Quelques exemples de technologies sans fil

équipe Privatics - Inria Rhône-Alpes

vincent.roca@inria.fr

6 octobre 2021

Vue d'ensemble

- Plusieurs technologies sont considérées :

1. **technologies IEEE-802.11* (Wifi)**
2. réseaux LTE/LTE Advanced et 4G
3. réseaux satellites

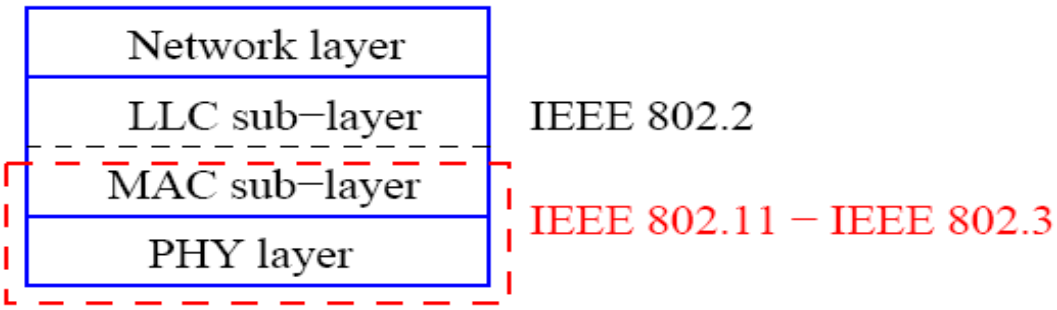
Partie 1:

Les réseaux sans fils IEEE-802.11/WiFi

Nombreux transparents inspirés/empruntés à Imad Aad. Merci…

Introduction au IEEE 802.11/Wifi

- IEEE 802.11 et Wifi
  - ***IEEE 802.11*** **(*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*)**
  - **WiFi (*Wireless Fidelity*) est le nom donnée à la certification délivrée par la « Wifi Alliance », l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et marketing), le nom de la norme et de la certification sont confondus…**
- norme qui couvre les couches PHY / MAC



Introduction au IEEE 802.11/Wifi… (suite)

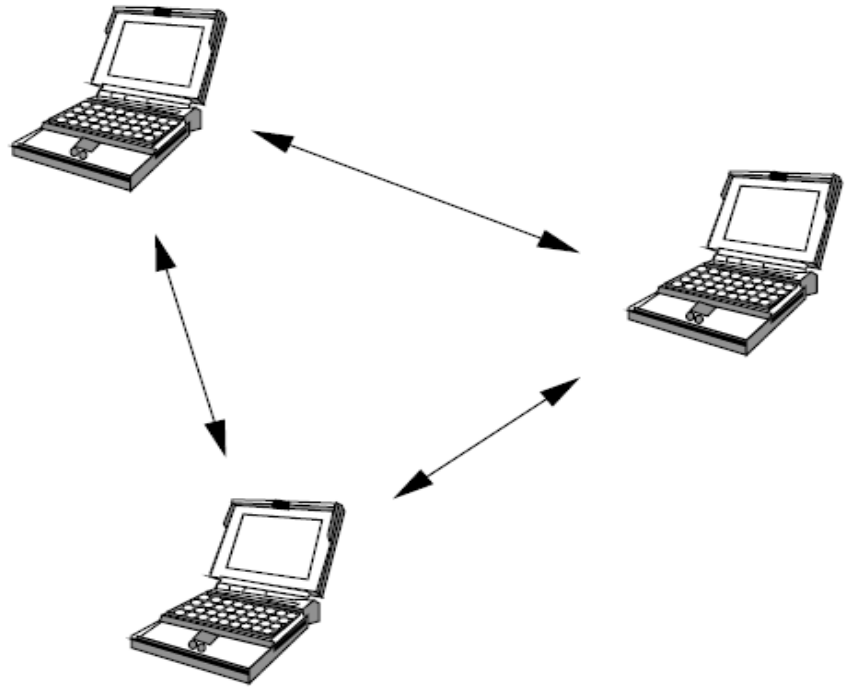
- une technologie qui évolue sans cesse :
  - 1997 802.11 2 Mbps, autour de 2.4 GHz
  - 1999 802.11**b** 11 Mbps, autour de 2.4 GHz
  - 1999 802.11**a** 54 Mbps, autour **5 GHz**
  - 2003 802.11**g** 54 Mbps, autour de 2.4 GHz
  - 2009 802.11**n** jusqu'à 600 Mbps, autour 2.4 ou 5 GHz
  - 2013 802.11**ac** jusqu'à 866 Mbps (par stream), **5 GHz**
  - 2019 802.11**ax** ou **Wi-Fi 6**, 2.4 et 5 GHz (1-7 GHz possible)
  - 2012 802.11**ad** jusqu'à 6,75 **G**bps, autour de **60 GHz**
- et des extensions :
  - 802.11e extension pour la QoS
  - 802.11i extension pour la sécurité

Connexion au réseau

- Connexion passive
  - la station écoute sur tous les canaux les trames balises (***beacon frame***) émises par la « Station de Base » (BS)
  - on obtient la liste des réseaux, leurs caractéristiques et leur rapport S/N
- Authentification
  - la station s'authentifie auprès de la BS choisie
    - **peut être implicite, toute station étant acceptée**
    - **peut être explicite (Shared Key Auth. System) ⇒ nécessite une clef secrète partagée**
- Association
  - la station envoie une trame ***"association request"***
  - la BS vérifie le SSID spécifié et accepte si OK avec une trame ***"association response"***

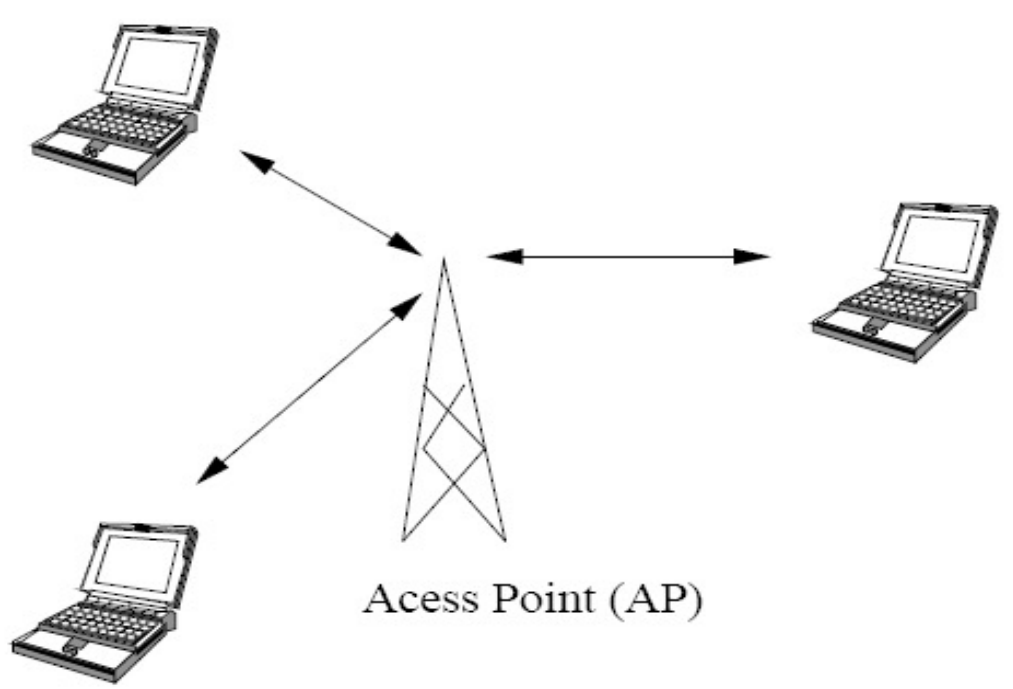
Les 3 modes de fonctionnement de 802.11

- le mode ad-hoc (ou IBSS, Independant Basic Service Set)
  - pas d'infrastructure fixe
  - interconnexion directe entre les équipements



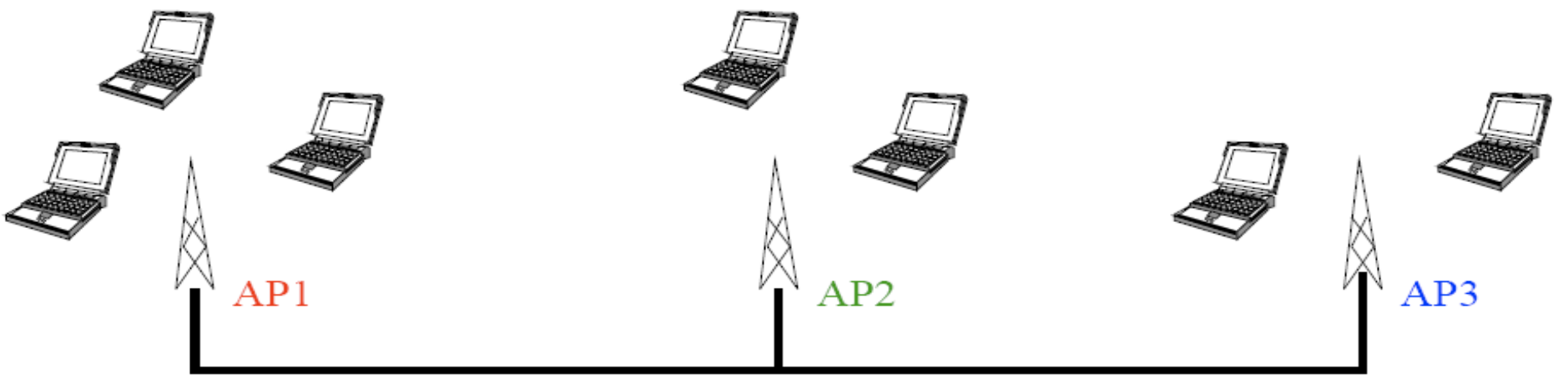
Les 3 modes de fonctionnement… (suite)

- le mode infrastructure basic (BSS, Basic Service Set)
  - présence d'un point d'accès qui peut aussi permettre l'interconnexion à l'Internet
  - pas de communication directe entre les équipements



Les 3 modes de fonctionnement… (suite)

- le mode infrastructure étendu (ESS, Extended Service Set)
  - présence de plusieurs points d'accès qui peuvent aussi permettre l'interconnexion à l'Internet
  - hand-off au niveau MAC entre différents points d'accès
    - **la mobilité est transparente aux couches supérieures !**



La couche MAC

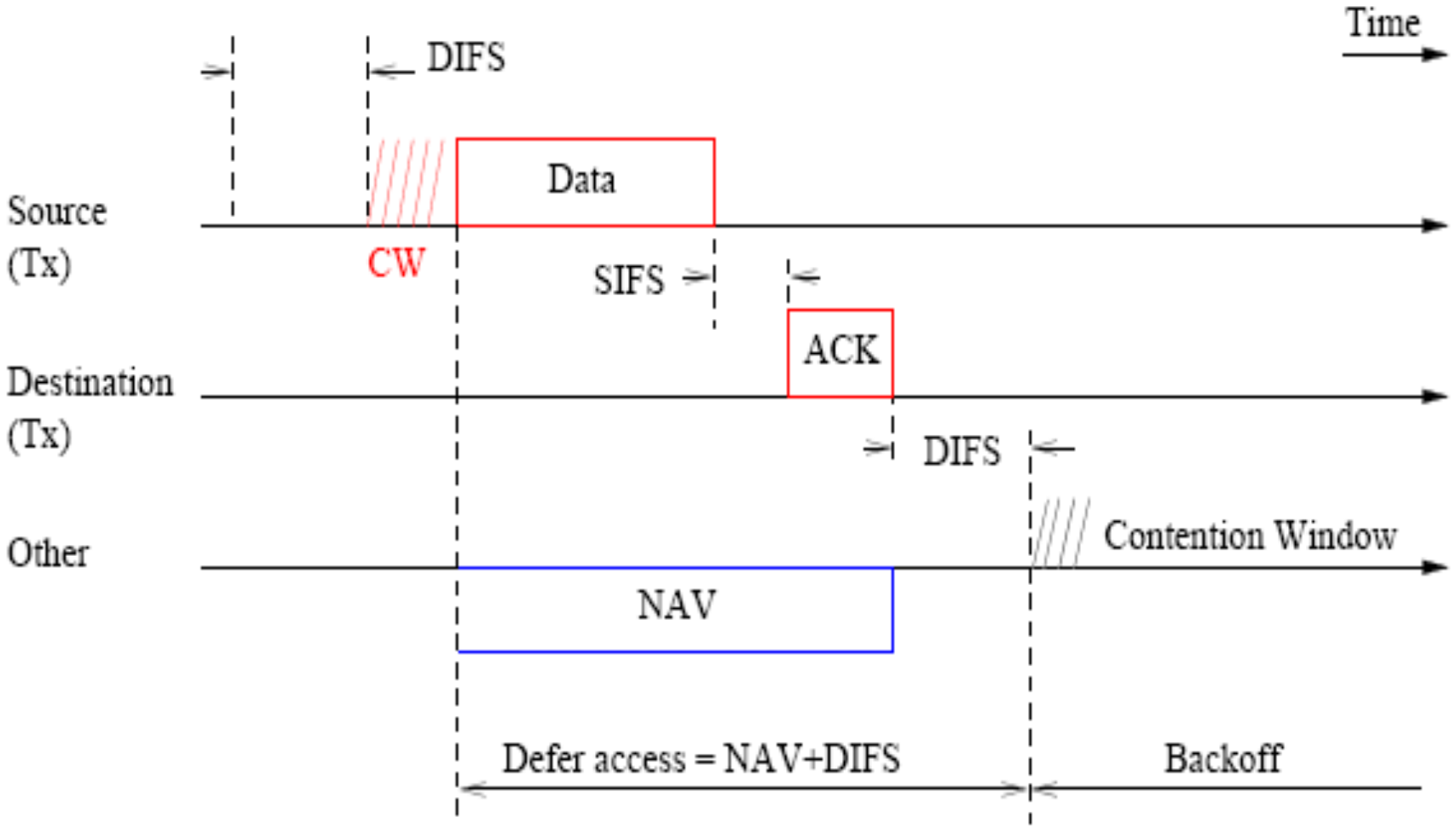
- Deux modes principaux
  - DCF (Distributed Coordinated Function)
    - en mode Ad-Hoc ou Infrastructure
    - version de base pour les *petits* paquets
    - version permettant le CSMA/CA (Collision Avoidance) pour les autres paquets
  - PCF (Polling Coordination Function)
    - seulement en mode Infrastructure (puisqu'il faut un arbitre)
    - permet de garantir à chaque station un accès minimum au médium (absence de famine)

La couche MAC… (suite)

- Mode DCF, version « petits paquets »
  - introduit des temps d'attente minimums (DIFS/SIFS)
  - des temps d'attente aléatoires (backoff) bornés par une valeur (CW) qui dépend de l'historique
    - **backoff = random(0, CW) * T_{slot}**
    - **initialement : CW = CW_{min} = 31**
    - **en cas de collision : CW = min(2 * CW; 1023)**
    - **dès qu'une transmission réussit : CW = CW_{min}**

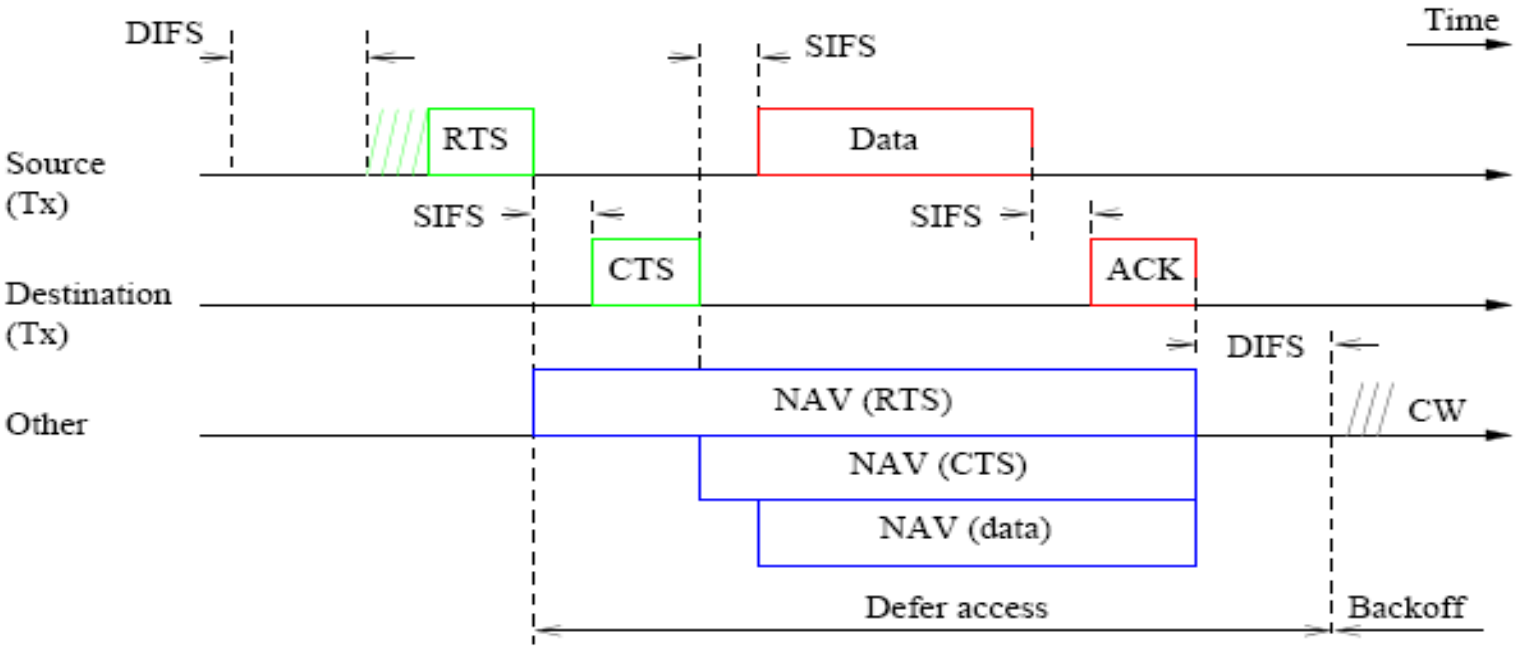
La couche MAC… (suite)

- Mode DCF, version « petits paquets »… (suite)



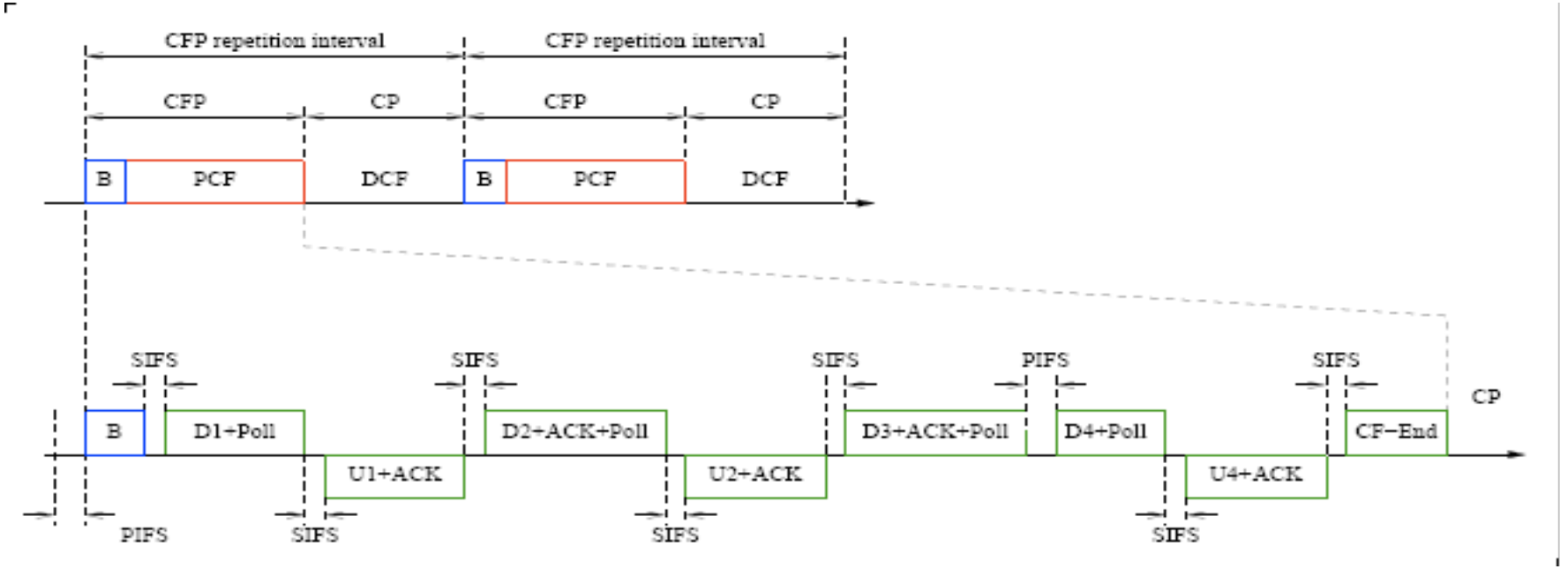
La couche MAC… (suite)

- Mode DCF, avec Collision Avoidance
  - les RTS (Request To Send)/CTS (Clear To Send) suivent la même approche
  - les paquets (de taille conséquente) ne peuvent être transmis qu'après réception du CTS



La couche MAC… (suite)

- Mode PCF pour garantir un accès minimum au médium (sans famine)
  - deux phases :
    - **polling, où le point d'accès interroge chaque station**
    - **DCF, où le système évolue librement sans intervention du point d'accès**

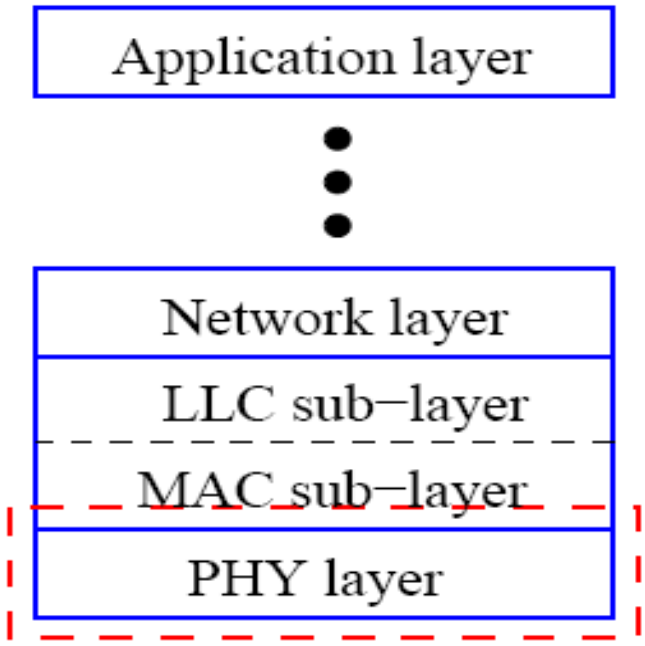


Les couches physiques du Wifi

- la couche physique de 802.11 de 1997
- la couche physique de 802.11a/g, de 1999 et 2003
- la couche physique de 802.11n de 2009
- la couche physique de 802.11ac de 2013
- la couche physique de 802.11ad
- la couche physique de 802.11ax

La couche physique de IEEE 802.11 (1997)

- 3 possibilités prévues par 802.11 - norme 1997
  - DSSS / FHSS / Infrarouge
  - mais seul DSSS (étalement de spectre) en pratique

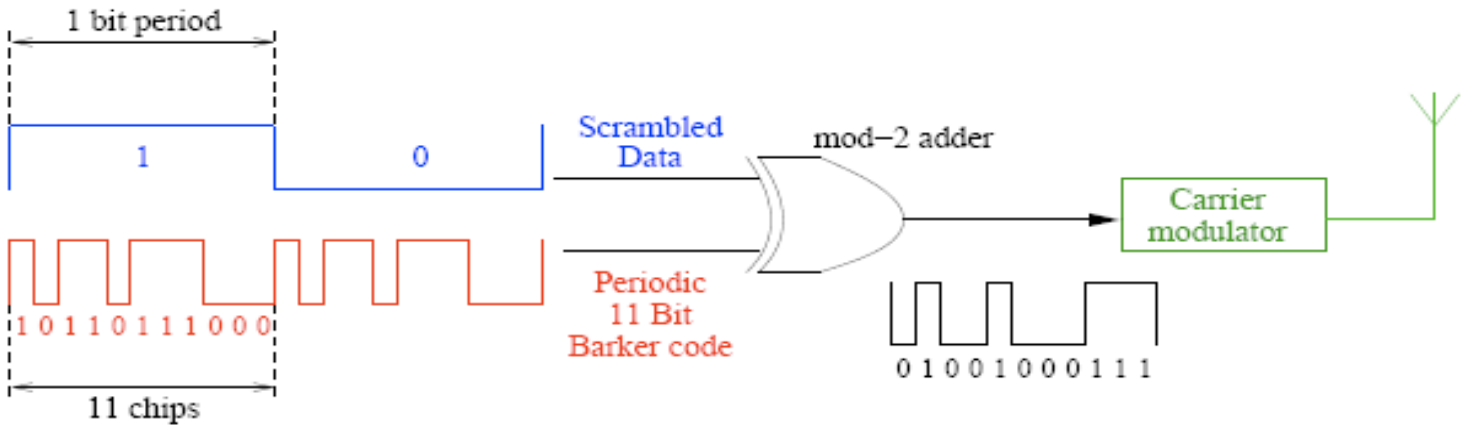


3 PHY types:

- DSSS (most products)
- FHSS (less products)
- IR (unknown products)

La couche physique de IEEE 802.11… (suite)

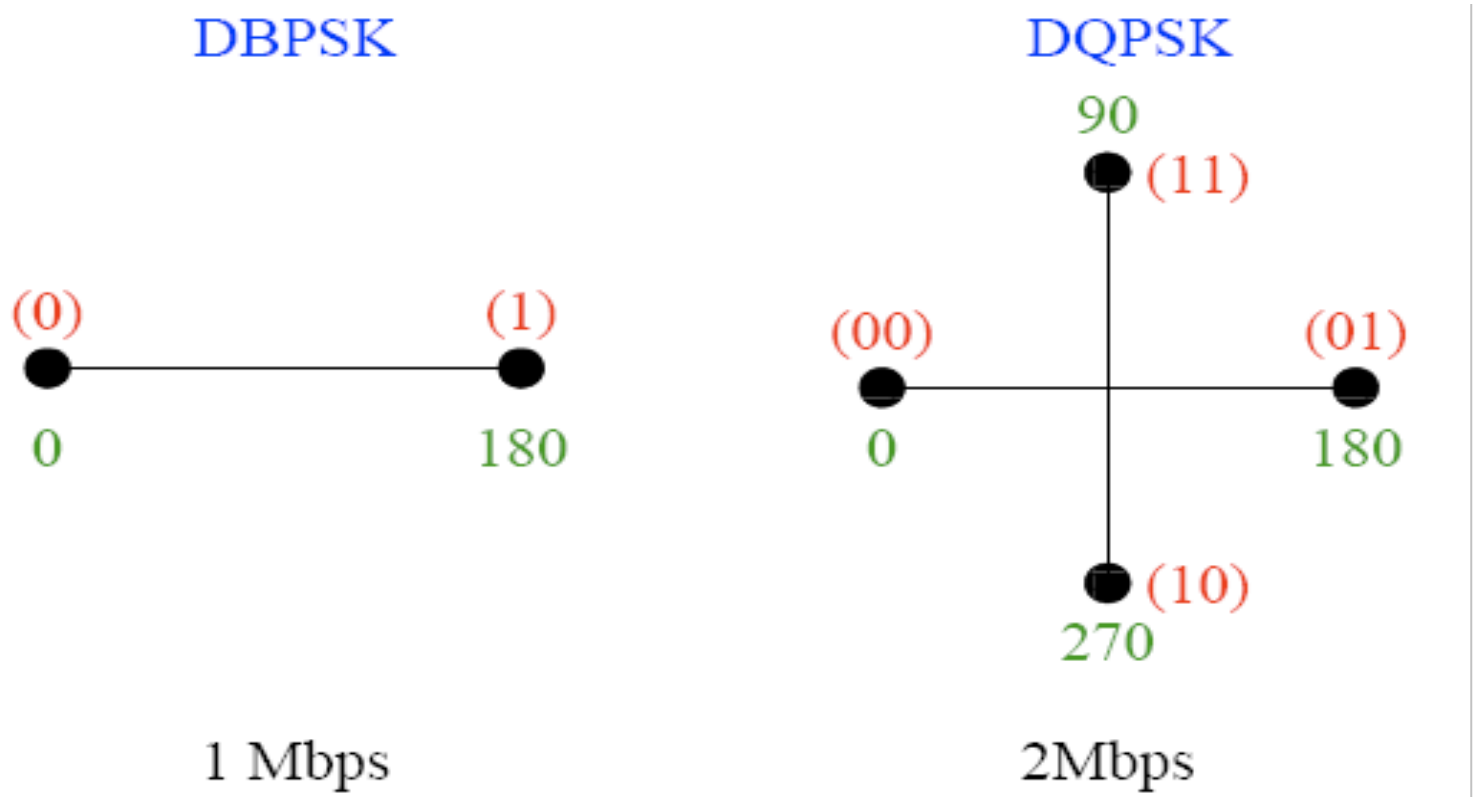
- Principe équivalent au DSSS présenté dans le cours sur la couche MAC…



- … avec une différence de taille !
  - un seul code de 11 bits **partagé** par tous les équipements
    - **n'apporte aucune sécurité**
    - **n'apporte aucun multiplexage d'accès**
    - **permet seulement la *suppression des interférences***

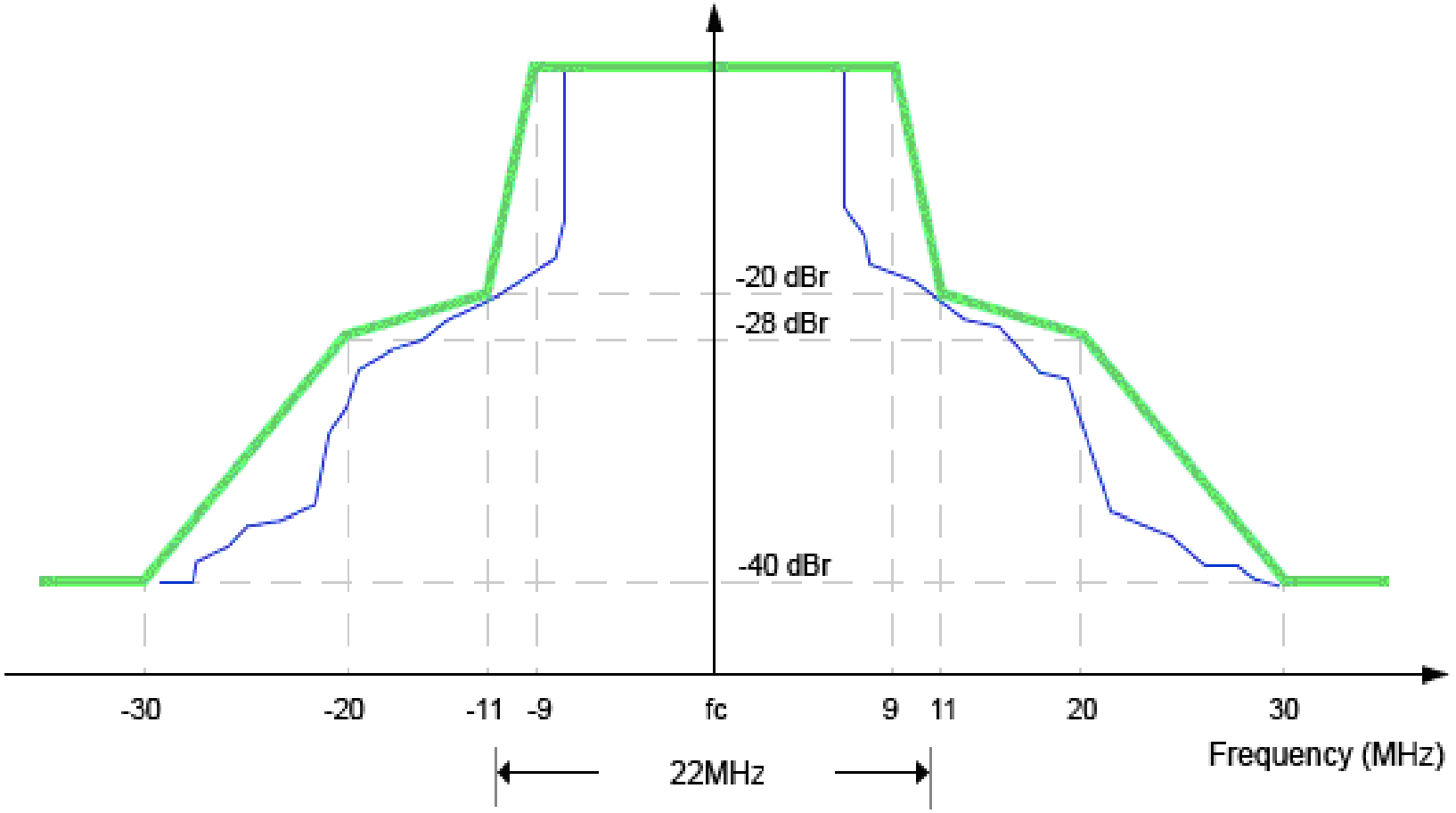
La couche physique de IEEE 802.11… (suite)

- Deux types de modulations, suivant le débit et la robustesse souhaités



La couche physique de IEEE 802.11… (suite)

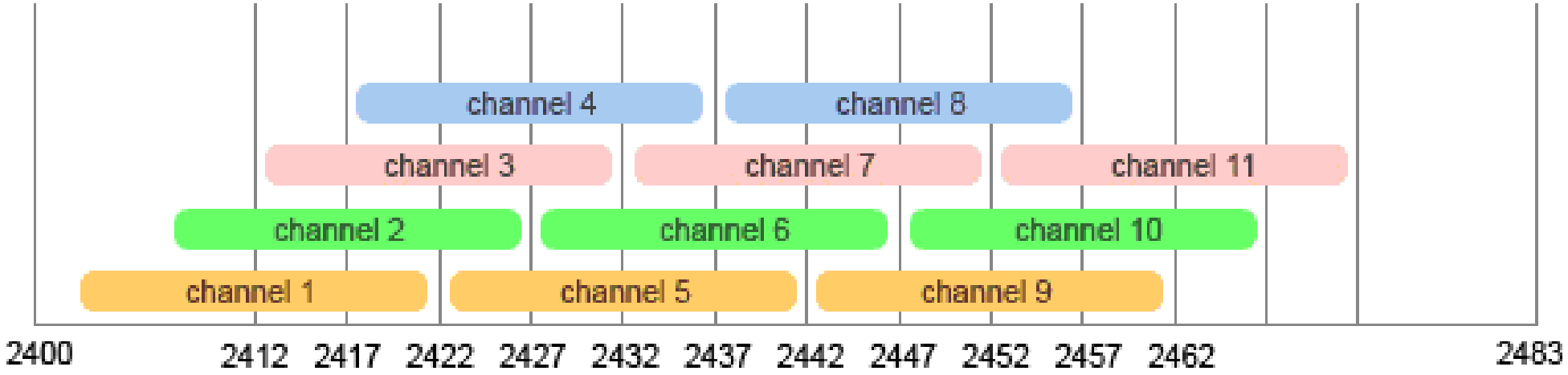
- le spectre de puissance
  - le maximum de puissance est sur le canal de taille B_w = 22 MHz
  - … mais le signal déborde !



Source : « 802.11n primer », AirMagnet, août 2008

La couche physique de IEEE 802.11… (suite)

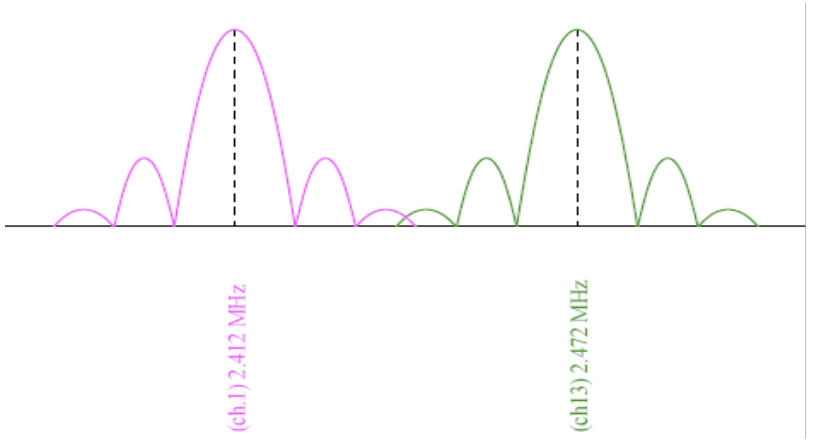
- les canaux possibles
  - 83,5 MHz de largeur de bande (2,4 à 2,4835 GHz)
  - 14 canaux de largeur (bande passante) B_w = 22 MHz
  - conduit à des recouvrements inévitables
- seuls 3 canaux sans chevauchement en 2.4 GHz



Source : « 802.11n primer », AirMagnet, août 2008

La couche physique de IEEE 802.11… (suite)

- les canaux possibles : stratégie
  - en pratique, sur un site disposant déjà de réseaux Wifi…
    - **… essayer d'éloigner les canaux le plus possible pour permettre un S/N élevé**
      - sinon interférences et débit réduit



    - **si impossible, choisir le même canal permet au mécanisme de d'évitement de collisions de fonctionner**
      - il y a bien sûr partage de la bande passante…

La couche physique de IEEE 802.11… (suite)

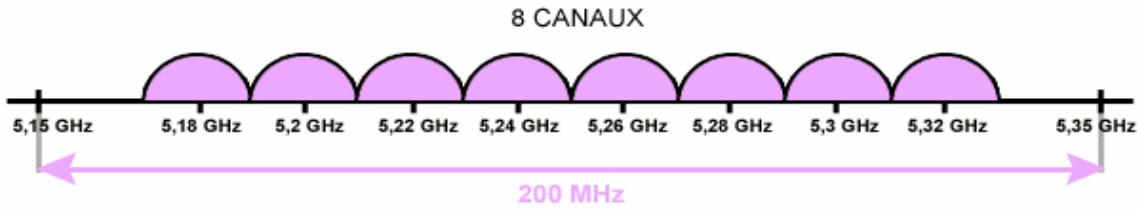
- puissance de transmission pour la bande 2.4GHz en France
  - **exprimée en PIRE (puissance isotrope rayonnée équivalente)**

	802.11
typique	2.5 mW
maximum	100 mW en intérieur et extérieur, sauf sur les canaux 10-13 qui sont limités à 10mW en extérieur

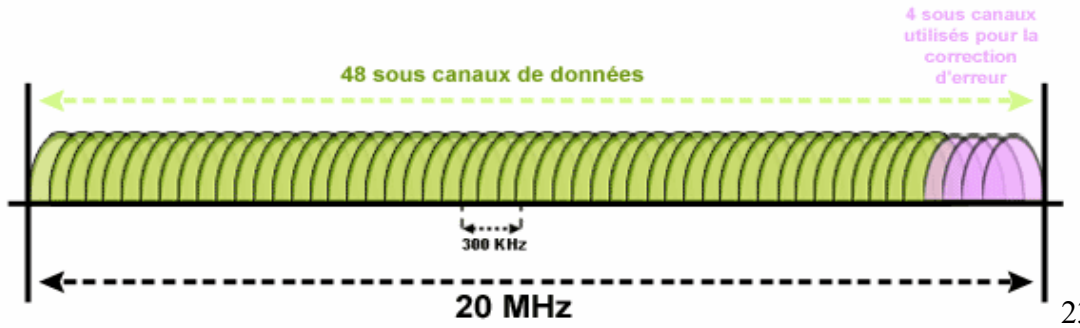
  - **pour comparaison : GSM 100 – 600 mW**

La couche physique du IEEE 802.11a/g

- 54 Mbps et deux fréquences (ISM)
  - 802.11a ⇒ 5 GHz, mais 802.11g ⇒ 2.4 GHz
- reposent sur OFDM
  - un canal de 20 MHz est découpé en 52 sous-canaux
    - **48 pour les données, 4 pour des codes correcteurs**
  - modulation indépendante et bas débit sur chaque sous canal
    - BPSK, QPSK, 16-QAM et 64-QAM

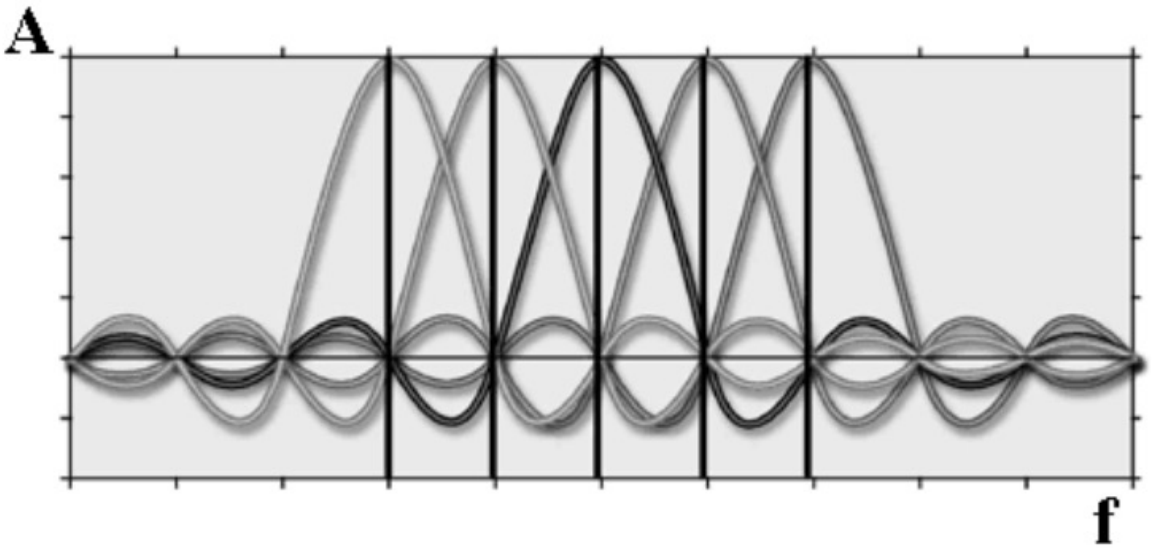


Exemple : 802.11a (bande des 5GHz)



La couche PHY du IEEE 802.11a/g… (cont')

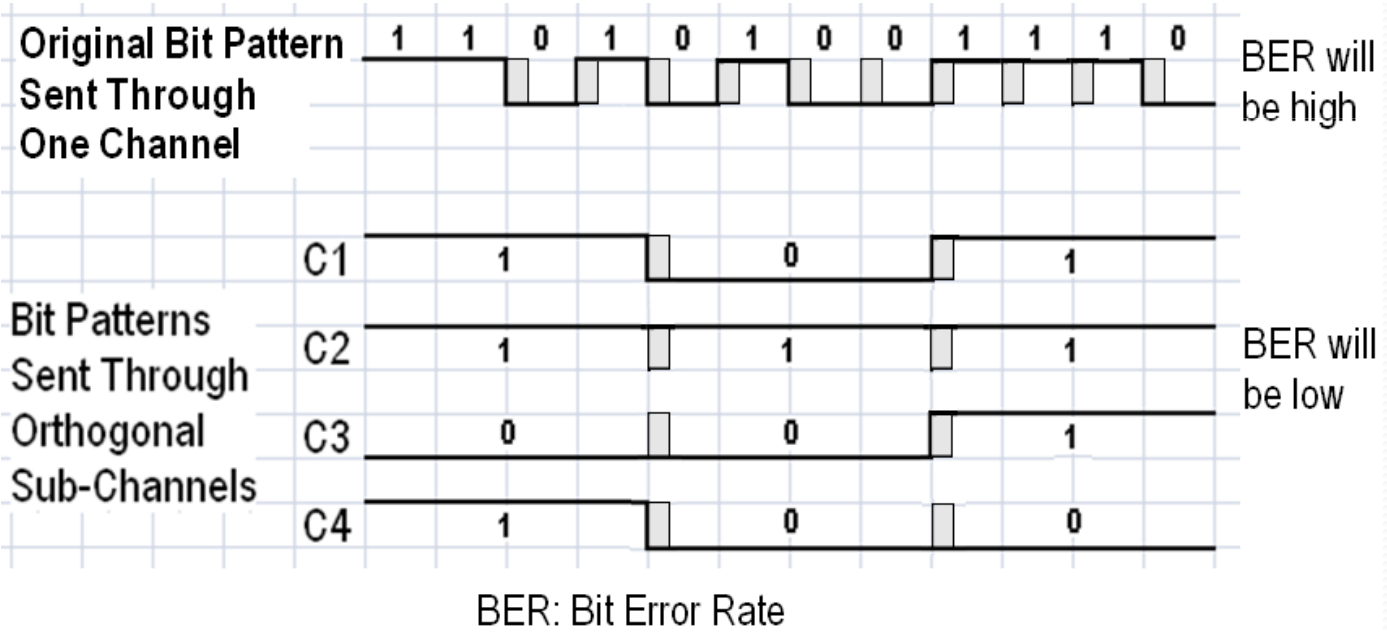
- OFDM fonctionne car…
  - **les fréquences des sous-canaux sont orthogonales (bien qu'il y ait recouvrement entre sous-canaux)**
    - au pic de chaque canal, les autres canaux ont une amplitude zéro
    - minimise les interférences inter-canaux
    - … à condition que émetteur et récepteurs soient précisément accordés sur la fréquence



Source : « 802.11 a/g OFDM PHY »
Juha Villanen

La couche PHY du IEEE 802.11a/g… (cont')

- OFDM fonctionne car…
  - **les signaux élémentaires sont transmis plus longtemps sur chaque sous-canal, ce qui limite les erreurs dues aux recouvrements de signal lors de transmission multi-chemins**



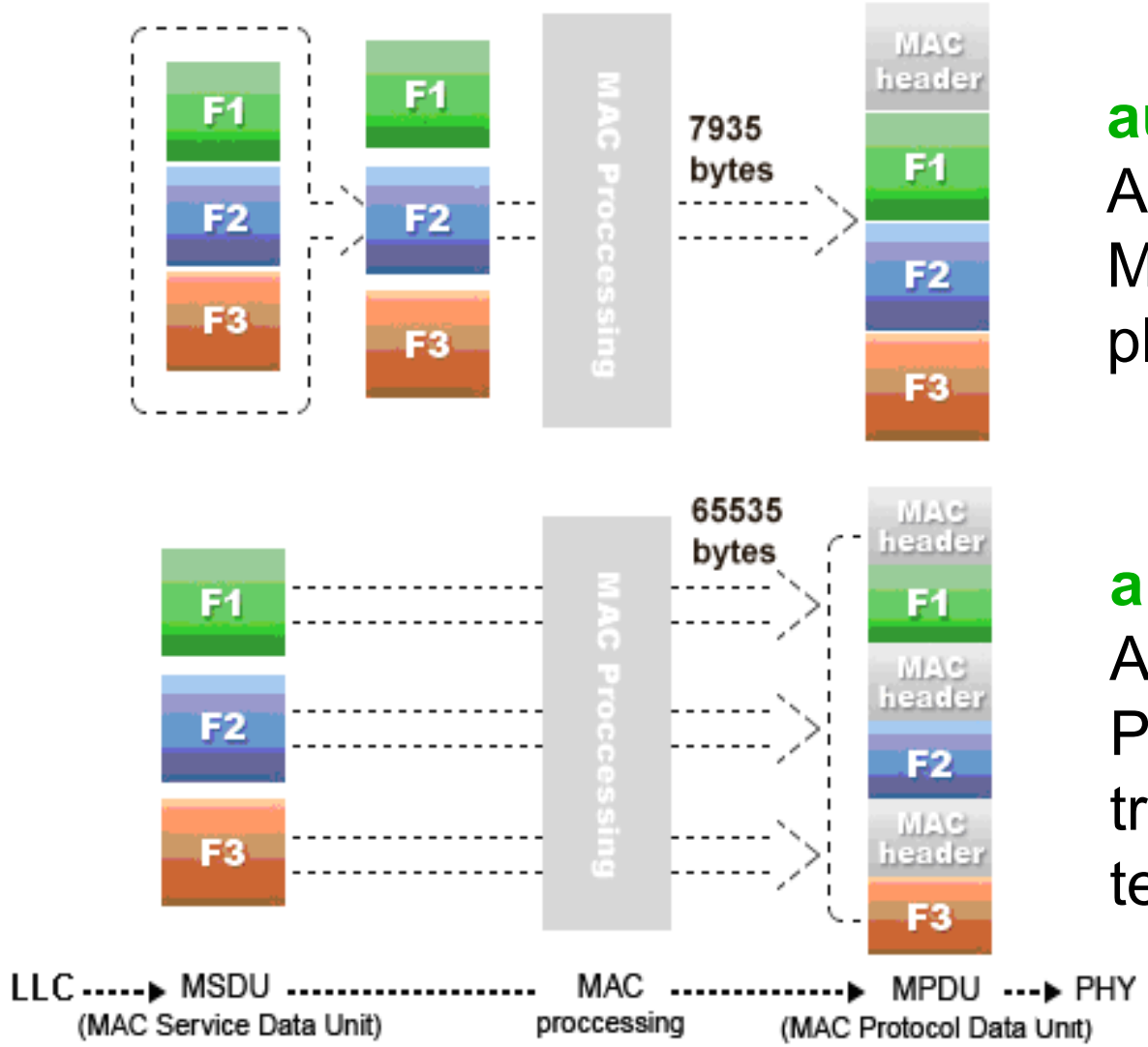
Source : « Spread spectrum and Wi-Fi basics », Syed M. Mahmud

La couche physique du IEEE 802.11n

- 802.11n est la norme de 2009
  - beaucoup en commun avec 802.11a/g, sur 2.4GHz ou 5GHz, mais débits jusqu'à 600 Mbps (4 flux)
  - plusieurs améliorations :
    - **doublement de la bande passante d'un canal : 20 ou 40 MHz**
      - le 40 MHz est réservé à la bande des 5 GHz, moins encombrée
    - **MIMO (mult. input/mult. output), via des antennes multiples**
      - permet 4 flux simultanés si 4 antennes, donc 4 fois le débit unitaire
      - un AP a 2 à 4 antennes, une station au moins 1

La couche physique du IEEE 802.11n… (cont')

❍agrégation des trames



au niveau MAC

A-MSDU : une seule trame MAC (et PHY) regroupant plusieurs paquets IP

au niveau PHY

A-MPDU : une seule trame PHY regroupant plusieurs trames MAC, chacune contenant un paquet IP

Source : « 802.11n primer », AirMagnet, août 2008

La couche physique du IEEE 802.11n… (cont')

- jusqu'à 600 Mbps avec 4 flux

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1 / 2	1	6.50	7.20	13.50	15.00
1	QPSK	1 / 2	1	13.00	14.40	27.00	30.00
2	QPSK	3 / 4	1	19.50	21.70	40.50	45.00
3	16-QAM	1 / 2	1	26.00	28.90	54.00	60.00
4	16-QAM	3 / 4	1	39.00	43.30	81.00	90.00
5	64-QAM	2 / 3	1	52.00	57.80	108.00	120.00
6	64-QAM	3 / 4	1	58.50	65.00	121.50	135.00
7	64-QAM	5 / 6	1	65.00	72.20	135.00	150.00
8	BPSK	1 / 2	2	13.00	14.40	27.00	30.00
9	QPSK	1 / 2	2	26.00	28.90	54.00	60.00
10	QPSK	3 / 4	2	39.00	43.30	81.00	90.00
11	16-QAM	1 / 2	2	52.00	57.80	108.00	120.00
12	16-QAM	3 / 4	2	78.00	86.70	162.00	180.00
13	64-QAM	2 / 3	2	104.00	115.60	216.00	240.00
14	64-QAM	3 / 4	2	117.00	130.00	243.00	270.00
15	64-QAM	5 / 6	2	130.00	144.40	270.00	300.00
16	BPSK	1 / 2	3	19.50	21.70	40.50	45.00
…	…	…	…	…	…	…	…
31	64-QAM	5 / 6	4	260.00	288.90	540.00	600.00

Source : « 802.11n primer », AirMagnet, août 2008

La couche physique du IEEE 802.11ac

- 802.11ac est la norme multi-Gbps de 2013
  - dépasse le Gbps
  - uniquement sur 5 GHz
    - **bande passante plus large et moins encombrée qu'en 2.4 GHz**
  - les canaux sont plus larges: 20, 40, 80 ou 160 MHz
    - 25 canaux 20MHz, ou 5 de 80MHz, ou 2 de 160MHz simultanément **sans recouvrement**

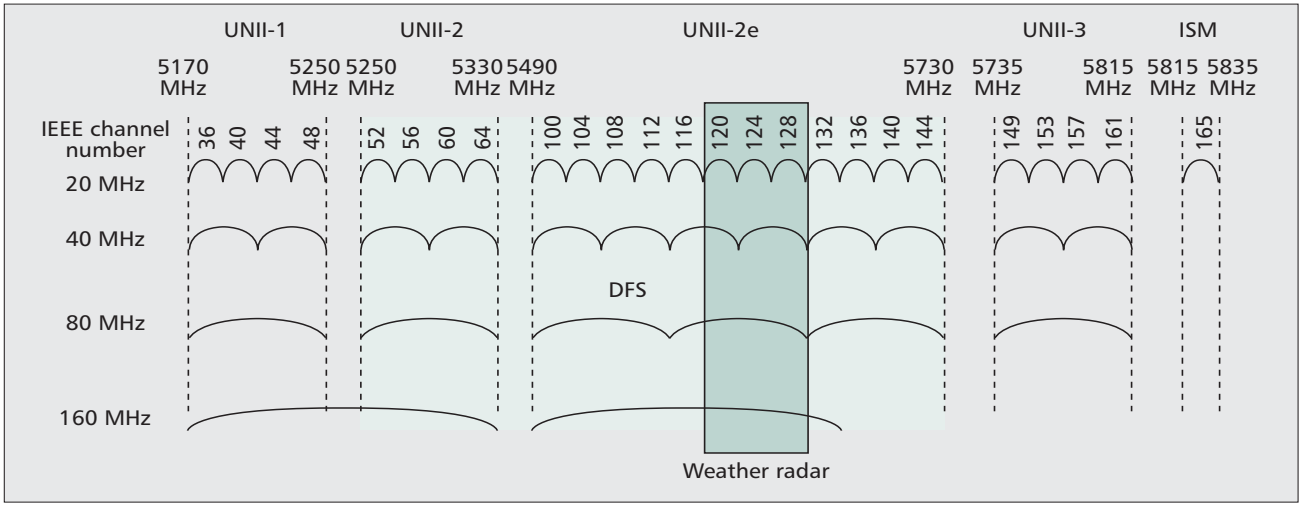


Figure 1. *The 5 GHz spectrum available for Wi-Fi usage with DFS and TDWR restrictions.*

Source : « WiFi on Steroids: 802.1ac and 802.11ad »
IEEE Wireless Communications, Déc.. 2013

La couche PHY du IEEE 802.11ac… (cont')

- modulation sur chaque canal jusqu'à 256-QAM en conditions optimales

La couche PHY du IEEE 802.11ac… (cont')

- MIMO amélioré, jusqu'à 8 flux
  - **pour différents destinataires (MU-MIMO) ou un seul (SU-MIMO)**
    - les équipements légers ne disposent que d'une antenne (un flux)
    - les équipements sur secteur peuvent disposer de plusieurs antennes et recevoir à plus haut débit

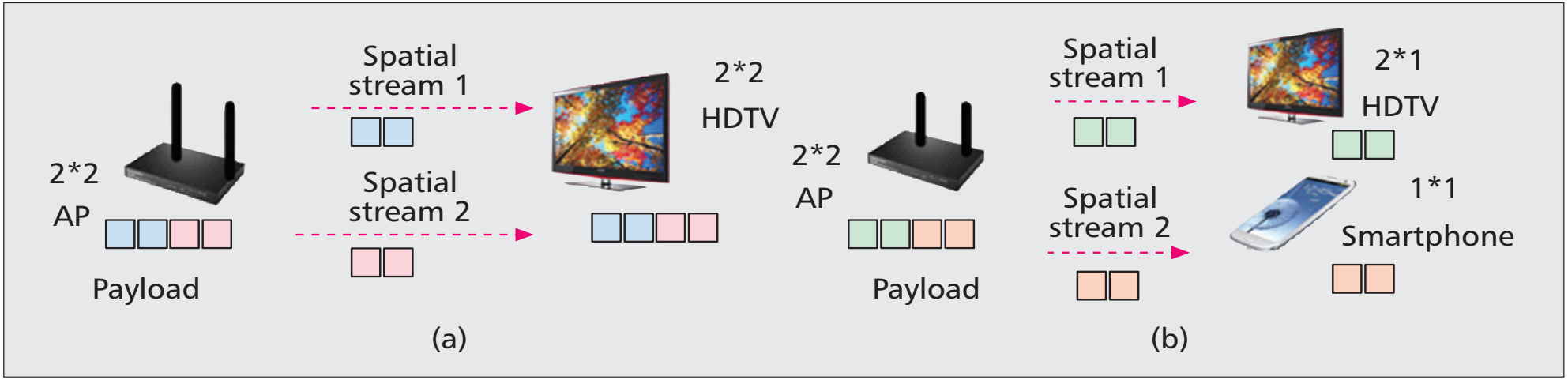


Figure 2. *a) SU-MIMO concept; b) downlink MU-MIMO concept.*

Source : « WiFi on Steroids: 802.1ac and 802.11ad »
IEEE Wireless Communications, Déc.. 2013

La couche PHY du IEEE 802.11ac… (cont')

- jusqu'à 866 Mbps par flux, soit 6.77 Gbps agrégé

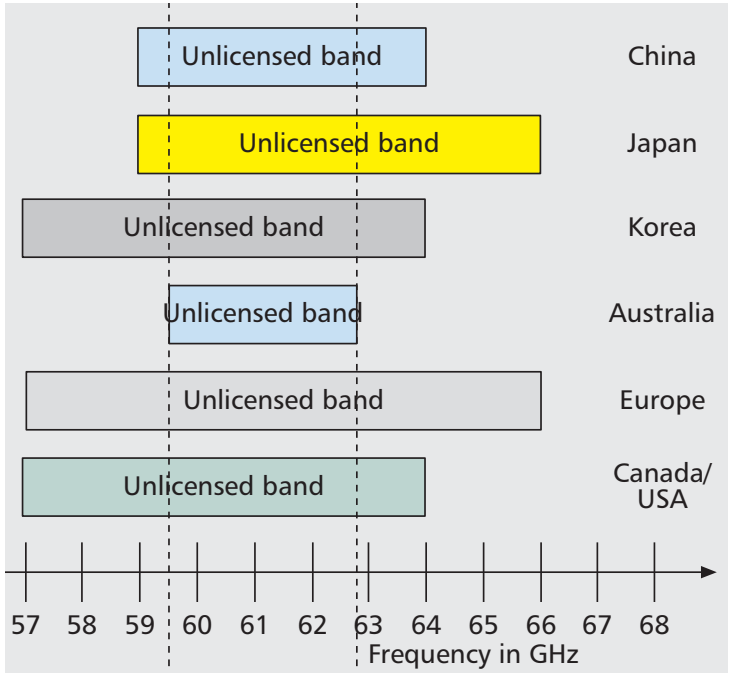
Scenario	Typical Client Form Factor	PHY Link Rate	Aggregate Capacity
1-antenna AP, 1-antenna STA, 80 MHz	Handheld	433 Mbit/s	433 Mbit/s
2-antenna AP, 2-antenna STA, 80 MHz	Tablet, Laptop	867 Mbit/s	867 Mbit/s
1-antenna AP, 1-antenna STA, 160 MHz	Handheld	867 Mbit/s	867 Mbit/s
2-antenna AP, 2-antenna STA, 160 MHz	Tablet, Laptop	1.69 Gbit/s	1.69 Gbit/s
4-antenna AP, four 1-antenna STAs, 160 MHz (MU-MIMO)	Handheld	867 Mbit/s to each STA	3.39 Gbit/s
8-antenna AP, 160 MHz (MU-MIMO) -- one 4-antenna STA -- one 2-antenna STA -- two 1-antenna STAs	Digital TV, Set-top Box, Tablet, Laptop, PC, Handheld	3.39 Gbit/s to 4-antenna STA 1.69 Gbit/s to 2-antenna STA 867 Mbit/s to each 1-antenna STA	6.77 Gbit/s
8-antenna AP, four 2-antenna STAs, 160 MHz (MU-MIMO)	Digital TV, Tablet, Laptop, PC	1.69 Gbit/s to each STA	6.77 Gbit/s

http://en.wikipedia.org/wiki/802.11ac

La couche PHY du IEEE 802.11ad

- 802.11ad est un norme multi Gbps
  - jusqu'à 6.75 Gbps
  - dans la bande des 60GHz

    (ondes millimétriques)
    - **libre au niveau mondial ☺**
    - **ne passe pas les murs ☹**
    - **a une portée réduite (~10 m) ☹**
    - **mais peu d'interférences avec d'autres réseaux ☺**
    - **les transmissions sont directionnelles, avec une antenne à haut gain pour combattre une rapide atténuation**
      - du fait de l'usage de fréquences élevées
      - λ = 5mm, ce qui facilite la conception d'antennes à haut gain



Wireless Gigabit Alliance

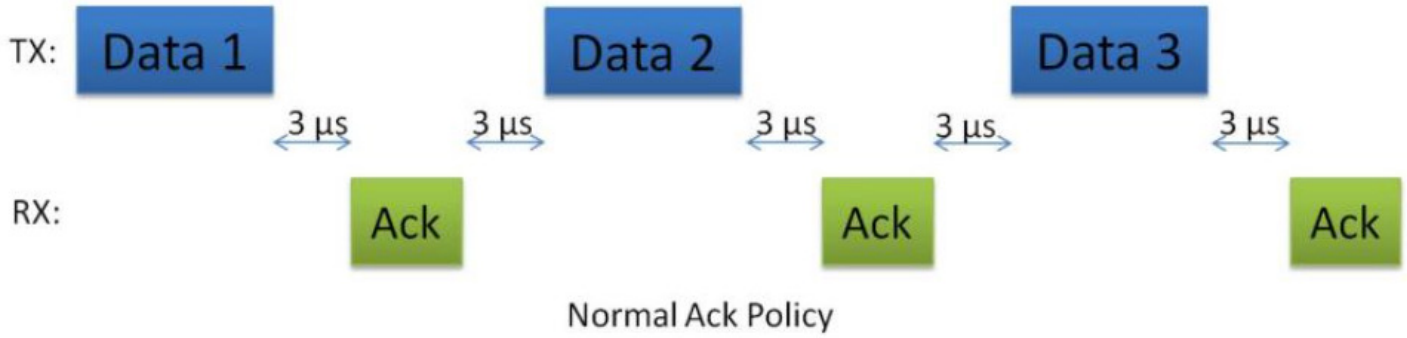
La couche PHY du IEEE 802.11ad… (cont')

- une modulation ultra simple : BPSK/QPSK
  - là où 802.11ac permet le 256-QAM
- … un unique stream
  - là où 802.11ac permet 8 streams
- …mais **$B_w \simeq 2$ GHz** (!)
  - permet d'atteindre le très haut débit
- le hardware est plus simple avec 802.11ad
  - **technologie idéale pour la connexion sans fils d'équipements, elle est moins adaptée à une couverture WiFi résidentielle (par ex.)**
- mais pas d'avenir :
  - « **Intel abandonne ses produits WiGig - IEEE 802.11ad** », **ZDNet,** http://www.zdnet.fr/actualites/intel-abandonne-ses-produits-wigig-39857096.htm, septembre 2017.

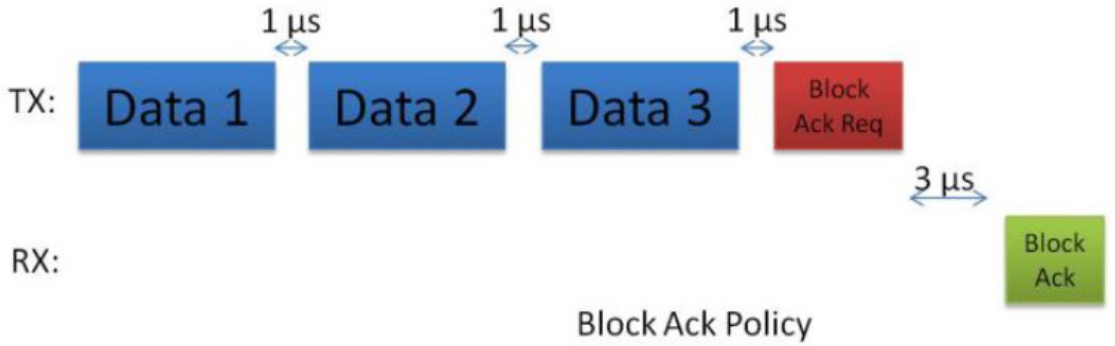
La couche PHY du IEEE 802.11ad… (cont')

- une politique d'acquittement par bloc de trames
  - **économise du temps**

Classic per-frame ACK (simplified)



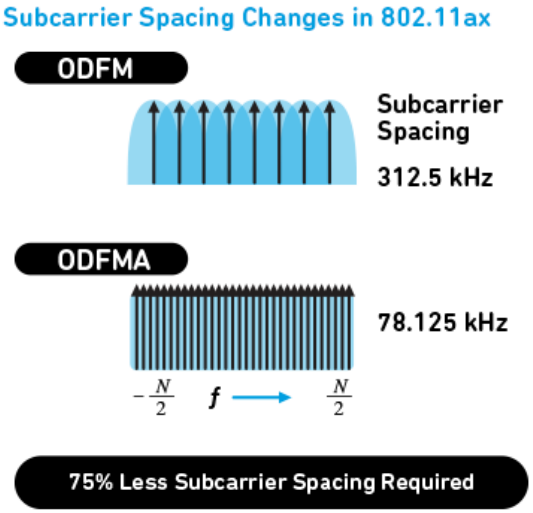
Block ACK for bulk transfers



Source : « WiGig and IEEE 802.11ad: for Multi-Gbps WPAN and WLAN », N. SaiShankar & al.

La couche physique du IEEE 802.11ax

- 802.11ax est la norme **Wi-Fi 6** de 2019
  - dépasse 11 Gbps (théorique)
  - sur 2.4 et 5 GHz (et sur 1 à 7 GHz si disponible)
    - **permet une gestion unifiée de toute la BP**
  - idem 802.11ac : canaux de 20, 40, 80 ou 160 MHz
  - une modulation OFDM plus fine…
    - **plus de canaux, plus étroits, plus denses, pour une meilleure utilisation du spectre**

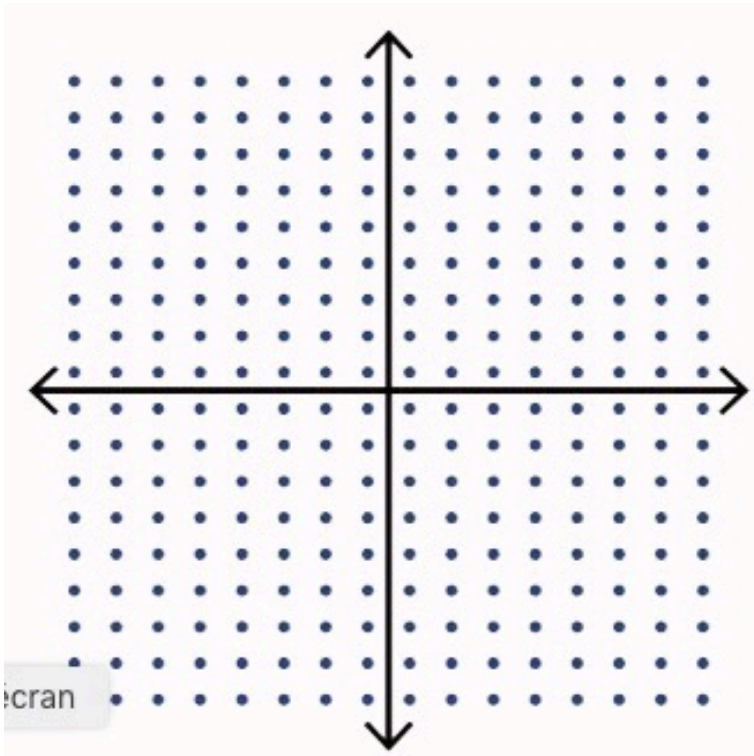


802.11ac

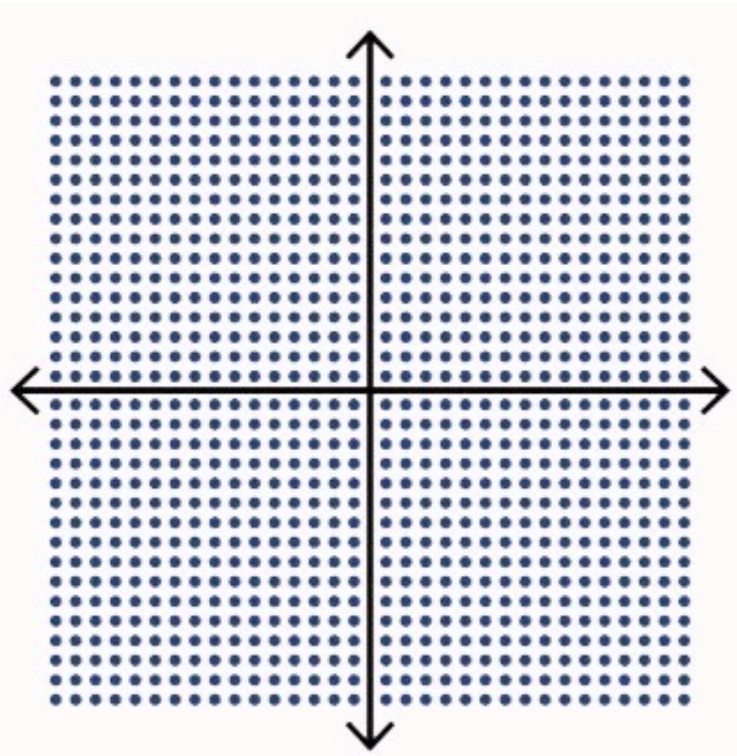
802.11ax

La couche PHY du IEEE 802.11ax… (cont')

- modulation jusqu'à **1024 QAM** en conditions optimales



256 QAM…



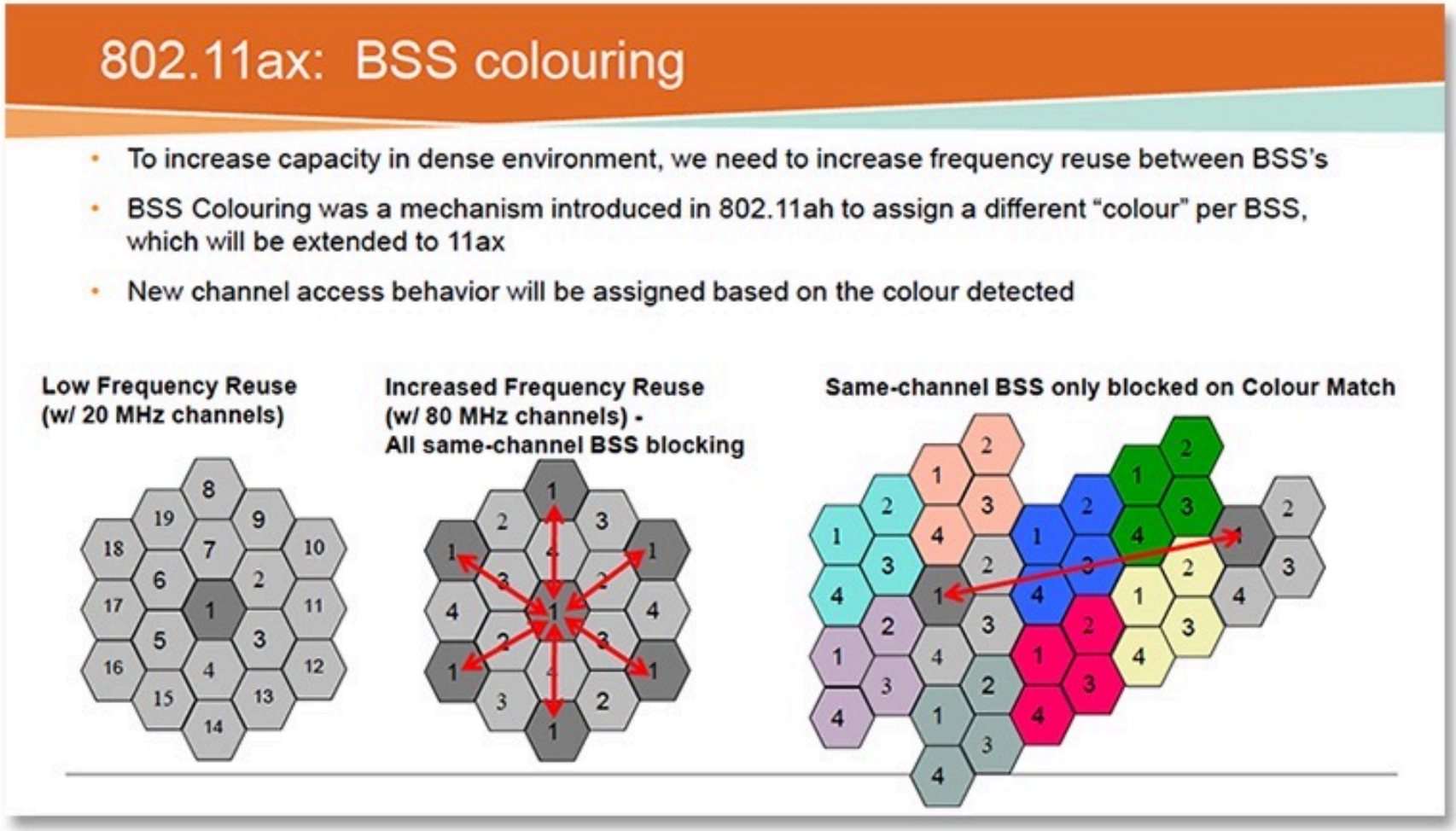
ou 1024 QAM ?

La couche physique du IEEE 802.11ax… (cont')

- une utilisation par "Resource Unit" (RU)
  - **au lieu d'affecter toute la BP à une station… à chaque station désirant tx/rx est affecté un ensemble de sous canaux (RU)**
  - **permet un usage parallèle (plusieurs transmissions en parallèle)**
    - jusqu'à 74 clients pour un canal de 160 MHz (au lieu de 1)
  - **peut considérablement réduire la latence**
    - plusieurs stations peuvent transmettre **simultanément** sur le support

La couche physique du IEEE 802.11ax… (cont')

- une meilleure **cohabitation** avec d'autres réseaux 801.11ax



les AP contigus choisissent une "couleur" différente et ajoutent un « color ID » dans les entêtes PHY/MAC

Wifi et sécurité

- Plusieurs mécanismes plus ou moins fiables...
- SSID *(historique !)*
  - habituellement envoyé en clair dans les trames balises, on peut configurer la BS pour ne pas le faire
  - empêche une station de se connecter...
    - **... tant qu'elle n'a pas pu sniffer la connexion d'une station autorisée car le SSID est transmis en clair à ce moment là**
- *Access* Control List (ACL) *(historique !)*
  - on liste sur la BS les adresses MAC autorisées
  - marche...
    - **... sauf si on sniffe des trames autorisées, et on change l'adresse MAC de sa carte (possible avec certaines cartes)**

Wifi et sécurité... (suite)

- WEP *(historique !)*
  - permet authentification et chiffrement
  - repose sur RC4 et une clef secrète partagée par BS et chaque station
  - marche bien...
    - **... tant que l'on n'a pas affaire à des attaquants un tout petit peu décidés**
    - **RC4 a bien des failles**
    - **les détails d'utilisation montrent qu'il y a des lacunes**
    - **on casse le tout après récupération d'un certain volume de trafic**

Wifi et sécurité... (suite)

- WPA2 / IEEE 802.11i-2004
  - https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
  - EAP (Extended Auth. Prot.) gère l'authentification
    - **inclue un contrôleur et un serveur d'authentification**
    - **plusieurs déclinaisons : par ex. EAP-TLS**
  - TKIP (Temporal Key Integrity Protocol)
    - **apporte chiffrement et intégrité**
    - **gère des clefs temporaires**
    - **indépendant du bloc de chiffrement : par ex. AES**

- maintenant WPA3…