

IUT DE COLMAR

R301

ANNÉE 2022-23

Réseaux de campus

MARTIN BAUMGAERTNER

5 septembre 2022

Table des matières

1	CM 1 - 5 septembre 2022	2
1.1	Les technologies sans fils	2
1.2	Organisme régulateurs	2
1.3	Portée du signal	3
1.4	Rappel collisions et intrerférences	3
1.5	Bande ISM	3
1.6	Les topologies de base	3
1.7	Mode infrasctucture	4
1.8	Mode répéteur (repeaters)	4
1.9	Sécuriser son réseau	4
1.10	Pirater son réseau	4

1 CM 1 - 5 septembre 2022

1.1 Les technologies sans fils

- WPAN (Wireless Personal Area Network) : réseau sans fil de petite portée (10m) entre des appareils mobiles (téléphones, ordinateurs portables, etc.). Exemples : Bluetooth, ZigBee, etc.
- WMAN (Wireless Metropolitan Area Network) : réseau sans fil de moyenne portée (1km) entre des appareils mobiles (téléphones, ordinateurs portables, etc.). Exemples : Wi-Fi, WiMax, etc.
- WLAN (Wireless Local Area Network) : réseau sans fil de grande portée (10km) entre des appareils mobiles (téléphones, ordinateurs portables, etc.). Exemples : Wi-Fi, WiMax, etc.
- WAN (Wide Area Network) : réseau sans fil de très grande portée (100km) entre des appareils mobiles (téléphones, ordinateurs portables, etc.). Exemples : Wi-Fi, WiMax, etc.

1.2 Organisme régulateurs

- Wifi alliance = consortium industriel qui possède la marque Wifi.
- IEE = Institute of Electrical and Electronics Engineers.

1.3 Portée du signal

- 2,4 GHz (802.11 b/g/n) : 70m en intérieur
- 5 GHz (802.11 n/ac/ax) : 35m en intérieur
- 6 GHz (802.11 be) : 30m en général

En gros, on peut retenir que quand la fréquence diminue, le débit diminue mais la portée augmente.

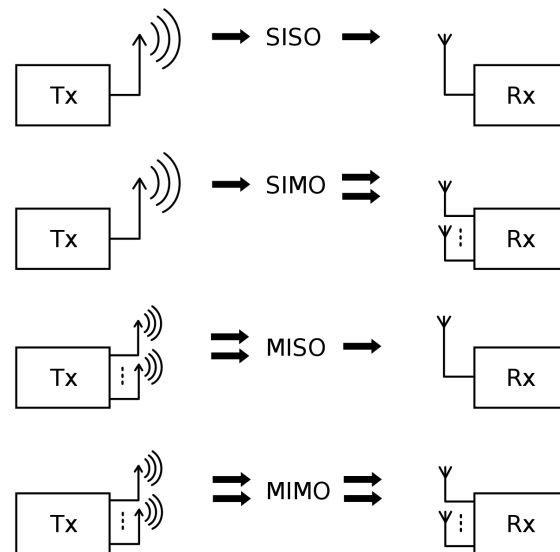


FIGURE 1 – Réception d'un signal

1.4 Rappel collisions et interférences

Collisions = sur un même canal gérées par un algorithme.

1.5 Bande ISM

Les canaux 12 et 13 sont quasi interdits aux USA sauf à faible puissance le 14 étant strictement interdit dans le pays.

1.6 Les topologies de base

Avec point d'accès = la borne n'est pas barrée
Sans point d'accès = la borne est barrée

1.7 Mode infrastucture

ESSID/SSID : nom du réseau

Un AP configuré dans ce mode va jouer le rôle de simple carte WIFI, via le câble ethernet.

1.8 Mode répéteur (repeaters)

- Sert à étendre le réseau dans des zones d'ombres
- Débit divisé par 2
- Risque de collision élevé car c'est sur la même fréquence

1.9 Sécuriser son réseau

- WEP : Wired Equivalent Privacy (déjà obsolète), très facile à pirater
- WPA : Wi-Fi Protected Access, plus sécurisé que WEP, solution transitoire
- conçue avant la finalisation de la norme 801.11i
- WPA2 : Wi-Fi Protected Access 2, plus sécurisé que WPA, respecte a norme 802.11i et imposee le protocole de gestion de cle CCMP
- WPA3 : Wi-Fi Protected Access 3, plus sécurisé que WPA2, introduit en 2018
- WPA Personal : WPA avec une seule clé partagée par tous les utilisateurs, conçue pour les petits réseaux
- WPA entreprise : WPA avec une clé différente pour chaque utilisateur, conçue pour les grands réseaux d'entreprise

Voici quelques solution pour sécurer son réseau :

- Cacher le SSID
- Filtrer adresses MAC
- Utiliser le WPA3

1.10 Pirater son réseau

- Utiliser Macchanger pour changer adresse MAC
- utiliser airodump-ng pour les stations disponibles
- utiliser aireplay-ng pour envoyer une trame de déconnexion d'une station connectéé, qui va alors tenter de se reconnecter automatiquement
- Utiliser AirCrack-ng avec un fichier adéquat