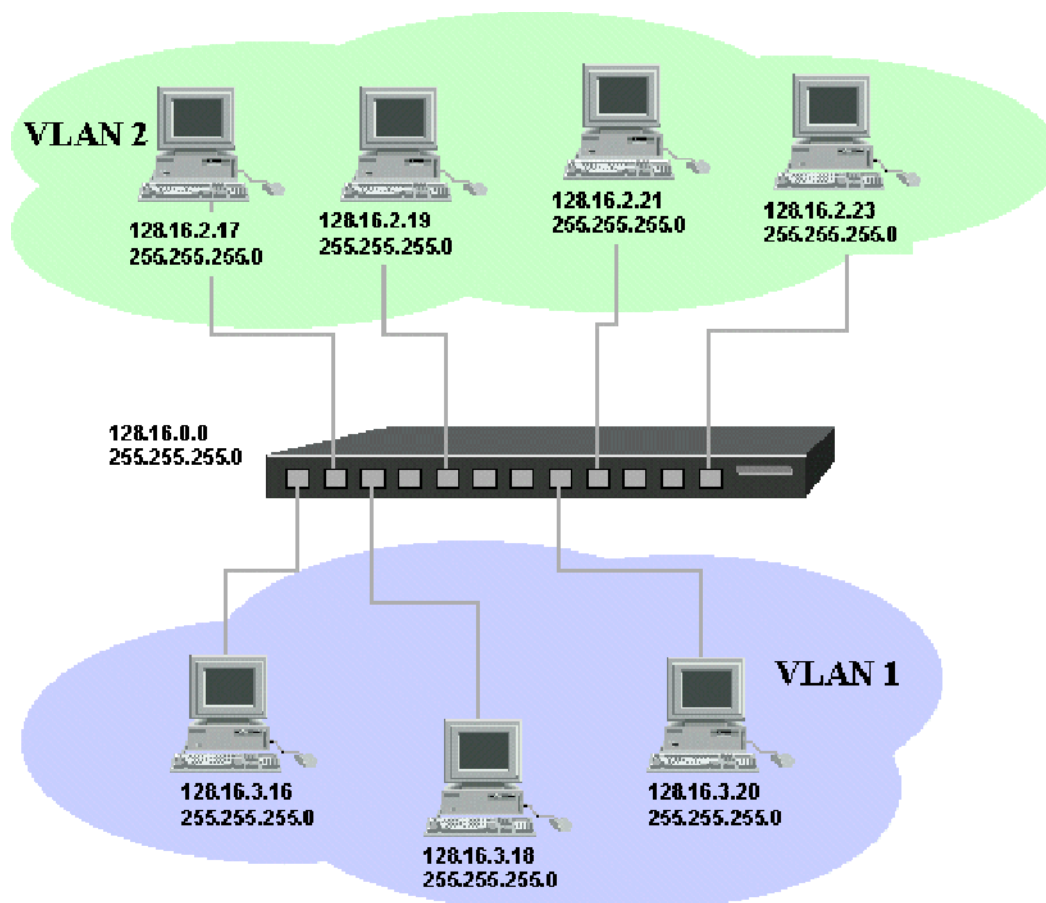


LES VLAN



I QU'EST-CE QU'UN RÉSEAU VIRTUEL ? VLAN

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. Vous pourrez ainsi mettre en œuvre des réseaux VLAN bien conçus et réduire les délais de dépannage, le cas échéant.

II POURQUOI CRÉER UN RÉSEAU VIRTUEL ?

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN) 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

III.1 QUELS CRITÈRES ?

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

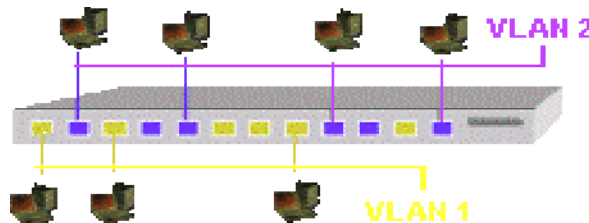
- Les réseaux VLAN basés sur les ports ;
- Les réseaux VLAN basés sur les adresses MAC ;
- Les réseaux VLAN basés sur les protocoles.

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

III.2 VLAN 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.



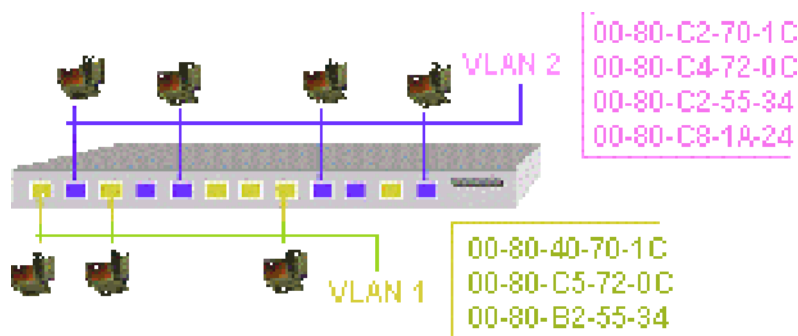
III.3 VLAN NIVEAU 2 L2

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 l'exemple du réseau VLAN composé d'imprimantes, imaginons qu'une imprimante soit 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 pas mal de temps et donc ce type de réseau VLAN est rarement utilisé.

III.4 VLAN NIVEAU 3 ~ L3 RÉSEAUX VLAN BASÉS SUR LES PROTOCOLES

Un 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 modifie 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.

III.5 QUELS 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 ;

Les VLAN sont définis par les standards IEEE 802.1D, 802.1p, 802.1Q et 802.10. Pour plus d'informations il est donc conseillé de se reporter aux documents suivants :

IEEE 802.1D

IEEE 802.1Q

IEEE 802.10

IV ETIQUETAGE DU RÉSEAU VLAN

IV.1 QU'EST-CE QU'UNE ÉTIQUETTE ?

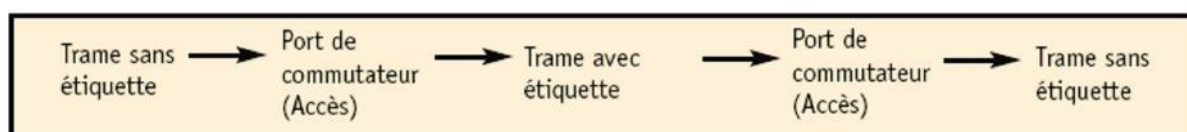
On utilise des étiquettes VLAN pour indiquer l'appartenance à tel réseau VLAN d'une trame en circulation.

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.

IV.2 PORTS D'ACCÈS

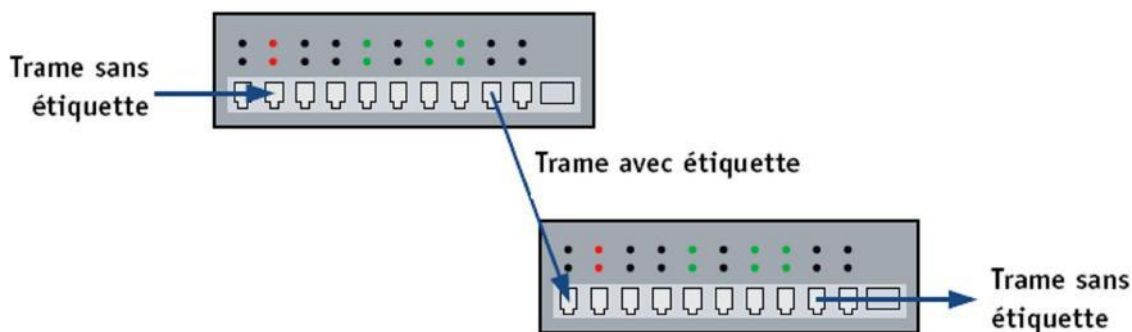
Les ports d'accès sont ceux par lesquels une trame entre et ressort d'un réseau VLAN. Lorsqu'un port d'accès reçoit une trame, celle-ci ne comporte pas d'étiquette VLAN. C'est au moment où la trame rentre dans le port d'accès que l'étiquette VLAN est fixée à la trame. Pendant que la trame transite par 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 jamais été utilisée.

Ports d'accès :



IV.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.



IV.4 TECHNOLOGIES D'ÉTIQUETAGE VLAN

Chaque trame avec une étiquette VLAN comporte des champs indiquant son appartenance à un réseau VLAN.

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.

V MAINTENANCE DES RÉSEAUX VLAN

L'une des principales difficultés d'un réseau qui emploie des réseaux VLAN réside dans la maintenance de la configuration VLAN au travers des différents commutateurs. Sans point central de configuration et de maintenance des informations VLAN, l'administrateur réseau doit configurer les réseaux VLAN sur chaque commutateur séparément. Pour faciliter les choses, Cisco propose un protocole de liaison (VLAN Trunk Protocol).

VI FAQ

- Quels sont les trois avantages principaux de l'utilisation de VLAN dans un réseau local important ?
- Une Ecole d'ingénieurs a deux VLAN : un VLAN 'professeurs' et un VLAN 'étudiants'. Comment est-il possible qu'un étudiant envoie un e-mail à un professeur ?
- Donnez un exemple d'utilisation d'un VLAN.

VII RÉPONSES FAQ :

- Chaque VLAN a son propre domaine de broadcast ce qui limite le nombre de trames de broadcast. Par conséquent cela limite le trafic du réseau ;
 - les communications entre les VLAN peuvent être sécurisées par des firewalls ;
 - les VLAN permettent d'affecter un utilisateur à un nouveau groupe sans re-câblage (à la différence de deux sous-réseaux physiques).
- Passer par un routeur
- Dans une usine, créer 3 VLAN : Administration, Comptabilité, Production