VLAN

I. Introduction

Un **VLAN** (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau Local Virtuel*) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN.

Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les switchs de niveau 2 minimum.

II. Intérêt des VLAN

Les VLAN présentent les intérêts suivants :

- **Améliorer la gestion du réseau** : réduire la diffusion du trafic (broadcast), apporter de la souplesse pour l'administration et la modification du/des réseaux informatiques en offrant la possibilité à l'administrateur de gérer le paramétrage via des switches.
- **Séparer les flux** : contrôle des échanges inter-VLAN.
- **Segmentation** : réduire la taille d'un domaine de broadcast et créer des groupes de travail indépendamment de l'infrastructure physique du réseau.
- **Sécurité** : les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.

Les échanges inter-VLAN se réalisent tout comme des échanges inter-réseaux, c'est-à-dire au travers de routeurs ou des switches de niveau 3. Il est par conséquent possible de mettre en œuvre un filtrage du trafic échangé entre ces VLAN par le biais d'ACL. C'est le routage inter-VLAN.

III. Types de VLAN

Il existe plusieurs types de VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI.

- **VLAN de niveau 1** associé à la couche physique
- **VLAN de niveau 2** associé à la couche liaison

- **VLAN de niveau 3** associé à la couche réseau

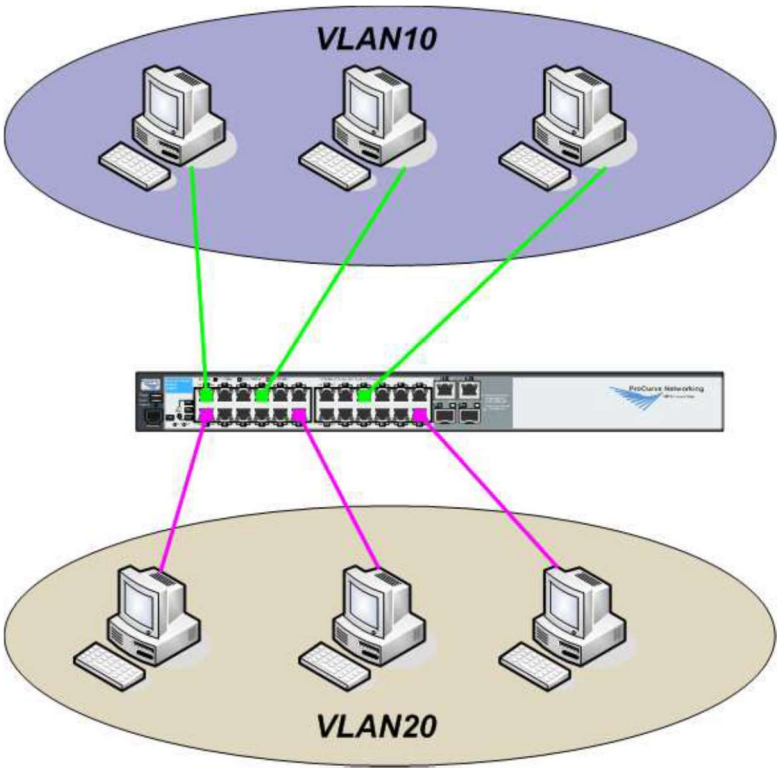
a) VLAN DE NIVEAU 1

Un **VLAN de niveau 1** (aussi appelés **VLAN par port**, en anglais *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le switch.

Dans ce type de VLAN, il n'y a pas de traitement lourd pour chaque trame dans le processus de routage.

Quelques notions importantes à savoir :

- Un brassage est nécessaire pour tout besoin de déplacement géographique
    - Ex : Mr Dupond du service comptabilité déménage du bureau A au bureau B. Mme Durand du service informatique passe du bureau B au bureau A.
        - Pour Mr Dupond il faudra brasser le port du bureau A vers le bureau B pour qu'il puisse accéder au réseau dédié.
        - Le cas inverse, il faudra procéder à la modification réseau du bureau B vers le bureau A pour Mme Durand.

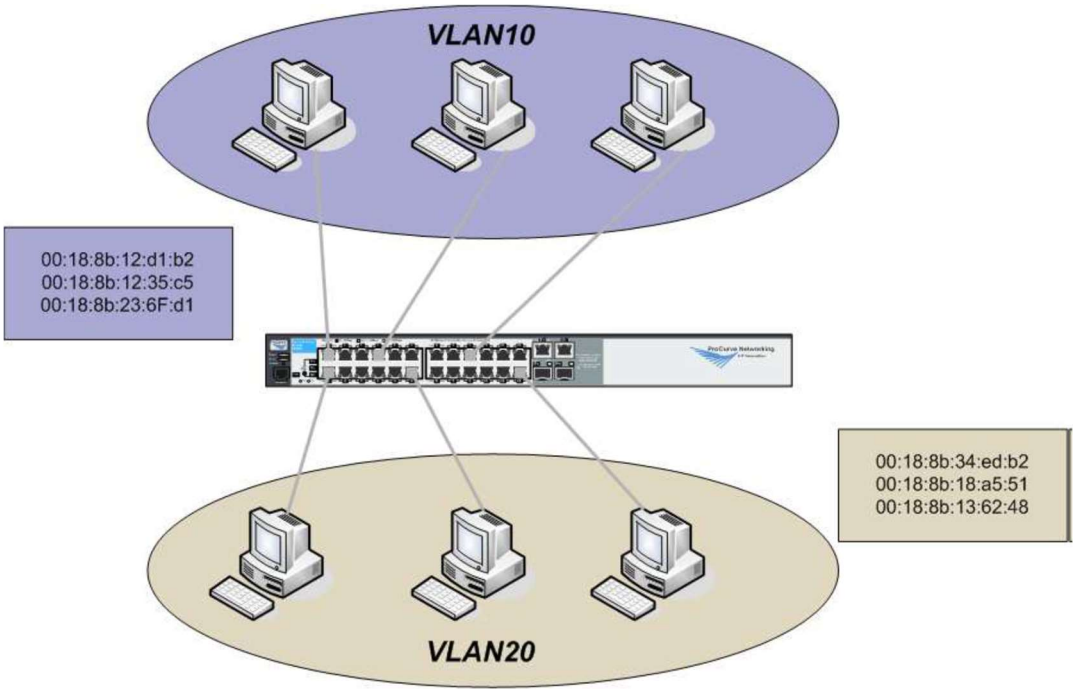


b) VLAN DE NIVEAU 2

Un **VLAN de niveau 2** (également appelé **VLAN MAC**, *VLAN par adresse IEEE* ou en anglais *MAC Address-Based VLAN*) consiste à définir un réseau virtuel en fonction des adresses MAC des stations.

Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

Différents VLAN sont donc possible sur un même segment.



L'intérêt de ce type de VLAN est surtout l'indépendance vis à vis de la localisation. La station peut être déplacée sur le réseau physique, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN.

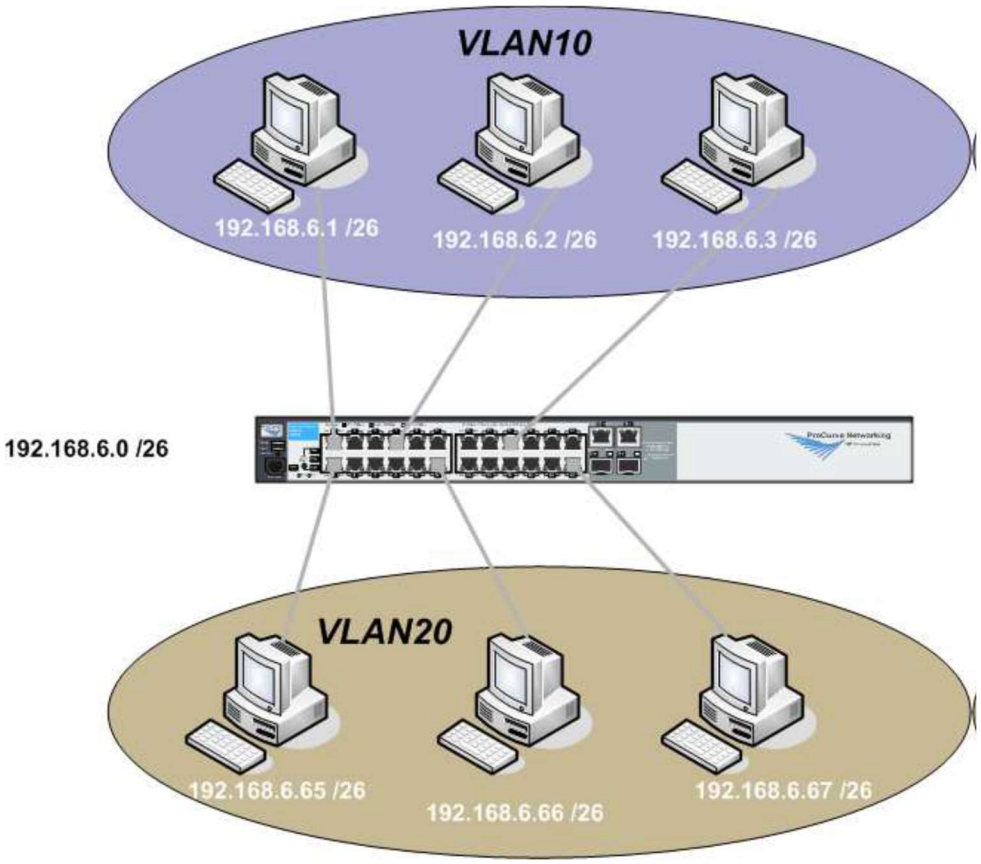
- Ex : Les VLAN par adresse MAC sont très adaptés à l'utilisation de stations portables.

La configuration peut s'avérer rapidement fastidieuse puisqu'elle nécessite de renseigner une table de correspondance avec toutes les adresses du réseau. Cette table doit aussi être partagée par tous les switchs, ce qui peut engendrer un trafic supplémentaire sur le réseau.

c) VLAN DE NIVEAU 3

Un **VLAN de niveau 3** présente plusieurs typologies : par protocole ou par sous réseau.

Le **VLAN par sous-réseau** (en anglais *Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.



- Ex : Dans ce cas, les commutateurs apprennent automatiquement la configuration des VLAN et il est possible de changer une station de place sans reconfiguration des VLAN.

Le **VLAN par protocole** (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN. Par contre, elle est légèrement moins performante puisque les commutateurs sont obligés d'analyser des informations de niveau 3 pour fonctionner.

IV. Extension des trames : VLAN taggé

Le marquage permet de reconnaître le VLAN d'origine d'une trame.
Il peut être implicite, c'est-à-dire que l'appartenance à tel ou tel VLAN peut être déduite des informations contenues dans la trame (adresse IEEE, protocole, sous-réseau IP) ou par son origine (port).
Il peut être explicite : dans ce cas, une information (souvent un numéro de VLAN) est insérée dans la trame. La définition de VLAN à travers plusieurs commutateurs se complique. Tout dépend du type de VLAN.

• Dans le cas d'un VLAN par port, le transfert d'une trame vers un autre commutateur ne conserve pas d'information sur l'appartenance à tel ou tel VLAN. Il est nécessaire de mettre en œuvre un marquage explicite des trames.

• Dans le cas d'un VLAN par adresse IEEE, il est possible d'envisager que la table de correspondance entre les adresses IEEE et les numéros de VLAN soit distribuée sur tous les commutateurs. C'est une solution lourde à laquelle on peut préférer un marquage explicite.

• Les VLAN de niveau 3 utilisent un marquage implicite. Il n'est pas nécessaire de marquer les trames sur les liaisons inter-commutateurs. L'analyse des trames dégradant les performances, il est là aussi préférable de marquer explicitement les trames.
Plusieurs solutions constructeurs ont été proposées telles Virtual Tag Trunking de 3Com ou encore InterSwitch Link Protocol de Cisco, toutes incompatibles entre elles. Pour cette raison, l'IEEE a défini une norme de définition des VLAN sous la référence 802.1Q.
• Extension du format d'Ethernet/IEEE 802.3 en 802.1q.
• Ajout de 4 octets pour spécifier ces informations (tag)

Rappel : Format d'une trame IEEE 802.3/Ethernet :(sans préambule et délimiteur)

Dans un réseau Ethernet IEEE 802.3, les appareils partagent des paquets de données entre eux, également appelés paquets Ethernet. Leur contenu comprend la trame Ethernet (souvent appelée trame de données), qui est à son tour divisée en plusieurs ensembles de données. Ces ensembles de données se composent d'un code binaire qui fournit des informations importantes, notamment les adresses, les informations de contrôle, les données utilisateur et les sommes de contrôle.

Selon le standard Ethernet, les trames Ethernet sont structurées différemment et peuvent contenir plus ou moins de champs de données, selon le protocole réseau.

Dans le modèle OSI la trame est située sur la couche liaison qui est responsable de la transmission sans erreur et sépare le flux de données binaires en blocs ou trames.

Les différents champs de la trame sont :

- ***Adresse MAC destination*** (6octets)

Permet de connaître la destination de la trame.

- ***Adresse MAC source*** (6 octets)

Permet en cas de problèmes sur la trame, d'avertir la station émettrice que sa trame n'a pu être livrée, et de redemander une retransmission.

- ***Long/type***: (2 octets)

Le champ Type/longueur est utilisé pour identifier quel protocole de réseau de niveau supérieur est utilisé dans la trame.

- ***Données***: (46 octets minimum, 1500 octets maximum)

Le champ de données/charge utile est ce que nous considérons généralement comme le plus important ce sont les données que nous transmettons.

- ***FCS*** (4 octets)

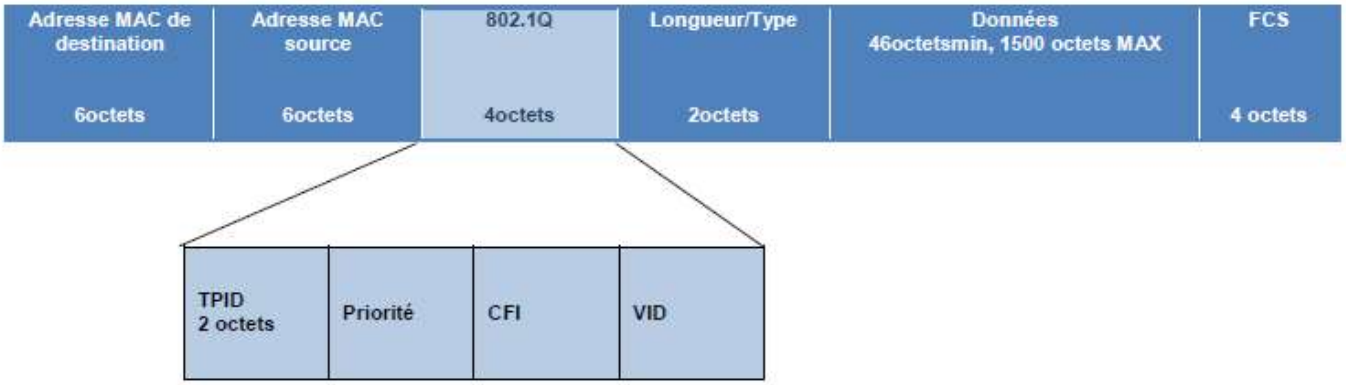
La fin de la trame contient un champ de 32 bits qui est une somme de contrôle de redondance cyclique (CRC).

Adresse MAC de destination	Adresse MAC source	Longueur/Type	Données 46octetsmin, 1500 octets MAX	FCS
6octets	6octets	2octets		4 octets

Format d'une trame Ethernet à la norme 802.1Q :

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. Comme dans le cas de l'encapsulation ISL précédente, l'en-tête de trame est complété par une balise de 4 octets. Le standard IEEE 802.1Q définit le contenu de la balise de VLAN (**VLAN tag**) avec laquelle on complète l'en-tête de trame Ethernet.
Ce VLAN tag est placé à la suite du champ « Adresse MAC Source » de la trame Ethernet.

Pour plus d'informations sur la norme 802.1Q : https://fr.wikipedia.org/wiki/IEEE_802.1Q



TPID (Tag Protocol Identifier). 2 octets
0x8100 pour les trames « taggées » 802.1q

TCI (Tag Control Information). 2 octets
3 premiers bits: « user priority » de 0 à 7
1 bit CFI (Canonical Format Indicator). Ethernet:0
12 bits: VID (VLAN Identifier)

Les trames provenant s'un switch qui les aura taguées doivent être réceptionnées par un hôtes du réseau qui comprend la norme 802.1Q. Si l'hôte ne sait pas lire cette norme, la trame sera rejetée.
Les périphériques réseaux qui acceptent la norme 802.1Q sont, par exemple :
- Les switches
- Les routeurs
- Les DSLAM
- Les cartes réseaux

Mais ce n'est pas une généralité, il faut absolument s'en assurer en consultant la documentation constructeur avant l'achat de l'un de ces périphériques.
Les switches HP Série Procurve, Netgear (manageables), les switches et routeurs CISCO, acceptent cette norme, mais il s'agit là de matériel professionnel.

Pour rappel, sur cisco la dénomination des VLAN :
TRUNK / ACCESS

Sur HPE :
TAG / UNTAG