Cours : Les VLANs

Domaine de collision et domaine de diffusion

Un domaine de collision est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux, en particulier dans les réseaux locaux Ethernet. Cela est lié à la topologie logique en bus (méthode d'accès) des réseaux Ethernet. Généralement, un concentrateur forme un seul domaine de collision alors qu'un commutateur en crée un par port, ce qui réduit les risques de collision.

Un domaine de diffusion (broadcast domain) est une aire logique d'un réseau informatique où n'importe quel hôte connecté au réseau peut directement transmettre à tous les autres hôtes du même domaine en envoyant une trame à l'adresse de diffusion.

Les limites de la segmentation physique :

La segmentation physique répond dans certains cas à la diminution des domaines de collision mais :

- l'architecture d'un réseau est fortement dépendante du câblage (et par extension de la couche physique) ;
- pose des problèmes d'évolutivité (dépendance entre les couches physique/services logiques);
- peut nécessiter des ponts (segmentation niveau 2), des routeurs (commutation niveau 3), ou des schémas de câblage redondants (⇒ augmentation des coûts infra-structure et maintenance) ;
- exploitation et maintenance trop lourde (brassage) ;

Le principe est de pouvoir **dissocier l'infrastructure physique d'un réseau et son organisation logique**. Cela est possible :

- par la création de sous-réseaux IP interconnectés par des routeurs (couche 3 du modèle OSI),
- par la configuration de commutateurs, au sein d'un LAN, en intégrant un protocole permettant la création de réseaux dits '**virtuels**' ou **VLAN**s (Virtual Lan Area Network).

Cette 2ème solution, utilisant les commutateurs, permet de réorganiser sous la forme de **réseaux logiques** (VLANs), des équipements matériels ou des ressources sur une infrastructure (couche 1 et 2) unique mais partagée. Un commutateur devra gérer plusieurs VLANs et un même VLAN doit pouvoir être réparti sur plusieurs commutateurs.

Notion de VLAN

Un VLAN (Virtual Lan Area Network) est un réseau virtuel (logique) s'appuyant sur une architecture de transport (pour les réseaux Ethernet, couche OSI 1 et 2).

Un VLAN permet d'organiser (regrouper ou séparer) des ressources (matérielles ou logicielles), selon des critères logiques tout en faisant abstraction des contraintes physique (câblage).

Du point de vue de la couche 2, un VLAN est un **domaine de diffusion** (broadcast domain) Ethernet logique géré par un ou des commutateurs supportant un protocole, la **norme IEEE 802.1q**.

Avantage des Vlans

Les VLANs, améliorent la flexibilité pour la segmentation des réseaux, simplifient l'administration tout en permettant d'augmenter ou améliorer les performances (débit, bande passante, sécurité...).

Pourquoi segmenter un LAN ?

La segmentation permet par exemple d'isoler le trafic entre les segments (pont, routeur, différents services ou type d'utilisateurs). Elle permet d'améliorer la bande passante disponible pour chaque utilisateur en supprimant des domaines de collisions ou en les réduisant.

Les ponts :

les ponts sont des unités de couche liaison qui acheminent des trames de données en fonction des adresses MAC contenues dans les trames. De plus, les ponts sont transparents pour les autres unités du réseau.

Les routeurs :

un routeur fonctionne au niveau de la couche réseau et fonde toutes ses décisions en matière d'acheminement des données entre les segments sur l'adresse de niveau protocole de la couche réseau.

Les commutateurs :

Un commutateur peut segmenter un LAN en microsegments, qui sont des segments à hôte unique. Cela a pour effet de créer des domaines sans collision à partir d'un grand domaine de collision.

Dans une implémentation Ethernet commutée, la bande passante disponible peut atteindre près de 100 %. Chaque ordinateur branché sur port dispose d'une bande passante maximale de point à point.

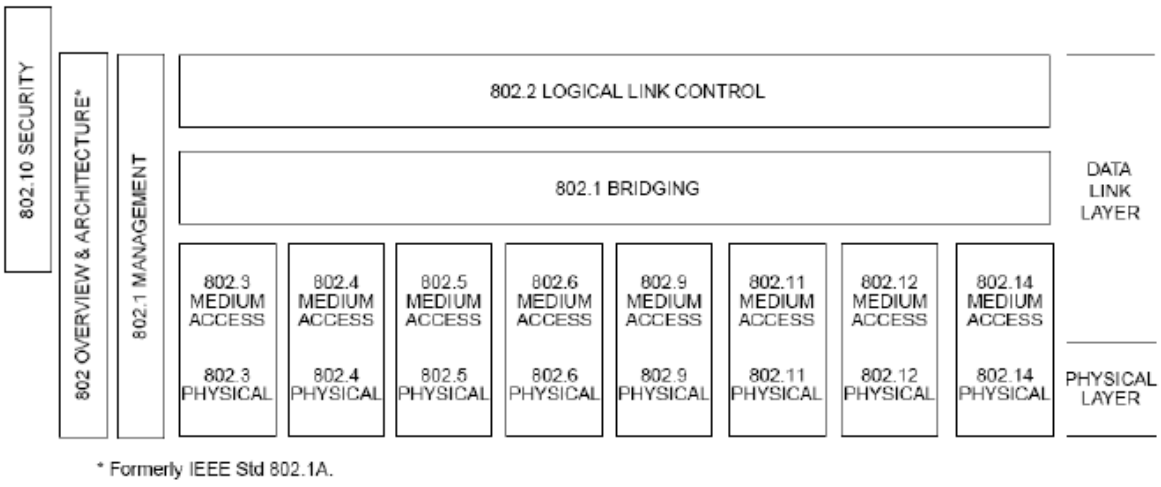
Typologie des VLANs

On considère généralement trois techniques de construction des VLANs

- Par **port ou dits de niveau 1** : on associe les ports physiques du commutateur à tel ou tel VLAN. La solution, simple à mettre en place, manque de souplesse sur les sites importants ou en cas de déplacement de machines. Si on déplace une machine ou si on la change de port, il faut que le nouveau port soit dans le bon VLAN. Cela peut entraîner des manipulations fastidieuses.
- Par **adresse MAC ou dits de niveau 2** : On associe les adresses MAC des clients à tel ou tel VLAN. Le déplacement de machines est possible avec moins de soucis car l'appartenance d'une trame à un VLAN est fonction de l'adresse MAC source. La configuration n'est pas toujours simple sur des parcs importants. Il faut gérer une table de correspondance entre les VLANs et les adresses MAC.
- Par **protocole ou dits de niveau 3**, on associe un protocole de niveau 3 à un VLAN ou alors (pour IP) un sous-réseau. Cette solution est la plus simple à administrer et peut-être même dynamique. En fonction du protocole ou de l'adresse de niveau 3, le nœud relié est rattaché dynamiquement au bon VLAN. Dans ce cas là, il ne s'agit pas de routage au sens 'réseau' (couche 3 du modèle OSI) du terme, car le commutateur n'analyse pas à chaque trame le contenu de la couche 3. Il ne lit que les informations lui permettant de déterminer à quel VLAN il doit affecter le port et commute toujours en s'appuyant sur la couche 2.

Le marquage des trames (tagged frame):

Afin de permettre la reconnaissance des trames, l'IEEE a définit la norme 802.1q. Elle s'insère entre la couche LLC (Logical Layer Control – norme IEEE 802.2) et la couche physique :



La norme, ajoute quatre champs sur deux octets à la trame Ethernet afin de pouvoir identifier les VLANs.

Format de la trame modifiée :

- **VPID :** Vlan Protocol Identifier est fixé à 0x8100. Permet d'identifier une trame de type 802.1q. À ne pas confondre avec le **PVID** (Port Vlan Identifier) qui est le numéro de Vlan affecté à un port.
- **Priorité** : permet de mettre 8 niveaux de priorité, comme par exemple pour les applications de ToIP.
- **CFI** : Cannonical Format Identifier. Indique que le format est standard afin de pouvoir utiliser la norme aussi bien sur Ethernet que sur TokenRing.
- **VID** : Vlan Identifier. Identifie le Vlan.

La norme prévoit trois types de trame :

- les trames non étiquetées (untagged frame)
- les trames étiquetées (tagged frames)
- les trames étiquetées et avec une priorité (priority tagged frame)

La notion d'agrégat de VLAN (VLAN Trunking) :

Le terme de 'trunk' est parfois utilisé pour désigner plusieurs choses. La première est d'augmenter la bande passante entre deux commutateurs par agrégat de liens (802.1ad). Si on a 2 brins de 100 Mbits chacun, on peut créer un 'trunk' de ces deux segments pour n'en faire plus qu'un de 200 Mbits. La seconde (terminologie Cisco) est de pouvoir faire passer des trames provenant de plusieurs VLANs (802.1q) différents sur un même lien. Par exemple pour atteindre un serveur, un routeur ou installer une console de supervision. On parle, dans ce cas de port en mode TAGGED (la trame est étiquettée avec un entête 802.1Q) par opposition au mode UNTAGGED (la trame ne comporte pas de tag 802.1Q).

Capture d'une trame marquée 802.1q: