Réseau avancé et virtualisation

2. Réseau - VLAN

VLAN

- VLAN = *Virtual LAN*
  - Séparation d'un réseau physique en différents domaines de *broadcast* (niveau 2 de la couche OSI)
  - Créé pour la performance initialement (dans le prolongement du gain concentrateurs => commutateurs qui s'occupe des trames normales, l'objectif était ensuite de réduire les domaines de *broadcast* de la méthode d'accès)
  - Se fait via des *switchs* ou des routeurs
- Mécanisme de séparation
  - Par port
  - Par adresse source (MAC ou IP)
  - Par marquage *(tagging)* des paquets : 802.1Q (appelé *dot1q*)
    - Ajout d'un champ de 32 bits entre l'adresse MAC source et le champ type (Ethernet 2) / longueur (802.3)
    - Rappel : fusion de ces deux standards en 1997 en 802.3x

VLAN

- *Tagging*
  - TPID = *tag protocol ID* = 16 bits = 0x8100 pour les trames marquées
  - TCID = *tag control ID* = 16 bits
    - PCP = *priority code point* = 3 bits : équivalent à la priorité du traffic
    - DE = *drop eligible* = 1 bit = peut-on détruire ces trames ?
    - VID = *VLAN identifier* = 12 bits = indique à quel VLAN la trame appartient
- Remarque sur les VID
  - 0x000 et 0xFFF sont réservés
  - 0x001 est souvent utilisé pour un VLAN de maintenance
- Double *tagging*
  - Permet aux FAI d'utiliser un VLAN en interne, sur des traffics qui sont déjà marqués (ajoute un champ supplémentaire au niveau MAC)

VLAN

- Multiplexage = *trunk*
  - Un *trunk* est un câble par lequel plusieurs VLAN différents passent
- Définitions
  - VLAN natif = VLAN par défaut
  - Trames natives = trames destinées au VLAN natif
  - *Port trunk* = port qui envoie et reçoit les trames marquées sur tous les VLAN, sauf sur le VLAN natif
    - En fait, ce sont les seuls ports qui ajoutent les tags
- Fonctionnement
  - Les trames pour le VLAN natif ne sont pas marquées
  - Si une trame non marquée est reçue sur un port trunk, on la marque avec le VLAN natif
  - Si une trame est marquée, elle est envoyée normalement pour son VLAN

VLAN

- Avantages
  - Simplifier la gestion
  - Séparer les flux
  - Optimiser la bande passante (en réduisant le domaine de *broadcast*)
  - Sécurité (logique)
- Remarques
  - On peut attribuer le VLAN en fonction du protocole source

VLAN

- Remarques
  - *Private* VLAN = on interdit aux *switchs* de communiquer autrement que par le uplink, et on place une entité qui contrôle
    - Exemple : hôtel
  - VPN = *Virtual Private Network*
    - Plusieurs entités distantes connectées par un tunnel au travers d'un réseau (alors qu'un VLAN est un LAN)
    - Protocole de *tunneling*, sécurité (confidentialité + authentification, IPSec + SSL/TLS + SSH)

VLAN

- Avant la configuration d'un VLAN
  - Soit VLAN désactivé
  - soit VLAN activé avec un VLAN par défaut qui contient tous les ports : chaque équipement d'un port peut envoyer un paquet sur tous les autres ports
- Configuration d'un nouveau VLAN (VLAN 2)
  - Enlever du VLAN par défaut les ports concernés par le VLAN 2
  - Si un seul équipement utilise le VLAN
    - Pas besoin de tagger, juste de forwarder sur le bon port
  - Si plusieurs équipements utilisent le VLAN
    - Il faut tagger les ports concernés
    - La plupart des VLAN doivent inclure les ports uplinks (reliant les switchs entre eux) pour que la communication entre switchs se fasse bien
    - Les tags ne sont pas forcément maintenus tout au long du réseau
- Remarque
  - Toujours garder un VLAN d'administration, pour éviter que l'admin perde la connectivité (nécessiterait une réinitialisation des paramètres de base du switch)

VLAN

- Exemple sur d'anciens routeurs Cisco
  - Activation
    - switchport trunk encapsulation dot1q
- Exemple sur Linux : outils vconfig et iproute
  - vconfig add eth0 *vid*
  - iproute link add link eth0 eth0.*vid* type vlan id *vid*
  - vconfig rem eth0.*vid*
  - iproute link delete eth0.*vid*
  - tcpdump -i eth0 -v *vid*