Emerging Wireless Networks Course/ M1 NDE: The WiFi (Continued)

Ali Benzerbadj

Ain Temouchent University BELHADJ Bouchaib (ATUBB)

26 septembre 2021

Plan

Plan

Plan

Plan

Bandes de fréquence

Qu'est ce qu'une bande de fréquence ?

- Une bande de fréquences est une plage de fréquences avec une fréquence minimale et une fréquence maximale spécifiques.
- La bande des 2,4 GHz, par exemple, démarre à 2,412 GHz et se termine à 2,462 GHz (en Europe et aux États-Unis) et à 2,484 GHz (au Japon).
- Une bande de fréquences est divisée en différents canaux.

Bandes de fréquence

- En 1985, les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine. Ces bandes de fréquence, baptisées ISM (Industrial, Scientific,and Medical), à savoir les bandes :
  - 902-928 MHz
  - 2.400-2.4835 GHz,
  - 5.725-5.850 GHz.
- En Europe, la bande allant de 890 à 915 MHz est utilisée pour les communications mobiles (GSM). Par conséquent, seules les bandes 2.400 à 2.4835 GHz et 5.725 à 5.850 GHz sont disponibles.

Bandes de fréquence

Bandes ISM : Industrial, Scientific and Medical ?

Les bandes ISM sont des bandes radioélectriques **réservées au niveau international** pour l'utilisation à des fins **industrielles**, **scientifiques** et **médicales**, comme leur nom l'indique. Ces bandes sont **gratuites** et sont définies par :

- *the Federal Communications Commission (FCC)*, en Amérique
- *l'European Telecommunications Standards Institute (ETSI)*, en Europe

Bandes de fréquence

Remarque

1. Les bandes de fréquence 2,4 GHz et 5 Ghz sont les bandes de fréquence les plus couramment utilisées :
   - La bande des 2,4 GHz (meilleure portée)
   - La bande des 5 GHz (meilleur débit)
2. Comme en téléphonie mobile :
   - Plus une fréquence est basse, plus elle porte loin.
   - A l'inverse, plus une fréquence est élevée, plus les débits sont élevés mais sur une plus courte distance.

Bandes de fréquence

Lower Frequency (MHZ)	Upper Frequency (MHZ)	
2400	2500	It carry a maximum of 3 non-overlapping channels Used by 802.11b/g/n
5725	5875	It carry up to 23 non-overlapping channels Gives shorter range than 2.4GHZ Used by 802.11a/n Gives a shorter range than 2.4 GHz

Bandes de fréquence

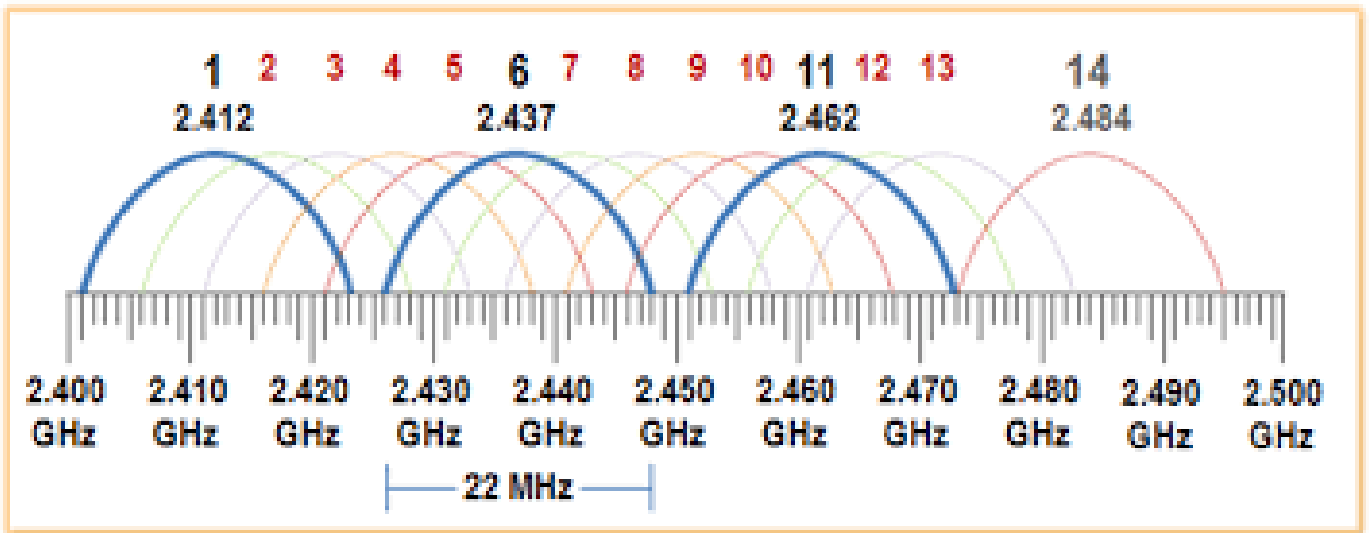


Figure 1 – 2.4 GHz 802.11 Channels.

Bandes de fréquence

Channel number	Lower Frequency (MHz)	Center Frequency (MHz)	Upper Frequency (MHz)
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Table 1 – Frequencies of the total of fourteen 802.11 WiFi Channels (2.4 GHz 802.11 Channel frequencies).

Bandes de fréquence

Channel Number	Europe (ETSI)	North America (FCC)	Japan
1	√	√	√
2	√	√	√
3	√	√	√
4	√	√	√
5	√	√	√
6	√	√	√
7	√	√	√
8	√	√	√
9	√	√	√
10	√	√	√
11	√	√	√
12	√	no	√
13	√	no	√
14	no	no	802.11b only

Table 2 – 2.4 GHz WiFi Channels availability.

Bandes de fréquence

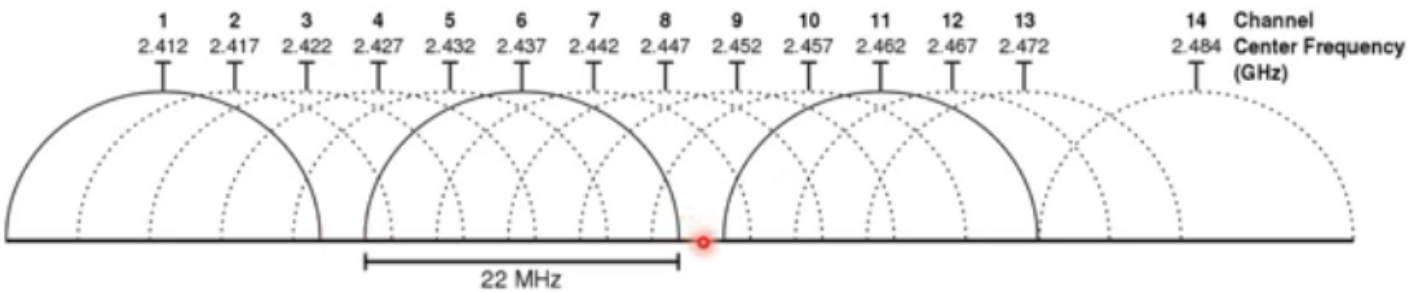


Figure 2 – Graphical representation of 2.4GHz band channels overlapping.

Bandes de fréquence

- 14 channels defined but not all allowed in all countries.
- The wlan/WIFI channels are spaced 5 MHz apart.
- Non-Ovelapping channels for 2.4GHz band are 1, 6 and 11.

Bandes de fréquence

Remarques

- Chaque canal est séparé du précédent de seulement 5 MHz $\Rightarrow$ un risque d'interférences élevé (sur la bande des 5 GHz, les canaux sont séparés de 20 MHz, ce qui évite le chevauchement des bandes).
- Chaque canal a une largeur de bande de 22 MHz (appelée "20 MHz"), ce qui recouvre les canaux voisins.
- Par exemple, le canal 6 avec sa largeur de bande de 22 MHz empiète sur les canaux 4, 5, 7 et 8. Des interférences peuvent donc avoir lieu si votre routeur Wi-Fi utilise le canal 6 et que d'autres sources utilisent ces canaux voisins.

Bandes de fréquence

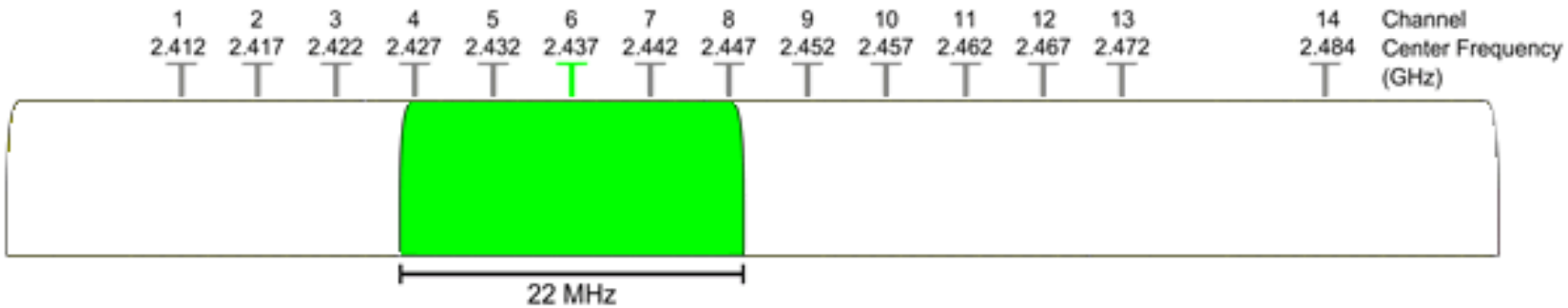


Figure 3 – Largeur de bande de 22 MHz du canal 6 sur la bande des 2,4 GHz.

Bandes de fréquence

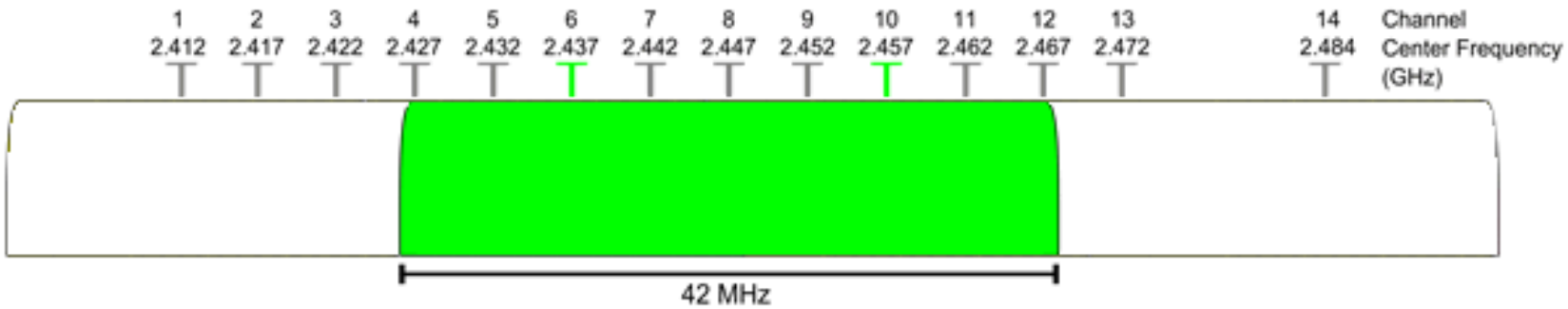


Figure 4 – Largeur de bande de 42 MHz du canal primaire 6 (canal secondaire définie sur 10) sur la bande des 2,4 GHz

Bandes de fréquence

Remarques

- Pour que les bandes ne se chevauchent pas, il est donc conseillé de séparer chaque émetteur sans-fil de 4 canaux sur la bande des 2.4 GHz (déjà pré-défini ainsi en 5 GHz).
- Le problème d'interférences peut être encore plus problématique dans le cas suivant par exemple :
  - La norme Wi-Fi 802.11n permet d'utiliser deux canaux simultanés, appelés "primaire" et "secondaire" qui permettent de doubler les débits – le choix du canal secondaire (primaire+4 ou primaire-4) se faisant automatiquement. Cela donne une largeur de bande de 42 MHz (appelée "40 MHz").

Bandes de fréquence

Reamarques

- Plus un canal est large, plus il est sujet aux interférences et susceptible d'interférer avec d'autres appareils
- Il est donc conseillé de séparer chaque émetteur sans-fil de 8 canaux en cas d'utilisation d'une largeur de bande de 40 MHz.
- Un canal ayant une largeur de 40 MHz est qualifié de canal large, un canal de 20 MHz étant qualifié d'étroit.

Bandes de fréquence : 5 GHz Channels and frequencies

- All of the 25 of the available 5GHz channels are non-overlapping at 20 MHz band.
- But gives a shorter range than 2.4GHz
- The 5GHz is divided into several different sections.
  - UNII-1 : 36, 40, 44, 48
  - UNII-2a : 52, 56, 60, 64
  - UNII-2c extended : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144)
  - UNII-3 : (149, 153, 157, 161, 165)
  - UNII stands for Unlicensed National Information Infrastructure
  - Channels were spaced 20 MHz apart, thereby providing nonoverlapping channels

Bandes de fréquence : 5 GHz Channels and frequencies

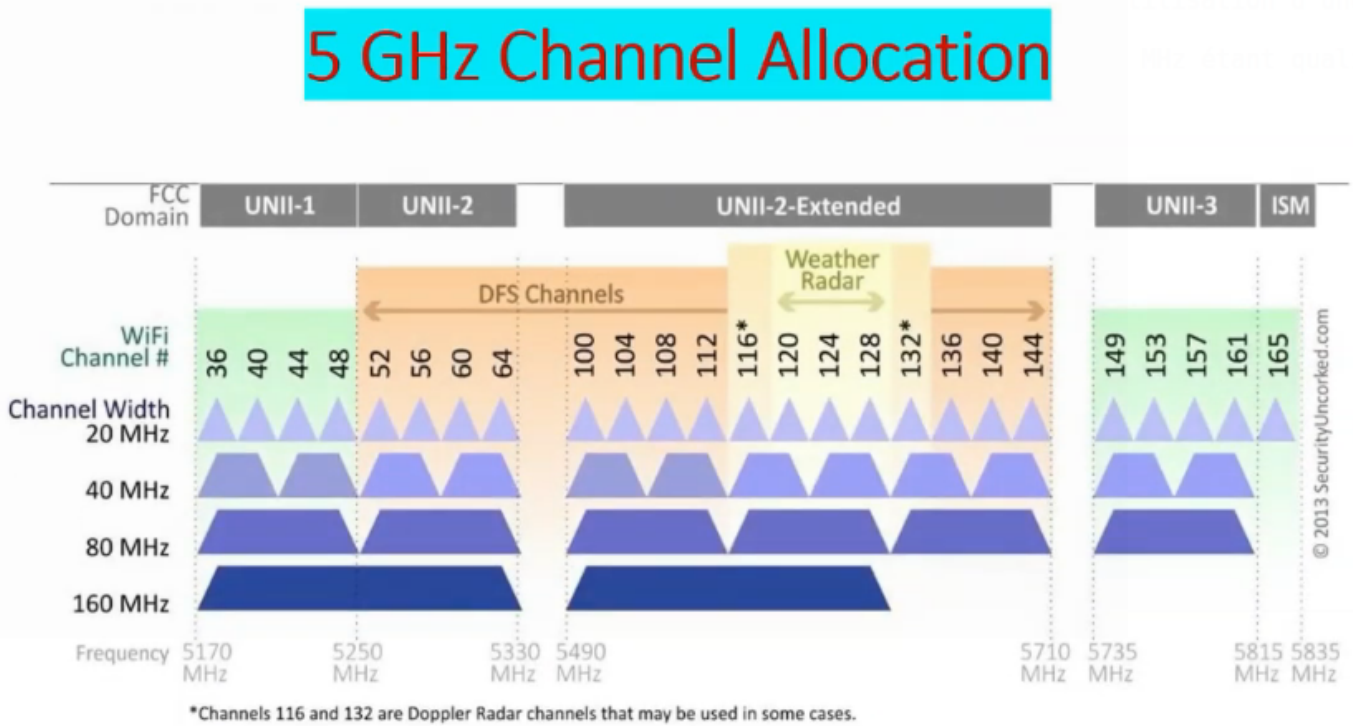


Figure 5 – 5 GHz Channels and frequencies

Bandes de fréquence : 5 GHz Channels and frequencies

5 GHz Channel Allocation

CHANNEL NUMBER	FREQUENCY MHZ	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
36	5180	Indoors	✓	✓
40	5200	Indoors	✓	✓
44	5220	Indoors	✓	✓
48	5240	Indoors	✓	✓
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✓	No Access
153	5765	SRD	✓	No Access
157	5785	SRD	✓	No Access
161	5805	SRD	✓	No Access
165	5825	SRD	✓	No Access

Bandes de fréquence : 5 GHz Channels and frequencies

- DFS channels are used for Defense purposes
- Weather radar
- Home purposes

Normes WiFi

Norme	Année	Débit Max. Théorique	Fréq.	Modulat.	Compatib. avec
802.11 d'origine	Juin 1997	1.2Mbps	2.4 GHZ	FHSS, DSSS Spread Spectrum)	
802.11a	Sept 1999	54 Mbps	5 GHZ	OFDM	
802.11b	Sept 1999	11 Mbps	2.4 GHZ	DSSS (Direct-Sequence Spread Spectrum)	
802.11g	Juin 2003	54 Mbps	2.4 GHZ	DSSS, OFDM	802.11b
802.11n	Juin 2009	600 Mbps (grâce au MIMO)	2.4 GHZ, 5GHZ		802.11g 802.11b
802.11ac	Juin 2013	> 1Gbps	5GHZ		
802.11ax WIFI6	Fin 2018	>10 Gbps	2.4GHZ, 5GHZ	OFDMA	

Normes WiFi

Rappel

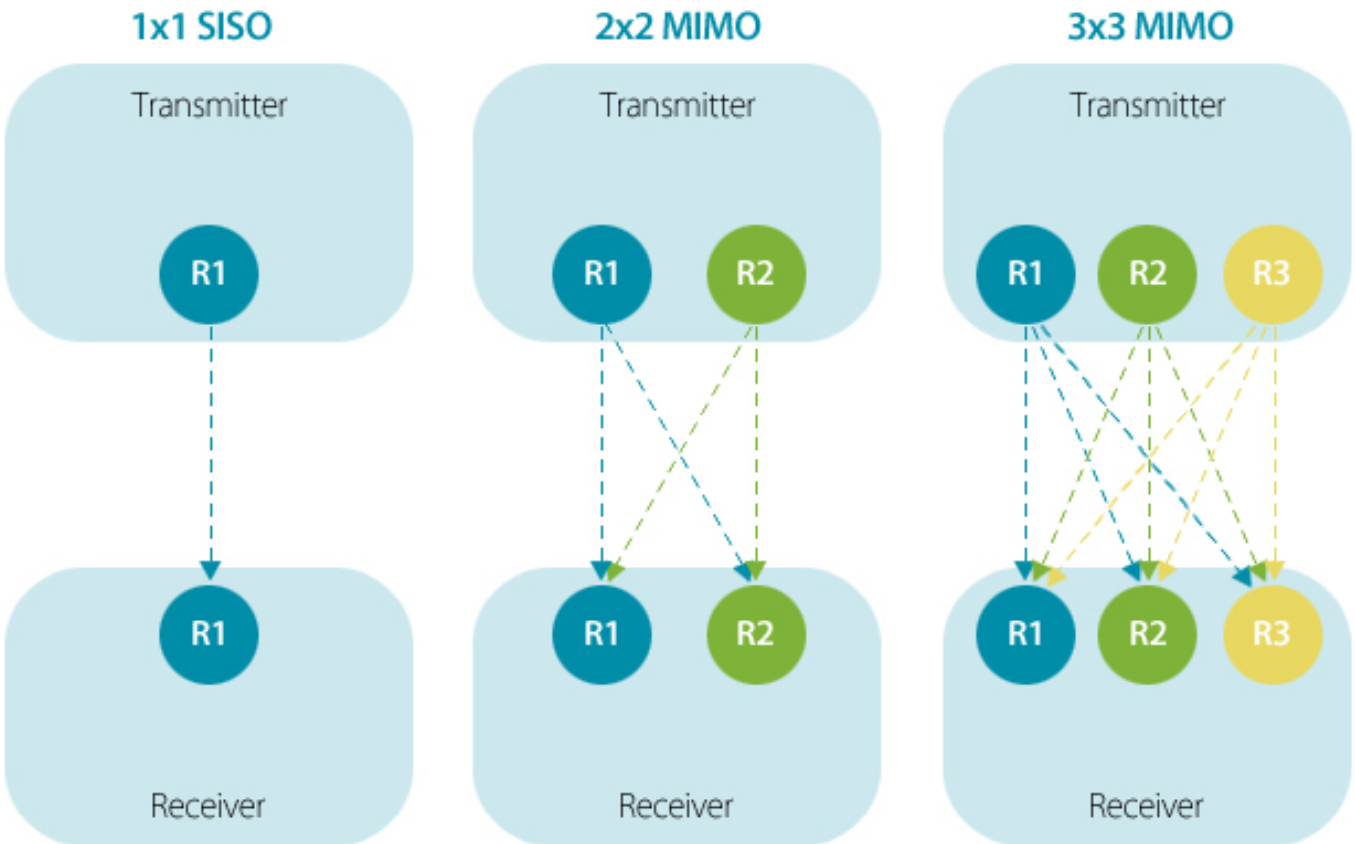
- La norme 802.11a (jusqu'à 54 Mb/s) sur la bande des 5 GHz. Elle était principalement destinée aux entreprises.
- La norme 802.11b (jusqu'à 11 Mb/s) sur celle des 2,4 GHz. Elle fera son apparition chez les particuliers au début des années 2000.
- Les deux normes datent de 1999 (Standard completed in 1999)
- Le 802.11b a été remplacée en 2003 par le 802.11g. Elle est rétrocompatible avec la précédente norme et capable de monter jusqu'à 54 Mb/s.

Normes WiFi

MIMO

- Par défaut, un flux Wi-Fi 802.11n permet de monter jusqu'à 150 Mb/s, mais il est possible d'atteindre un débit maximum théorique de 600 Mb/s grâce au MIMO (Multiple Input, Multiple Output) en opposition au SISO (Single Input, Single Output). Cette technique permet d'utiliser jusqu'à quatre flux simultanément, et améliorer le débit d'autant.
- Si une seule antenne permet d'atteindre 150 Mb/s, une configuration 2x2 MIMO (deux antennes en réception, deux en émission) passe à 300 Mb/s, contre 450 Mb/s avec du 3x3 MIMO (3 flux) et jusqu'à 600 Mb/s pour du 4x4 MIMO (le maximum selon la norme IEEE du Wi-Fi

Normes WiFi (MIMO-Suite)



Normes WiFi

MIMO-Suite

- Il faut que l'émetteur et le récepteur disposent du même nombre d'antennes pour profiter au mieux du MIMO. On peut faire une analogie avec une route avec une ou plusieurs voies : s'il y a trois voies en entrée, mais une seule en sortie (ou vice-versa), cela ne sert pas à grand-chose.

Normes WiFi

Wi-Fi HaLow (802.11ah)

- 802.11ah, aussi connu sous le nom de Wi-Fi HaLow est une norme récente.
- Annoncée officiellement en janvier 2016.
- Principalement pensée pour les objets connectés avec une portée plus importante que le Wi-Fi classique, tout en consommant moins d'énergie.

Normes WiFi

Wi-Fi HaLow (802.11ah) (Suite 1)

- Les débits sont évidemment assez faibles puisqu'il est question de quelques dizaines de Mb/s.
- La bande de fréquence utilisée est bien plus basse et se situe en dessous du gigahertz. Comme en téléphonie mobile, elle porte plus loin et pénètre mieux dans les bâtiments.
- Attention : les fréquences ne sont pas unifiées au niveau mondial.

Normes WiFi

Wi-Fi HaLow (802.11ah) (Suite 2)

- Trouver des blocs disponibles sous le Gigahertz n'est pas chose évidente, car il s'agit de fréquences très préciseuse. Par exemple, en Europe elles sont de 863 à 868 MHz, contre 902 à 928 MHz aux États-Unis et de 916.5 à 927.5 MHz au Japon, etc.

Normes WiFi

Norme 802.11af

- La norme 802.11af est une autre norme Wi-Fi qui permet de connecter des objets connectés sur des distances encore plus longues avec des fréquences comprises entre 54 et 790 MHz.

Normes WiFi

WiFi 6 : Un Wi-Fi intelligent ?

- Wi-Fi intelligent et écologique sont des mots qui reviennent souvent pour désigner le Wi-Fi 6. Cela est dû à ses nouvelles fonctionnalités qui font la promesse d'une réelle évolution pour 2019.
  Nous pouvons notamment citer le MU-MIMO qui sera ici utilisable pour l'envoi et le téléchargement, l'OFDMA (Orthogonal Frequency-division multiple access) qui adapte les bandes de fréquences à chaque utilisateur selon ses besoins afin de libérer de la bande passante sur le réseau. OFDMA est une technologie que l'on retrouve déjà dans les réseaux 4G et permettra en outre de communiquer avec un grand nombre de périphériques simultanément.

Normes WiFi

WiFi 6 : Un Wi-Fi intelligent ?

- Le TWT (Target Wakeup Time) qui passe le réseau en mode veille si le point d'accès n'est pas sollicité, ce qui aura pour résultat de réduire la facture énergétique de l'appareil, mais aussi d'éviter les interférences et autres perturbations avec d'autres réseaux à proximité. Le WPA 3 succèdera lui au WPA 2 dont la fiabilité a été remise en cause de nombreuse fois ces dernières années.

Normes WiFi

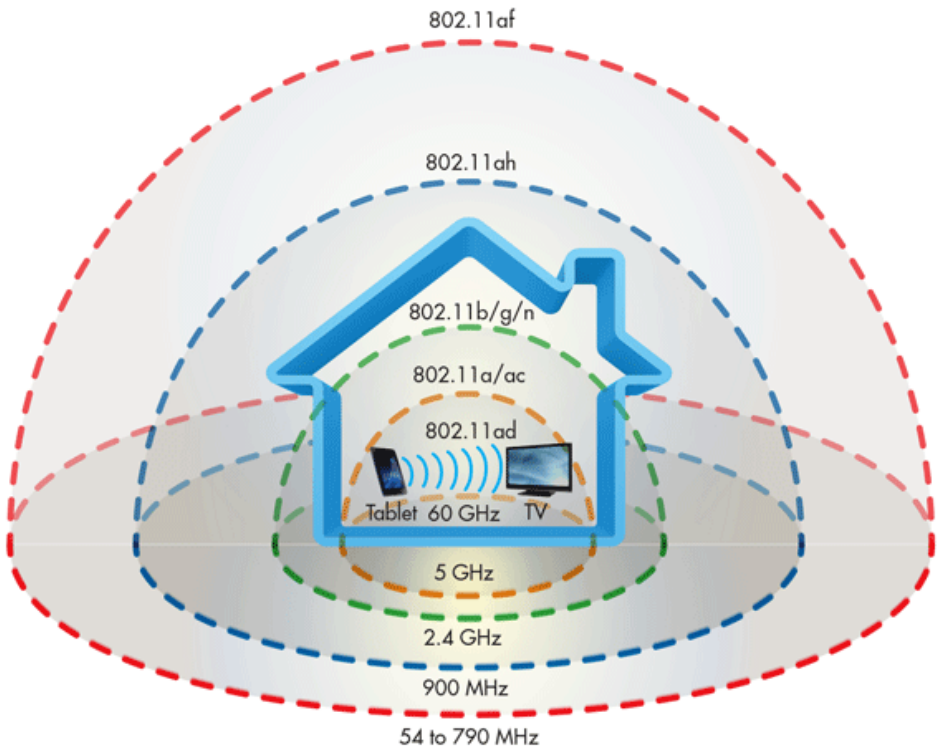


Figure 6 – Fréquences, Portées et débits des normes WiFi.

Normes WiFi

Remarque

La portée dans un réseau sans fil dépend de :

- La puissance des emetteurs (AP+antennes choisis)
- La sensibilité du recepteur
- Affaiblissement du signal (masque radio + interférences)

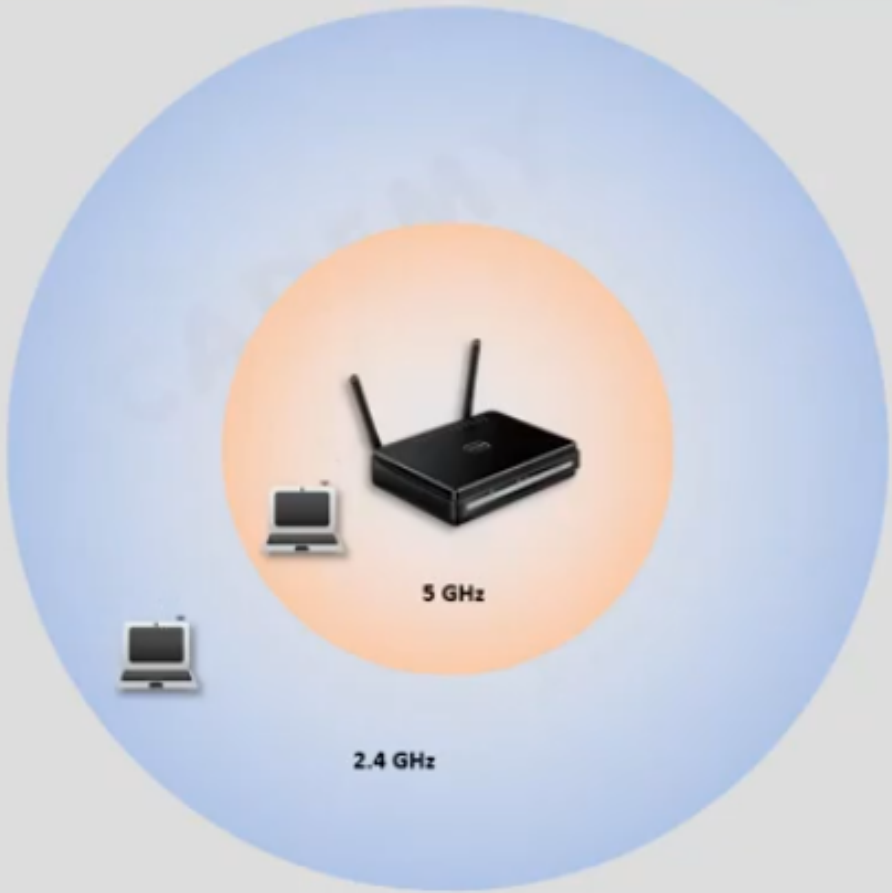
Normes WiFi

Remarques

- Les débits évoqués sont des maximums théoriques. Ils seront donc toujours inférieurs dans la pratique, même dans des conditions parfaites.
- En Wi-Fi, les fabricants parlent toujours de Mb/s (ou Gb/s) et pas de Mo/s (ou Go/s) : pour les convertir il faut les diviser par 8.
- Ainsi, 300 Mb/s correspond à 37,5 Mo/s et 1 Gb/s correspond à environ 125 Mo/s. Là encore, toujours en théorie et au maximum bien évidemment.

Normes WiFi

2.4 GHz	5 GHz
➢ 802.11 b, g, n, ax	➢ 802.11 a, n, ac, ax
➢ Slower Speed	➢ Faster Speed
➢ Longer Range	➢ Shorter Range
➢ More Radio Interference	➢ Less Radio Interference
➢ 3 non-overlapping	➢ 25 non-overlapping at 20 MHz wide ➢ 12 non-overlapping at 40 MHz wide ➢ 6 non-overlapping at 80 MHz wide ➢ 2 non-overlapping at 160 MHz wide



www.everestacademy.in 8

Analyseurs Wifi pour Ubuntu

- nmcli d wifi (Network manager command line interface nmcli)
- wavemon (sudo apt-get install wavemon)
- linssid (sudo apt-get install linssid)

Capture du trafic wifi

- Disable Networking in Network Manager
- iwlist wlan0 scan
- iwlist wlan0 freq
- sudo ifconfig wlan0 down
- sudo iwconfig wlan0 mode monitor
- iwconfig
- ifconf wlan0 up
- sudo tcpdump -iwlan0 -s 1500 -w trafic.cap
- sudo ifconfig wlan0 down
- sudo iwconfig wlan0 mode managed
- sudo ifconfig wlan0 up
- sudo iwconfig wlan0 essid MyNetwork

airmon-ng

- airmon-ng est un Script permettant d'activer (ou désactiver) le mode moniteur d'une carte réseau. Dans ce cas la carte Wi-Fi, se place en "observateur" du réseau. (https ://doc.ubuntu-fr.org/aircrack-n)
- Activer le mode moniteur sur wlan0 $\rightarrow$ sudo airmon-ng start wlan0
- N'écouter que sur le canal 3 $\rightarrow$ sudo airmon-ng start wlan0 3
- Arrêter le mode moniteur $\rightarrow$ sudo airmon-ng stop wlan0
- vérifier l'état du système $\rightarrow$ sudo airmon-ng

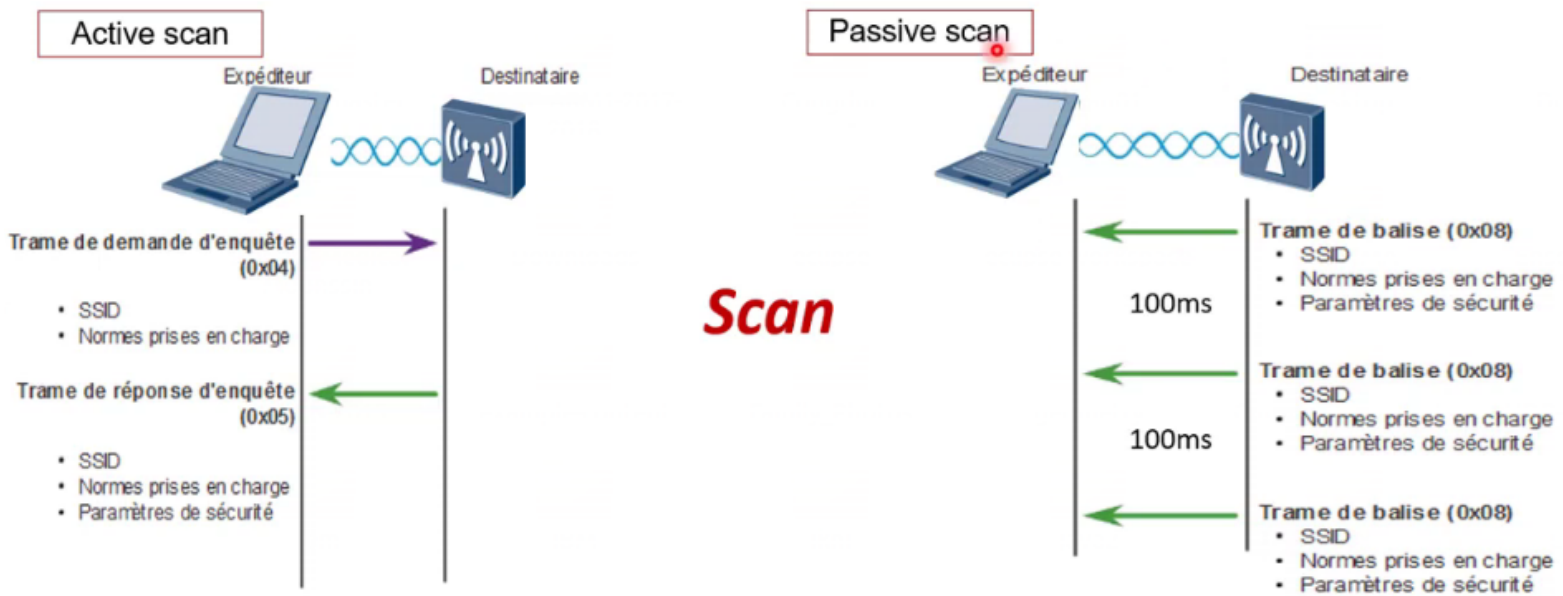
Création d'un interface virtuelle capturer le trafic

1. Créer une interface virtuelle mon0 en mode **monitor** pour snifer le trafic 802.11 :
   - iwconfig
   - sudo airmon-ng start wlan0
2. Notez que l'inteface wlan0 possède maintenant une interface virtuelle active
3. Lancer une capture wireshark ou tcpdump sur l'interface mon0.

Types de scanning dans les WLAN

- A client (or STA) can use two types of scan :
  - Active scanning
  - Passive scanning
- During an active scan, a client transmits a probe request ans listens for a probe response from an AP.
- In a passive scan, the client listens on each channel for beacons sent periodically by an AP.
- A passive scan generally takes more time, since the cleint must listens and wait for beacon versus actively probing to find an AP.
- Another limitation with a Passive scan, is that if a client does not wait long enough on a channel, than the client may miss an AP beacon.

Types de scanning dans les WLAN



Types de scanning dans les WLAN

- AP silencieux
- AP diffusant des beacon frames et la STA entre dans la zone de couverture de l'AP

Débit d'association

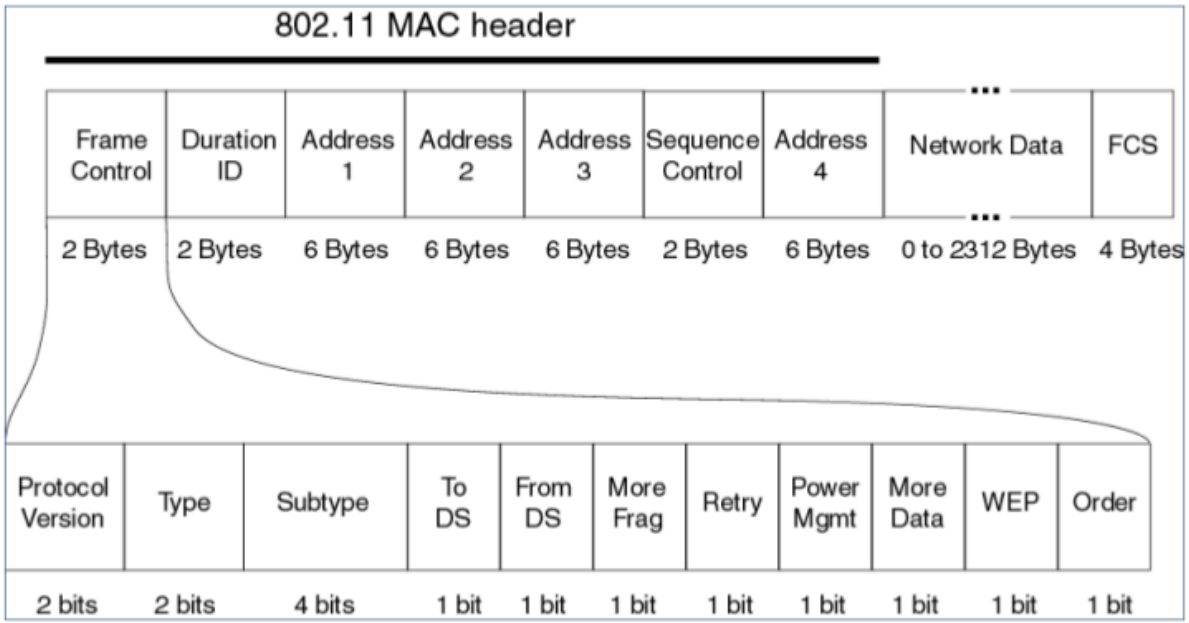
- Variable : 54 48 36 24 12 11 5,5 2 1 Mbit/s
- Adapté automatiquement en fonction :
  - de la puissance reçue par l'appareil (distance)
  - du rapport Signal/Bruit (qualité du signal)

IEEE 802.11 Frame Types

1. Data Frames : Carrying "useful" payloads
2. Control Frames : Facilitate the exchange of data frames
   - Ready-to-send (RTS) and Clear-to-send (CTS) frames
   - Acknowledgement (ACK) frames
3. Management Frames : Maintenance of the network
   - Beacon frames
   - Authentication / deauthentication frames
   - Association / deassociation frames
   - Probe request / response frames
   - Reassociation request / response frames

Slide borrowed from Jürgen Schönwälder (Jacobs University Bremen), Computer Networks' 2019

IEEE 802.11 Frame Format



The maximum size of an 802.11 frame is **2346** bytes.

IEEE 802.11 Frame Format

1. Type values :
   - Management Frame : 00
   - Control Frame : 01
   - Data Frame : 10
   - The value 11 is reserved
2. Subtype is the specific type of frames (Beacon frame, RTS frame, CTS frame, Probe request frame etc.)
   - RTS : 1011
   - CTS : 1100
   - ACK : 1101

Wi-Fi naming system

A new naming system identifies Wi-Fi generations by a numerical sequence

- Wi-Fi 6 identifies devices that support 802.11ax technology
- Wi-Fi 5 identifies devices that support 802.11ac technology
- Wi-Fi 4 identifies devices that support 802.11n technology

Modes et mécanismes d'association

- Mode Master (AP)
- Mode Managed or Client (Station mode)
- Mode Adhoc et mode bridge
- Mode repeater
- Mode Monitor