Réseau
Wi-Fi

Sommaire

1. Introduction

2. Modes de fonctionnement

3. Le médium

4. La loi

5. Sécurité

- Le terme Wi-Fi suggère la contraction de Wireless Fidelity, par analogie au terme Hi-Fi.
- Le terme Wi-Fi a été utilisé pour la première fois de façon commerciale en 1999, et a été inventé par la société Interbrand.

- La norme 802.11 définit les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques ;

- la **couche physique** (notée parfois couche PHY), proposant trois types de codage de l'information (DHSS / FHSS / Infrarouge) ;

- la **couche liaison de données**, constituée de deux sous-couches :
  - le contrôle de la liaison logique (Logical Link Control, ou LLC) ;
  - le contrôle d'accès au support (Media Access Control, ou MAC).

- La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données ;
- La couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations ;
- La norme 802.11 propose donc en réalité trois couches :
  - une couche physique appelée PHY ;
  - deux sous-couches relatives à la couche liaison de données du modèle OSI.

- Le mode Infrastructure permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès (AP) ;
- Les AP agissent comme des concentrateurs (exemple : répéteur ou commutateur en réseau Ethernet).
- La mise en place d'un tel réseau oblige de poser à intervalles réguliers des AP dans la zone qui doit être couverte par le réseau.
- Les AP doivent être configurées avec le même nom de réseau (SSID = Service Set IDentifier) afin de pouvoir communiquer.
- L'avantage est de garantir un passage obligé par l'AP, il est donc possible de vérifier qui accède au réseau.

- Le mode 'Ad-Hoc' permet de connecter directement les machines équipés du Wi-Fi sans utiliser d'AP ;
- La mise en place d'un tel réseau se borne à configurer les machines en mode ad hoc, la sélection d'un canal (fréquence), d'un nom de réseau (SSID) communs à tous et si nécessaire d'une clé de chiffrement ;
- L'avantage de ce mode est de s'affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de point d'accès ;
- Des protocoles de routage dynamique (OLSR, AODV, …) permettent l'utilisation de réseaux maillés autonomes dans lesquels la portée ne se limite pas à ses voisins (tous les participants jouent le rôle du routeur).

- Un point d'accès en mode pont sert à connecter un ou plusieurs points d'accès entre eux pour étendre un réseau filaire ;
- La connexion se fait au niveau de la couche 2 OSI ;
- Un point d'accès doit fonctionner en mode racine « root bridge » (généralement celui qui distribue l'accès Internet) et les autres s'y connectent en mode « bridge » pour ensuite retransmettre la connexion sur leur interface Ethernet ;
- Chacun de ces points d'accès peut éventuellement être configuré en mode pont avec connexion de clients ;
- Ce mode permet de faire un pont tout en accueillant des clients comme le mode infrastructure.

- Un point d'accès en mode « Répéteur » permet de répéter un signal Wi-Fi plus loin ;
- Contrairement au mode pont, l'interface Ethernet reste inactive ;
- Chaque « saut » supplémentaire augmente le temps de latence de la connexion ;
- Un répéteur a également une tendance à diminuer le débit de la connexion car son antenne doit recevoir un signal et le retransmettre par la même interface ce qui en théorie divise le débit par deux.

- L'onde électromagnétique est formée par le couplage de deux champs :
  - le champ électrique (E) ;
  - le champ magnétique (B).

- On en déduit que la longueur d'onde est défini par la fréquence et la célérité: $\lambda = c/f$

  avec λ en m, c en m/s et f en Hz

- Calculons λ sachant que f = 2,4Ghz et c = 3.10^9 m/s

  $\lambda = 2,4.10^6 \times 3.10^9 = 0,12248$m soit 12,248 cm

- L'atténuation est un facteur à prendre en compte lorsque l'on utilise des ondes électromagnétique. Une onde n'est pas envoyée à l'infini et plus on va s'éloigner de la source, plus la qualité du signal diminuera ;
- L'onde électromagnétique qui voyage rencontre des électrons qu'elle va exciter. Ceux-ci vont rayonner et perturber le signal et donc l'atténuer ;
- Plus la fréquence est élevée, plus la distance de couverture est faible mais plus la vitesse de transmission des données est forte.
- La diffraction est une zone d'interférence entre l'onde directe d'une source et l'onde réfléchie par un obstacle ;

- Il existe deux principaux modèles d'antennes : les omnidirectionnels et les directionnelles ;

- Les antennes omnidirectionnelles ont un gain variant entre 1 et 15 dBi et qui offrent un rayonnement sur 360° ;

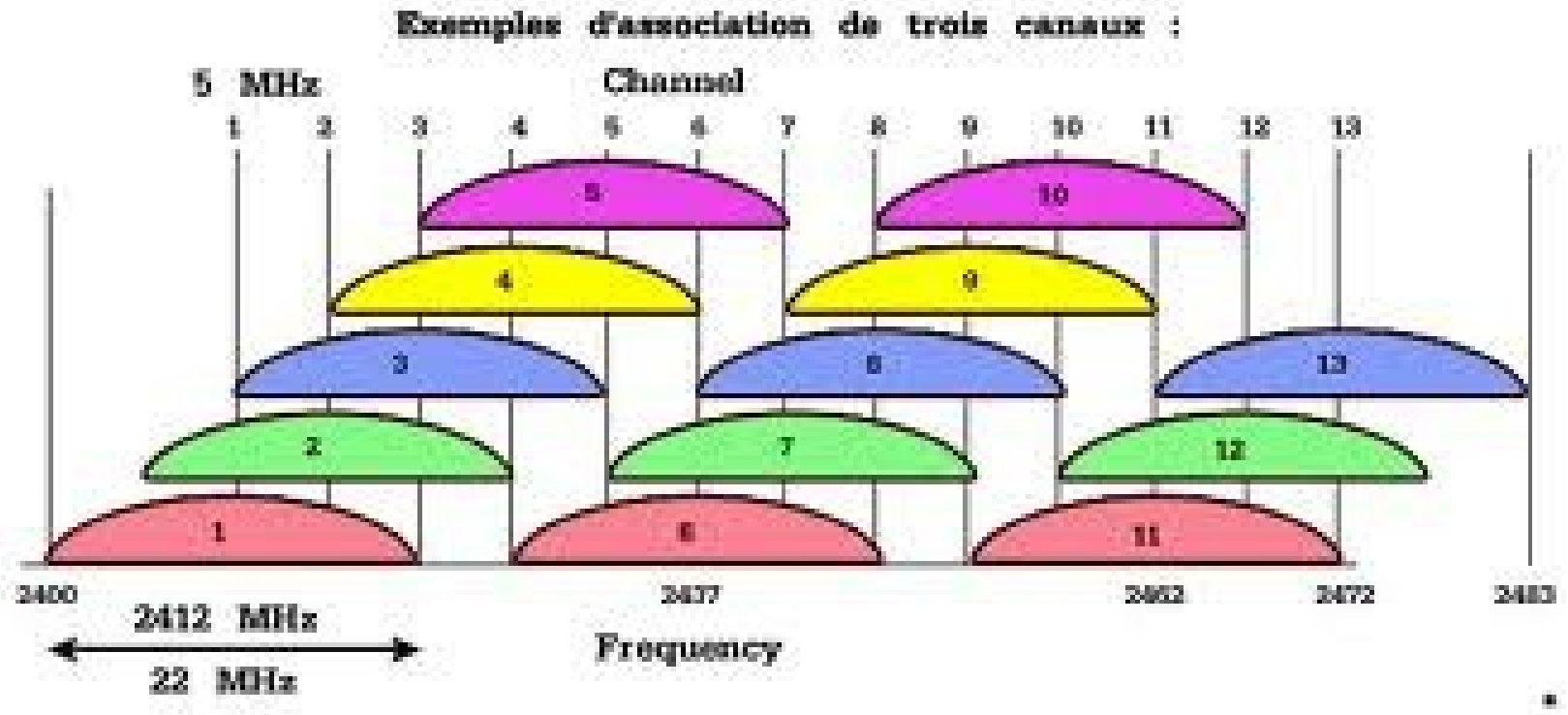
- Les antennes directionnelles ont un gain allant de 5 à 24 dBi avec un rayonnement directif. Elles permettent d'établir des liaisons point à point mais également de couvrir une zone limitée dans le cas d'une antenne à angle d'ouverture important.

- antenne omnidirectionnel :

- antenne directionnelles :

- L'ARCEP www.arcep.fr/ ex ART - Autorité de Régulation des Télécommunications - est un organisme français chargé de réguler les télécommunications. Ses activités vont de la délivrance de permis pour réseaux indépendants à la sanction en cas d'infraction ;
- Les conditions techniques à respecter établies par l'ART sont les suivantes :
  - la puissance de rayonnement ne doit pas excéder 100 mW à l'intérieur des murs ;
  - la puissance de rayonnement ne doit pas excéder 10mW à l'extérieur des murs.

En France on peut émettre sur 13 canaux différents :



- Pour remédier aux problèmes de confidentialité des échanges sur un réseau sans fil, le standard 802.11 intègre un mécanisme simple de chiffrement de données, le WEP ;
- Ce cryptage travaille avec l'algorithme RC4 pour chiffrer les données et utilise des clés statiques de 64 ou 128 voire 152 bits suivant les constructeurs.
- Le principe consiste à définir une clé sécrète qui doit être déclarée au niveau de chaque adaptateur sans fil du réseau ainsi que sur le point d'accès.
- La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame.

- Cependant, le WEP possède un grand nombre de failles, le rendant vulnérable ;
- Concernant l'intégrité des données, le CRC32 (implanté dans le WEP) comporte une faille permettant la modification de la chaîne de vérification du paquet à comparer à la chaîne finale issue des données reçues, ce qui permet à un pirate de faire passer ses informations pour des informations valides ;
- L'utilisation du WEP réduit le débit de la connexion du fait du cryptage/décryptage des paquets ;
- Il s'agit d'une solution de sécurité existant dans tous les équipements Wi-Fi (très utilisé par le grand public ainsi que par certaines entreprises) ;
- Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données.

- Le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (Temporal Key Integrity Protocol) qui sont dynamiques et permet l'authentification des utilisateurs grâce au 802.1x et à l'EAP (Extensible Authentification Protocol) ;
- Le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP, lui, utilisait la même clé pour tout le réseau sans fil.
- Les clés WPA sont générées et distribuées de façon automatique par le point d'accès sans fil ;
- Un vérificateur de données permet de vérifier l'intégrité des informations reçues pour être sûr que personne ne les a modifiées.

- Quelques problèmes subsistent tout de même à ce protocole et notamment l'attaque de type « déni de service ».
- Si deux paquets utilisant une clé de cryptage incorrecte sont envoyés chaque seconde, le point d'accès sans fil « tuera » toutes les connexions utilisateurs pendant une minute. C'est un mécanisme de défense pour éviter les accès non-autorisés.
- Le SSID (Service Set IDentifier) n'est pas sécurisé ;
- Il manque :
  - une déconnexion rapide et sécurisée ;
  - une dé-authentification et une dé-association sécurisées ;
  - un meilleur cryptage (ex. AES)

- Le 802.11i, norme ratifiée en 2004, propose une solution de sécurisation poussée grâce à l'utilisation de l'AES au lieu du RC4 ;
- Le WPA-2 assure le cryptage ainsi que l'intégrité des données mais offre de nouvelles fonctionnalités de sécurité telles que le « Key Caching » et la « Pré-Authentification » ;

Key Caching :

Il permet à un utilisateur de conserver la clé PMK (Pairwise Master Key) - variante de PSK (Pre-Shared Key) du protocole WPA - lorsqu'une identification s'est terminée avec succès afin de pouvoir la réutiliser lors de ses prochaines transactions avec le même point d'accès.

Pré-Authentification :

Cette fonction permet à un utilisateur mobile de s'identifier avec un autre point d'accès sur lequel il risque de se connecter dans le futur. Ce processus est réalisé en redirigeant les trames d'authentification générées par le client envoyé au point d'accès actuel vers son futur point d'accès par l'intermédiaire du réseau filaire.

- C'est une fonctionnalité qui permet d'exclure ou de ne tolérer que certaines adresses MAC à accéder au réseau sans fil ;
- Ce système, qui permet donc de contrôler quelles cartes réseaux peuvent entrer sur le réseau, aurait permis une grande sécurité, malheureusement, le protocole 802.11b/g n'encrypte pas les trames où apparaissent ces adresses MAC ;

- Un simple logiciel, comme « kismet » par exemple, permet de voir les adresses MAC des clients et il suffit de l'usurper pour accéder au réseau...