1 Introduction

Les réseaux Ethernet sont sujets à divers problèmes affectant les performances du réseau, à savoir :

- Les collisions
- La latence des équipements réseaux
- La remise de données de type broadcast

Afin d'optimiser les performances du réseau, la segmentation est nécessaire.
Le but de la segmentation (subnetting) sur un LAN est d'obtenir une réduction de la taille des domaines de collision afin d'économiser la bande passante disponible, ou de la taille des domaines de diffusion afin d'améliorer la sécurité et de diminuer la taille des réseaux.

Il est possible de recourir à trois types de segmentation des domaines de collisions :

- **Segmentation par pon**t :

Segmentation du domaine de collision en 2 grâce au pont, dispositif de couche 2 permettant un filtrage des trames en fonction des adresses MAC des hôtes.

- **Segmentation par routeurs** :

Segmentation du domaine de broadcast en fonction des adresses réseau de couche 3.

- **Segmentation par commutateur** :

Segmentation du domaine de collision par la mise en place de chemins commutés entre l'hôte émetteur et le destinataire (micro segmentation)

2 Le commutateur

2.1 Présentation

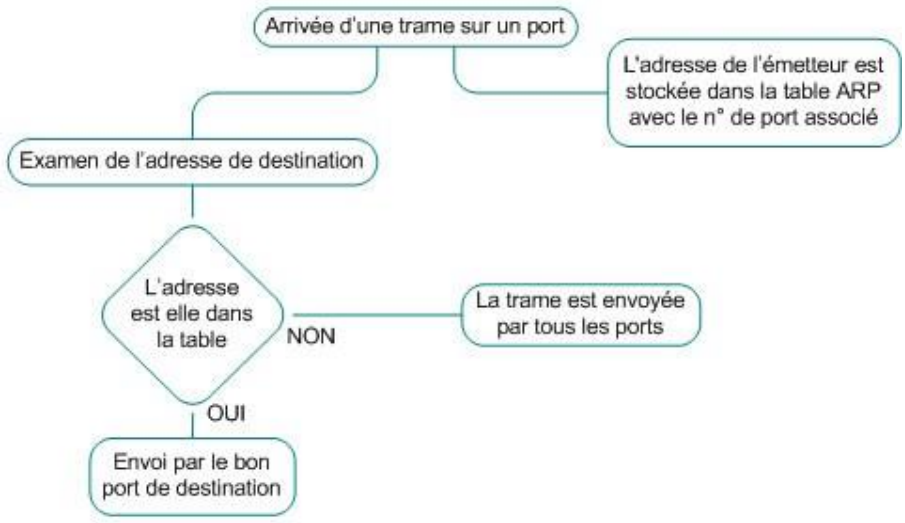
Le commutateur est un pont multi-ports. Il permet de relier plusieurs segments réseau et d'acheminer les trames sur le bon segment de destination grâce aux informations de couche 2.

Un environnement commuté présente les avantages suivants :

- Réduction du nombre de collisions
- Plusieurs communications simultanées
- Liaisons montantes haut débit
- Amélioration de la réponse du réseau
- Hausse de la productivité de l'utilisateur

Les décisions d'acheminements du commutateur sont basées sur les adresses MAC contenues dans les trames circulant sur le réseau :

Fonctionnement d'un commutateur



3 Les commutateurs de niveau 3

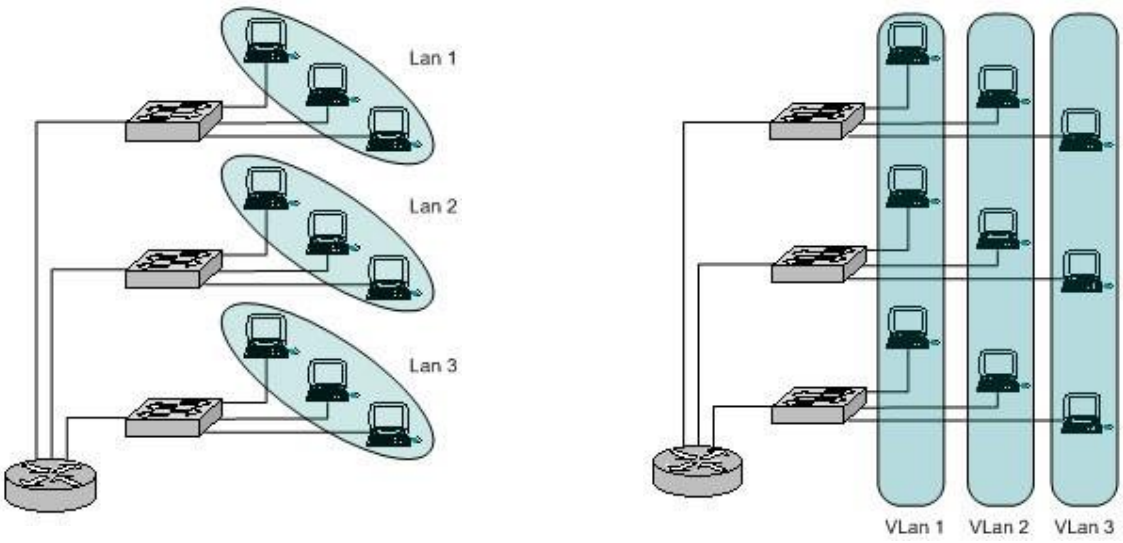
Les commutateurs de niveau 3 agissent au niveau IP. Ils permettent la création de VLAN (LAN Virtuels).

3.1 Principe des VLAN

Le principe des VLAN consiste à regrouper des machines dans un ou plusieurs segments quelque soit leur emplacement physique. En fait, cette technologie permet de créer des segments Ethernet logiques, indépendamment de l'implantation géographique.

Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusion gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce Vlan

Attention, la mise en place de VLAN nécessite l'utilisation d'équipements supportant cette technologie.



Segmentation traditionnelle a Segmentation avec VLAN

Les principales différences entre la commutation traditionnelle et les VLAN sont :

- Les VLAN fonctionnent au niveau des couches 2 et 3 du modèle OSI
- La communication inter VLAN est assurée par le routage de couche 3
- Les VLAN fournissent une méthode de contrôle des broadcasts
- Les VLAN permettent d'effectuer une segmentation selon certains critères
  - Des collègues travaillant dans le même service
  - Une équipe partageant le même applicatif
- Les VLAN peuvent assurer la sécurité des réseaux en définissant quels nœuds réseaux peuvent communiquer entre eux

Il est alors possible de segmenter le réseau en plusieurs domaines de broadcast afin d'en améliorer les performances.

La communication inter VLANS est assurée par des routeurs

3.2 Méthodes d'attribution des VLAN

chaque VLAN est identifié par un numéro qui l'identifie:
VLAN no 2, VLAN no 3 … (le no de VLAN étant codé sur 12 bits, on peut théoriquement créé 4096 VLAN).

Il existe différentes méthodes de gestion et de paramétrage

- **VLAN statiques** : ou dénommé VLAN par port :

Les ports du commutateur sont affectés à un VLAN

  - Facilité d'administration
  - Fonctionnent idéal dans les réseaux ou les déplacements sont rares et gérés

- **VLAN dynamiques** :

Les ports des commutateurs peuvent automatiquement déterminer leur VLAN d'appartenance.

Le filtrage peut être basé sur :

  - Les adresses MAC
  - L'adressage logique source (IP)
  - Le type de protocole des paquets de données

Cette dernière méthode est celle qui demande le moins d'administration au niveau du local technique et qui permet la migration des utilisateurs

3.3 Principes de fonctionnement des VLAN

On distingue 2 méthodes pour regrouper les utilisateurs en VLAN :

- **Le filtrage de trames**
  - Un examen de chaque trame permet d'élaborer pour chaque commutateur une table de filtrage afin de permettre de prendre les décisions appropriées.

- Cela suppose une table de filtrage par commutateurs, donc des temps de mise à jour lents ainsi que des problèmes d'évolutivité

- **L'identification des trames**
  - Chaque trame dispose d'un code d'identification VLAN (TCI = Tag Control Information) définit par la norme IEEE 802.1q

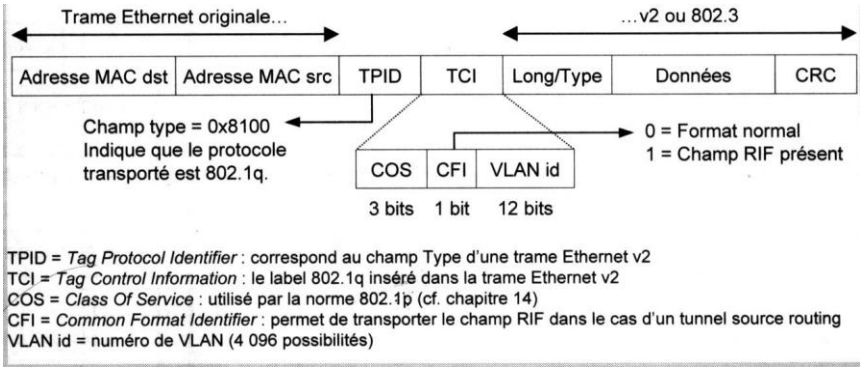
  - L'identificateur est utilisé lors du transfert des paquets sur le réseau
  - Il est enlevé lorsque le paquet quitte le réseau pour atteindre les hôtes ou les routeurs.

Cette dernière méthode est la plus couramment utilisée. Elle est identifiée de manière claire au niveau des commutateurs par le support de cette norme.

Exemple de trame 802.1 q

3.4 Les différents niveaux des VLAN

Afin d'identifier ces différentes techniques d'attribution des VLAN, on attribue un niveau à chaque type de VLAN.



Il existe différentes façons d'associer des ports à un VLAN, les principales sont les suivantes :

- **VLAN de niveau 1 ou VLAN par port** : chaque port du commutateur est affecté à un VLAN, donc chaque carte réseau est affectée à un VLAN en fonction de son port de connexion.
- **VLAN de niveau 2 ou VLAN d'adresses MAC** : chaque adresse MAC est affectée à un VLAN, donc chaque port du commutateur se voit affecter dynamiquement à un VLAN en fonction de l'adresse MAC de la carte réseau qui y est connectée.
- **VLAN de niveau 3 ou VLAN d'adresses IP** : chaque carte réseau est affectée à un VLAN en fonction de son adresse IP, donc chaque port du commutateur se voit affecter dynamiquement à un VLAN en fonction de l'adresse IP de la carte réseau qui y est connectée

Chaque VLAN peut être géré par un ou plusieurs commutateurs, un commutateur peut gérer plusieurs VLAN.

Les commutateurs identifient le VLAN auquel appartient une trame grâce au protocole 802.1q, ils échangent ces trames via des ports d'interconnexion.

En pratique, un port de commutateur ne sera associé qu'à un seul VLAN (à l'exception des ports d'interconnexion).

3.5 Communication inter VLAN

Le principe des VLAN est de limiter la diffusion des informations entre VLAN. Ce qui rend imperméable la communication entre 2 machines situées sur des VLAN différents.

Les ports d'interconnexion entre commutateurs supportant les VLAN sont dénommés Port "TRUNK". Cette dénomination permet de prendre en compte de façon particulière la communication inter commutateurs. Cette communication maintien l'isolement entre les VLAN.

La seule solution technique permettant de partager des ressources ou d'échanger des données est soit de passer par un routeur qui assurera la communication à l'aide de ses tables de routage, soit de rendre disponible les ressources aux 2 VLAN

Exemple de mise à disposition de ressources sur un serveur :