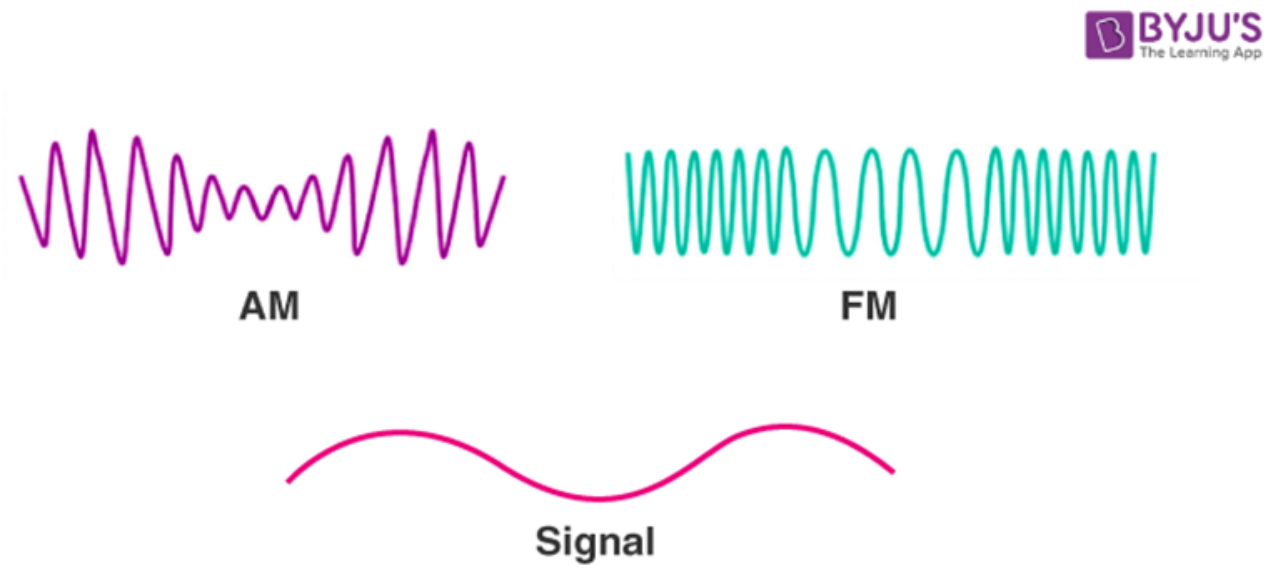
Signaux électromagnétiques/Wifi

Fréquences et canaux

Les transmissions des technologies sans-fil telles que WiFi, radio FM, LTE et Bluetooth sont des pulsations électromagnétiques permettant l'acheminement de données au même titre que des pulsations dans un circuit électrique ou des pulsations lumineuses dans une fibre optique.

Type de signal

Pour ce qui a trait aux communications numériques, le signal est généralement mesuré par modulation de fréquence plutôt que par modulation d'amplitude. Ceci implique que la fréquence/vitesse des pulsations est mesurée plutôt que la variation de leur force pour identifier le signal.



Puisqu'il s'agit d'un signal circulant dans l'air, il est possible de le comparer à des ondes sonores pour mieux comprendre son fonctionnement. Plusieurs termes représentant du son sont même utilisés pour décrire certaines caractéristiques de ces types de signaux.

Puissance de signal

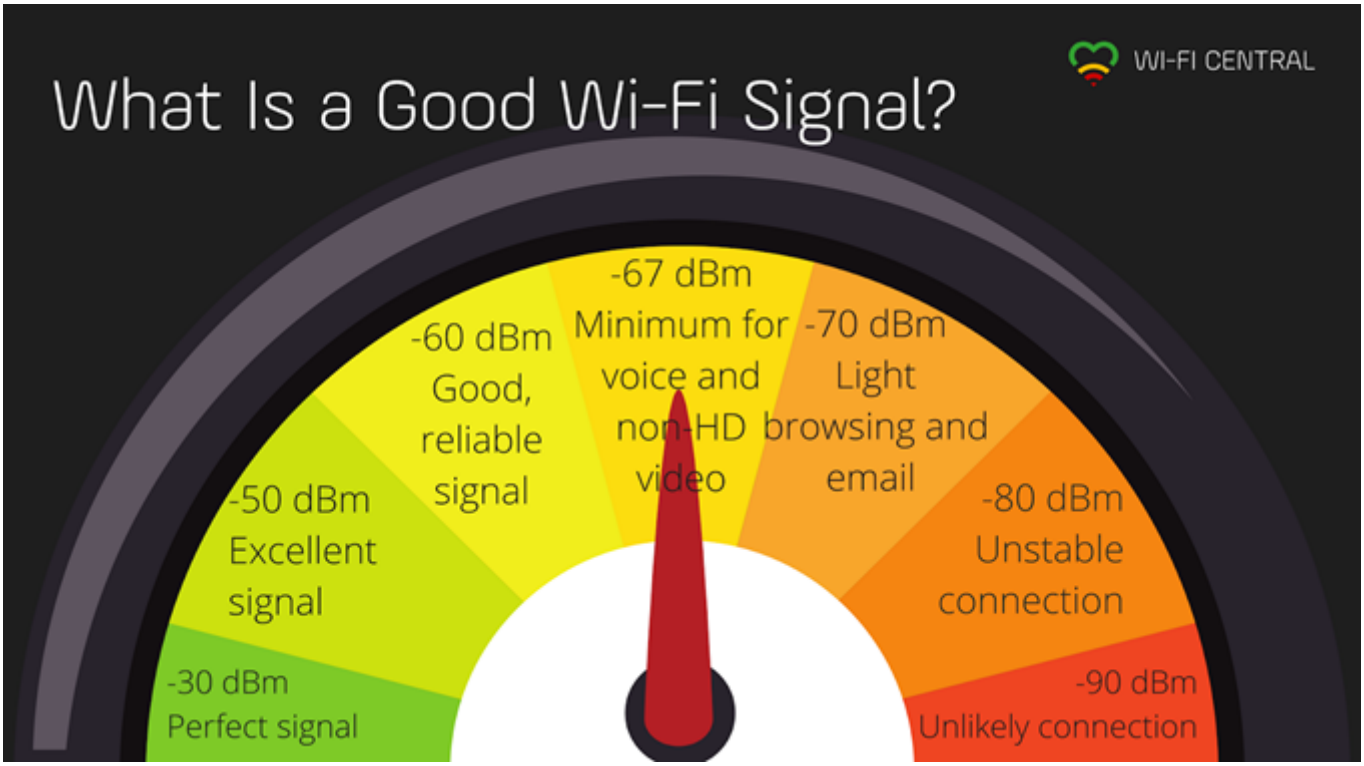
Tout comme pour un bruit audible, la puissance de signal est calculée en décibels et représente le volume auquel la radio de l'adaptateur sans-fil entend le signal. Le décibel est une mesure

logarithmique plutôt que linéaire. Dans le cas du décibel, une augmentation de 10 dB représente un volume 10 fois plus élevé. 20 dB serait un volume 10 fois plus élevé que 10 dB et 30 dB serait un volume 100 fois plus élevé que 10 dB. Cette unité de mesure permet de quantifier l'intensité d'une onde sonore perçue et sa valeur réduit lorsqu'on s'éloigne de la source ainsi que si l'on ajoute de l'insonorisation entre notre point de mesure et la source du bruit.

Pour transposer ce concept en communications sans fil, le volume de réception d'un signal est aussi mesuré en décibels mais puisqu'un signal électromagnétique n'est pas un signal audible, l'unité de mesure doit être comparée à une puissance électrique. Cette unité de mesure est le dBm (décibel-milliwatt). Cette mesure compare le niveau de signal perçu à un milliwatt. Puisqu'un signal WiFi est généralement sous 1 mW, la valeur représentant le signal reçu sera généralement négative.

0 dBm = 1 mW
-10 dBm = 0.1 mW
-20 dBm = 0.01 mW
-30 dBm = 0.001 mW
Et ainsi de suite...

Au même titre qu'à un concert où le volume peut être trop élevé peut nuire à notre perception des détails plus fins de la musique, le niveau de signal d'un signal WiFi peut être trop élevé. Le niveau de signal recherché en WiFi est généralement situé entre -45 et -55 dBm pour une bonne communication. Si le volume est trop élevé, il arrivera plus souvent que certaines informations soient mal reçues et devront être retransmises. Différentes applications (ex. FaceTime ou la réception de courriels) nécessitent différents niveaux de signaux et ce niveau de signal changera en fonction de la génération de WiFi employée. Il est accepté de façon générale qu'un signal inférieur à -80 dBm sera instable.



Il est aussi important de garder en tête que tout comme différentes paires d'oreilles seront plus ou moins sensibles au bruit et que différentes personnes auront différentes capacités vocales, certaines antennes sans-fil seront plus puissantes ou moins puissantes et certaines antennes sans-fil seront plus sensibles ou moins sensibles à la réception de signal. Certaines antennes seront optimisées pour émettre et recevoir dans une direction particulière et d'autres seront optimisées pour émettre et recevoir dans toutes les directions.

Interférence

Tout comme avec un signal sonore, des signaux électromagnétiques avoisinants peuvent interférer avec la communication entre deux appareils sans-fil.

Bruit de fond

Lorsqu'on parle de bruit de fond, il s'agit de tout signal électromagnétique ne faisant pas partie de la technologie employée. On peut ici penser à tenter d'avoir une conversation avec un voisin lors d'un concert extérieur où le volume du spectacle enterre la voix de notre interlocuteur. Dans cette situation, l'information se perd et devra être retransmise à moins de pouvoir parler assez fort ou de trouver une façon d'atténuer le bruit de fond (ex. mettre ses mains autour d'une oreille).

Quelques exemples de bruit de fond affectant le wifi sur la bande 2.4 GHz sont un four à micro-ondes, bluetooth, des interphones de surveillance, des téléphones sans fil, des appareils audiovisuels sans fil (ex. microphones et haut-parleurs, radio et télévision amateur, etc.), certains radars et même des télécommandes de portes de garage.

Temps d'antenne

À défaut de pouvoir bien cohabiter avec d'autres technologies sur une fréquence, lorsque l'on parle de WiFi, la méthode employée pour éviter de l'interférence est que chaque appareil d'un réseau sans fil parlera à tour de rôle pour éviter qu'un appareil enterre le signal d'un autre et que les deux informations entrent en collision et soient perdues.

Bandes de fréquences et canaux

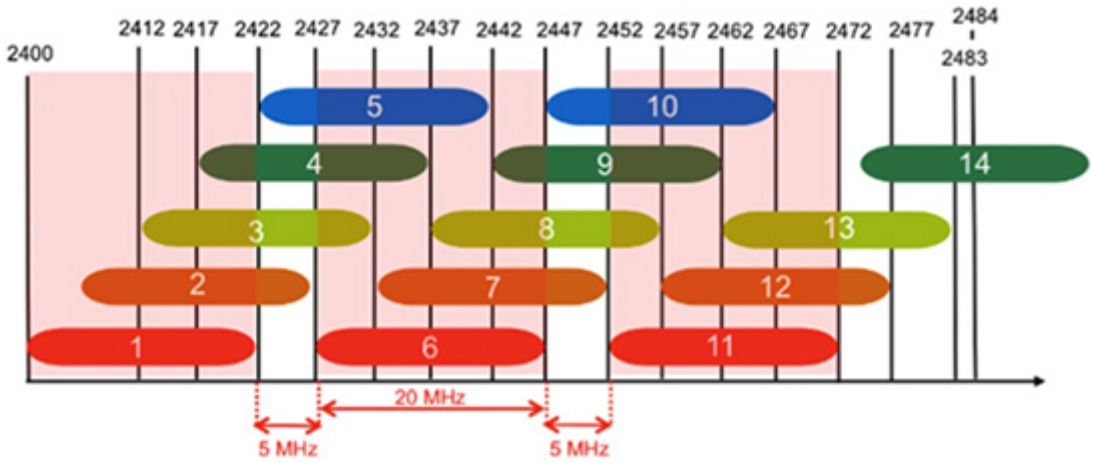
Afin de permettre à plusieurs réseaux sans fil de cohabiter sans interférer entre eux, plusieurs fréquences sont mises à la disposition du public général pour interconnecter leurs appareils. Ces bandes de fréquences sont réglementées par des organismes tels que l'ITU aux états-unis, la CRTC au Canada et le CEPT en Europe. Chaque organisme détermine ses propres standards mais les standards pour les appareils personnels sont généralement similaires pour éviter de devoir manufacturer des appareils sans fil spécifiques à chaque organisation.

Les bandes de fréquences allouées au WiFi les plus connues sont entre 2.4 et 2.5 GHz et entre 5 et 6 GHz. Plusieurs autres existent mais sont moins communes telles que le 900 MHz, le 6 GHz (de plus en plus courant pour WiFi 7), 45 GHz et 60 GHz (pour des liens à longue portée et à haute vitesse).

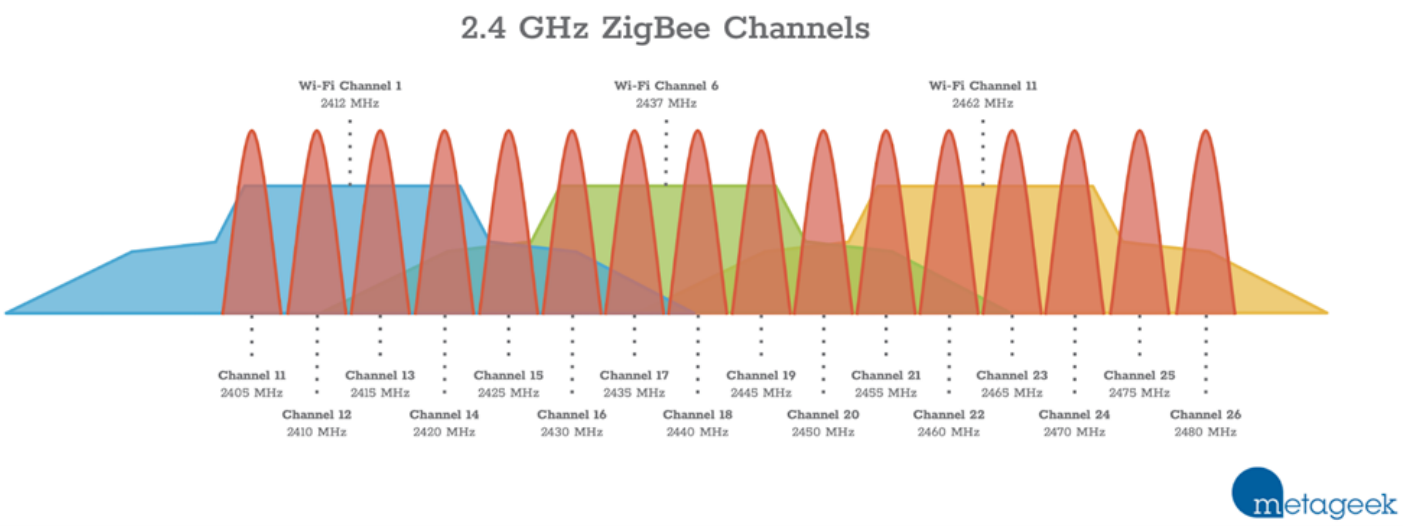
Canal

Un canal sans fil est une étendue de fréquences contiguës qui serviront à interconnecter plusieurs appareils sur un seul réseau. Pour ceux ayant déjà utilisé une radio à roulette, vous aurez remarqués que même si vous n'avez pas précisément sélectionné la fréquence du poste de radio, vous êtes en mesure d'entendre le canal avec un peu de grésillement et que si vous sélectionnez une fréquence entre deux stations de radio ayant une fréquence voisine, il est parfois possible d'entendre les deux stations en même temps. Lorsque l'on peut écouter deux stations à la fois, on appelle ce phénomène le "chevauchement" ou "overlapping" de fréquences où deux appareils communiquent simultanément sur la même fréquence.

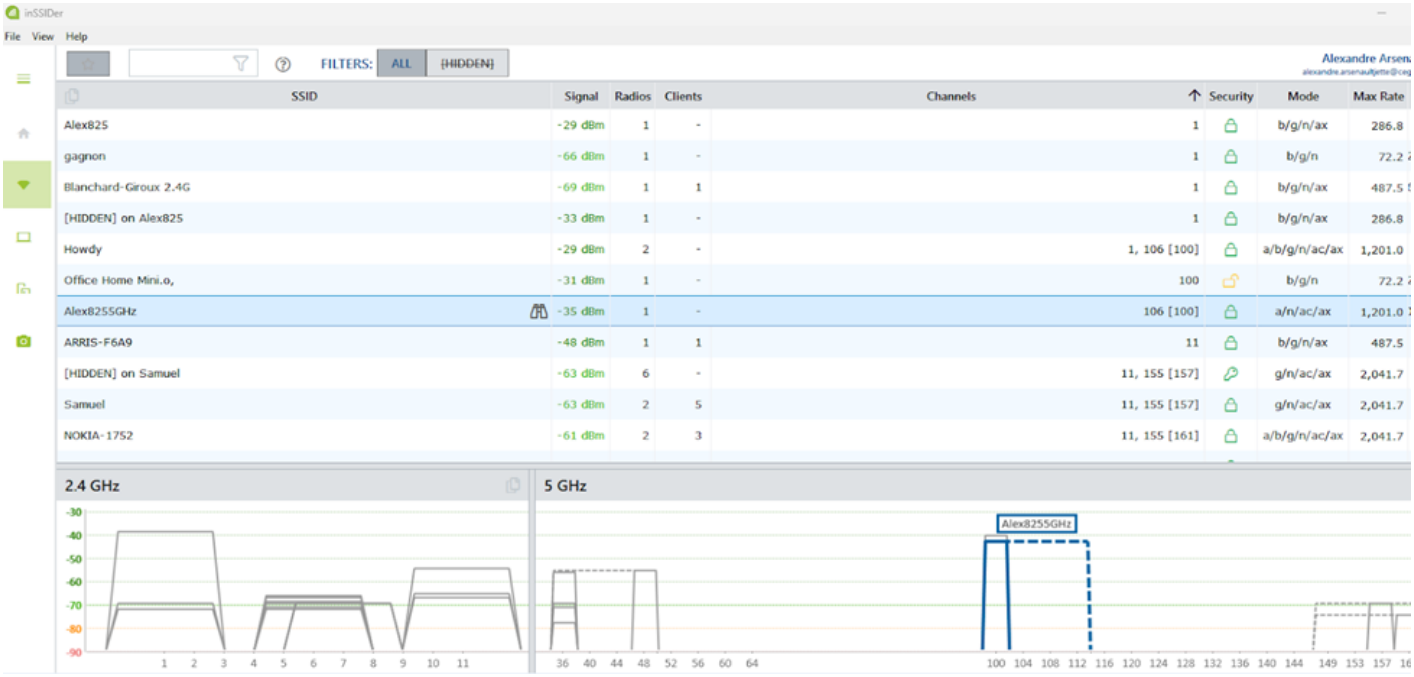
Un canal est donc défini par une fréquence centrale et occupe une largeur/tolérance de fréquences autour de cette fréquence centrale. Chaque canal sans-fil se situe à 5 MHz d'écart les uns des autres mais la largeur d'un canal peut varier. Par exemple, en 2.4 GHz, il est possible d'établir un canal d'une largeur de 10 MHz, 20 MHz ou 40 MHz. Plus un canal est étroit, moins il est susceptible à l'interférence des réseaux voisins mais la bande passante ou la vitesse de ce réseau sera plus restreinte que celle d'un réseau plus large.



La majorité des réseaux 2.4 GHz sont par défaut configurés avec une largeur de 20 MHz. En 2.4 GHz au Canada, seulement les canaux de 1 à 11 sont permis. Le graphique ci-dessus représente tous les canaux d'une largeur de 20 MHz, on peut y déterminer que seulement 3 canaux de 20 MHz de largeur sont utilisables sans chevauchement. La majorité des réseaux occupent donc les canaux 1, 6 et 11 avec une largeur de 20 MHz. Si aucun autre réseau est à portée, il serait possible de configurer une largeur de canal de 40 MHz pour augmenter la bande passante disponible sur le réseau. On peut par contre remarquer avec le graphique suivant que si l'on utilise le canal 6 avec une largeur de 40 MHz, ce réseau chevaucherait à la fois les canaux 1 et 11 ayant une largeur de 20 MHz.



La répartition de réseaux sans fil sur plusieurs canaux sans chevauchement permet donc à plusieurs appareils de parler simultanément sans interférer ensemble. Certains outils tels que inSSIDer permettent de visualiser l'utilisation des différents canaux pour choisir le bon canal en fonction des réseaux avoisinants.



Authentification et encryption

Noms des réseaux

Le "SSID" (Set Service IDentifier) est le nom que porte un réseau sans fil. Cet identifiant est composé de deux valeurs, le BSSID (Base SSID) et le ESSID (Extended SSID). Le BSSID représente l'adresse MAC de la radio diffusant le réseau sans fil. Le ESSID quant à lui représente le nom du réseau configuré que vous verrez en cherchant les réseaux disponibles.

Méthodes d’authentification

Puisque les communications sont émises dans l’air, il est possible d’intercepter et écouter le trafic de tous les appareils WiFi à portée d’une carte WiFi permettant ce genre de capture. Il est donc important de sécuriser ces réseaux et encrypter les données circulant entre un point d’accès et une station (client) d’un réseau.

Ouvert

Un réseau ouvert ne nécessite pas d’authentification et n’effectue aucune encryption de données.

Ouvert amélioré

Un réseau ouvert amélioré ne nécessite toujours pas d’authentification mais bénéficie d’encryption malgré tout grâce à un protocole nommé Opportunistic Wireless Encryption (OWE) permettant d’encrypter le trafic de chaque client du réseau individuellement. Ceci prévient la capture de trafic non encrypté par des acteurs malveillants.

Clé prépartagée

La plupart des réseaux domestiques utilisent une clé prépartagée ou PSK (Pre-Shared Key) qui est un mot de passe commun à tous les appareils clients du réseau. Cette méthode d’authentification est simple à mettre en place et à petite échelle peut facilement être modifiée en cas de piratage. Différentes générations d’authentification et d’encryption existent pour ce standard.

Historiquement, WEP (Wired Equivalent Privacy ou “sécurité équivalente à une connexion câblée”) était sécurisé par une clé hexadécimale d’une valeur jusqu’à 156 bits. Cette méthode d’encryption est très facile à casser en écoutant le processus d’authentification d’un appareil à un réseau sécurisé par ce protocole.

WPA, WPA2 et WPA3 (WiFi Protected Access) sont maintenant les standards de sécurité des réseaux sans-fil. WPA utilisait un processus d’encryption nommé TKIP (Temporal Key Integrity Protocol) et les versions plus récentes utilisent maintenant un processus d’encryption nommé AES (Advanced Encryption Standard). Ces deux processus changent périodiquement la clé d’encryption pour sécuriser davantage les communications entre les appareils WiFi, AES étant plus robuste que TKIP.

Protocole d’Authentification Extensible

EAP (Extensible Authentication Protocol) est une méthode d’authentification à un réseau sans-fil utilisant les mêmes standards d’encryption qu’une clé prépartagée mais faisant emploi d’une identité unique pour chaque client du réseau. On peut penser ici au réseau d’une entreprise où l’on s’y authentifie avec une adresse de courriel et un mot de passe. Ce type d’authentification a comme avantage de pouvoir autoriser et révoquer l’accès au réseau individuellement plutôt que de devoir remplacer le mot de passe pour tous les usagers afin de bannir seulement un appareil ou une personne du réseau mais nécessite la mise en place d’un serveur d’authentification.

Revision #9
Created 2024-11-14 06:29:00 UTC by Alexandre Arsenault-Jetté
Updated 2025-11-13 16:43:19 UTC by Alexandre Arsenault-Jetté