# TD-TP – Réseaux locaux sans-fil au standard WIFI

**Noms et prénoms** (à réaliser en binôme) : GUARDIA Quentin (aucun binôme trouvé)

**Date limite de remise du TP** : Dimanche 18h00 par courriel à « master2srs.dir@gmail.com »

**Instructions** : préciser dans le sujet de votre émail « **M1 CYBER TP6 WIFI** »

Installer et configurer votre point d'accès sans-fil en choisissant un SSID et une clé. Vous pourrez utiliser votre AP Wifi en local pour interconnecter votre PC portable et réaliser le TP qui suit.

Veuillez répondre aux questions ci-dessous pour réviser vos connaissances sur la technologie WIFI. Le logiciel MetaGeek est un scanner wifi. Vous l'utiliserez pour répondre aux questions 4 et 5 ci-dessous.

**Exercice 1**

Donnez les différents types de réseaux sans-fils, leur normalisation, leur portée.

**Exercice 2**

Faites un tableau récapitulatif des 3 types de réseaux 802.11 avec leurs bandes de fréquences, le débit, la portée.

Que peut-on dire sur les débits théoriques et réels ?

Donnez les différents modes de fonctionnement.

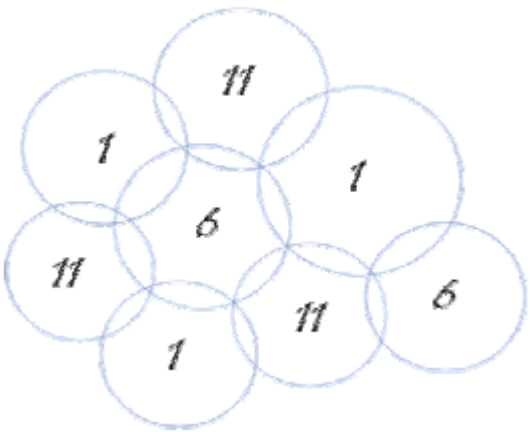
**Exercice 3**

Quelle est la méthode d'accès au support en 802.11 ?

Comparer avec celle pour Ethernet classique.
Donnez les 3 types de trames pour l'association au point d'accès et l'envoi de données. Faites un schéma décrivant l'établissement d'une connexion.

**Exercice 4**

Si on veut déployer le WIFI au sein de l'IUT pour qu'il couvre tout le campus, à quoi doit-on faire absolument attention ? Quels sont les canaux à utiliser ? Faites un schéma des zones de recouvrement.



## Exercice 1

Voici quelques types de réseau sans fils :

| Type de réseau | Normalisation | Portée maximale |
|---|---|---|
| WAN | GSM, GPRS, UMTS, LTE | Grandes zones géographiques (plusieurs dizaines de kilomètres) |
| MAN | 802.16- WiMax | 30km |
| LAN | 802.11, HiperLan1/2, HomeRF | 100m |
| PAN | 802.15 Bluetooth,Infrarouge | 10m |

## Exercice 2

| Type | Bandes de fréquence | Débit maximal | Portée maximale à l'intérieur |
|---|---|---|---|
| 802.11a | 5GHz | 54Mbit/s | 35m |
| 802.11b | 2,4GHz | 11Mbit/s | 35m |
| 802.11g | 2,4GHz | 54Mbit/s | 38m |

Le débit théorique se calcule en intérieur et dans le meilleur environnement, sans obstacle. Le débit réel est donc forcément plus faible.

On peut observer deux modes de fonctionnement sur la couche physique, par étalement de spectre, FHSS et DSSS :

- FHSS divise l'onde en sauts. Il y a alors 75 sous-canaux de 1MHz chacun. Les sous-canaux ont une durée de vie de 400ms. Ce mode est efficace pour lutter contre les interférences radio et pour optimiser l'usage de la bande passante.
- DSSS diviser la bande ISM en 14 canaux. Il envoie lui toutes les informations sur le même canal. Ces dernière sont alors converties en Chipping Code. Ce mode est plus efficace pour éviter les erreurs et pour éviter une limitation du débit.

Les appareils sont alors mis en relation selon deux types d'architecture:

- Basic Service Set (BSS) : le réseau est centralisé grâce à un Acces Point (AP)
- Independant Basic Service Set (IBSS) ou Ad Hoc : chaque machine est interconnectée, sans passer par un AP

## Exercice 3

En 802.11, l’accès au support peut se faire en PCF (Point Coordination Function) en mode AP ou en DCF (Distribued Coordination Function) en mode Ad Hoc ou AP. On

remarque que le mode DCF est basé sur le mode CSMA/CA, ressemblant au CSMA/CD d'Ethernet. En effet, CSMA/CD permet à une machine de s'assurer qu'aucune information ne soit en transit sur le câble pour éviter la collision. Pour 802.11, CSMA/CA permet d'assurer à un émetteur qu'il n'y ait pas d'autre station et donc que le canal soit libre également, pour éviter les collisions.

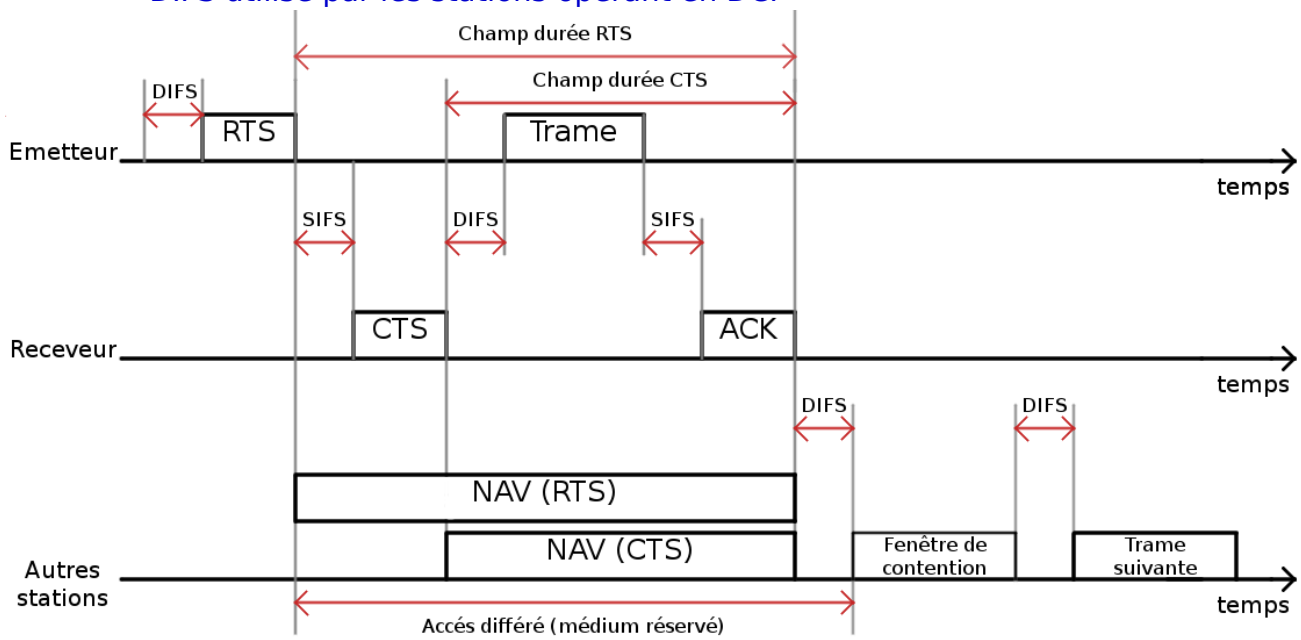
DCF vérifie que le canal soit libre. Si il l'est, alors il indique qu'il va envoyer des données (RTS) et demande à qui il doit l'envoyer (CTS). Puis il envoyé les données (DATA), avec pour intervalle les SIFS, et ce en attendant l'ACK.

Il y a trois types de trames MAC : les trames de données, de gestion et de contrôle accès médium. Les trames de contrôle accès médium se répartissent donc en :

- RTS (Request To Send)
- CTS (Clear To Send)
- ACK (ACKnoledgement).

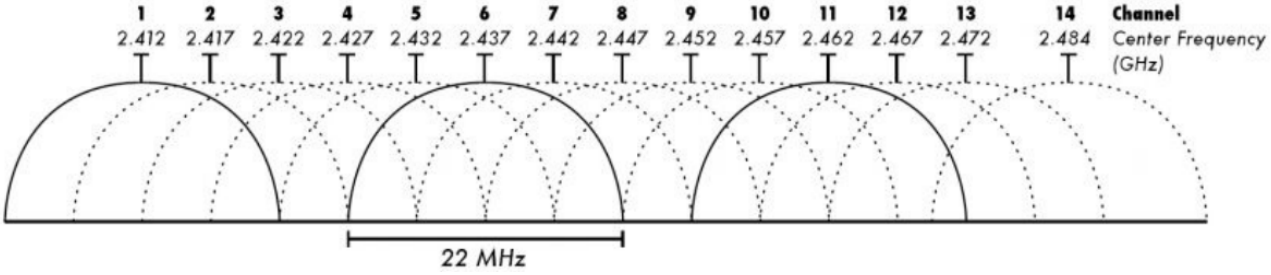
Voici un schéma avec :

- des NAV (Network Allocation Vector)
- IFS (Inter Frame Space) :
  - Short IFS (SIFS) qui est utilisé par les trames prioritaires comme CTS et ACK
  - DIFS utilisé par les stations opérant en DCF




## Exercice 4

Si on veut déployer le Wi-Fi sur un IUT, il faut éviter que deux points d'accès qui utilisent les mêmes canaux soient proches et recouvrent un même espace. Il y a 14 canaux à utiliser de 22MHz chacun. Voici le schéma de recouvrement des zones du cours ci-dessous. On peut y voir que l'écart entre chaque canal est de 5 MHz :




**Exercice 5 : Analyseur de réseaux Wifi avec Metageek Inssider**

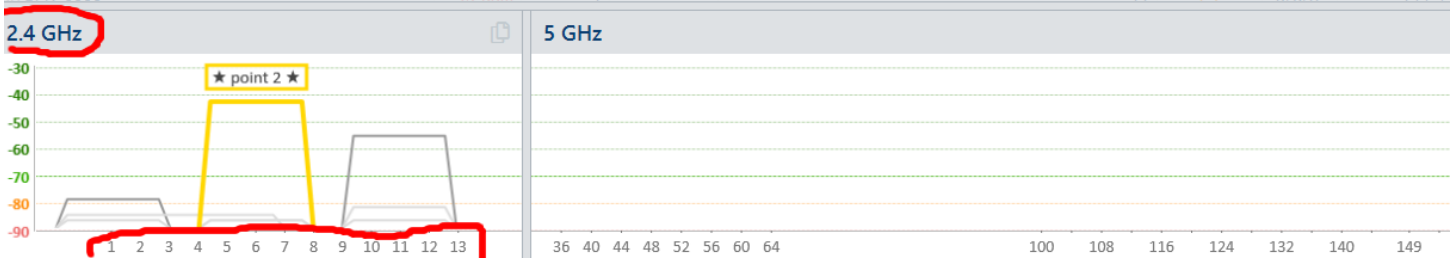
Télécharger et installer le logiciel Inssider ; https://www.metageek.com/products/inssider/

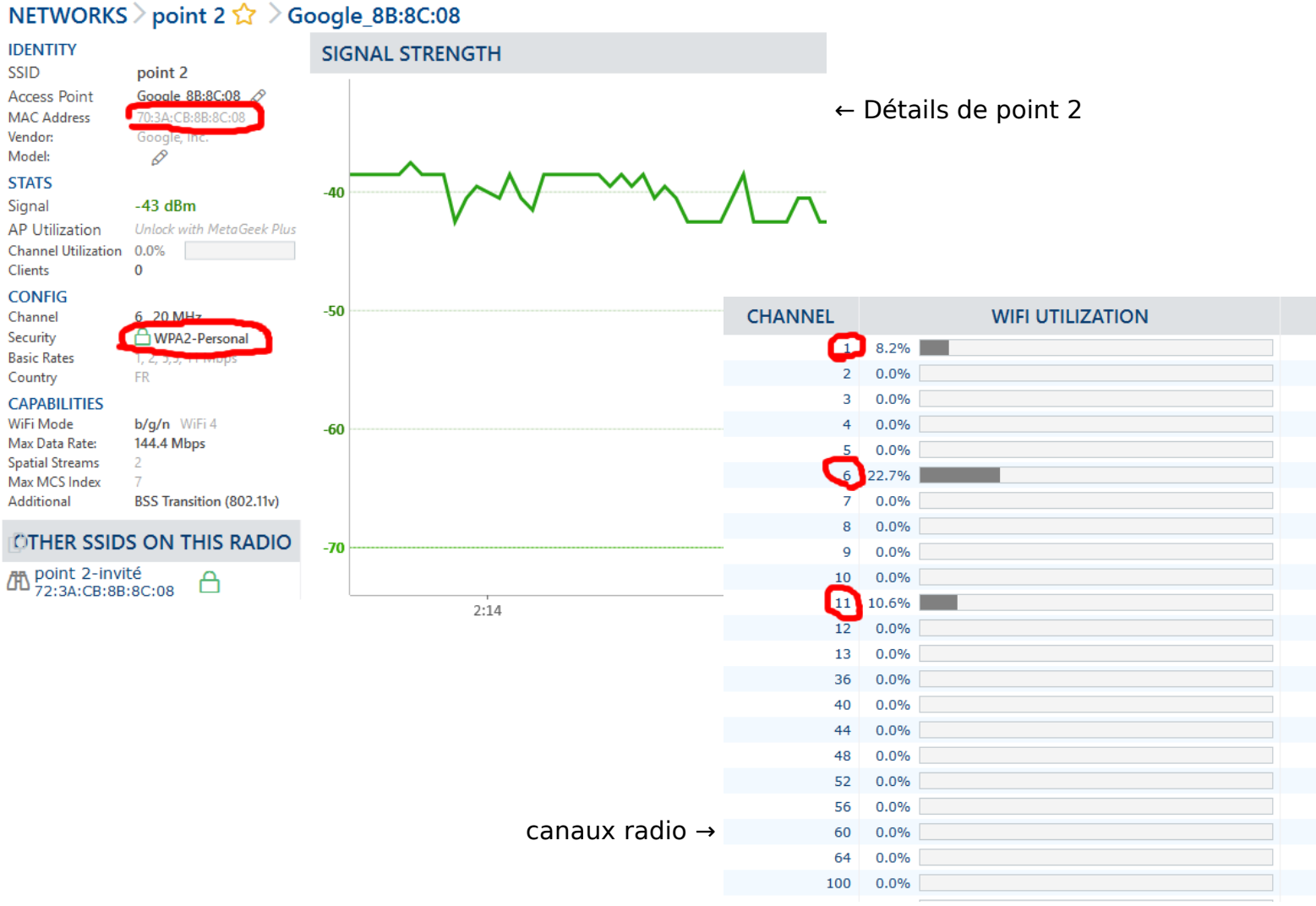
a. Identifier dans l'onglet NETWORK les informations suivantes pour votre réseau WIFI et le point d'accès Wifi DESCARTES ou DESCARTESPRO : mon Wi-Fi a pour SSID « point 2 »
   - Bandes de fréquences où opèrent les AP : 2,4 GHz
   - La puissance d'émission : environ -43 dBm
   - Les canaux utilisés : le 6 pour mon WIFI (il y a des canaux disponibles de 1 à 13)
   - Le mode de sécurité : WPA2 Personal
   - Le débit maximum : 144.4 Mbps
   - L'adresse MAC du AP : 70:3A:CB:8B:8C:08

b. Identifier dans l'onglet CHANNEL le canal radio le plus utilisé par votre AP. Les canaux radio 1, 6 et 11 sont utilisés par mon AP.

Voici toutes les captures d'écran associées à l'exercice :

| SSID | SIGNAL | RADIOS | CLIENTS | CHANNELS | SECURITY | MODE | MAX RATE |
|---|---|---|---|---|---|---|---|
| point 2-invité | -42 dBm | 1 | - | 6 | | b/g/n | 144.4 |
| point 2 | -43 dBm | 1 | - | 6 | | b/g/n | 144.4 |
| point 1-invité | -55 dBm | 1 | - | 11 | | b/g/n | 144.4 |
| point 1 | -57 dBm | 1 | - | 11 | | b/g/n | 144.4 |
| orange | -79 dBm | 2 | - | 1, 6 | | b/g/n | 144.4 |
| Livebox-ADE7 | -81 dBm | 1 | - | 1 | | b/g/n | 144.4 |
| DIRECT-J6M2070 Series | -82 dBm | 1 | - | 11 | | g | 54.0 |
| CPL_WIFI_1200_2.4G_91A360 | -85 dBm | 1 | 2 | 1+5 | | b/g/n | 300.0 |
| Bbox-A27DA968 | -87 dBm | 1 | - | 11 | | b/g/n | 144.4 |
| SFR_EF40_EXT | -87 dBm | 1 | - | 1 | | b/g/n | 144.4 |
| Livebox-F96A | -87 dBm | 1 | - | 6 | | b/g/n | 144.4 |
| SFR WiFi Mobile | -91 dBm | 3 | - | 1, 11 | | b/g/n | 144.4 |
| SFR_EF40 | -95 dBm | 1 | 3 | 1 | | b/g/n | 144.4 |
| SFR WiFi FON | -95 dBm | 2 | - | 1, 11 | | b/g/n | 144.4 |
| SFR_6000 | -95 dBm | 1 | - | 11 | | b/g/n | 144.4 |






**Exercice 6 : Configuration du filtrage des accès avec l'adresse MAC**

Vous devez avoir l'accès admin (root)pour la gestion de votre Point d'Accès Wifi pour réaliser cette exercice.

Le **filtrage d'adresses MAC** autorise uniquement les adresses MAC du client sans fil sélectionné à avoir accès à votre réseau. Les clients sans fil, à l'exception de ceux qui se trouvent dans la liste MAC, n'auront pas accès à votre réseau sans fil. On dit liste "**blanche**" pour une liste contenant des adresses MAC légitimes.

a. Depuis votre client, faites un ping vers le point d'accès (gateway ou box). Connectez vous à un site web sur Internet pour vérifier votre connectivité.

```
C:\Users\qguar>ping 192.168.1.1

Envoi d'une requête 'Ping'  192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

La connectivité fonctionne bien.

b. Sur l'interface d'administration de votre point d'accès, trouvez une solution pour interdire maintenant l'adresse Mac de votre portable. Décrire votre méthode.

Dans une premier temps, je récupère mon adresse MAC en cherchant l'adresse physique du Wi-Fi en tapant « ipconfig /all » dans l'invite de commande. Puis je me connecte à http://livebox/, l'interface d'administration de mon point d'accès. Je vais dans la rubrique « Mon Wi-Fi » puis sélectionne « Wi-Fi avancé » dans le menu. Dans le réseau « Wi-Fi 2,4 GHz », je clique sur « activer » dans la colonne « Filtrage MAC ». Je supprime mon adresse MAC si elle figure dans la liste.


Puis

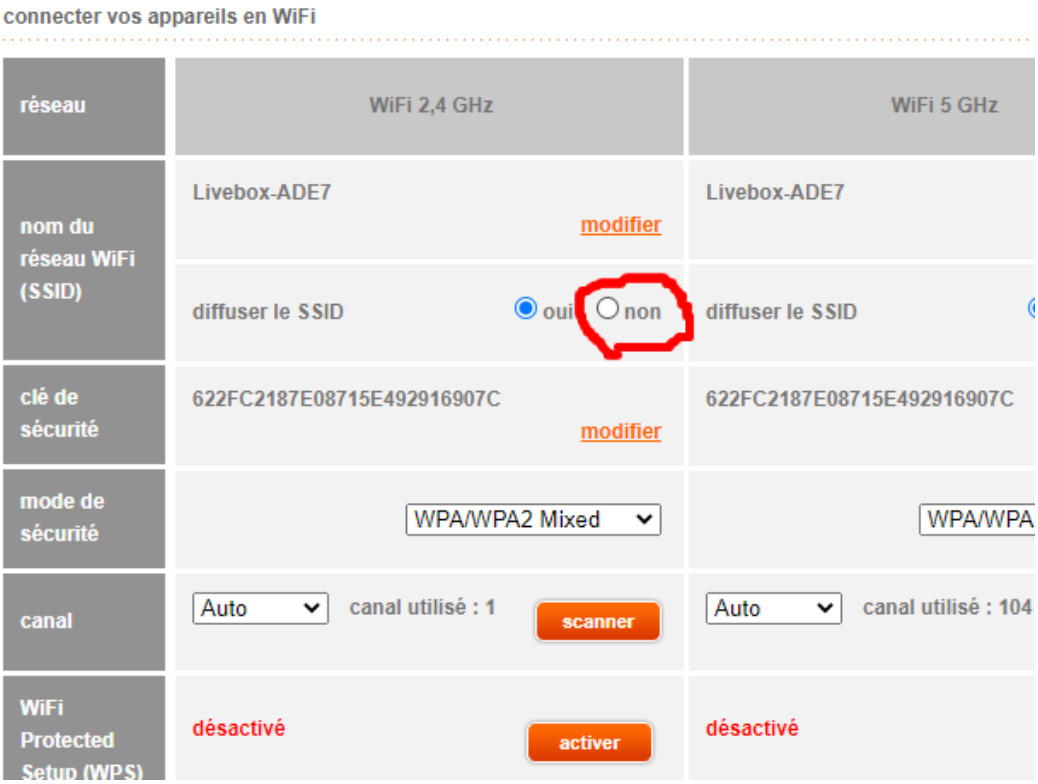

c. Supprimer cette configuration sur votre AP Wifi pour rétablir la connectivité de votre ordinateur à Internet.

Fait.

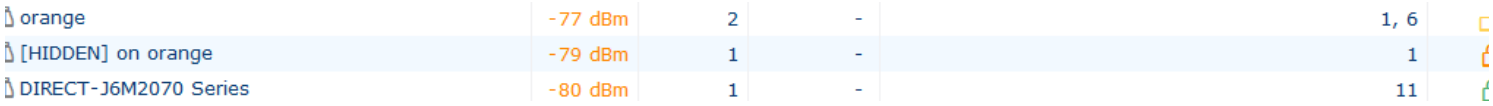
**Exercice 7 : Cacher le SSID**

Le SSID – Service Set IDentifier – est l'identifiant de votre WLAN. Lorsque vous souhaitez vous connecter à un WLAN, votre carte WiFI vous affiche différents WLAN qui sont dans les alentours. Le nom de chacun est appelé SSID. Et ce SSID est diffusé régulièrement dans les airs par la borne pour avertir sa présence. Ce SSID est contenu dans un message WiFi appelé un "Beacon" (ou "Balise" en français).

Sur certains bornes WiFi, vous avez la possibilité de cacher le SSID. Réaliser cette opération et vérifier sur votre PC ainsi que sur InSSIDer le résultat. Que constatez-vous sur vos écrans ?




Si j'arrête de diffuser le SSID, alors il n'est plus proposé à l'ordinateur lorsqu'il cherche un réseau. Cependant, le point d'accès apparaît toujours sur inSSIDer, avec la mention HIDDEN et le nom du FAI dans mon cas :




Si je cache mon SSID alors suis-je vraiment sécurisé ? Et bien pas du tout ! **Cacher son SSID** permet de cacher votre WLAN pour la majorité des personnes novices en WiFi. Mais en utilisant un sniffeur comme Wireshark, vous pouvez récupérer les trames échangées entre un client légitime et une borne d'accès. Et au sein de ces trames se trouve la valeur du SSID. Donc en cherchant un peu, vous trouverez très rapidement la valeur SSID du réseau qui se veut être invisible.

**Exercice 8 : Authentification Wifi avec 802.1x**

a. Qu'est-ce que 802.1x ?
C'est un standard mis au point par l'IEEE qui permet de sécuriser les réseaux, qu'ils soient sans fil ou par câble. Cela en contrôlant l'accès aux équipements d'infrastructure réseau.

b. Qu’est-ce que EAP ?
Un EAP (Extensible Authentication Protocol) est un protocole réseau qui comporte plusieurs méthode d'authentification sur les réseaux, filaires ou non. 801.1x utilise EAP.

c. Qu’est-ce que EAPOL ?
EAPOL (EAP Over Lan) est EAP utilisé sur un réseau LAN.

d. Pourquoi faut-il utiliser la technique du **tunneling** avec EAPOL en WIFI ?
Les données ne sont pas chiffrées avec EAPOL. En Wi-Fi, tout le monde peut les intercepter et lire en clair. Donc il faut utiliser un tunnel TLS afin que les données soient sécurisées.

e. Qu’est-ce que RADIUS ? Son utilité dans le processus d’authentification d’un client sur un réseau WIFI ?
RADIUS (Remote Authentification Dial-In User Service) est un serveur d'authentification, qui permet à un client d'identifier le réseau et vice-versa. Le point d’accès internet est l'intermédiaire entre le RADIUS et le client. RADIUS négocie avec le client la méthode de chiffrement avec EAP et est également utilisé par 802.1x.

f. Pourquoi TLS est-t-il intégré dans le processus d’Authentification
TLS permet d'assurer la sécurité par un certificat  venant du serveur. De plus, la confidentialité et l'intégrité sont assurées. C'est une méthode très sûre et utilisée.

g. Quels sont les problèmes associés lors de l’utilisation de certificats dans le processus d’authentification
Il est difficile d'attribuer les certificats. De plus, les utilisateurs sont plus familiarisés au principe d'identifiants que de certificats. Aussi, les certificats s'expirent donc le client doit le renouveler de temps en temps, ce qui modifie toute la chaîne de confiance.

h. Identifier et décrire la méthode d’authentification du client pour accéder au réseau WIFI DESCARTESPRO.
On peut vérifier avec inSSIDer, voire Wireshark. Sans pouvoir le faire, je peux deviner qu'il s'agit d'une authentification avec 802.1x et EAP et un chiffrement avec AES (WPA2 entreprise/802.11i)

**Exercice 9 : Chiffrement WIFI**

a. Quelles sont les différences entre WPA et WPA2 en termes de chiffrement et de gestion des clés ?
WPA chiffre avec TKIP. TKIP utilise l'algorithme RC4 pour chiffrer et permet une génération aléatoire de clés, avec une clé régulièrement modifiée au cours de la connexion. Les clés sont pré-partagées en mode personnel, et sont privées en mode entreprise. WPA2 reprend le même principe, mais en chiffrant avec AES-CCMP à la place de RC4 et TKIP.

b. Le mode de chiffrement adopté par WPA est TKIP. Quelles sont ses caractéristiques ?
TKIP utilise le chiffrement en continu RC4, en dérivant régulièrement la clé à partir de la clé principale. La clé est concaténée avec un vecteur d'initialisation. Les vecteurs d'initialisation sont hachés. Chaque paquet est chiffré avec une nouvelle clé. Il y a également un code permettant d'assurer l'intégrité du message, le MIC.

c. Le mode de chiffrement adopté par WPA2 est AES-CCMP. Quelles sont ses caractéristiques ?
Les paquets sont chiffrés par bloc de 128bits avec AES puis subissent un XOR avec les 128 bits suivantes. Ainsi de suite jusqu'à tout chiffrer. On extrait les 64 bits de poids forts du bloc chiffré pour obtenir le MIC.

d. Quelles sont les différences entre le chiffrement TKIP et AES-CCMP ? Lequel est le plus performant ? Complexe à déployer ?
WPA est une solution temporaire qui a suivi le cassage de WEP. WPA2 est bien plus optimal. Le chiffrement d'AES-CCMP est bien plus sûr et performant que celui de RC4 et TKIP.

e. Arrivée en 2018, qu'apporte WPA3 par rapport à WPA2 en termes de chiffrement et gestion des clés ?
WPA3 est bien plus sûr. Il ajoute un chiffrement sur 192 bits. Il chiffre avec AES-256 (et non plus 128) en mode Galois/counter Mode (GCM et non plus CCMP) avec SHA-384 en tant que HMAC.

f. Ordonner ces modes de sécurité WIFI du moins robuste au plus robuste :
   - Réseau ouvert (pas de sécurité du tout)
   - WEP-64
   - WEP-128
   - WPA-PSK + TKIP
   - WPA2-PSK + TKIP
   - WPA-PSK + AES
   - WPA2-PSK + AES

**Exercice 10 : Attaques sur les réseaux WIFI et contre-mesures**

Il existe aussi des attaques qui impacte le Wifi, non pas dans le sens **vol de données** et **pénétration** dans le réseau mais plutôt dans le sens de la **disponibilité** du service.

a. Quelles sont les différentes attaques de déni de service (DoS) courantes sur les réseaux Wifi ? Veuillez en citer 4 en précisant les vulnérabilités exploitées. Voir le document :
https://www.cisco.com/c/en/us/td/docs/wireless/prime_infrastructure/1-3/configuration/guide/pi_13_cg/wips_ench.html

Association Flood : Des utilisateurs malveillants se font passer pour de nombreux clients sur un réseau en cas d'open authentification. Ainsi, la table contenant les associations clients est vite saturée, et les vrais clients ne peuvent plus se connecter. Le point d'accès est hors-service.

EAPOL Start-Attack : Dans un serveur LAN avec EAP, un nouveau client commence l'association au point d'accès avec une trame indiquant le début de l'échange. Alors, des attaquants peuvent inonder le point d'accès de ces trames afin de le rendre hors-service.

PS Poll Flood : Dans le réseau sans fil LAN, un client peut se mettre en veille. Dans ce cas, le point d'accès stocke les trames dans un tampon, afin de les lui envoyer quand il sera réveillé. Pour demander les trames stockées, le client envoie au point d'accès un trame PS Poll. Cependant, si un utilisateur malveillant usurpe l'adresse MAC du client endormi, alors il peut faire envoyer les trames stockées au client, qui n'est pas en mesure de les recevoir.

Authentification-Failure Attack : l'attaquant usurpe l'identité d'un vrai client, afin d'envoyer des trames de requête d'authentification invalides. Ainsi, le vrai client est déconnecté par le point d'accès.

b. Qu'est-ce que l'attaque « Evil Twin », ou jumeau maléfique ?
Dans un réseau sans fil, le point d'accès internet est désactivé par une attaque DoS. Le pirate crée alors un point d'accès usurpant l'identité du point d'accès original. C'est le « jumeau maléfique ». Les clients se connectent dessus en pensant se reconnecter au point d'accès original. Ainsi, ils entrent leurs informations personnelles.

c. Le standard 802.11i intègre des mécanismes de protection contre les attaques extérieures visant à faire tomber l'infrastructure Wifi. Ces mécanismes sont appelés W-IDS pour **Wireless Intrusion Detection System**. Sélectionner dans la liste ci-dessous les actions de détection et de prévention réalisées par ces W-IDS : **en gras et bleu les réponses sélectionnées**
    1. **Détecter les bornes pirate qui se font passer pour une borne légitime**
    2. **Détecter les demandes excessives d'association de client sur une borne d'accès.**
    3. **Détecter les attaques MITM – Man In The Middle dont la philosophie est pour le pirate d'être au milieu d'une communication entre un client légitime et la borne d'accès**
    4. **Détecter l'usurpation d'adresse MAC**
    5. **Détecter les dénis de service contre les bornes d'accès (voir liste de la question 10.a ci-dessus)**
    6. **Mettre en liste noire (blacklist) l'adresse MAC d'un client pirate**
    7. **Réduire la couverture Wifi pour interdire que les voisins voient le réseau Wifi**