

Wi-Fi avancé

Gérard Chalhoub

gerard.chalhoub@uca.fr

BUT 3 Réseaux et Télécommunications

Objectifs de ce cours

- Etudier l'évolution des différentes versions de WiFi (IEEE 802.11)
- Comprendre les mécanismes utilisés au niveau des couches physiques et MAC
- Avoir les bons réflexes d'analyse pré-déploiement et post-déploiement

Organisation du cours

- 9 heures de cours
- 2 heures d'examen
- 18 heures de TP
- 3 heures d'examen de TP

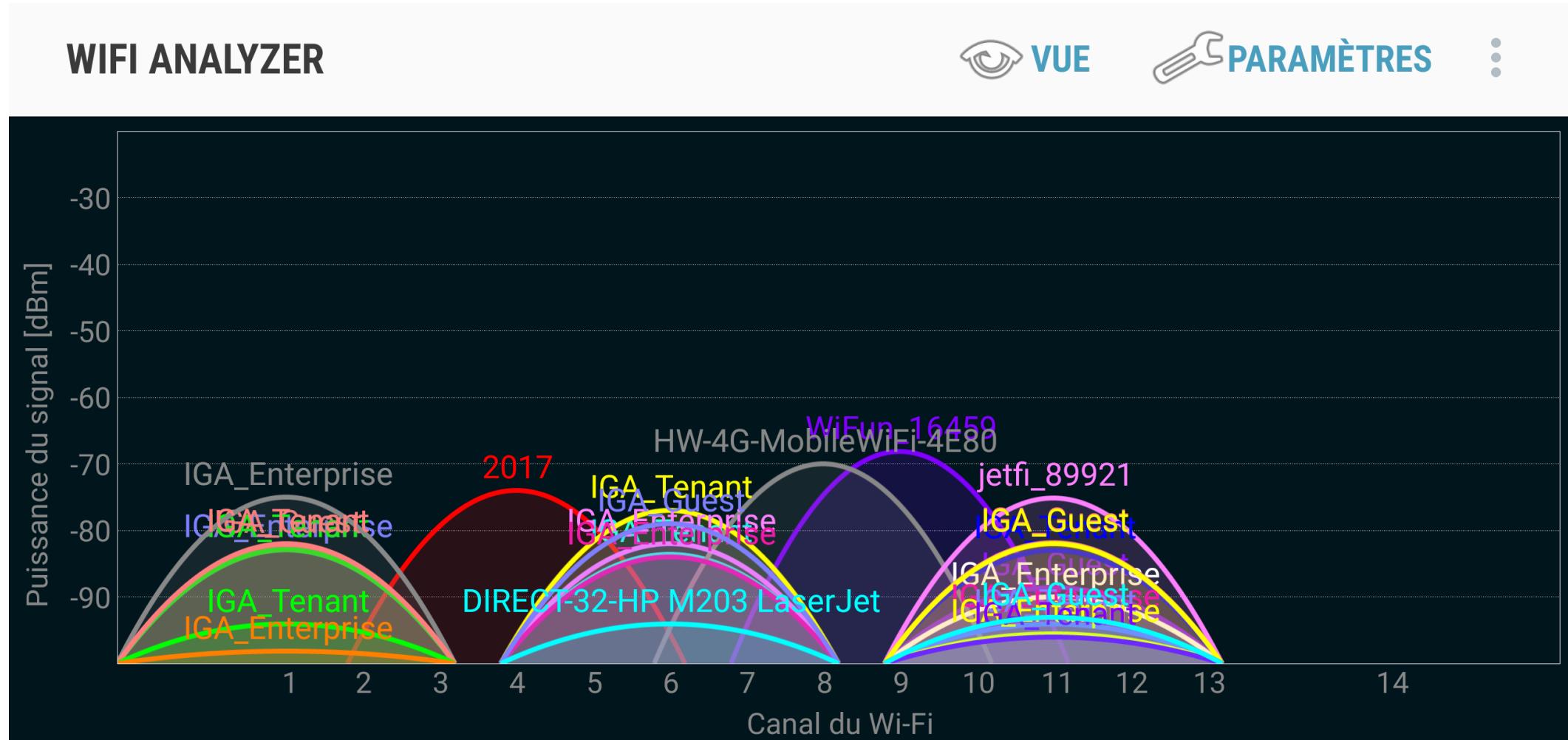
Contenu du cours

- Evolution des différentes versions de 802.11
- Propagation, collision, capture, CSMA/CA
- Terminal caché/terminal exposé
- Mécanismes de gestion du réseau : association, beacon, authentification, probe request/response
- Gestion des priorités : 802.11e

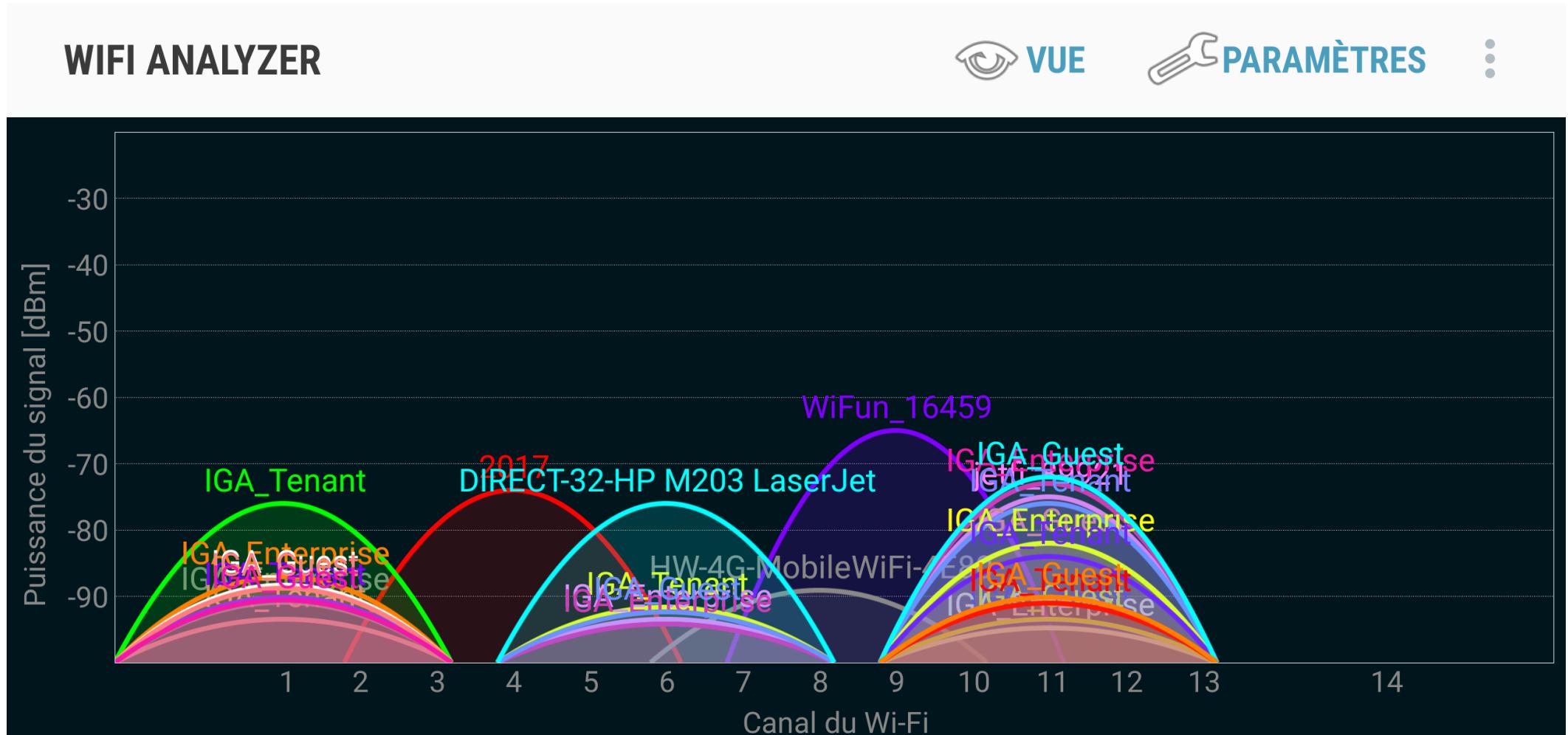
Problème

- Pourquoi le WiFi n'atteint pas les performances annoncées ? (surtout en débit)

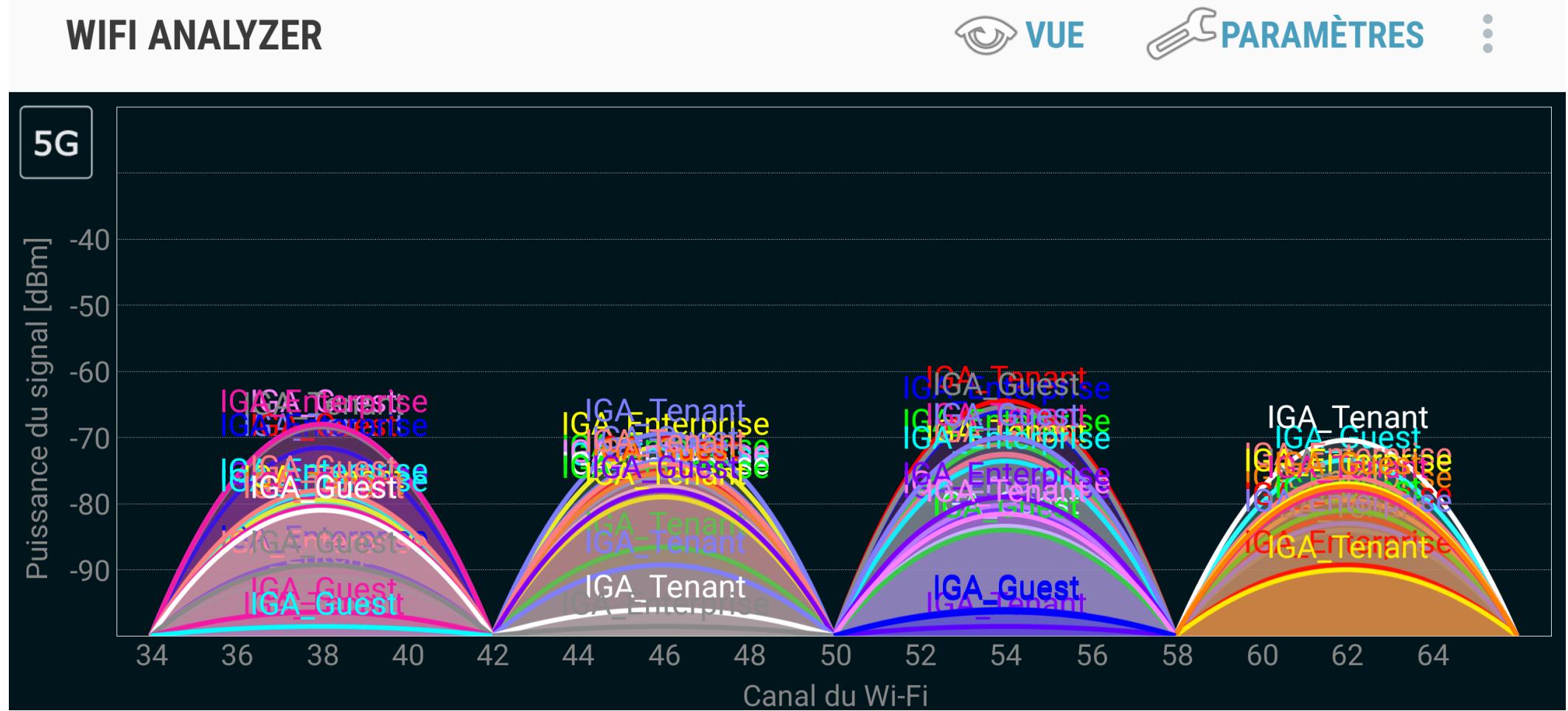
Exemple de réseaux WiFi par canal en 2.4 GHz



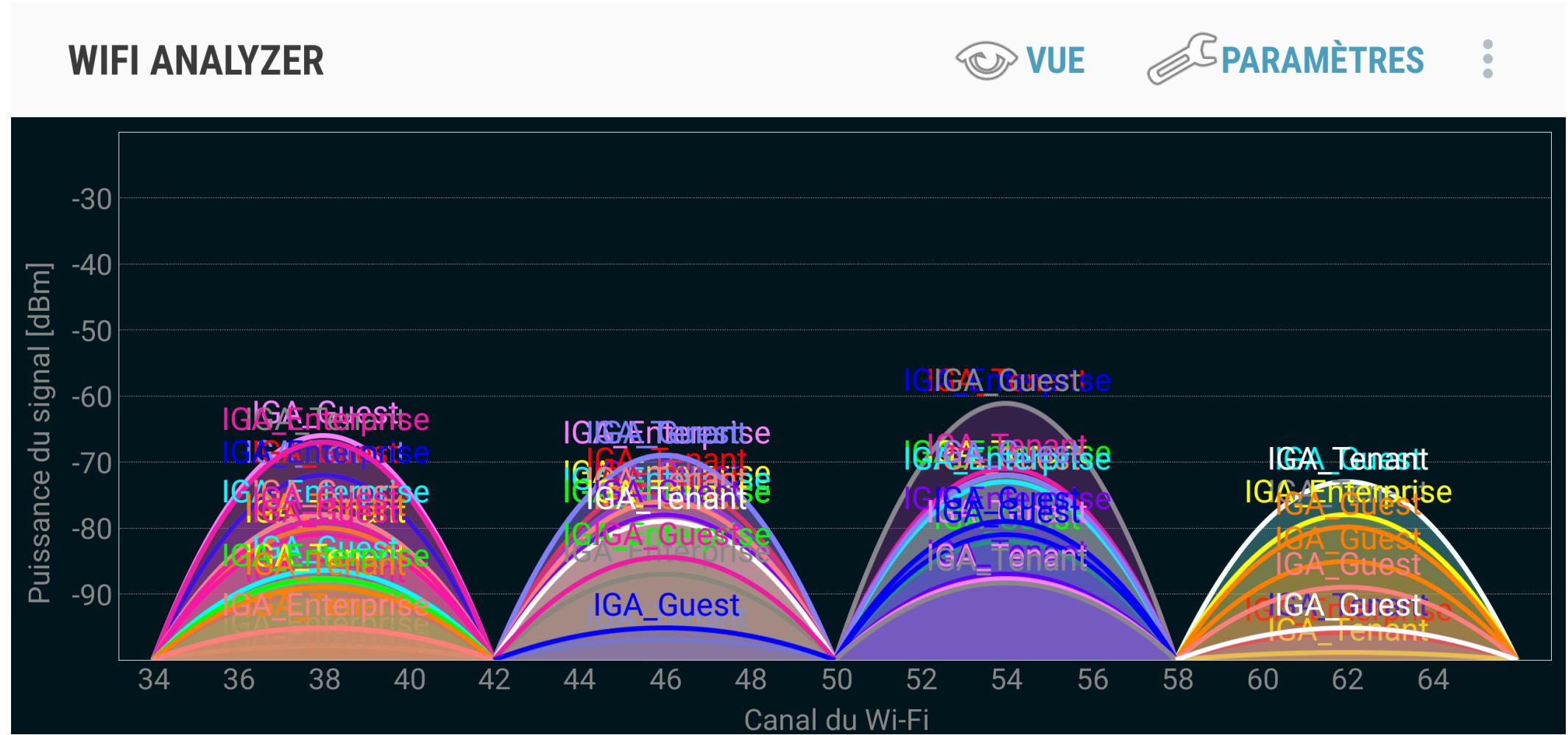
Exemple de réseaux WiFi par canal en 2.4 GHz



Exemple de réseaux WiFi par canal en 5 GHz

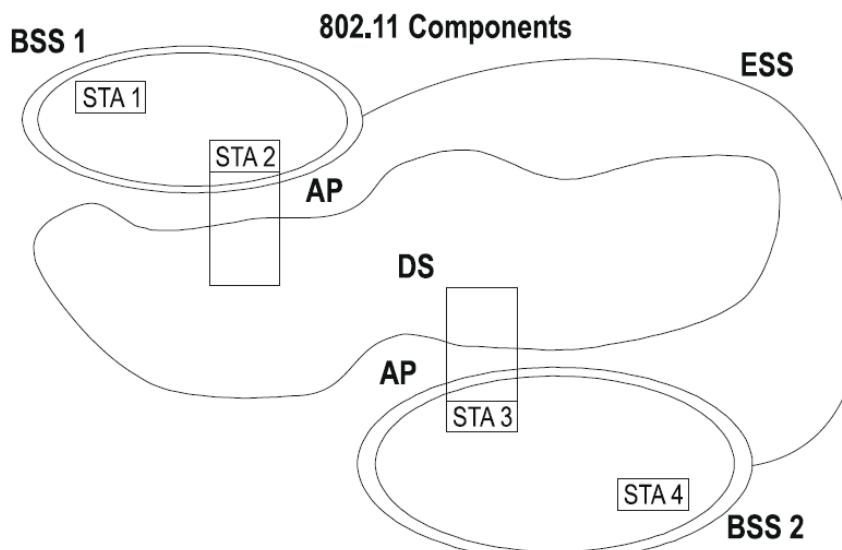


Exemple de réseaux WiFi par canal en 5 GHz



Architecture d'un réseau WiFi

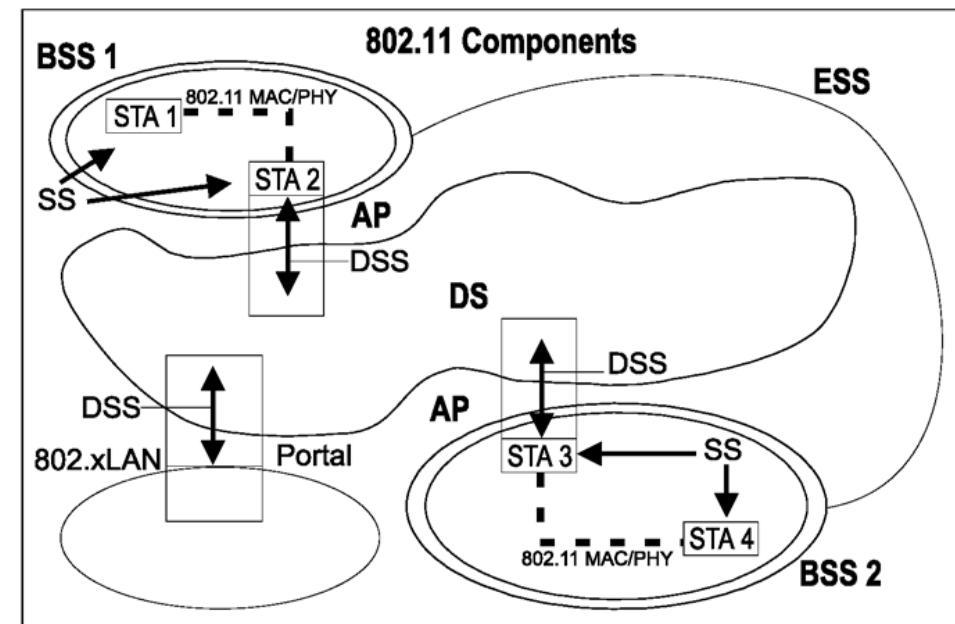
- BSS : Basic Service Set. Cela définit une zone géographique dans laquelle les stations peuvent communiquer entre elles
- DS : Distribution System. Permet de relier des BSS entre eux.
- DSS : Distribution Service System. L'ensemble des services permettant à une station de rejoindre un BSS et communiquer au sein d'un DS
- ESS : Extended Service Set. C'est la constitution d'un réseau étendu au-delà de la portée physique de deux nœuds (multiples BSS faisant partie d'un même LAN)



- Un AP permet aux stations d'intégrer un DS à travers les services du DSS
- Un AP est aussi vu comme une station capable de faire le lien entre un BSS et DS

Distribution Service System

- Un ensemble de services est défini afin de garantir l'acheminement des trames au sein d'un ESS
- C'est ce qui permet à la station 1 de joindre la station 4
- La norme 802.11 ne spécifie pas comment la distribution des trames doit se faire, mais fournit les éléments nécessaires pour le faire



Par quels équipements passe une trame générée par STA1 à destination de la STA4 ?

Types de trames et mobilité

- Il existe 3 types de trames dans un réseau 802.11 :
 - Trames de données : contiennent les données des niveaux supérieurs
 - Trames de gestion : utilisées pour assurer les différents services
 - Trames de contrôle : utilisées pour assurer l'acheminement des trames de données et de gestion
- Il existe trois niveaux de mobilité dans un réseau 802.11 :
 - Sans transition : la station reste au sein d'un BSS
 - Transition BSS : la station passe d'un BSS à un autre au sein d'un même ESS
 - Transition ESS (permis mais non géré par 802.11) : la station passe d'un BSS dans un ESS à un autre BSS dans un autre ESS

Mécanismes de gestion d'association

- Association : ce mécanisme permet d'identifier l'AP à contacter pour joindre la station
 - Cela crée un mappage entre la station et l'AP
 - Une station ne peut être associée qu'à un seul AP à la fois
 - La demande d'association est initiée par la station
- Réassociation : ce mécanisme permet à une station de changer d'AP au sein d'un ESS
 - Cela met à jour le mappage entre la station et son AP
 - La demande de réassociation est initiée par la station
- Désassociation : Ce mécanisme permet de supprimer une association
 - Cela supprime le mappage entre la station et son AP
 - La demande se fait par la station ou l'AP
 - La demande est à titre informative (elle ne peut pas être refusée)

Evolution de WiFi (mode infrastructure)

Version	Norme IEEE	Année	Fréquence (GHz)	Largeur de bande (MHz)	Débit max (Mbps)
WiFi 1	802.11b	1999	2.4	22	11
WiFi 2	802.11a	1999	5	5/10/20	54
WiFi 3	802.11g	2003	2.4	5/10/20	54
WiFi 4	802.11n	2009	2.4/5	20/40	288.8/600
WiFi 5	802.11ac	2013	5	20/40/80/160	770.4/1 600/3 466.8/6 933.6
WiFi 6	802.11ax	2019	2.4/5	20/40/80/160	10 530 (10.53 Gbps)

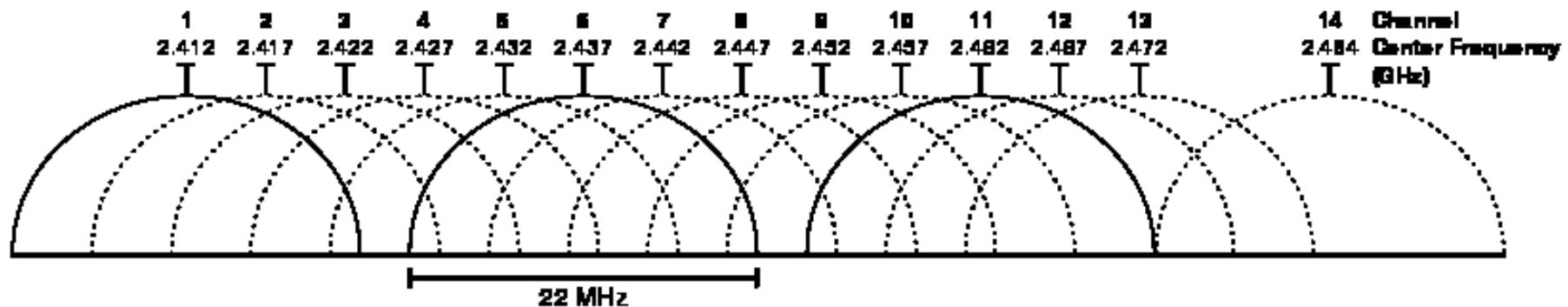
802.11-1997

- Avant 802.11b il y a eu 802.11 en 1997 (dénommé 802.11-1997)
- Le débit maximal de 802.11-1997 est de 2 Mbps
- Cette version utilise l'un des mécanismes de transmission suivants:
 - DSSS (BPSK, QPSK)
 - Infrarouge
 - FH (Frequency Hopping), saut de fréquences
- 802.11-1997 a aussi défini le fameux CSMA/CA qui est toujours utilisé aujourd'hui
- La bande de fréquences utilisée : 2.4GHz

WiFi 1 (802.11b-1999)

- Amélioration par rapport à 802.11-1997
 - 802.11b annonce un débit maximal de 11 Mbps
 - 802.11b adopte DSSS comme technique de transmission
 - Complementary Code Keying (64 CCK)
 - Modulations : BPSK, QPSK
 - Adaptation du débit en fonction de la qualité du lien

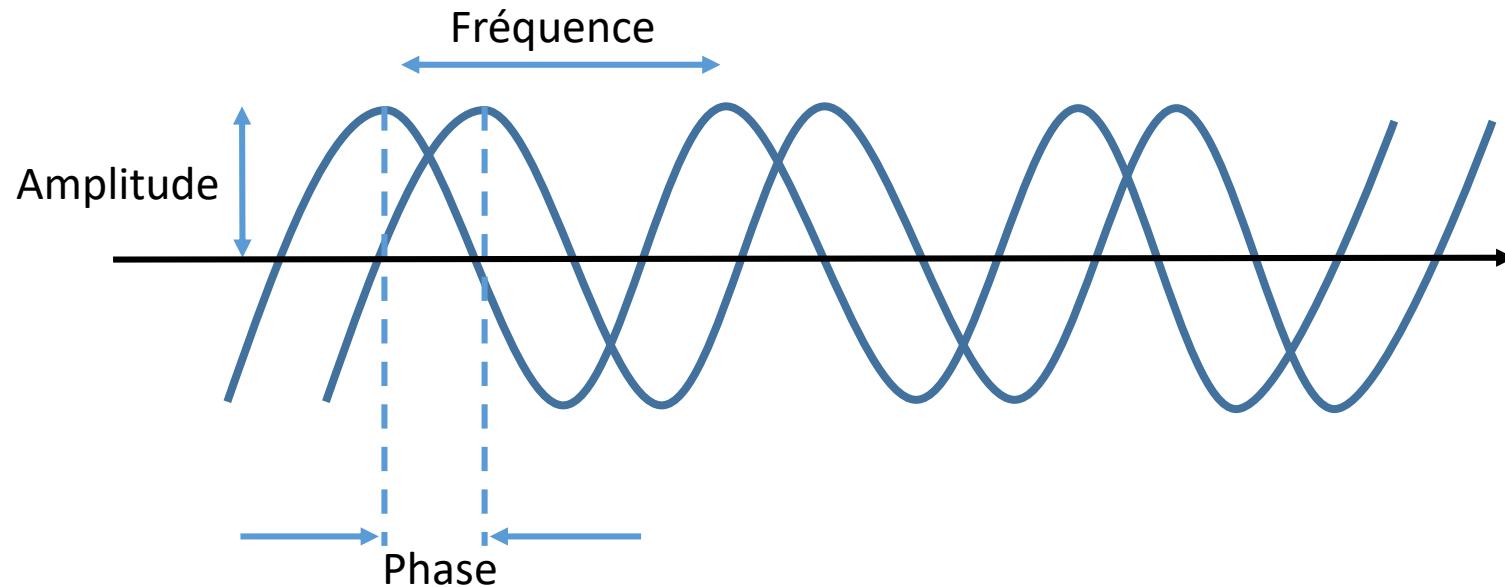
Les canaux dans la bande 2.4GHz



- La bande 2.4GHz est découpée en 14 canaux (seulement 11 sont disponibles partout dans le monde)
 - Les canaux 12 et 13 ne sont pas disponibles aux Etats Unis
 - Le canal 14 est disponible au Japon uniquement (pour 802.11b)
- Seulement 3 canaux sont utilisables en même temps sans interférence : 1, 6 et 11

Rappel

- Une onde radio a la forme suivante

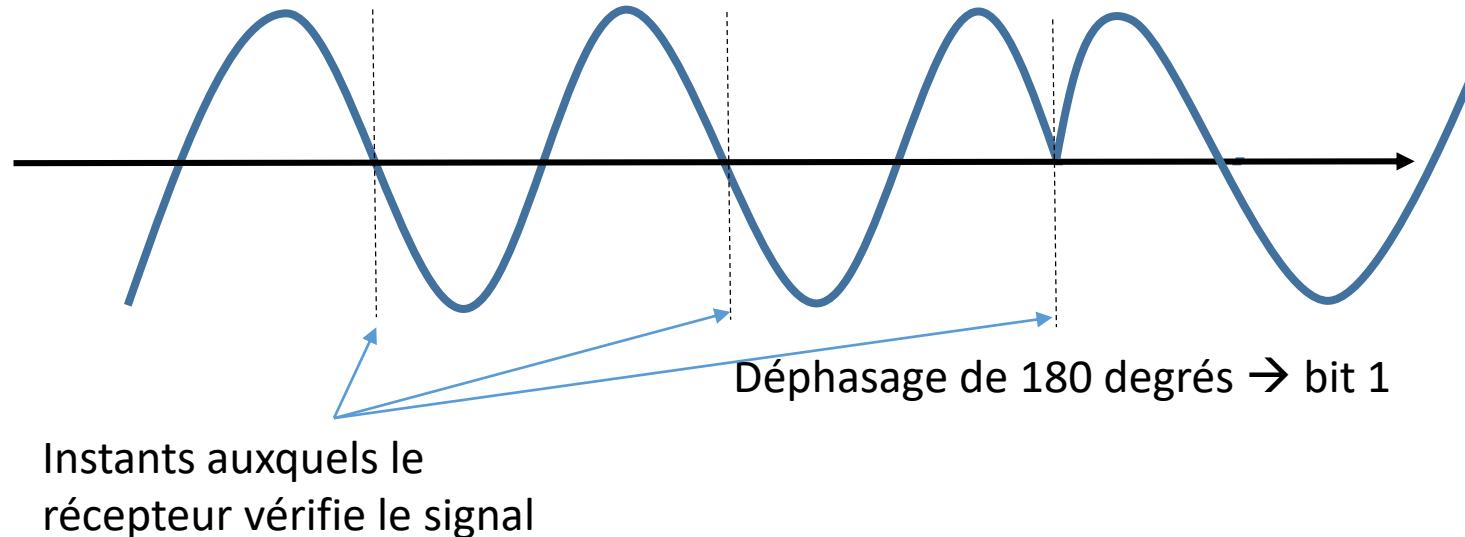


- Pour faire passer une information on modifie l'amplitude, la fréquence, et/ou la phase

BPSK

- La modulation par changement de phases est appelée PSK : Phase Shift Keying
- BPSK : Binary PSK
 - Très robuste contre le bruit

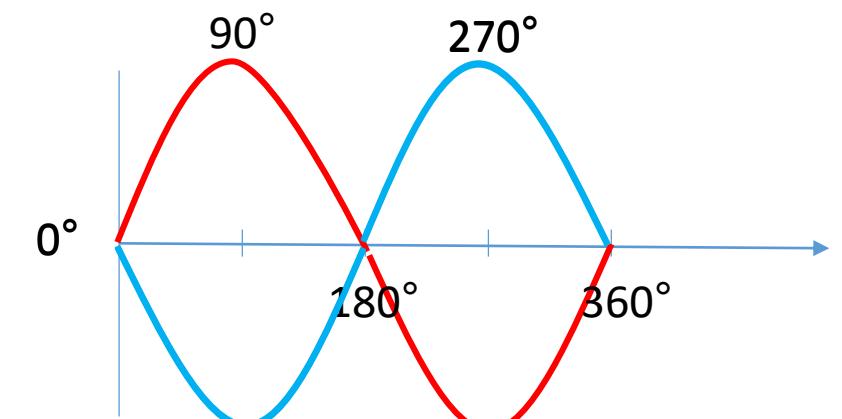
Déphasage de 0 degré → bit 0



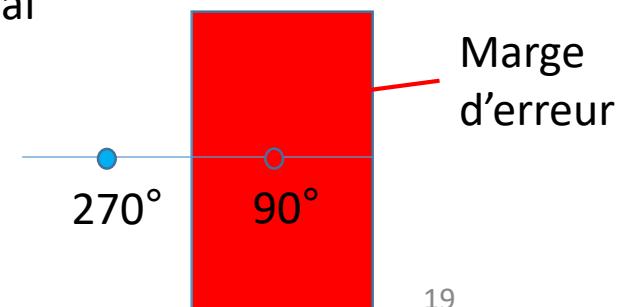
Bit de donnée

0 → -SIN

1 → SIN

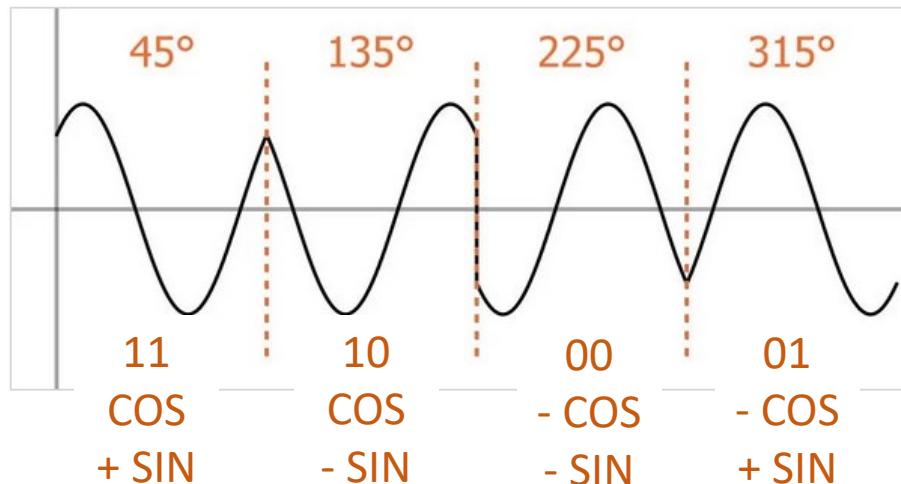


Ici la représentation des coordonnées polaires montre les pics de valeur de chaque signal



QPSK

- QPSK : Quadrature PSK

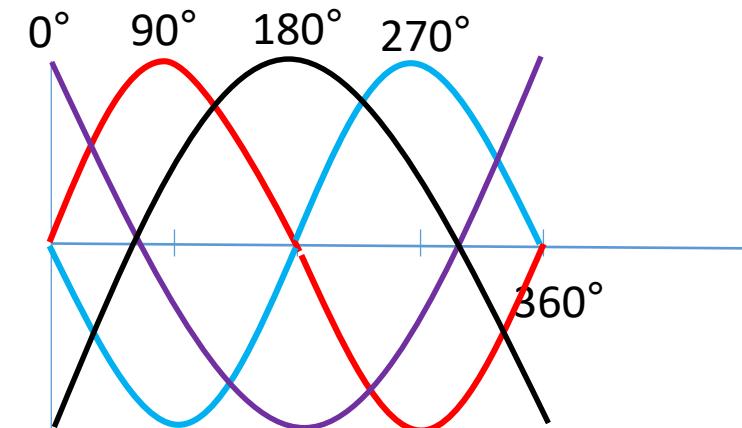


Source : Robert Keim

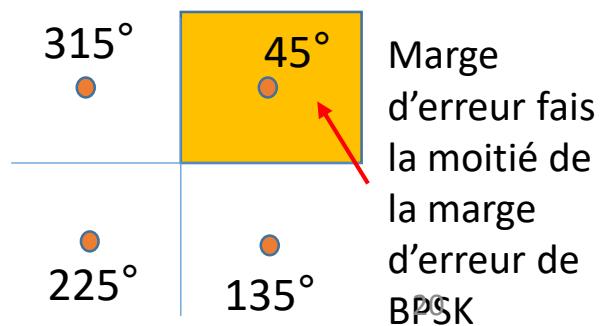
QPSK est 2 fois plus rapide que BPSK
QPSK est 2 fois plus sensible aux erreurs

Bit de donnée

- $-\text{COS} \leftarrow 00 \rightarrow -\text{SIN}$
- $-\text{COS} \leftarrow 01 \rightarrow \text{SIN}$
- $\text{COS} \leftarrow 10 \rightarrow -\text{SIN}$
- $\text{COS} \leftarrow 11 \rightarrow \text{SIN}$



Ici la représentation des coordonnées polaires montre les pics de valeur de chaque signal



DSSS (Direct Sequence Spread Spectrum)

- Technique d'étalement de spectre
- Consiste à multiplier les bits de données par une séquence de bits aléatoire ayant un débit plus élevé
- La séquence aléatoire (PRN, Pseudo Random Noise) est appelée « chipping sequence »
- Le débit de la séquence est appelé « chipping rate »
- Cette séquence devrait ressembler au bruit
- Si le récepteur ne possède pas la séquence, il ne peut pas récupérer les bits de données

Barker Code

- Pour définir les séquences de bits à transmettre par symbole, 802.11 utilise le code Barker
- Un Barker Code est une séquence de -1 et +1
- Le Barker Code utilisé par 802.11 définit 11 valeurs de -1 et +1 :
 $+1 \ -1 \ +1 \ +1 \ -1 \ +1 \ +1 \ +1 \ -1 \ -1 \ -1$
- Pour transmettre un bit à 1, la séquence transmise est $+1 \ -1 \ +1 \ +1 \ -1 \ +1 \ +1 \ +1 \ -1 \ -1 \ -1$
- Pour transmettre un bit à 0, la séquence transmise est $-1 \ +1 \ -1 \ -1 \ +1 \ -1 \ -1 \ -1 \ +1 \ +1 \ +1$
- Ceci permet de mieux résister au bruit et aux interférences

Barker Code avec BPSK et QPSK

- Barker Code avec BPSK permet d'atteindre 1 Mbps
 - Chaque symbole transmis contient un bit de donnée
- Barker Code avec QPSK permet d'atteindre 2 Mbps
 - Chaque symbole transmis contient 2 bits de données (voir <https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-demodulation/understanding-i-q-signals-and-quadrature-modulation/> pour plus d'informations sur la transformation du signal contenant 2 bits de données)

Correction de code (CCK)

- Afin d'atteindre un débit de 11 Mbps avec Barker Code il faut être en mesure de faire 2048 rotations (2 avec BPSK, 4 avec QPSK)
 - Ceci engendrera trop d'imprécision → inefficace
- L'utilisation de la CCK permet d'atteindre les débits 5 Mbps et 11 Mbps
 - La séquence de 11 bits de Barker est remplacée par une séquence de 8 bits
 - Avec 8 bits nous obtenons moins d'étalement dans le spectre (portée plus petite, moins de résistance aux interférences)
- CCK-4 permet d'atteindre 5.5 Mbps avec 4 séquences de chipping
- CCK-8 permet d'atteindre 11 Mbps avec 8 séquences de chipping

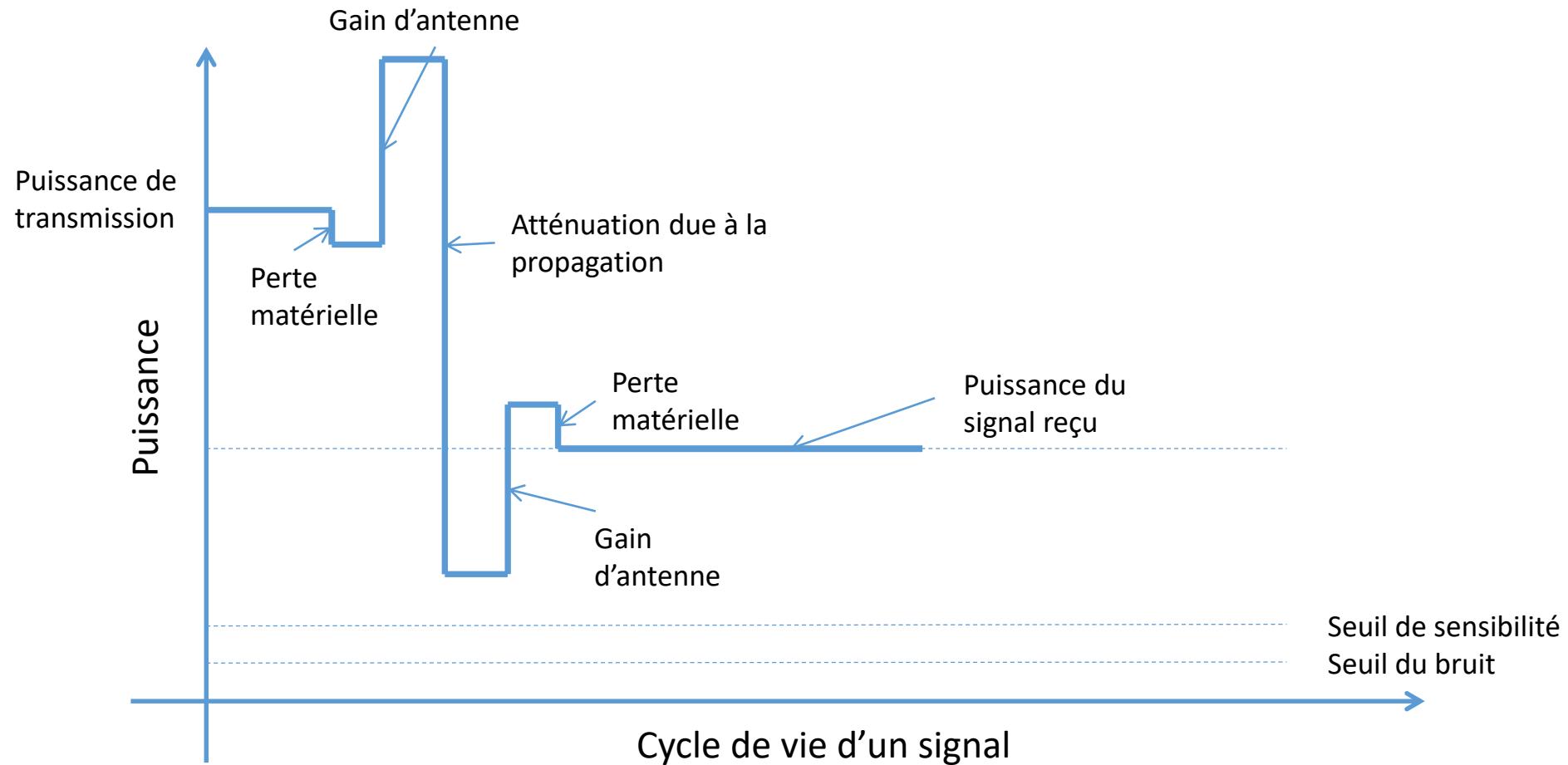
Débits de 802.11b

Débit	Modulation	Code correcteur	Taille du symbole	Bits par symbole
1 Mbps	BPSK	Barker	11 bits	1
2 Mbps	QPSK	Barker	11 bits	2
5.5 Mbps	QPSK	CCK	8 bits	4
11 Mbps	QPSK	CCK	8 bits	8

Recevoir un signal

- Puissance de réception (dBm) = puissance de transmission (dBm) + gain d'antennes (dBi) – atténuation (dB) – perte matérielle (dB)
- Afin de recevoir le signal, cette puissance de réception doit être :
 - Supérieure au seuil de bruit
 - Supérieure à la sommes des puissances des signaux simultanés (supérieur de 10 dB en général)
- L'écart entre la puissance reçue et ces deux facteurs permet de négocier une modulation adéquate pour une meilleure efficacité

De l'émetteur au récepteur



dB : décibel

- dB est une unité qui mesure la ratio de l'intensité du son ou du signal RF (en général par rapport à une valeur de référence)
- Un son presque inaudible mesure 0 dB, un son 10 fois plus fort mesure 10 dB, 100 fois plus fort 20 dB, 1000 fois plus fort 30 dB, etc.
- Exemples :
 - Silence = 0 dB
 - Un chuchotement = 15 dB
 - Une conversation normale = 60 dB
 - Une tondeuse à gazon = 90 dB
 - Un klaxonnement = 110 dB
 - Un concert de rock = 120 dB
 - Coup de feu ou feux d'artifice = 140 dB
- Si vous criez pour être entendu, le bruit est d'au moins 85 dB
- 8 heures d'exposition à un bruit supérieur à 90 dB engendre des problèmes d'audition
- Tout ce qui est au dessus de 140 dB peut générer une douleur et des problèmes d'audition immédiatement

dB, dBm, dBi

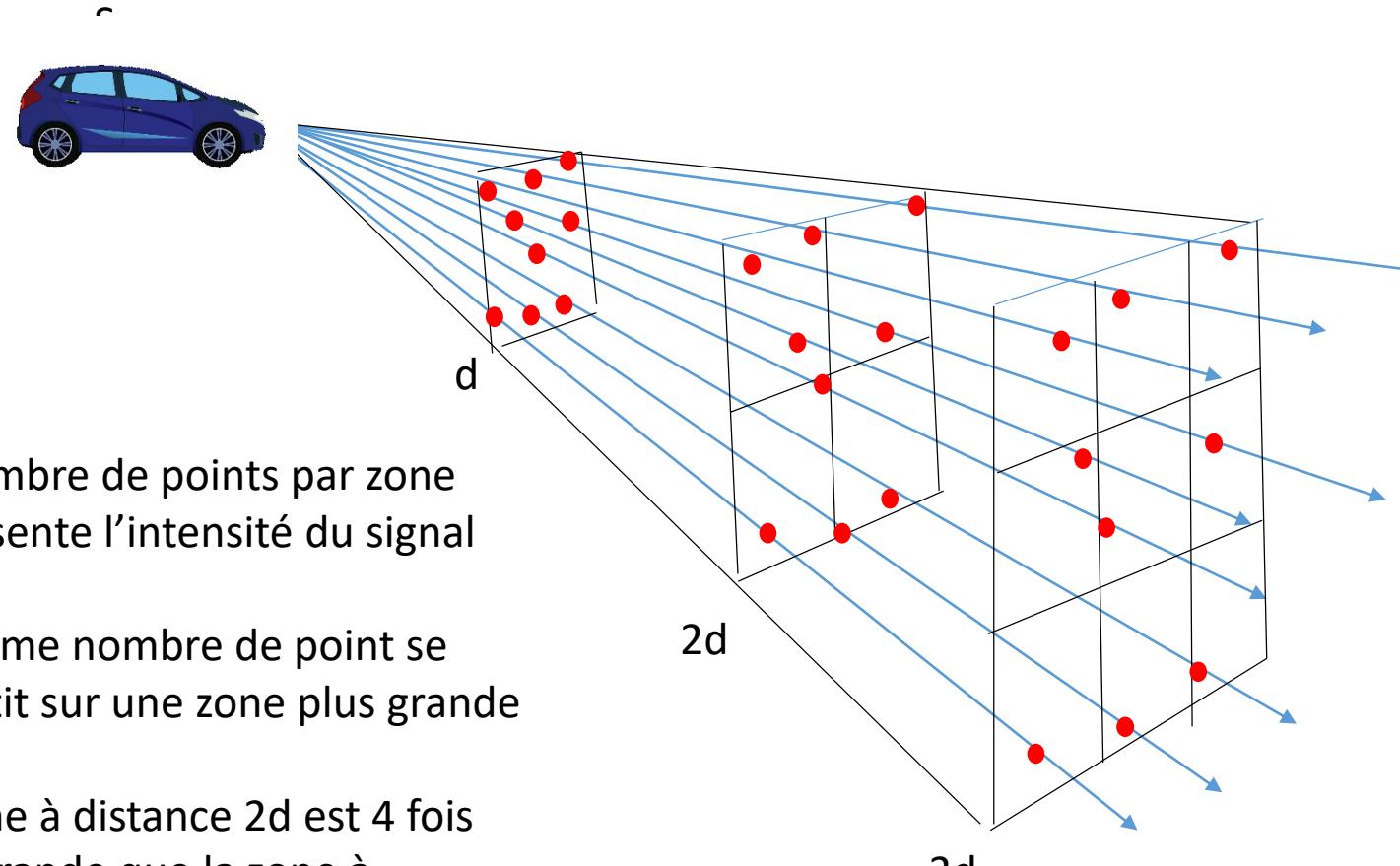
- dBm est une unité qui exprime la puissance d'un signal par rapport à 1 mW
- $P_{dBm} = 10 * \log_{10}(P_{mW}/1mW)$
- 0dBm = 1mW
- Quand la puissance en mW est doublée, sa valeur en dBm est incrémentée de 3
- 2mW = 3dBm, 4mW = 6dBm, 8mW = 9dBm
- -3dBm = 0.5mW, -6dBm = 0.25mW, -9dBm = 0.125mW
- Aussi, quand on incrémente de 10 en dBm, on multiplie par 10 en mW
- dBi exprime la valeur rajoutée par une antenne par rapport à une antenne isotrope

Modèles de propagation

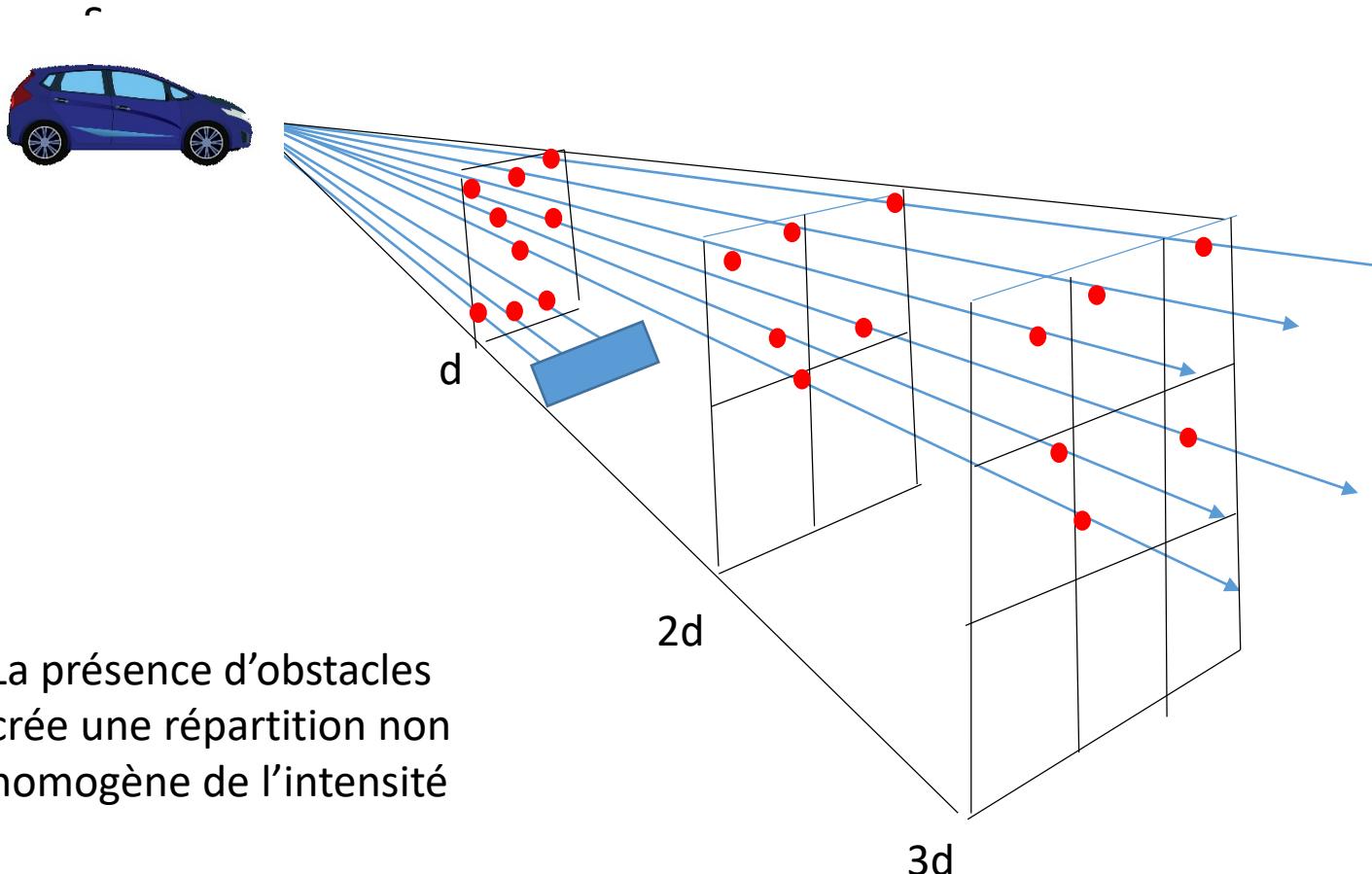
- Un modèle de propagation des signaux radio permet d'estimer la puissance de réception d'un signal
- Cette puissance est fonction de la distance et dépend essentiellement de l'environnement dans lequel se propage le signal
- A quoi ça sert ?
 - Etude de pré-déploiement :
 - Estimer le nombre de points d'accès à déployer
 - Réglage les puissances de transmission des points d'accès
 - Estimer les performances des protocoles avec des outils de simulation :
 - Simuler le réseau et les positions des nœuds facilement
 - Implémenter des protocoles et analyser les résultats

Loi en carré inverse

(source : https://fr.wikipedia.org/wiki/Loi_en_carr%C3%A9_inverse)



Loi en carré inverse



Modèle de Friis

➤ Friis equation (modèle de Free Space):

$$\frac{P_r}{P_t} = Gt * Gr * \left(\frac{\lambda}{4\pi D} \right)^2$$

P_r puissance de réception,

P_t puissance de transmission,

G_t le gain de l'antenne de l'émetteur,

G_r le gain de l'antenne du récepteur,

λ (lambda) la longueur d'onde,

D distance entre les 2 antennes.

Quand G_t et G_r sont en dB and P_t en dBm, l'équation devient :

$$P_r = Pt + Gt + Gr + 20 \log_{10} \left(\frac{\lambda}{4\pi D} \right)$$

Différents modèles de propagation

- Prise en compte des réflexions : modèle 2-Ray Ground
- En environnement à l'intérieur : modèle ITU
- En environnement extérieur : modèles Okumura, Hata, COST
- Prise en compte de l'instabilité des liens : modèle Log-distance
- Modèles hybride : selon la distance ou le secteur

Collision

- Une collision est le résultat d'une réception simultanée d'au moins 2 signaux ayant des niveaux « proches » de puissance de réception
- Elle a toujours lieu au niveau du récepteur
- Suite à une collision, la trame est perdue et doit être retransmise
- La détection d'une collision en sans fil se fait grâce aux acquittement (ACK)
- L'émetteur considère qu'une trame non acquittée est perdue

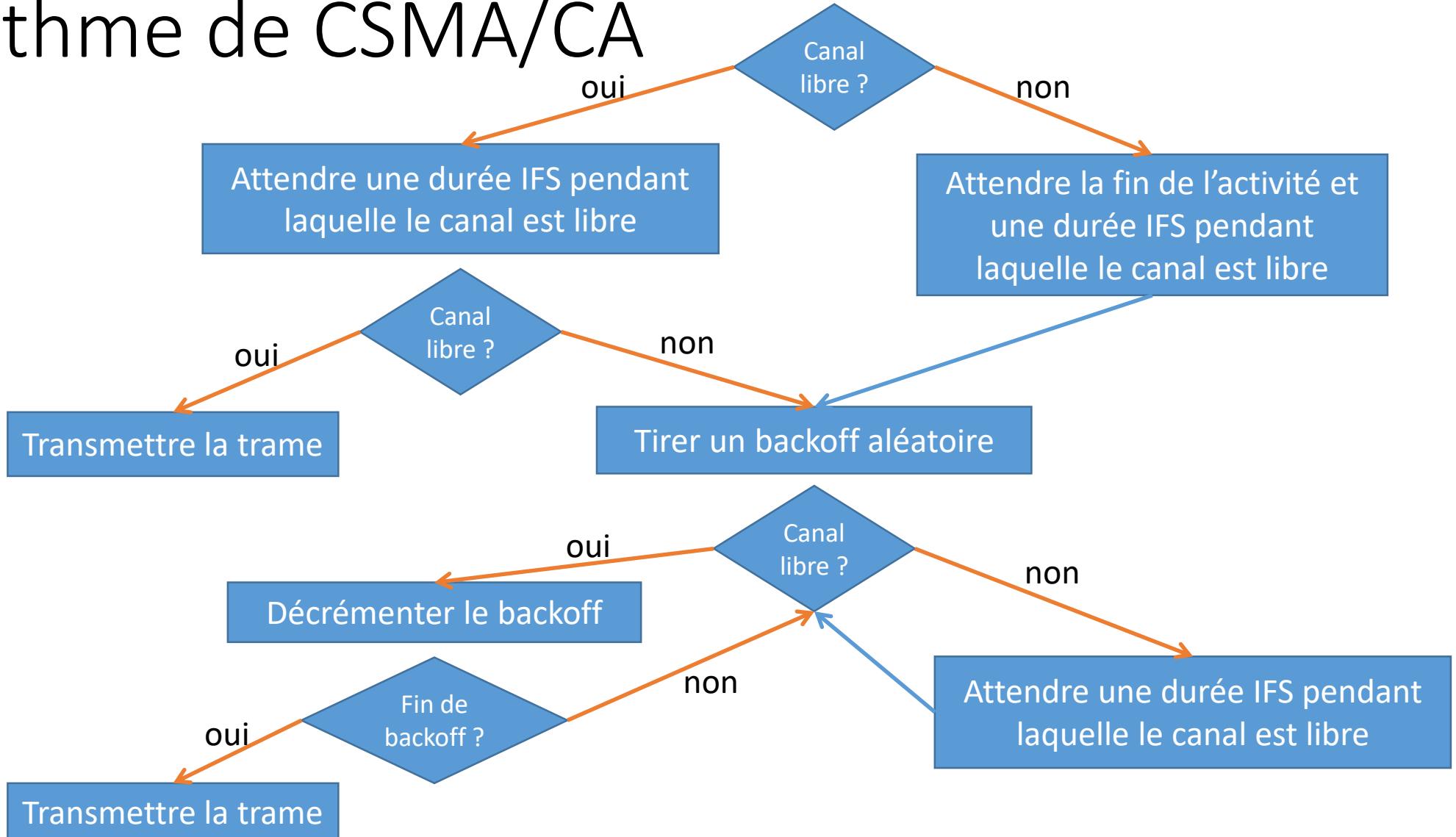
Capture

- Plusieurs signaux reçus simultanément ne donnent pas lieu systématiquement à des collisions
- Quand le signal reçu est au moins 10 dB supérieur à l'ensemble des autres signaux, il peut résister aux interférence et être capturé par le récepteur
- 10 dB d'écart veut dire que le signal doit être 10 fois plus fort que l'ensemble des autres signaux

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- Basé sur MACAW (*Vaduvur Bharghavan; et al. SIGCOMM '94*) inventé par Berkeley et Xerox
- Inspiré du réseau sans fil PARC développé en 1993 (réseau formé d'un ensemble de stations de base d'une portée de 6 mètres, d'un débit de 250 kbps par cellule, interconnectées par Ethernet)
- Le CSMA/CA permet d'éviter les collisions mais ne les supprime pas complètement

Algorithme de CSMA/CA



Backoff de 802.11

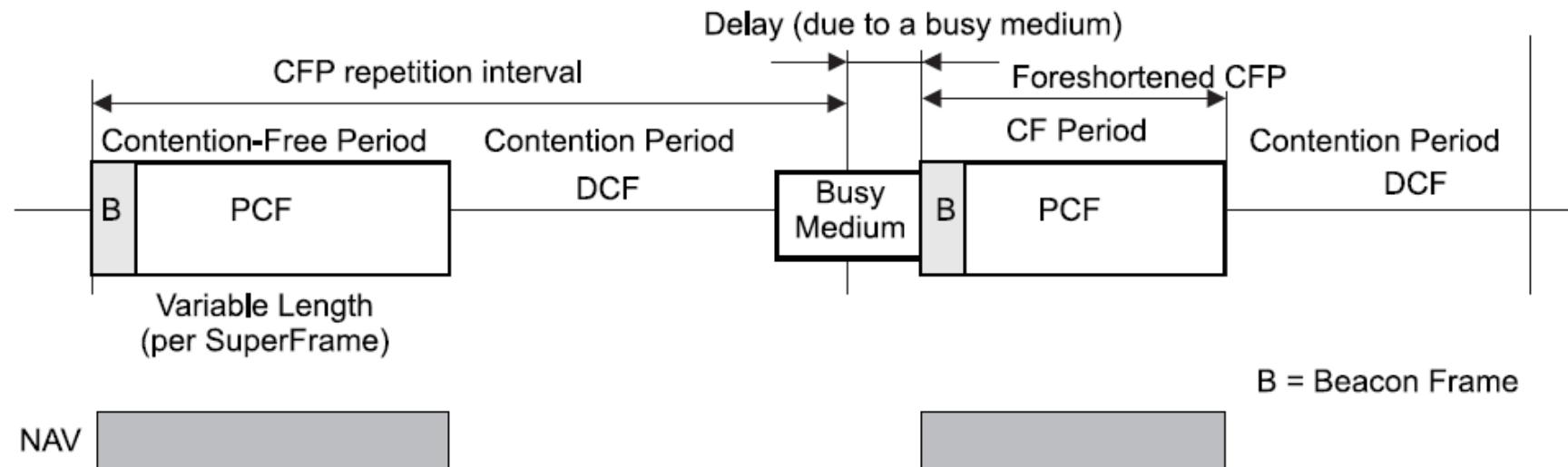
- La valeur du backoff est tirée au sort d'un intervalle $[0 ; CW]$ où $CW = 2^{be} - 1$
- Pour le mode DSSS, CW commence à $CW_{min} = 31$ ($be = 5$), et plafonne à $CW_{max} = 1023$ ($be = 10$)
- be est incrémenté à chaque tirage de backoff pour une même trame
- CW repasse à CW_{min} après une transmission réussie
 - CW_{min} varie selon la couche physique (31 pour DSSS, 15 pour OFDM)
- La valeur tirée est un entier qui est ensuite multipliée par une durée aSlotTime (20 micro secondes pour le mode DSSS)

IFS : Inter-Frame Spacing

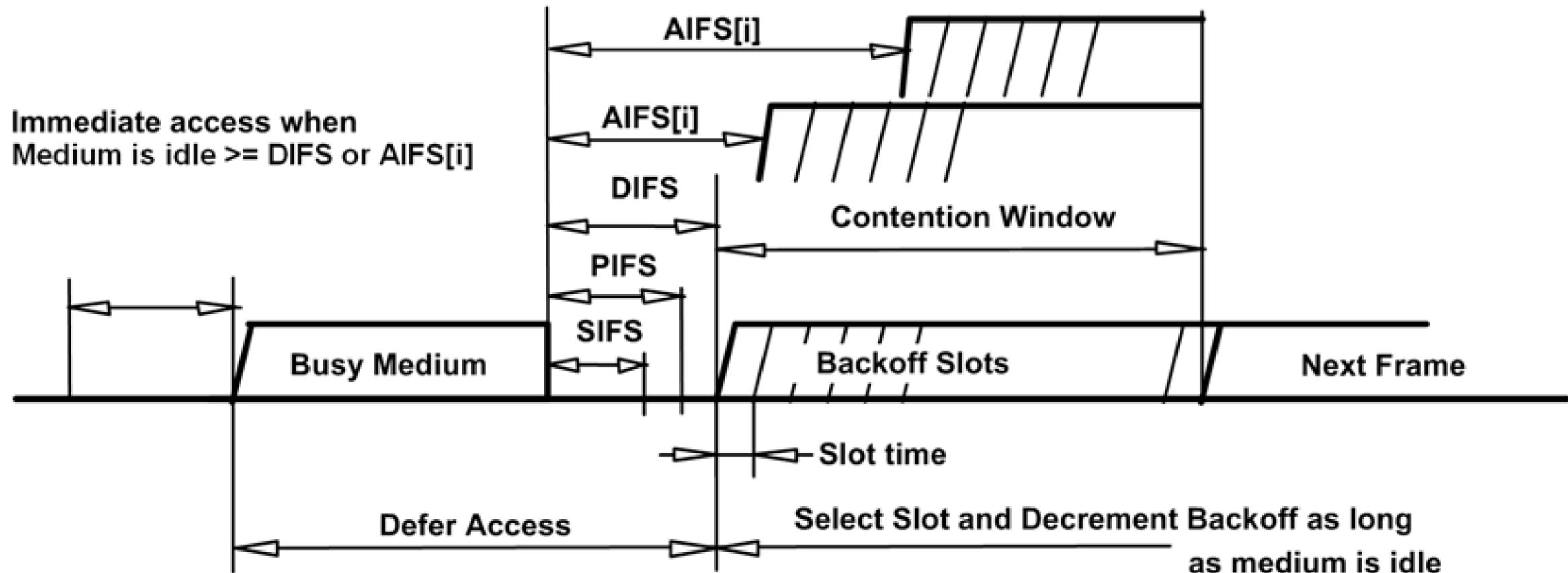
- La durée IFS à attendre peut prendre l'une des valeurs suivantes :
 - RIFS : Reduced IFS (quand le mode de réduction d'overhead est activé) rajouté avec 802.11n et supprimé avec 802.11ac
 - SIFS : Short IFS (pour les trames de contrôle CTS, ACK, fragments d'une trame, réponse à un Poll)
 - PIFS : PCF IFS (pendant la période PCF)
 - DIFS : DCF IFS (valeur standard)
 - AIFS : Arbitrary IFS (utilisée par le mode QoS durant la EDCAF)
 - EIFS : Extended IFS (suite à une retransmission)

DCF et PCF

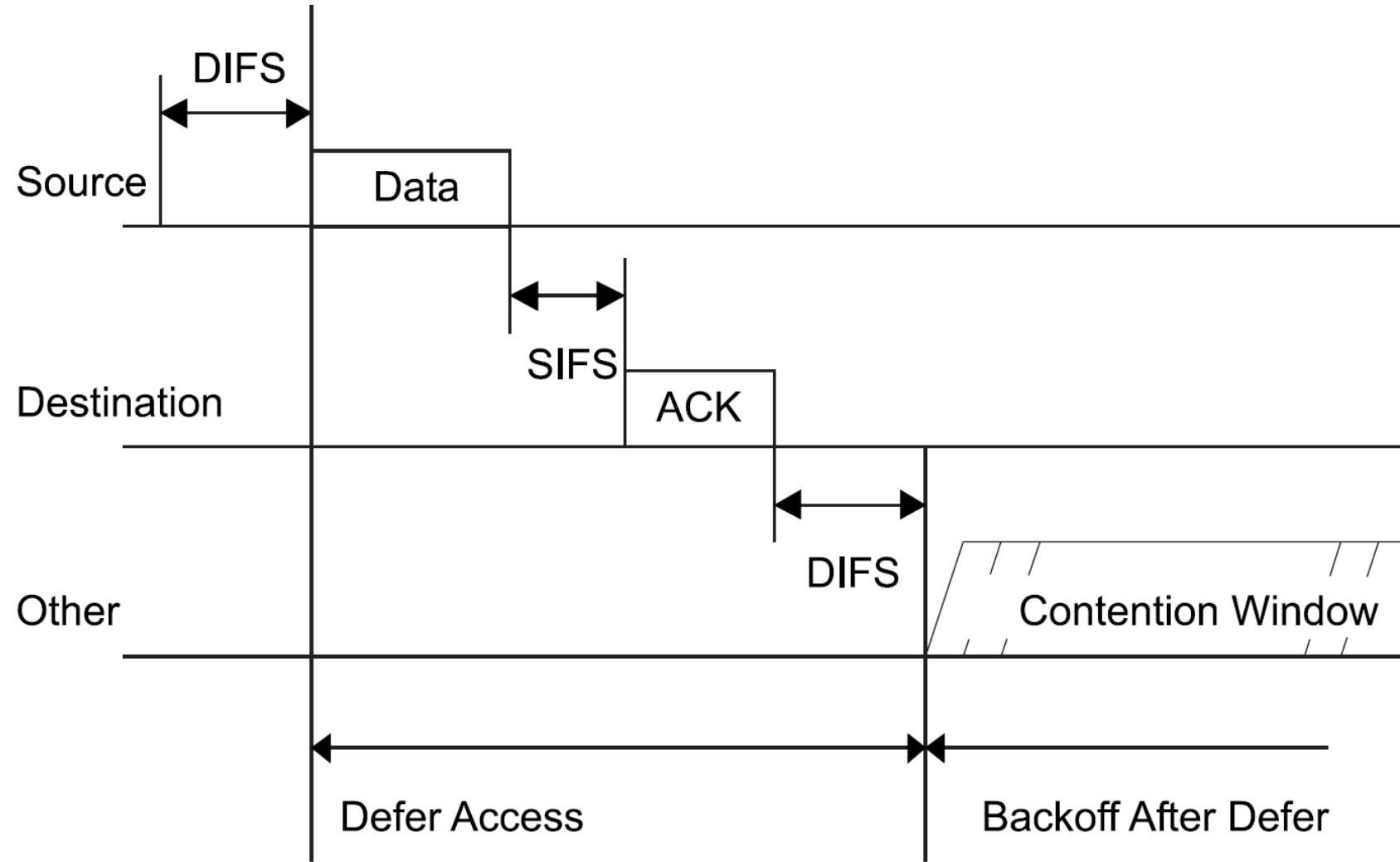
- 802.11 a été initialement spécifié pour opérer selon 2 modes
- DCF (Distributed Coordination Function) :
 - C'est le mode qui utilise le CSMA/CA sans coordination du point d'accès
- PCF (Point Coordination Function) :
 - C'est le mode qui permet de faire des réservations de slot de temps
 - Rarement implémenté car requiert une synchronisation et une précision temporelle



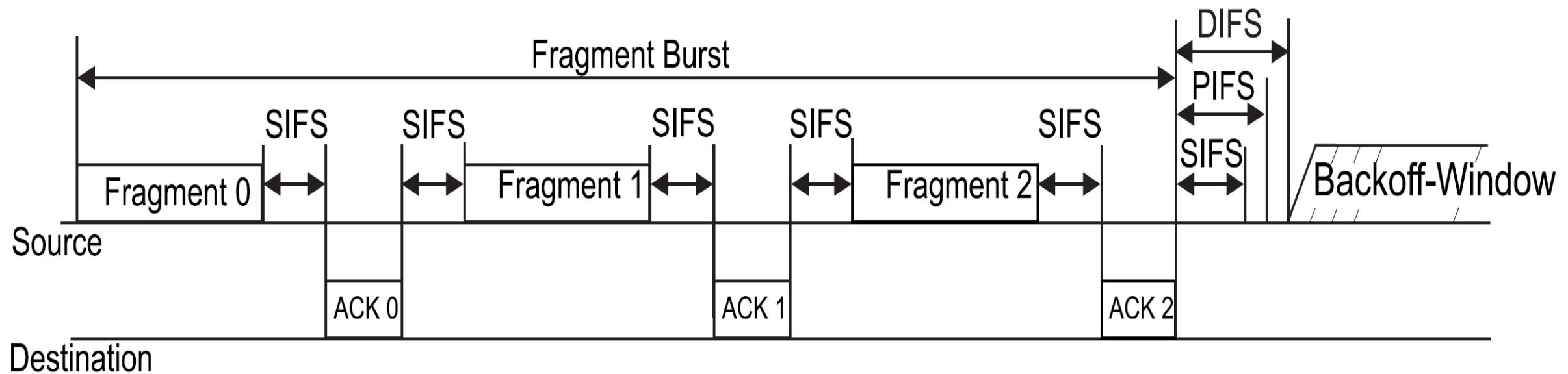
Exemple d'accès



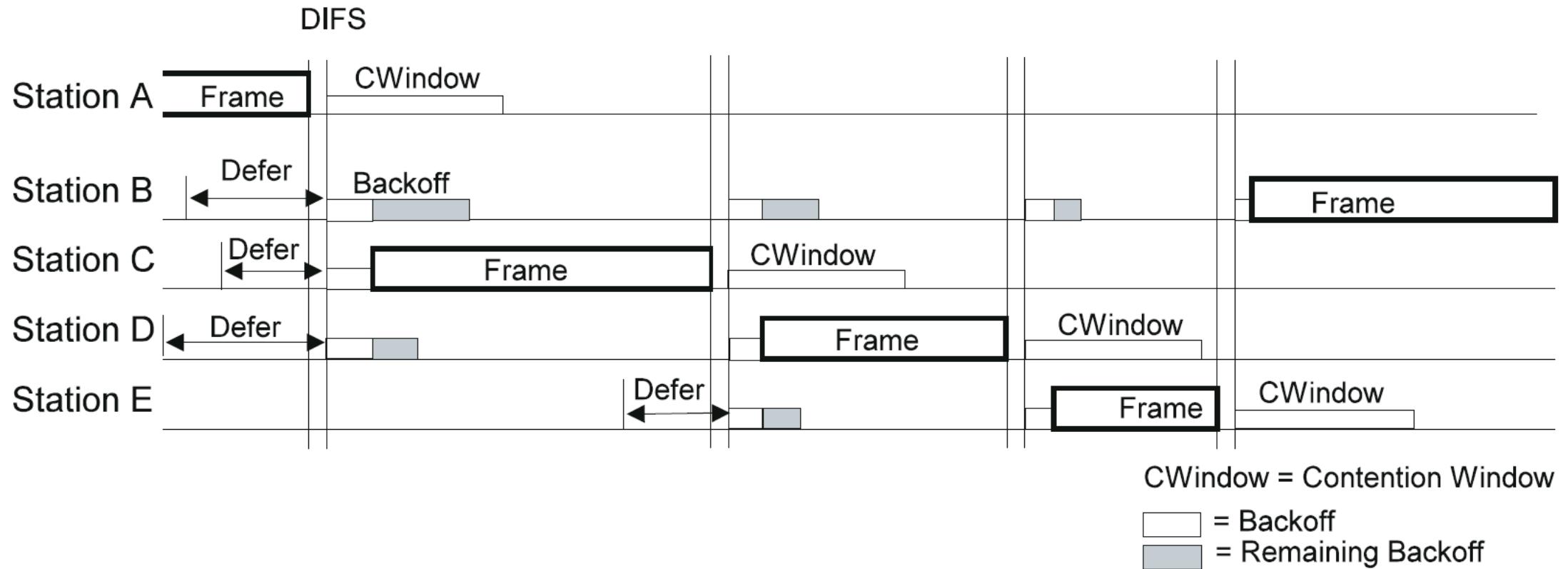
Exemple d'échange de trames



Echange d'une donnée fragmentée



Exemple d'échange de trames (plusieurs nœuds)



Probabilité de collision

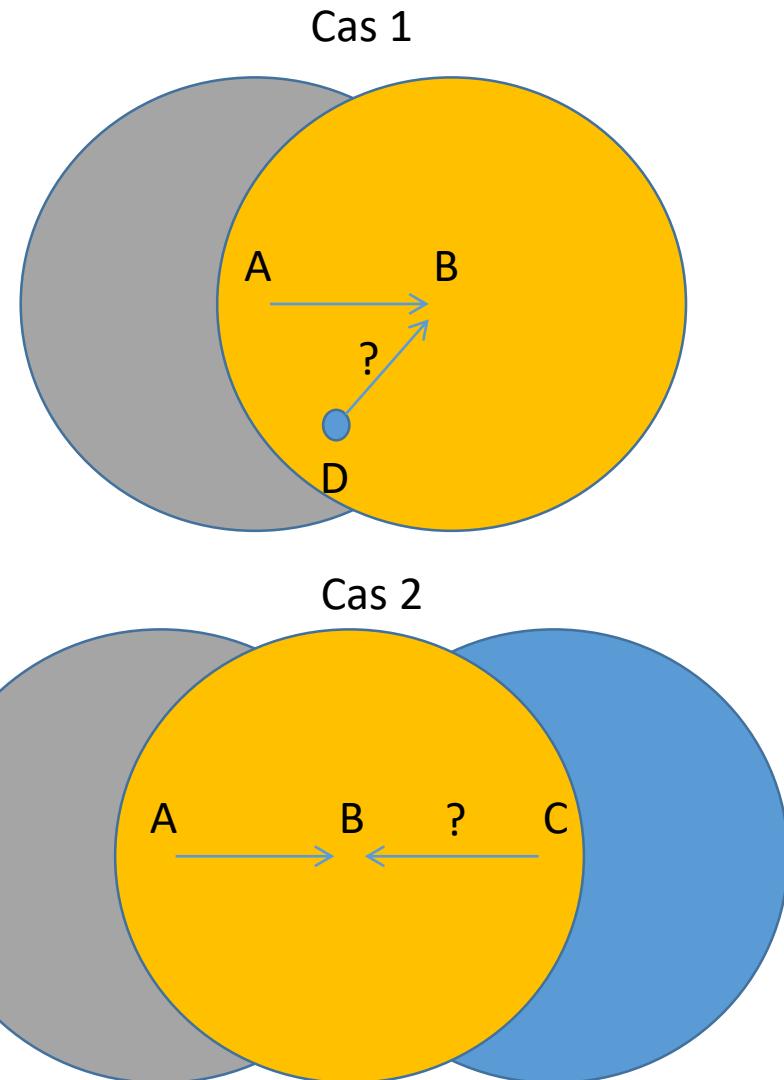
- Considérons le cas suivant :
 - Un nœud est en train de transmettre une trame
 - Tous les autres nœuds ont une trame à transmettre
 - Tous les nœuds sont à portée radio les uns des autres
- A partir de combien de nœuds dans ce réseau WiFi nous aurons une collision après la fin de la transmission en cours avec une probabilité de 100% ?

Réflexion sur le CSMA/CA

- Avec CSMA/CA, c'est l'émetteur qui fait le test alors que les collisions ont lieu au niveau du récepteur
- Emetteur et récepteur sont souvent dans des positions géographiques qui font que le test fait par l'émetteur ne lui permet pas de savoir si le récepteur serait disposé à bien décoder le signal
- Dans quel cas de figure le CSMA/CA aurait été efficace ?

Terminal caché

- Cas 1 :
 - A est en train de transmettre un message à B
 - D souhaite transmettre un message à B
 - D fait un CCA et détecte que le canal est occupé
 - D ne transmet pas son message
- Cas 2 :
 - A est en train de transmettre un message à B
 - C souhaite transmettre un message à B
 - C fait un CCA mais ne détecte pas que le canal est occupé
 - C transmet son message à B
 - Selon le rapport SNR, cela donne lieu à une collision mais dans tous les cas, il y aura une perte



RTS/CTS

- MACA est l'un des premiers protocoles à utiliser le principe des messages RTS/CTS
 - Quand un émetteur souhaite transmettre un message, il envoie un RTS (Request To Send) au destinataire
 - Si le destinataire n'est pas occupé ni en train de reporter sa transmission, il répond avec un CTS (Clear To Send)
 - Si l'émetteur ne reçoit pas de CTS, il retransmet le RTS après un backoff
 - Les RTS et CTS contiennent la durée de la transmission à venir
 - Les nœuds qui écoutent le RTS reportent leurs transmissions à un moment après la fin de réception de l'éventuel CTS
 - Les nœuds qui écoutent le CTS reportent leurs transmissions à un moment après la fin du message de données

RTS/CTS

- Les stations susceptibles d'interférer sur le récepteur recevront le CTS transmis par ce récepteur, mais pas tous, pourquoi ?
- Les nœuds qui reçoivent un RTS et pas le CTS peuvent émettre après le CTS, pourquoi ?

Algorithme de backoff de MACA

- Suite à un RTS sans réception de CTS, un nœud choisit d'une façon aléatoire selon une loi uniforme une valeur entière entre 1 et BO (BackOff)
- Le nœud retransmet le message d'une durée qui correspond à la durée de transmission de 30 octets (taille des messages RTS et CTS) multipliée par le nombre aléatoire choisi
- BO commence à 2 (minBO) et plafonne à 64 (maxBO)
- A chaque retransmission d'une même trame, le BO double de valeur
- A chaque transmission de RTS avec succès, le BO est remis à 2
- Cet algorithme est dit BEB (Binary Exponentiel Backoff)

Réflexion sur l'algorithme de backoff

- Une méthode d'accès efficace devrait permettre à plusieurs nœuds de partager le médium d'une façon équitable
- Or cet algorithme pénalise le nœud qui n'a pas pu accéder au médium et favorise celui qui a réussi
- Comment peut on rendre cet algorithme équitable ?

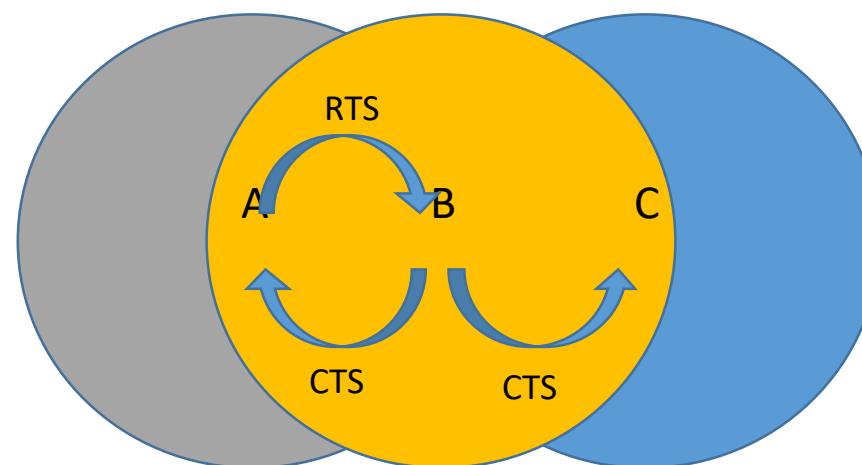
RTS-CTS-Data vs RTS-CTS-Data-ACK

- Un ACK au niveau 2 du modèle permet de réagir plus vite aux pertes
- Sans l'ACK niveau 2, c'est TCP qui devrait corriger l'erreur (cela prend plus de temps)
- MACAW (version mise à jour de MACA) propose d'inclure un ACK après la réception d'une Data
 - La donnée est répétée suite à un ACK non reçu sans incrémenter le backoff
 - Si la donnée est reçue mais l'ACK est perdu, le récepteur répondra au RTS répété avec un ACK et non pas avec un CTS
- L'ACK présente un overhead mais fait augmenter le débit à partir d'un taux d'erreur de 1%

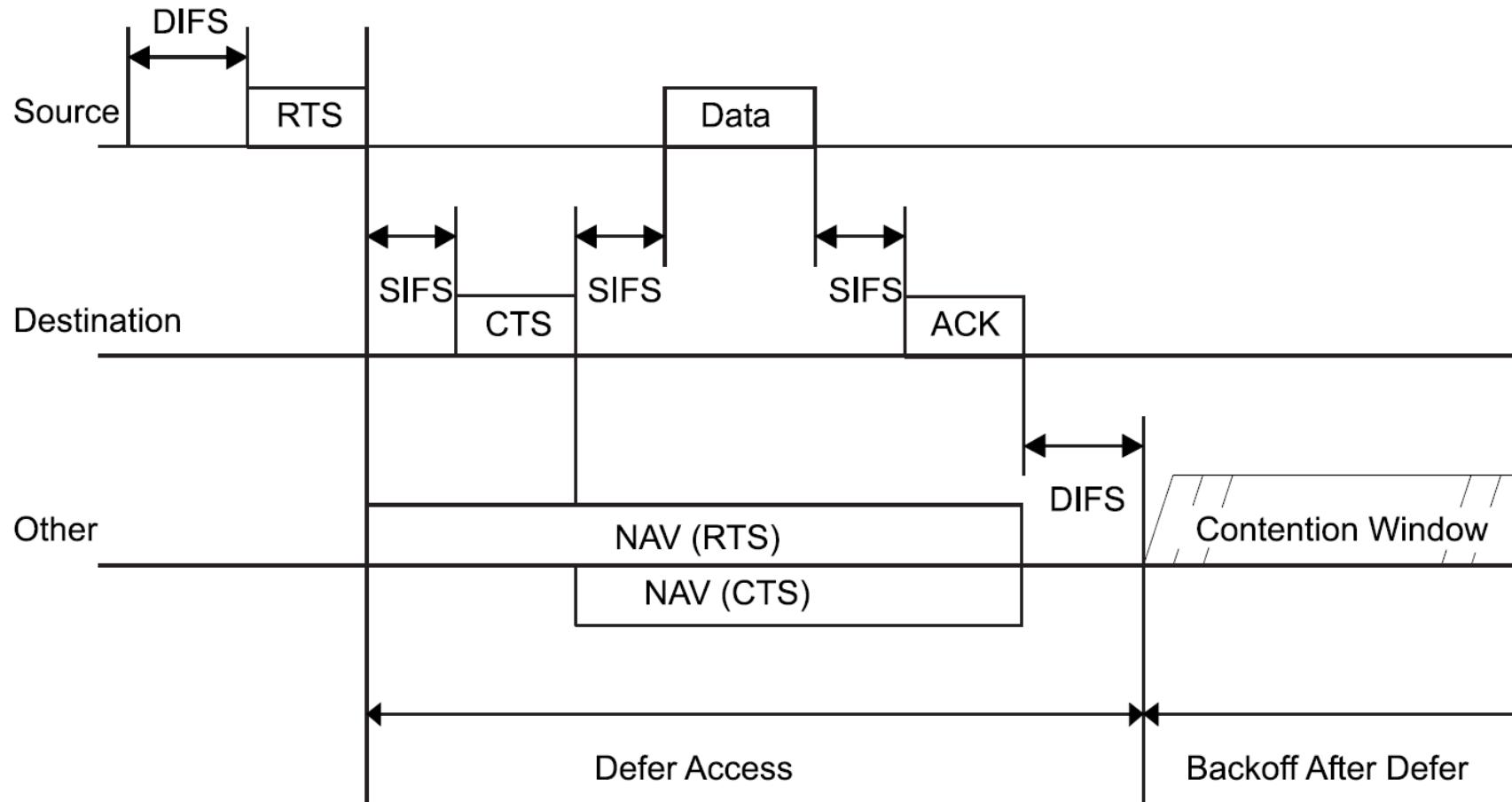
RTS/CTS de 802.11

- 802.11 utilise des acquittements directs : RTS/CTS/Data/ACK
- Ceci implique que l'émetteur est aussi censé être un récepteur d'un ACK
- Toute station qui reçoit un RTS ou un CTS doit considérer que le médium est occupé pour la durée indiquée dans les RTS/CTS

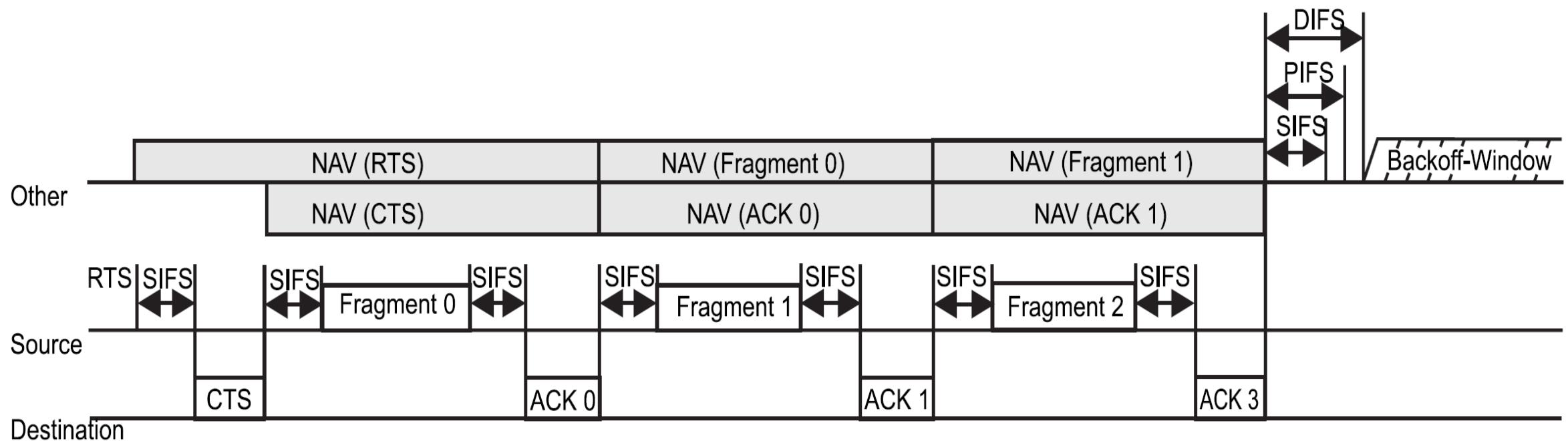
A la réception de la trame CTS, le nœud C déduit que le médium sera occupé pour la durée du message de donnée qui sera transmis par A



Exemple d'échange avec RTS/CTS

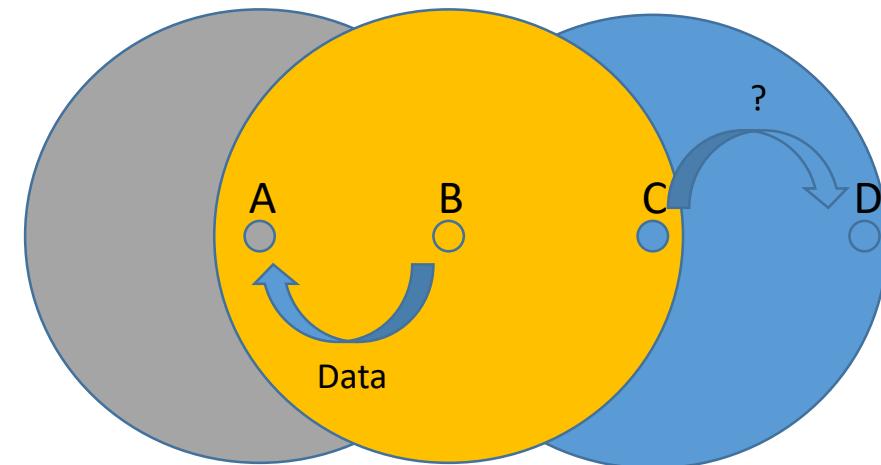


Exemple d'échange de données fragmentées



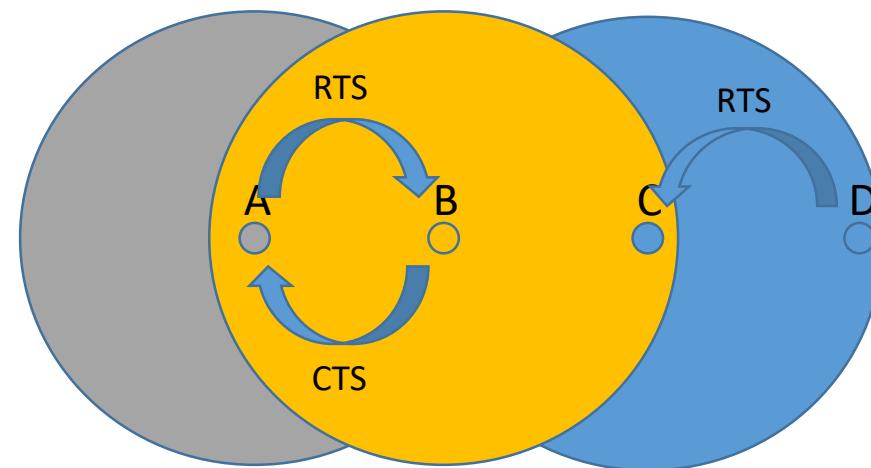
Terminal exposé

- Selon CSMA/CA, C détecte l'activité de B et ne peut pas accéder au médium
- Est-ce que la transmission de C pose problème ?



Terminal exposé

- D souhaite transmettre à C, mais C à déjà entendu le CTS de B, C ne peut pas répondre à D
- Est-ce que la transmission de D pose problème ?



Format des trames de données et adressage

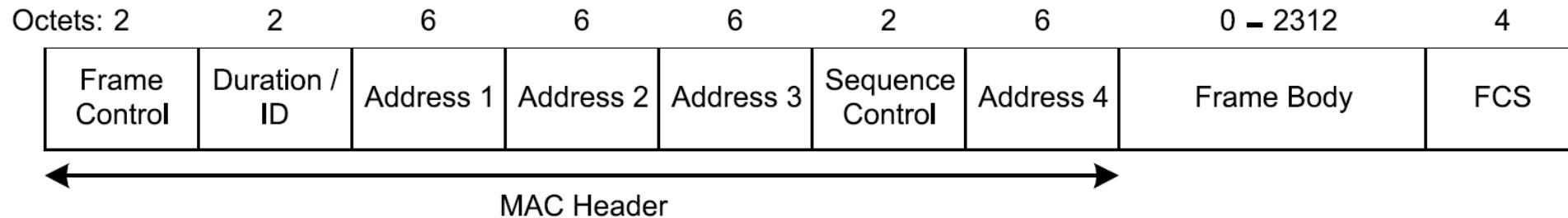


Figure 22—Data frame

Table 4 —Address field contents

DS : Distribution System

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Trame de contrôle

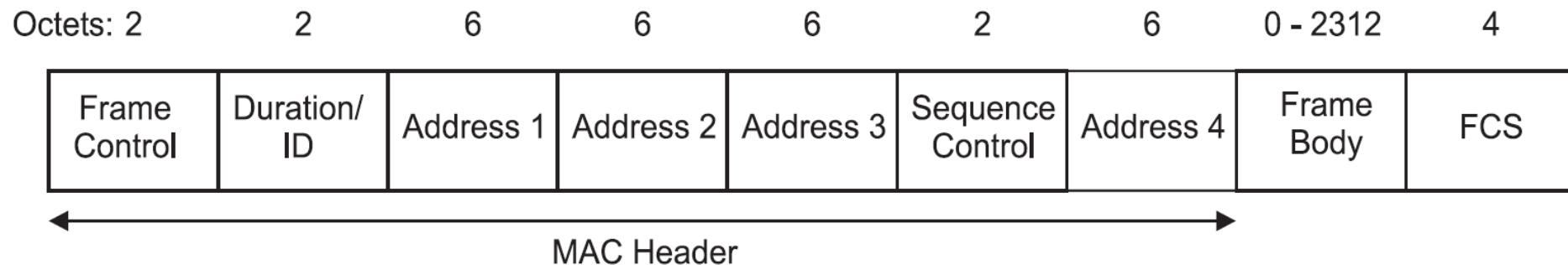


Figure 12—MAC frame format

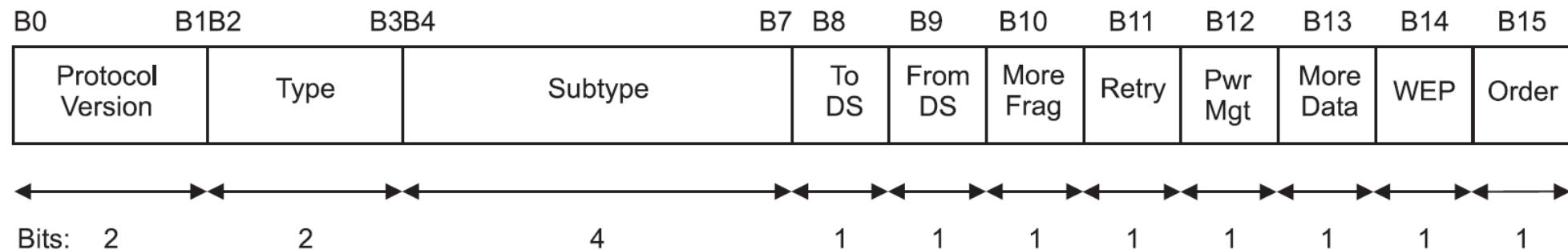


Figure 13—Frame Control field

RTS/CTS dans 802.11

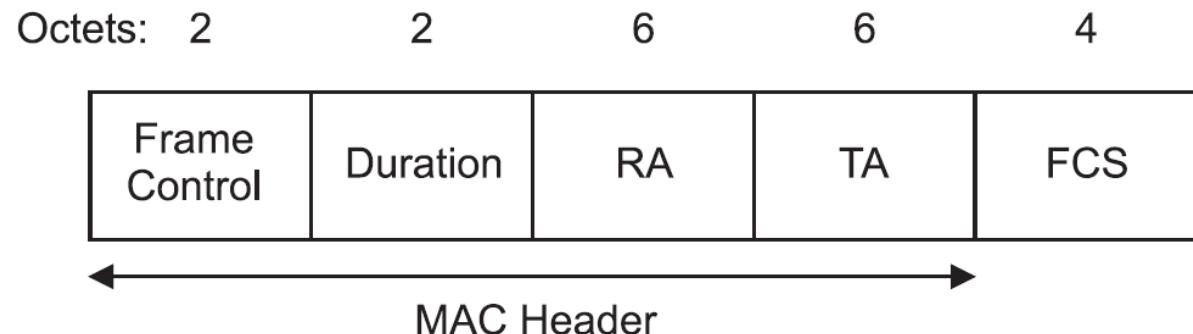


Figure 16—RTS frame

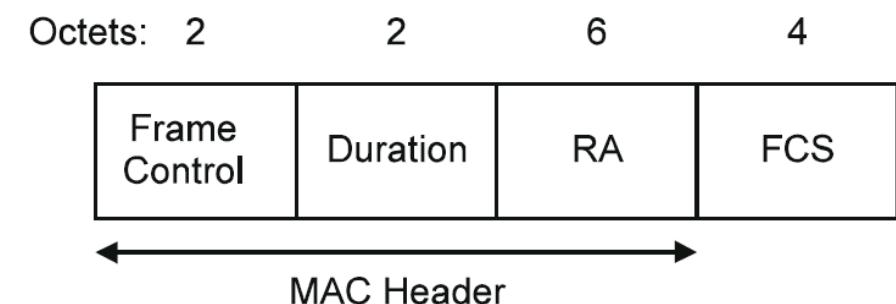


Figure 17—CTS frame

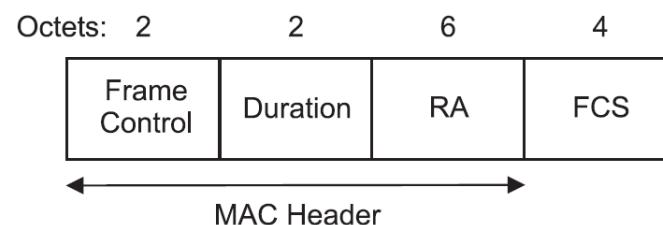


Figure 18—ACK frame

- Transmis avec le débit le plus bas pour que tous les nœuds puissent les comprendre

Trames de gestion

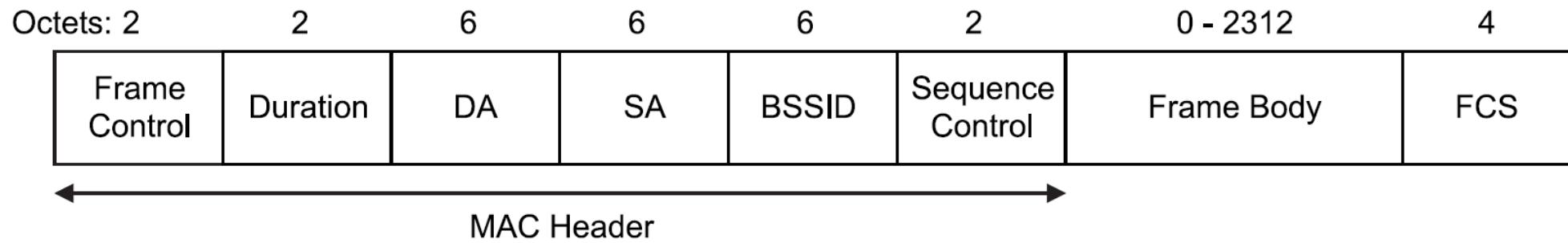
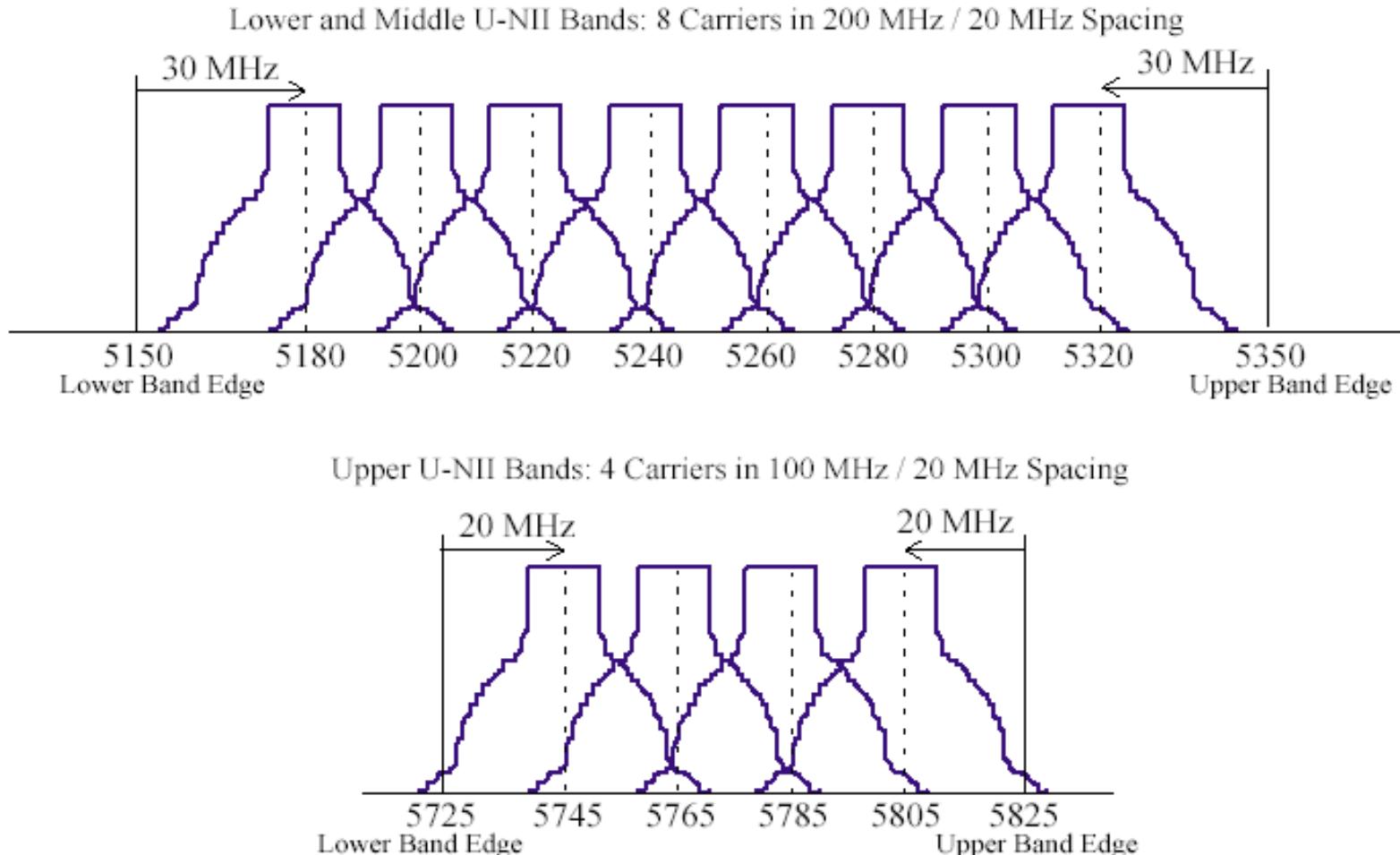


Figure 23—Management frame format

WiFi 2 (802.11a-1999)

- 802.11a opère sur la bande 5GHz
- Par rapport à 802.11b :
 - Utilisation d'OFDM au lieu du DSSS et CCK
 - Modulations : BPSK, QPSK, 16-QAM et 64-QAM
- Débits supportés : 54, 48, 36, 24, 18, 12, 9 et 6 Mbps

Les canaux de 802.11a



- WiFi est considéré comme utilisateur secondaire sur la bande 5.47–5.725 GHz qui a comme utilisateur primaire TDWR (Terminal-area Doppler Weather Radar)
- Quand un signal TDWR est détecté, les antennes WiFi doivent être éteintes

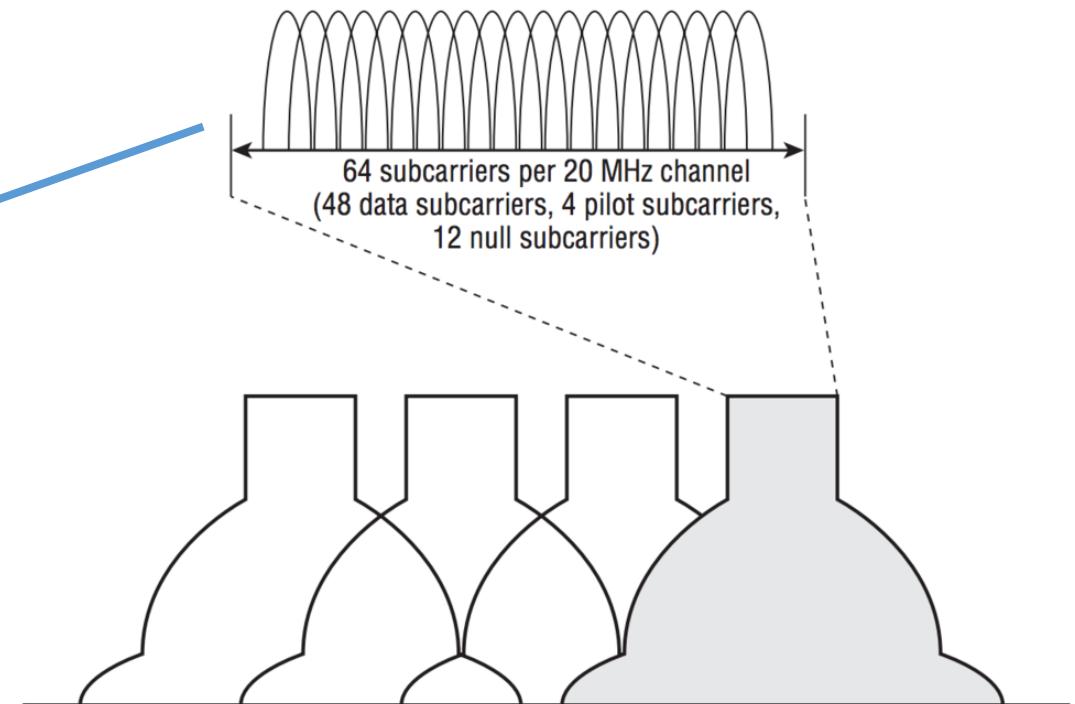
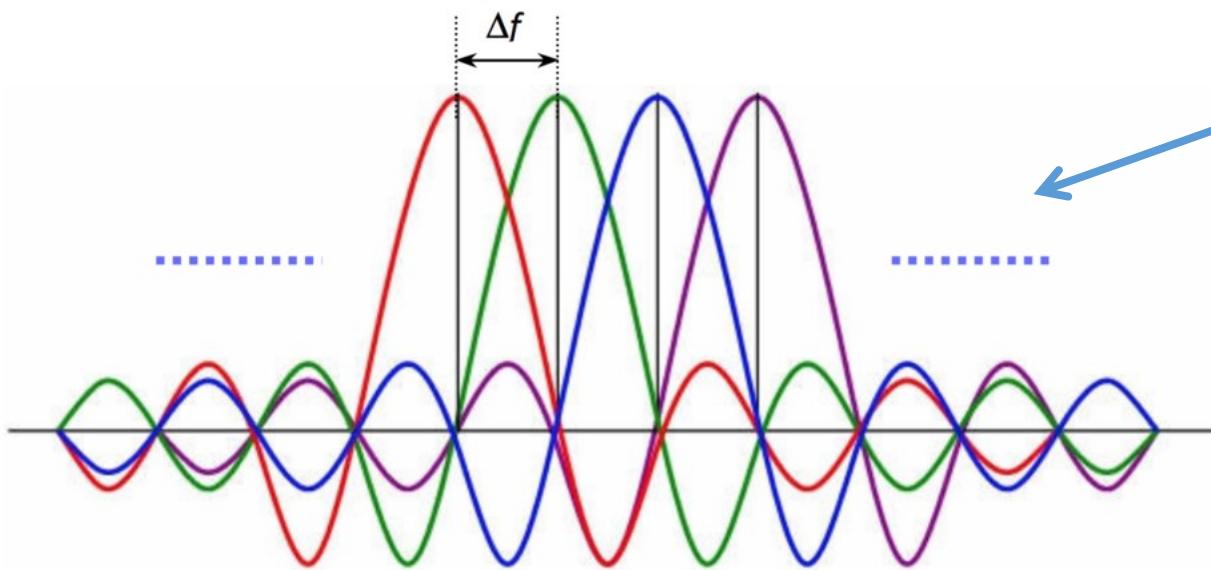
source : Denis Bakin, <http://www.okob.net/texts/mydocuments/80211physlayer/>

Orthogonal Frequency Division Multiplexing (OFDM)

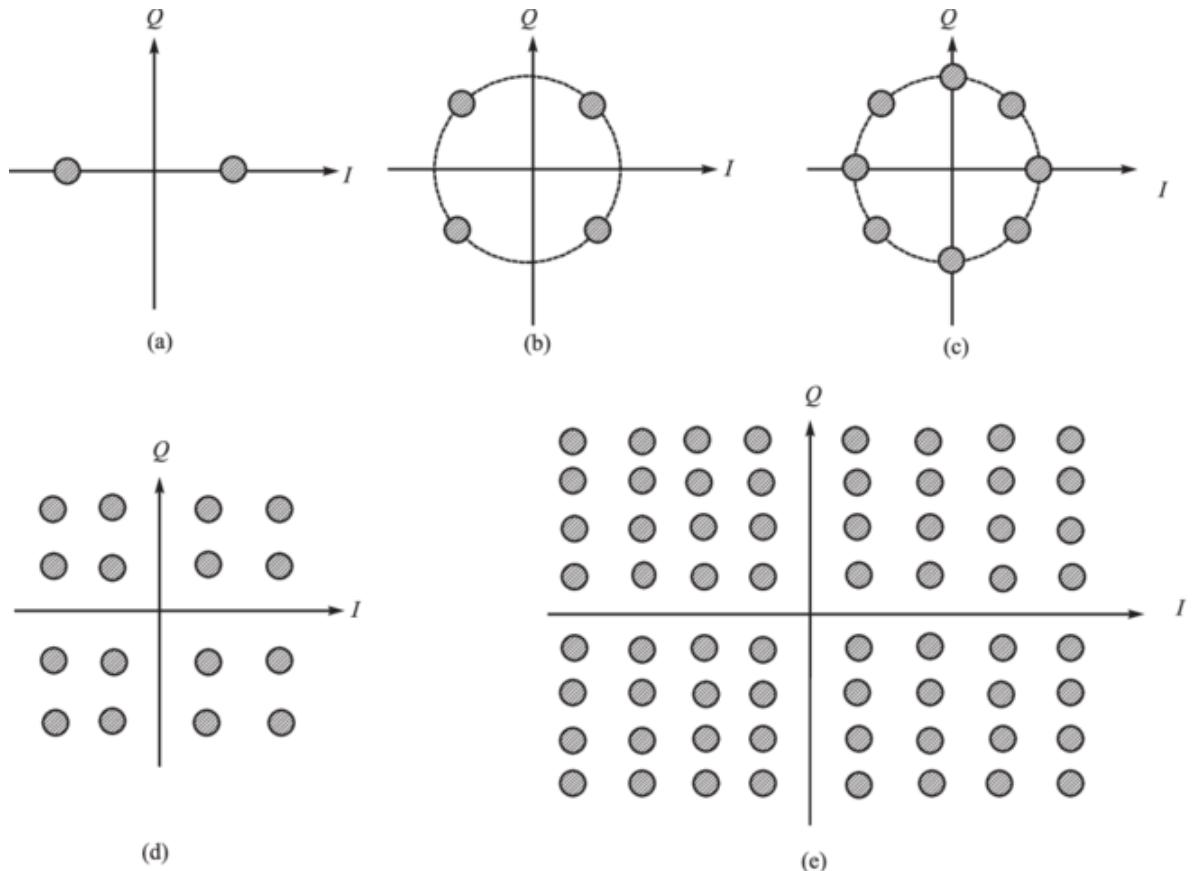
- Chaque canal est divisé en 52 sous porteuses orthogonales : 48 utilisées pour les données, et 4 pour les signaux de contrôle (appelées pilotes)
- Les sous porteuses adjacentes sont séparées par un intervalle de garde : pour éviter les interférences inter-symbole (ISI)
- Chaque sous porteuse est modulée selon l'une des modulations BPSK, QPSK, 16-QAM, 64 -QAM
- Les sous porteuses pilotes utilisent BPSK
- Un préambule pour la synchronisation est suivi d'un champ SIGNAL qui précise le débit et la modulation à utiliser

La forme des sous porteuses

- Les sous porteuses sont orthogonales entre elles
- A chaque point de pic d'amplitude d'une sous porteuse les autres sous porteuse ont une amplitude nulle



Modulation plus riche

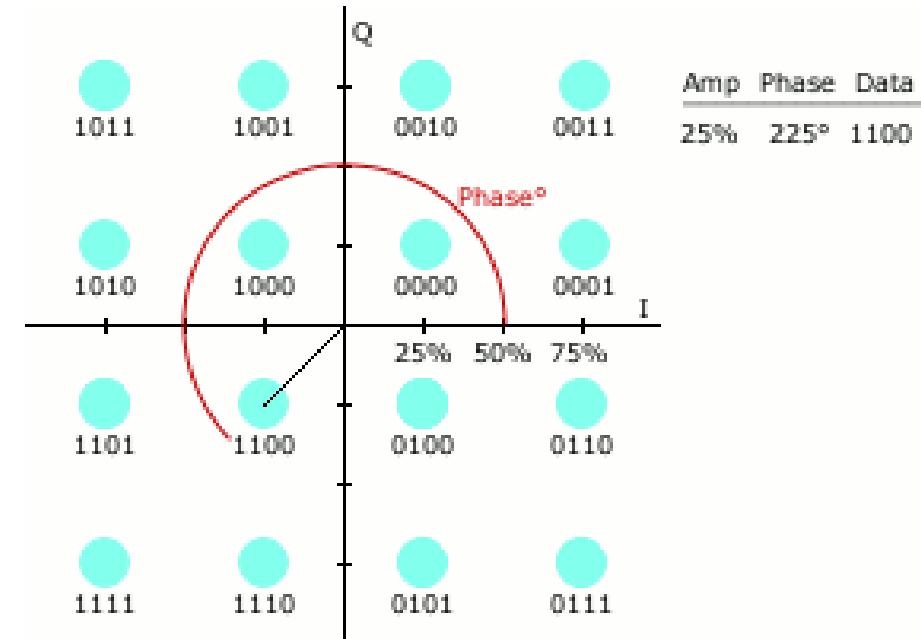


- Possibilité de transmettre plus de bits par symbole sans utiliser plus de bande passante
- (a) BPSK : 1 bit par symbole
- (b) QPSK : 2 bits par symbole
- ~~(c) 8-PSK : 3 bits par symbole~~
- (d) 16-QAM : 4 bits par symbole
- (e) 64-QAM : 8 bits par symbole

Source : Singh, Shree & Sengar, S & Bajpai, Rochak & Iyer, Sridhar. (2014)
Next-Generation Variable-Line-Rate Optical WDM Networks: Issues and Challenges.
Journal of Optical Communications. 34. 331-350.

Modulation 16-QAM

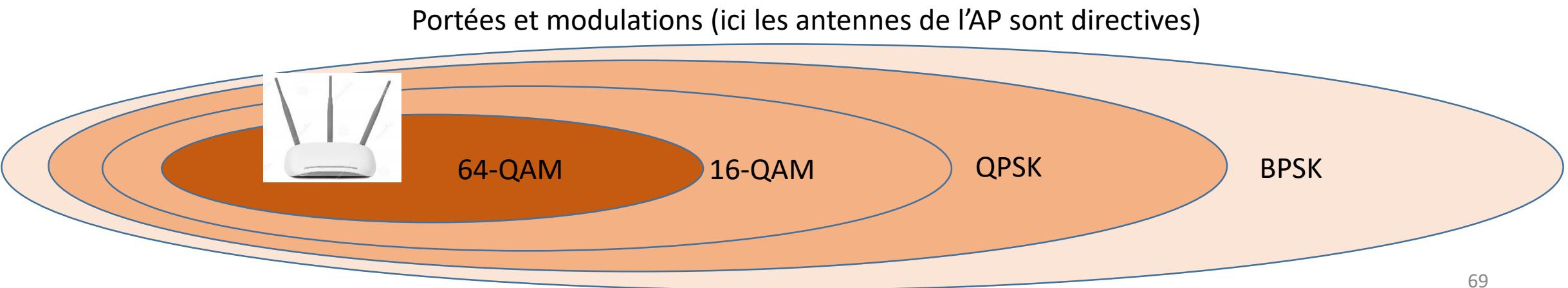
- Chaque symbole représente une valeur de 4 bits
- Selon l'amplitude et la phase, on déduit la valeur du symbole
- Exemple :
 - Un niveau d'amplitude de 25% et un déphasage de 225 degree représente la valeur 1100
 - Un niveau d'amplitude de 75% et un déphasage de 225 degree représente la valeur 1111



*By Chris Watts - Own work, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=15781908>*

Débits et modulations

- Avec un SNR suffisamment élevé, on peut utiliser 64-QAM
- Dès que le SNR diminue, la modulation s'adapte et par conséquence le débit est réduit
- Conclusion :
 - Pour atteindre les débits les plus élevés il faut avoir un SNR suffisamment élevé



Débits et modulation pour 802.11a

Modulation	Codage	Nombre de bits par sous porteuse	Nombre de bits par symbole OFDM	Nombre de bits de données	Débit en Mbps
BPSK	1/2	1	48	24	6
BPSK	3/4	1	48	36	9
QPSK	1/2	2	96	48	12
QPSK	3/4	2	96	72	18
16-QAM	1/2	4	192	96	24
16-QAM	3/4	4	192	144	36
64-QAM	2/3	6	288	192	48
64-QAM	3/4	6	288	216	54

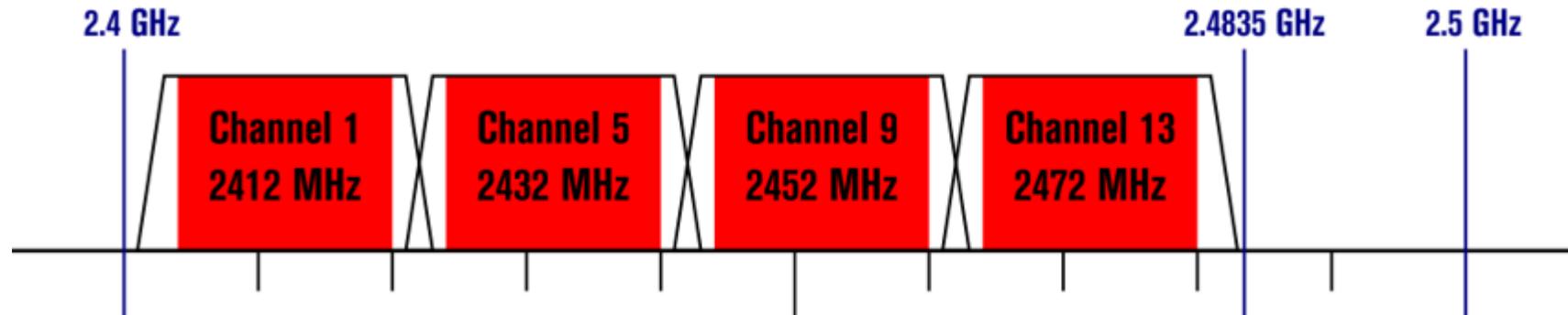
Code rate (Ratio de codage) :

- Codage convolutif qui rajoute des bits de parité pour corriger les erreurs
- k/n : n bits transmis, dont k bits de données
- $(n - k)$ bits sont introduits pour résister aux erreurs dues essentiellement à cause des interférences

WiFi 3 (802.11g-2003)

- 802.11g est une évolution de 802.11b
 - Elle opère sur la bande 2.4GHz
 - Utilise OFDM au lieu du DSSS
 - Mêmes débit que 802.11a

Les canaux de 802.11g



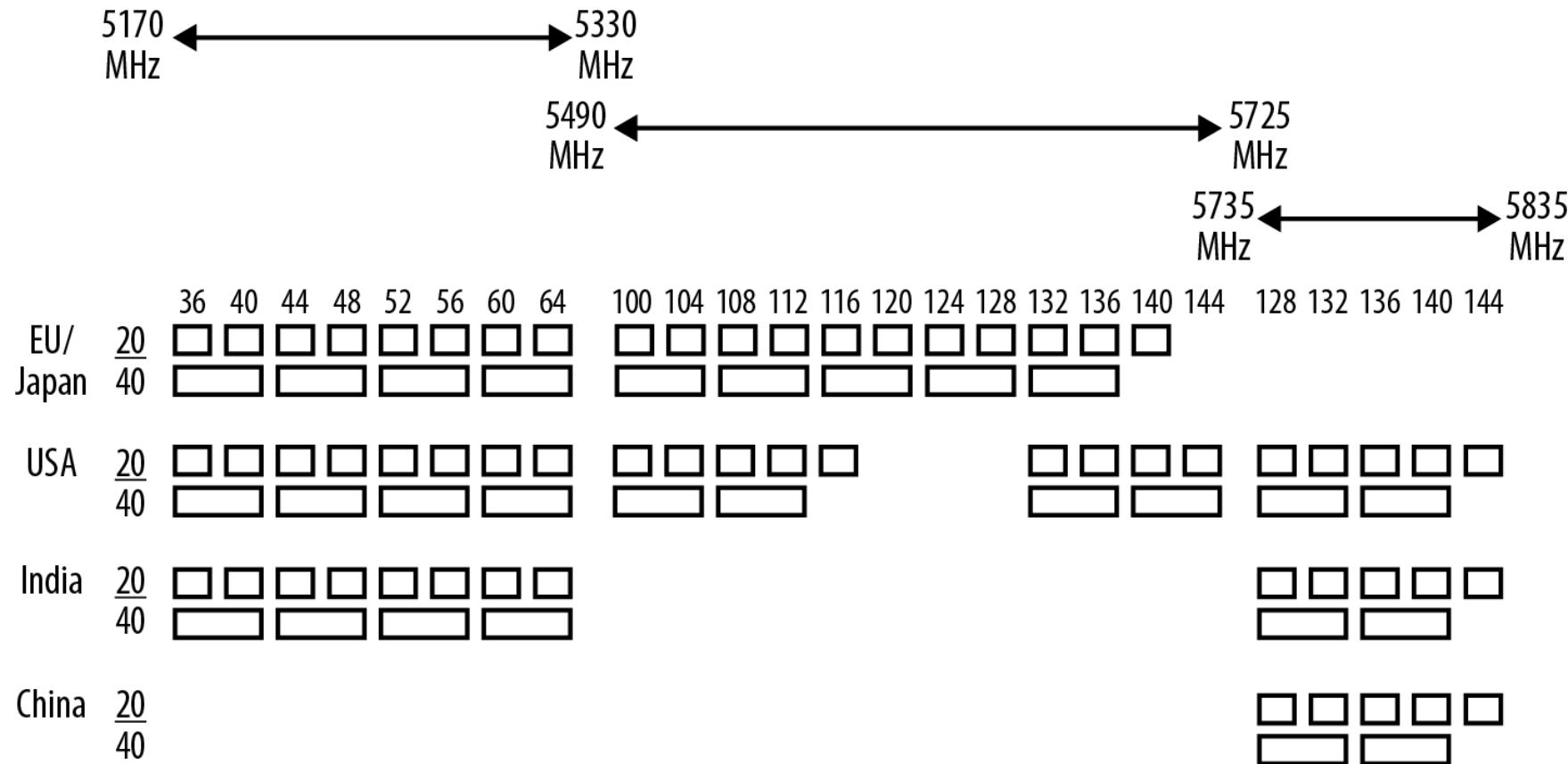
source en.wikipedia.org

- La bande 2.4GHz est découpée en 14 canaux
 - 4 seulement sont utilisables sans interférence (en Europe) : 1, 5, 9 et 13 avec une séparation de 20 MHz
 - 3 aux Etats Unis : 1, 6 et 11 avec une séparation de 25 MHz
- Chaque canal est de 20 MHz
 - Il est découpé en 52 sous-porteuses OFDM (dont 4 sont des porteuses pilotes pour monitorer l'état du canal)

WiFi 4 (802.11n-2009)

- Aussi appelé High Throughput OFDM (HT-OFDM)
- Amélioration par rapport à 802.11b/g/a
 - Plus de MCS (Modulation and Coding Schemes)
 - MIMO
 - Beamforming (antenne intelligente)
 - Largeur de canal de 40 MHz

Vue globale sur les canaux dans la bande 5GHz



Source : 802.11n A survival guide, Matthew Gast

High Throughput OFDM

- Le haut débit est atteint grâce à :
 - des techniques au niveau MAC :
 - Agrégation de trames MAC (moins d'ACK, moins d'entête, moins de IFS et délai d'accès)
 - des techniques au niveau PHY :
 - Fusion des canaux de 20 MHz en 40 MHz
 - Réduction des intervalles de garde de 800 à 400 us
 - Augmentation du nombre de sous-porteuse OFDM
 - 20 MHz : 56 au lieu de 52 avec a/g, dont 4 pilotes)
 - 40 MHz : 114 dont 6 pilotes
 - Transmission de plusieurs flux sur le même canal en même temps (MIMO)

MCS : Modulation and Coding Schemes

- Avant 802.11n, le débit était seulement fonction de la modulation et de la technique de codage
- A partir de 802.11n, la largeur et le nombre des canaux, ainsi que l'intervalle de garde sont aussi des éléments qui influent sur le débit
- L'état du canal vu par le récepteur détermine le MCS à utiliser parmi 77 MCS (la majorité des équipements implémentent 32 MCS seulement)
- Un compromis est à trouver entre maximisation du débit et réduction du taux d'erreur
- La négociation se fait en cours de transmission dans les champs HT Control Field des trames

Débit et MCS

<https://www.semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates>

$$\text{Data Rate} = \frac{N_{SD} * N_{BPSCS} * R * N_{SS}}{T_{DFT} + T_{GI}}$$

Number of Data Subcarriers → N_{SD}

Number of Coded Bits per Subcarrier per Stream → N_{BPSCS}

Coding → R

Number of Spatial Streams → N_{SS}

OFDM Symbol Duration → T_{DFT}

Guard Interval Duration → T_{GI}

Eléments de MCS

- Nombre de sous porteuse : N_{SD}
- Ratio de codage : R
- Nombre de flux spatial : N_{SS}
- Nombre de bits par sous porteuse : N_{BPSCS}
- Durée du symbole OFDM : T_{DFT}
- Durée de l'intervalle de garde : T_{GI}

Valeurs possibles

<https://www.semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates>

PHY	Modulation		R	N _{ss}	N _{SD}		T _{DFT}	T _{GI}	
	Name	N _{BPSCS}			20MHz	40MHz		Long	Short
802.11n (HT)	BPSK	1	1/2	1 to 4	52	108	3.2 µs	0.8 µs	0.4 µs
	QPSK	2	1/2 & 3/4						
	16-QAM	4	1/2 & 3/4						
	64-QAM	6	1/2 & 2/3 & 3/4						

Source :

<https://www.controleng.com/articles/understanding-modulation-and-coding-schemes/>

MCS index	Spatial streams	Modulation type	Code rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns Guard interval	400 ns Guard interval	800 ns Guard interval	400 ns Guard interval
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
16	3	BPSK	1/2	19.50	21.70	40.50	45.00
17	3	QPSK	1/2	39.00	43.30	81.00	90.00
18	3	QPSK	3/4	58.50	65.00	121.50	135.00
19	3	16-QAM	1/2	78.00	86.70	162.00	180.00
20	3	16-QAM	3/4	117.00	130.70	243.00	270.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
24	4	BPSK	1/2	26.00	28.80	54.00	60.00
25	4	QPSK	1/2	52.00	57.60	108.00	120.00
26	4	QPSK	3/4	78.00	86.80	162.00	180.00
27	4	16-QAM	1/2	104.00	115.60	216.00	240.00
28	4	16-QAM	3/4	156.00	173.20	324.00	360.00
29	4	64-QAM	2/3	208.00	231.20	432.00	480.00
30	4	64-QAM	3/4	234.00	260.00	486.00	540.00
31	4	64-QAM	5/6	260.00	288.80	540.00	600.00

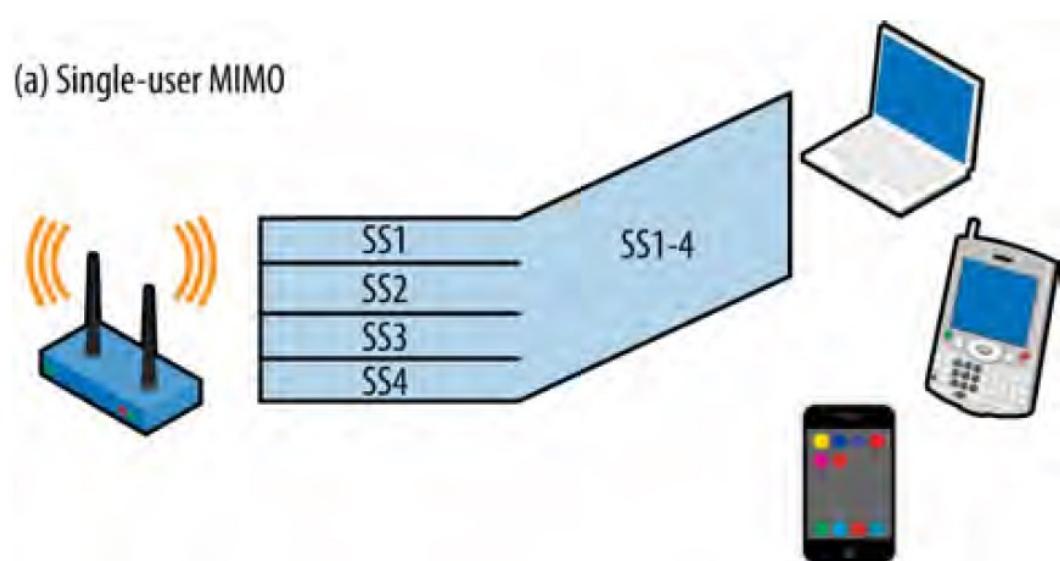
Quelques exemples de MCS 802.11n

Guard interval :

- Les intervalles de garde sont introduits pour mieux résister aux interférences inter symboles (ISI)
- Le délai d'étalement maximal est de 200 ns (en réalité il est autour de 50-75 ns en indoor)
- A chaque symbole un intervalle de garde de 800 ns est rajouté pour laisser suffisamment de temps entre 2 symboles consécutifs
- La réduction à 400 ns de cet intervalle permet un gain en débit de 10% environ
- Cette réduction peut être appliquée sans problème

Multiple Input Multiple Output (MIMO)

- Aussi appelé Single User MIMO, utilisé dans WiMAX et LTE
- Avec la technique MIMO chaque station devrait avoir plusieurs antennes
- Avec un signal par antenne
- Emetteur et récepteur doivent avoir des antennes MIMO
- L'ensemble des flux est destiné à un seul récepteur



Source : 802.11ac A survival guide, Matthew Gast

Les antennes MIMO peuvent exploiter les répliques du signal issues des multi-trajets pour améliorer la qualité du lien

Bénéfices des antennes MIMO

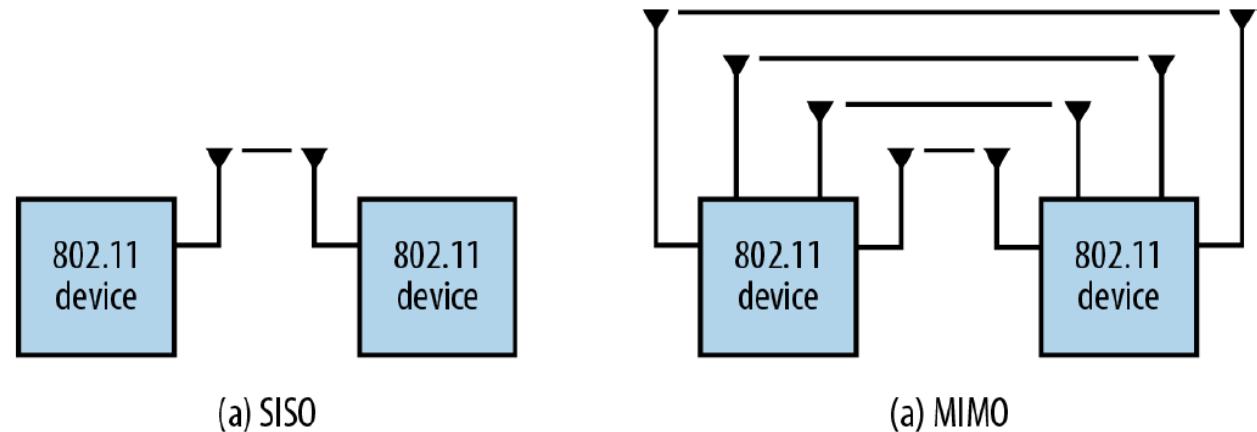
- Multiplexage spatial (augmentation de l'efficacité spectrale) : traitement parallèle de signaux différents. La séparation des signaux côté récepteur se fait ayant connaissances de l'état du canal
- Beamforming (amélioration de la qualité du signal) : transmissions simultanées par l'ensemble des antennes émettrices de façon à créer des interférences constructives sur le récepteur
- Codage espace-temps (diversité d'antenne) : réception multiple des différentes répliques et traitement du signal ayant la meilleure qualité

CSI (Channel State Information)

- Estimation de l'état du canal : quantification de l'effet de la propagation sur le signal reçu
 - Atténuation
 - Interférences
 - Interférences inter-symboles
 - Interférences inter-technologies
 - Interférences inter-canaux
- Ces informations sont souvent obtenues grâce à des séquences d'apprentissage transmis dans les trames de données et sur chaque sous porteuse
- Ces séquences sont connues et prédéfinies (insérées dans les champs HT-LTF, High Throughput Long Training Field)
- Le signal reçu est comparé au signal transmis, un feedback est renvoyé à l'émetteur

SISO vs MIMO

- Single Input Single Output : un seul flux circule entre l'émetteur et le récepteur
- En MIMO, plusieurs flux spatiaux circulent entre l'émetteur et le récepteur
- On parle de flux spatial car chaque signal traverse un trajet différent
- Chaque flux peut être assimilé à un lien 802.11b/a/g indépendant
 - Equal modulation : tous les flux utilisent le même MCS (le cas de la majorité des équipements)
 - Unequal modulation : chaque flux utilise un MCS différent (la fréquence peut avoir des impacts différents sur le phénomène multi-trajet)



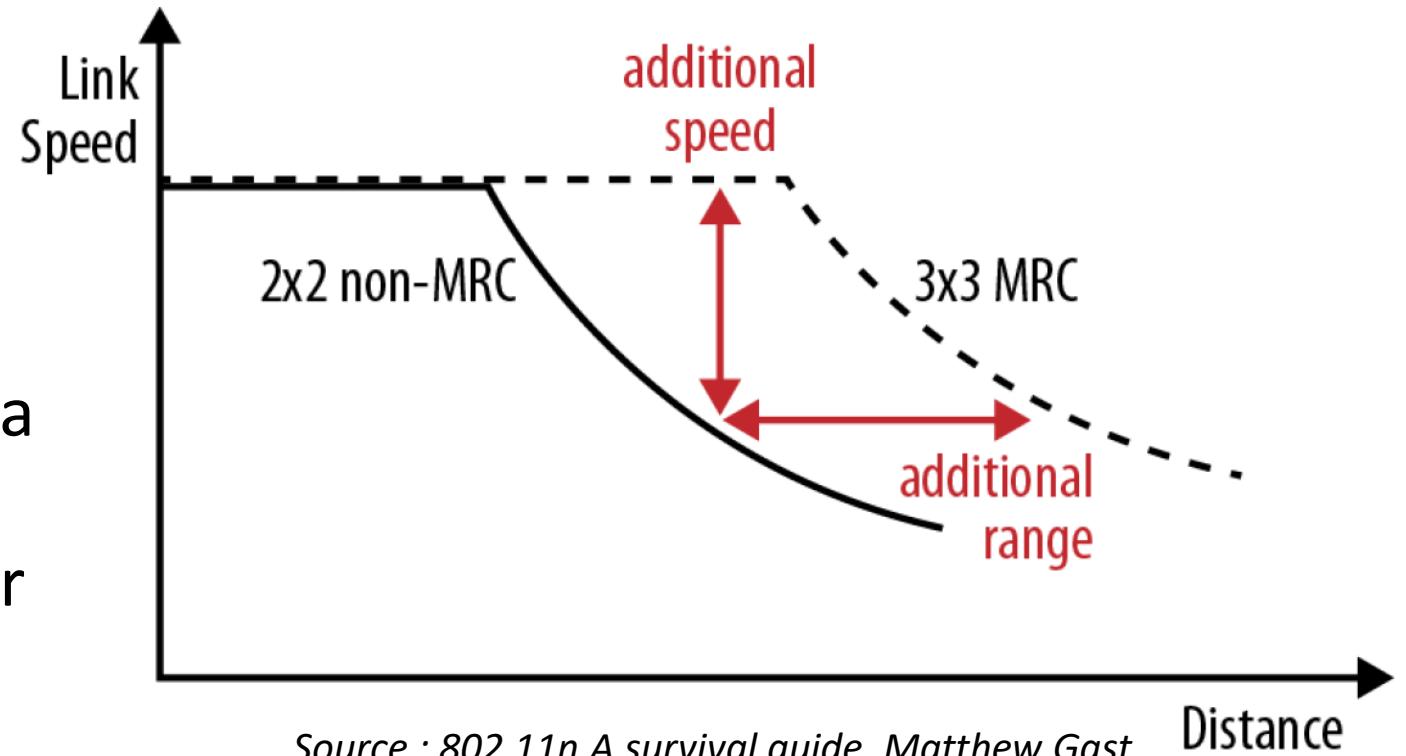
Source : 802.11n A survival guide, Matthew Gast

Terminologie MIMO

- Un système de communication MIMO est souvent désigné par la forme suivante : T x R : S
 - T représente le nombre d'antennes côté émetteur
 - R représente le nombre d'antennes côté récepteur
 - S représente le nombre de flux (chaque ayant sa propre chaîne de radio)
- T et R doivent au moins avoir la même valeur que S
- Exemples : 3x3:2 et 2x2:2
 - Ces deux systèmes donnent sensiblement les mêmes performances
 - Les premiers produits n sur le marché ne supportaient que 2 flux parallèles

Maximal Ratio Combining (MRC)

- Les systèmes ayant plus d'antennes que de flux spatiaux : les antennes supplémentaires permettent d'améliorer la qualité des liens
- Ceci permet au récepteur de récupérer différents bouts du signal à partir des antennes ayant la meilleure qualité par sous porteuse



Source : 802.11n A survival guide, Matthew Gast

- Ce graphe représente le gain que pourrait apporter un système 3x3:2 par rapport à un système 2x2:2
- Le pic de débit est le même, mais un meilleur débit est disponible sur un plus grande portée

Diversité d'antennes vs MIMO

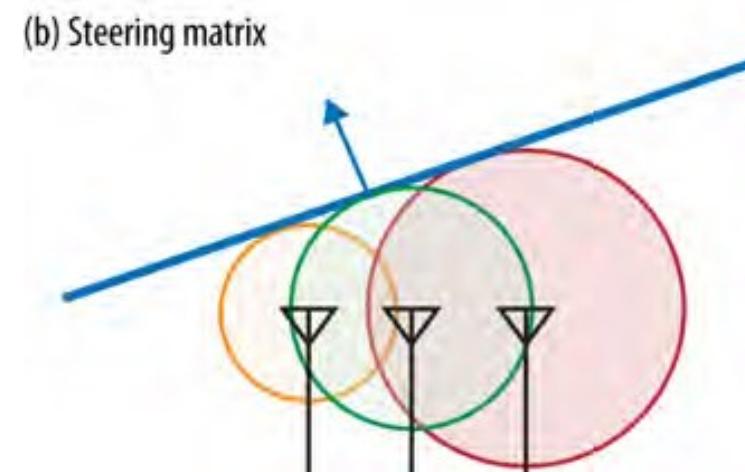
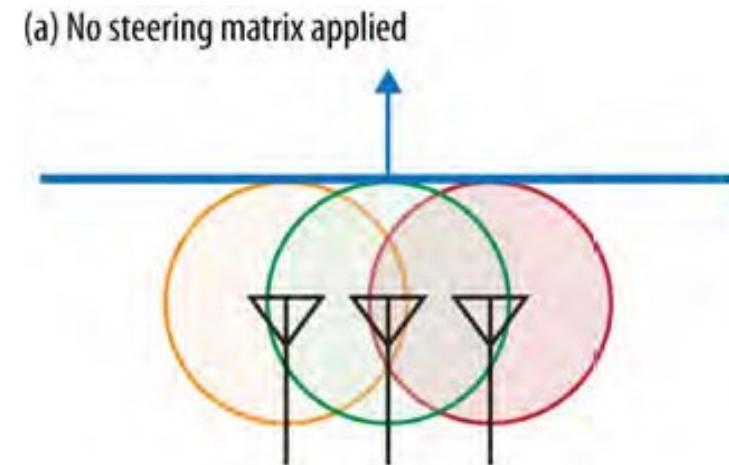
- Avoir plusieurs antennes ne veut pas toujours dire MIMO
- Un récepteur peut avoir plusieurs antennes reliées à un seul système de réception (transceiver) permettant une meilleure résistance au phénomène de multi-trajet
- Une seule antenne est utilisée à la fois dans un système de diversité d'antennes
- Un système de diversité d'antennes permet de choisir l'antenne qui offre le meilleur trajet du signal entre l'émetteur et le récepteur
- Un système MIMO permet d'exploiter plusieurs signaux contenant des informations différentes en même temps

Beamforming (antenne intelligente)

- C'est un mécanisme qui permet de diriger la transmission vers le récepteur avec un calibrage des phases des signaux générées par les différentes antennes
- On parle d'une matrice d'antennes qui permet de diriger le faisceau de transmission pour chaque trame (antenne intelligente)
- Ceci permet d'augmenter le ratio signal/bruit, ainsi permettre un meilleur débit pour certaines positions
- Il existe deux types de beamforming:
 - Beamforming implicite
 - Beamforming explicite (très peu implémenté)

Beamforming = décalage de phase

- Dans la figure (a), le réseau d'antennes commence la transmission en même temps
 - Le faisceau se dirige avec la même intensité dans toutes les directions
- Dans la figure (b), l'antenne de droite commence sa transmission en premier ensuite celle du milieu et ensuite celle de gauche
 - Le croisement des signaux se fera différemment
 - Le faisceau ainsi généré est orienté à gauche avec une intensité plus élevée



Beamforming explicite

- Selon cette méthode, l'entité qui souhaite ajuster le faisceau de son antenne (Beamformer, émetteur) envoie un message au destinataire appelé Sounding Frame (des messages spécifiques sans payload de type Null Data NDP, peuvent aussi être utilisés)
- Le destinataire répond avec un message indiquant « comment » la Sounding Frame a été reçue
- L'émetteur ajuste sa matrice d'antennes en comparant le message transmis à sa représentation issue de la réception
- Les équipements b/a/g ne peuvent pas faire de beamforming explicite, cette méthode fonctionne seulement avec 802.11n des 2 côtés

Beamforming implicite

- Cette méthode exploite les messages de données et d'ACK (surtout la perte des trames) pour estimer l'état du lien et ajuster le rayonnement de l'antenne
- Elle fonctionne avec des récepteurs b/a/g, seulement l'émetteur doit être en 802.11n
- Elle est moins précise que la méthode explicite
- C'est la méthode la plus implémentée sur les AP

Rétrocompatibilité

- Un réseau 802.11n peut permettre d'accueillir des équipements b/a/g
 - Modes : non-HT et HT-Mixed Mode (HT-MM)
- Quand le réseau 802.11n est strictement déployé pour des équipements 802.11n, il annonce ceci dans le beacon
 - Ce mode est appelé Greenfield Mode (HT-GF)

CCA avec 802.11n

Largeur du canal	Seuil détection de signal (dBm)	Seuil détection de signal Greenfield (dBm)	Seuil détection d'énergie canal secondaire (dBm)
20 MHz	-82	-72	-62
40 MHz	-79	-69	-59

- Comme pour les versions 802.11 précédentes, il existe 3 types de teste de CCA : détection de signal 802.11, détection d'énergie, détection de Greenfield
- Le seuil de détection de signal pour un canal de 20 MHz est -82 dBm
- On considère que le signal doit être suffisamment plus fort pour perturber la réception de 802.11
- On double le niveau quand on double la largeur du canal

20 MHz et 40 MHz

- Dans la bande 5 GHz, l'utilisation de canaux de 40 MHz est préconisée : il y a suffisamment de largeur de bande pour le faire
- Dans la bande 2.4 GHz, l'utilisation des 40 MHz est possible mais souvent non conseillée à cause du fait que la largeur totale de la bande est de 83 MHz
- Les 40 MHz permettent un meilleur débit par client par moment et sont fragilisées par les interférences
- Les 20 MHz permettent un meilleur débit par réseau et résistent mieux aux interférences

WiFi 5 (802.11ac-2013)

- Aussi appelé Very High Throughput (VHT-OFDM)
- Amélioration par rapport à 802.11n
 - MU-MIMO : 8 flux parallèles (vague 2)
 - Modulation 256 QAM
 - Choix de MCS simplifié (un MCS commun à l'ensemble des flux d'un beam)
 - Largeur de canal 80 (vague 1) et 160 (vague 2)
 - Beamforming : un seul mécanisme
 - CCA et RTS/CTS par canal

VHT-OFDM

- VHT est atteint grâce à :
 - La possibilité d'utiliser 8 flux en parallèle
 - A condition d'avoir 8 antennes sur l'AP
 - Avoir des canaux plus larges améliore le ratio sous porteuse de données par rapport aux sous porteuses pilotes
 - Moins d'overhead et de perte spectrale
 - 8 bits par porteuse avec la modulation 256-QAM, au lieu de 6 bits
 - Ceci donne une augmentation de capacité d'1/3

Valeurs possibles

<https://www.semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates>

PHY	Modulation		R	N _{ss}	N _{SD}				T _{DFT}	T _{GI}	
	Name	N _{BPSCS}			20MHz	40MHz	80MHz	160MHz		Long	Short
802.11n (HT)	BPSK	1	1/2	1 to 4					3.2 µs	0.8 µs	0.4 µs
	QPSK	2	1/2 & 3/4								
	16-QAM	4	1/2 & 3/4								
	64-QAM	6	1/2 & 2/3 & 3/4								
802.11ac (VHT)	BPSK	1	1/2	1 to 8	52	108	234	468	3.2 µs	0.8 µs	0.4 µs
	QPSK	2	1/2 & 3/4								
	16-QAM	4	1/2 & 3/4								
	64-QAM	6	1/2 & 2/3 & 3/4								
	256-QAM	8	2/3 & 5/6								

MCS Index - 802.11n and 802.11ac

802.11n 802.11ac

HT MCS Index	VHT MCS Index	Spatial Streams	Modulation	Coding	20MHz		40MHz		80MHz		160MHz	
					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
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
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

L'indexe MCS avec 802.11ac indique seulement le couple modulation/codage, contrairement à 802.11n où l'indexe désigne aussi le nombre de flux spatiaux

802.11ac - VHT

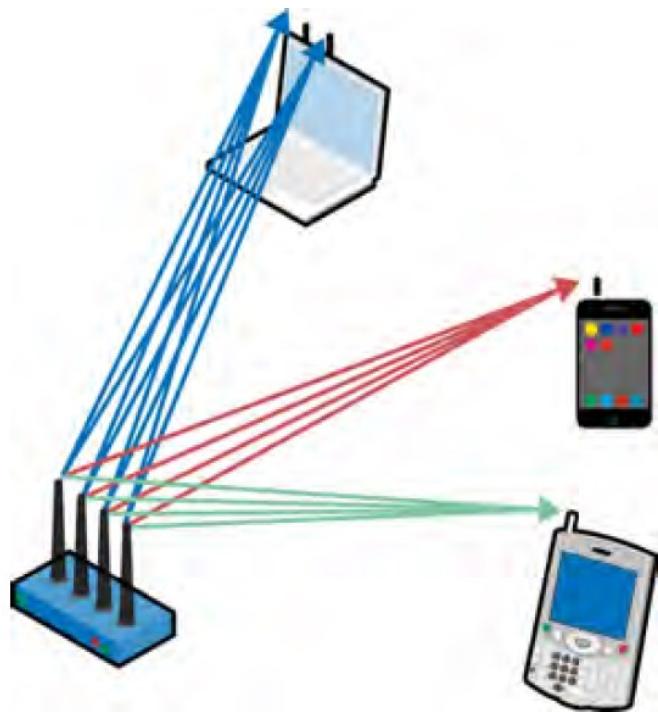
MCS, SNR and RSSI

VHT MCS	Modulation	Coding	20MHz				40MHz				80MHz				160MHz			
			Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI
			800ns	400ns			800ns	400ns			800ns	400ns			800ns	400ns		
1 Spatial Stream																		
0	BPSK	1/2	6.5	7.2	2	-82	13.5	15	5	-79	29.3	32.5	8	-76	58.5	65	11	-73
1	QPSK	1/2	13	14.4	5	-79	27	30	8	-76	58.5	65	11	-73	117	130	14	-70
2	QPSK	3/4	19.5	21.7	9	-77	40.5	45	12	-74	87.8	97.5	15	-71	175.5	195	18	-68
3	16-QAM	1/2	26	28.9	11	-74	54	60	14	-71	117	130	17	-68	234	260	20	-65
4	16-QAM	3/4	39	43.3	15	-70	81	90	18	-67	175.5	195	21	-64	351	390	24	-61
5	64-QAM	2/3	52	57.8	18	-66	108	120	21	-63	234	260	24	-60	468	520	27	-57
6	64-QAM	3/4	58.5	65	20	-65	121.5	135	23	-62	263.3	292.5	26	-59	526.5	585	29	-56
7	64-QAM	5/6	65	72.2	25	-64	135	150	28	-61	292.5	325	31	-58	585	650	34	-55
8	256-QAM	3/4	78	86.7	29	-59	162	180	32	-56	351	390	35	-53	702	780	38	-50
9	256-QAM	5/6			31	-57	180	200	34	-54	390	433.3	37	-51	780	866.7	40	-48
2 Spatial Streams																		
0	BPSK	1/2	13	14.4	2	-82	27	30	5	-79	58.5	65	8	-76	117	130	11	-73
1	QPSK	1/2	26	28.9	5	-79	54	60	8	-76	117	130	11	-73	234	260	14	-70
2	QPSK	3/4	39	43.3	9	-77	81	90	12	-74	175.5	195	15	-71	351	390	18	-68
3	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71	234	260	17	-68	468	520	20	-65
4	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67	351	390	21	-64	702	780	24	-61
5	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63	468	520	24	-60	936	1040	27	-57
6	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62	526.5	585	26	-59	1053	1170	29	-56
7	64-QAM	5/6	130	144.4	25	-64	270	300	28	-61	585	650	31	-58	1170	1300	34	-55
8	256-QAM	3/4	156	173.3	29	-59	324	360	32	-56	702	780	35	-53	1404	1560	38	-50
9	256-QAM	5/6			31	-57	360	400	34	-54	780	866.7	37	-51	1560	1733.3	40	-48
3 Spatial Streams																		
0	BPSK	1/2	19.5	21.7	2	-82	40.5	45	5	-79	87.8	97.5	8	-76	175.5	195	11	-73
1	QPSK	1/2	39	43.3	5	-79	81	90	8	-76	175.5	195	11	-73	351	390	14	-70
2	QPSK	3/4	58.5	65	9	-77	121.5	135	12	-74	263.3	292.5	15	-71	526.5	585	18	-68
3	16-QAM	1/2	78	86.7	11	-74	162	180	14	-71	351	390	17	-68	702	780	20	-65
4	16-QAM	3/4	117	130	15	-70	243	270	18	-67	526.5	585	21	-64	1053	1170	24	-61
5	64-QAM	2/3	156	173.3	18	-66	324	360	21	-63	702	780	24	-60	1404	1560	27	-57
6	64-QAM	3/4	175.5	195	20	-65	364.5	405	23	-62			26	-59	1579.5	1755	29	-56
7	64-QAM	5/6	195	216.7	25	-64	405	450	28	-61	877.5	975	31	-58	1755	1950	34	-55
8	256-QAM	3/4	234	260	29	-59	486	540	32	-56	1053	1170	35	-53	2106	2340	38	-50
9	256-QAM	5/6	260	288.9	31	-57	540	600	34	-54	1170	1300	37	-51			40	-48

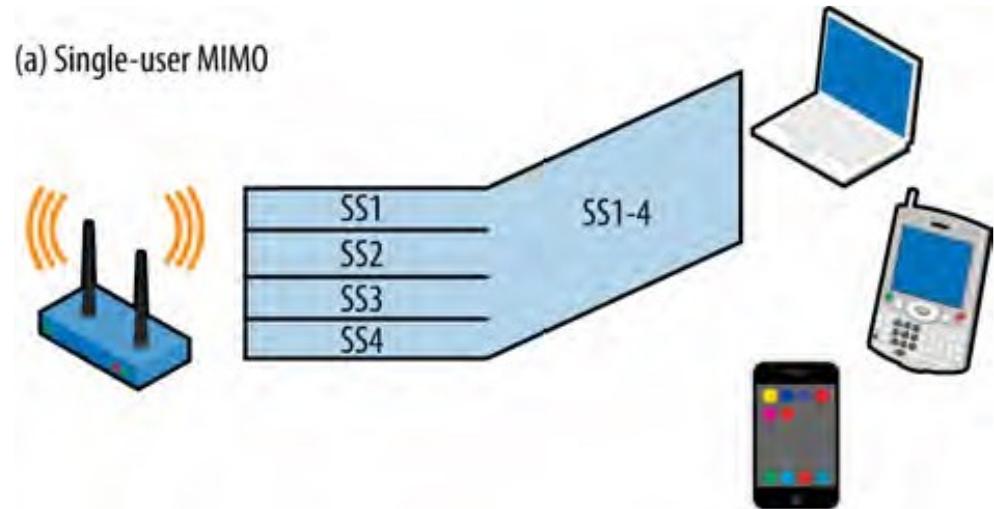
Valeurs min SNR et RSSI permettant d'utiliser les MCS

MU-MIMO

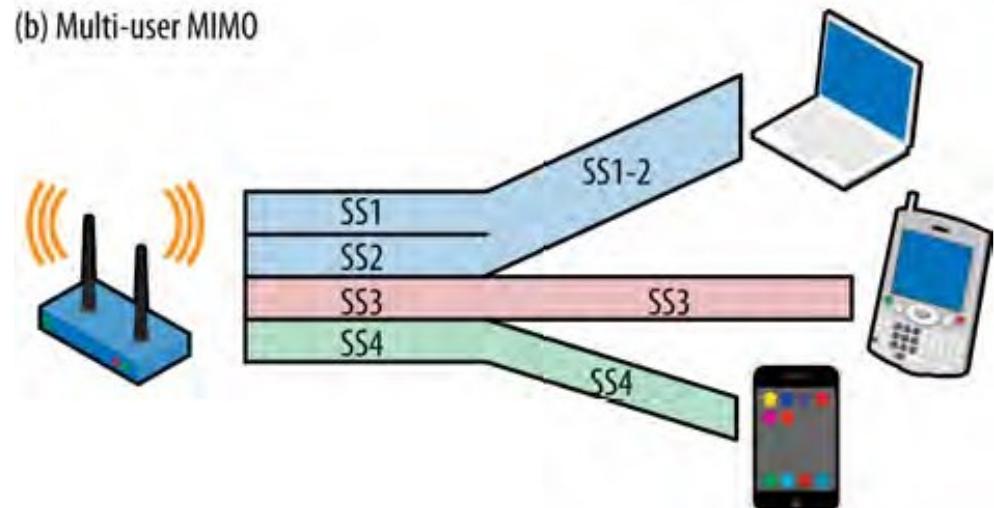
- Avant 802.11ac, on ne pouvait transmettre qu'une trame à la fois
- SU-MIMO tous les SS (Spatial Stream) sont à destination d'un client
- MU-MIMO les SS sont partagés entre plusieurs clients (4 clients simultanés maximum, appelés utilisateurs, avec max 4 SS par utilisateur)



(a) Single-user MIMO

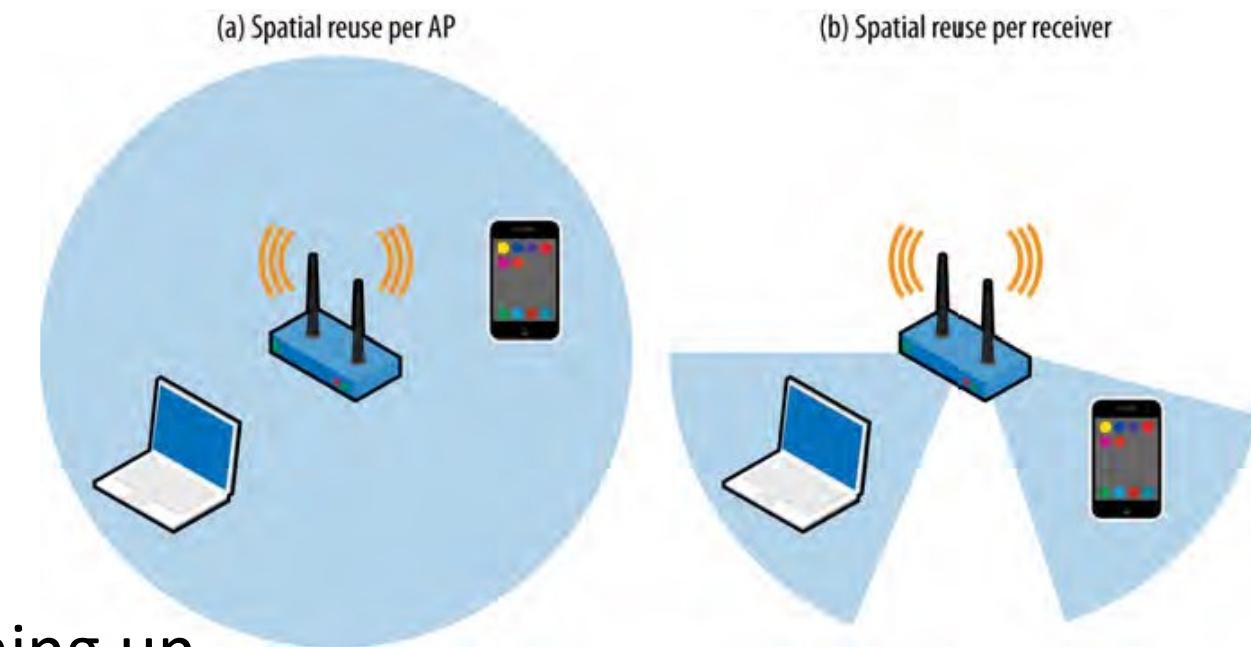


(b) Multi-user MIMO



Réutilisation spatiale

- La réutilisation spatiale permet de réutiliser le même canal de communication dans un endroit physique différent sans risque d'interférence
- Avec le MU-MIMO et le beamforming un AP divise le domaine de collision en plusieurs domaines (un domaine par faisceau)



Source : 802.11ac A survival guide, Matthew Gast

Un seul mécanisme de beamforming avec ac

- Plusieurs mécanismes de beamforming avec 802.11n
- Résultat :
 - Deux nœuds doivent négocier le mécanisme (se mettre d'accord un mécanisme commun)
 - Les différentes implémentations ne supportent pas toujours les mêmes mécanismes : échec de négociation
 - Beamforming rarement utilisé avec 802.11n
- 802.11ac spécifie un seul mécanisme de beamforming : Null Data Packet Sounding

Calibrage du canal (channel sounding)

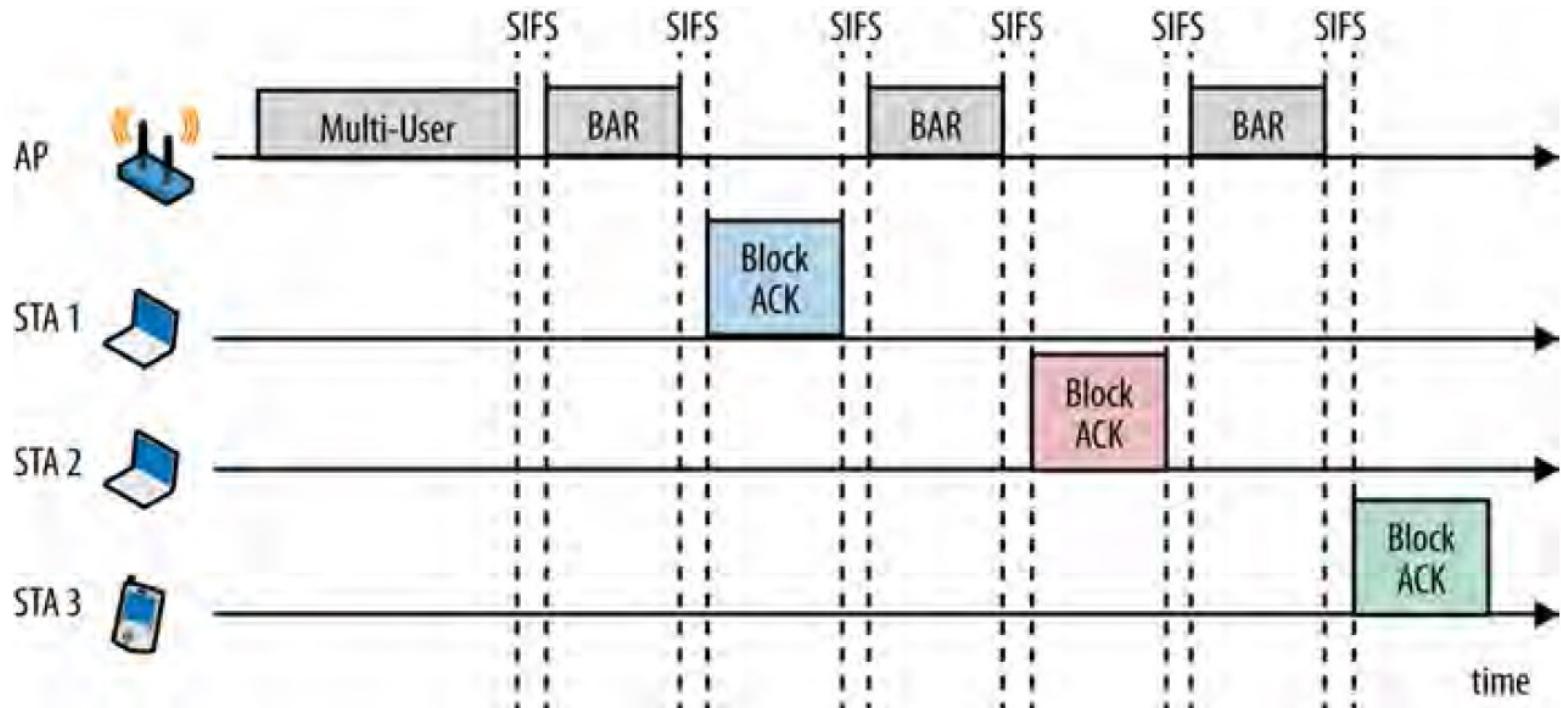
- Le calibrage du canal se fait à l'initiative de l'émetteur
- Cette opération se fait à travers l'échange de messages NDP (un message NDP est transmis à chaque destinataire)
- Le destinataire renvoie à l'émetteur un feedback (matrice de feedback) qui lui permet d'orienter son faisceau (on parle de steering matrix, matrice de guidage)
 - Le feedback est calculé en analysant les symboles des champs de training
- Ce calibrage représente un overhead non négligeable qui peut représenter 1% (surtout avec un grand nombre de clients par AP)
- La matrice de feedback est une version allégée de la matrice de guidage (ceci pour réduire la quantité d'information à transmettre)

La matrice de feedback

- Chaque sous porteuse du signal NDP est analysée indépendamment
 - Un champ VHT-LTF par flux dans la trame NDP
 - La valeur des puissances reçues et le décalage de phase sont relevés
- L'émetteur doit conserver une matrice de guidage pour chaque destinataire issue de sa matrice de feedback
- La taille de la matrice de feedback dépend :
 - De la largeur du canal : un canal plus large contient plus de sous porteuses et donc plus d'informations pour qualifier chaque sous porteuse
 - Le nombre d'antennes côté émetteur et côté récepteur : chaque sous porteuse est qualifiée pour chaque couple d'antennes
 - Le MU-MIMO et le fait d'avoir un beamforming par utilisateur et la précision de la qualification de chaque sous porteuse

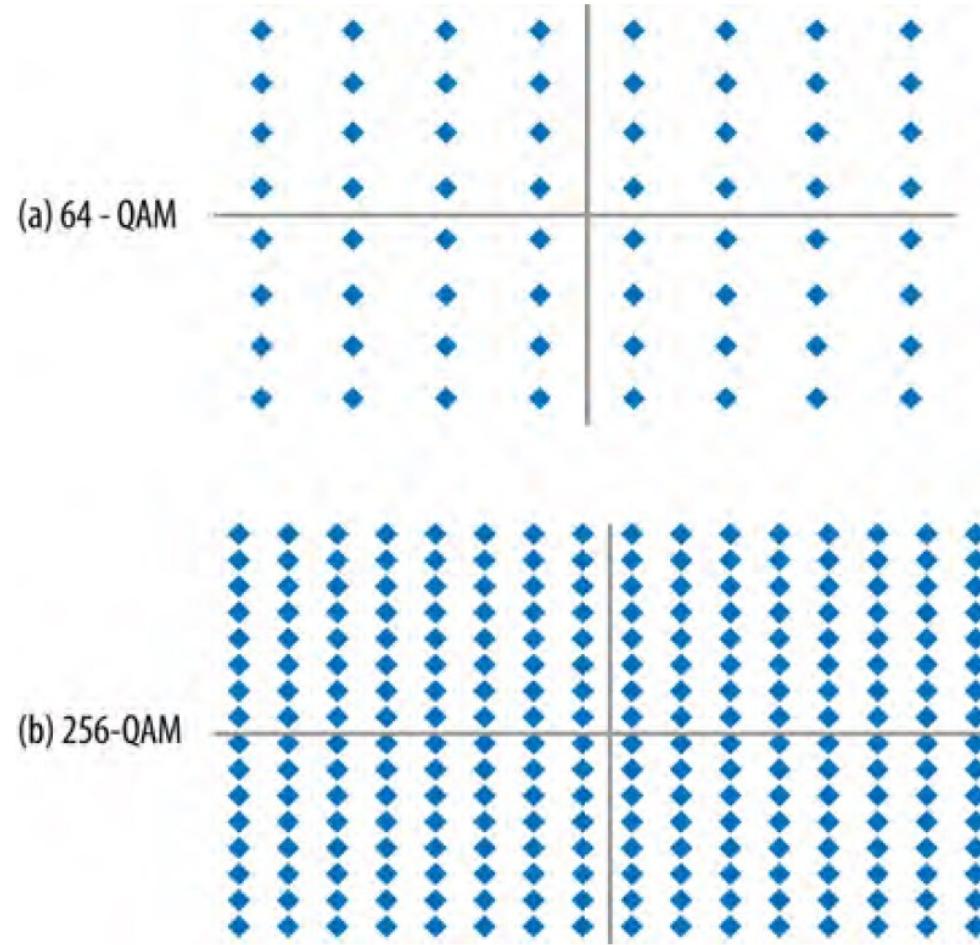
ACK in MU-MIMO

- Dans cet exemple, l'AP envoie les données en parallèle aux stations
- L'AP demande des ACK ensuite avec des Block ACK Requests (BAR) à destination de chaque station



Modulation 256-QAM

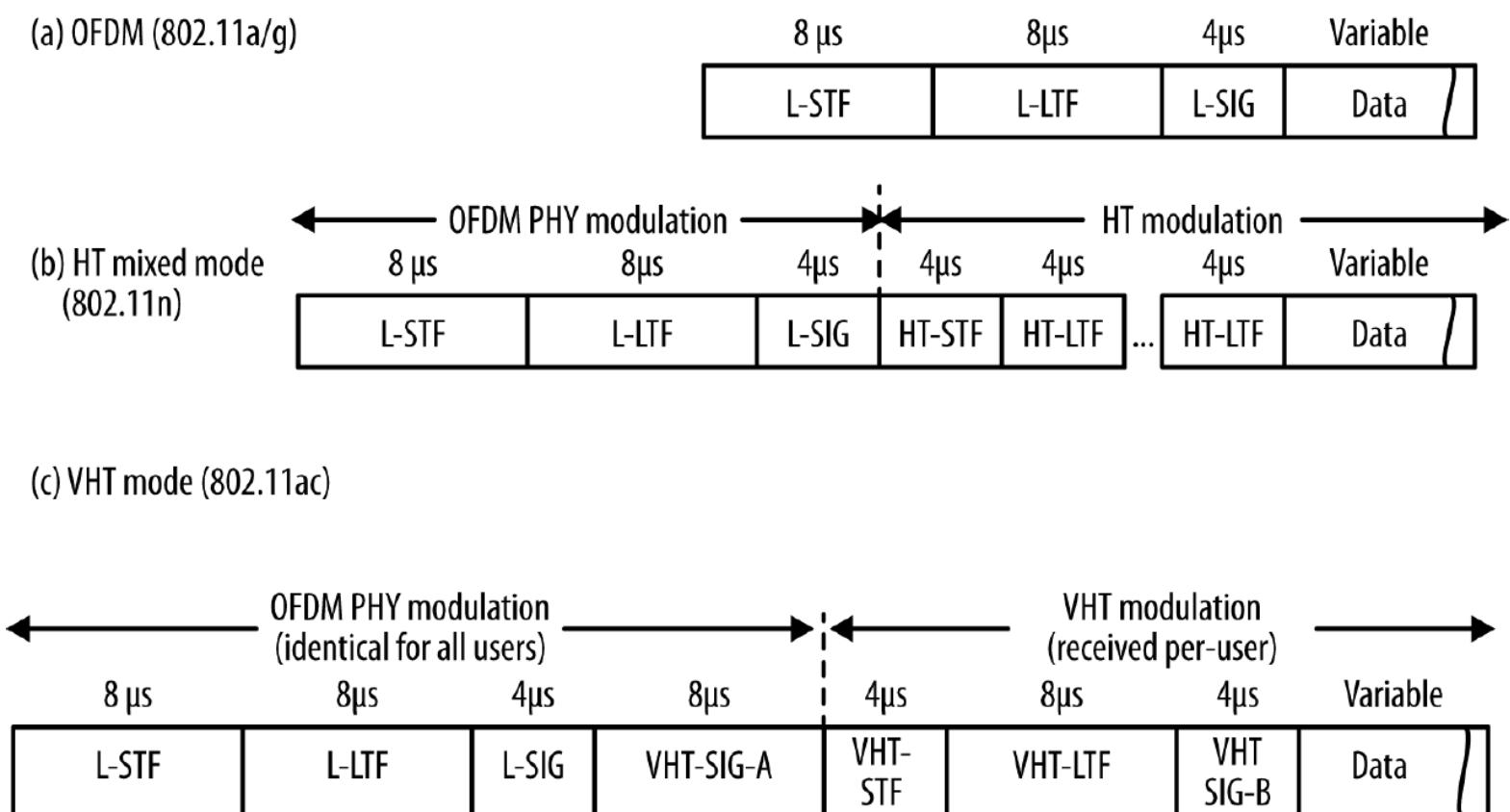
- La modulation 256-QAM permet de transmettre plus de données par sous porteuse
- En contre partie, elle est beaucoup moins robuste aux interférences et à l'atténuation
- Elle est donc essentiellement utilisée en LOS et à courte distance



Source : 802.11ac A survival guide, Matthew Gast

Entête PHY des trames

- Les champs L-STF et L-LTF sont conservés pour garantir la rétrocompatibilité
- Les champs VHT sont propres à 802.11ac (équivalents aux champs HT de 802.11n)



Source : 802.11ac A survival guide, Matthew Gast

Le champ VHT-SIG

- Ce champ qui est transmis en partie à tous les nœuds en BPSK permet, entre autre, d'indiquer :
 - la largeur du canal utilisé pour cette trame
 - le nombre de flux parallèles
 - le fait d'utiliser un long intervalle de garde ou pas
 - l'index MCS utilisé
 - le fait d'utiliser du beamforming ou pas
 - un CRC propre à ce champ

Débits 802.11ac

- Méthode simplifiée pour calculer le débit :
 - Partir de débits basiques avec 1 SS et 20 MHz
 - Multiplier le débit selon le nombre de SS
 - Multiplier le débit selon la largeur du canal

MCS value	20 MHz data rate (1SS, short GI)	Spatial stream multiplication factor	Channel width multiplication factor	Maximum 40 MHz rate (8 SS, short GI)	Maximum 80 MHz rate (8 SS, short GI)	Maximum 160 MHz rate (8 SS, short GI)
MCS 0	7.2 Mbps	x2 for 2 streams	x1.0 for 20 MHz	120.0 Mbps	260.0 Mbps	520.0 Mbps
MCS 1	14.4	x3 for 3 streams	x2.1 for 40 MHz	240.0	520.0	1040.0
MCS 2	21.7	x4 for 4 streams	x4.5 for 80 MHz	360.0	780.0	1560.0
MCS 3	28.9	x5 for 5 streams	x9.0 for 160 MHz	480.0	1040.0	2080.0
MCS 4	43.3	x6 for 6 streams		720.0	1560.0	3120.0
MCS 5	57.8	x7 for 7 streams		960.0	2080.0	4160.0
MCS 6	65.0	x8 for 8 streams		1080.0	2340.0	4680.0
MCS 7	72.2			1200.0	2600.0	5200.0
MCS 8	86.7			1440.0	3120.0	6240.0
MCS 9	96.3 ^a			1600.0	3466.7	6933.3

Source : 802.11ac A survival guide, Matthew Gast

Dynamic Frequency Selection (DFS)

- Sélection dynamique des fréquences
- Ce mécanisme est mis en place pour éviter d'utiliser des canaux utilisés par les **radars** :
 - Quand un AP détecte la présence de radar (il interprète un signal reçu comme étant émis par un radar) il abandonne le canal et passe sur un autre
 - Les radars émettent des impulsions qui durent entre 0.5 et 30 micro secondes
 - Pas de format prédéfini (**difficile à détecter**)
 - Ceci force tous les clients d'être déconnectés et à se reconnecter (faire des « probe requests » et recommencer l'association)
- **64% des canaux de la bande 5GHz doivent être utilisés avec DFS** (canaux 52 à 144)

Les canaux DFS

5 GHz Channel Allocations

Frequency (GHz)	5.150				5.250				5.470				5.600				5.640				5.725				5.850			
802.11 Allocations	UNII-1				UNII-2a				UNII-2c (Extended)								TDWR				UNII-3							
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720	5745	5765	5785	5805	5825			
20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165			
40 MHz	38	46			54	62			102	110		118		126		134	142				151	159						
80 MHz	42		58		106				122				138				155											
160 MHz	50				114																							
FCC	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250mw w/6dBi Indoor & Outdoor DFS Required 144 Now Allowed				120, 124, 128 Devices Now Allowed															
DFS Channels	DFS Channels																											

source : <https://www.ekahau.com>, Wireless LAN Professionals

Test de disponibilité des canaux

- Channel Availability Test
 - Au démarrage l'AP vérifie si le canal est utilisé par un radar
 - Si c'est le cas, le canal est évité pendant 30 minutes
 - Au bout de 30 minutes, l'AP teste à nouveau la disponibilité du canal
- L'AP écoute pendant 60 secondes sur chaque canal
 - Ce test peut prendre entre 1 et 10 minutes (ceci dépend des canaux disponibles dans la région du déploiement, voir https://en.wikipedia.org/wiki/List_of_WLAN_channels)

In-Service Monitoring

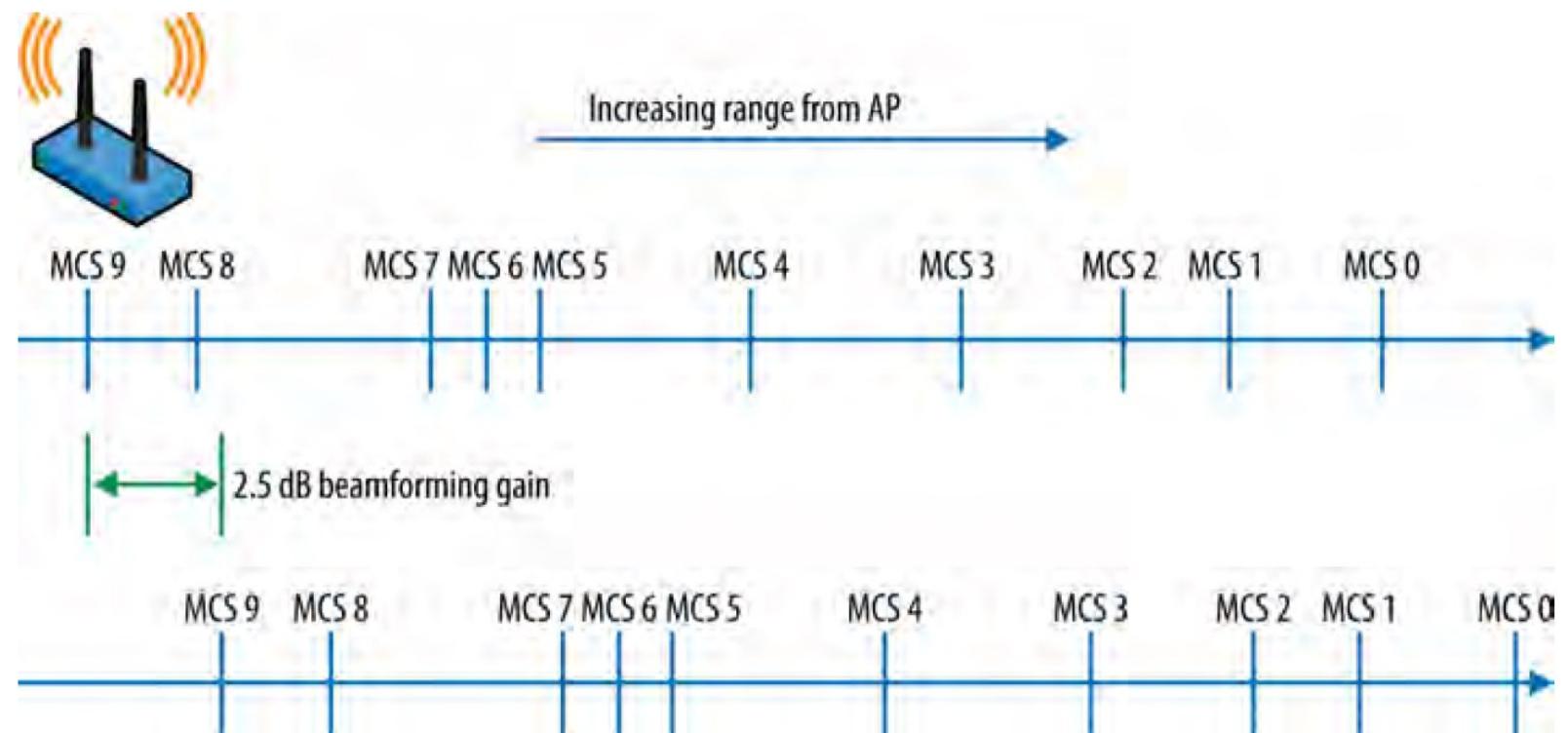
- Vérification en continu
 - Après le démarrage, un AP vérifie en continu la présence de radar à proximité
 - Si un signal est détecté, l'AP change de canal
 - Le changement de canal peut prendre environ 10 secondes
- Certains AP annoncent le changement de canal aux clients (ceci n'est pas supporté par tous les AP, ni tous les clients)
 - Channel Switch Announcement (CSA)
- Le choix du canal n'est pas spécifié dans la norme et chaque marque l'implémente à sa façon (prendre le canal 36, un autre canal non-DFS, ou bien n'importe quel autre canal)
- Au bout de 30 minutes, l'AP essaie de revenir sur le canal DFS

DFS

- Sur la plupart des AP, l'utilisation du DFS est souvent désactivée par défaut
 - Ceci fait que 64% des canaux ne soit pas utilisé
- **Les faux positifs**
 - Souvent, quand la charge du réseau augmente, certains AP se trompent et pensent avoir détecté un radar et lancent le processus de changement de canal
 - Ceci peut arriver à cause :
 - D'AP voisins
 - De fonctionnement anormal des cartes des clients
 - D'équipements à proximité qui émettent dans la bande 5GHz
 - D'une forte densité de clients
- Analyse des logs
 - En général, les faux positifs sont des évènements sporadiques et observés sur des canaux différents
 - Les vraies détections ont tendance à être observées sur les mêmes canaux et de façon régulière

Impact du beamforming

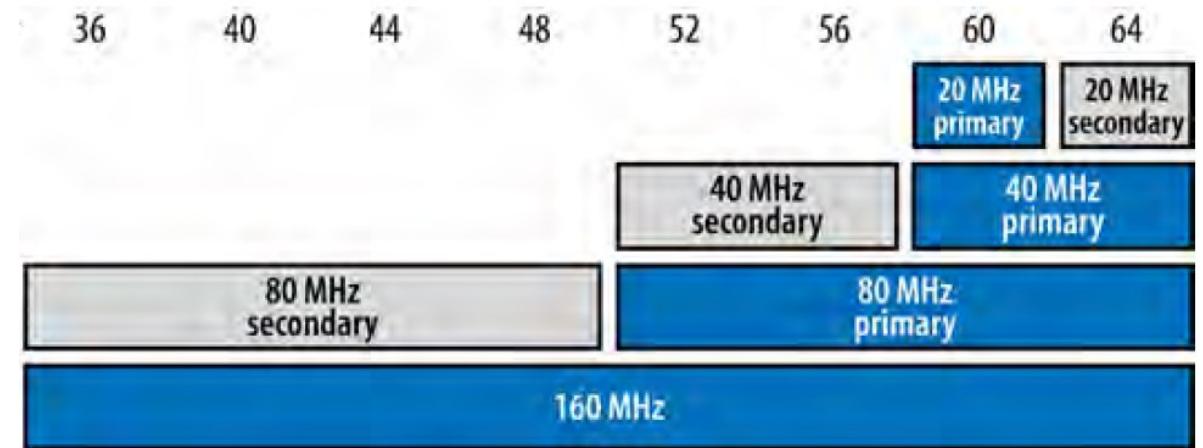
- Le beamforming permet d'utiliser des MCS à des distances plus grandes
- Ainsi, le débit est augmenté par rapport à un AP n'appliquant pas du beamforming
- Il peut apporter entre 2 et 5 dB d'augmentation (surtout à des distances moyennes)



Source : 802.11ac A survival guide, Matthew Gast

CCA par canal

- Notion de canal primaire et canal secondaire
- Le canal primaire est le canal utilisé de base auquel est associé un canal secondaire
- Le canal secondaire est adjacent au canal primaire
- Pour utiliser un canal de 160 MHz il faudra que l'ensemble des 8 canaux soit disponible
- La disponibilité du canal secondaire se fait à chaque transmission
- Ceci permet à plusieurs WLAN de partager les canaux disponibles (un réseau n'a pas toujours besoin d'utiliser la totalité des canaux)

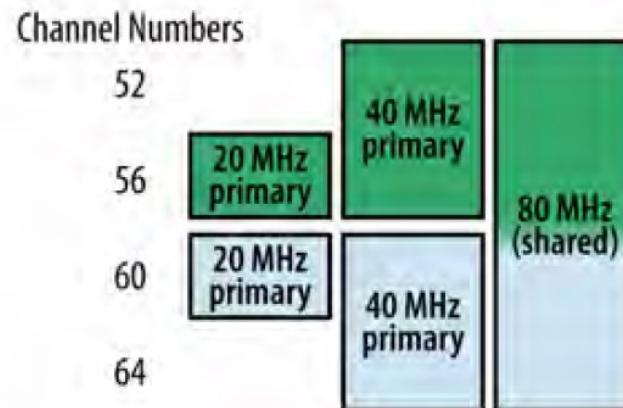


Source : 802.11ac A survival guide, Matthew Gast

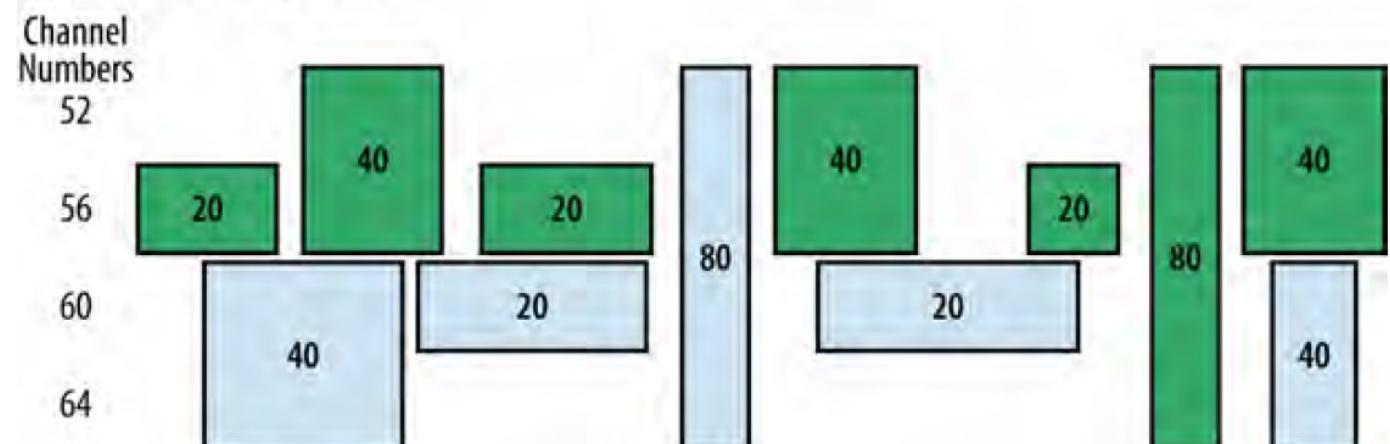
Utilisation des canaux

- La répartition des canaux est faite tel que indiqué dans la partie (a) entre 2 WLAN
- La partie (b) montre un exemple d'utilisation des canaux dans le temps

(a) Channel map



(b) Transmissions over time



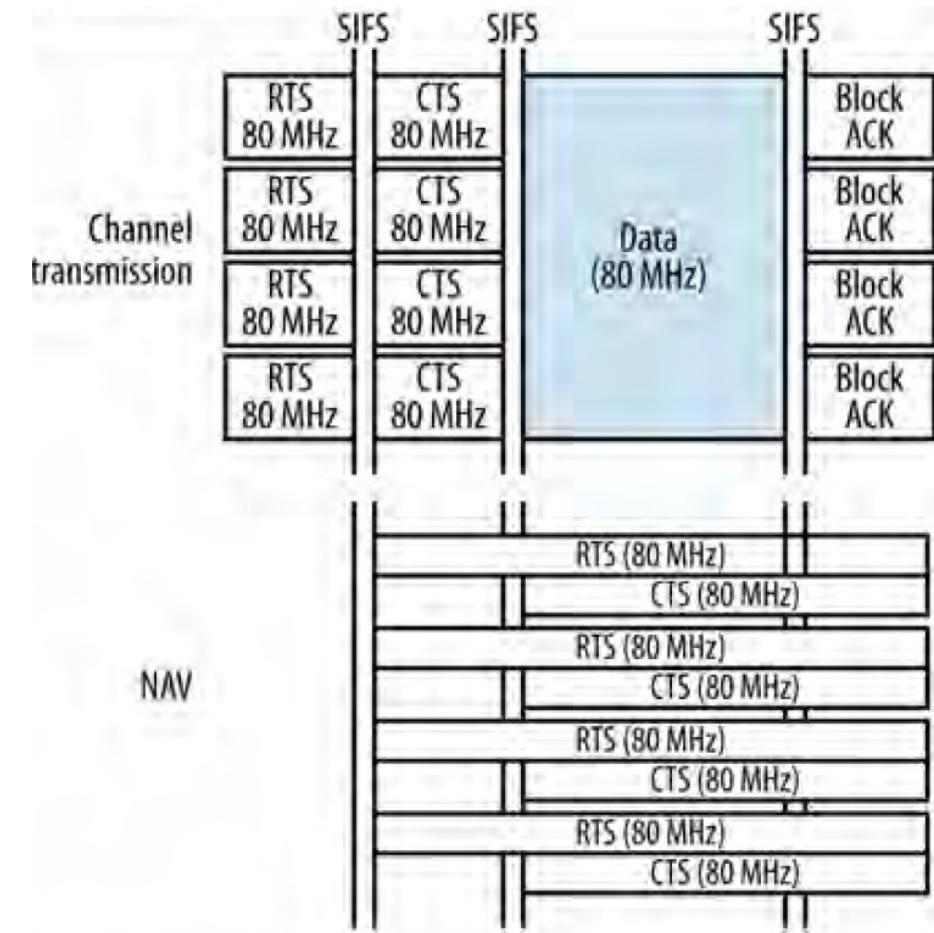
Disponibilité d'un canal

Largeur du canal	Seuil détection de signal canal primaire (dBm)	Seuil détection de signal canal secondaire (dBm)	Seuil détection d'énergie canal secondaire (dBm)
20 MHz	-82	-75	-62
40 MHz	-79	-72	-59
80 MHz	-76	-69	-56
160 MHz	-73	NA	NA

- Il existe 2 types de teste de CCA : détection de signal 802.11 et détection d'énergie
- La règle est la suivante : quand la largeur du canal est doublée, le seuil est aussi doublé (+3 dB veut dire que le seuil est doublé)
- Ceci permet de tenir compte du fait qu'un émetteur aurait réparti sa puissance d'émission sur un canal de largeur double et donc perdu la moitié de l'intensité de son signal
- En réalité, la puissance de transmission est répartie sur l'ensemble du canal, et donc la puissance par sous porteuse est proportionnelle à la largeur de la porteuse (312,5KHz)

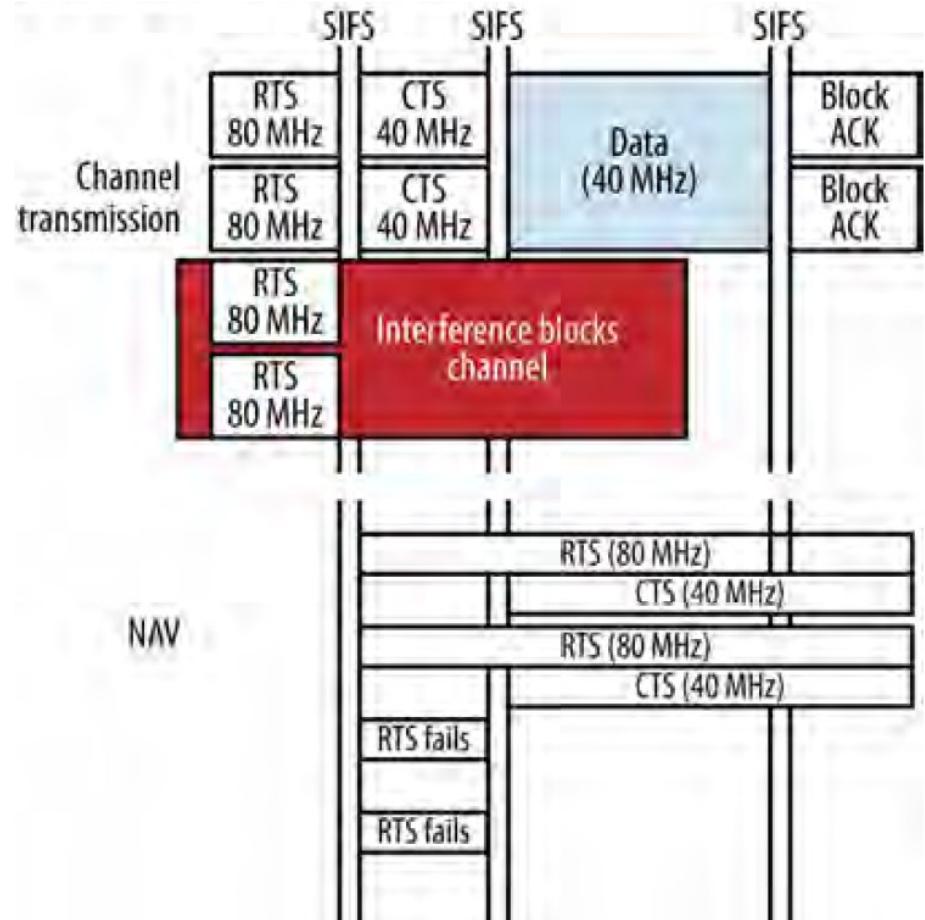
RTS/CTS par canal

- Un émetteur qui souhaite envoyer une donnée sur un canal de 80 MHz transmet un RTS sur chacun des 4 canaux 20 MHz
- Le récepteur répond par 4 CTS
- Les RTS/CTS sont transmis avec des débits de 802.11a pour que toutes les stations puissent mettre à jour leur NAV



RTS/CTS par canal

- Dans cet exemple seulement 2 des 4 canaux 20 MHz sont disponibles
- Ceci peut être dû à des collisions par exemple
- 2 CTS sont reçus et la transmission des données se fait sur un canal de 40 MHz



WiFi 6 (802.11ax-2019)

- Aussi appelé High Efficiency (HE-OFDMA)
- OFDMA (Orthogonal Frequency Division Multiple Access) en UL et DL (Up Link et Down Link)
- MU-MIMO UL et DL (avec ac c'était seulement en DL)
- Une modulation supplémentaire : 1024-QAM
- Utilisation des 2 bandes : 2.4 GHz et 5 GHz
- Durée du symbole passe de 3.2 à 12.8 us
- ... il y a 72 nouvelles fonctionnalités spécifiées

Ce qui a vraiment changé avec 802.11ax

802.11b



Ce qui a vraiment changé avec 802.11ax

802.11a/g



Ce qui a vraiment changé avec 802.11ax

802.11n



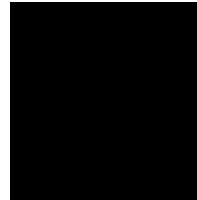
Ce qui a vraiment changé avec 802.11ax

802.11ac



Ce qui a vraiment changé avec 802.11ax

802.11ax



HE-OFDM et HE-OFDMA

- Avec 802.11ax, on passe de 52 sous porteuses à 234 sous porteuses par canal de 20 MHz (HE-OFDM) appelées tones
 - On passe de 312.5 KHz à 78.125 KHz par sous porteuse (x4)
- OFDMA : déjà utilisée dans WiMAX, 4G et LTE
- En OFDMA, les sous porteuses d'un canal sont réparties sur plusieurs clients (HE-OFDMA)
 - Ceci permet de transmettre des données en parallèle avec des délais réduits
 - Mais, à un débit réduit car moins de bits par seconde sont transmis par client
- OFDMA permet de réduire le temps perdu à gagner la contention au canal
 - Une fois la contention gagnée, la station peut transmettre plusieurs trames en parallèle, au lieu de perdre du temps de contention pour chacune des trames

Allocation des sous porteuses avec OFDMA

- L'allocation des sous porteuses peut se faire par trame
- Cette allocation permet de gérer plus d'utilisateurs (mais à débit réduit)
 - Chaque utilisateur aura un nombre de sous porteuse (une part du canal) adapté à sa situation
- Pour le flux descendant (AP → utilisateurs), l'AP gère la répartition des canaux
- Pour le flux montant (utilisateurs → AP), l'AP transmet une trame de déclanchement (Trigger Frame) qui indique à chaque utilisateur son intervalle de transmission ainsi que les sous porteuses, MCS et puissance de transmission
 - Les utilisateurs informent l'AP de leur besoin en transmission avec des trames Buffer Status Report (BSR) en réponse à une BSR Poll envoyée par l'AP

Débit et MCS

<https://www.semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates>

$$\text{Data Rate} = \frac{N_{SD,U} * N_{BPSCS,U} * R * N_{SS}}{T_{DFT} + T_{GI}}$$

Number of Data Subcarriers per Resource Unit

Number of Coded Bits per Subcarrier per Stream for the Resource Unit

Coding

Number of Spatial Streams

OFDM Symbol Duration

Guard Interval Duration

```
graph TD; A[NSD,U] --> B[Number of Data Subcarriers per Resource Unit]; C[NBPSCTS,U] --> D[Number of Coded Bits per Subcarrier per Stream for the Resource Unit]; E[R] --> F[Coding]; G[NSS] --> H[Number of Spatial Streams]; I[TDFT] --> J[OFDM Symbol Duration]; K[TGI] --> L[Guard Interval Duration]
```

Eléments de MCS

- Nombre de sous porteuse par unité de ressource : $N_{SD,U}$
- Ratio de codage : R
- Nombre de flux spatial : N_{SS}
- Nombre de bits par sous porteuse par unité de ressource : $N_{BPSCS,U}$
- Durée du symbole OFDM : T_{DFT}
- Durée de l'intervalle de garde : T_{GI}

Valeurs possibles (HE, High Efficiency)

HE-OFDM

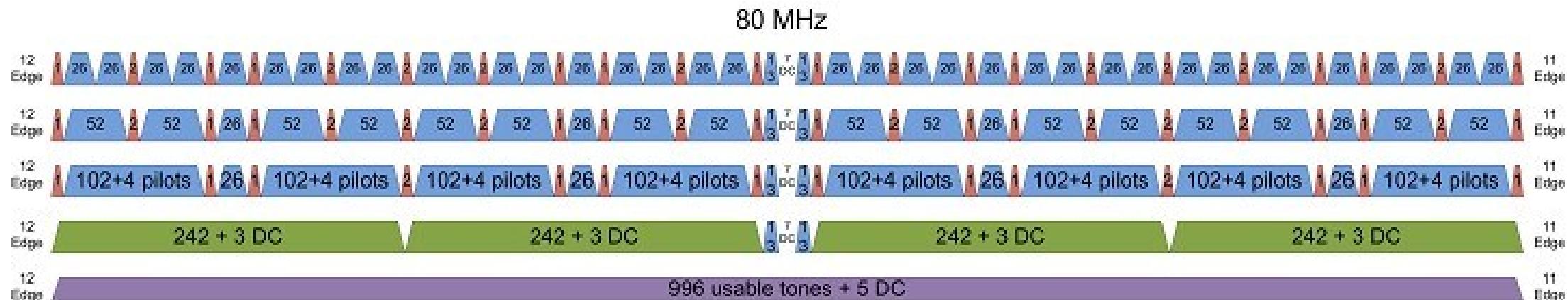
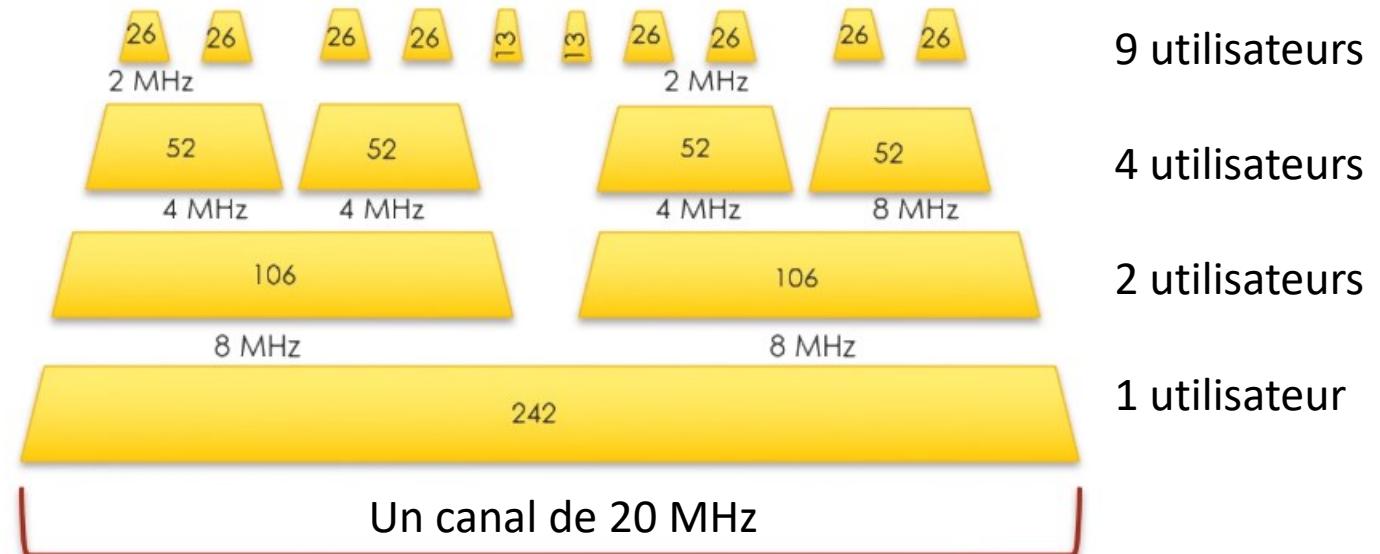
PHY	Modulation		R	N _{ss}	N _{SD}				T _{DFT}	T _{GI}		
	Name	N _{BPSCS}			20MHz	40MHz	80MHz	160MHz		Long	Medium	Long
802.11ax (HE)	BPSK	1	1/2	1 to 8	234	468	980	1960	12.8 µs	0.8 µs	1.2 µs	3.2 µs
	QPSK	2	1/2 & 3/4									
	16-QAM	4	1/2 & 3/4									
	64-QAM	6	1/2 & 2/3 & 3/4									
	256-QAM	8	2/3 & 5/6									
	1024-QAM	10	3/4 & 5/6									

HE-OFDMA

PHY	Modulation		R	N _{ss}	N _{SD}						T _{DFT}	T _{GI}		
	Name	N _{BPSCS}			26-tone	52-tone	106-tone	242-tone	484-tone	996-tone		Long	Medium	Long
802.11ax (HE)	BPSK	1	1/2	1 to 8	24	48	102	234	468	980	12.8 µs	0.8 µs	1.2 µs	3.2 µs
	QPSK	2	1/2 & 3/4											
	16-QAM	4	1/2 & 3/4											
	64-QAM	6	1/2 & 2/3 & 3/4											
	256-QAM	8	2/3 & 5/6											
	1024-QAM	10	3/4 & 5/6											

RU (Resource Units)

- LE canal peut être découpé en RU
- Les RU peuvent avoir des tailles différentes
- On peut avoir 9 RU par canal de 20 MHz (2x13 forment une RU)



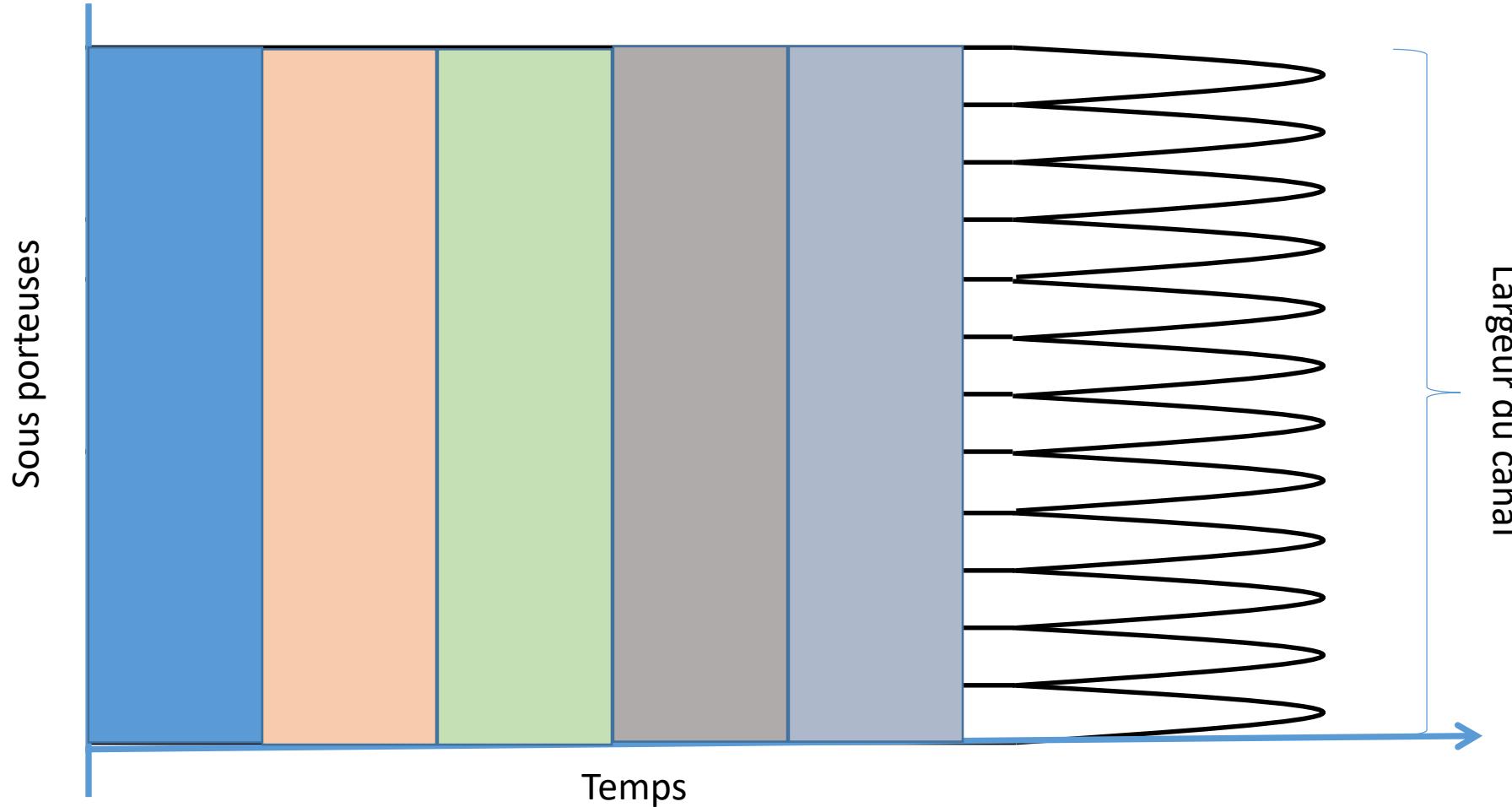
source : <http://www.ni.com/fr-fr/innovations/white-papers/16/introduction-to-802-11ax-high-efficiency-wireless.html>

Allocation des RU dans les champs User Information d'une trame Trigger

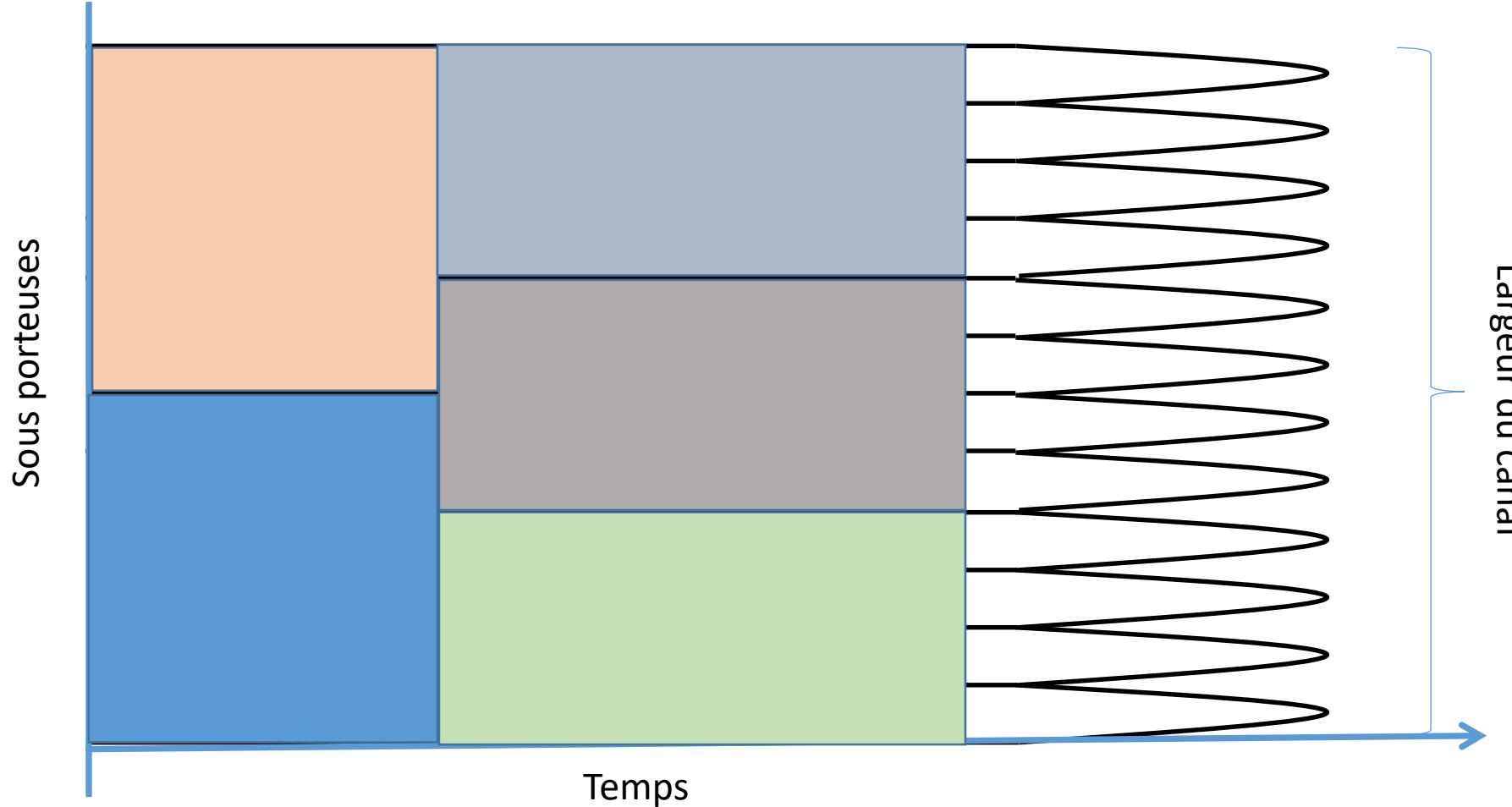
26 tone RU	RU-1	RU-2	RU-3	RU-4	RU-5	RU-6	RU-7	RU-8	RU-9
Subcarrier range	-121:-96	-95:-70	-68:-43	-42:-17	-16:-4, 4:16	17:42	43:68	70:95	96:121
RU allocation bits	0000000	0000001	0000010	0000011	0000100	0000101	0000110	0000111	0001000
52 tone RU	RU-1	RU-2			RU-3		RU-4		
Subcarrier range	-121:-70	-68:-17			17:68		70:121		
RU allocation bits	0100101	0100110			0100111		0101000		
106 tone RU		RU-1				RU-2			
Subcarrier range		-122:-17				17:122			
RU allocation bits		0110101				0110110			
242 tone RU			RU-1						
Subcarrier range			-122:-2, 2:122						
RU allocation bits			0111101						

source : <https://blog.aerohive.com/802-11ax-allocate-ofdma-ru/>

Allocation des sous porteuses avec OFDM

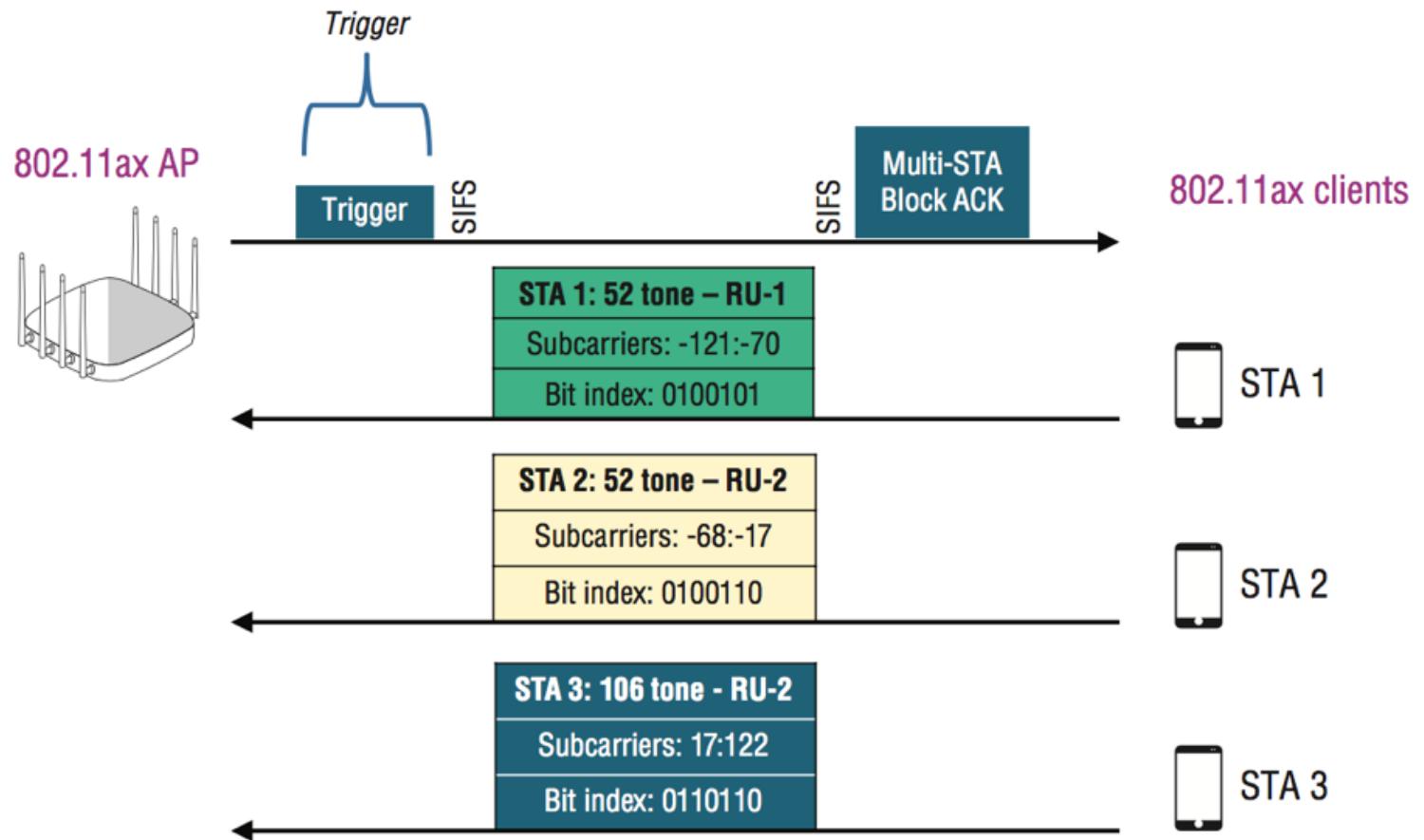


Allocation des sous porteuses avec OFDMA



Exemple d'échange OFDMA

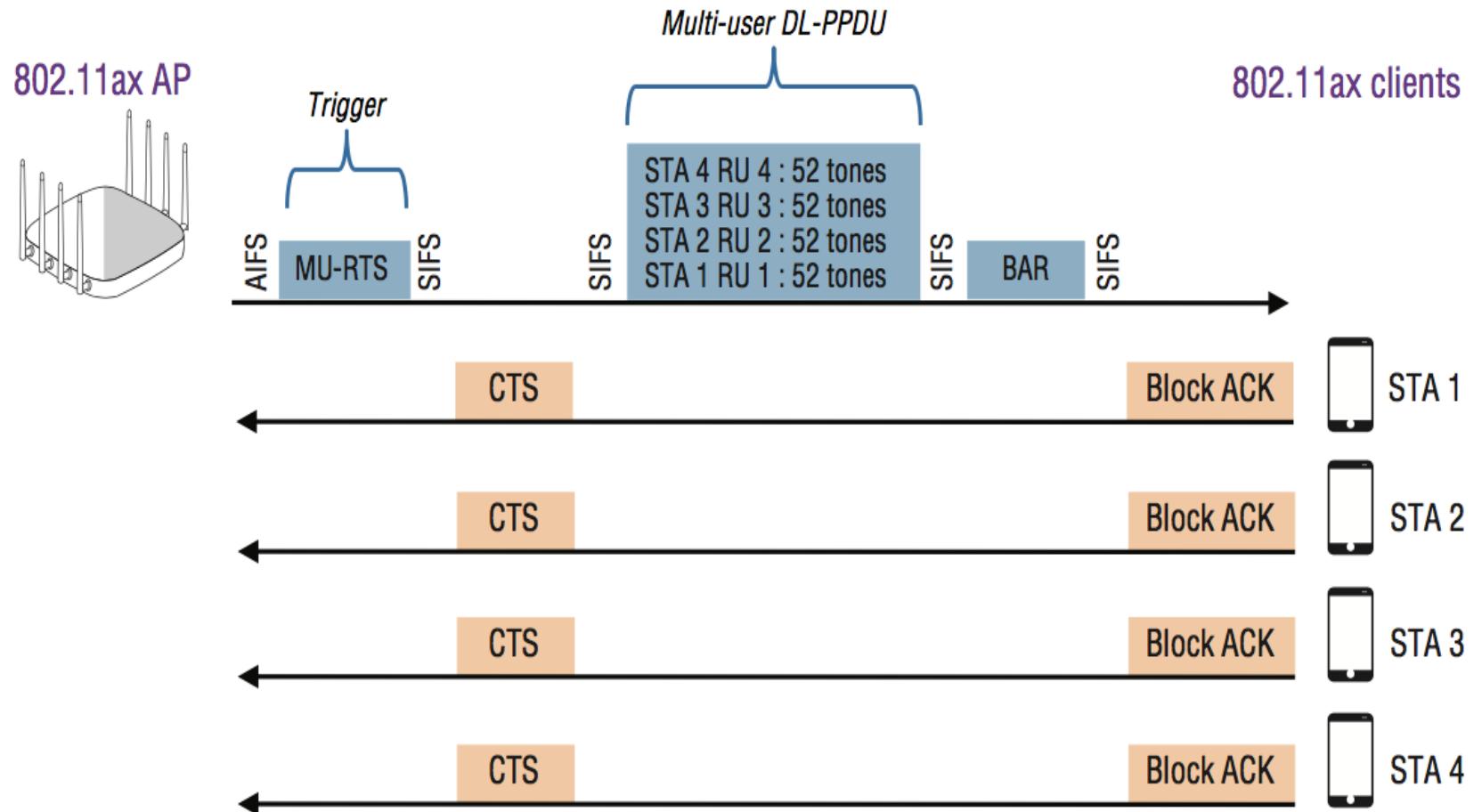
- Dans cet exemple les utilisateurs 1 et 2 ont été attribués des tones de 52 sous porteuses, et l'utilisateur 3 un tone de 106 sous porteuses
- L'AP annonce les allocations dans la trame Trigger
- Les trois utilisateurs envoient en même temps
- L'AP acquitte aux 3 en même temps



source : <https://blog.aerohive.com/802-11ax-allocate-ofdma-ru/>

Avec 802.11ax c'est l'AP qui contrôle tout

- L'AP transmet un MU-RTS sur l'ensemble du canal
 - Ceci permet aux utilisateurs non ax de mettre à jour leur NAV
- MU-RTS contient des informations indiquant aux stations où transmettre leur CTS
- MU-RTS contient aussi les RU à utiliser pour recevoir les données
- L'AP demande un Block ACK avec Block Ack Request (BAR)



Source : <https://blog.aerohive.com/dl-ofdma/>

UORA (UL OFDMA Random Access)

- Ce mode d'échange est l'équivalent de CSMA/CA
- Il est dédié aux stations n'ayant pas eu des RUs
- L'AP transmet une trame Trigger indiquant les RUs à utiliser de façon aléatoire
- Chaque station tire un backoff aléatoire
- Les stations décrémentent le backoff d'une valeur indiquée dans la trame de Trigger
- Quand le backoff d'une station atteint 0, elle transmet sa trame en utilisant une RU choisie aléatoirement parmi celles indiquées par l'AP
- Les autres stations temporisent leur backoff
- L'AP transmet une trame Trigger après la fin de la transmission de la station qui a gagné, les autres stations enchaînent la décrémentation du backoff

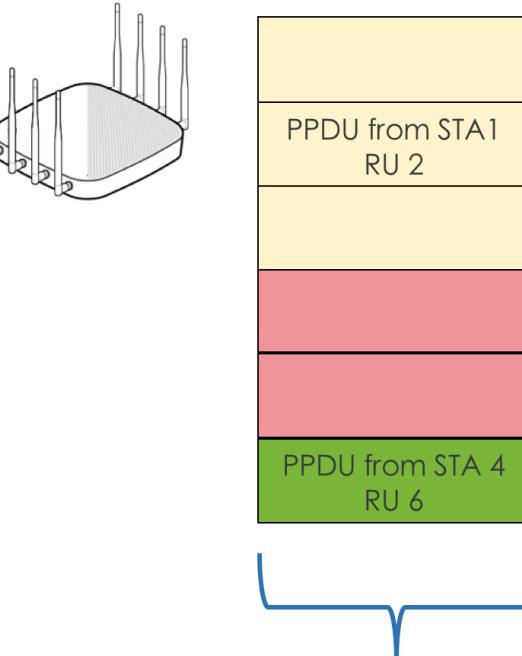
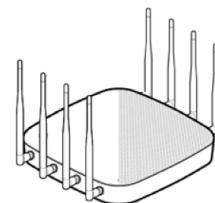
Exemple UORA (source <https://blog.aerohive.com/ul-ofdma-random-access-uora-part-2/>)

- L'AP annonce les RUs disponibles en accès aléatoire
- Les stations tirent des backoff dans un intervalle indiqué par l'AP
- La trame Trigger indique la valeur de décrémentation du backoff
 - 3 pour les stations associées (AID = 0)
 - 2 pour les stations non associées (AID = 2045)



Exemple UORA

- La station 1 ayant choisi 802.11ax AP le backoff le plus petit, choisit la RU 2 pour transmettre
- La station 4 ayant une RU réservée, transmet aussi
- Les 2 autres stations ont décrémenté leurs backoff de 3 et 2, et temporisent la décrémentation



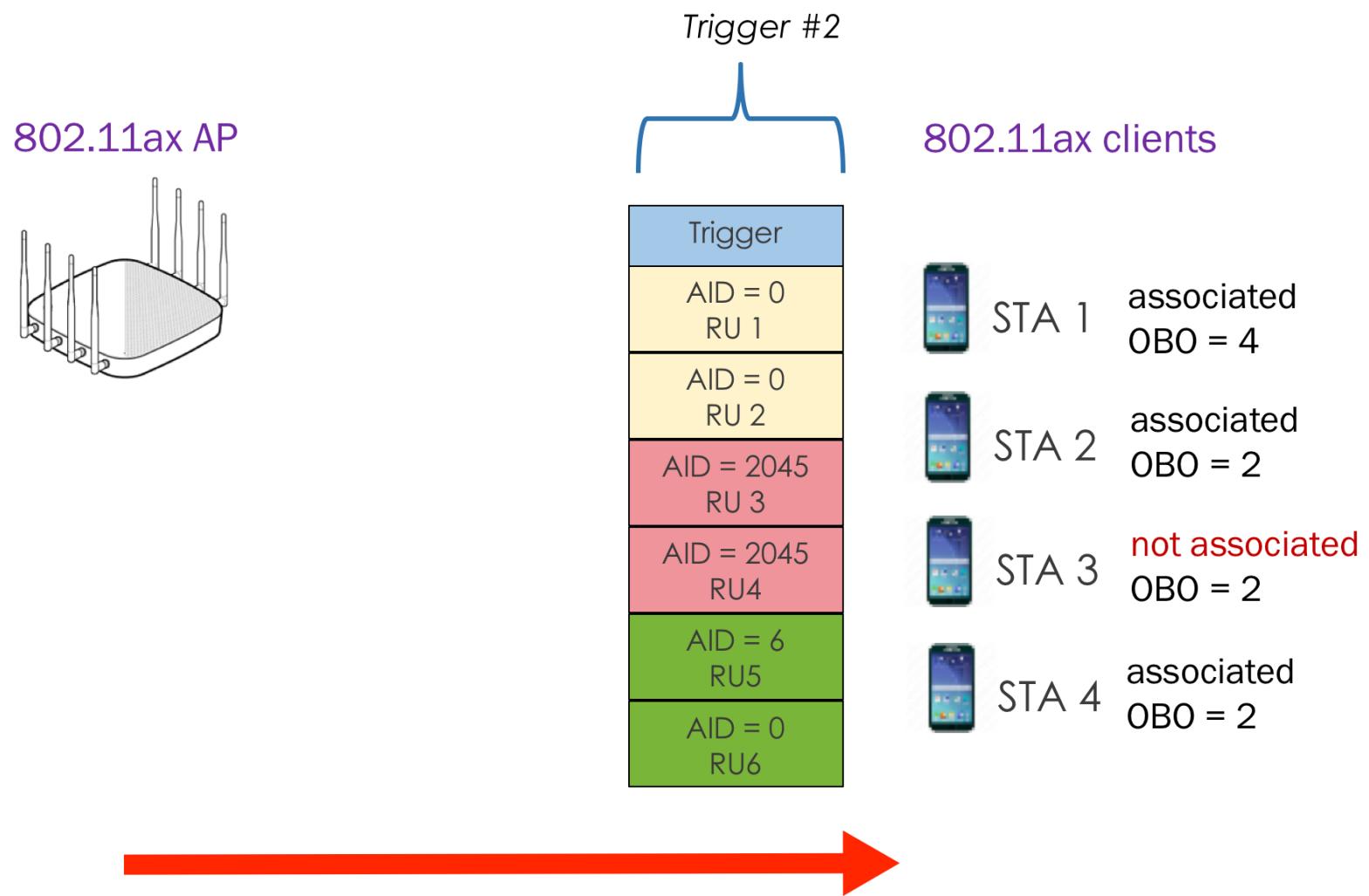
802.11ax clients

STA 1	associated OBO = 0	Decrement OBO counter by 3
STA 2	associated OBO = 2	Decrement OBO counter by 3
STA 3	not associated OBO = 2	Decrement OBO counter by 2
STA 4	associated OBO = 2	Assigned to dedicated RU

STA 1 randomly assigned RU because OBO counter = 0

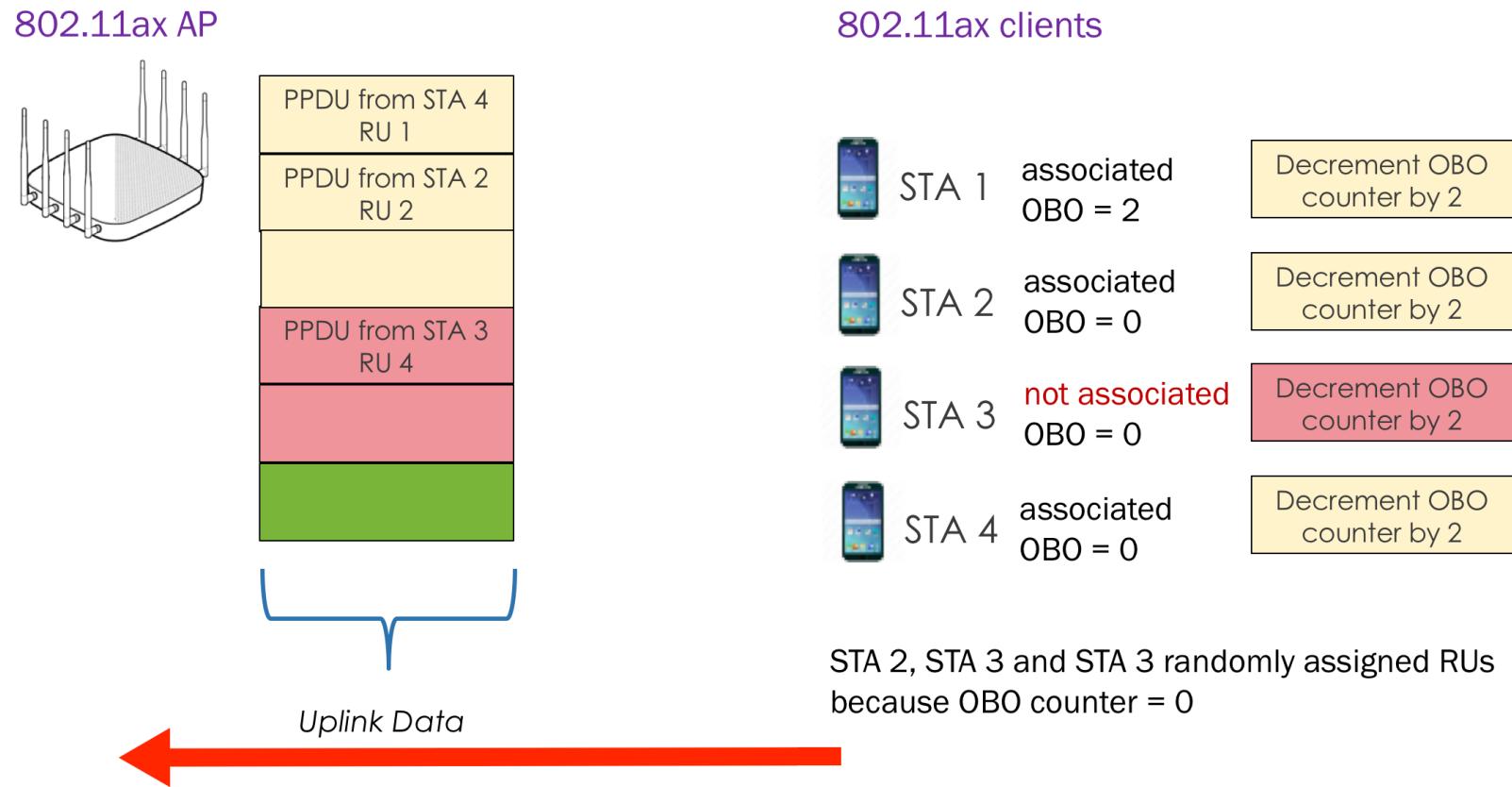
Exemple UORA

- L'AP transmet une trame Trigger
- Station 1 et station 4 ont de nouvelles trames à transmettre
- La valeur à utiliser pour décrémenter les backoff pour les stations associées est 2



Exemple UORA

- Les stations 2, 3 et 4 ont un backoff de 0
- Elles choisissent des RUs et transmettent leurs trames
- Station 1 doit attendre la prochaine trame Trigger pour savoir comment décrémenter son backoff
- Si une trame de Trigger ne contient pas de AID = 2045, les stations non associées ne décrémentent pas leur backoff



802.11e intégré à 802.11 à partir de 2007

- Différenciation de trafic
- EDCA : Enhanced Distributed Channel Access
- HCCA : Hybrid Coordination Function Controlled Channel Access
- TxOP : opportunité de transmission sans contention
- Acquittement par bloc de trames

EDCA

- Similaire au mode DCF avec 8 niveaux de priorité (définis dans IEEE 802.1D) convertis en 4 catégories d'accès (AC)

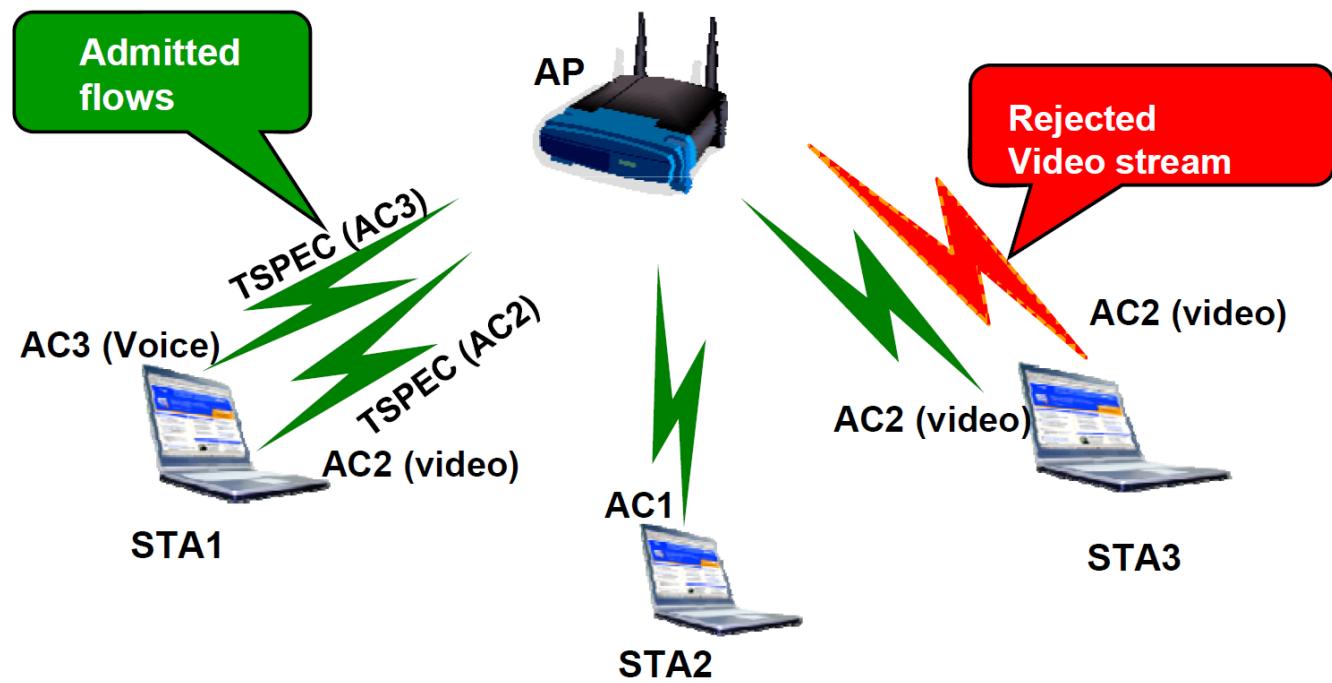
Priorité	Priorité 802.1D	Désignation 802.1D	Catégorie d'accès (AC)	Désignation
Plus petite	1	BK	AC_BK	Background
	2	-	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Vidéo
	5	VI	AC_VI	Vidéo
↓	6	VO	AC_VO	Voix
Plus haute	7	NC	AC_VO	Voix

Les trames de gestion entre stations supportant la QoS sont transmises selon l'AC_VO

TxOP : opportunité de transmission sans contention

- Similaire aux slots réservés en PCF si attribué par l'AP (HCCA)
- Permet à la station de transmettre plusieurs trames une fois elle a gagné la contention au médium en mode EDCA :
 - AC_BK et AC_BE ne permettent pas de transmettre plus d'une trame,
 - AC_VO et AC_VI ont des durées prédéfinies
- La négociation de ces slots de temps se fait durant la phase Admission Control (contrôle d'admission avec des échanges ADDTS pour Add Traffic Stream) qui a lieu durant la phase d'association
- La capacité des AP à accepter de nouveaux flux est indiquée dans les beacons, ceci permet aux stations de choisir l'AP selon ces capacités (entre autres critères)

Contrôle d'admission



- Négociation selon les capacités de l'AP durant la phase d'association
- La station envoie un ADDTS (Add Traffic Stream) request en précisant les caractéristiques du trafic (TSPEC)
- L'algorithme d'acceptation ne fait pas partie de la norme

Source : Philippe Klein IEEE Plenary Meeting – Nov 08 Dallas, TX

AIFSN : Arbitrary IFS Number

- Chaque catégorie d'accès a son propre AIFSN
- Ce numéro représente le nombre minimum de slots à attendre avant de commencer à décrémenter le backoff (remplace DIFS)
- Cette valeur est propre à chaque catégorie d'accès
- Chaque catégorie d'accès possède ses propres CWmin et CWmax
 - Contrairement au mode DCF où ces limites sont les mêmes par station