

I/ Qu'est-ce qu'un réseau virtuel ?

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**.

Définition

Un réseau local virtuel est un regroupement virtuel d'au moins deux périphériques. Ce regroupement virtuel peut s'étendre au-delà de plusieurs commutateurs. Les périphériques sont regroupés sur la base d'un certain nombre de facteurs suivant la configuration du réseau.

Comme avec n'importe quelle technologie de mise en réseau, il convient de bien comprendre les caractéristiques opérationnelles des réseaux VLAN avant de les mettre en œuvre dans votre réseau. Il sera ainsi possible de mettre en œuvre des réseaux VLAN bien conçus et réduire les délais de dépannage, le cas échéant.

II/ Pourquoi créer un réseau virtuel ?

Dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) **il est possible de s'affranchir des limitations de l'architecture physique** (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

III/ Typologie de VLAN

1) Les critères

Trois méthodes sont généralement utilisées pour attribuer un équipement à un réseau VLAN :

- a) Les réseaux VLAN basés sur les ports
- b) Les réseaux VLAN basés sur les adresses MAC
- c) Les réseaux VLAN basés sur les protocoles

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue.

2) 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 ou commutateur**.

Dans le cadre des réseaux VLAN basés sur les ports, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.

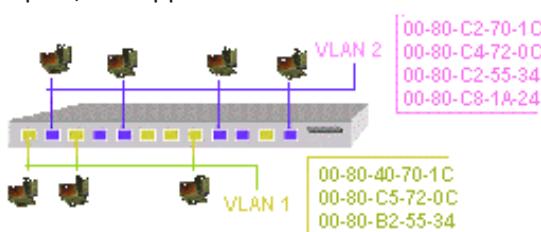
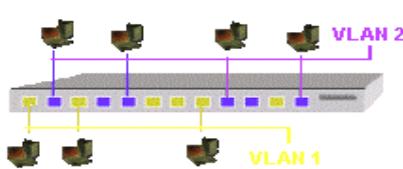
3) VLAN de niveau 2

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.

L'un des problèmes que posent les réseaux VLAN basés sur les ports est que si le périphérique d'origine est retiré du port pour être remplacé par un autre périphérique, le nouveau périphérique appartiendra au même réseau VLAN que son prédécesseur.

Dans le cas d'un réseau VLAN composé d'imprimantes, si une imprimante est retirée d'un port du commutateur pour être remplacée par un périphérique du service de comptabilité, ce dernier dépendra désormais du réseau VLAN des imprimantes. Ceci risque de limiter l'accès du périphérique de comptabilité aux ressources du réseau.

Les réseaux VLAN basés sur les adresses MAC permettent de résoudre ce problème. En effet, dans ce cas, l'appartenance au réseau VLAN dépend de l'adresse MAC du périphérique et non du port de commutation physique. Lorsque le périphérique est retiré pour être connecté à un autre port, son appartenance au réseau VLAN le suit.



Malheureusement, la corrélation entre les adresses MAC et le numéro VLAN prend beaucoup de temps et donc ce type de réseau VLAN est rarement utilisé.

4) VLAN de niveau 3

On distingue plusieurs types de VLAN de niveau 3 :

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.

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.

Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP.

IV/ Les avantages des VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants:

- **Plus de souplesse pour l'administration** et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs ;
- **Gain en sécurité** car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées. Réduction de la diffusion du trafic sur le réseau ;

V/ Étiquetage du réseau VLAN

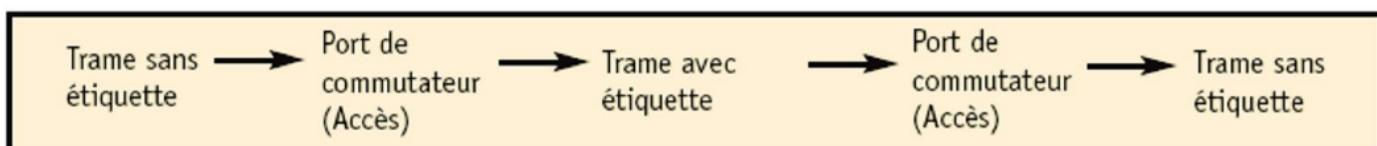
1) Qu'est-ce qu'une étiquette ?

On utilise des étiquettes VLAN pour indiquer l'appartenance à tel réseau VLAN d'une trame en circulation. Ces étiquettes sont fixées à la trame au moment où elle fait son entrée dans un port de commutateur appartenant à un réseau VLAN. Elles sont retirées lorsque la trame quitte un port appartenant à ce réseau VLAN. Le type du port appartenant au réseau VLAN détermine si l'étiquette VLAN doit ou non rester fixée à la trame. Les deux types de ports possibles au sein d'un environnement VLAN sont les ports d'accès et les ports de liaison.

2) Ports d'accès

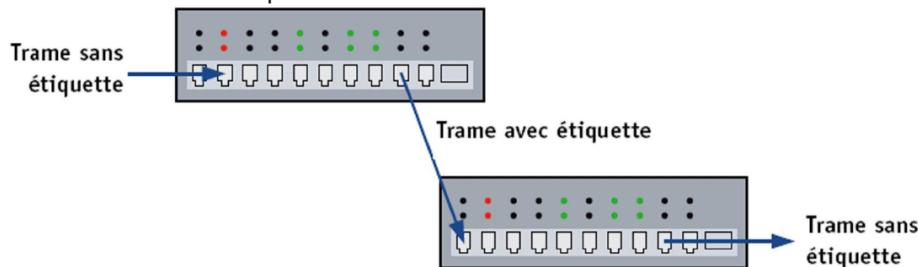
Les ports d'accès sont ceux par lesquels une trame entre et ressort d'un réseau VLAN.

Lorsqu'un port d'accès reçoit une trame, celle-ci ne comporte pas d'étiquette VLAN. C'est au moment où la trame rentre dans le port d'accès que l'étiquette VLAN est fixée à la trame. Pendant que la trame transite par le commutateur, elle transporte l'étiquette VLAN qui lui a été attribuée au moment d'entrer dans le port d'accès. L'étiquette VLAN est supprimée lorsque la trame quitte le commutateur via le port d'accès de destination. Les périphériques d'émission et de réception ignorent qu'une étiquette VLAN a été utilisée.



3) Ports de liaison

Dans les réseaux comportant plusieurs commutateurs, il est indispensable de pouvoir envoyer des trames avec étiquette VLAN d'un commutateur à un autre. La différence entre les ports d'accès et de liaison est que les ports de liaison ne retirent pas l'étiquette VLAN de la trame lorsqu'ils l'envoient. La présence de l'étiquette VLAN permet au commutateur de réception de connaître l'appartenance de la trame en transit. La trame peut ainsi être renvoyée aux ports appropriés du commutateur de réception.



VI) Technologies d'étiquetage VLAN

Chaque trame avec une étiquette VLAN comporte des champs indiquant son appartenance à un réseau VLAN. Il existe deux grands formats d'étiquettes VLAN :

- le format de liaison inter-commutateur ISL de Cisco
- le format standard 802.1Q.

1) Format de Cisco

Le format de liaison inter-commutateur ISL est un format propriétaire de Cisco pour les étiquettes VLAN. Cette étiquette VLAN ajoute 26 octets d'informations à l'avant de la trame et un CRC de 4 octets en fin de trame. Le format de ce type d'étiquette est le suivant :

Nb bits	40	4	4	48	16	24	24	15	1	16	16	8 à 196600 Bits 1 à 24575 octets	32
Champ trame	DA	Type	User	SA	Len	AAAA03	HSA	VLAN	BPDU	Index	Res	Encap frame	FCS

Signification des différents champs :

Champ	Description
DA	Comporte une adresse multidestinataire de type 0x01-00-0C-00-00 ou 0x03-00-0c-00-00.
Type	Indique la topologie utilisée pour transporter la trame encapsulée
User	Ce champ à quatre bits indique la priorité attribuée à la trame par 1 utilisateur.
SA	Adresse MAC du port du commutateur qui transmet cette trame étiquetée ISL.
Len	La longueur de la trame encapsulée. Ce champ exclut les champs en-tête ISL et FCS ISL.
AAAA03	Champ constant
HSA	Bits élevés de 1 adresse source De type 0x00-00-0C.
VLAN	Champ de 15 bits indiquant l'appartenance VLAN.
BPDU	Champ de 1 bit défini sur 1 si la trame encapsulée est de type Spanning Tree Bridge 802.1D.
Index	Comporte 1 index du port de commutateur émetteur.
Res	Réserve pour les trames encapsulées Token Ring ou FDDI.
Encap frame	La trame complète, non modifiée, telle que reçue par le port d'accès
FCS	(Frame Check Sequence). Séquence de contrôle de trame pour la trame ISL.

2) Format standard 802.1Q

Tandis que ISL est un format propriétaire de Cisco, 802.1Q est un format IEEE standard. Le format 802.1Q permet aux trames étiquetées de circuler entre les commutateurs de plusieurs constructeurs.

L'étiquette 802.1Q comporte moins de champs que l'étiquette ISL. Elle est insérée dans la trame et non placée en début de trame.

Nb bits	48	48	16	3	1	12	16	368 à 12000	32
Champ trame	DA	SA	8100	Priority	CFI	VLAN	Ether type	Data	FCS

CFI : (Canonical Format Indicator). Champ à 1 bit indiquant quelles options sont liées à l'étiquette VLAN. Surtout utilisé dans les réseaux Token Ring.

VII/ Le Spanning tree (arbre recouvrant)

1) Définition

Le *Spanning Tree Protocol* (aussi appelé STP) est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle (appelée arbre) dans les LAN avec ponts. Il est défini dans la norme IEEE 802.1D et est basé sur un algorithme décrit par Radia Perlman en 1985.

Les techniques d'arbres recouvrant permettent de connecter un ensemble de commutateurs avec des liens redondants (boucles), qui seront automatiquement activés en cas de panne d'un lien actif. Un algorithme (distribué) construit un arbre recouvrant du réseau, pour assurer qu'il n'y a pas de boucles possibles (les boucles seraient catastrophiques pour le protocole Ethernet !). Les réseaux commutés de type Ethernet doivent avoir un chemin unique entre deux points, cela s'appelle une topologie sans boucle. En effet, la présence de boucle génère des tempêtes de diffusion qui paralysent le réseau. Cependant, un bon réseau doit aussi inclure une redondance pour fournir un chemin alternatif en cas de panne d'une liaison ou d'un commutateur. L'algorithme de « *spanning tree minimum* » garantit l'unicité du chemin entre deux points du réseau en affectant un port dédié (*root port*), celui qui a le chemin le plus court vers le *root bridge*, à chaque segment du LAN (domaine de collision).

2) Élection du root bridge

Une topologie sans boucle ressemble à un arbre et à la base de chaque arbre, on trouve ses racines (*roots*). Dans un réseau commuté, le *root bridge* (commutateur maître) est déterminé par l'algorithme du *spanning tree*.

Chaque commutateur a une adresse MAC et un numéro de priorité paramétrable (0x8000 par défaut), ces deux nombres constituant l'identification du *bridge* (nommée *BID*). Le *BID* est utilisé pour élire le *root bridge* en fonction des numéros de priorité, en cas d'égalité, l'adresse MAC la plus basse l'emporte, et comme toutes les adresses MAC sont uniques, il existera toujours un *root bridge* unique. Les autres commutateurs du réseau vont alors calculer la distance la plus courte vers le *root bridge* en utilisant le « *coût* » le plus faible vers celui-ci, ce coût dépendant de la bande passante des liens vers celui-ci.

En général, l'administrateur du réseau configure la priorité du *root bridge* le plus opportun en fonction de la topologie particulière du réseau, ainsi que la priorité d'un autre commutateur qui deviendra *root bridge* en cas de défaillance du *root bridge* principal.