Sécurité de niveau 2 &
Réseaux locaux sans fil

Sécurité de niveau 2

- Si un attaquant peut recevoir des paquets dans un réseau local, qui ne lui sont pas destinés, il est en mesure de récupérer de nombreuses informations (sur les couches 2, 3 et 4, et éventuellement applicative si cette partie n'est pas chiffrée)
- Deux attaques ont été réalisées en TP
  - Si l'attaquant peut configurer les équipements d'un LAN, il peut rediriger tout le trafic transitant dans le LAN vers une interface qu'il peut écouter
    - grâce à la technique de port-mirroring
  - Attaque par inondation de la table d'adresses MAC d'un commutateur
    - les trames dont l'@MAC destination n'est pas dans la table d'adresses MAC sont diffusées sur tous les ports (sauf le port entrant)
    - remplir la table d'adresses MAC d'adresses « bidon » pour empêcher le stockage des correspondances @Mac légitimes - num de port
- Politiques de sécurité de niveau 2
  - Sécuriser l'accès aux commutateurs pour empêcher les configuration malicieuses : mot de passe, chiffrement
  - Fermer tous les ports non utilisés
  - Activer la sécurité des ports actifs : par ex. limiter le nombre d'adresses MAC par port

Réseaux locaux sans fil

- C'est la technologie Wi-Fi qui est utilisée dans le scénario Packet Tracer qui était à étudier
- Dans ce scénario
  - 3 bandes de fréquences étaient possibles
    - une en 2,4 GHz et deux dans la bande des 5 GHz
  - Chaque bande est divisée en canaux
    - Canal = sous-bande de fréquence qui permet à deux équipements de communiquer en Wi-Fi
    - Canal peut être de 20 MHz ou 40 MHz
  - Capacité d'émission offerte est de 300 Mb/s
    - Plusieurs capacités d'émission sont possibles en Wi-Fi
    - Plus les capacités d'émission sont élevées, moins les transmissions sont robustes
  - Possible de sécuriser l'accès au réseau Wi-Fi avec une clé partagée