TEA : Le Wifi

Agathe Perrin

1.Objectif

2.Recherches

a. Que veut dire Wifi ?

"Wifi" signifie en anglais "Wireless Fidelity" littéralement en français "fidélité sans fil". On peut également trouver une autre traduction moins littérale "accès sans fil à l'Internet".

b. Déterminez l'ensemble des caractéristiques du premier Wifi (norme, fréquence, vitesse, portée, canaux,..).

La première version du protocole 802.11 a été publiée en 1997. Elle permet d'atteindre des vitesses de liaison allant jusqu'à 2 Mbit/s. Cela a été mis à jour en 1999 avec 802.11b pour permettre d'atteindre des vitesses de liaison de 11 Mbit/s. La norme IEEE 802.11b sera ensuite renommé "wifi".
La portée était de 10 mètres et 8 canaux.

c. Quelles différences y'a t'il entre le WEP, WPA, WPA2 ? Sécurité personnelle et d'entreprise ?

WEP, WPA et WPA2 sont des protocoles de sécurité sans fil qui empêchent des connexions intrusives et non désirées sur un réseau.

WEP signifie "Wired Equivalent Privacy". Il a été mis en place de 1999 à 2004, il a été rapidement abandonné car difficile à mettre en place et difficile à configurer. Il devait être aussi sécuritaire qu'un réseau câblé mais il s'est avéré être très difficile à configurer.

Le protocole WPA (Wifi Protected Access) était une amélioration du WEP, WPA a été adopté peu avant l'abandon de WEP. Cependant WPA était également peu sécuritaire, le rendant vulnérable à différentes attaques.

WPA2 est la version 2 de WPA, la sécurité est meilleure et la configuration également. La principale faille est au niveau de l'accès à un réseau wifi sécurisé, si l'attaquant y à accès il peut utiliser certaines clés pour attaquer d'autres dispositifs sur le réseau.
Pour un particulier cela n'est pas très grave, en revanche beaucoup plus pour une entreprise.

d. Quelles différences y'a t'il entre les modes infrastructures, ad-hoc, pont et répéteur ?

Dans le mode infrastructure, chaque ordinateur se connecte à un point d'accès sans fil. Cet ensemble est nommé "ensemble de services de base" (basic service set en anglais, BSS). Chaque BSS possède un identifiant de 6 octets (48 bits) le BSSID qui correspond à l'adresse MAC du point d'accès.

Le mode ad-hoc permet à des machines sans fils de se connecter entre elles afin de créer un réseau "peer to peer". Dans ce mode la machine est en même temps le point d'accès et le client. Cet ensemble est nommé un "ensemble de services de base indépendants" (IBSS Independant Basic Service Set).

Le mode pont (ou "bridge") est un objet qui relie physiquement plusieurs réseaux, ces réseaux doivent être configurés en mode "pont". Le but est d'avoir un "relais" entre les appareils sur le réseau et le routeur qui reçoit Internet.

Enfin, un répéteur est un objet connecté à un point d'accès existant et répétant le signal wifi déjà émis pour en augmenter la portée.

e. A quoi servent les canaux pour un réseau wifi ?

Les canaux wifi servent à communiquer sur différentes fréquences. La radio est un bon exemple, une station de radio utilise un canal.

f. Quelle est la dernière norme sortie en regardant ses avantages ou ses avancées techniques ? (par rapport à la précédente et à la première).

La dernière norme est : 802.11-2016 parue en 2016. Elle ajoute par rapport à la précédente norme le standard 802.11ac : une plus grande fréquence (jusqu'à 6 GHz) permettant un débit jusqu'à 1300 Mb/s. Elle lui ajoute aussi le standard 802.11ad : qui ajoute une bande de fréquence de 60 GHz, peu compatible avec le matériel précédent et donc peu utilisé.
En comparaison avec la première version, 802.11a : le rayon de diffusion est plus large, la bande de fréquence est plus large, il y a plus de canaux, les débits sont plus élevés et plus d'appareils peuvent se connecter simultanément.

g. A quoi sert le WPS ?

Le WPS (Wifi Protected Setup) est un bouton physique qui permet à différents appareils de se connecter sur le réseau wifi librement, les sécurités étant temporairement coupées. Les appareils qui se sont

connectés pendant cette période sont mis en “liste blanche” par leur adresse MAC.

h. Peut-on hacker un réseau wifi ? Comment ?

Il existe 2 manières principales de pirater un réseau wifi :
“Passive Sniffing”, l’ordinateur écoute et tente de déchiffrer les activités du réseau cible.
“Man in the middle Attack”, un hacker se fait passer pour un point d’accès existant invitant l’utilisateur à s’y connecter et volant par la même occasion les identifiants.

3. Expérimentations

a. Combien de réseaux wifi différents détectez-vous à l’intérieur de votre domicile ? À l’extérieur? Y a-t-il une différence de nombres et de puissance et si oui pourquoi selon vous ?

A l’intérieur wifi analyser détecte 10 réseaux wifi, et 15 à l'extérieur.
Il y a une différence de nombre et de puissance à cause de la distance, du nombre et de l’épaisseur des murs entre l'application et les routeurs.

b. Quelles sont les sécurités utilisées pour ces réseaux ?

La majorité des réseaux sont en WPA2, et certains en WPA ou non sécurisés.

c. Quelles fréquences et quels canaux utilisent-ils ?

Ils utilisent la bande de fréquence de 20 MHz et les canaux 1, 11 et majoritairement 6.

d. Déterminez la portée de votre connexion wifi ? Vous vous déplacez en dehors de chez vous et vous regardez que le signal disparaît, réapparaît.

Le signal apparaît encore à 100m (selon l’application).

e. Peut-on connaître l’adresse MAC et l’adresse IP des bornes installées autour de chez vous ?

L’adresse MAC apparaît dans l’application, ainsi que l’adresse IP de mon routeur mais pas l’adresse IP des autres bornes.

f. Existe-t-il des réseaux ouverts. Est-ce que cela veut dire qu’ils ne sont pas sécurisés ?

N’importe qui peut “ouvrir” son réseau, et n’importe qui peut se connecter à un réseau ouvert. Selon la configuration du réseau les risques peuvent être plus ou moins important allant de la simple utilisation du réseau pour consulter Internet (hotspot wifi) à l’usage illégal d’un réseau personnel ouvert.

g. Quel est le débit maximum si je suis tout seul près de votre box ? Si vous êtes plusieurs ? Vous pouvez par exemple lancer des tests de débits avec plusieurs périphériques (téléphone, ordinateur,…)

Mon débit wifi maximum seule près de la box est 104 Mb/s.
Mon débit maximal avec un autre téléphone en test simultanément est de 64 Mb/s.