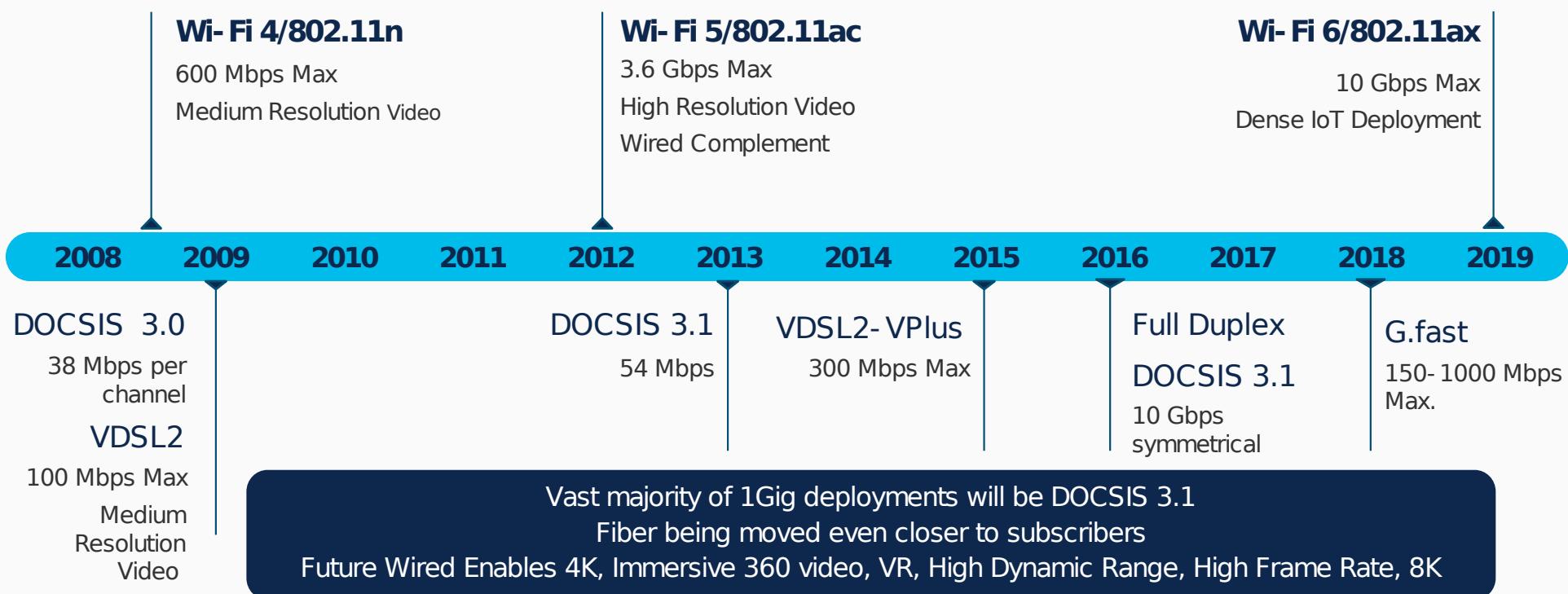
- Interopérabilité obligatoire avec les anciennes versions
- Problème des failles trouvées depuis, et du matériel encore utilisé. Nécessité donc de :
 - bloquer les portes d'entrées « trouées »
 - de mettre à jour les appareils (quand cela est possible)
 - de renouveler les appareils/le parc sinon
- Nécessité de comprendre l'historique de la norme, et sa construction incrémentale

Statistiques & Prévisions CISCO

By 2023, 27.4% of WLAN Endpoints will be equipped with 802.11ax (Wi-Fi 6)

By 2023, 66.8% of WLAN Endpoints will be equipped with 802.11ac (Wi-Fi 5)

Future Wi-Fi Enables Virtualization, IoT, Speech Processing, Security, Data Analytics



source : Cisco Annual Internet Report, 2018-2023

Statistiques & Prévisions CISCO

- Wi-Fi momentum
 - Wi-Fi hotspots will grow four-fold from 2018 to 2023. Globally, there will be nearly **628 million public Wi-Fi hotspots by 2023**, up from 169 million hotspots in 2018.
 - **Wi-Fi6 hotspots** will grow 13-fold from 2020 to 2023 and will be **11 percent of all public Wi-Fi hotspots by 2023**
- Security analysis
 - The number of breaches and total records exposed per breach continue to grow. Globally, there was a 776% growth in attacks between 100 Gbps and 400 Gbps Y/Y from 2018 to 2019, and **the total number of DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023.**

Portée du signal

Rappel: la portée d'un rayonnement électromagnétique diminue avec la fréquence !

- 2,4 Ghz (802.11 b/g/n) : environ 70 m en intérieur
- 5 Ghz (802.11 n/ac/ax) : environ 35 m en intérieur
- 6 Ghz (802.11 be) : ? (sûrement 30m)

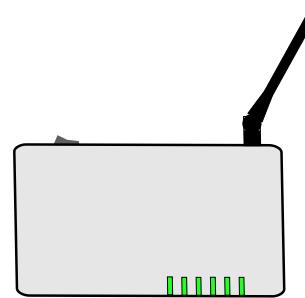
Fréquence diminuée

= Débit diminué

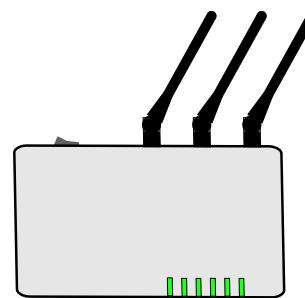
= Portée augmentée

Multiple-Input Multiple-Output – 1/3

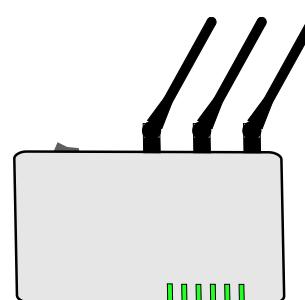
entrées multiples, sorties multiples



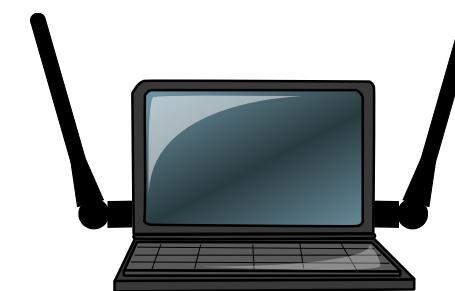
SISO



MISO



MIMO



Multiple-Input Multiple-Output – 2/3

Mono ou multi-utilisateurs

- **SU-MIMO = Single User MIMO** (défini dans 802.11n) est orienté mono-utilisateur
- **MU-MIMO = Multi User MIMO** (défini dans 802.11ac) est orienté multi-utilisateurs. Permet de mieux utiliser la bande passante disponible.

Multiple-Input Multiple-Output – 3/3

débits et diversité

- Il existe plusieurs types de MIMO :
 - Certains **multiplexent le signal sur plusieurs antennes**, à la fois en émission et en réception, pour augmenter le débit de transmission.
 - D'autres luttent contre l'évanouissement du signal en jouant sur **la diversité des antennes**.
 - D'autres enfin utilisent **le déphasage entre antennes**, pour favoriser la direction de propagation (beamforming ou formation de faisceau) et diminuer la pollution électromagnétique environnante.
- Certains appareils peuvent combiner ces fonctions.

Rappel collisions et interférences

Quand 2 ondes se rencontrent...

- **collisions** sur un même canal, gérées par un algorithme de détection.
- **interférences** avec les autres appareils environnants utilisant les mêmes fréquences : radio-amateurs, fours micro-onde, autres équipements WiFi (caméras, ...), radars, ...
- **zones d'ombres** dues à des trajets différents de l'onde. Résolu en activant la **diversité des antennes** (au moins 2 en émission/réception).

Bandé ISM – 2,4 Ghz - 2/4

WiFi1 / 802.11b – WiFi 3 / 802.11g – WiFi 4 / 802.11n - WiFi 6 / 802.11ax – WiFi 7 / 802.11be

Canal	Fréquence (MHz)	Zones
1	2412	
2	2417	
3	2422	
4	2427	
5	2432	
6	2437	Japon / Europe / USA
7	2442	
8	2447	
9	2452	
10	2457	
11	2462	
12	2467	Japon / Europe
13	2472	
14	2484	Japon

bande ISM

- Industrielle
- Scientifique
- Médicale

En Europe

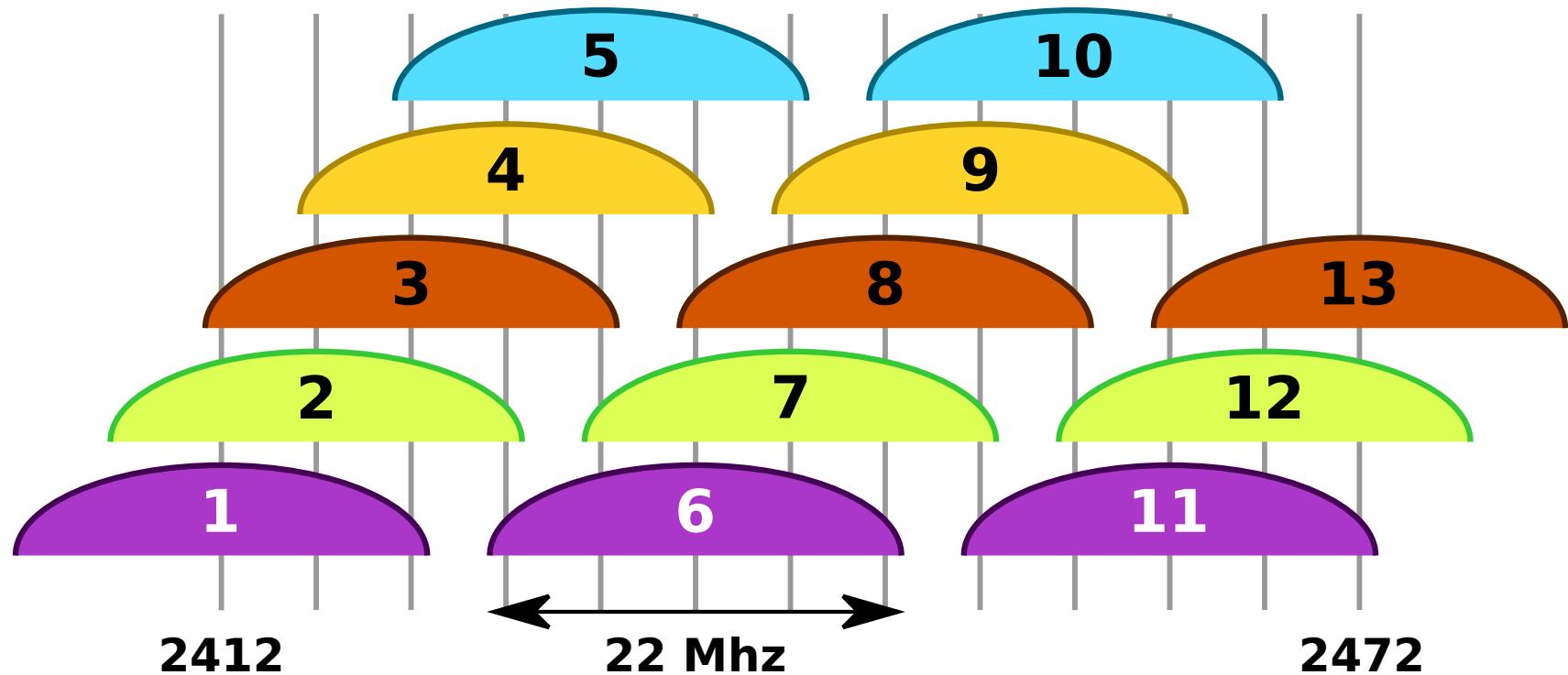
- 2400-2483,5 Mhz
- bande UHF

En France

- canaux 1 à 11

Band ISM – 2,4 Ghz – 1/4

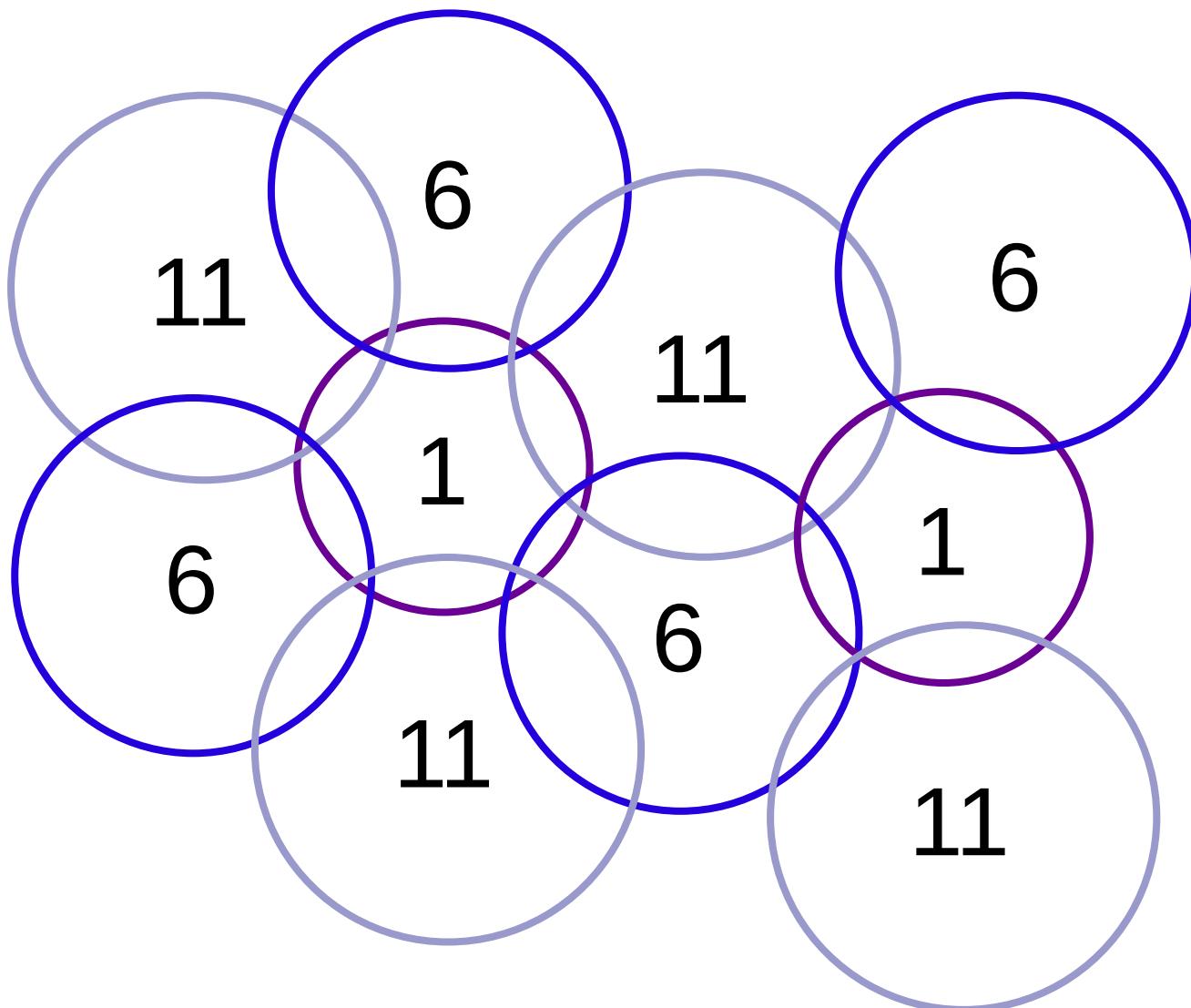
recouvrement de fréquence en 802.11 b



- Les canaux 12 et 13 sont quasi interdits aux USA (sauf à faible puissance / low power), le 14 étant strictement interdit dans ce pays.

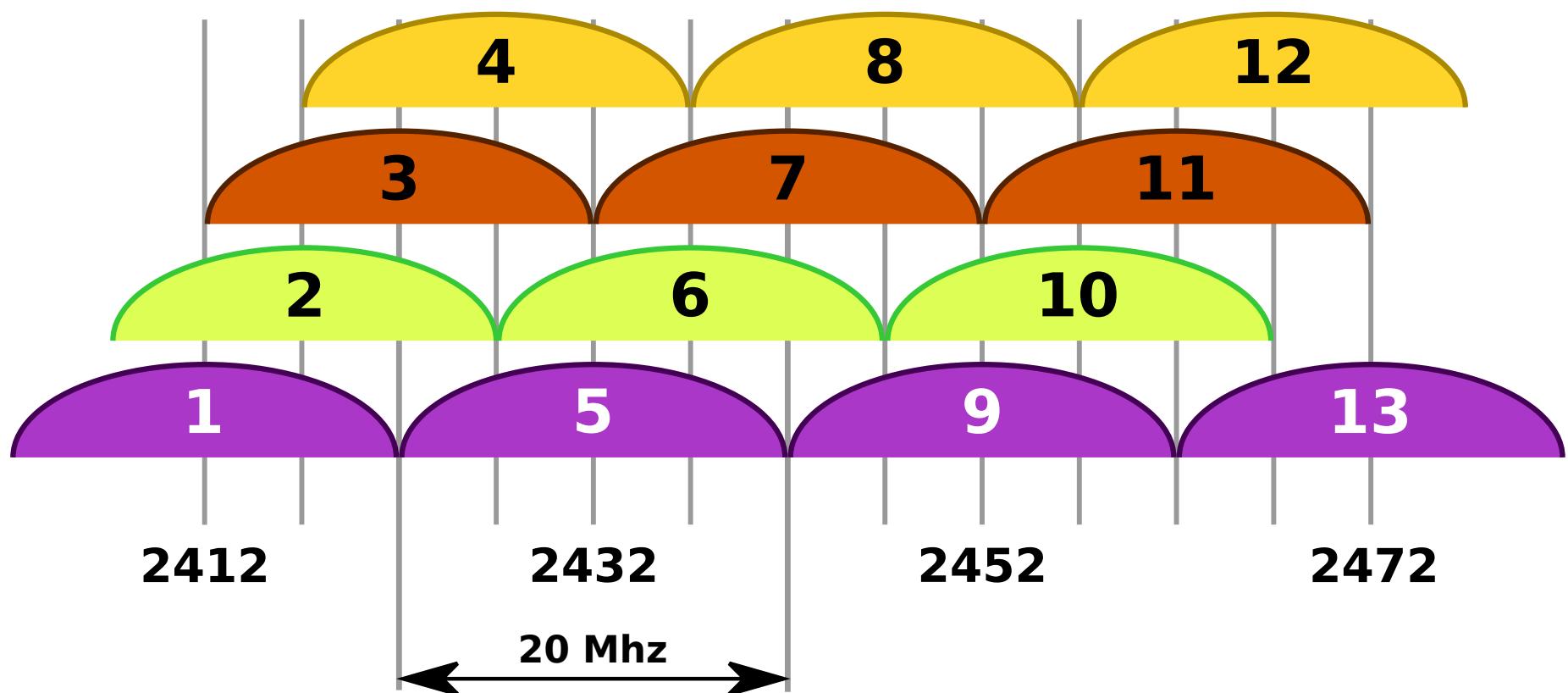
Bande ISM – 2,4 Ghz – 3/4

recouvrement des canaux en 802.11b/g/n



Band ISM – 2,4 Ghz – 4/4

recouvrement de fréquence en 802.11 g/n



- FDM = Frequency Division Multiplexing

Bandes U-NII – 5 Ghz - 1/4

WiFi 2 / 802.11 a – WiFi 4 / 802.11n - WiFi 5 /802.11ac – WiFi 6 / 802.11ax – WiFi 7 / 802.11be

Canal	Bandes	Fréquence (MHz)	Zones
36	1	5180	Europe / USA
40	1	5200	
44	1	5220	
48	1	5240	
52	2	5260	
56	2	5280	
60	2	5300	
64	2	5320	
100	2e	5500	
104	2e	5520	
108	2e	5540	
112	2e	5560	
116	2e	5580	
120	2e	5600	

Canal	Bandes	Fréquence (MHz)	Zones
124	2e	5620	Europe / USA
128	2e	5640	
132	2e	5660	
136	2e	5680	
140	2e	5700	
144	2e	5720	
149	3	5745	
153	3	5765	
157	3	5785	
161	3	5805	
165	3	5825	

Regroupement canaux adjacents

- par 2 en 802.11 n (2 x 20 MHz)
- par 2/4/8 en 802.11 ac/ax

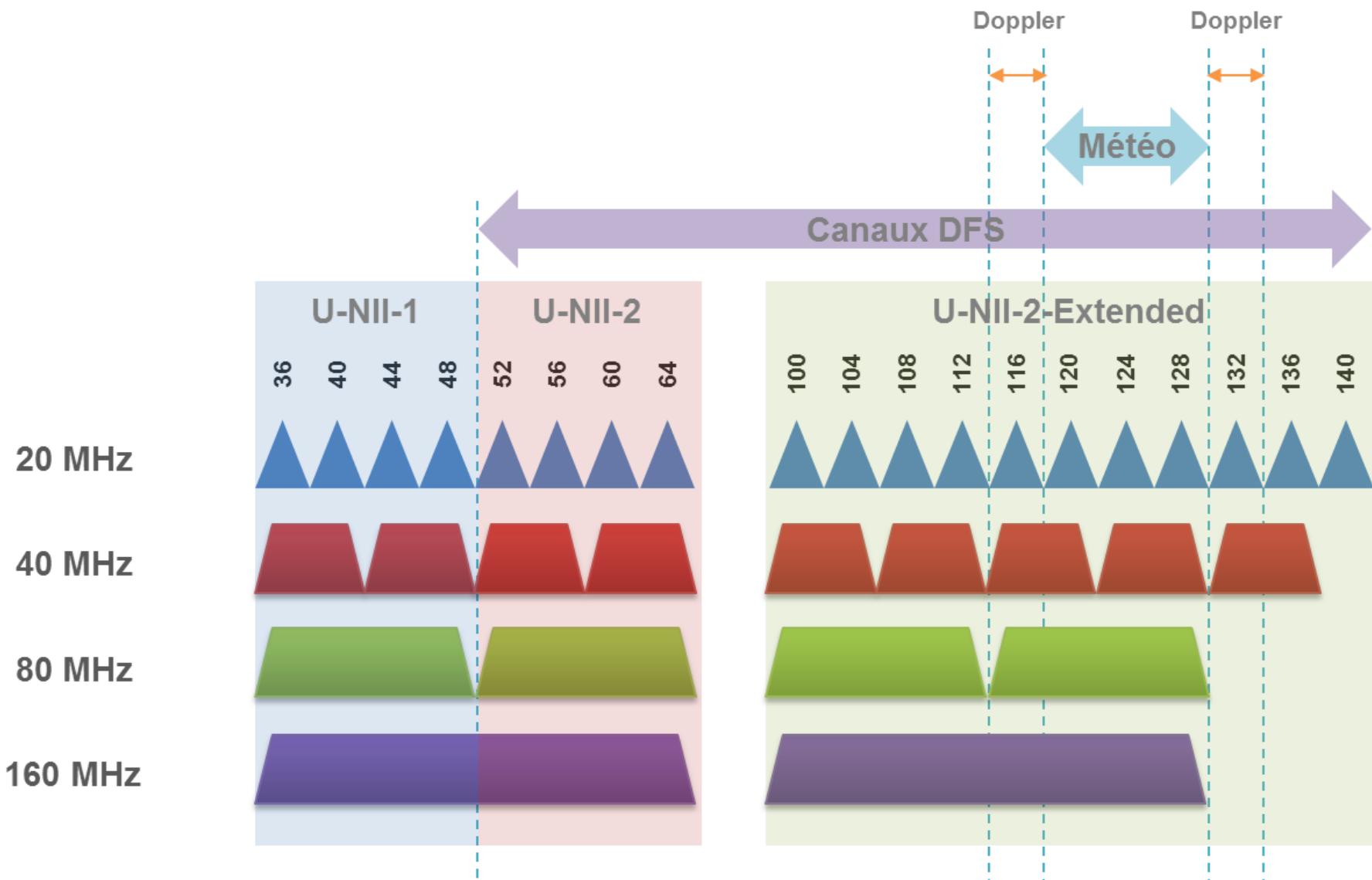
Bandes U-NII – 5 Ghz - 2/4

WiFi 2 / 802.11 a – WiFi 4 / 802.11n - WiFi 5 /802.11ac – WiFi 6 / 802.11ax – WiFi 7 / 802.11be

- 2 sous-bandes de 8 et 11 canaux de 20 MHz.
 - Avant 802.11ax, chaque canal de 20 MHz est divisé en 64 sous-canaux espacés de 312,5 KHz.
 - À partir de 802.11ax, chaque canal de 20 MHz est divisé en 256 sous-canaux espacés de 78,125 Khz.
- MAIS... **les bandes UNII-2 et U-NII-2-Extended sont soumises au DFS (Dynamic Frequency Selection)** : en cas de détection de signaux radars météo ou militaires, la station est sensée changer automatiquement de canal.
- « le responsable d'un brouillage par manquement réglementaire encourt par ailleurs des sanctions pénales qui peuvent aller jusqu'à six mois d'emprisonnement et 30 000 euros d'amende en application de l'article L39-1 du CPCE ».
- « l'utilisateur responsable du brouillage est redevable d'une taxe de 450 euros pour frais d'intervention (Art. 45, chapitre II de la loi de finances pour 1987, modifié par l'article 90 de la loi de finances rectificative pour 2003) »

Bandes U-NII – 5 Ghz - 3/4

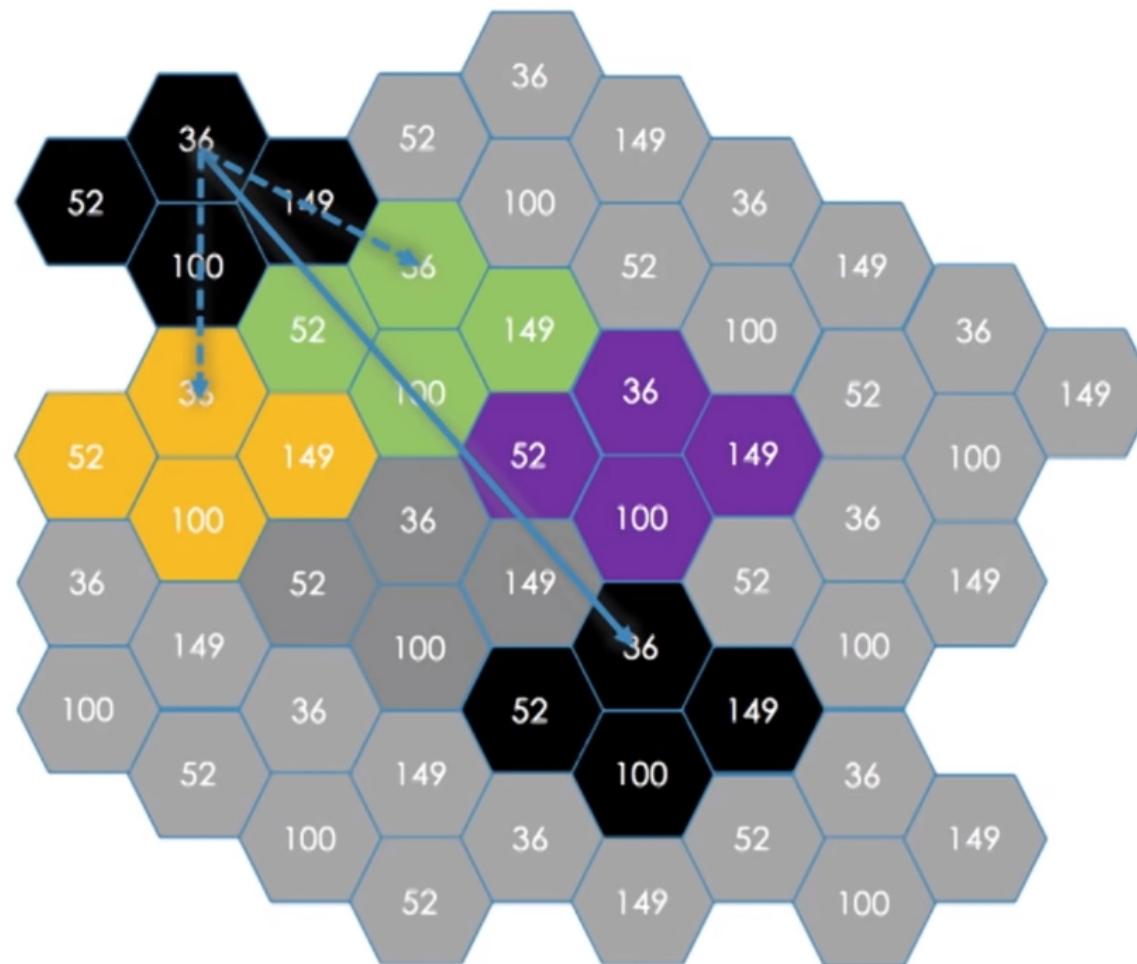
WiFi 2 / 802.11 a – WiFi 4 / 802.11n - WiFi 5 /802.11ac – WiFi 6 / 802.11ax – WiFi 7 / 802.11be



Source : <https://wifispeed.pressbooks.com/chapter/introduction-2/>

Bandes U-NII – 5 Ghz - 4/4

recouvrement des canaux en 802.11ac/ax/be



Attention : certains numéros de canaux ici représentés sont interdits en France !

Bandes U-NII - 6 GHz

WiFi 6E / 802.11ax – WiFi 7 / 802.11be

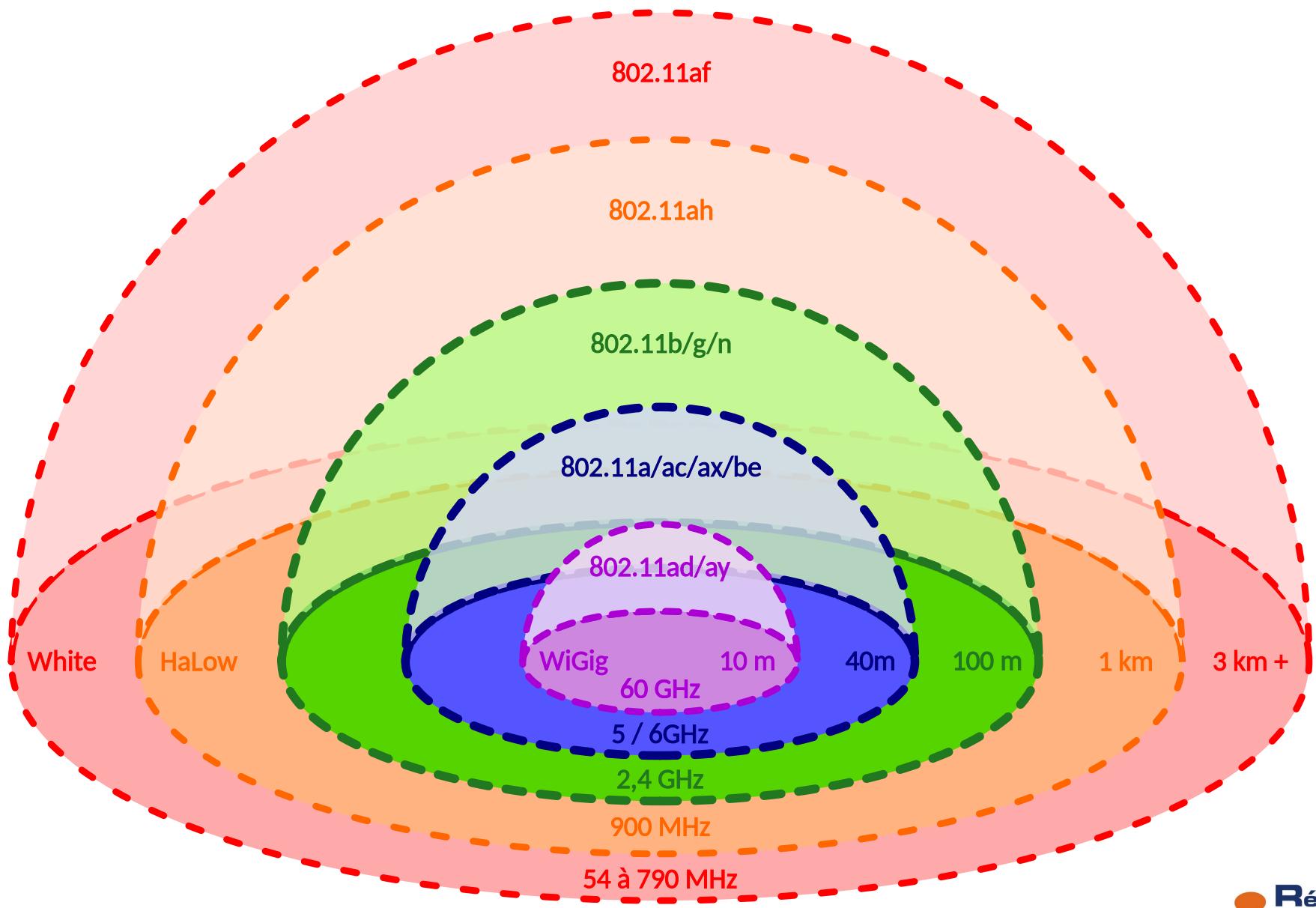
Canal	Bandes	Fréquence (MHz)	Zones
36	5	5935	Europe
40	5	5955	
44	5	5975	
48	5	5995	
52	5	6015	
56	5	6035	
60	5	6055	
64	5	6075	
100	5	6095	
104	5	6115	
108	5	6135	
112	5	6155	
116	5	6175	
120	5	6195	

Canal	Bandes	Fréquence (MHz)	Zones
36	5	6215	Europe
40	5	6235	
44	5	6255	
48	5	6275	
52	5	6295	
56	5	6315	
60	5	6335	
64	5	6355	
100	5	6375	
104	5	6395	
108	5	6415	

Regroupement canaux adjacents

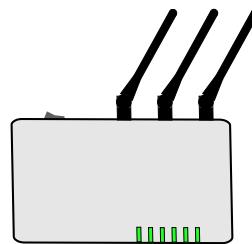
- par 16 en 802.11be

Couverture

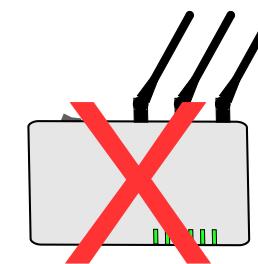


Les deux topologies de base

Avec point d'accès



Sans point d'accès



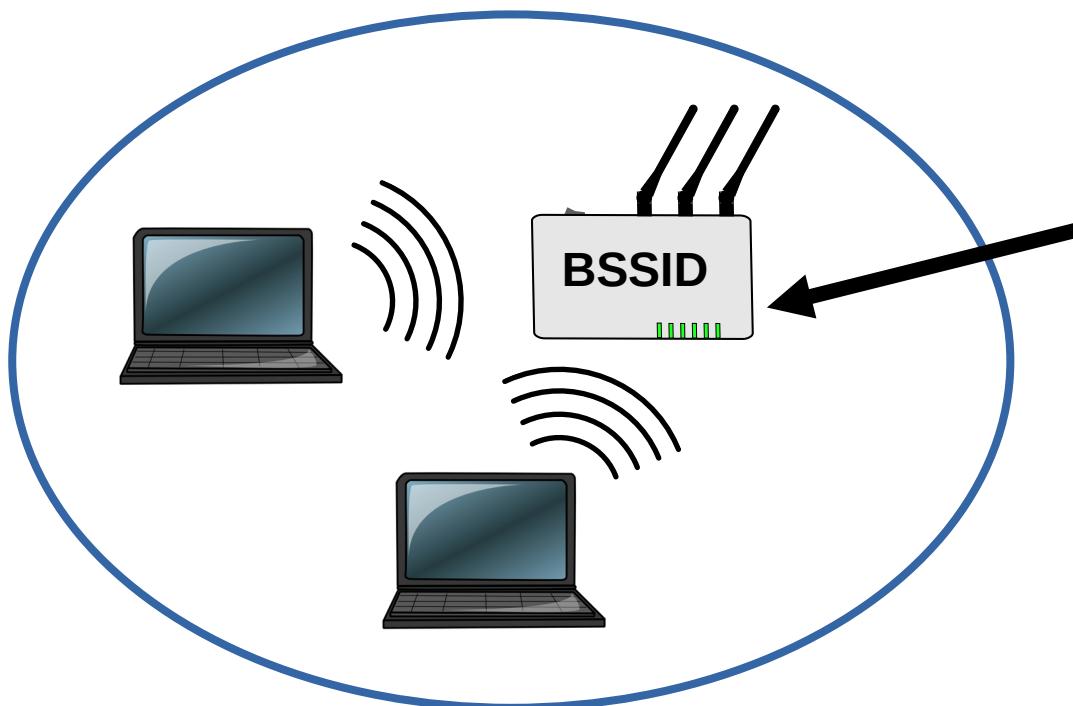
**Mode infrastructure
(en étoile)**

**Mode ad-hoc / mesh
(en P2P)**

Mode « Infrastructure » - 1/3

La « cellule BSS »

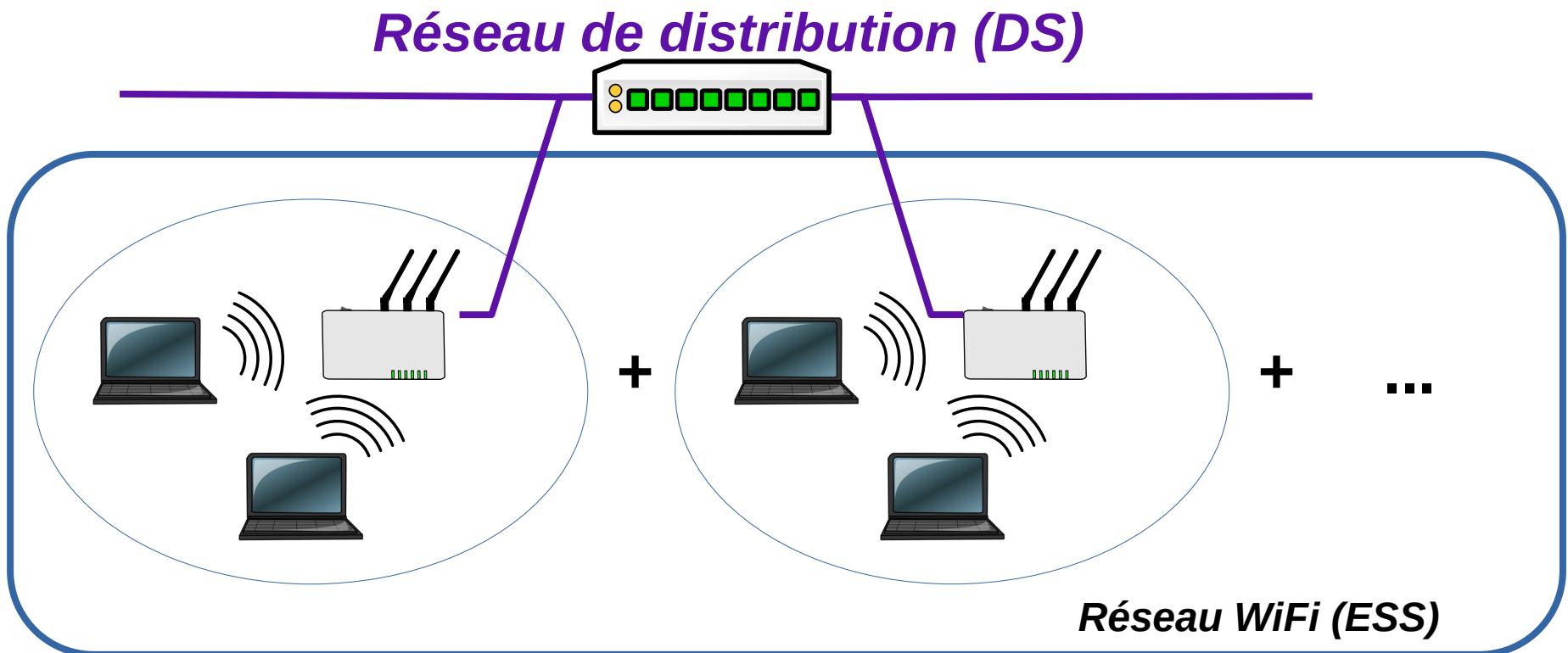
- **BSS = Basic Service Set** ou ensemble de services de base. **BSSID** = adresse MAC de l'AP sur 6 octets (48 bits).
- Le débit de l'AP est partagé entre les stations



1 point d'accès
(Access Point)
fait le lien entre réseau
filaire et sans-fil (donc
2 interfaces minimum)

Mode « Infrastructure » - 2/3

Les cellules **BSS** sont reliées entre elles par un réseau de distribution (**DS** - *Distribution System*) pour former un ensemble de service étendu (**ESS** - *Extended Service Set*).

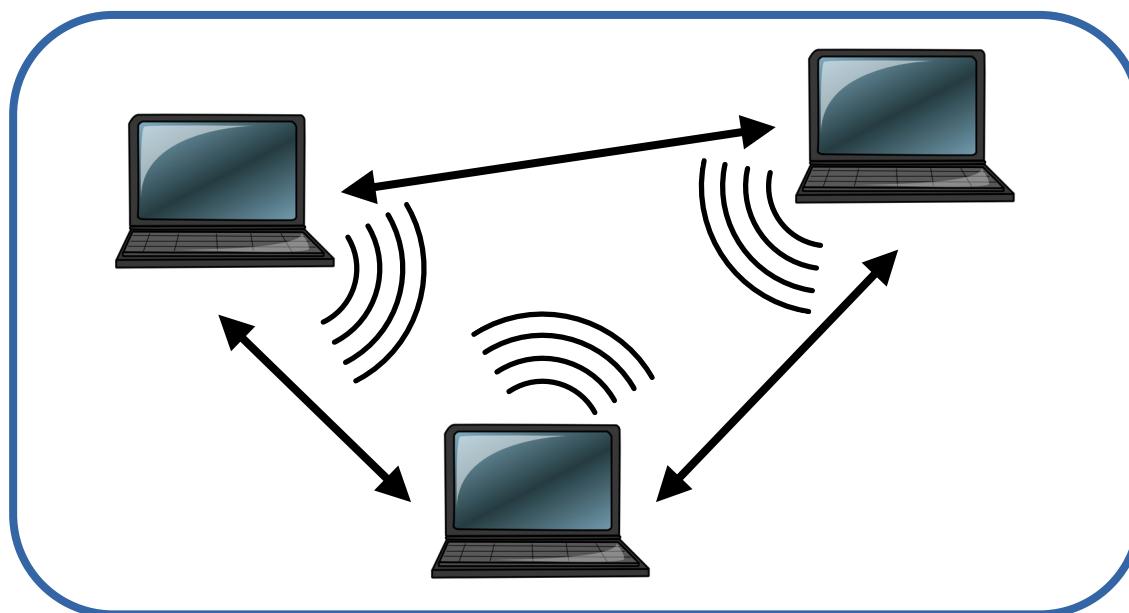


Mode « Infrastructure » - 3/3

- **ESSID / SSID (ESS Identifier)** : nom du réseau WiFi sur 32 caractères alphanumériques.
- Le réseau de distribution peut-être filaire, ou sans-fil (**WDS** = *Wireless DS*).
- Chaque AP émet une **trame balise** (ou « **beacon** ») toutes les 102,4 ms, avec ses caractéristiques (BSSID, timestamp, vitesses supportées, canal utilisé, carte d'indication de trafic, etc), et son ESSID (comportement par défaut).

Modes «Ad Hoc» ou «Mesh» - 1/2

Le principe est celui du réseau P2P : chaque machine est à la fois un AP et un client.



En **ad-hoc** : pas de routage.

En **mesh** : routage automatique (réseau maillé).

Modes «Ad Hoc» ou «Mesh» - 2/2

- Le réseau reste identifié par son **ESSID** éphémère.
- En ad-hoc, l'ensemble formé se nomme un **IBSS** (*Independant Basic Service Set*) ou ensemble de services de base indépendants.
- En réseau maillé (mesh), l'IBSS devient un **MBSS** (Mesh BSS).

Autres configurations de l'AP - 1/4

mode «Client»

- Un AP configuré dans ce mode va jouer le **rôle de simple carte WiFi**, via le câble ethernet.
- Méthodologie de configuration :
 - Au départ, on fixe les IP du poste client et de l'AP en statique, dans le même réseau, ce qui permet d'accéder à l'interface d'administration web de la borne.
 - On désactive le serveur DHCP de l'AP, et on configure la borne en tant que client WiFi en fixant le SSID auquel on veut se connecter, avec le mot de passe associé.
 - on laisse l'AP avec son IP statique en filaire, et **on bascule le poste client en DHCP**. Le poste reçoit alors son IP de la borne distante.

Autres configurations de l'AP - 2/4

mode «Pont» (bridge)

- Sert à **relier un ou plusieurs réseaux LAN filaires** via des passerelles sans fil.
- Les points d'accès partagent un **même SSID**.
- Un point d'accès configuré dans ce mode demande les **adresses MAC** des autres AP à utiliser.
- Les bornes forment ensemble un **WDS**.

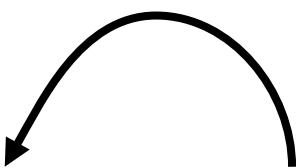
Autres configurations de l'AP - 3/4

mode «Répéteur»(repeater)

- Sert à étendre le réseau dans des zones d'ombres ou éloignées.
- La configuration utilise l'**adresse MAC de l'AP maître**. Le serveur maître reste en mode « master ».
- **Débit divisé par 2 !**
- Risque de collisions élevé car même plage de fréquence.

Autres configurations de l'AP - 4/4

résumé des différents modes

	AP [master]		Client [managed]		Ad-Hoc/Mesh [ibss/mbss] (p2p)		Bridge [wds]		Repeater		Monitor [monitor]
---	-----------------------	--	----------------------------	---	--	---	------------------------	---	-----------------	---	-----------------------------

Sécuriser son réseau – 1/4

l'authentification

- **WEP (Wired Equivalent Privacy)**, très facile à pirater (cf. logiciel aircrack-ng).
- **WPA (Wi-Fi Protected Access)**, solution transitoire conçue avant la finalisation de la norme 802.11i, et reposant sur le protocole de gestion de clés **TKIP** (Temporary Key Integrity Protocol) + le chiffrement **AES** (Advanced Encryption Standard).
- **WPA2** respecte la norme **802.11i** et **impose** le protocole de gestion de clés **CCMP** (Counter-Mode/CBC-Mac protocol) au lieu de TKIP, toujours avec le chiffrement **AES**. Faille KRACK découverte en 2017 dans le protocole, puis faille KROOK en 2020 dans les puces WPA2 d'environ 1 milliards de smartphones...
- **WPA3** introduit en 2018, mais déjà plusieurs failles découvertes (DragonBlood, etc). **Chiffrement unique par utilisateur**. Augmentation de la taille des clefs de chiffrement et des vecteurs d'initialisation.

Sécuriser son réseau – 2/4

les deux types de WPA

- **WPA Personal** (ou **WPA-PSK** pour **Pre Shared Key** en WPA/WPA2, **WPA-SAE** pour **Simultaneous Authentication of Equals** en WPA3) : conçu pour les petits réseaux sans serveurs d'authentification.
- **WPA Entreprise** (ou **WPA-802.1X** ou **WPA-EAP** pour **Extensible Authentication Protocol**) : demande un serveur **RADIUS**. Les méthodes d'authentification EAP peuvent être **TLS** (**Transport Layer Security**), **TTLS** (**Tunneled Transport Layer Security**) et **SIM** (**Subscriber Identity Module** pour la téléphonie mobile).

Sécuriser son réseau – 3/4

les possibilités « classiques »

Types de réseau	Authentification	Algorithme de chiffrement	Protocole de chiffrement des clés
<i>Open</i>	-	Aucun	-
<i>WEP</i>	WEP	RC4	-
<i>WPA Personnel</i>	PSK	AES	TKIP
<i>WPA Entreprise</i>	EAP	AES	TKIP
<i>WPA2 Personnel</i>	PSK	AES	CCMP
<i>WPA2 Entreprise</i>	EAP	AES	CCMP
<i>WPA3 Personnel</i>	SAE	AES	CCMP
<i>WPA3 Entreprise</i>	EAP	AES	GCMP

Sécuriser son réseau – 4/4

les bonnes pratiques

- **Cacher le SSID**
- **Filtrer les adresses MAC**
- **Utiliser le WPA3 avec son nouveau protocole SAE (Simultaneous Authentication of Equals) / Dragonfly (Libellule)**
- **Mettre à jour son matériel et/ou firmware !**
(donc FCC a côté de la plaque à vouloir fermer les appareils !)

Pirater son réseau

les (mauvaises) pratiques

- Méthodologie fournie à titre purement académique. Vous savez ce qui vous attend si vous l'utilisez sur un réseau qui n'est pas le vôtre...
- Utiliser **macchanger** pour changer son adresse MAC.
- Utiliser **airodump-ng** pour repérer les stations connectés à l'AP.
- Utiliser **aireplay-ng** pour envoyer une trame de déconnexion d'une station connectée, qui va alors tenter de se reconnecter automatiquement et en toute discréction, et nous permettre de capter la poignée de main WPA.
- Utiliser **aircrack-ng** avec un fichier de dictionnaire adéquat...
- Limitations : ce genre d'attaque en force brute ne marche que pour des petits mots de passe. Raison pour laquelle il est IN-DIS-PENSABLE d'utiliser des mots de passe longs (jusqu'à 63 caractères ou 64 hexa - soit 256 bits) et complexes !

Pirater son réseau

les (mauvaises) pratiques

- Temps nécessaire : moins de 5mn sur un portable actuel. Il faut juste une carte WiFi qui supporte le mode monitoring, et un AP offrant la possibilité de modifier le MDP.
- Sur VOTRE point d'accès, configurez un mot de passe court (8 caractères), puis :
 - apt install macchanger aircrack-ng
 - ip a / macchanger -Ar wlan0 / ip a
 - airmon-ng start wlan0
 - airodump-ng wlan0mon
 - airodump-ng -c X -bssid 00:11:22:33:44:55 -w /tmp/capture wlan0mon
- Attente d'un handshake client (on peut aussi provoquer une désauthentification en repérant les stations connectées avec la commande précédente sans le -w /tmp/capture, puis : aireplay-ng -0 1 -e SSID -a 00:11:22:33:44:55 -c AB:CD:EF:AB:CD:EF wlan0mon) – puis CTRL-C.
- créez un petit dictionnaire dictio.txt avec plusieurs mots de passe bidons sur chaque ligne, et votre mot de passe final (attention, la casse compte)
 - aircrack-ng /tmp/capture-01.cap -w dictio.txt

Pirater son réseau

les (mauvaises) pratiques

Conclusion en WPA / WPA2 :

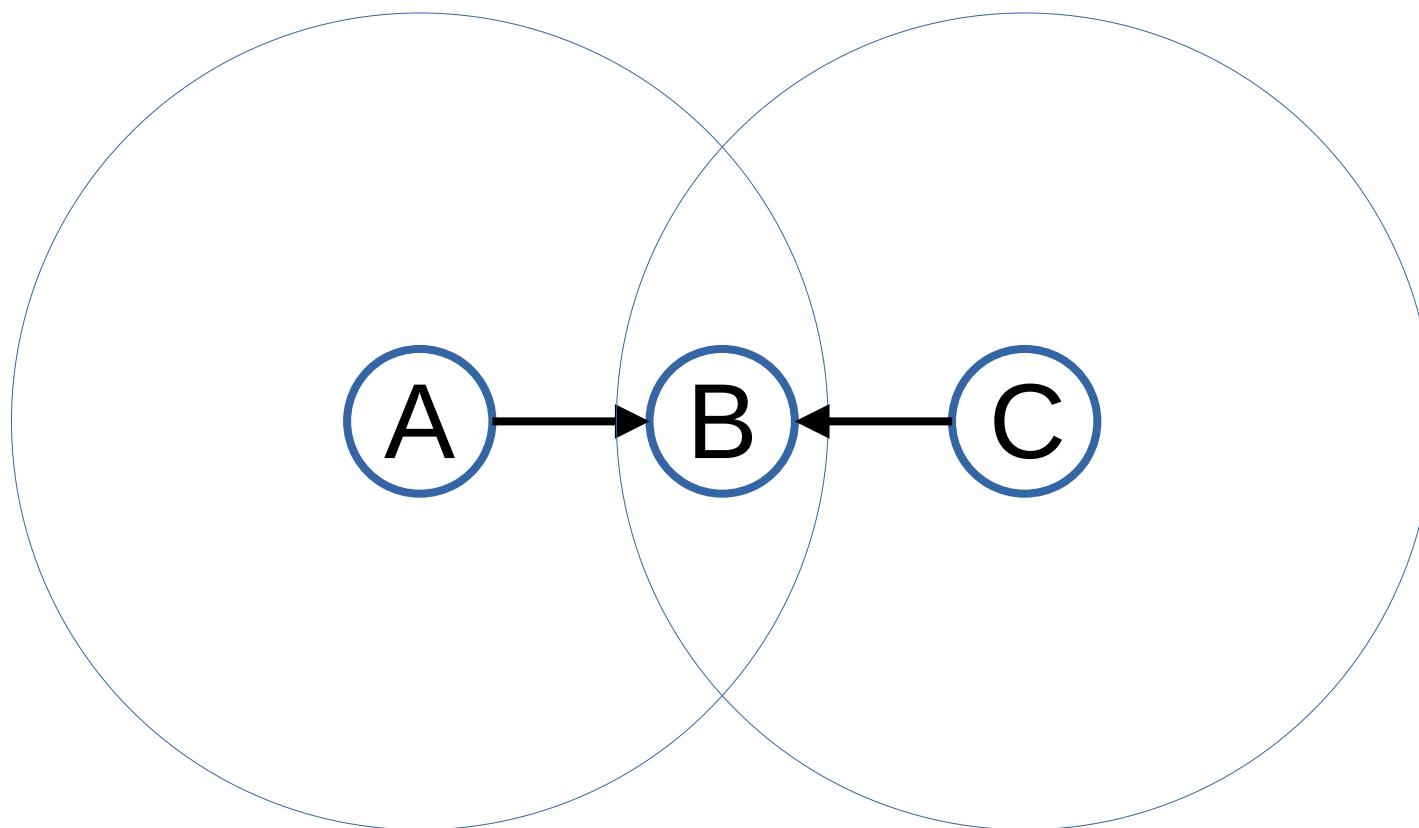
Votre sécurité ne tient toujours qu'à :

la longueur & la complexité de votre clé

la puissance de calcul du pirate

Problème des stations cachées – 1/2

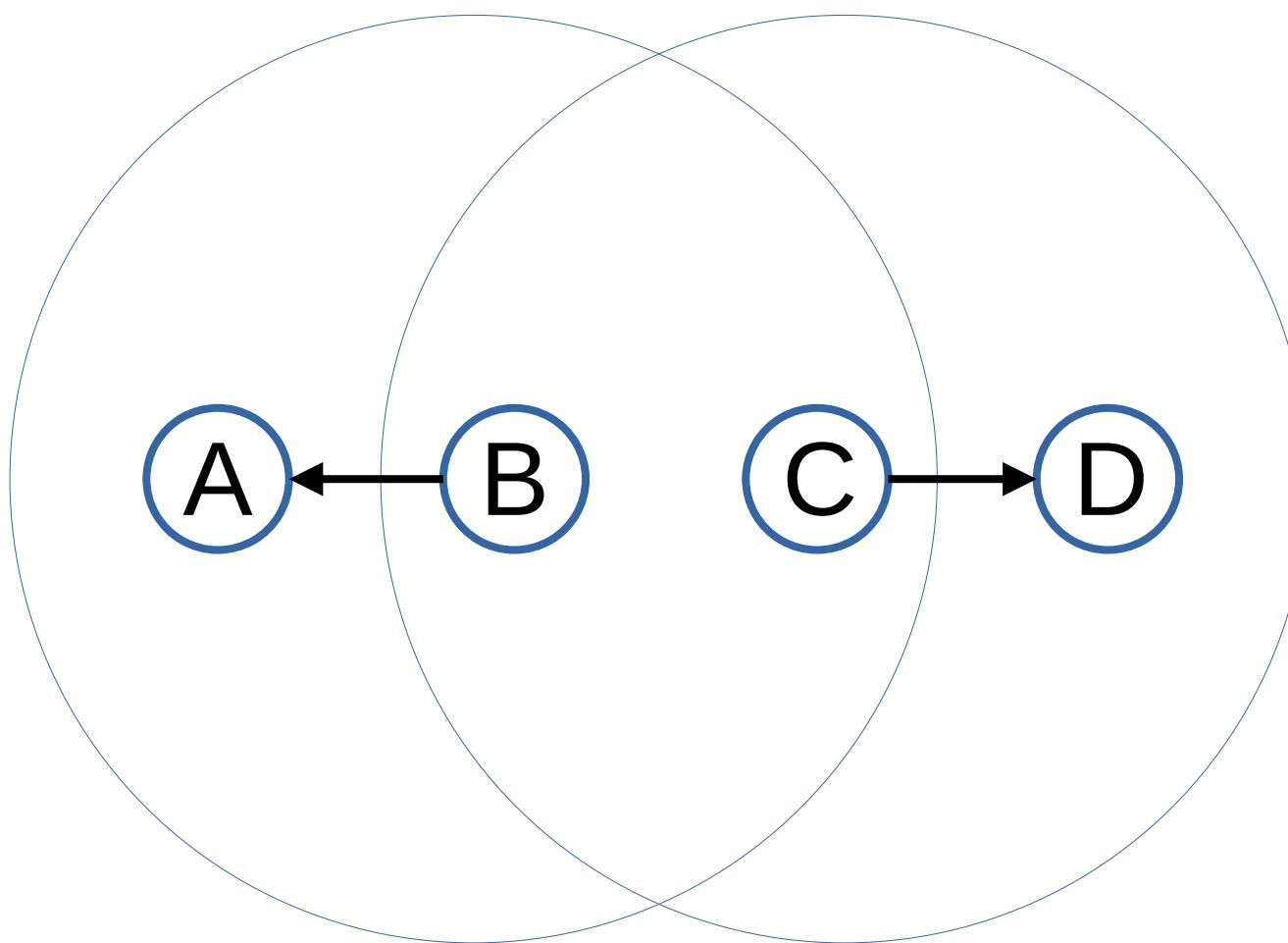
hidden stations



A et C ne se voient pas (portée limitée et / ou obstacles). Elles émettent en même temps à B → collisions !

Problème des stations exposées – 2/2

exposed stations



- B et C veulent émettre
- B émet en 1^{er}: C attend = temps perdu !

CSMA / CD – 1/2

gestion des collisions réseau en mode filaire

- **CSMA = Carrier Sense Multiple Access** ou écoute d'un support à accès multiples.
- **CD = Collision Detection**
- Utilisé par défaut dans les réseaux filaires ethernet.
- Principe : quand un silence se présente sur le support, la station est libre d'émettre ses données, mais **elle reste simultanément à l'écoute**. Si une autre station émet en même temps (collision), les deux s'arrêtent et attendent un temps aléatoire avant de retenter leur chance.
- **Demande un accès robuste en écoute.**

CSMA/CD – 2/2

les limites du sans-fil

- En sans-fil, on ne peut simultanément émettre et recevoir sur une même fréquence. Même avec deux antennes, le signal d'émission viendra « recouvrir » le signal de réception.
- Les stations trop éloignées ne se voient pas.
- Les ondes électromagnétiques subissent de nombreux phénomènes de réflexion, d'atténuation et d'absorption
- Conclusion : **l'écoute robuste du support est impossible en WiFi**. La détection de collision classique en CSMA/CD ne marche pas. On utilise donc un autre mécanisme : **l'évitemennt de collision ou CSMA/CA** (Collision Avoidance).

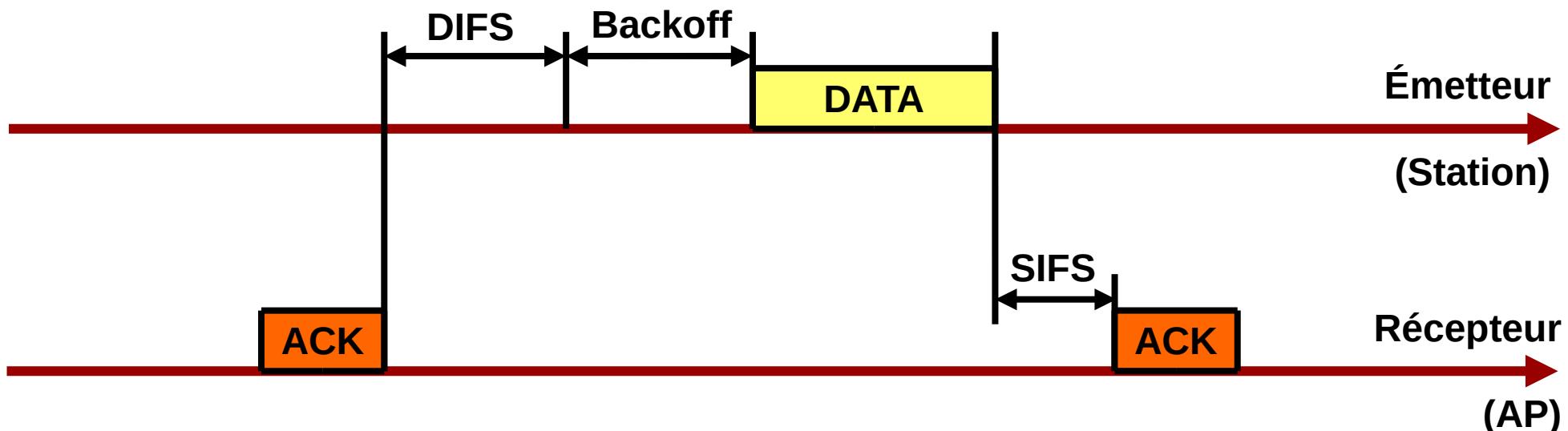
CSMA / CA – 1/10

le DIFS et le Backoff

- Comme en ethernet, les stations écoutent le support.
- Si aucune transmission n'a eu lieu auparavant, et que le **support reste libre** pendant un temps **DIFS** (Distributed Inter Frame Space = SIFS + 2 Slot Time), la station peut commencer à émettre.
- Si une transmission vient de se terminer (**ACK**), elle génère une **durée d'attente aléatoire (backoff)**, qui se rajoute au **DIFS**. Si le support est toujours libre au bout de cette durée, l'émission peut commencer.

CSMA/CA – 2/10

Emission sans RTS/CTS



- Le **SIFS** (Short Inter Frame Space) permet à l'électronique de l'appareil de traiter le signal reçu.
- Règle de base : **SIFS < DIFS**.

Slots temporels / intertrames

Time Slot / Interframe spaces

Standard	TS (μs)	SIFS (μs)	PIFS (μs)	DIFS (μs)
IEEE 802.11-1997 (FHSS)	50	28	78	128
IEEE 802.11-1997 (DSSS)	20	10	30	50
IEEE 802.11b	20	10	30	50
IEEE 802.11a	9	16	25	34
IEEE 802.11g	9 ou 20	10	19 ou 30	28 ou 50
IEEE 802.11n	9 ou 20	10	19 ou 30	28 ou 50
IEEE 802.11n (5 GHz)	9	16	9	34
IEEE 802.11ac (5 GHz)	9	16	9	28 ou 50
IEEE 802.11ax (5 GHz)		16		

CSMA / CA – 3/10

la fenêtre de contention

- $T_{\text{backoff}} = \text{Rand}[0, \text{CW}] \times T_s$ avec $\text{CW}_i = 2^k - 1$
- La fenêtre aléatoire débute à la valeur CW_{\min} et augmente après chaque collision jusqu'à CW_{\max}
- dans 802.11b : $\text{Cw}_{\min} = 31$ et $\text{CW}_{\max} = 1023$
- dans 802.11a/g : $\text{CW}_{\min} = 15$ et $\text{Cw}_{\max} = 1023$

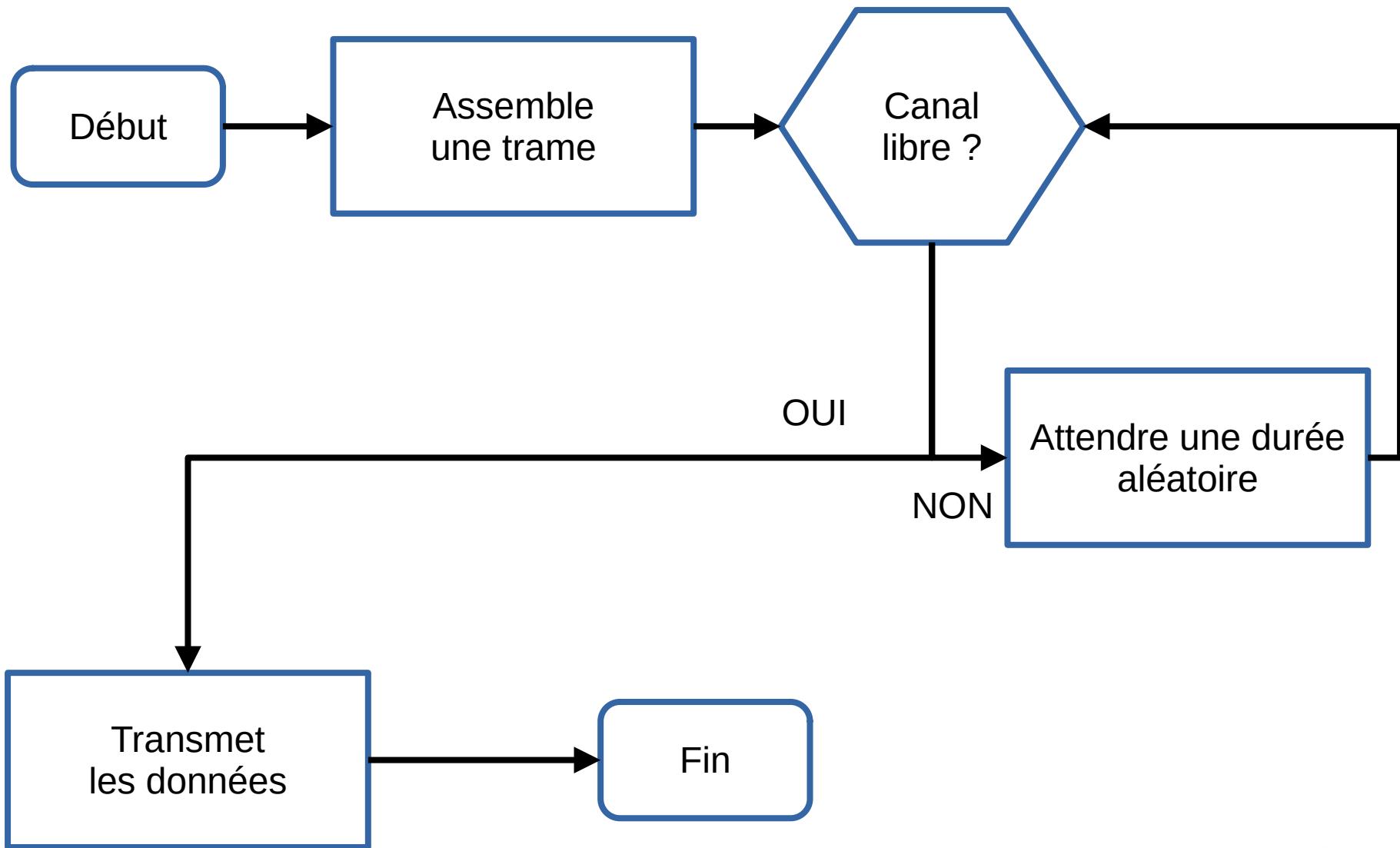
CSMA / CA – 4/10

l'évitement de collision

- Si deux stations (ou plus) ont la même durée d'attente, la collision engendre une mise à jour des compteurs respectifs, en augmentant respectivement la taille de la fenêtre de contention $CW = \min(2CW+1, CW_{\max})$.
- Exemple avec $CW_{\min}=3$ et $CW_{\max}=63$, les valeurs seront 3, 7, 15, 31, 63, 63, 63, ...
- Après plusieurs tentatives infructueuses, la trame est considérée perdue, et l'information remontée aux couches supérieures.

CSMA / CA - 4/10

schéma de base



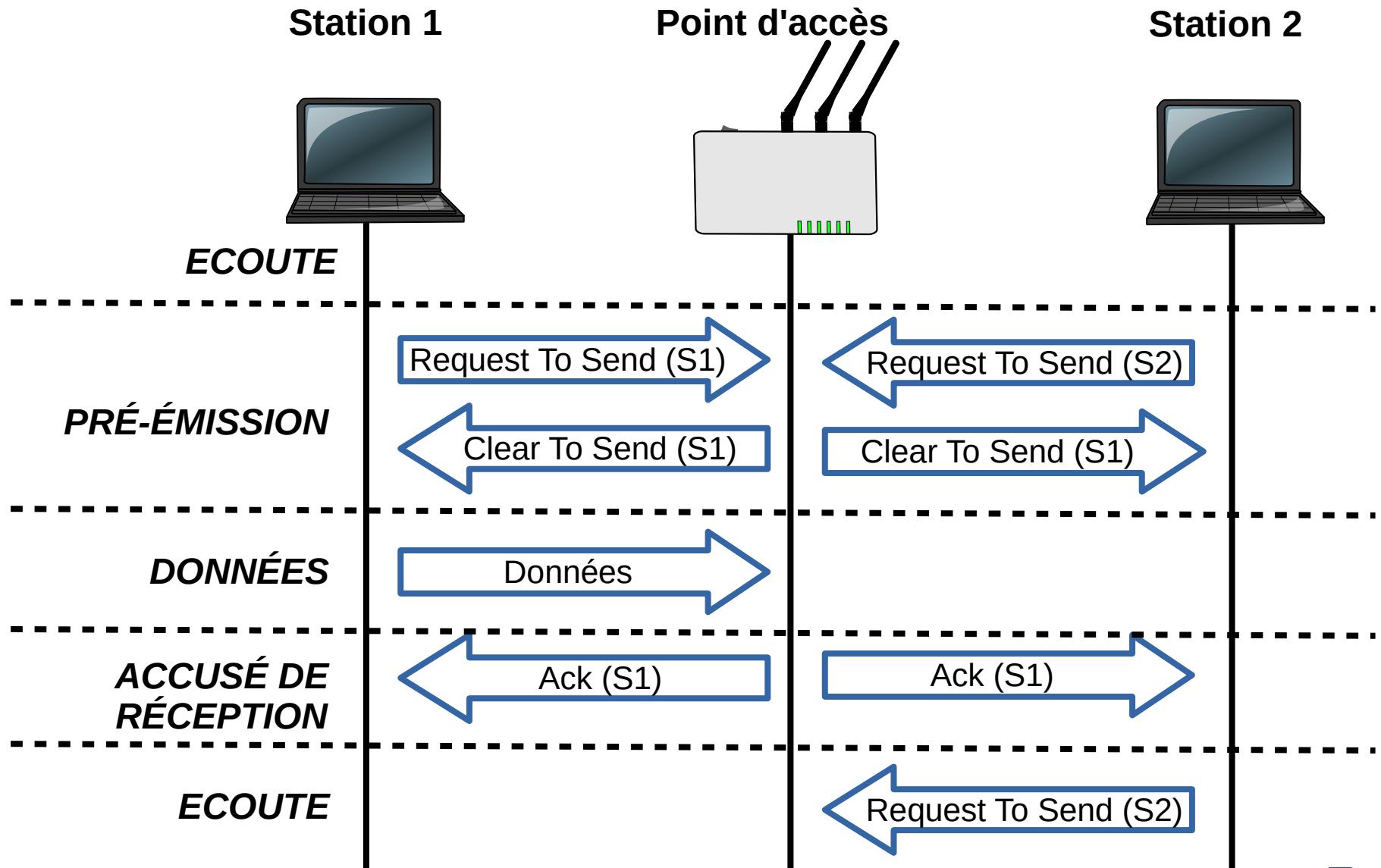
CSMA/CA – 5/10

ajout du mécanisme RTS/CTS

- Ce mécanisme **optionnel** permet de régler en partie les problèmes des stations cachées ou exposées.
- Deux stations, qui ne se voient pas, veulent envoyer des données : elles émettent simultanément un **RTS** (Request To Send) vers l'AP.
- L'AP en choisit une, et renvoie un **CTS** (Clear To Send) indiquant sa préférence. Toutes les stations recevant le CTS se mettent en attente.

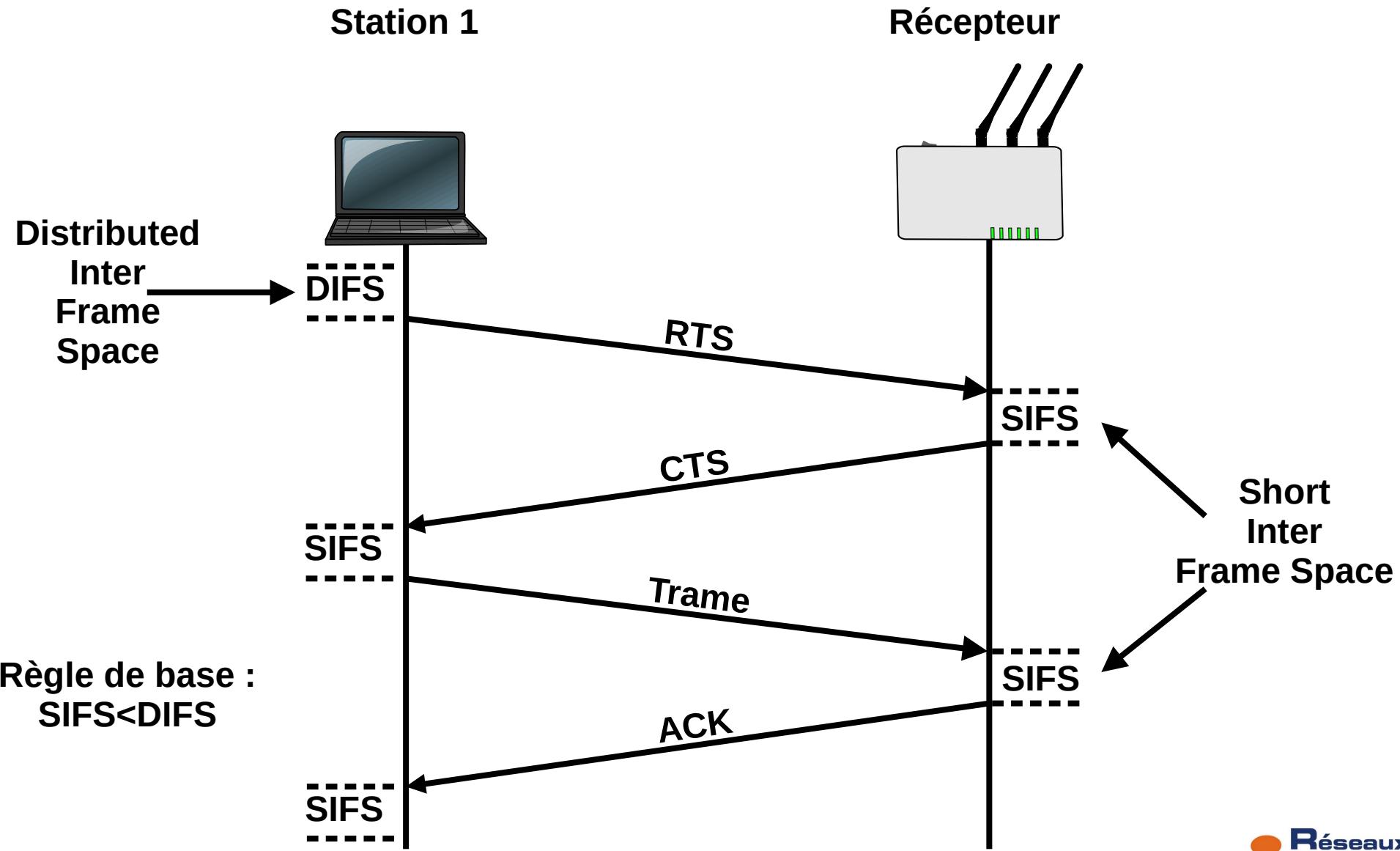
CSMA/CA – 6/10

RTS/CTS avec 2 stations + 1 AP



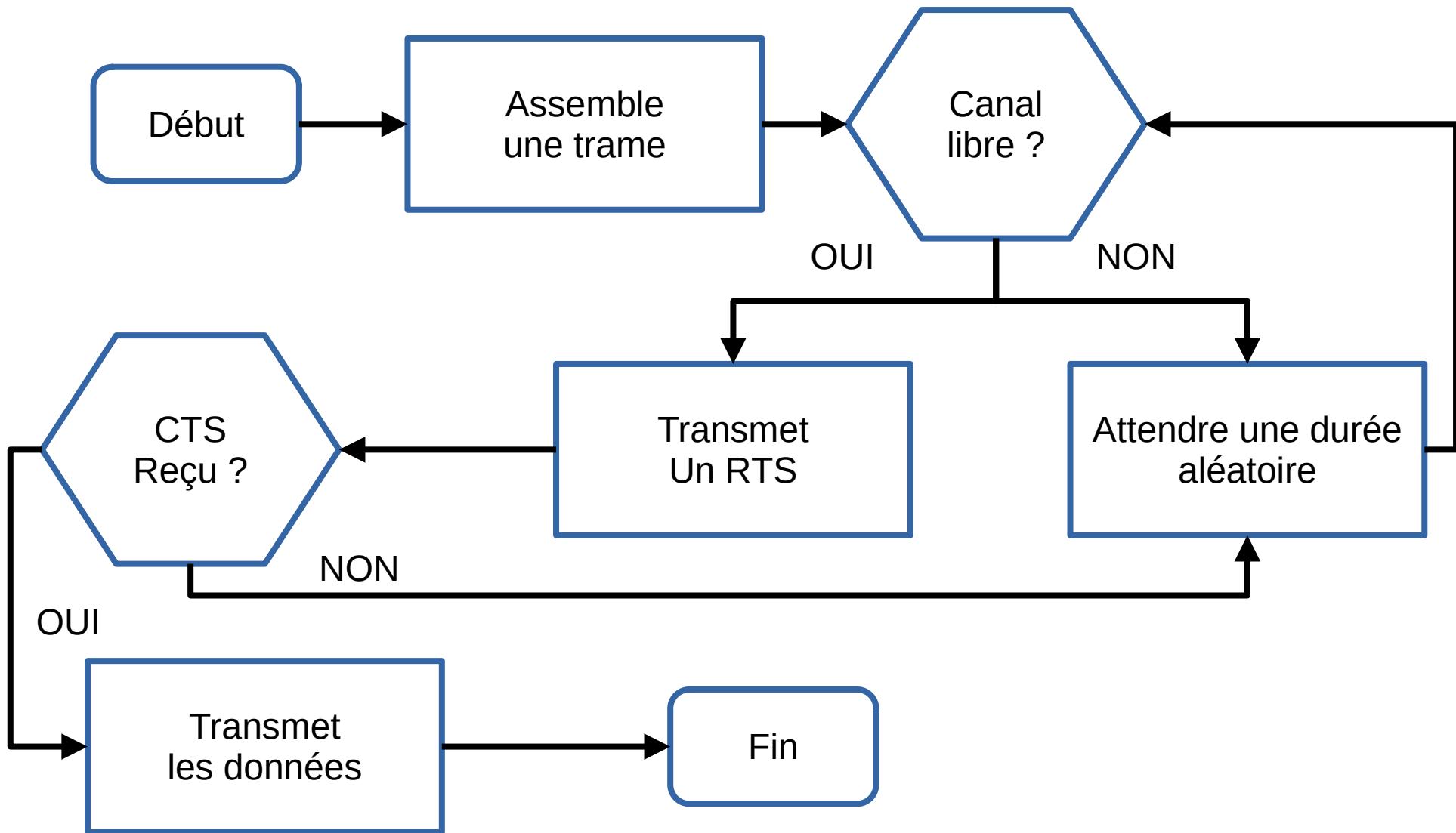
CSMA/CA – 7/10

RTS/CTS avec une station + 1 AP



CSMA/CA – 8/10

avec RTS/CTS



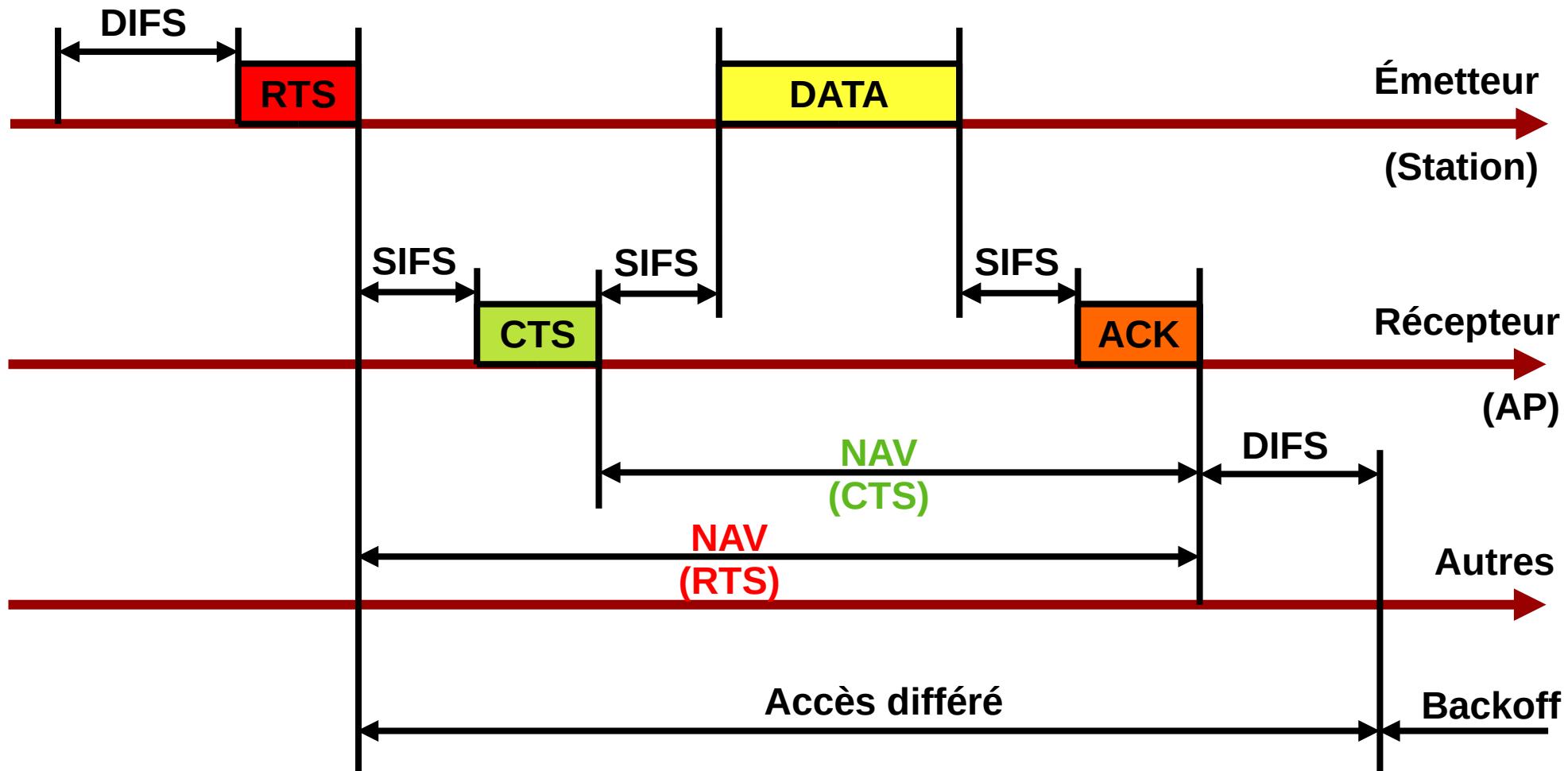
CSMA / CA – 9/10

l'évitement de collision

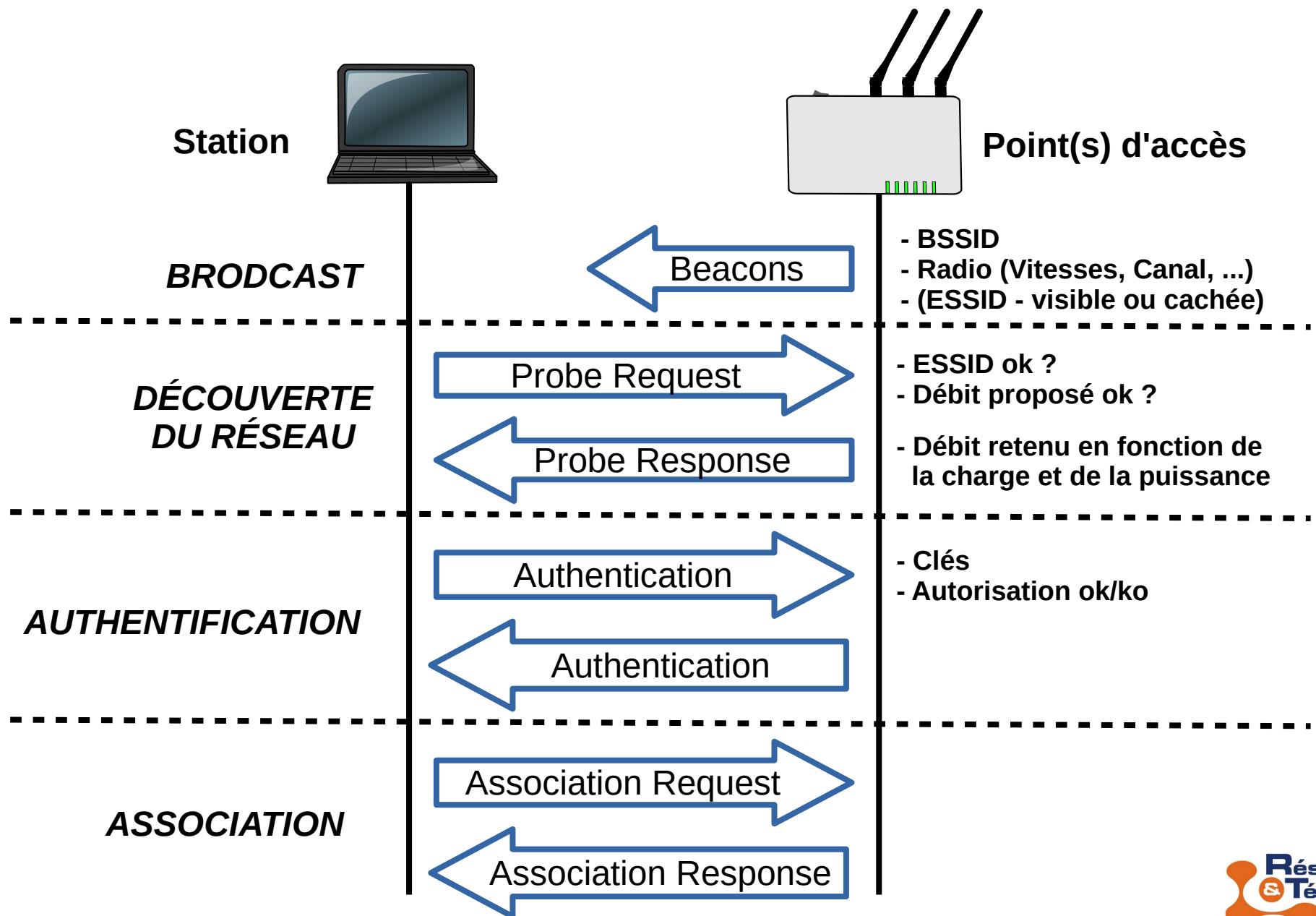
- Les stations se mettent également en pause en fonction du trafic perçu !
- Exemple : lors d'un transfert de données, les en-têtes de trames contiennent une durée, sur 2 octets, qui permet le calcul du vecteur d'allocation réseau ou **NAV** (Network Allocation Vector), lequel neutralise temporairement l'émission des autres stations.

CSMA/CA – 10/10

le NAV neutralise les autres stations



Association à un AP – 1/4 fonctionnement de base

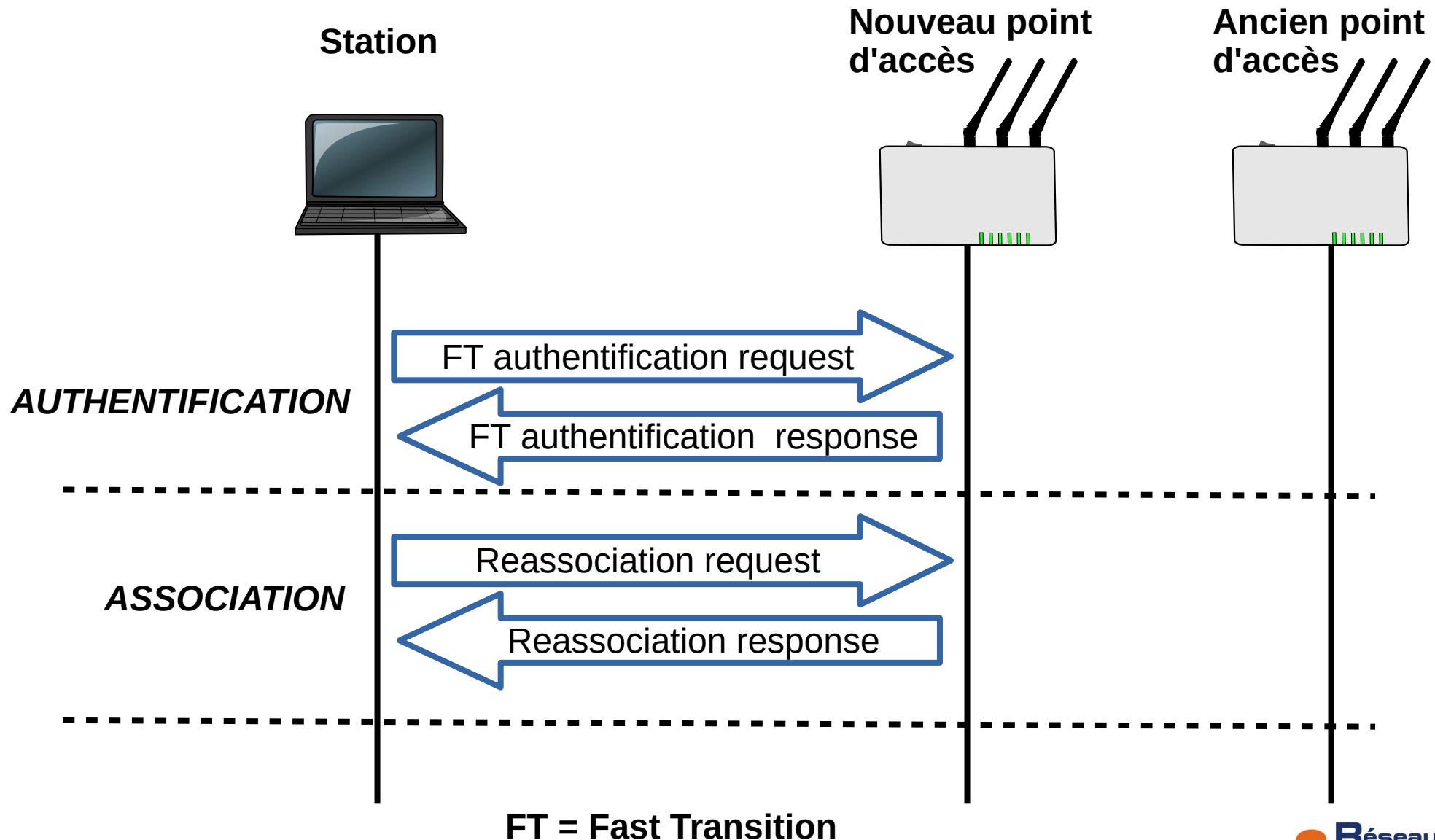


Association à un AP – 2/4 avec 802.1x / mode itinérant 802.11r

- Dans le cas où 802.1x est activé, l'association est suivie de 4 trames **EAPol** (Extended Authentication Protocol over Lan)
- Le passage d'une borne à une autre en mode itinérant (802.11r) se fait à l'initiative du client suivant deux modes : le mode **Over the air** où le client s'associe directement avec le nouveau point d'accès sans prévenir l'ancien, et en mode **Over the DS**, où l'ancien point d'accès va envoyer des informations de pré-authentification à la nouvelle borne, via le DS, pour accélérer la transition.

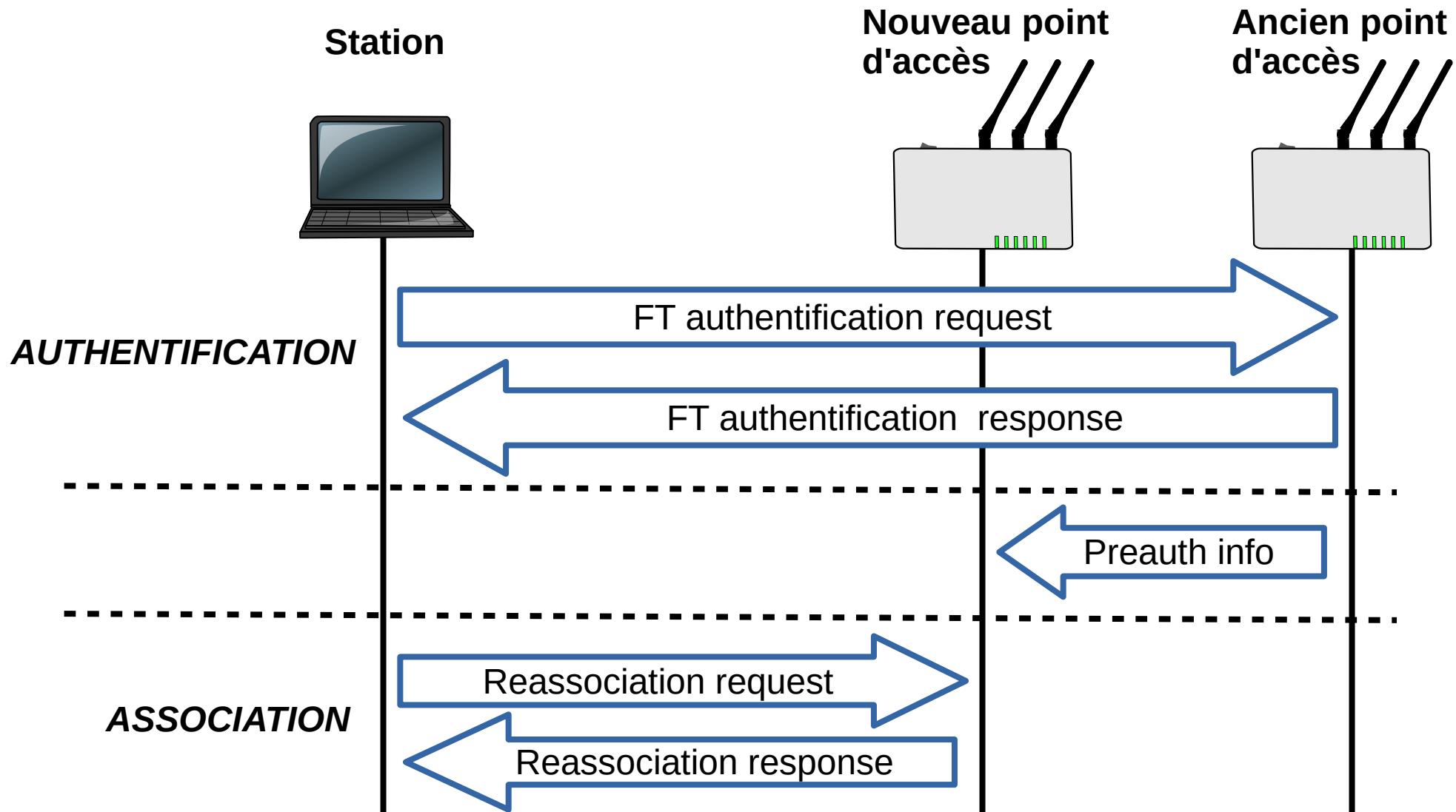
Association à un AP – 3/4

802.11r / Over the air



Association à un AP – 4/4

802.11r / Over the DS



Trames WiFi 802.11

3 différents types

- Les trames de **données**
- Les trames de **contrôle** :
 - RTS, CTS, ACK, ...
- Les trames de **gestion** :
 - association,
 - authentification,
 - ...

La transmission hertzienne

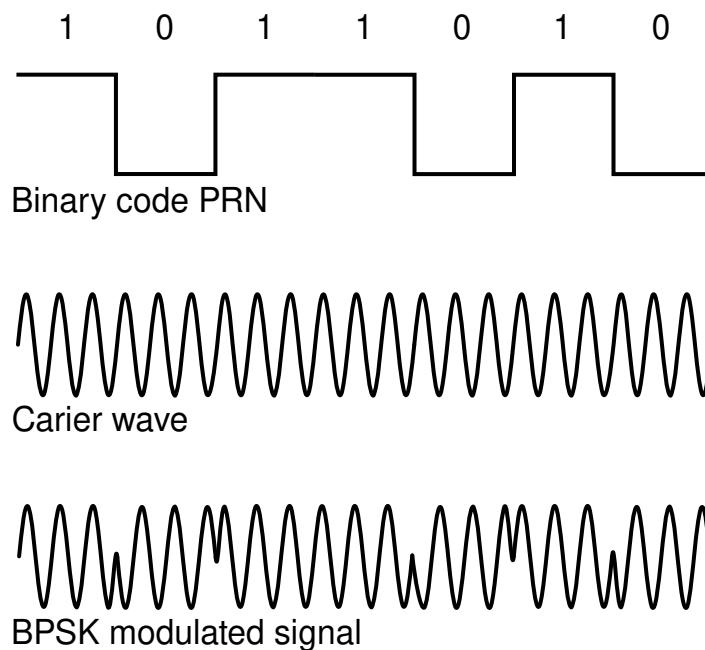
rappels

- La transmission par radio-fréquences utilise toujours des **signaux sinusoïdaux**.
- On joue sur 3 paramètres :
 - l'**amplitude**
 - la **fréquence**
 - la **phase**
- On transforme le signal binaire en signal analogique côté émission (CNA), et on réalise l'opération inverse côté réception (CAN).

Binary Phase Key Shifting (BPSK)

modulation par changement de phase

- La porteuse, de fréquence f constante, émule le 0 et le 1 logique en décalant la phase de 180° .
- Très robuste, mais **1 bit/signal** (faible débit).



http://commons.wikimedia.org/wiki/File:Phase_modulation_BPSK_GPS.svg – Auteur : Enemy

Binary Phase Key Shifting (BPSK)

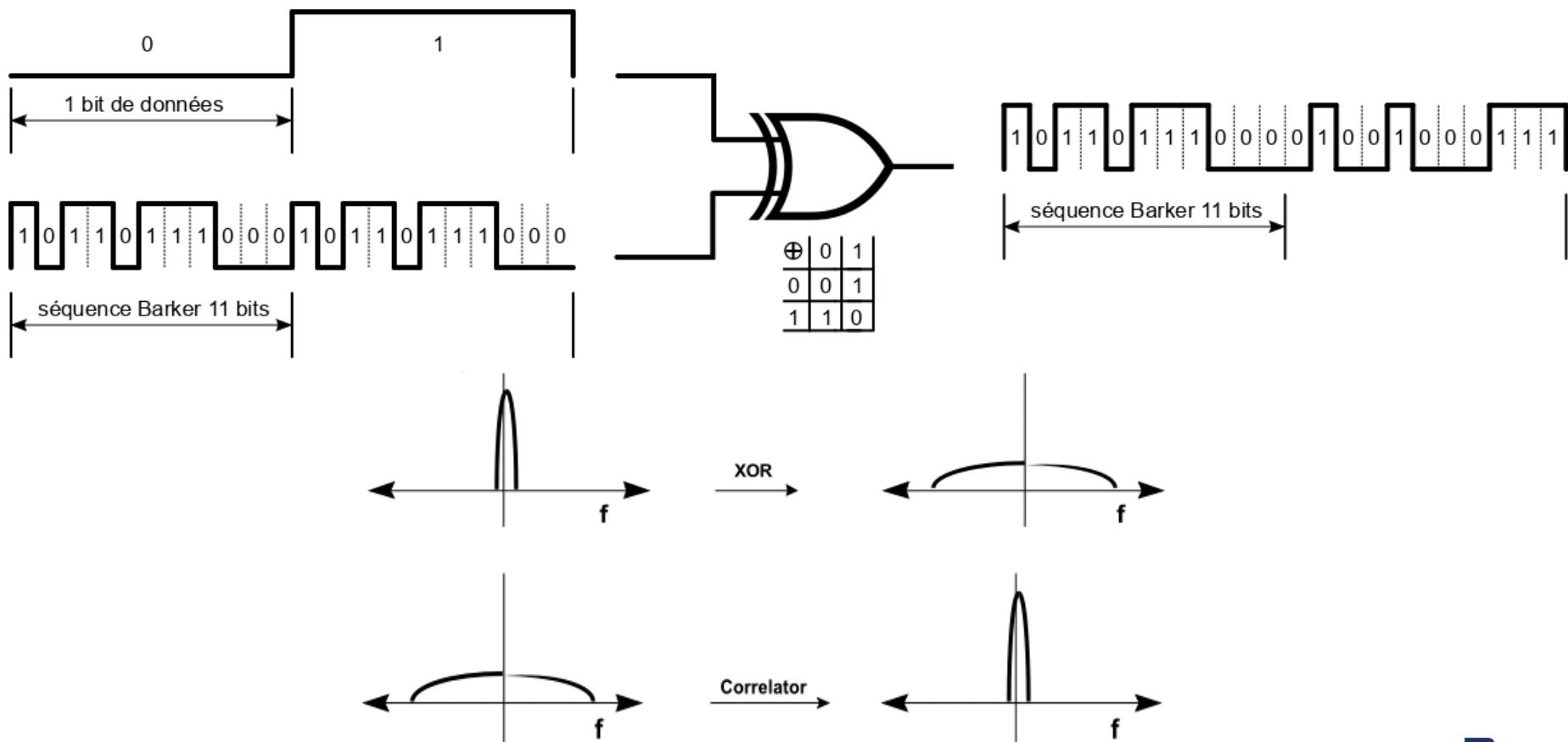
modulation par changement de phase

- Deux problèmes :
 - Tant qu'il n'y pas de changement $0 \rightarrow 1$ ou $1 \rightarrow 0$, on ne sait pas ce qui est transmis...
 - On travaille sur une fréquence unique, qui peut être occupée.
- Solution :
 - introduire des séquences pseudo-aléatoires qui vont « étaler » le spectre
 - le 0 sera codé via une suite de bits et le 1 via les bits complémentaires. Un algorithme viendra corriger les erreurs de transmission (jusqu'à un certain point).

Encodage « Code Barker »

802.11b - jusqu'à 2 Mbit/s

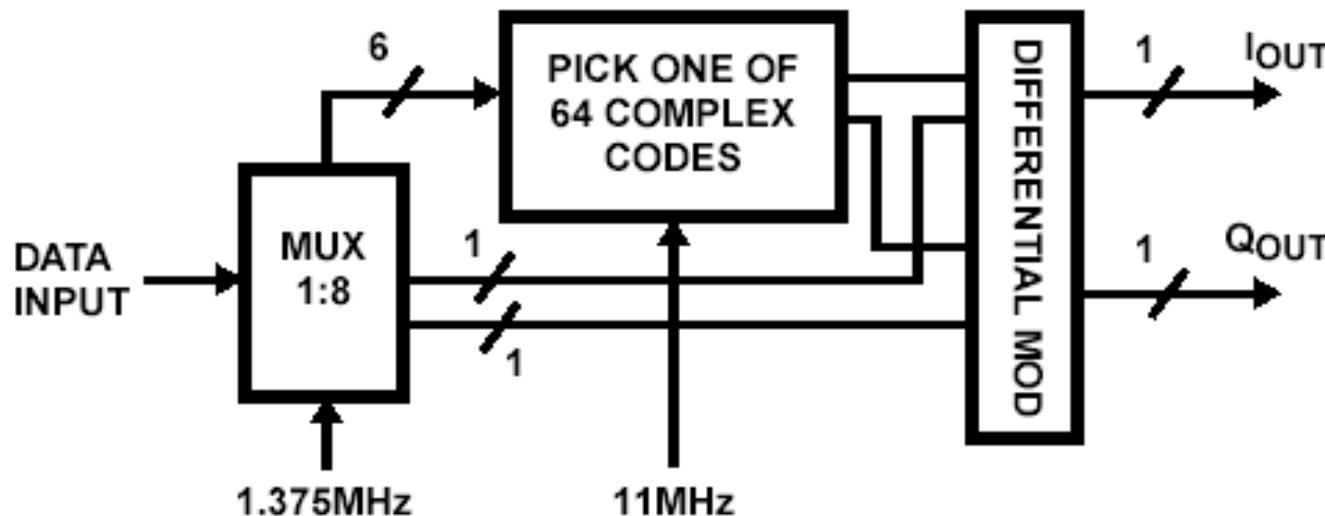
- Exemple d'une séquence Barker sur 11 bits utilisée en 802.11b : on transforme le 0 logique en 10110111000, et le 1 logique en son complément 01001000111.



Encodage CCK

Complementary code keying
802.11b – 5,5 ou 11 Mbit/s

- Utilise un algorithme de codage complexe, moins « gourmand » que le code Barker (4 bits par symbole en 5,5 Mbit/s et 8 bits en 11 Mbit/s au lieu de 11).



Étalement de spectre à séquence directe

« DSSS = Direct Sequence Spread Spectrum »

- Côté émetteur, le signal binaire A est multiplié par une séquence pseudo-aléatoire B, appelée « chipping sequence », de plus haute fréquence, via un OU exclusif.
- Le récepteur utilise la même séquence binaire B avec un OU exclusif sur le signal reçu pour reconstituer le signal d'origine.
- Plus la séquence est longue, plus le spectre est étalé autour de la porteuse.
- Peut corriger des bits erronés.

Code Division Multiple Access ou CDMA

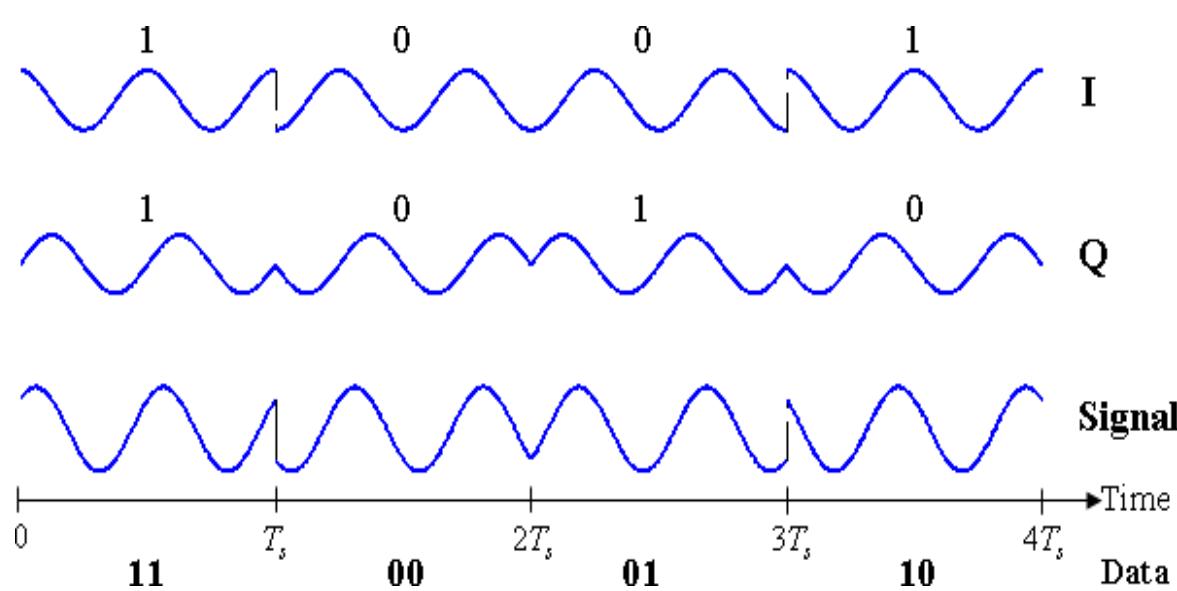
accès multiple par répartition en code

- L'idée est de reprendre le principe de l'étalement de spectre du **DSSS** (étalement de spectre) en imposant un signal binaire B répétitif et **différent pour chaque utilisateur**.
- Chaque client peut ainsi **reconnaître ses propres données dans un canal partagé**.
- Permet d'envoyer un **flux en broadcast** à plusieurs usagers (multiplexage).

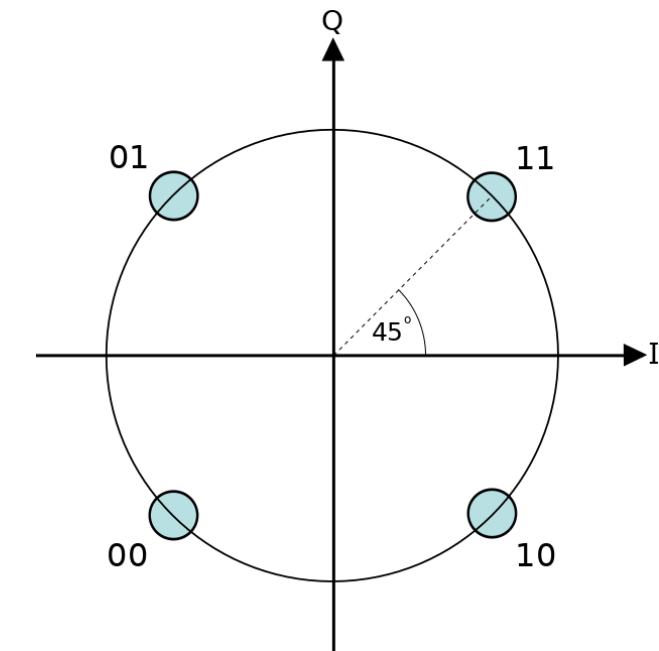
Quadrature Phase Shift Keying (QPSK)

modulation par changement de phase en quadrature

- Même principe que le BPSK mais cette fois, on utilise **2 porteuses**, et on joue sur **2 bits**, avec des déphasages de 90° .



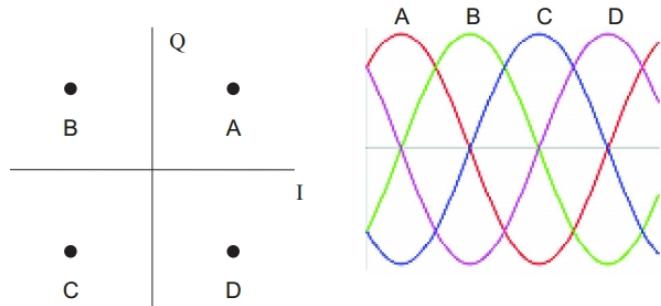
http://commons.wikimedia.org/wiki/File:QPSK_timing_diagram.png – Auteur : Splash – CC BY-SA 3.0



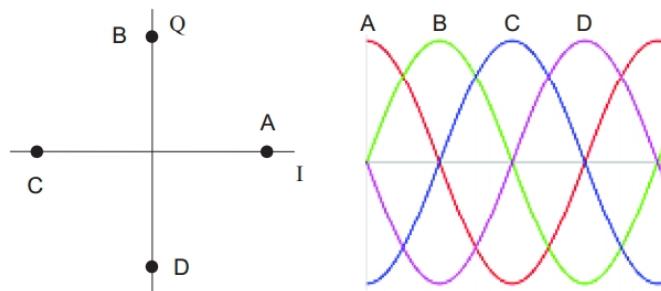
Quadrature Phase Shift Keying (QPSK)

modulation par changement de phase en quadrature

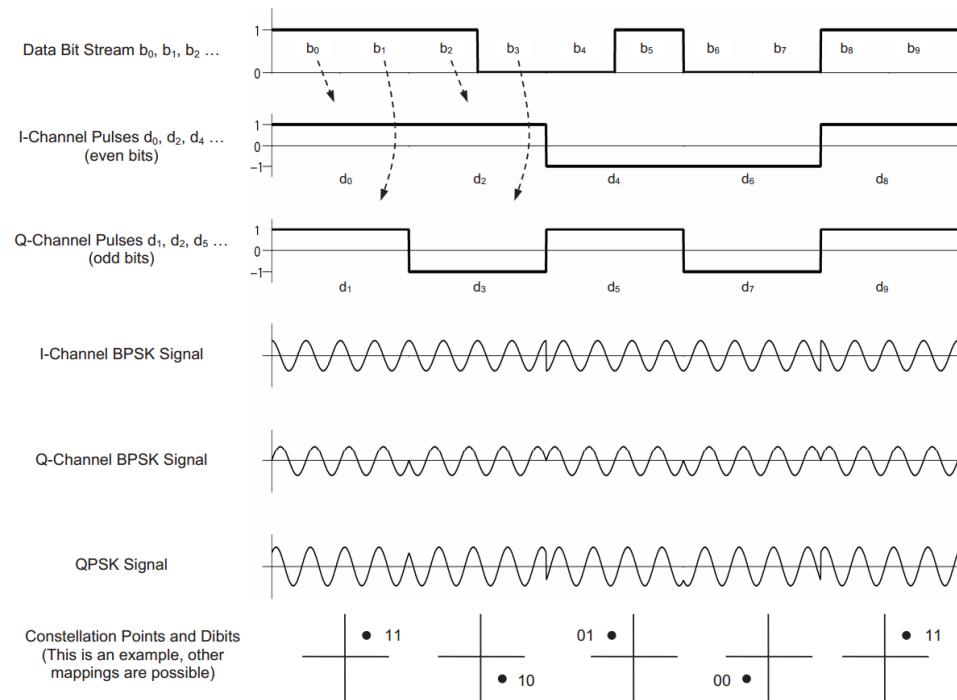
- Variantes QPSK – exemple avec $\varphi=0$



a) QPSK ($\varphi = \pi/4, 3\pi/4, 5\pi/4, 7\pi/4$)



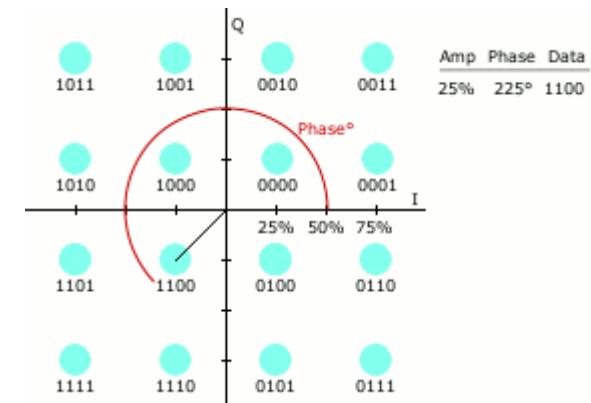
b) QPSK ($\varphi = 0, \pi/2, \pi, 3\pi/2$)



Quadrature Amplitude Modulation (QAM)

modulation d'amplitude en quadrature

- Toujours **deux porteuses et un décalage de phase**, auquel on ajoute un **décalage en amplitude**.
 - **16 QAM / 4x4 : 4 bits / symbole (2^4)**
 - **64 QAM / 8x8 : 6 bits / symbole (2^6)**
 - **256 QAM / 16x16 : 8 bits / symbole (2^8)**
 - **512 QAM : 9 bits / symbole (2^9)**
 - **1024 QAM / 32x32 : 10 bits / symbole (2^{10})**
 - **4096 QAM / 64x64 : 12 bits / symbole (2^{12})**



http://commons.wikimedia.org/wiki/File:QAM16_Demonstration.gif - Auteur : Chris Watts (CC-BY-SA-3.0)

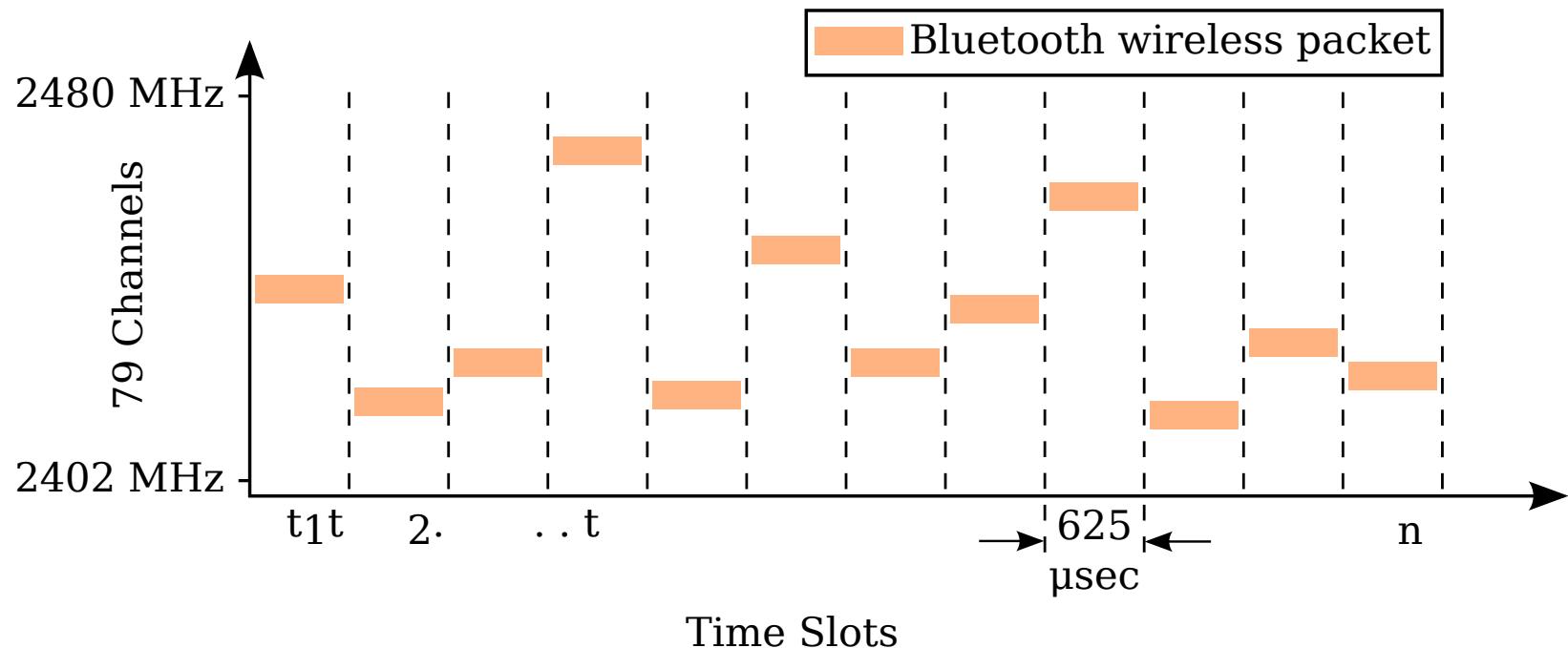
- Problème : le bruit augmente avec la taille de la « constellation » utilisée. Il faut donc constamment trouver le bon compromis entre vitesse et qualité...

La modulation FHSS (Bluetooth)

« Frequency-Hopping Spread Spectrum »
étalement de spectre par évolution de fréquence

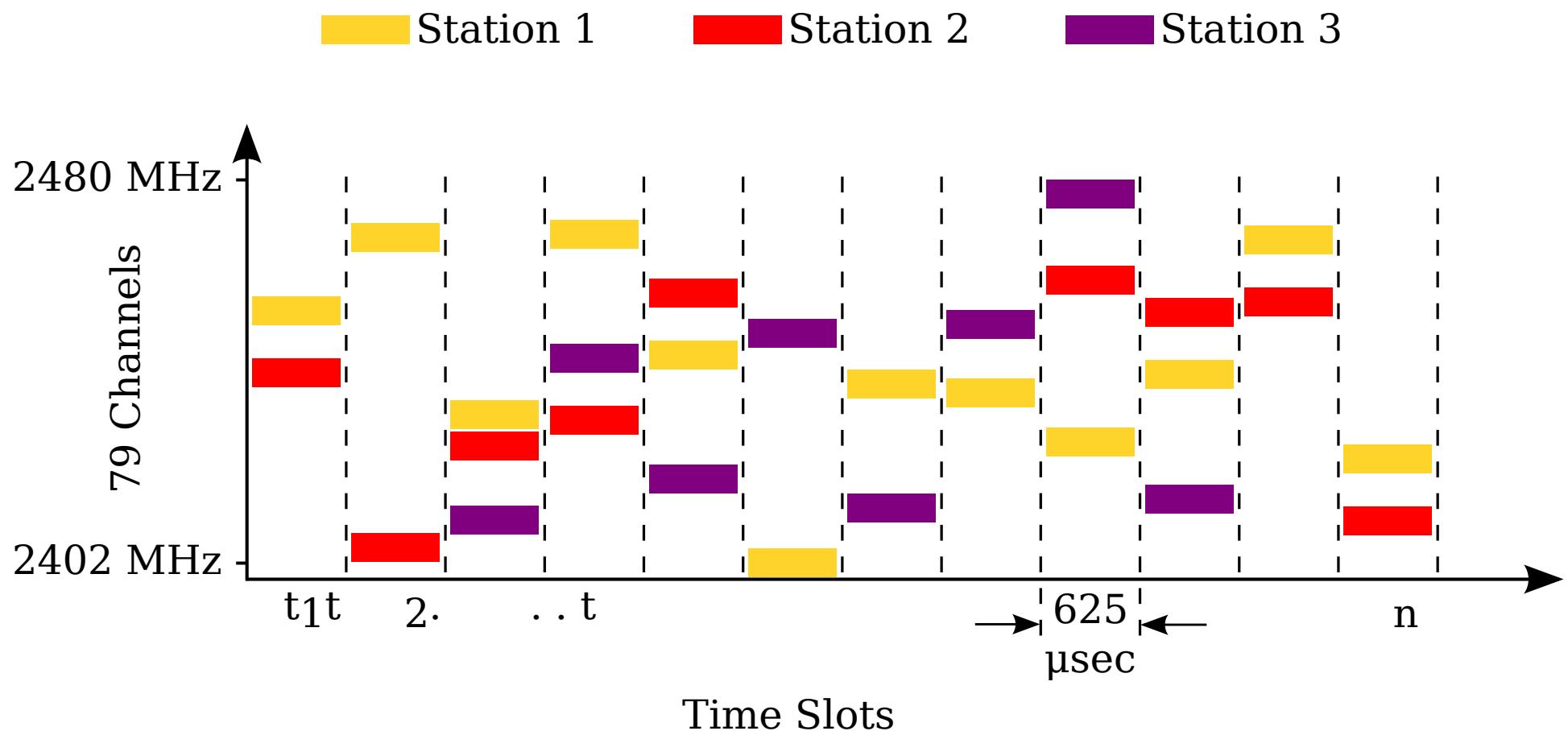
- L'émetteur **change constamment la fréquence de la porteuse du signal.**
- Le récepteur doit être à l'écoute des bonnes fréquences au bon moment.
- Au départ conçu par l'armée pour brouiller la transmission des signaux (très résistant aux interférences). Aujourd'hui désuet en WiFi, mais **toujours utilisé en Bluetooth.**
- Permet d'utiliser efficacement la bande passante avec d'autres types de transmission.

La modulation FHSS (Bluetooth)



Source : A STUDY OF BLUETOOTH FREQUENCY HOPPING SEQUENCE: MODELING AND
A PRACTICAL ATTACK – Thesis By WAHHAB ALBAZRQAOE

La modulation FHSS (Bluetooth)

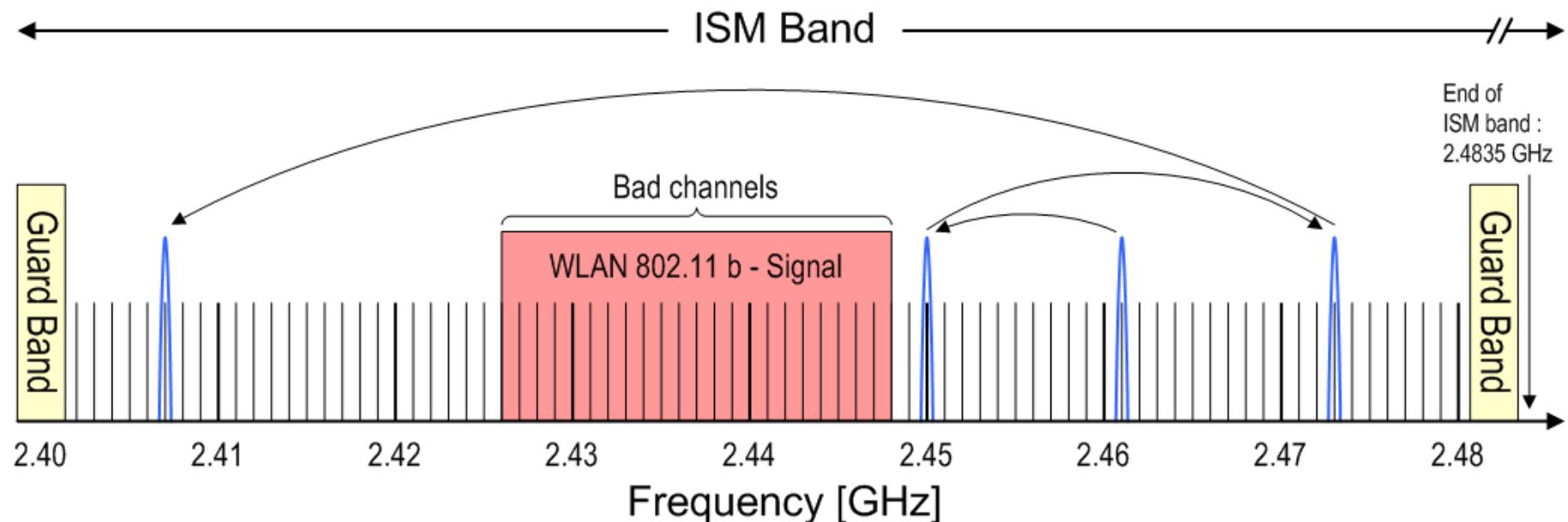


La modulation FHSS

(Bluetooth)

- 79 canaux de 1 MHz
- $f_c = 2402 \text{ MHz} + k \cdot 1\text{MHz}$; $k = 0, 1, \dots, 78$
- 1600 slots de $625 \mu\text{s}$ / canal
- En BT 4.2, on en était à 12 séquences distinctes de sauts de fréquences, non optimisés pour la QoS
- Depuis BT 5.0, les séquences de saut sont pseudo-aléatoires et peuvent être beaucoup plus larges, afin d'éviter les interférences avec les canaux WiFi occupés.

Exemple de collision entre WiFi/OFDM et BT (seulement en bande ISM)



Source : Rohde & schwartz – Bluetooth Adaptive Frequency Hopping on a R&S CMW

- L'idée est d'éviter les mauvais canaux (bad channels) jusqu'à ce qu'ils soient libérés côté WiFi.

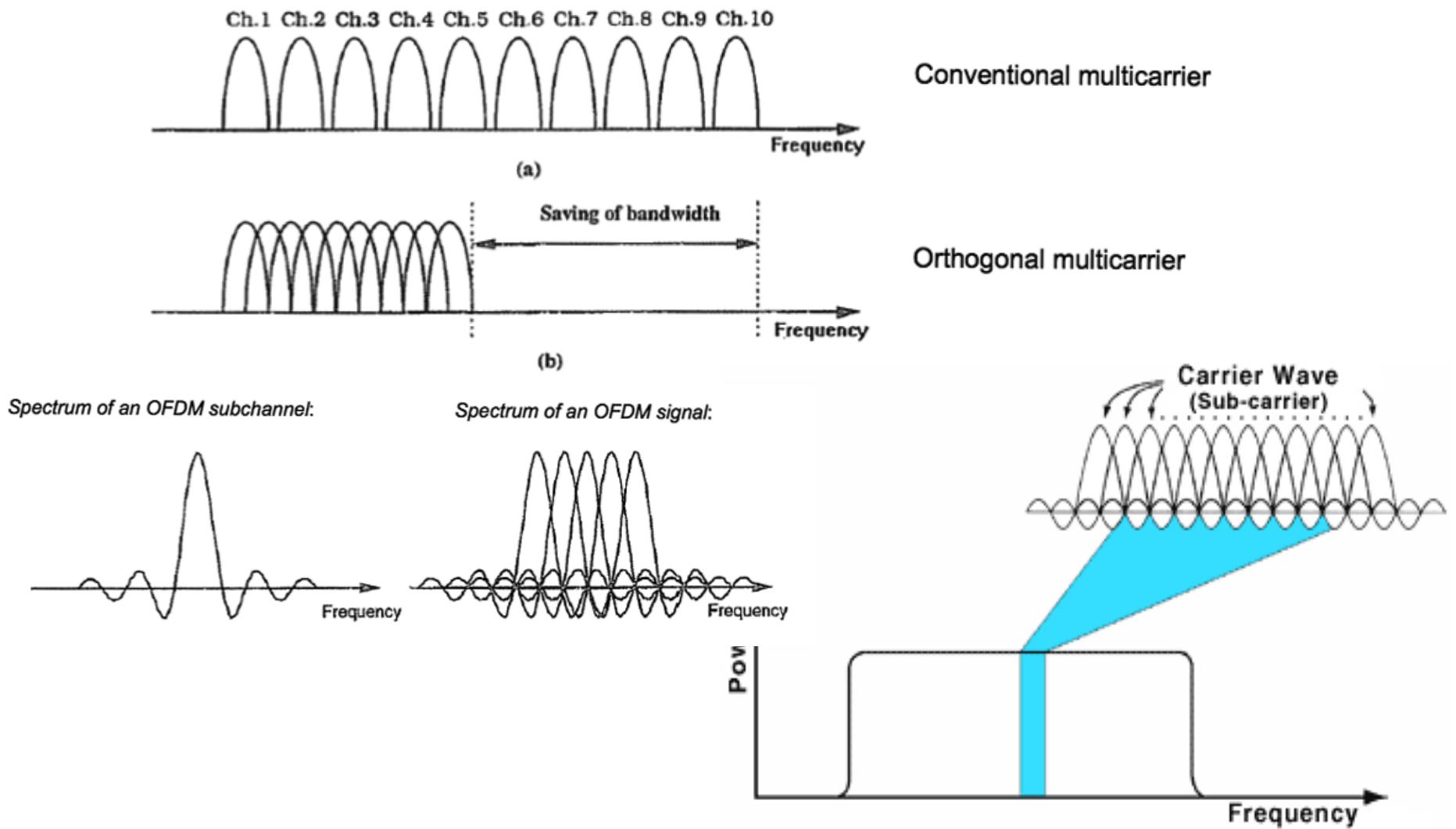
La modulation OFDM – 1/4

« Orthogonal Frequency Division Multiplexing »
(multiplexage par division fréquentielle orthogonale)

- On joue sur un grand nombre de **sous-porteuses orthogonales** pour transmettre les données numériques.
- Les sous-porteuses se recouvrent partiellement, mais grâce au décalage des phases (orthogonalité), on évite les effets d'interférences.
- Le multiplexage du signal sur plusieurs canaux permet de **baisser le bitrate** (vitesse d'émission) et d'éviter **les « échos »** (retards suite à un trajet différent de l'onde).

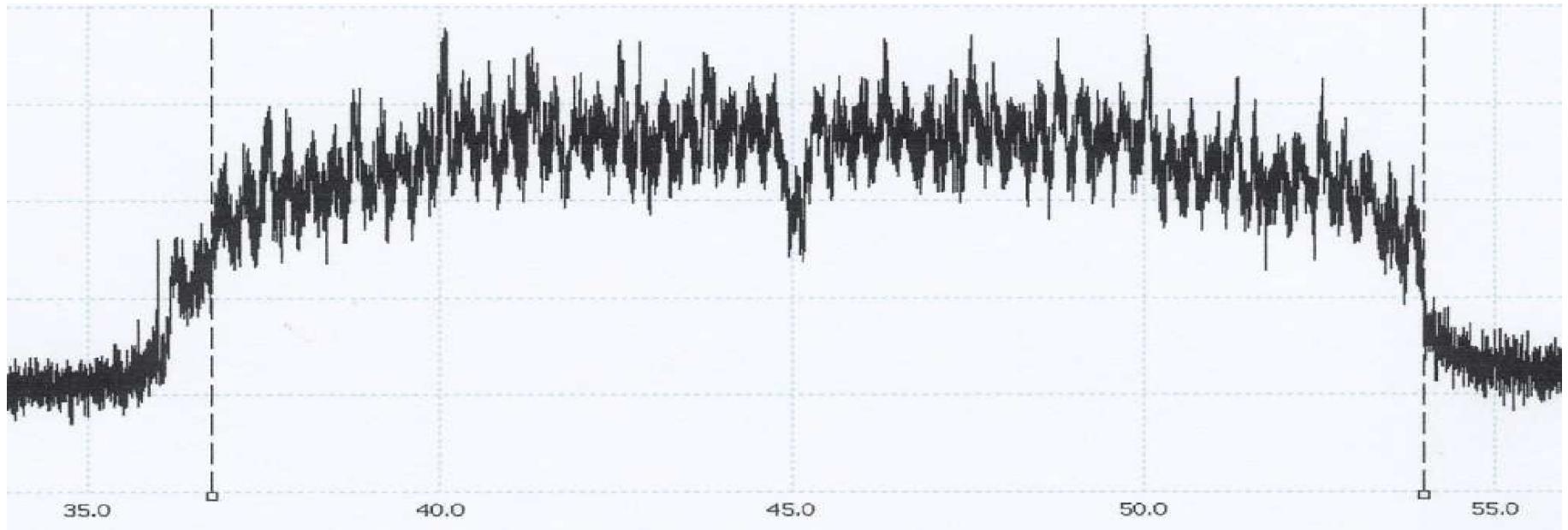
La modulation OFDM – 2/4

Orthogonal Frequency Division Multiplexing



La modulation OFDM 3/4

Spectre d'une transmission sur un canal 20 MHz en mode g/n



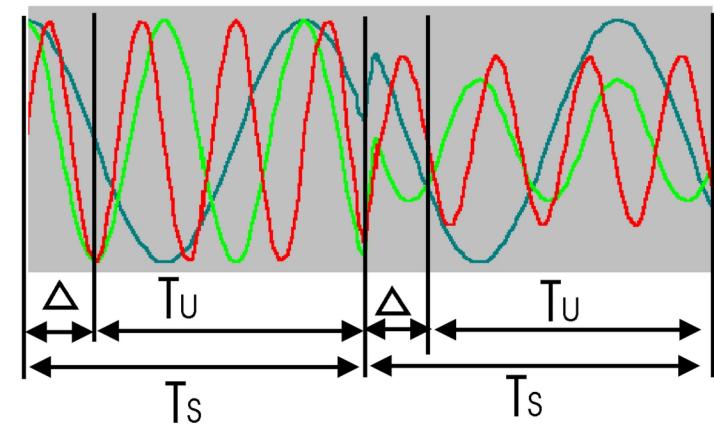
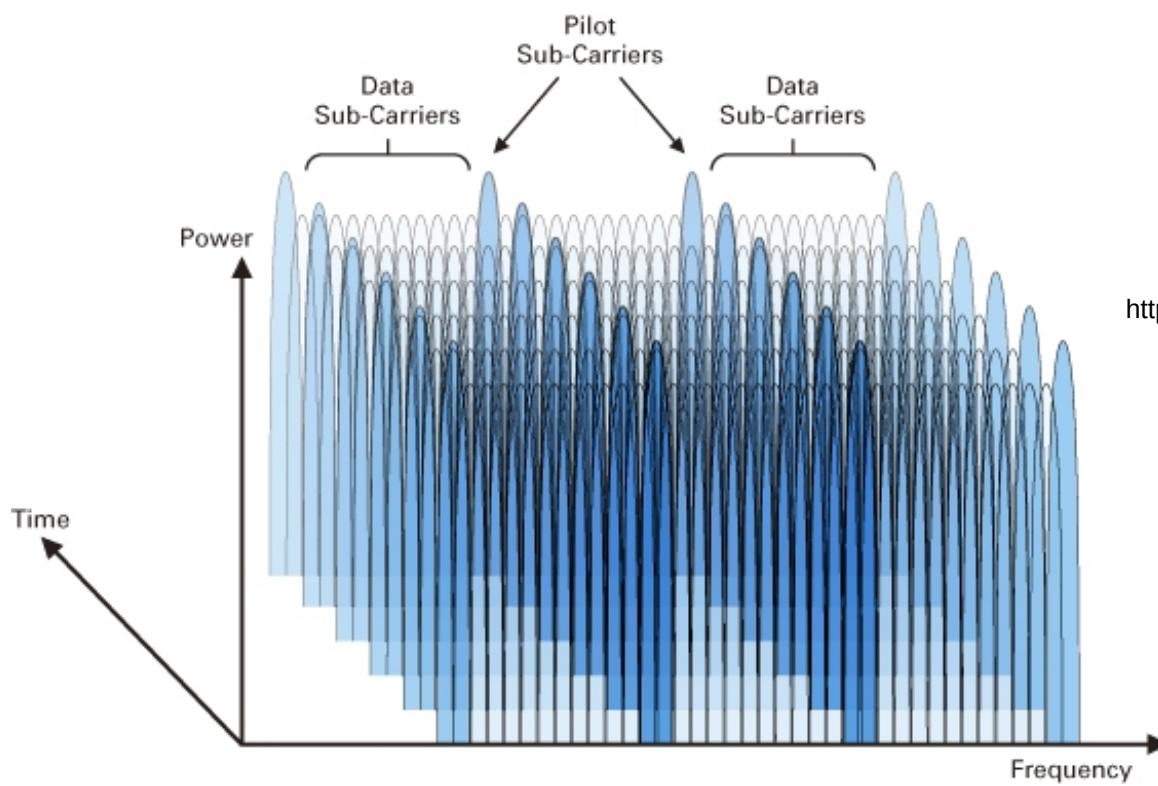
Spectre de 16,25 MHz (plage d'une sous-porteuse) d'une transmission OFDM
Avec les 52 sous-porteuses actives ; espacées de 312,5 KHz

Source : Le WIFI alias WLAN en OFDM sur 2.4 GHz.

Par Kurt Ritter he9dyy Rev.mai 2014

La modulation OFDM – 3/3

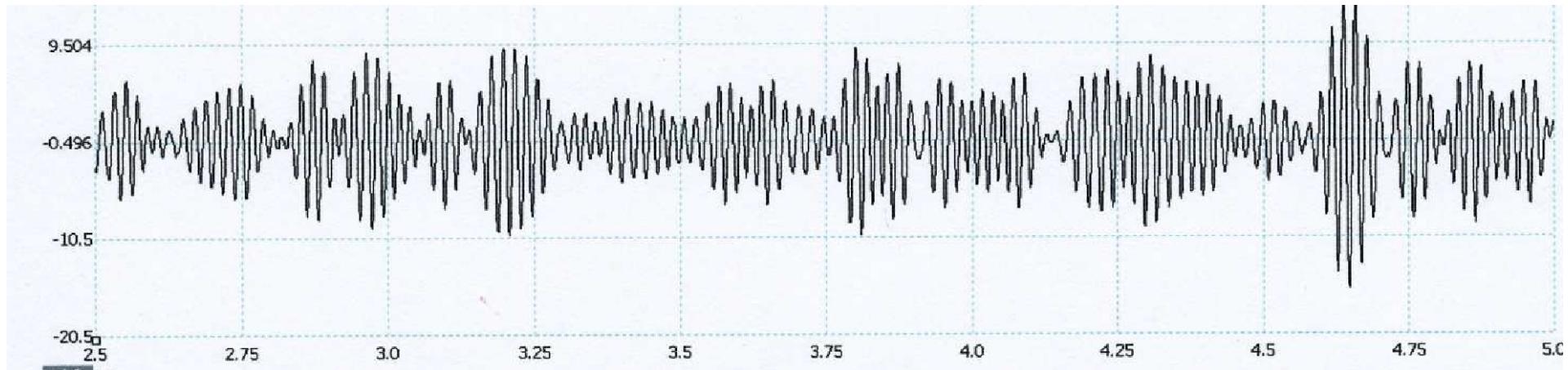
Orthogonal Frequency Division Multiplexing



http://nl.wikipedia.org/wiki/Orthogonal_frequency_division_multiplexing
Auteur : Gerben49 – CC-BY-SA-4.0

Modulation QAM

Exemple d'une porteuse



Chaque porteuse peut être modulée différemment, suivant le débit et la QoS souhaités (vidéo, audio, texte, ...). Aujourd'hui le QAM l'emporte évidemment sur les modes BPSK/QPSK historiques.

Source : Le WIFI alias WLAN en OFDM sur 2.4 GHz.

Par Kurt Ritter he9dyy Rev.mai 2014

Nombre de sous-porteuses utiles en OFDM / OFDMA

	Sous-porteuses					
	Espacement des sous-porteuses (KHz)	Total des sous-porteuses réelles	Largeur de bande (MHz)	Total des sous-porteuses « utiles »	Données	Pilotes
802.11a/g WiFi 2/3	312,5	64	20	52	48	4
802.11n WiFi 4	312,5	64	20	56	52	4
	312,5	128	40	114	108	6
802.11ac WiFi 5	312,5	256	80	242	234	8
	312,5	512	160	484	468	16
802.11ax WiFi 6	78,125	1024	80	996	980	16

Les sous-porteuses réelles s'obtiennent en ajoutant les porteuses de garde (basses et hautes), les sous-porteuses pilotes / nulles / et DC (centre d'une bande)

Calculs de débits réels MIMO 2x2

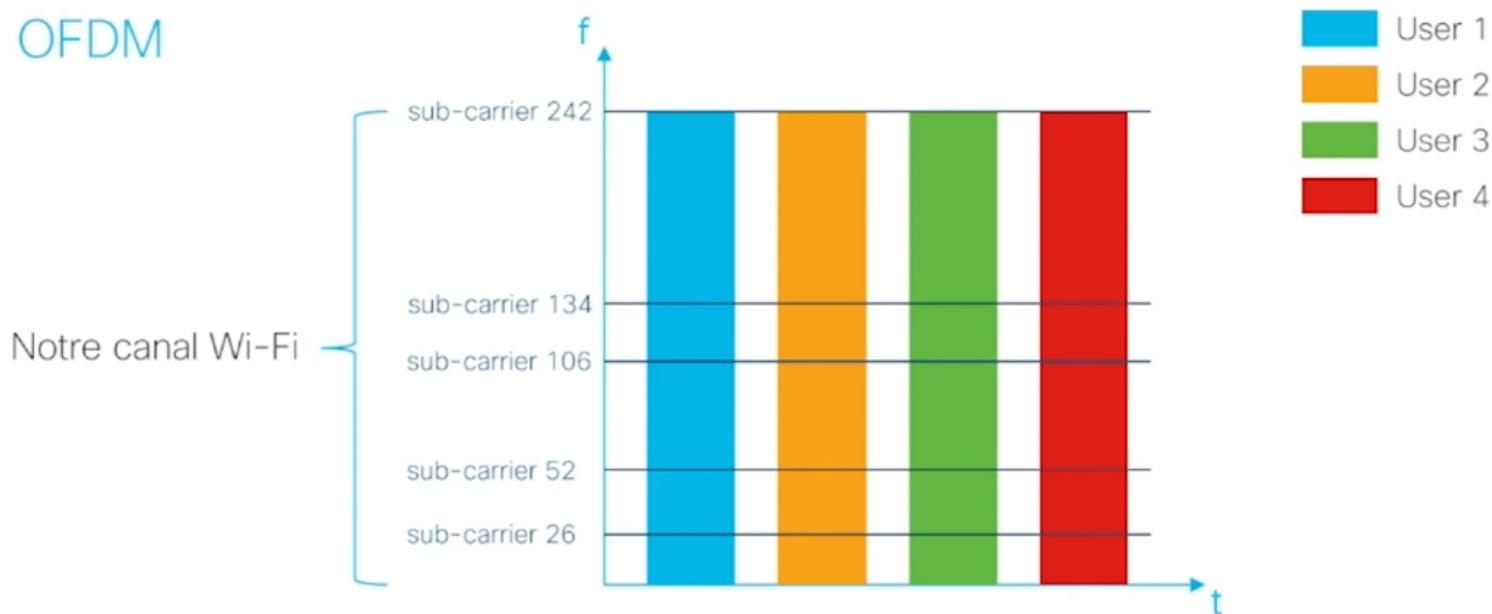
(avec généralement 2 antennes dans un PC...)

	802.11a/g WiFi 2/3	802.11n WiFi 4	802.11ac WiFi 5	802.11ax WiFi 6	802.11be WiFi 7
Sous-porteuses de données	48	108	468	1960	?
Largeur de bande (MHz)	20	40	160	2x80	
Flux spatiaux	1	4	8	8	(16)
Taux de codage	3/4	5/6	5/6	5/6	?
Bits/Symbole	6 (64 QAM)	6 (64 QAM)	8 (256 QAM)	10 (1024 QAM)	12 (4096 QAM)
Durée symbole OFDM(A) + garde min	4 µs	3,6 µs	3,6 µs	13,6 µs	(13,6 µs)
Vitesse max (SPxFSxVCxBs)/ DS	54Mbit/s	600 Mbit/s	6,933 Gbit/s	9,6 Gbit/s	(46,1 Gbit/s)
Rapport pour 2 flux spatiaux	-	300 Mbit/s	1,73 Gbit/s	2,4 Gbit/s	(2,88 Gbit/s)

La modulation OFDM / OFDMA

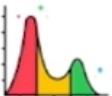


Efficiency spectrale : OFDMA

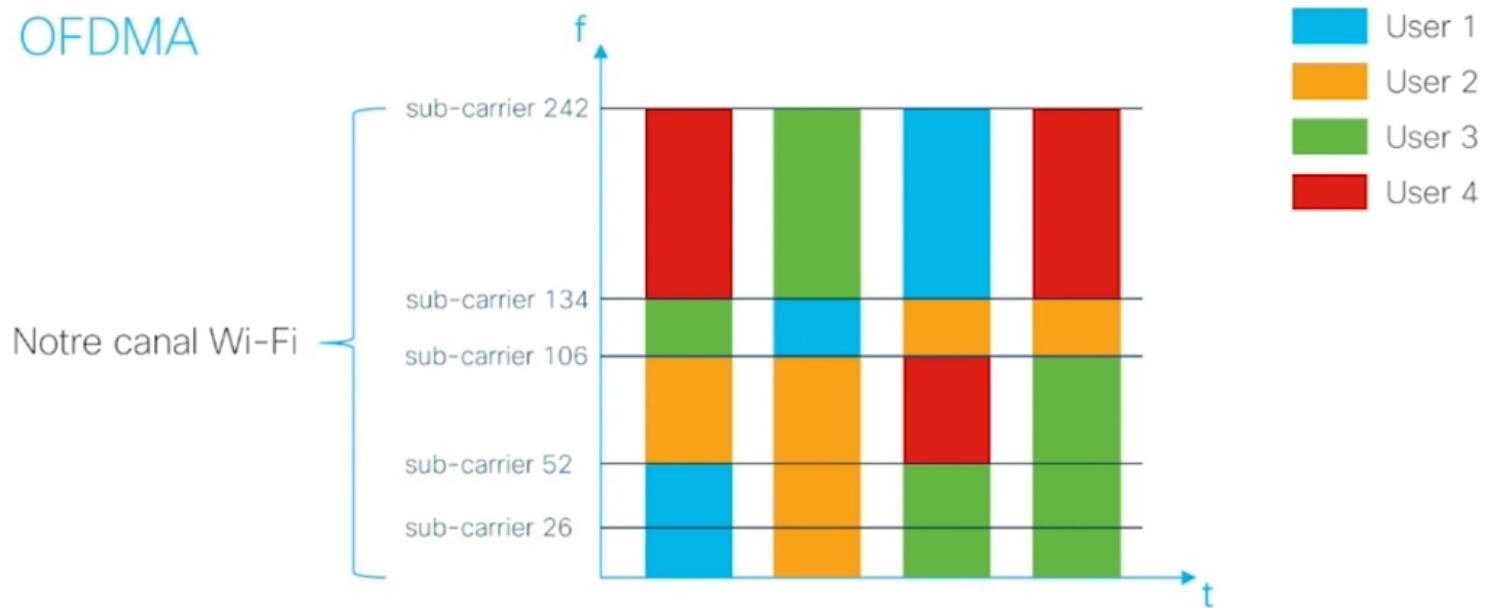


OFDM = Orthogonal Frequency Division Multiplexing
OFDMA = Orthogonal Frequency Division Multiple Access

La modulation OFDM / OFDMA

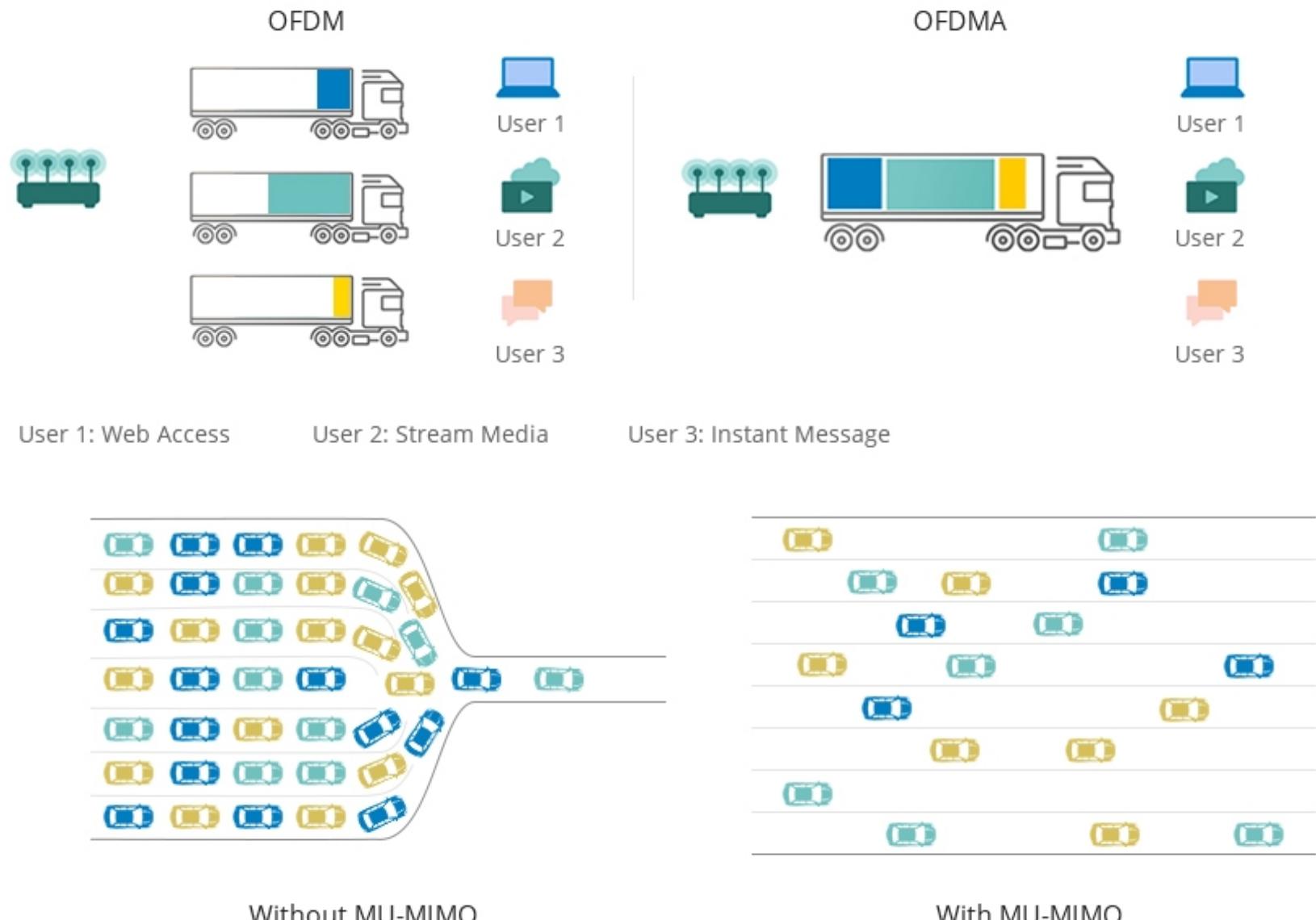


Efficiency spectrale : OFDMA



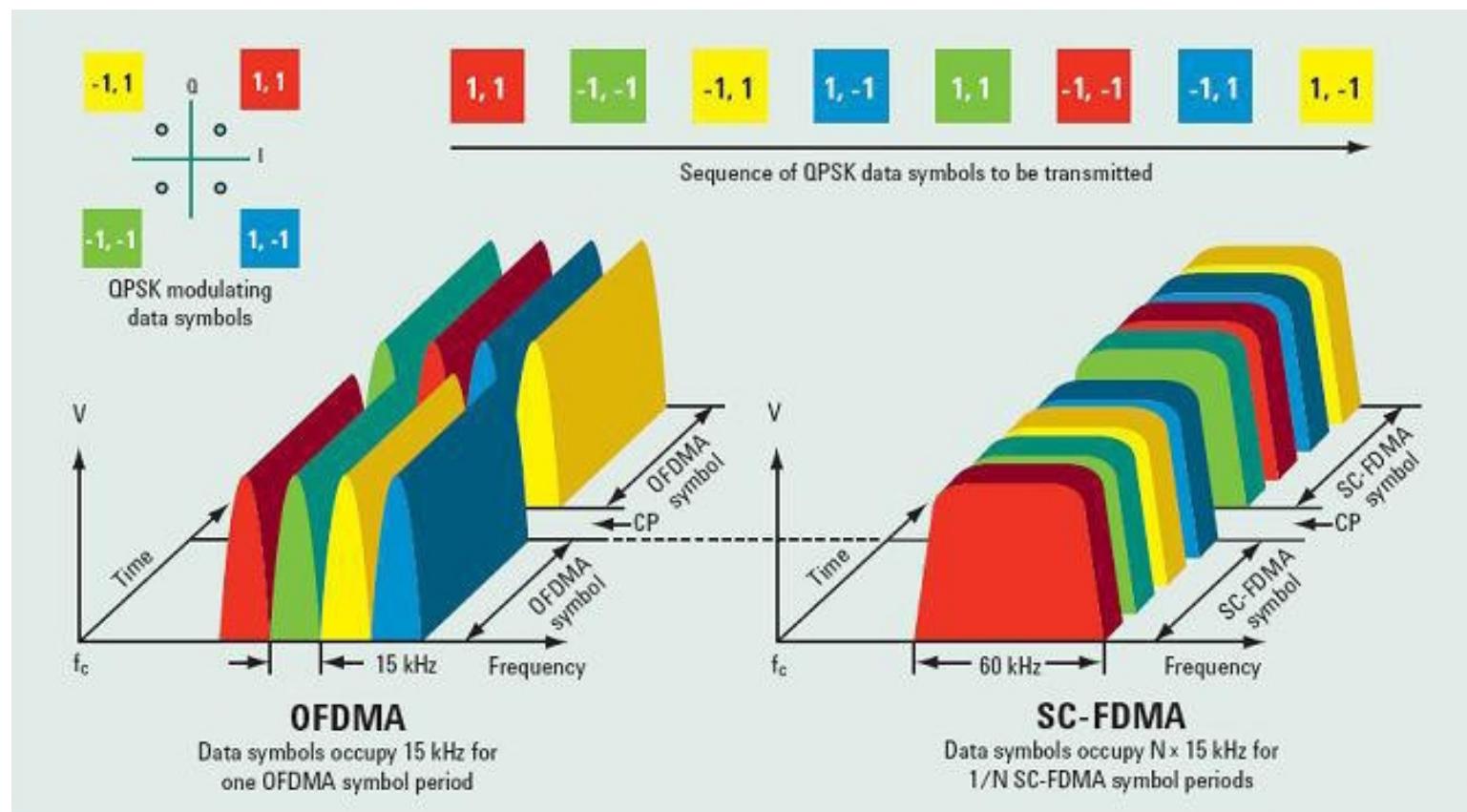
OFDM = Orthogonal Frequency Division Multiplexing
OFDMA = Orthogonal Frequency Division Multiple Access

La modulation OFDM / OFDMA



La modulation OFDM / OFDMA

- **OFDMA = version multi-utilisateurs de l'OFDM** : on attribue à chaque utilisateur un ensemble de sous-porteuses.



Résumé codages/modulations

Bande ISM

Norme 802.11	Bandes	Transmission	Codage	Modulation	Débit théorique Mbit/s	Compatibilité descendante
a	U-NII	OFDM		BPSK QPSK 16-QAM 64-QAM	6-9 12-18 24-36 48-54	
b	ISM	HR/DSSS	Barker (11bits) CCK (4-8bits)	BPSK QPSK	1-2 5,5-11	
g	ISM	OFDM	CCK si 5,5-11 Mbits/s	BPSK QPSK 16-QAM 64-QAM	6-9 12-18 24-36 48-54	802.11b
n	ISM + U-NII	OFDM MIMO		64-QAM	600	802.11a 802.11g

Résumé codages/modulations

Bande U-NII

Norme 802.11	Bandes	Transmission	Codage	Modulation	Débit théorique Gbit/s	Compatibilité descendante
ac	U-NII	OFDM MIMO		256-QAM	6,9	802.11a (802.11n)
ax	U-NII	OFDM(A) MIMO		1024-QAM	9,6	802.11ac

WiFi – normes – 1/4

Protocole	802.11a (WiFi 2)	802.11b (WiFi 1)	802.11g (WiFi 3)	802.11n (WiFi 4)
Bande	5 Ghz	2,4 Ghz	2,4 Ghz	2,4 <u>ou</u> 5 Ghz
Année	1999	1999	2003	2009
MIMO	-	-	-	SU-MIMO (***)
Largeur canal max.	20Mhz	22Mhz	20Mhz	40Mhz
Modulation	64 QAM(*)	BPSK/QPSK (**)	64 QAM	64 QAM
Flux max. théorique	4	3	4	4
Débit max. théorique	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s (****)

* : QAM : modulation d'amplitude en quadrature

** : Bi-Quad Phase-Shift Keying (2-4 valeurs de phases)

*** : introduit le beam forming (focalisation sur un lobe)

**** :en MIMO 4x4 avec 150 Mbit/s max par flux/antenne

WiFi – les tables MCS

Modulation and Coding Scheme

MCS Index - 802.11n and 802.11ac

HT MCS Index	VHT MCS Index	Spatial Streams	Modulation	Coding	20MHz		40MHz		80MHz		160MHz		802.11n 802.11ac	
					Data Rate No SGI	Data Rate SGI								
0	0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65		
1	1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130		
2	2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195		
3	3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260		
4	4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390		
5	5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520		
6	6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585		
7	7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650		
	8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780		
	9	1	256-QAM	5/6	n/a	n/a	180	200	390	433.3	780	866.7		
8	0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130		
9	1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260		
10	2	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390		
11	3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520		
12	4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780		
13	5	2	64-QAM	2/3	104	115.6	216	240	468	520	936	1040		
14	6	2	64-QAM	3/4	117	130.3	243	270	526.5	585	1053	1170		
15	7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300		
	8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560		
	9	2	256-QAM	5/6	n/a	n/a	360	400	780	866.7	1560	1733.3		
16	0	3	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195		
17	1	3	QPSK	1/2	39	43.3	81	90	175.5	195	351	390		
18	2	3	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585		
19	3	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780		
20	4	3	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170		
21	5	3	64-QAM	2/3	156	173.3	324	360	702	780	1404	1560		
22	6	3	64-QAM	3/4	175.5	195	364.5	405	n/a	n/a	1579.5	1755		
23	7	3	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950		
	8	3	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340		
	9	3	256-QAM	5/6	260	288.9	540	600	1170	1300	n/a	n/a		

SGI : Short Guard Interval (cf. partie OFDM/OFDMA)

WiFi – normes - 2/4

Protocole	802.11ac (wave 1)	802.11ac (wave 2)	802.11ac (WiFi5)	[802.11.ad] (WiGig)
Bande	5 Ghz	5 Ghz	5 Ghz	57,24-65,88 Ghz (UE) 57,24-63,72 Ghz (US)
Année	2015	2016	2014	2016
MIMO	SU-MIMO	MU-MIMO (DL) (***)	MU-MIMO (DL)	-
Largeur canal max.	80MHz	160Mhz	160 Mhz	2160Mhz
Modulation	256 QAM	256 QAM	256 QAM	64 QAM
Flux max. théorique	3 (*)	4(**)	8 (**)	-
Débit max. théorique	1,3 Gbit/s	3,47 Gbit/s	6,9 Gbit/s	6,8 Gbits/s (***)

* : 433 Mbit/s par flux de 80 Mhz

** : 867 Mbit/s par flux de 160 Mhz

*** : 4,6 Gbit/s en mode simple porteuse, 6,8 Gbits/s en OFDM

**** : un/plusieurs lobe(s) focalisé(s) pour chaque appareil compatible

WiFi – normes - 3/4

Protocole	[802.11af] (White-WiFi)	[802.11ah] (HaLow ***)	802.11ax (WiFi 6)	[802.11.ay] (WiGig v2 ?)
Bandé	470-790 Mhz (UE) 54-790 Mhz (US)	863-868 Mhz (UE) 902-929 Mhz (US)	2,4 <u>ou</u> 5 GHz	57,24-65,88 Ghz (UE) 57,24-63,72 Ghz (US)
Année	2016	2016	2021	2021
MIMO	MU-MIMO	MU-MIMO	MU-MIMO (DL+UL)	MU-MIMO
Largeur canal max.	8 Mhz (*)	16 Mhz (*)	160 MHz	8640 Mhz
Modulation	256 QAM	256 QAM	1024 QAM	256 QAM
Flux max. théorique	4	2	8	4
Débit max. théorique	568,9 Mbit/s (*)	347 Mbit/s (*)	9,6 Gbit/s (**)	176Gbit/s (****)

* : dépend des fréquences UHF/VHF libérées dans chaque pays et de la largeur des canaux

** : l'espacement entre sous-porteuses passe de 312,5 kHz à 78,125 kHz

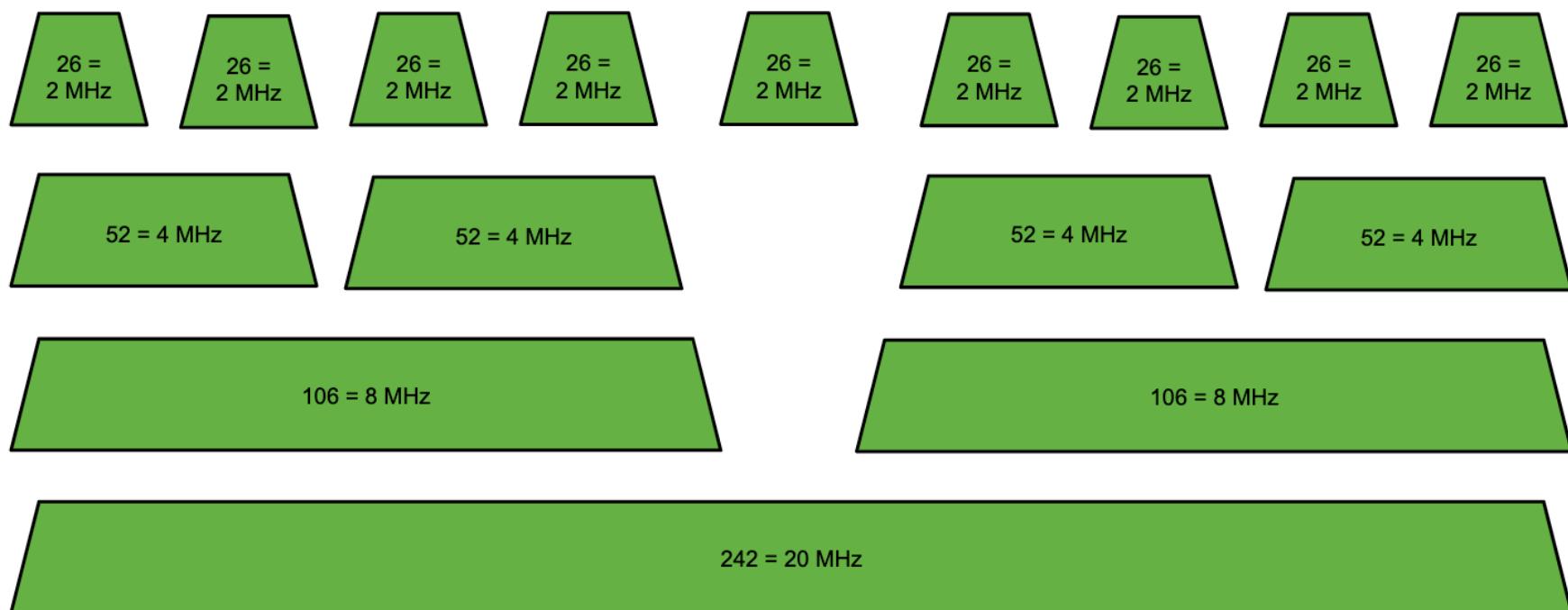
*** : également nommé **HEW = High Efficiency WLAN**

**** : 5,5Gbit/s par canal x 8 canaux = 44 Gbit/s par antenne

WiFi 6 – 802.11ax

nombre de clients réels...

Nombre de sous-porteuses et largeur de bande



Source : [https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_\(802.11ax\)_Technical_Guide](https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_(802.11ax)_Technical_Guide)

WiFi 6 – 802.11ax

nombre de clients réels...

Génération / SP	SP*	Largeur (MHz)	Largeur de canal disponible par agrégation (Mhz)				
			20	40	80	160**	80+80**
802.11ax WiFi 6	996 (x2)	160	-	-	-	1	1
	996	80	-	-	1	2	2
802.11ac WiFi 5	484	40	-	1	2	4	4
	242	20	1	2	4	8	8
802.11n WiFi 4	106	8	2	4	8	16	16
	52	4	4	8	16	32	32
	26***	2	9	18	37	74	74

Source : [https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_\(802.11ax\)_Technical_Guide](https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_(802.11ax)_Technical_Guide)

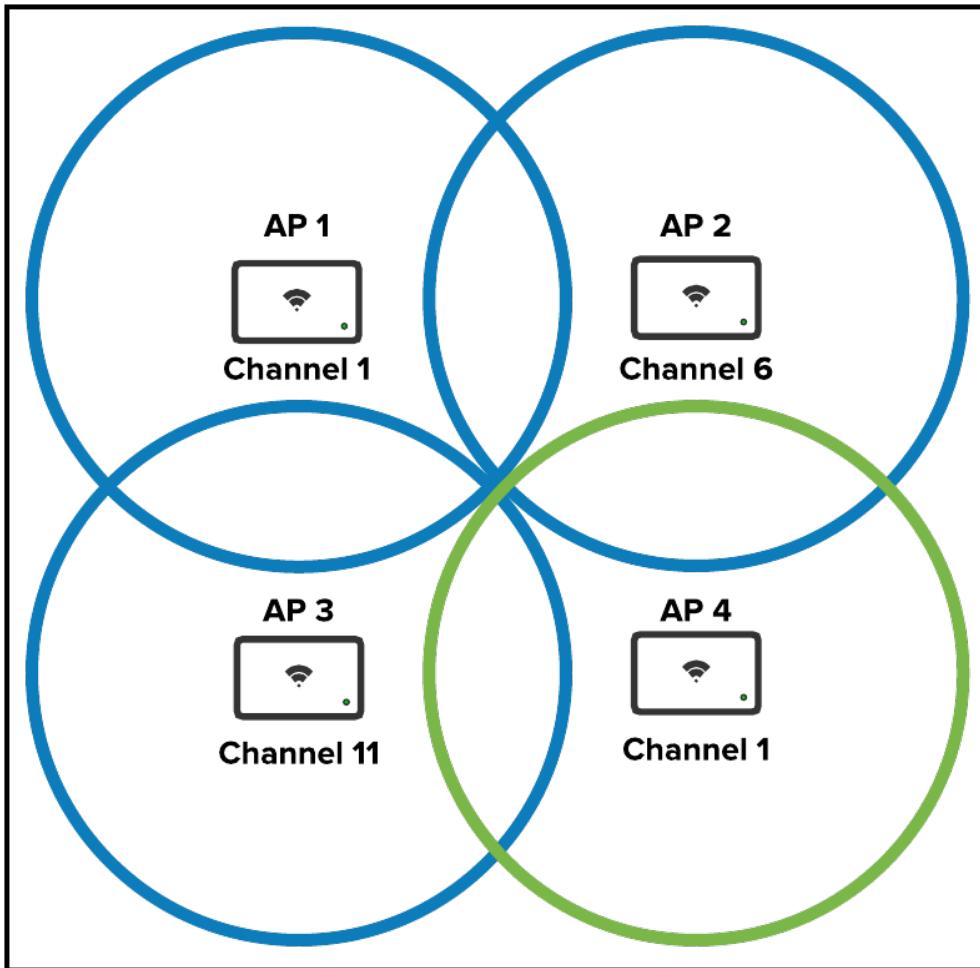
* : SP = Sous porteuses

** : 802.11ax autorise les largeurs de canaux 160 ou 80+80 MHz

*** : nombre minimal de porteuses en OFDM / OFDMA

WiFi 6 – 802.11ax

le coloriage BSS / CSS coloring



- Fonctionne en 2,4 GHz et 5GHz.
- 6 bits ajoutés dans la couche physique et les trames de gestion.
- 63 couleurs BSS disponibles.
- Les clients du canal1 n'ont plus besoin d'attendre que les deux APs soient libres.

Source : [https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_\(802.11ax\)_Technical_Guide](https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_(802.11ax)_Technical_Guide)

WiFi – normes - 4/4

Protocole	802.11ax (WiFi 6E)	802.11be (WiFi 7)		
Bande	2,4 - 5 <u>ou</u> 6 GHz	2,4 - 5 <u>et</u> 6 GHz		
Année	2021	2024 ?		
MIMO	MU-MIMO (DL+UL)	MU-MIMO (DL+UL) + MLO +MAP *		
Largeur canal max.	160 MHz	320MHz (France !) 		
Modulation	1024 QAM	4096 QAM		
Flux max. théorique	8	16		
Débit max. théorique	9,6 + 1 Gbit/s	46,1 Gbit/s		

* MLO : Multi Link Operation – le client peut désormais envoyer/recevoir sur les différentes bandes de fréquence et canaux, là où les normes précédentes le limitait à une seule bande active.
 MAP : Multi-Access Point – nouvelles techniques de synchronisation des AP pour optimiser les transferts

WiFi 7 - MLO / MultiLink Operation

(opérations multi-liens)

- **Mode STR (Simultaneous Transmit and Receive) :** utilisation des bandes disponibles pour des opérations simultanées et indépendantes, par exemple pour télécharger un fichier sur une bande, et téléverser un fichier sur une autre.
- **Mode NSTR (Non STR) :** regroupement des bandes disponibles pour télécharger ou téléverser un fichier plus rapidement.
- Il existe d'autres modes MLO orientés vers les réseaux maillés.

WiFi 7 – MAP

Multiple Access-Point

- **Joint Distributed MIMO** : des points d'accès liés (lien « backhaul ») peuvent transmettre ensemble et en même temps des données au client.
- **Coordinated OFDMA** : répartition de l'OFDMA entre les points d'accès.
- **Coordinated null steering** : filtrage spatial (beamforming) synchronisé entre points d'accès. Un AP peut atténuer son signal dans une direction, laissant les autres « arroser » la zone.

Trames 802.11 - 1/4

trames MAC générales 1997/1999

Frame Control	Duration / Id	Adr 1	Adr2	Adr 3	Sequence control	Adr 4	Frame body	FCS
	2 x 2 bytes		3 x 6 bytes		2 bytes	6 bytes	0-2312 bytes	4 bytes
Header							Body	Control

- FCS = Frame Check Sequence = CRC recalculé côté réception pour garantir l'intégrité de la trame.
- Tous les champs ne sont pas toujours présents :
 - Pour les trames RTS, les champs Adr3 à Frame body sont vides.
 - Pour les trames CTS et ACK, les champs Adr2 à Frame body sont vides.

Trames 802.11 - 2/4

trames MAC générales 2007

Frame Control	Duration / Id	Adr 1	Adr 2	Adr 3	Seq control	Adr 4	QoS control	Frame body	FCS
2 x 2 bytes		3 x 6 bytes			2 bytes	6 bytes	2 bytes	0-2310 bytes	4 bytes
Header						Body		Ctrl	

Le champ Frame body diminue de 2 octets pour laisser place à l'arrivée de la 802.11e QoS.

TABLE 3.4 QoS Control field

QoS Station	Bits 0-3	Bit 4	Bits 5-6	Bit 7	Bits 8-15
AP	TID/Access Class	EOSP	ACK Policy	Reserved	TXOP Limit
AP	TID/Access Class	EOSP	ACK Policy	Reserved	AP PS Buffer State
Client STA	TID/Access Class	0	ACK Policy	Reserved	TXOP Duration Requested
Client STA	TID/Access Class	1	ACK Policy	Reserved	Queue Size

Trames 802.11n - 3/4

trames MAC générales 2012

Frame Ctrl	Durat. / Id	Adr 1	Adr 2	Adr 3	Seq ctrl	Adr 4	QoS ctrl	HT ctrl	Frame body	FCS
2 x 2 bytes		3 x 6 bytes			2 bytes	6 bytes	2 bytes	4 bytes	0-7951 bytes	4 bytes
Header							Body		Control	

- La ratification de 802.11n en 2009 et son arrivée effective en 2012 autorise un **Frame body beaucoup plus long** avec utilisation des **A-MSDU**.
- L'ajout champ **High Throughput** introduit notamment les mécanisme de **Beamforming** en transmission, de sélection d'antennes (**Antenna Selection** ou **ASEL**), ...

Trames 802.11ac - 4/4

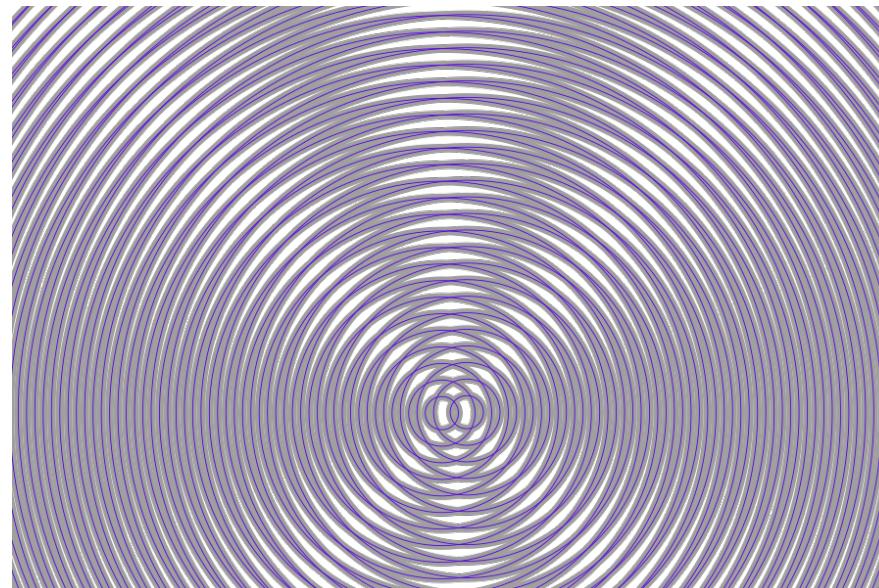
trames MAC générales 2013

Frame Ctrl	Durat. / Id	Adr 1	Adr 2	Adr 3	Seq ctrl	Adr 4	QoS ctrl	HT ctrl	Frame body	FCS
2 x 2 bytes		3 x 6 bytes			2 bytes	6 bytes	2 bytes	4 bytes	0 to variable	4 bytes
Header								Body		Control

- Le champ **Frame body** devient complètement **variable**, suivant la taille des (A-)MSDU/MPDU « encapsulés » dans les PPDU à transférer, le cryptage retenu.

Le beamforming modelage spatial de lobes

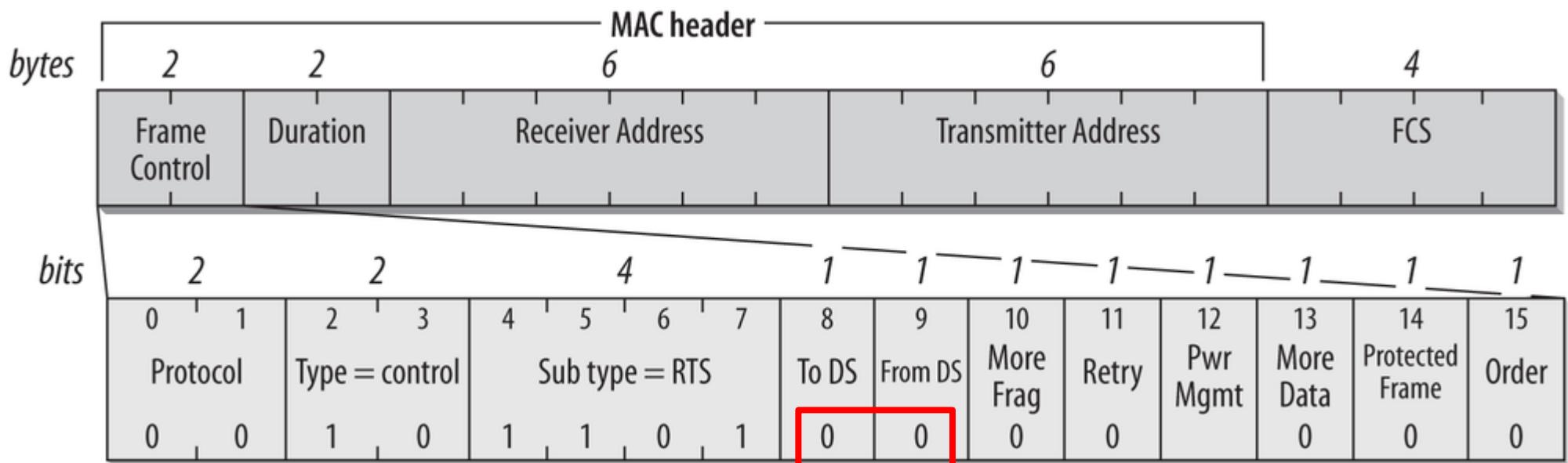
- L'idée est d'utiliser plusieurs antennes émettrices avec des interférences constructives/destructives. Exemple avec 2 antennes émettrices ci-dessous.
- Stations et AP « testent » les combinaisons possibles via des **Null Data Packet**.



Source : https://www.ens-louis-lumiere.fr/sites/default/files/2019-02/ENSLL_2015_Son_Grislin_BD.pdf

Trames de contrôle - 1/7

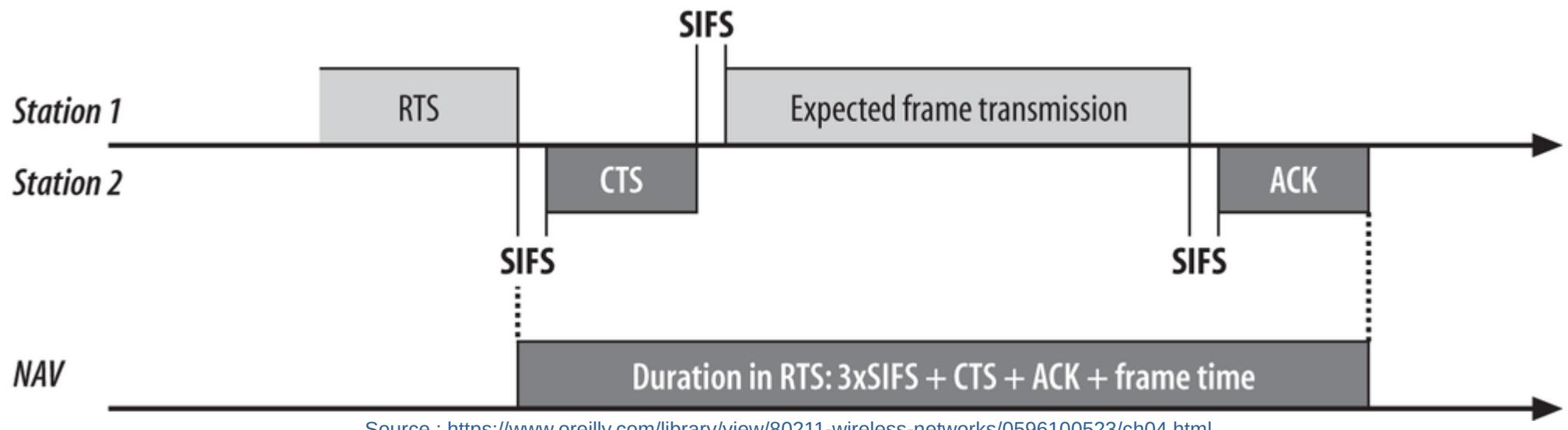
la trame RTS



Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

Trames de contrôle - 2/7

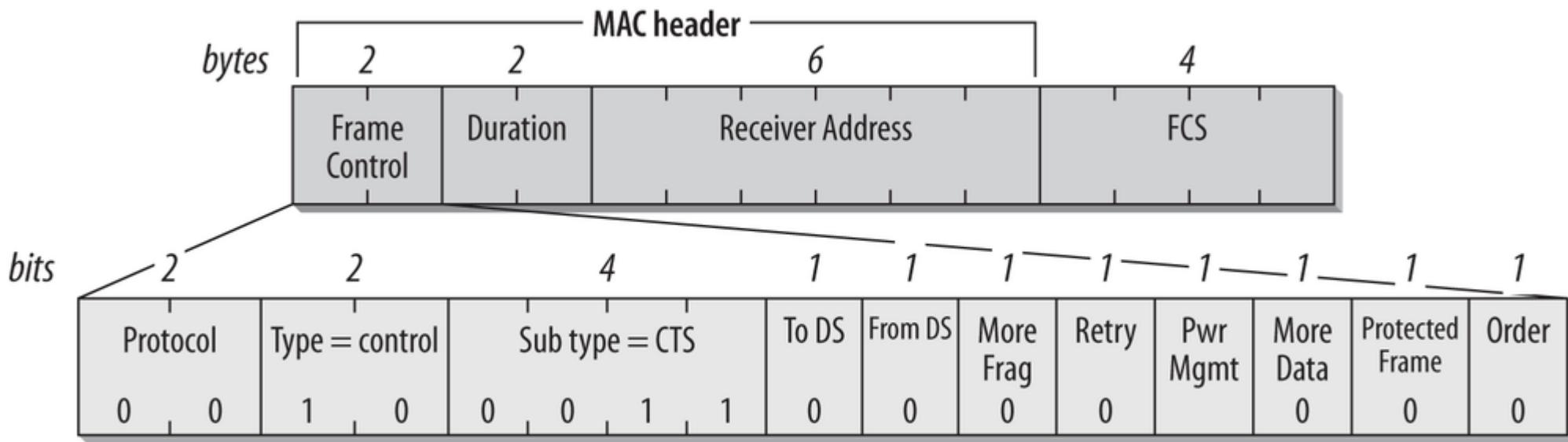
la trame RTS



$$\text{NAV(CTS)} = \text{SIFS} + t(\text{CTS}) + \text{SIFS} + t(\text{DATA}) + \text{SIFS} + t(\text{ACK}) \mu\text{s}$$

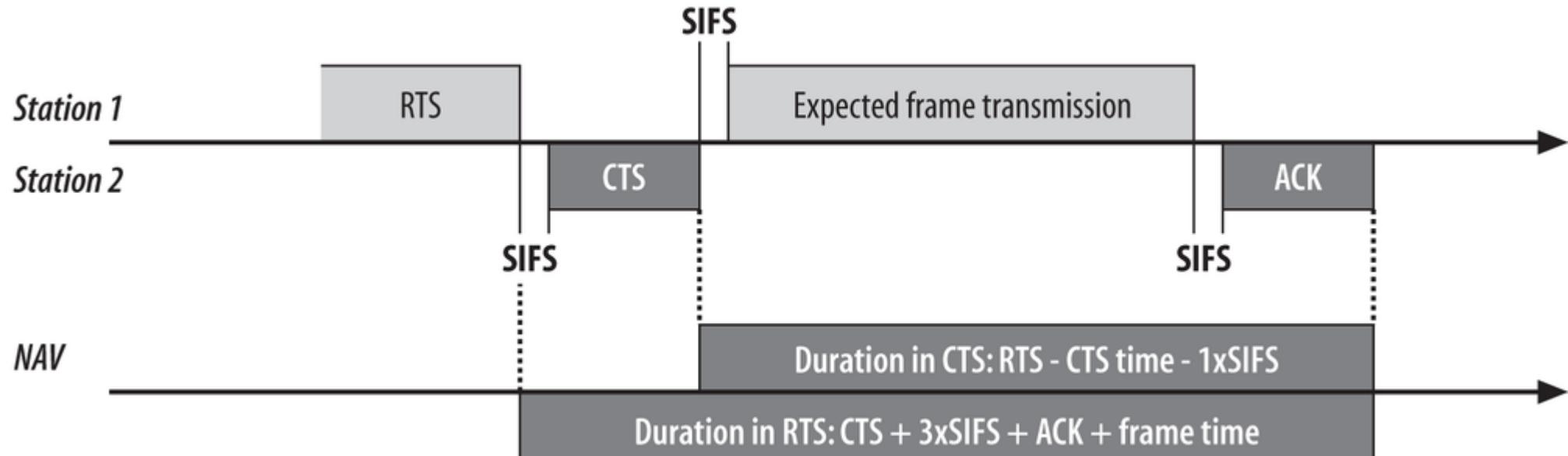
Trames de contrôle - 3/7

la trame CTS



Trames de contrôle - 4/7

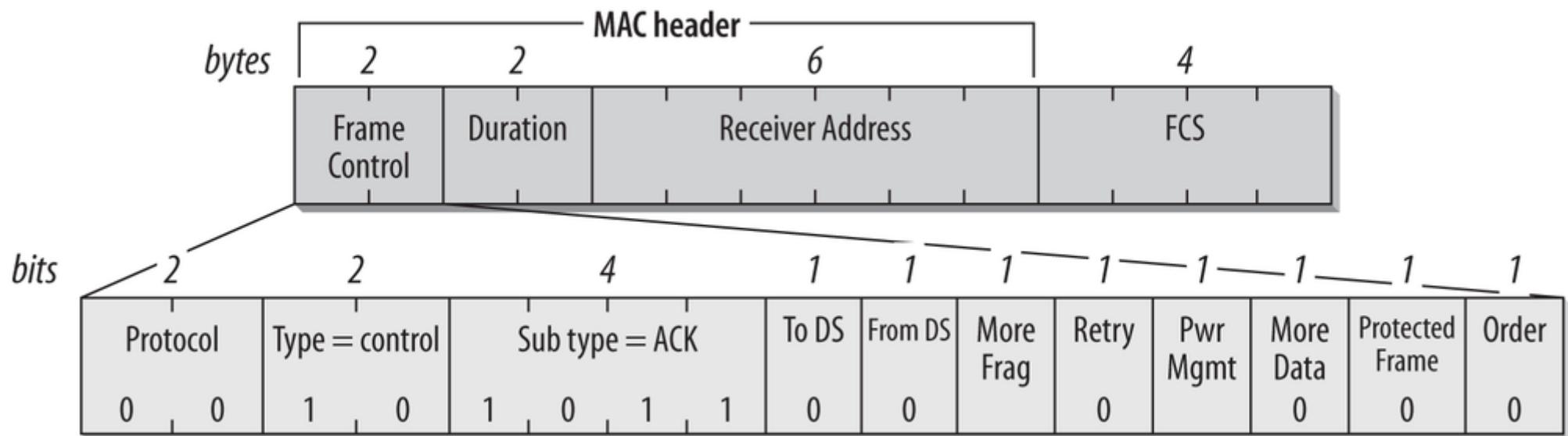
la trame CTS



$$\text{NAV(CTS)} = \text{SIFS} + t(\text{DATA}) + \text{SIFS} + t(\text{ACK}) \mu\text{s}$$

Trames de contrôle - 5/7

la trame ACK

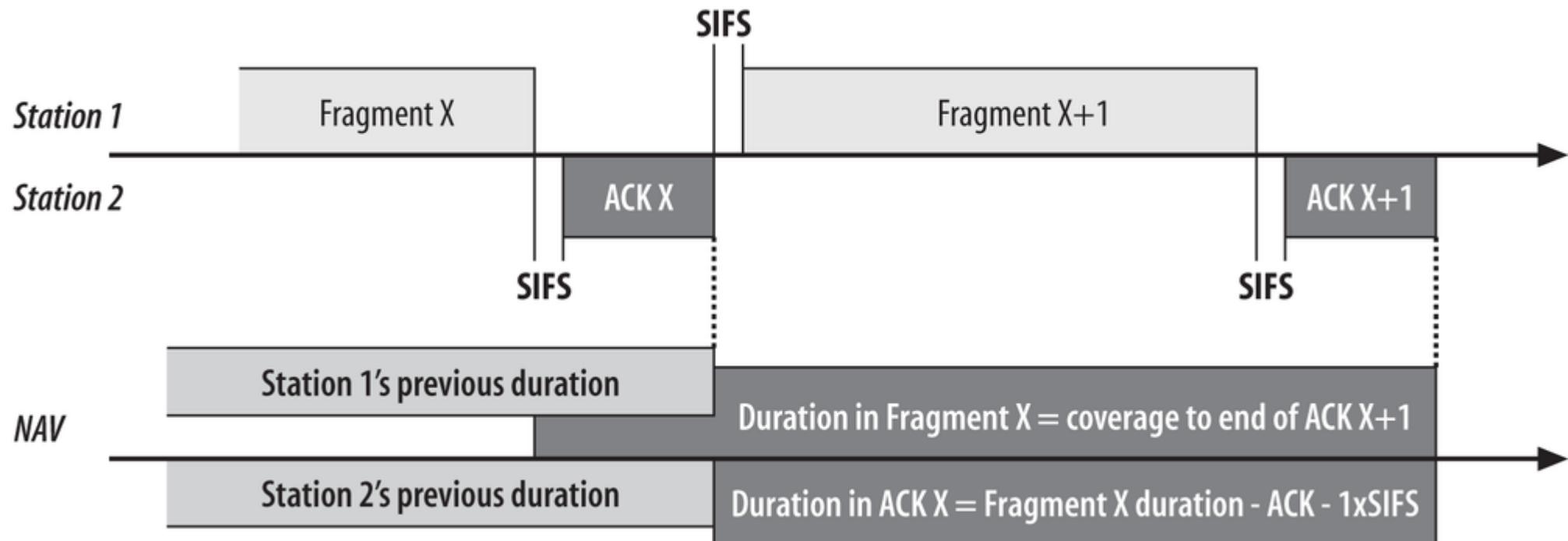


Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

$$\text{NAV(ACK)} = (\text{More Fragment} == 0 ? 0 : \text{SIFS} + t(\text{DATA}) + \text{SIFS} + t(\text{ACK})) \mu\text{s}$$

Trames de contrôle - 6/7

la trame ACK

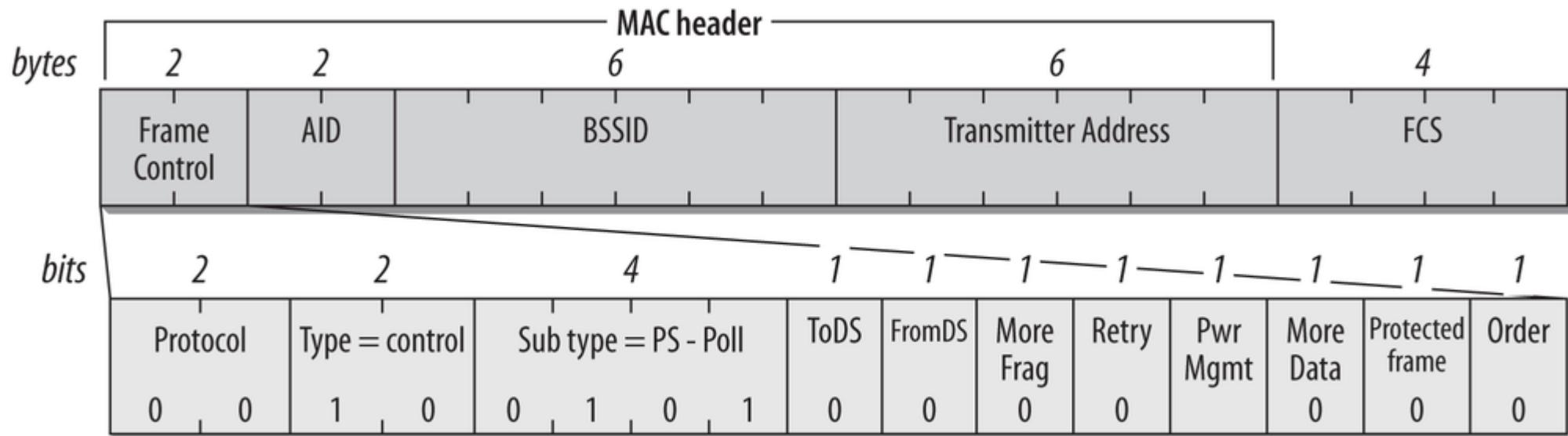


Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

- L'expéditeur indique la fin d'une transmission de données en mettant le bit More Fragment à 0, ce qui mettra la durée du ACK suivant également à 0.
- Les ACK sont transmis en réponse à des trames de données, de gestion et des trames PS-Poll (Power-Save Poll)

Trames de contrôle - 7/7

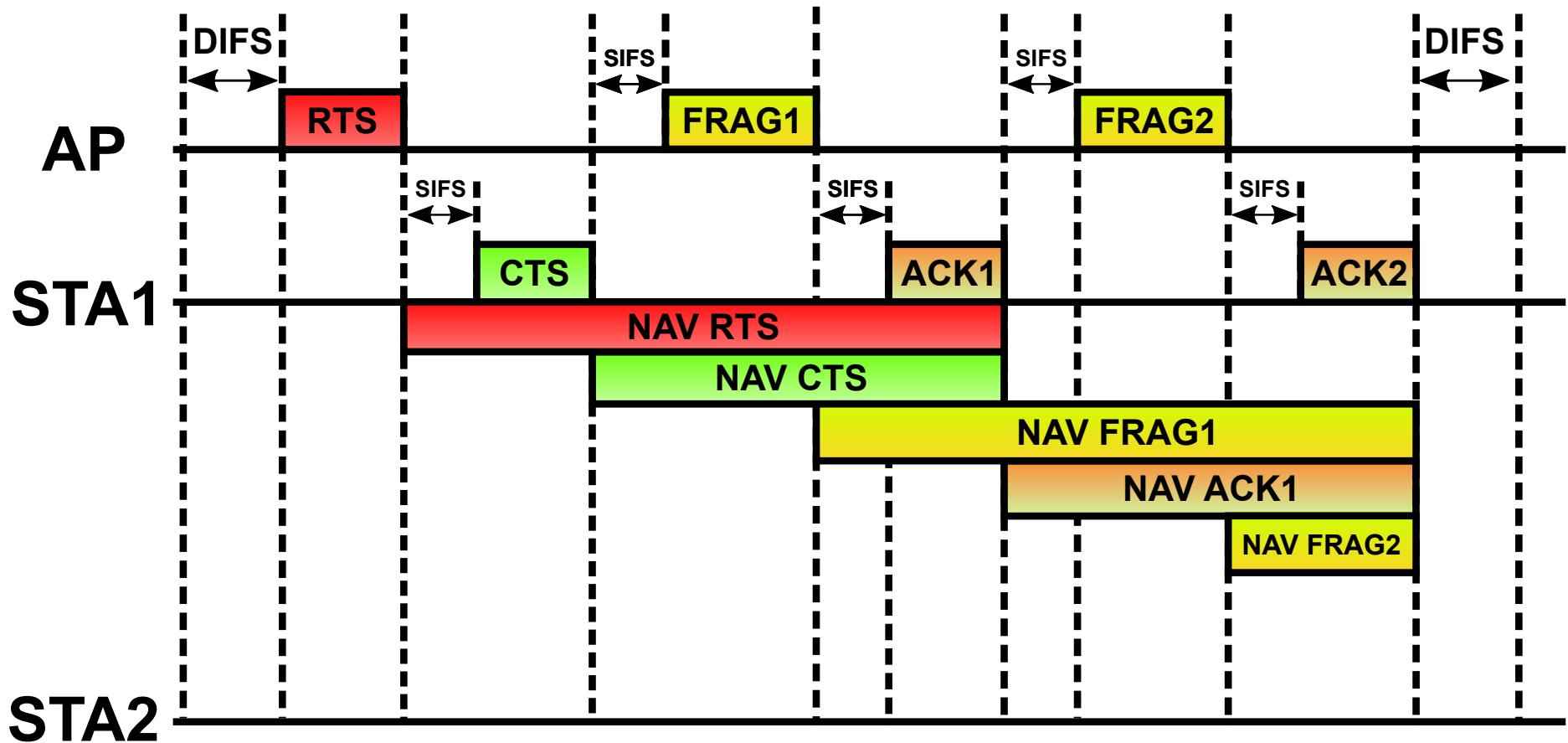
la trame PS-Poll (Power-Save Poll)



- Envoyée quand une station se réveille, pour récupérer les données reçues par l'AP.
- La particularité est le remplacement de la durée Duration par une Association ID (AID) - valeur numérique assignée par le point d'accès.
- À noter que malgré l'absence du champ Duration, les stations captant une trame PS-Poll se fabriquent automatiquement un NAV(PS-Poll) = SIFS + t(ACK).

Données fragmentées

exemple de transfert AP vers STA1 sans BO



Trames 802.11 – 1/4

Détail de la trame de contrôle

Protocol version	Type	Subtype	To DS	From DS	More frags	Retry	Power Mgt	More data	WEP	Order
2x2 bits	4 bits						8 x 1bit			
	byte 1							byte 2		

- Protocol version = 00 en 802.11
- Type de trame = 00 (Management), 01 (Control), 10 (Data), 11 (Reserved)
- Rappel : DS = Distribution System
- More frags : si 1, il reste des fragments de données unicast à transmettre
- Power Mgt : si 1, la station client entre en mode veille, et informe l'AP
- More data : quand une station se réveille, le champ TIM (Trafic Indication Map) des balises lui indique si l'AP a des données en attente pour elle. Si c'est le cas, elle reste éveillée, et l'AP lui envoie ses données, avec More data=1 tant qu'il reste des données à transmettre.
- Order : Anciennement : la trame a été envoyée en utilisant la classe de service strictement ordonnée (Strictly-Ordered service class). Aujourd'hui : 1 si QoS.

Trames 802.11 - 2/4

Types et sous-types pour la gestion

Valeur du type	Description du type	Valeur du sous-type (b7 b6 b5 b4)	Description du sous-type
00	Gestion	0000	Requête d'association
		0001	Réponse d'association
		0010	Requête de ré-association
		0011	Réponse de ré-association
		0100	Demande d'enquête (probe request)
		0101	Réponse d'enquête (probe response)
		0110-0111	Réservés
		1000	Balise (beacon)
		1001	ATIM
		1010	Désassociation
		1011	Authentification
		1100	Désauthentification
		1101-1111	Réservés

Trames 802.11 - 3/4

Types et sous-types pour les données

Valeur du type	Description du type	Valeur du sous-type (b7 b6 b5 b4)	Description du sous-type
10	Données	0000	Données
		0001	CF-ACK - avec données
		0010	CF-Poll - avec données
		0011	CF-ACK + CF-Poll - avec données
		0100	Fonction nulle - sans données
		0101	CF-ACK - sans données
		0110	CF-Poll - sans données
		0111	CF-ACK + CF-Poll - sans données
11	Réserve	1000-1111	Réserve (QoS)
		0000-1111	Réserve

Trames 802.11 - 4/4

Types et sous-types pour le contrôle

Valeur du type	Description du type	Valeur du sous-type (b7 b6 b5 b4)	Description du sous-type
01	Contrôle	0000-1001	Réservés
		1010	PS-Poll (Power-Save Poll)
		1011	RTS
		1100	CTS
		1101	ACK
		1110	CF End
		1111	CF End et CF-ACK

From / To DS – 1/13

Les 4 combinaisons de base

From DS	To DS	Signification
0	0	Trame entre deux stations d'un réseau ad-hoc/mesh, ou trame de gestion/contrôle.
0	1	Trames issue d'une station sans fil et à destination d'une autre station via le DS. Cette trame transitant via un point d'accès, c'est l'adresse du point d'accès qui est utilisée comme destination suivante.
1	0	Trame issue du DS, passant par un point d'accès et à destination d'une station sans fil, la source pouvant être filaire ou sans fil.
1	1	Trame issue d'un point d'accès et à destination d'un autre point d'accès, utilisé pour l'interconnexion de réseaux locaux.

From / To DS - 2/13

Emplacements des champs d'adresses

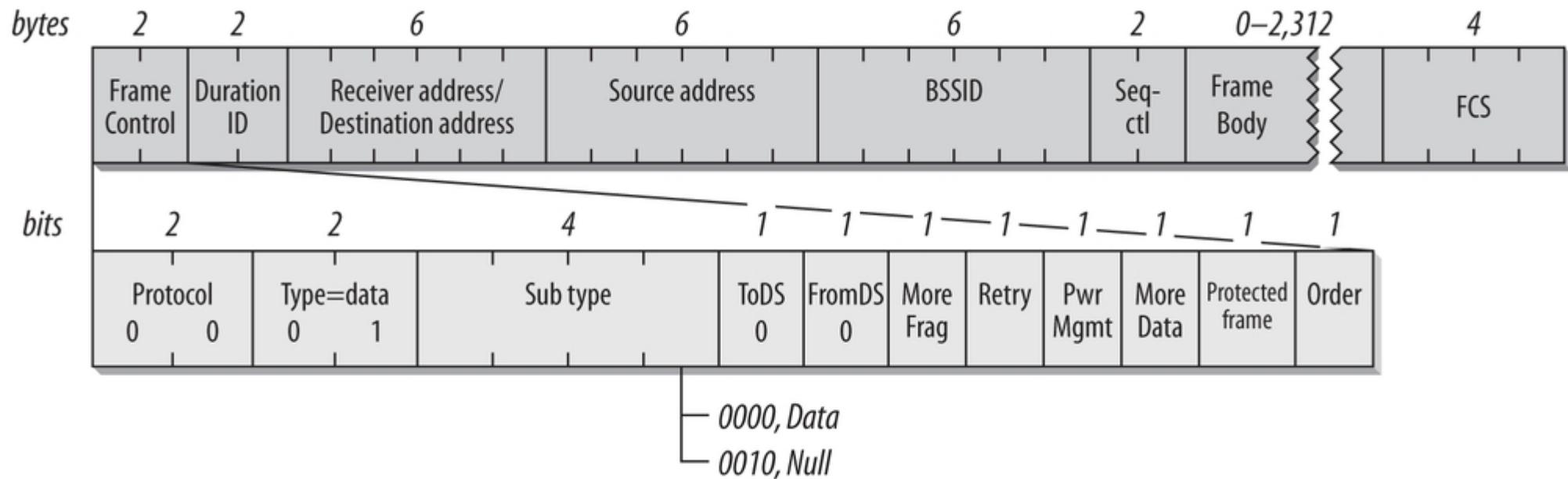
Mode	From DS	To DS	Adr1	Adr2	Adr3	Adr4
Ad hoc	0	0	DA = RA	SA = TA	IBSSID	-
Vers DS	0	1	RA = BSSID	SA = TA	DA	-
Depuis DS	1	0	DA = RA	BSSID = TA	SA	-
DS	1	1	RA	TA	DA	SA



Trajet parcouru : SA (Source) > TA (Transmitter) > RA (Receiver) > DA (Destination)

From / To DS – 3/13

From DS=0 et To DS=0



Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

- Dans un réseau ad-hoc, le BSSID est utilisé comme IBSSID commun entre stations. Les trames de données Null sont utilisées uniquement pour communiquer l'état de veille aux autres stations.

From / To DS – 4/13

From DS=0 et To DS=0

```

    ▷ IEEE 802.11 Beacon frame, Flags: .....C
      Type/Subtype: Beacon frame (0x0008)
      ▷ Frame Control Field: 0x8000
        .... .00 = Version: 0
        .... 00.. = Type: Management frame (0)
        1000 .... = Subtype: 8
      ▷ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0... .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
        .000 0000 0000 0000 = Duration: 0 microseconds
      Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
      Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
      Transmitter address: ZebraTec_c1:24:20 (84:24:8d:c1:24:20)
      Source address: ZebraTec_c1:24:20 (84:24:8d:c1:24:20)
      BSS Id: ZebraTec_c1:24:20 (84:24:8d:c1:24:20)
        .... .... 0000 = Fragment number: 0
        1001 1110 0000 .... = Sequence number: 2528
      Frame check sequence: 0x3aabf5bc [correct]
      [FCS Status: Good]

```

source : <https://dot11stream.com/2018/12/01/mac-address-to-ds-from-ds-in-a-wireless-frame/>

Diffusion (broadcast) en mode ad-hoc d'une trame balise (trame de gestion)

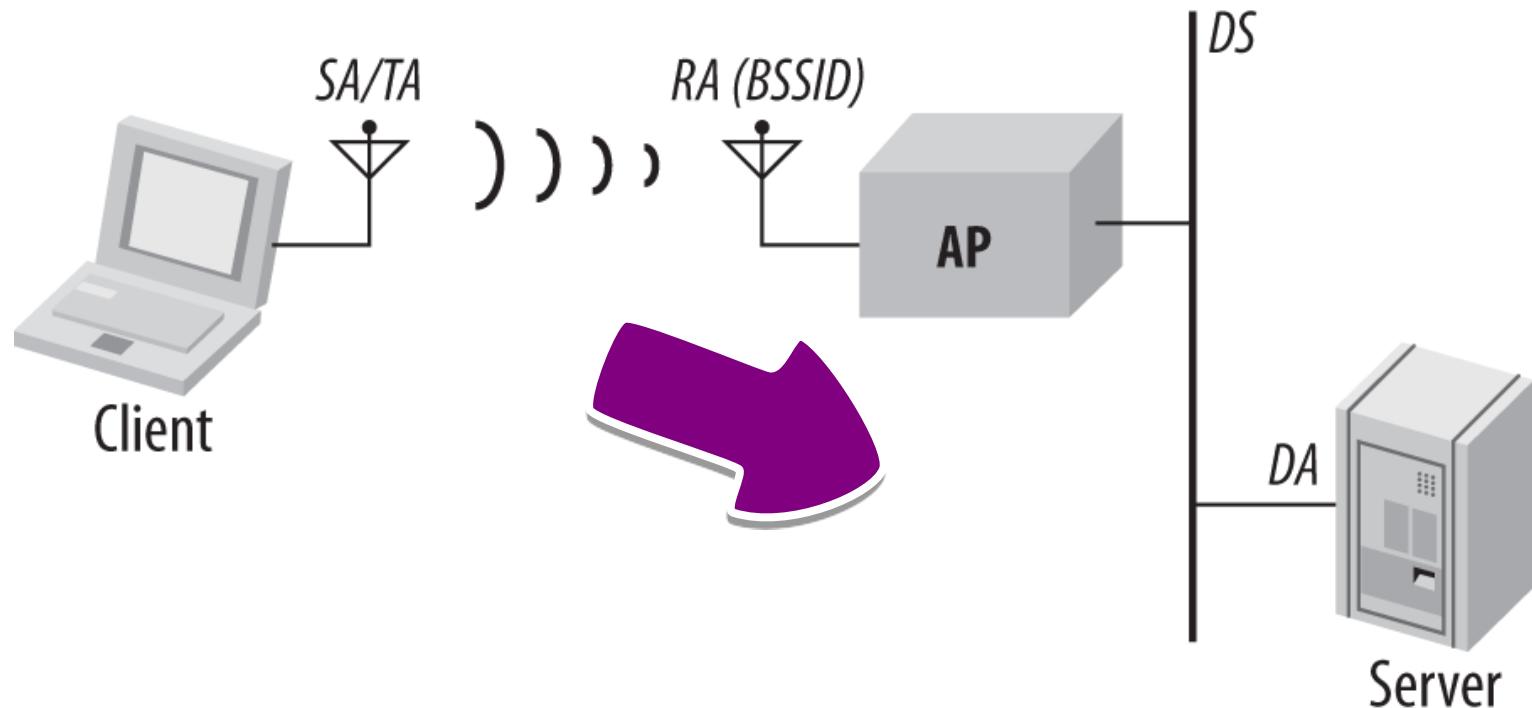
Trame balise envoyée depuis un AP en mode ad-hoc (SA=TA + BSSID), à toutes les stations (DA=RA).

- **Adresse 1 – DA=RA, ff:ff:ff:ff:ff:ff – adresse de diffusion**
- **Adresse 2 – SA=TA, 84:24:8d:c1:24:20 – BSSID de l'AP**
- **Adresse 3 – BSSID, 84:24:8d:c1:24:20 – BSSID de l'AP**

From / To DS – 5/13

From DS=0 et To DS=1

Mode	From DS	To DS	Adr1	Adr2	Adr3	Adr4
Vers DS	0	1	RA = BSSID	SA = TA	DA	-



Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

From / To DS – 6/13

From DS=0 et To DS=1

```

IEEE 802.11 OoS Data. Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8841
      .... .00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = subtype: 8
    Flags: 0x41
      ..... 01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .1.. .... = Protected flag: Data is protected
      0.... .... = Order flag: Not strictly ordered
      .000 0000 0011 0000 = Duration: 48 microseconds
      Receiver address: ZebraTec c1:24:20 (84:24:8d:c1:24:20)
      Transmitter address: Apple 1b:2d:fa (cc:44:63:1b:2d:fa)
      Destination address: BrocadeC 4f:02:76 (74:8e:f8:4f:02:76)
      Source address: Apple 1b:2d:fa (cc:44:63:1b:2d:fa)
      BSS Id: ZebraTec_c1:24:20 (84:24:8d:c1:24:20)
      STA address: Apple_1b:2d:fa (cc:44:63:1b:2d:fa)
      .... ..... 0000 = Fragment number: 0
      0010 0111 0110 .... = Sequence number: 630
      Frame check sequence: 0xe686c44a [correct]
      [FCS Status: Good]

```

source : <https://dot11stream.com/2018/12/01/mac-address-to-ds-from-ds-in-a-wireless-frame/>

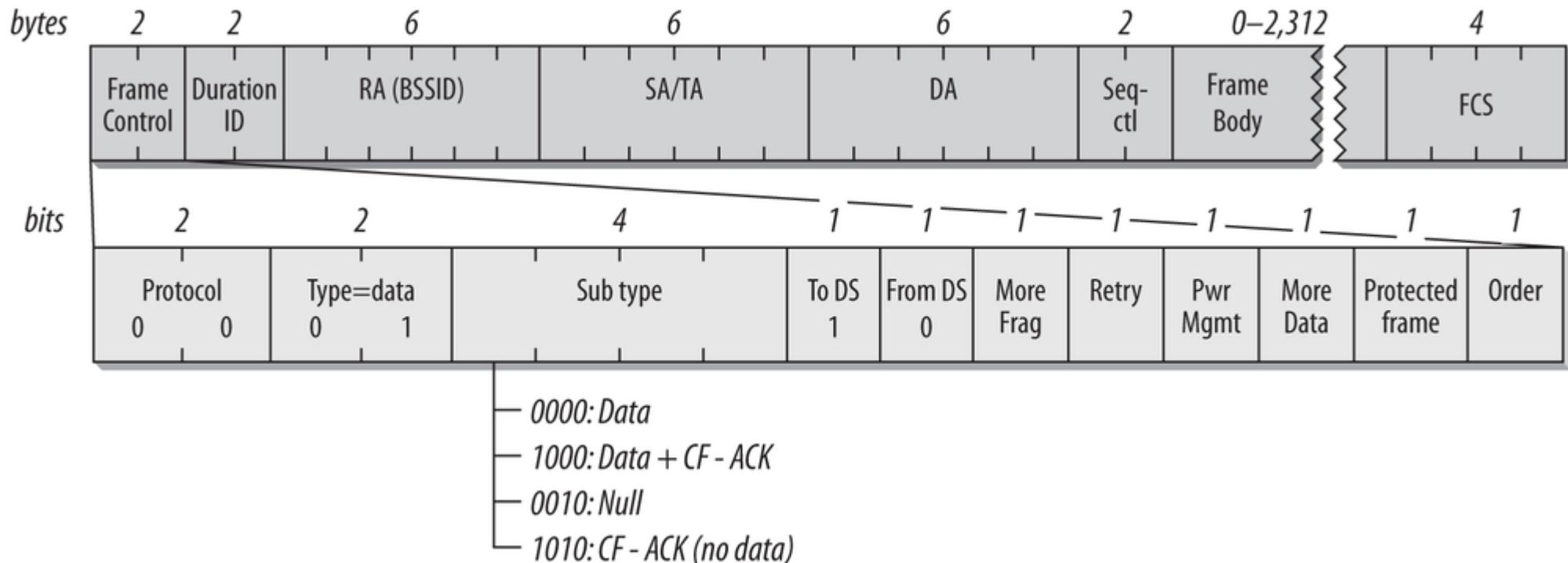
Écho ICMP vers une passerelle

Trame de donnée envoyée depuis le client (SA=TA), transitant par le point d'accès (RA=BSSID) et à destination finale d'une passerelle (DA)

- **Adresse 1 – RA=BSSID, 84:24:8d:c1:24:20 – BSSID de l'AP**
- **Adresse 2 – SA=TA, cc:44:63:1b:2d:fa – Station cliente**
- **Adresse 3 – DA, 74:8e:f8:4f:02:76 – passerelle**

From / To DS – 7/13

From DS=0 et To DS=1



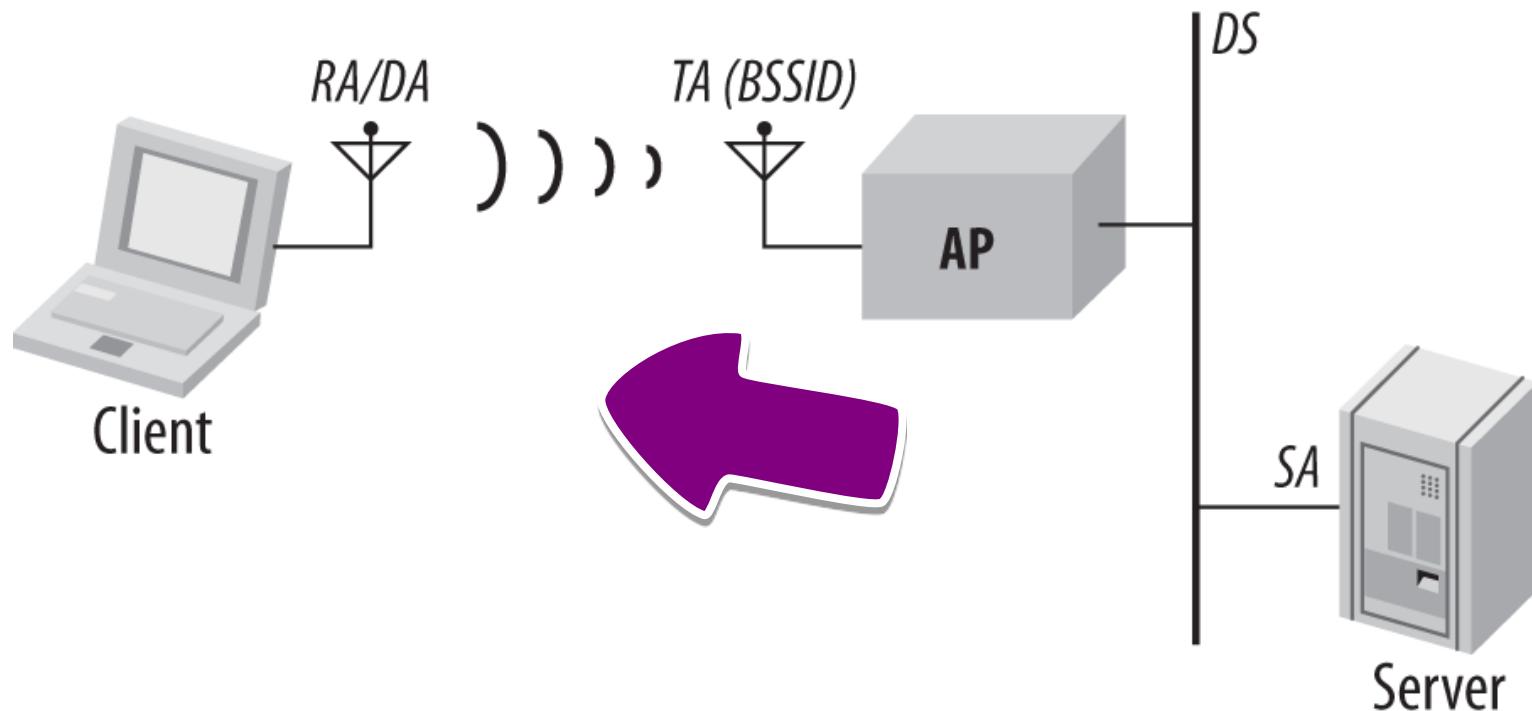
Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

- Les stations ne pouvant devenir des points d'accès (point coordinator), elles n'envoient jamais de trames contenant des fonctions de contention/compétition de type CF-Poll.

From / To DS – 8/13

From DS=1 et To DS=0

Mode	From DS	To DS	Adr1	Adr2	Adr3	Adr4
Depuis DS	1	0	DA = RA	BSSID = TA	SA	-



Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

From / To DS – 9/13

From DS=1 et To DS=0

```

▲ IEEE 802.11 OoS Data, Flags: .p....F.C
    Type/Subtype: QoS Data (0x0028)
    ▲ Frame Control Field: 0x8842
        .... .00 = Version: 0
        .... 10.. = Type: Data frame (2)
        1000 .... = Subtype: 8
    ▲ Flags: 0x42
        .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0.... .... = Order flag: Not strictly ordered
        .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Apple_1b:2d:fa (cc:44:63:1b:2d:fa)
    Transmitter address: ZebraTec_c1:24:20 (84:24:8d:c1:24:20)
    Destination address: Apple_1b:2d:fa (cc:44:63:1b:2d:fa)
    Source address: BrocadeC_4f:02:76 (74:8e:f8:4f:02:76)
    BSS Id: ZebraTec_c1:24:20 (84:24:8d:c1:24:20)
    STA address: Apple_1b:2d:fa (cc:44:63:1b:2d:fa)
        .... ..... 0000 = Fragment number: 0
        0010 0100 1101 .... = Sequence number: 589
    Frame check sequence: 0x2c7fdc80 [correct]
    [FCS Status: Good]

```

source : <https://dot11stream.com/2018/12/01/mac-address-to-ds-from-ds-in-a-wireless-frame/>

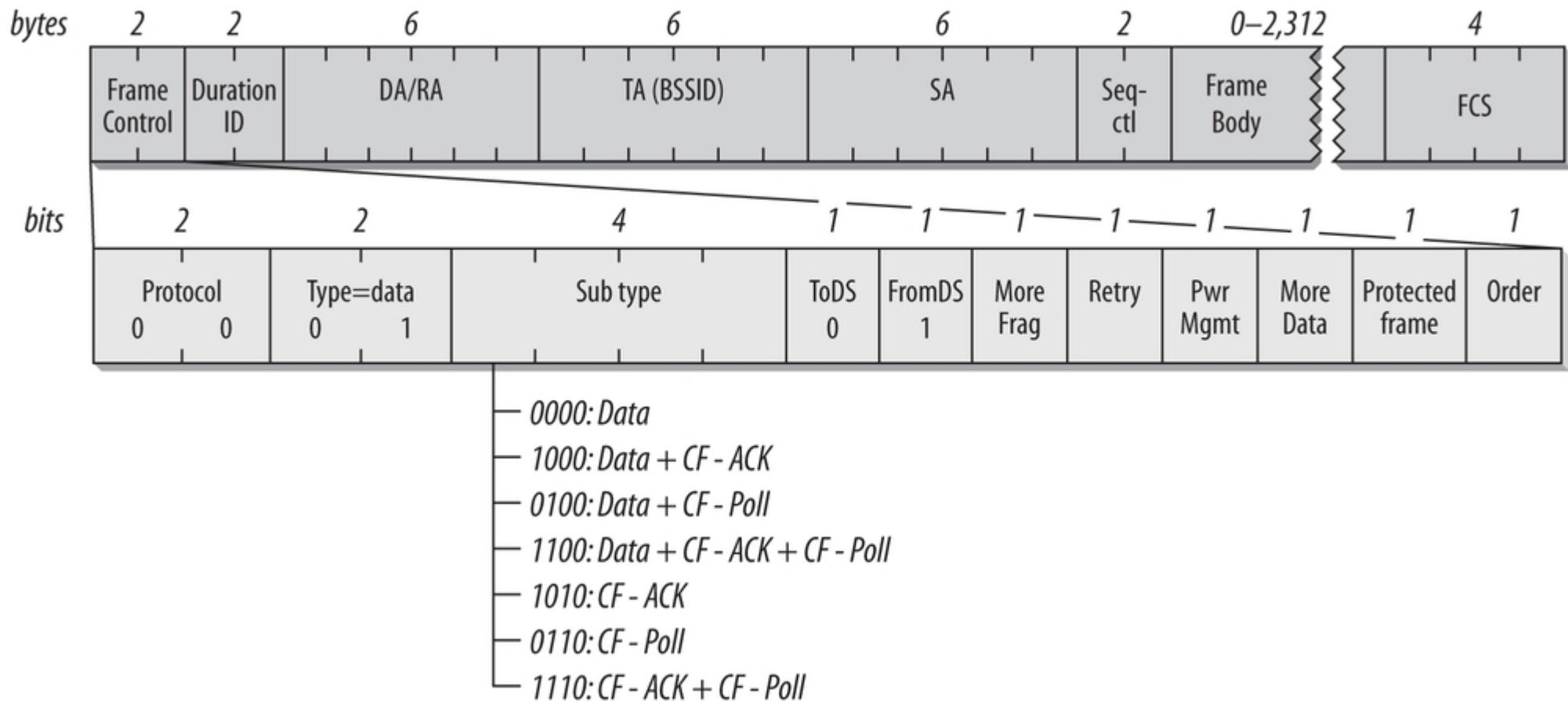
Envoi depuis le réseau filaire vers le réseau sans-fil

Réponse à un echo ICMP de la passerelle (SA) au client (DA=RA) en passant par le point d'accès (BSSID=TA)

- **Adresse 1 – DA=RA, cc:44:63:1b:2d:fa – Station cliente**
- **Adresse 2 – BSSID=TA, 84:24:8d:c1:24:20 – BSSID de l'AP**
- **Adresse 3 – SA, 74:8e:f8:4f:02:76 – passerelle**

From / To DS – 10/13

From DS=1 et To DS=0



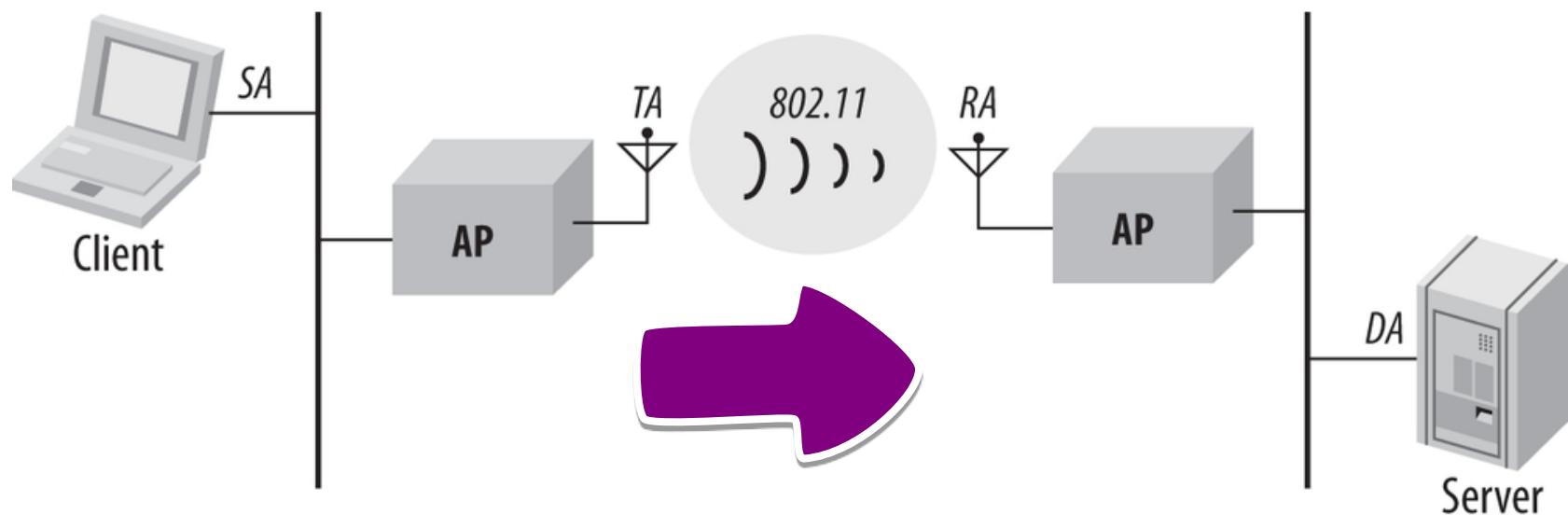
Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

- Le point d'accès n'étant jamais en veille, il n'envoie pas de trames Null aux stations. Les trames CF sont envoyées durant la période sans contention/compétition en mode PCF.

From / To DS – 11/13

From DS=1 et To DS=1

Mode	From DS	To DS	Addr1	Addr2	Addr3	Addr4
ESS	1	1	RA	TA	DA	SA



Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

From / To DS – 12/13

From DS=1 et To DS=1

```

▲ IEEE 802.11 QoS Data, Flags: .p.....FTC
  Type/Subtype: QoS Data (0x0028)
  ▲ Frame Control Field: 0x8843
    ..... 00 = Version: 0
    ..... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▲ Flags: 0x43
    ..... 11 = DS status: WDS (AP to AP) or Mesh (MP to MP) Frame (To DS: 1 From DS: 1) (0x3)
    ..... 0.. = More Fragments: This is the last fragment
    ..... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .1.. .... = Protected flag: Data is protected
    0... .... = Order flag: Not strictly ordered
    .000 0000 0011 0000 = Duration: 48 microseconds
  Receiver address: ArubaNet 65:64:30 (f0:5c:19:65:64:30)
  Transmitter address: ArubaNet 65:60:f1 (f0:5c:19:65:60:f1)
  Destination address: Apple 1b:2d:fa (cc:44:63:1b:2d:fa)
  Source address: BrocadeC 4f:02:76 (74:8e:f8:4f:02:76)
  BSS Id: ArubaNet_65:60:f1 (f0:5c:19:65:60:f1)
    ..... .... 0000 = Fragment number: 0
  0100 0111 0110 .... = Sequence number: 1142
  Frame check sequence: 0xee906918 [correct]
  [FCS Status: Good]

```

source : <https://dot11stream.com/2018/12/01/mac-address-to-ds-from-ds-in-a-wireless-frame/>

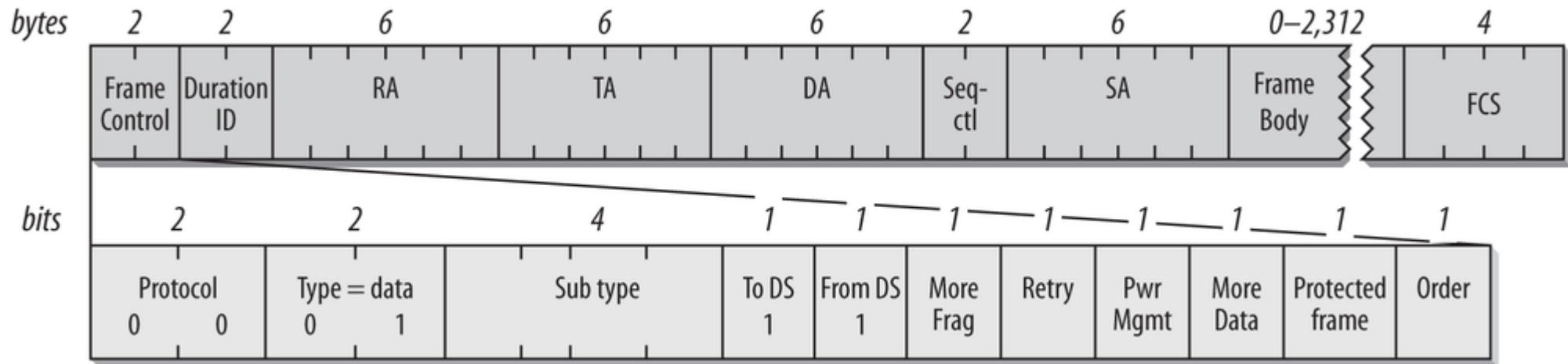
Envoi dans le système de distribution

Réponse à un echo ICMP de la passerelle (SA) au client (DA) en passant par le transmetteur (TA) puis le récepteur (RA)

- **Adresse 1 – RA, f0:5c:19:65:64:30 – AP/MP destination**
- **Adresse 2 – TA, f0:5c:19:65:60:f1 – AP/MP source**
- **Adresse 3 – DA, cc:44:63:1b:2d:fa – station cliente destinatrice**
- **Address 4 – SA, 74:8e:f8:4f:02:76 – passerelle source**

From / To DS – 13/13

From DS=1 et To DS=1

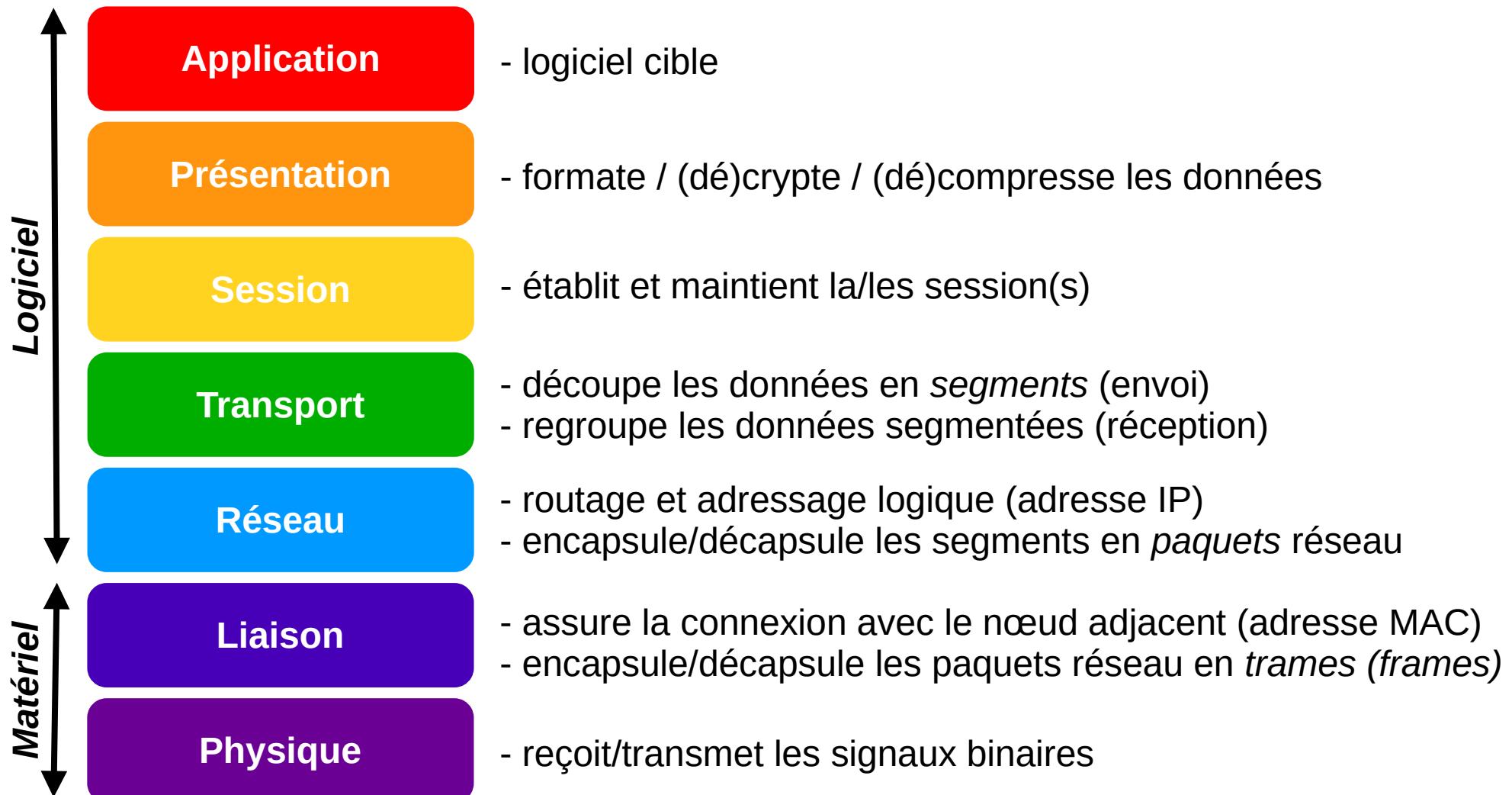


Source : <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

- Dans un WDS, les points d'accès ne pouvant entrer en veille, le bit Pwr Mgmt est toujours à 0.
- Pour les trames chiffrées, le bit Protected frame est mis à 1, et le chiffrement utilisé est indiqué au début du champ Frame Body

Rappel des 7 couches OSI

(Open System Interconnection)



Mais où est le WiFi ?

Application

- Telnet, SSH, FTP, DNS, DHCP, HTTP, IMAP, POP3, SMTP, SMB, SIP, ...

Présentation

- ASCII, MIME, Unicode, ...

Session

- SOCKS, TLS, H.323, ...

Transport

- TCP, UDP, RTP, ...

Réseau

- IPv4, IPv6, ARP/RARP, ICMP, IGMP, BOOTP, RIP, ...

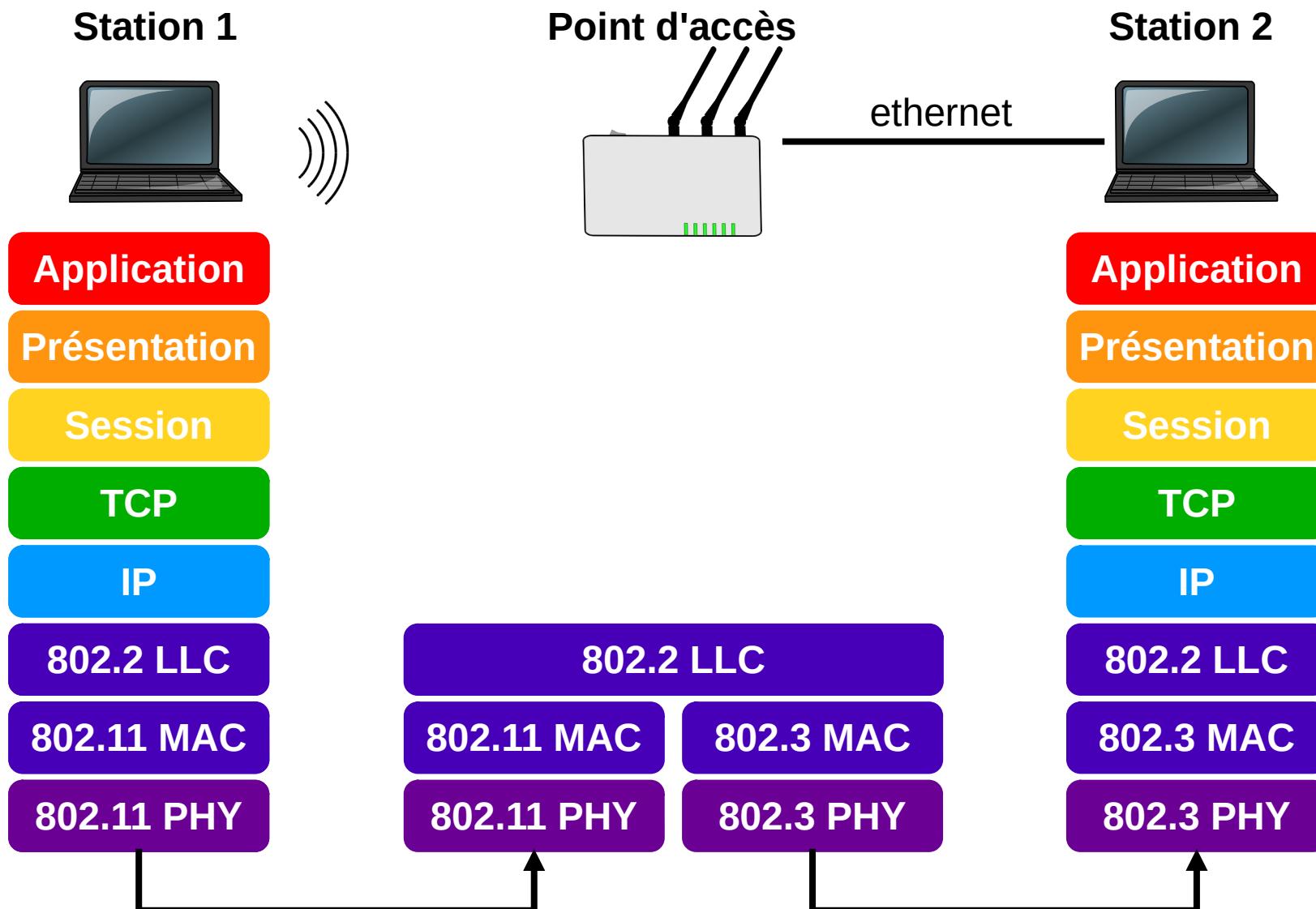
Liaison

- adresse MAC, ESSID, WEP/WPA/WPA2/WPA3

Physique

- canal, vitesse, modulation

Le point d'accès sans fil



Couches LLC / MAC / PHY



- **FHSS** : Frequency-Hopping Spread Spectrum
- **IR** : Infrared
- **HR/DSSS** : *High Rate / Direct Sequence Spread Spectrum*
- **OFDM** : *Orthogonal Frequency Division Multiplexing*
- **ERP** : *Extended Rate PHY*
- **MIMO** : *Multiple-Input Multiple-Output*

Sous-couches PHY

PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent

La couche PHY est séparée en deux :

- **PLCP** gère l'écoute du support et signale à la couche MAC quand le support est libre (via un Clear Channel Assessment).
- **PMD** gère l'encodage des données et la modulation finale.

La couche 802.11 MAC – 1/11

fonction de coordination DCF

- **DCF = Distributed Coordination Function**
(fonction de coordination distribuée)
- **Avantages :**
 - Présente dans tous les AP du commerce
 - Convient bien aux données asynchrones
 - Permet un accès équitable côté stations
- **Inconvénients :**
 - **pas de QoS = Quality of Service** (qualité de service)
 - risque élevé de collisions si RTS/CTS non activé
(optionnel par défaut)

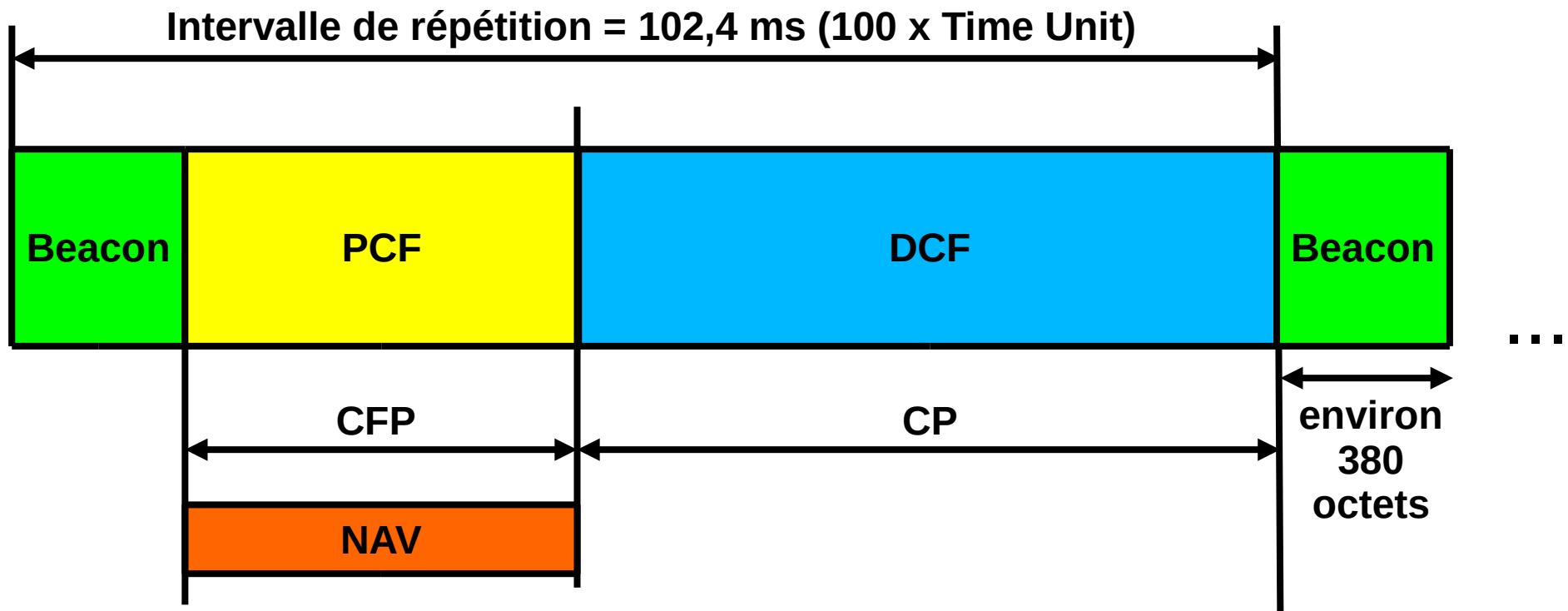
La couche 802.11 MAC – 2/11

fonction de coordination PCF

- **PCF = Point Coordination Function** (fonction de coordination par point)
- L'AP interroge les stations associées en PCF à tour de rôle (**polling**) en jouant le rôle d'arbitre.
- Pour rester compatible avec les stations ne supportant pas le mode PCF, l'AP définit 2 périodes entre chaque trame balise (beacon) :
 - une **Contention Free Period (CFP)**, ou période sans compétition (ou contestation/dispute), où l'AP prend la main sur les stations.
 - une **Contention Period (CP)** qui utilise la DCF classique (accès distribué avec compétition).

La couche 802.11 MAC – 3/11

Coexistence entre PCF et DCF



Le NAV de la trame balise neutralise les stations en DCF durant la CFP.

P.S. : les trames balises sont toujours envoyées au débit le plus bas pour assurer la rétrocompatibilité...

La couche 802.11 MAC - 4/11

fonction de coordination PCF

- À noter que les trames **PCF** (beacon ou CF-XXX) utilisent un espace inter-trame **PIFS** (= PCF IFS = SIFS + 1 Slot Time) tel que **SIFS < PIFS < DIFS**.
- Ainsi, les trames PCF sont toujours prioritaires sur les trames DCF !
- Avantages :
 - Garantit un accès équitable entre stations en PCF.
 - Reste compatible avec les stations en DCF.
- Inconvénients :
 - pas de QoS, juste une meilleure synchronisation.
 - Implémentation optionnelle chez les fabricants.

L'EIFS : un *intervalle inter-trames particulier*

Extended IFS

- Quand une station reçoit une trame qu'elle n'est pas capable de décoder, elle substitue le DIFS par l'EIFS avant de retenter une transmission.
- **EIFS = SIFS + DIFS + temps de transmission d'un ACK au débit le plus bas**
- L'idée ici est que la trame reçue peut être valide pour une autre station : il faut donc laisser le temps à l'autre station de réagir (ACK)...

La couche 802.11 MAC – 5/11

fonction de coordination EDCA

- **EDCA = Enhanced DCF Channel Access**
- Reprend le principe de la DCF en introduisant **8 classes de trafic** (ou TC = Trafic Classes – cf. 802.1p) et **4 priorités d'accès** (ou AC = Access Categories – cf. 802.11e) : Voice (AC_VO) > Video (AC_VI) > Best effort (AC_BE) > Background (AC_BK).
- Utilise le protocole **TMCA** (une variation de CSMA/CA) dans lequel le **DIFS** est remplacé par un **temporisateur AIFS** (Arbitration IFS), variable suivant le type de flux. Ainsi, SIFS < AIFS(AC_VO) < AIFS(AC_VI) < AIFS (AC_BE) < AIFS(AC_BK).

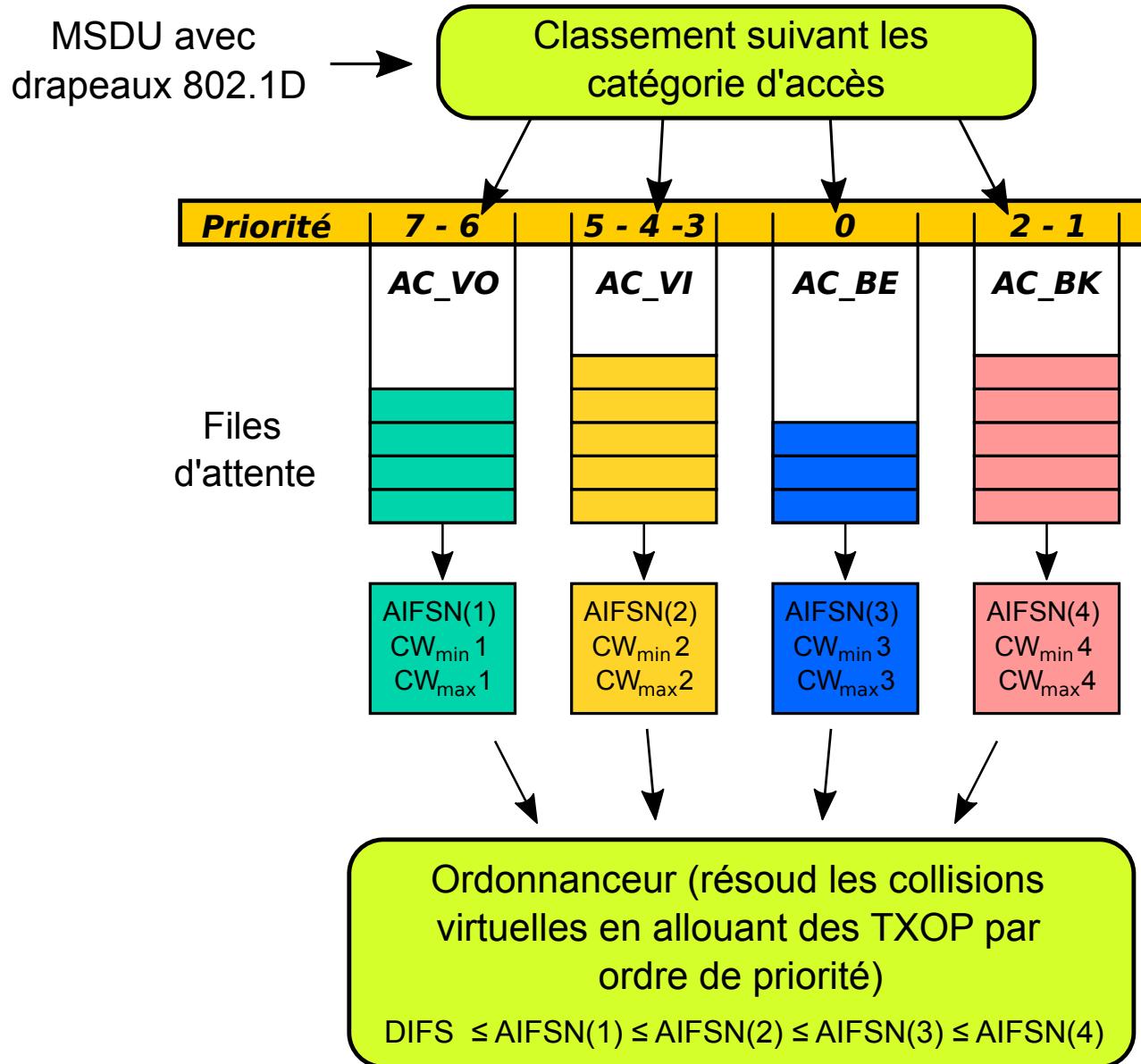
La couche 802.11 MAC – 5/11

QoS – les catégories d'accès

Priorité	Priorité utilisateur 802.1D	Désignation 802.1D	AC / Access Categories 802.1e	Type de trafic
faible	1	BK / Background	AC_BK	tâche de fond
	2	- / Spare	AC_BK	tâche de fond
	0	BE / Best Effort	AC_BE	meilleur effort
	3	EE/ Excellent Effort	AC_BE	meilleur effort
	4	CL/ Controlled Load	AC_VI	vidéo
	5	VI/ Video	AC_VI	vidéo
↓	6	VO / Voice	AC_VO	voix
élevée	7	NC / Network Control	AC_VO	voix

La couche 802.11 MAC – 5/11

QoS – les catégories d'accès



- MSDU : Mac Service Data Unit (trame ethernet avec Destination Adress / Source Adress / Type / Data)**

La couche 802.11 MAC – 6/11

fonction de coordination EDCA

- **EDCA** Introduit également les **TXOP** (Transmission Opportunities), qui définissent le droit d'accès d'une station et son **temps alloué en fonction de son niveau de priorité**.
- Une opportunité de transmission peut être demandée par une station (Reservation Request), et offerte par l'AP via une trame **CF-Poll**, contenant le temps de transmission accordé. Après un SIFS, la station retenue peut répondre avec un paquet QoS-Data si elle a des données à transmettre, sinon par un paquet QoS-Null.
- La méthode **Contention Free Burst** (salve de données) permet d'envoyer plusieurs trames QoS-Data acquittées côté réception, pendant toute la durée de la TXOP offerte.

La couche 802.11 MAC – 7/11

fonction de coordination EDCA

- Avantages :
 - EDCA introduit une **ébauche de qualité de service**, basée sur des catégories de trafic.
 - Offre plus de souplesse aux stations via les **opportunités de transmission**.
- Inconvénients :
 - La QoS n'est pas parfaite : **les flux de même priorité seront concurrents**
 - on retrouve la **compétition d'accès au medium** de la DCF de base.

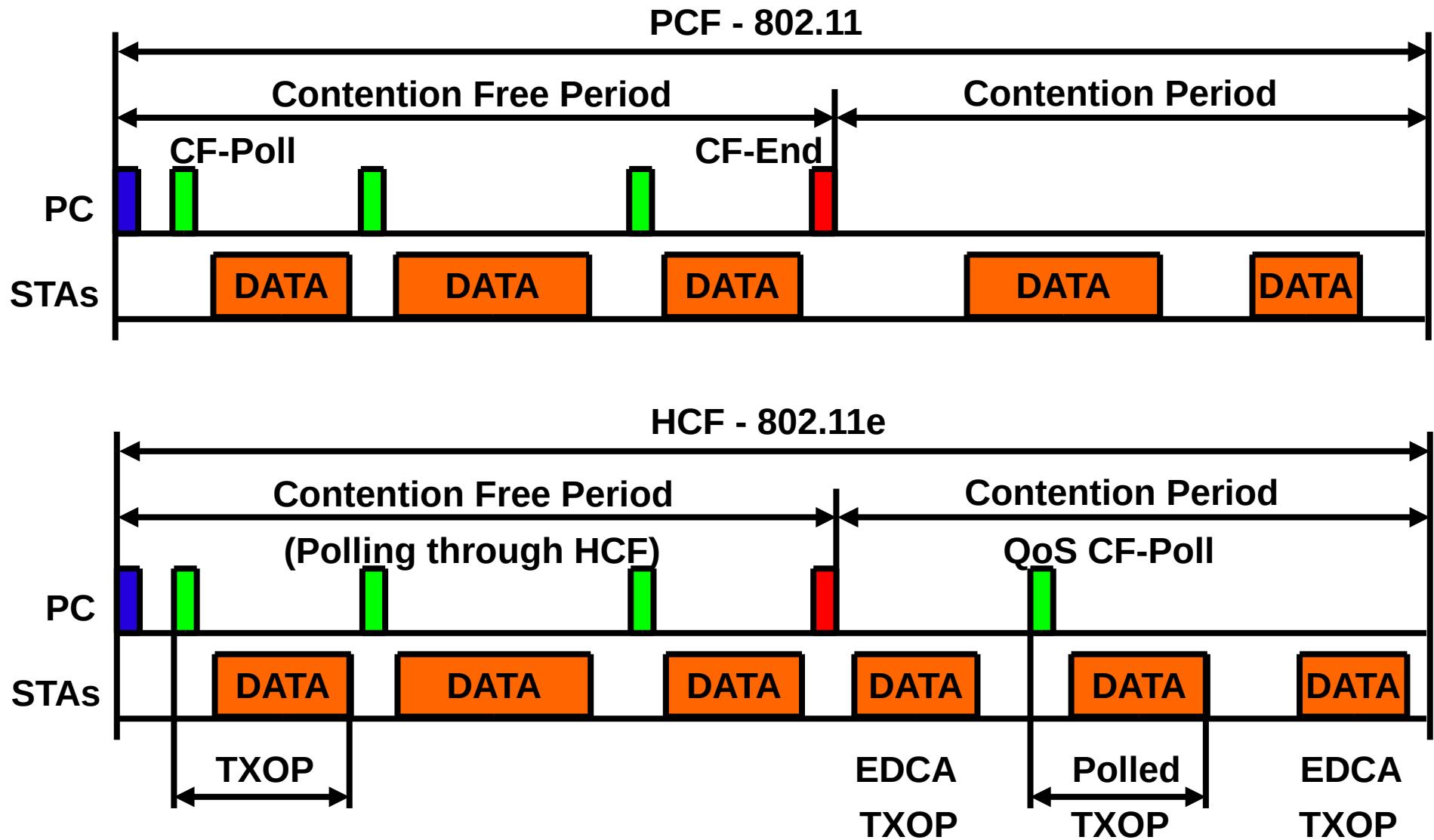
La couche 802.11 MAC – 8/11

fonction de coordination HCCA

- **HCF** = Hybrid Coordination Function ou EPCF (Enhanced PCF)
- **HCCA** = HCF Channel Access est la plus complexe des fonctions de coordination.
- Reprend le mécanisme de **polling** de la PCF, y ajoute les **TXOP**, **les classes de flux et de trafic**, et permet d'initier une **CFP** durant une **CP**, pour envoyer ou recevoir des données à tout moment.
- Pendant la CP, les stations travaillent en EDCA.

La couche 802.11 MAC – 9/11

comparaison entre PCF et HCF



Attention : PC = Point Coordinator (point d'accès ici)

La couche 802.11 MAC – 10/11

fonction de coordination HCCA

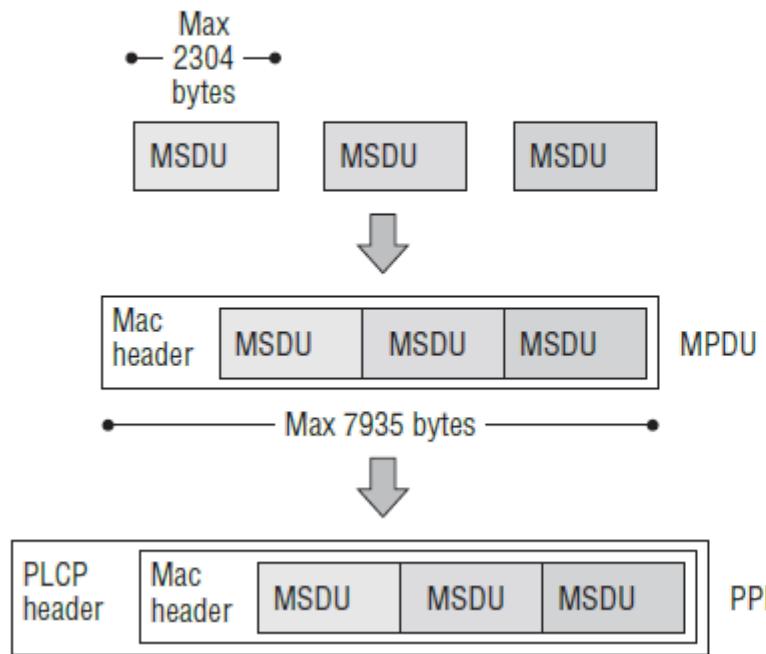
- Avantages :
 - **HCCA** permet théoriquement d'améliorer la **QoS** via un **HC** (= Hybrid Coordinator - ici notre AP), qui peut envoyer ses données à tout moment.
- Inconvénients :
 - Impose le support de l'**EDCA**, pour les stations qui ne supportent pas l'**HCCA**.

Autres spécifications QoS

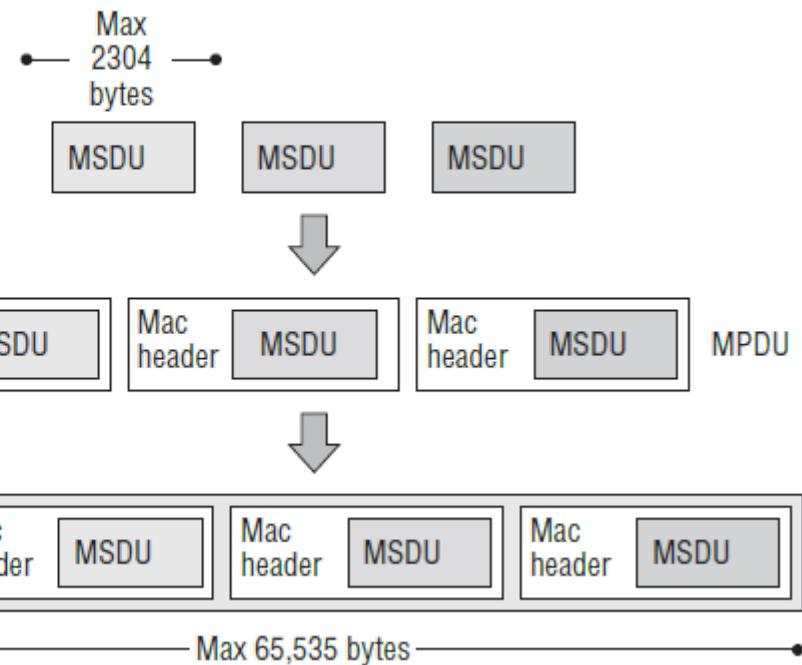
L'agrégation de trames

BA (Block Acknowledgements) ou acquittements groupés : on agrège les données en A-MSDU (Aggregation Service Data Unit) ou A-MPDU (Aggregation MAC Protocol Data Unit), que l'on envoie dans une **TXOP**, acquittée par un **Block ACK**.

A-MSDU frame aggregation



A-MPDU frame aggregation



Source : <https://inet.omnetpp.org/docs/showcases/wireless/aggregation/doc/index.html>

Autres spécifications QoS

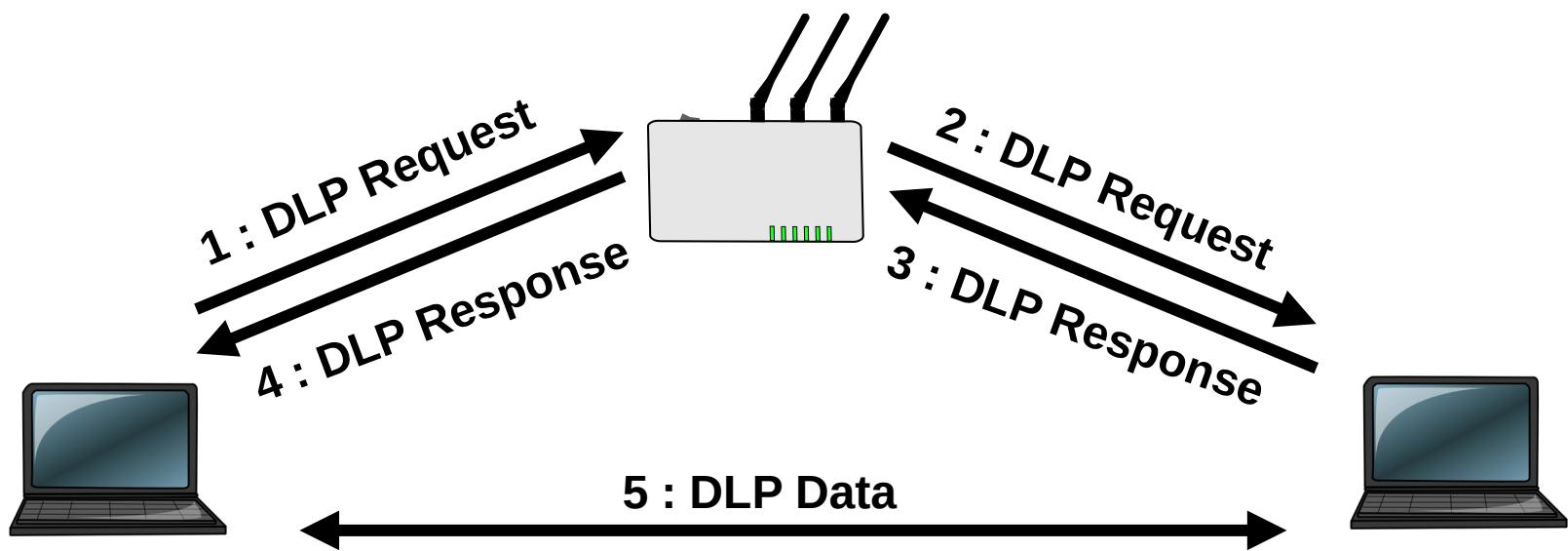
L'agrégation de trames

- **NoAck (No Acknowledgement)** : Permet la mise en place de classes de services avec **QoSAck** ou **QoSNoAck**. Dans ce dernier cas, les messages transmis ne seront pas acquittés.
- Respect des échéances **TBTT (Target Beacon Transmission Time)** annoncées dans les trames balises. Une station qui veut transmettre ses données vérifie que le temps total de transmission (avec ACK) ne dépassera cette valeur. On garantit ainsi des **CFP régulières**.

Autres spécifications QoS

Le protocole de lien direct

- Le **DLP (Direct Link Protocol)** de 802.11e donne la possibilité aux stations proches de s'envoyer directement des données.
- Seule la phase d'initialisation (DLP Request / DLP Response) passe par l'AP



La couche 802.11 MAC – 11/11

Résumé des 4 fonctions de coordination

Fonction de coordination	DCF	PCF	EDCA	HCCA
Type d'IFS	DIFS	PIFS	AIFS	AIFS
CP	x	x	x	x
CFP		x		x
TXOP			x	x
QoS			x	x

Les différents types d'antenne

- **Omnidirectionnelles** (ou isotropiques) : tige, dipôle (lobes en 2D ou tore en 3D), ...
- **Directionnelles** : panneau, parabole, Augmente le gain dans une direction.
- **Le gain définit l'augmentation de puissance émise ou reçue dans le lobe principal**, et s'exprime en dBi (décibels par rapport à l'antenne isotrope).
- Dans tous les cas, la **PIRE** (Puissance Isotrope Rayonnée Équivalente) est **limitée**.

Les phénomènes dispersifs

- **polarisation des antennes** : verticale, horizontale ou les deux par rapport à la terre.
- il faut que l'émetteur et le récepteur soient polarisés dans la **même direction**.
- problème des **interférences destructives** suivant le trajet de l'onde (réflections).
- problèmes d'**absorption de l'environnement** immédiat (murs, cloisons, ...).

Puissances maximales en intérieur

source ARCEP

- Dans la bande ISM : PIRE maxi = 100mW.
- Dans la bande U-NII :

Fréquences (Mhz)	Limite de PIRE moyenne maximale autorisée	Techniques d'atténuation
5150-5250	200 mW	-
5250-5350	200 mW si régulateur de puissance	obligatoires (norme harmonisée EN 301 893 de l'ETSI)
	100 mW sinon	
5470-5725	1W si régulateur de puissance	
	500 mW sinon	

Bandes U-NII – 5 Ghz - 2/3

WiFi 2 / 802.11a – WiFi 4 / 802.11n - WiFi 5 /802.11ac – WiFi 6 / 802.11ax – WiFi 7 / 802.11be

CONDITIONS ET SPÉCIFICATIONS TECHNIQUES

Dans la bande 5150 – 5250 MHz	Dans la bande 5250 – 5350 MHz	Dans la bande 5470 – 5725 MHz
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Limitation à une utilisation en intérieur <input checked="" type="checkbox"/> PIRE maximale autorisée : 200 mW 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Limitation à une utilisation en intérieur <input checked="" type="checkbox"/> PIRE max. autorisée : 200 mW avec TPC 100 mW sans TPC <input checked="" type="checkbox"/> Obligation de disposer d'un DFS 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Possibilité d'utilisation en intérieur et en extérieur <input checked="" type="checkbox"/> PIRE max. autorisée : 1 W avec TPC 500 mW sans TPC <input checked="" type="checkbox"/> Obligation de disposer d'un DFS



RLAN ou « Radio Local Area Network » : réseau local radioélectrique
TPC ou « Transmitter Power Control » : système de régulation de puissance
DFS ou « Dynamic Frequency Selection » : système dynamique de sélection de fréquences
PIRE : Puissance Isotrope Rayonnée Équivalente

source : <https://www.nextinpath.com/article/30126/108816-quand-reseaux-wi-fi-viennent-perturber-previsions-meteo>