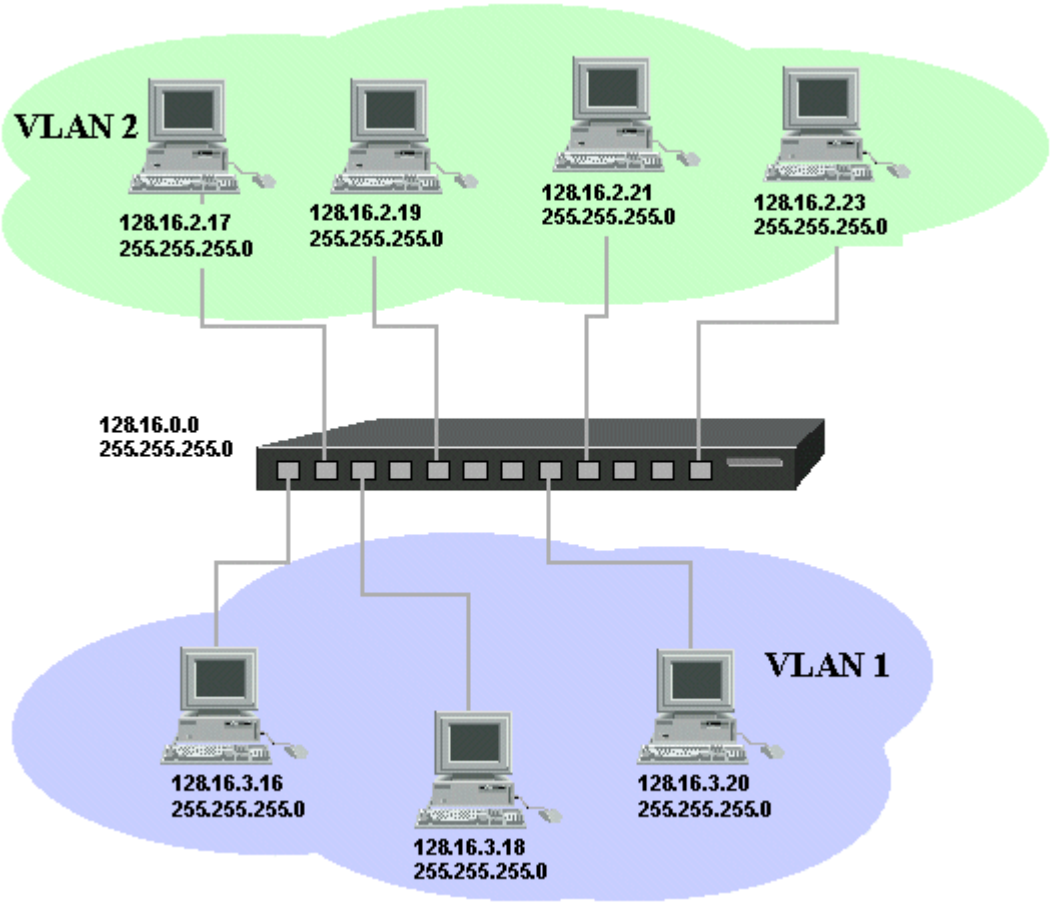
RESEAUX	LES RESEAUX VIRTUELS VLAN → switch manageable	COURS



1. Quêest-ce quûun 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 dûau moins deux périphériques. Ce regroupement virtuel peut sûétendre au-delà de plusieurs commutateurs. Les périphériques sont regroupés sur la base dûun certain nombre de facteurs suivant la configuration du réseau.

Comme avec nûimporte quelle technologie de mise en réseau, il convient de bien comprendre les caractéristiques opérationnelles des réseaux VLAN avant de les mettre en î uvre dans votre réseau. Vous pourrez ainsi mettre en î uvre des réseaux VLAN bien conçus et réduire les délais de dépannage, le cas échéant.

2. 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 (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.).

3. Typologie de VLAN

3.1 Quels critères ?

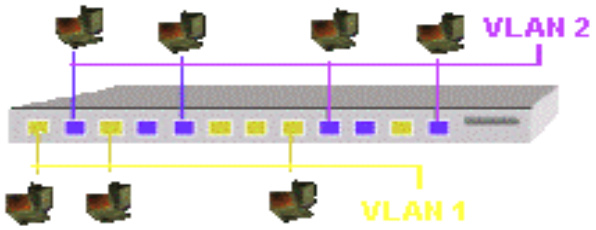
Trois méthodes sont généralement utilisées pour attribuer un équipement à un réseau VLAN :

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.

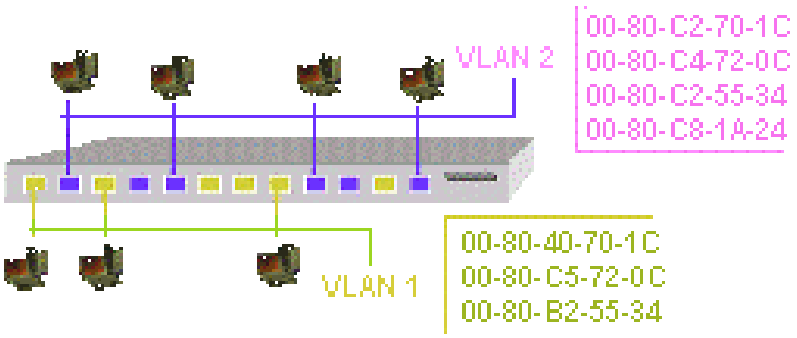
3.2 VLAN niveau 1

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.



3.3 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.



Points + :

Point - :
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.

3.4 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 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.

4. Quels avantages des VLANs ?

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'information il est donc conseillé de se reporter aux documents suivants :
IEEE 802.1D
IEEE 802.1Q
IEEE 802.10

5. Etiquetage du réseau VLAN

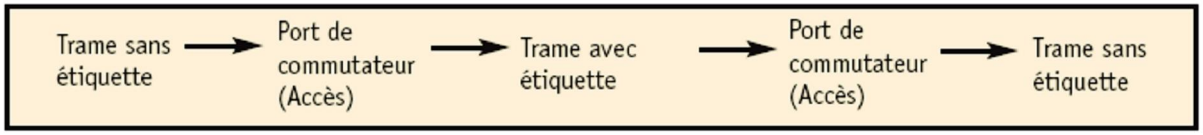
5.1 Qu'est-ce qu'une étiquette ?

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.

5.2 Ports d'accès

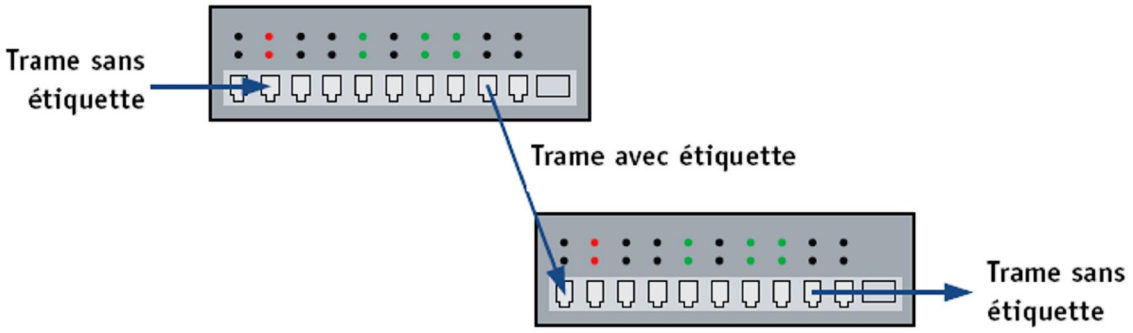
Les ports d'accès sont ceux par lesquels une trame entre et ressort d'un réseau VLAN. Lorsqu'un port d'accès reçoit une trame, celle-ci ne comporte pas d'étiquette VLAN. C'est au

moment où la trame rentre dans le port dôaccès que lôétiquette VLAN est fixée à la trame. Pendant que la trame transite par le commutateur, elle transporte lôétiquette VLAN qui lui a été attribuée au moment dôentrer dans le port dôaccès. Lôétiquette VLAN est supprimée lorsque la trame quitte le commutateur via le port dôaccès de destination. Les périphériques dôémission et de réception ignorent quôune étiquette VLAN a jamais été utilisée.
Ports dôaccès :



5.3 Ports de liaison

Dans les réseaux comportant plusieurs commutateurs, il est indispensable de pouvoir envoyer des trames avec étiquette VLAN dôun commutateur à un autre. La différence entre les ports dôaccès et de liaison est que les ports de liaison ne retirent pas lôétiquette VLAN de la trame lorsquôils lôenvoient. La présence de lôétiquette VLAN permet au commutateur de réception de connaître lôappartenance de la trame en transit. La trame peut ainsi être renvoyée aux ports appropriés du commutateur de réception.



6. Technologies dôétiquetage VLAN

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

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

6.1 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 dôinformations à lôavant de la trame et un CRC de 4 octets en fin de trame. Le format de ce type dôétiquette 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 lôutilisateur.
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 lôadresse source ï De type 0x00-00-0C.
VLAN	Champ de 15 bits indiquant lôappartenance VLAN.
BPDU	Champ de 1 bit défini sur 1 si la trame encapsulée est de type Spanning Tree Bridge 802.1D.
Index	Comporte lôindex du port de commutateur émetteur.
Res	Réservé pour les trames encapsulées Token Ring ou FDDI.
Encap frame	La trame complète, non modifiée, telle que reçue par le port dôaccès
FCS	(Frame Check Sequence). Séquence de contrôle de trame pour la trame ISL.

6.2 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.

Lôétiquette 802.1Q comporte moins de champs que lôétiquette 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 lôétiquette VLAN. Surtout utilisé dans les réseaux Token Ring.

7. Le Spanning tree → arbre recouvrant

7.1 Quôest-ce que le spanning tree ?

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 recouvrants permettent de connecter un ensemble de switchs avec des liens redondants (boucles), qui seront automatiquement activés en cas de panne d'un lien actifs. 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).

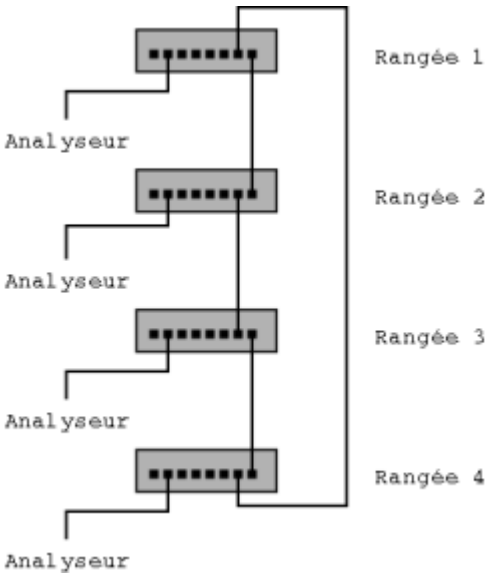
7.2 Election du root bridge

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.

7.3 Manipulation

Pour réaliser cette partie, il faut interconnecter les switchs de toutes les rangées comme sur la figure suivante :



Chaque rangée doit avoir installé un analyseur (`Wireshark`) sur un port SPAN, afin d'observer tout le trafic.

7.3.1 Lorsqu'aucune station n'est active sur le réseau (pas de transferts ni de pings), qu'observe-t-on ?

7.3.2 Lancer un échange (ping) entre la rangée 1 et la rangée 3. Quel est le chemin suivi par la trame ?

7.3.3 Lancer un ping continuel entre 1 et 3, et déconnecter le lien entre les switchs 2 et 3. Qu'observe-t-on ? Combien de temps met le réseau à se rétablir ? Peut-on agir sur ce délai dans la configuration des équipements ?

8. Maintenance des réseaux VLAN

Lôune des principales difficultés dôun 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, lôadministrateur réseau doit configurer les

réseaux VLAN sur chaque commutateur séparément. Pour faciliter les choses, Cisco propose un protocole de liaison (VLAN Trunk Protocol).

9. FAQ

a) Quels sont les trois avantages principaux de lôutilisation de VLAN dans un réseau local important ?
b) Une Ecole dôingénieurs a deux VLAN : un VLAN ôprofesseursô et un VLAN ôétudiantsô. Comment est-il possible quôun étudiant envoie un e-mail à un professeur ?
c) Donnez un exemple dôutilisation dôun VLAN.

10. Ressources bibliographiques

10.1 Livres & revues

- Article Revue Flukenetworks

10.2 URLographie

- **http://www.commentcamarche.net/internet/vlan.php3**
- **http://fr.wikipedia.org/wiki/Virtual_LAN**
- **http://www.lococheb.net/vlan.php**

Réponses FAQ :
a) 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 ;
ï les communications entre les VLAN peuvent être sécurisées par des firewalls ;
ï les VLAN permettent dôaffecter un utilisateur à un nouveau groupe sans re-câblage (à la différence de deux sous-réseaux physiques).

b) Passer par un routeur
c) Dans une usine, créer 3 VLAN :
- Administration,
- Comptabilité,
- Production.