UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Les Virtual LAN

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Les Virtual LAN

Introduction

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Les Réseaux Locaux Virtuels (VLAN)

- Avantages des LAN
  - Communication rapide, broadcasts
- Problèmes des LAN
  - Sécurité, broadcast storms, connectique
- Objectifs des VLAN
  - Avoir des fonctions de la couche 3 avec la vitesse de la couche 2
  - Faciliter la gestion de la mobilité des postes
  - Supprimer la possibilité de communication entre certaines parties du réseau, sécurisé des domaines
  - Conserver la compatibilité ascendante

Avantages des VLAN

- Segmentation du réseau local flexible
  - Regrouper les utilisateurs / ressources qui communiquent le plus fréquemment indépendamment de leur emplacement
- Organisation virtuelle, gestion simple des ressources
  - Modifications logiques ou géographiques facilitées et gérées via une console d'administration plutôt que changer des câbles dans une armoire de brassage
- Efficacité de bande passante / utilisation des serveurs
  - Limiter l'effet des inondations de broadcasts
  - Partage possible d'une même ressource par plusieurs VLAN
- Sécurité du réseau améliorée
  - Un VLAN est une frontière virtuelle, franchissable avec un routeur

Définitions

- Un réseau local (LAN)
  - est défini par un domaine de diffusion
  - Limité par des équipements fonctionnant au niveau 3 du modèle OSI : la couche réseau
- Un **réseau local virtuel** (VLAN) est un **LAN distribué** sur des équipements fonctionnant au **niveau 2** du modèle OSI : la couche liaison (Ethernet)
- A priori, nous n'avons plus besoin d'avoir recours à un équipement de niveau 3 pour délimiter le LAN
- Les VLANs peuvent être définis en fonction
  - Du protocole de niveau 3 utilisé dans le réseau
  - Des groupes de personnes, département ou service
  - De sécurités différentes nécessaires sur certaines ressources
  - Des applications utilisées sur le réseau

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Les Virtual LAN

Les implémentations

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Les VLANs End-to-End

- Les utilisateurs sont regroupés dans des VLAN en fonction de leur rôle au sein de l'entreprise
- L'utilisateur conserve les mêmes droits, quelque soit le port du switch sur lequel il est connecté
- Implémentation typiquement choisi pour des raisons de sécurité ou de nécessité pour certaines applications
- Difficile à mettre en place et à débugger !

Les VLANs locaux

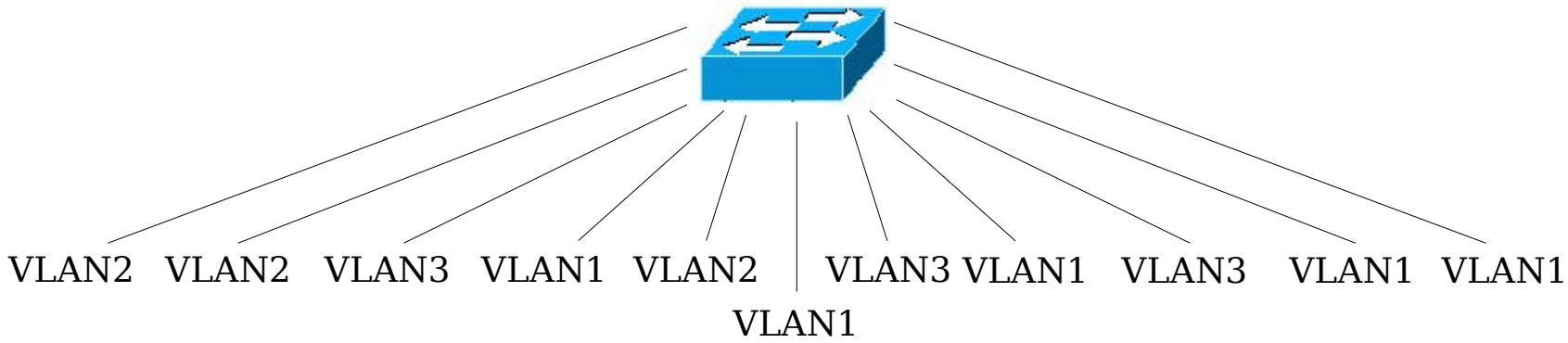
- Problème du VLAN End-to-End : difficile à administrer, des utilisateurs avec les mêmes droits sont réparties sur de nombreux switchs
- Les VLANs locaux sont basés sur la position géographique de chaque utilisateur, en respectant la hiérarchisation du réseau : coeur de réseaux, distribution et accès réseau
- Pas de propagation d'un VLAN entre des switchs placés hiérarchiquement sur des niveaux différents
- Tentative du respect de la règle du 80/20 : 80% du trafic reste sur le VLAN local et 20% sort et donc passe par un équipement de niveau 3

Les Virtual LAN

Les solutions classiques

VLAN statique ou par ports

- Permet de faire une division d'un équipement de niveau 2 (un commutateur) en plusieurs domaines de diffusion
- Obligation de gérer manuellement sur chaque équipement la distribution des réseaux locaux
- Problème : une station ne peut pas changer de VLAN ou appartenir à plusieurs VLAN. Le commutateur assure une isolation complète entre la station et le VLAN auquel il appartient



Affectation d'un port

- Sur un switch Cisco, avec IOS :
  - Switch(config)# interface *fastethernet 0/3*
  - Switch(config-if)# switchport mode access
  - Switch(config-if)# switchport access vlan *number*
- Vérification de la configuration
  - Switch# show vlan
- Pour afficher les informations d'un port
  - Switch# show interface *type slot/num* switchport
- Pour afficher la table MAC d'un port
  - Switch# show mac-address-table

Les VLANs

Le mode Trunk

Principe

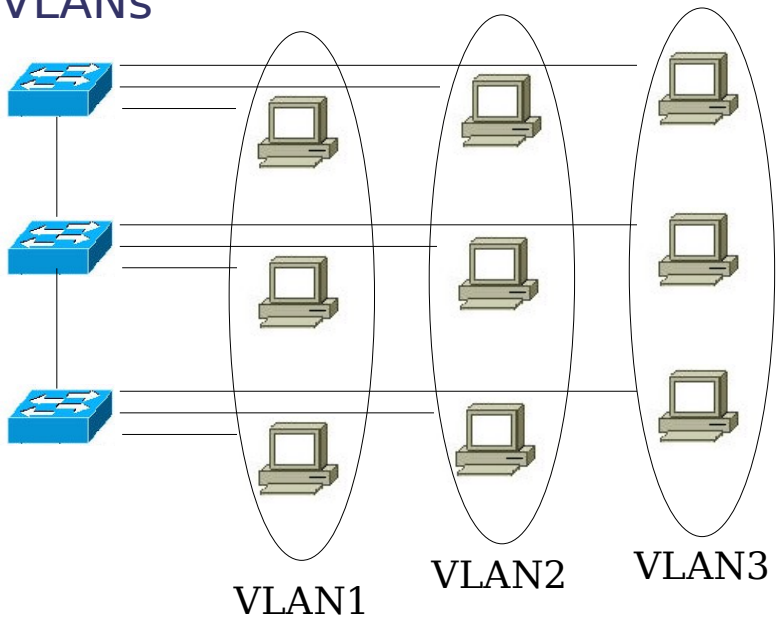
- Afin de pouvoir réaliser des VLANs, les switchs vont marquer les paquets Ethernet d'un VLAN ID
- Une trame Ethernet doit donc porter le bon VLAN ID pour être acheminer sur un port du switch configuré dans un VLAN
- Donc comment faire pour faire communiquer ces VLAN entre-eux ?
  - La solution est le trunk
  - C'est un port qui accepte de faire passer des trames Ethernet portant des VLAN ID différents
  - Ce port trunk appartient donc à plusieurs VLANs en même temps
  - Par défaut, un port trunk transporte le trafic de n'importe quel VLAN
- Si vous avez un serveur qui doit être accessible part plusieurs VLANs, son interface doit donc être en mesure de pouvoir être dans le mode trunk

VLAN type Cisco Inter-Switch Link (ISL VLAN)

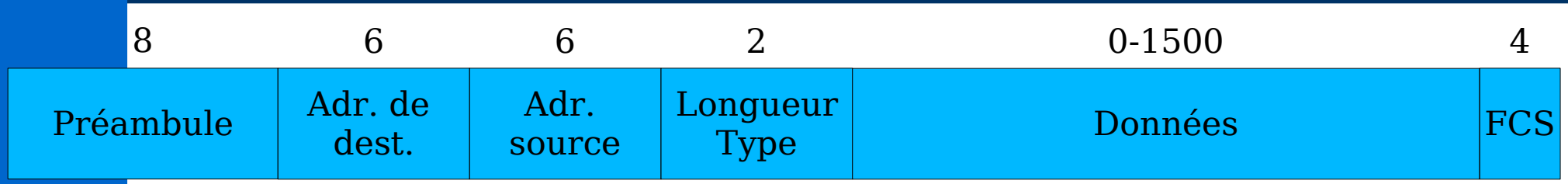
- Technique développée pour les équipements Cisco. Chaque trame Ethernet est encapsulée dans une trame ISL, d'en-tête 26 octets et d'en-queue 4 octets qui est un CRC
- Solution surtout utilisée dans le Voice over IP des équipements Cisco
- Fonctionne avec Ethernet et Token Ring
- Technique non compatible avec les standards IEEE 802.1Q
- Supporte jusque 1005 VLANs

VLAN IEEE 802.1Q

- Standard qui fournit un mécanisme d'encapsulation très répandu, implanté dans de nombreux équipements de marques différentes
- L'en-tête de la trame est complétée par une balise de 4 octets
- Supporte jusque 4095 VLANs



La trame Ethernet 802.3



- Le champ Type est remplacé par le champ longueur
- Pour éviter des problèmes de compatibilité, IEEE a décidé de considérer ce champ comme indiquant une longueur si la valeur est <= 1500 sinon c'est le type de données transportées

La trame IEEE 802.1Q

8	6	6	4	2	0-1500	4
Préambule	Adr. de dest.	Adr. source	802.1q	Longueur	Données	FCS

- 4 octets du 802.1q découpés de la façon suivante :
  - EtherType ou Tag Protocol IDentifier (TPID)
    - 12 bits utilisés pour identifier le protocole de la balise insérée. Pour une balise 802.1q, la valeur est fixée à 0x8100
  - Priority
    - 3 bits pour coder 8 niveaux de priorité. Aucun rapport avec les priorités sur IP. Uniquement pour mettre des priorités entre les trames de certains VLAN par rapport à d'autres
  - Canonical Format Identifier
    - 1 bit pour la compatibilité entre les adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe toujours cette valeur à 0. Si une trame avec la valeur 1 pour ce champ arrive, celle-ci ne sera pas propagée
  - VLAN Identifier
    - 12 bits qui permettent de définir l'appartenance de la trame à un VLAN, au maximum 4094 VLAN possibles

Le VLAN natif ?

- 802.1Q supporte le VLAN natif qui est le VLAN qui ne marque pas la trame
- Différent d'ISL qui marque toutes les trames, quelque soit le VLAN
- Par défaut, le VLAN natif est le VLAN 1
- Il est important que tous les matériels connectés au trunk doivent avec le même VLAN natif

VLAN service providers ?

- Supposons que vous aillez des VLANs à répartir entre sites distants, séparé par une ligne d'un provider
- Certains providers offrent du tunneling pour les trames 802.1Q
- Le provider ajoute dans ce cas son propre tag 802.1Q dans la trame (juste derrière source MAC)

Les Virtual LAN

VLAN Trunk Protocol

VLAN Trunk Protocol

- VTP est un protocole propriétaire Cisco qui permet de faire de la communication entre périphériques sur leurs ports trunk
- Il permet de propager la configuration des VLANs sur plusieurs matériels actifs
- Permet de simplifier la configuration des VLANs
- Un switch sera le maître et propagera la configuration à d'autres switchs

Le management domain

- Pour fonctionner, VTP nécessite la définition d'un management domain
- Ce domaine doit être identique sur tous les switchs qui devront partager des informations sur les VLANs
- Un switch n'appartient qu'à un seul VLAN
- Chaque switch supportant VTP multicaste périodiquement des informations aux autres switchs par leur port trunk. Ces informations comprennent le management domain, la version de VTP, les VLANs et leurs configurations
- Un switch peut être configurer dans 3 modes

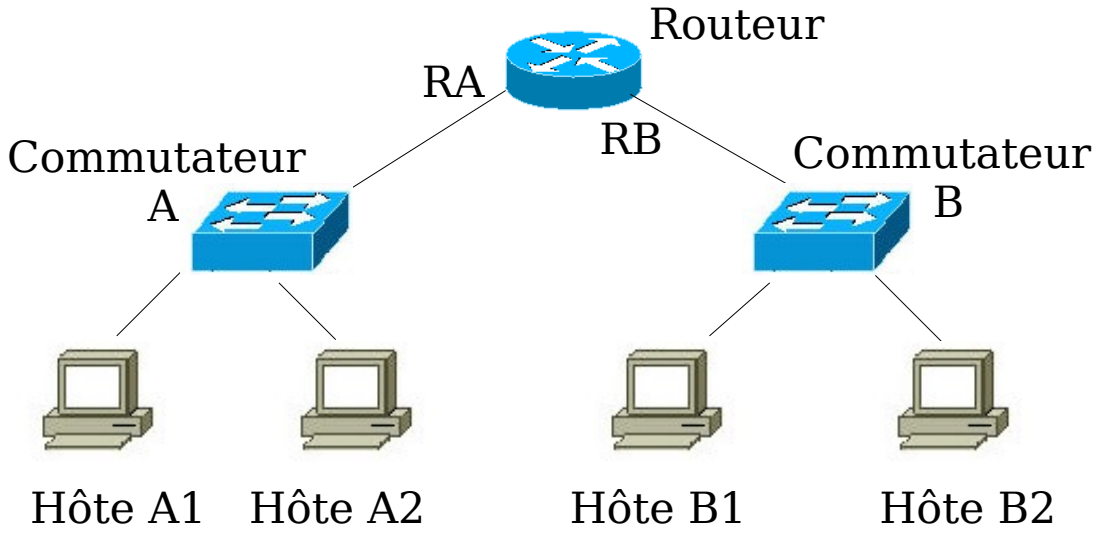
Les modes de VTP

- Les serveurs et les clients VTP propagent les configurations à travers les liens trunk aux autres switchs connectés et reçoivent les mises à jour également par les liens trunk
- Les serveurs VTP sont responsables de la configuration des VLANs : création, suppression et changement. Ils stockent ces config en NVRAM
- Les clients VTP n'acceptent les changements que s'ils sont annoncés par un serveur VTP
- Le mode transparent permet aussi de configurer des VLANs, de sauvegarder la config. En NVRAM mais aucun message VTP n'est transmis aux autres switchs
  - C'est le mode de fonctionnement par défaut d'un switch.
  - Par contre il transmet les informations VTP qu'il peut voir passer

Les Virtual LAN

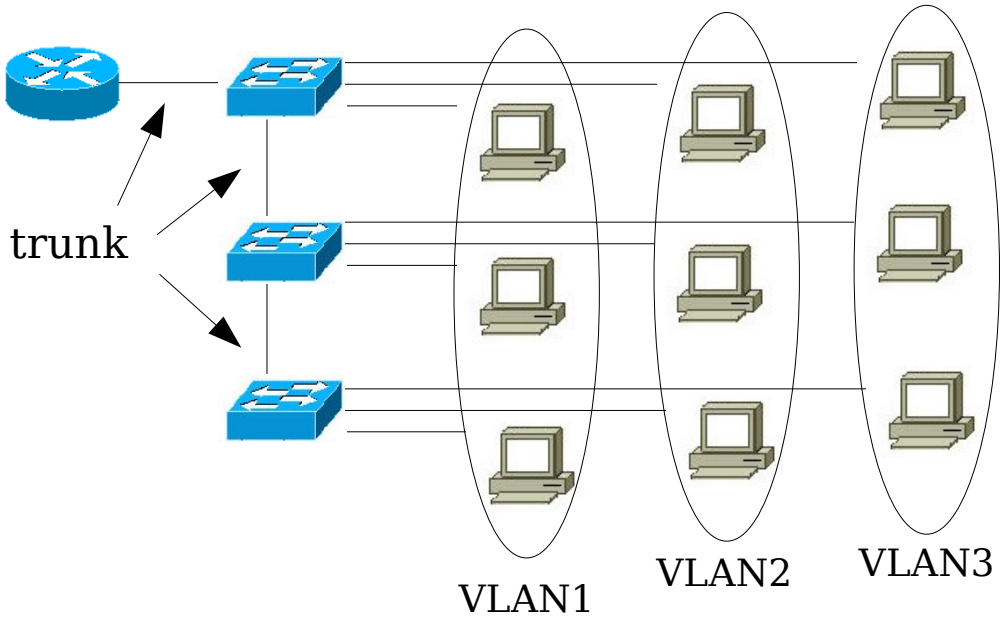
Le routage inter-VLAN

Sans le routage inter-VLAN



- Si le comm. A possède un VLAN pour A1 et un VLAN pour A2, A1 et A2 ne peuvent pas communiquer entre-eux. Si l'un d'entre-eux veut communiquer avec un autre VLAN, il faut que l'interface RA appartiennent aux 2 VLAN
- Si la machine A1 déménage dans un autre endroit !
  - Installation d'un nouveau switch et connecter celui-ci vers le VLAN A1

Avec le routage inter-VLAN



- Le contrôle d'accès est centralisé au niveau du routeur
- Gestion optimisée des ports de commutation. Tous les VLAN peuvent être accessible sur n'importe quel port. L'administration est donc concentré sur un nombre minimum de matériel, contrairement à la solution sans routage inter-VLAN

Utilisation des trunks

- Les trunk peuvent être utilisés
  - Entre 2 commutateurs
    - C'est le mode de distribution des réseaux locaux le plus courant
  - Entre un commutateur et un hôte
    - Si un hôte supporte le trunking, il a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels
  - Entre un commutateur et un routeur
    - Permet d'accéder aux fonctionnalités de routage entre des VLAN