Notes - Théorie

"Vecteur de distance" vs "a état de lien"

Protocole	Type de protocole	Infos
RIP / EIGRP	A "vecteur de distance"	On fait confiance à ses voisins.
OSPF	A "état de lien"	On récupère toutes les informations possible sur le réseau et on construit sa propre base de donnée.

OSI

Couches	données transmises / utilisées	Infos
Application	Donnée	Fait le lien entre les processus réseaux et les applications
Présentation	Donnée	Représentation des données
Session	Donnée	Communication entre les hôtes
Transport	Segments	Assure le contrôle du transfert de bout en bout
Réseau	Paquet	Sa fonction principale est la sélection du chemin (routage)
Liaison de donnée	Trame	Elle gère l'accès au média
Physique	Bits	Détermine comments les éléments binaires sont transportés sur un support physique

Encapsulation

- Lorsque les données d'application descendent la pile de protocoles en vue de leur transmission sur le support réseau, différentes informations de protocole sont ajoutées à chaque niveau.

Couche 2

- Full duplex = Envois et réception simultanément possible
- Half duplex = Envois et réception simultanément PAS possible (l'un ou l'autre)
- CSMA/CD = Détection de collision (savoir quand on peut envoyer un msg quoi)
- LLC = Pilote de lacarte réseau. Logiciel qui interagit avec le matériel de la carte réseau.
- Sous-couche MAC a 2 fonctions :
    - Encapsuler les données
    - Contrôler l'accès au support
- FF:FF:FF:FF:FF:FF => Broadcast MAC
- 2 méthodes de transmission de trame sur un switch :
    - Store and Forward
        - Attends de recevoir la trame complète, vérifie son CRC(checksum quoi), si valide, va rechercher sur quelle interface envoyer la trame.
        - Voir ça comme TCP
    - Cut-through
        - Envois directement la trame à la cible, sans pour autant vérifier le CRC.
        - Voir ça comme UDP

ARP (Adress Resolution Protocol)

- Requete ARP
    - Je veux contacter 10.10.10.2 dans mon réseau. Je connais pas la MAC, donc j'envois un packet "who has (ip) tell (mon ip)" en broadcast
- Reponse ARP
    - Celui a qui l'ip est la sienne, va répondre "(ip) is at (mac)"

⚠️ Particularité si pas dans le même réseau => On va demander la MAC de la passerelle, puis lui envoyer notre packet.

IPv6 :

- FF02::1 = Je parle IPv6
- FF02::2 = Je suis un routeur (donc permet de contacter les routeurs)

Routage :

- AD (Distance administrative) permet à un routeur qui fait du routage OSPF et RIP de choisir une ou l'autre distance.
- PK ? Car métrique pour RIP=nbr de saut et métique pour OSPF= Bande passante

MAC Adress flooding

- La table des address MAC d'un switch (CAM) est limité.
- Si un pirate inonde d'adresse MAC le switch jusqu'à ce que la table du switch soit saturée, le switch va passer en mode fail-open (envoit partout)

DHCP snooping

- Avoir 2ème serveur DHCP qui va répondre au discover.
- Système de port "trusted" et "untrusted" sur le switch

DHCP starvation attack (ou DHCP flooding)

- Remplir le pool dhcp avec pleins de discover afin qu'il ne puisse plus proposer d'ip.