



RT 12

Routage IP



Chapitre II

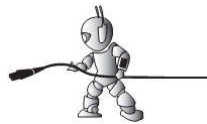
Les réseaux locaux virtuels (VLAN)

Dr. H. Zerrouki

<zerrouki.hadj@gmail.com>

UDL-SBA, Faculté de Génie Electrique

DÉPARTEMENT
Télécommunications



Plan de cours



Introduction

Principes généraux des VLAN

Les types des VLAN

- ❖ Les VLAN de **niveau 1** (Port-based VLAN)
- ❖ Les VLAN de **niveau 2** (MAC Address -based VLAN)
- ❖ Les VLAN de **niveau 3** (Network Address -based VLAN)

L'identification des VLAN (802.1Q)

Le routage inter-VLAN

INTRODUCTION

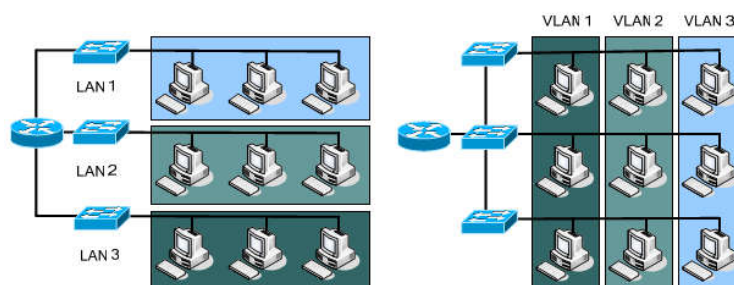
Définition

- Un réseau virtuel ou **VLAN** (*Virtual Local Area Network*) est un regroupement logique, et non physique, de plusieurs stations.
- Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN.
- La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage.
- Les réseaux VLAN permettent de définir des domaines de diffusions restreints, quelque soit l'emplacement de leur segment physique.
- Cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN.

INTRODUCTION

Les principales différences entre la commutation traditionnelle et les VLAN :

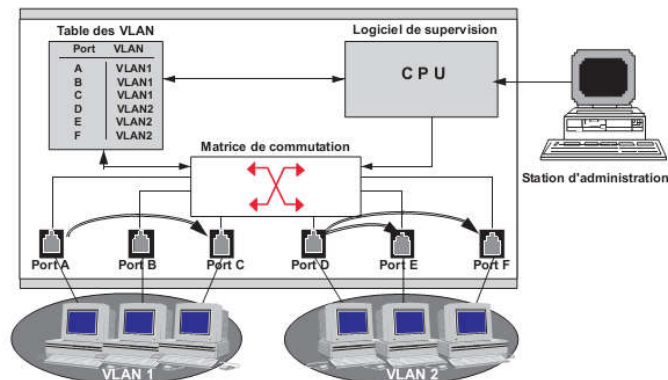
- Les VLAN fonctionnent au niveau des couches 2 et 3 du modèle OSI.
- La communication inter VLAN est assurée par le routage de couche 3.
- Les VLAN fournissent une méthode de contrôle des diffusions (broadcasts).
- Les VLAN permettent d'effectuer une segmentation selon certains critères:
 - Des collègues travaillant dans le même service.
 - Une équipe partageant le même applicatif.
- Les VLAN peuvent assurer la sécurité (quels nœuds peuvent communiquer entre eux).



PRINCIPES GENERAUX DES VLAN

Principe

- ❑ Les VLAN autorisent, sur un même réseau physique la réalisation de plusieurs réseaux logiques totalement indépendant les uns des autres.
- ❑ La communication n'est autorisée qu'entre machines d'un même VLAN. Les communications inter-VLAN doivent transiter par un routeur ou Switch niveau 3.



PRINCIPES GENERAUX DES VLAN

Les avantages d'un VLAN

- ❑ Les principaux avantages des VLAN sont les suivants :
 - Ils permettent de supporter les organisations virtuelles, en rendant l'appartenance à un groupe indépendant de sa position géographique.
 - Ils optimisent la bande passante, en réalisant des réseaux différents, donc en réalisant des domaines de collision différents.
 - Ils simplifient l'administration, en utilisant des commandes centralisées pour gérer un réseau plutôt que des interventions dans les armoires de brassage.
 - Ils améliorent la sécurité, en créant des règles de communication inter-VLAN.

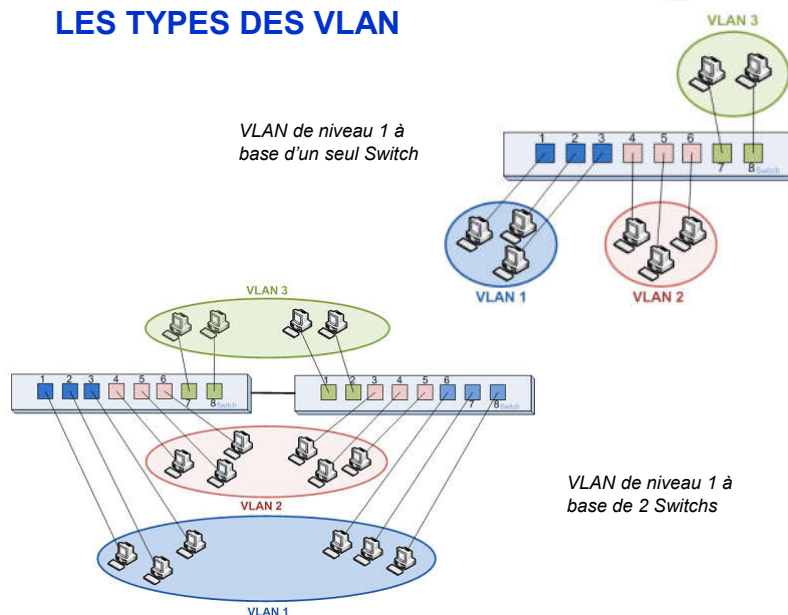
LES TYPES DES VLAN

- ❑ 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** ou VLAN par port (**Port-based VLAN**) : associé à la couche physique
 - **VLAN de niveau 2** ou VLAN MAC (**MAC Address-based VLAN**) : associé à la couche liaison
 - **VLAN de niveau 3** ou VLAN d'adresses IP (**Network Address-based VLAN**) : associé à la couche réseau.

Les VLAN de niveau 1

- Ces VLAN associent chaque port d'un commutateur à un VLAN.
- Une station raccordée à un port est automatiquement affectée au VLAN du port.
- Si le port est raccordé à un hub, toutes les stations de ce hub appartiennent au même VLAN (VLAN par segment).
- Le déplacement d'une station implique son changement de VLAN.
- C'est le mode le plus sécurisé, un utilisateur ne peut changer sa machine de VLAN.
- Avec ce type de VLAN, on ne dispose pas d'une souplesse très importante, et c'est pour quoi ils sont peu utilisés.

LES TYPES DES VLAN



LES TYPES DES VLAN

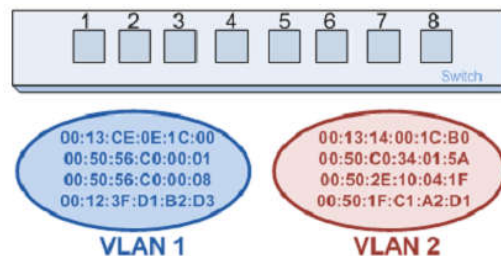
Les VLAN de niveau 2

- Ces VLAN associent les stations par leur adresse MAC.
- Deux stations raccordées à un même port (segment ou Hub) peuvent appartenir à deux VLAN différents.
- Les relations adresses MAC/VLAN sont introduites par l'administrateur.
- Il existe des mécanismes d'apprentissage automatique d'adresses (lecture des adresses MAC des stations raccordées).
- L'administrateur n'ayant plus qu'à effectuer les regroupements par simple déplacement et regroupement de stations dans le logiciel d'administration.
- Une station peut appartenir à plusieurs VLAN.
- Les VLAN de niveau 2 sont indépendants des protocoles supérieurs.
- La commutation, s'effectuant au niveau MAC, autorise un faible temps de latence ;
- Cela offre une grande souplesse et permet d'avoir des stations sur un même port du Switch et pourtant appartenant à des VLAN différents.

LES TYPES DES VLAN

Les VLAN de niveau 2

- La seule différence à ce type de VLAN est la nécessité de maintenir un fichier de correspondance entre l'adresse MAC et VLAN, le Switch l'ayant créé lors de sa configuration, il suffit de l'exporter.



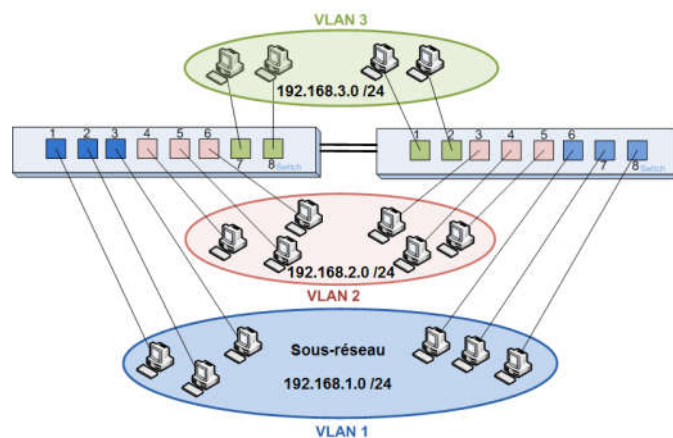
LES TYPES DES VLAN

Les VLAN de niveau 3

- Ces VLAN sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (*Subnet* d'IP).
- Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN.
- Une station peut appartenir à plusieurs VLAN par affectation statique.
- Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance.
- L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de commutation et non de routage.
- L'entête n'est pas modifié, c'est l'adresse IP de la station qui détermine le VLAN auquel elle appartient.
- Plus précisément, on associe à un VLAN à une plage d'adresse.
- Avec les VLAN de niveau 3, la configuration est facile car on se trouve au niveau IP, donc loin de toute configuration matérielle tels que ports ou adresses MAC.

LES TYPES DES VLAN

Les VLAN de niveau 3



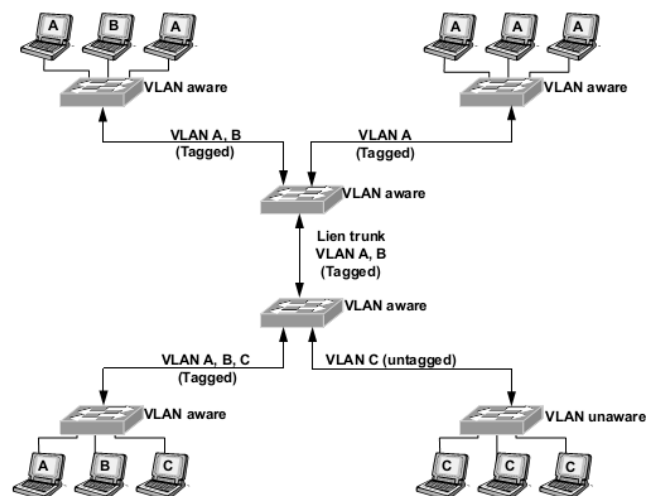
L'IDENTIFICATION DES VLAN (802.1Q)

Principe de l'étiquetage des trames

- Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines (table d'acheminement) et connaître le VLAN d'appartenance de la source et du destinataire, il est plus efficace d'étiqueter les trames.
- L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLAN d'appartenance des stations qui lui sont raccordées.
- On distingue deux types d'équipements, ceux qui savent gérer l'étiquetage et qui ont donc connaissance des VLAN (les *VLAN aware*) et ceux qui ignorent cette appartenance (*VLAN unaware*).
- Les trames émises par les équipements *aware* sont marquées (*tagged*), celles émises par les équipements *unaware* ne sont pas marquées (*untagged*).

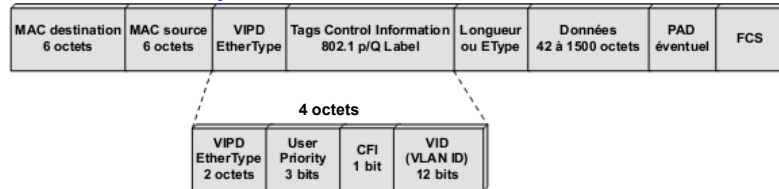
L'IDENTIFICATION DES VLAN (802.1Q)

Principe de l'étiquetage des trames

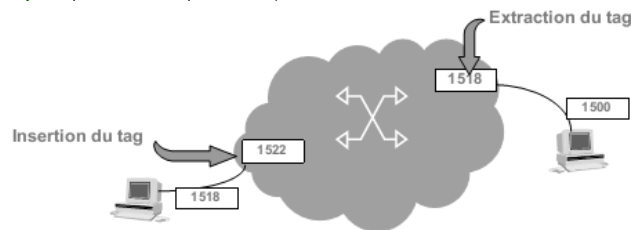


L'IDENTIFICATION DES VLAN (802.1Q)

La norme IEEE 802.1p/Q



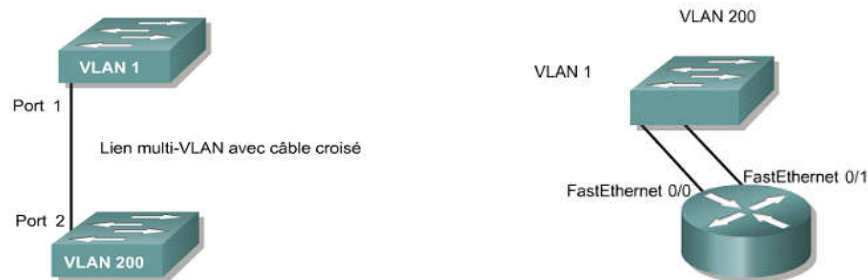
- Le champ **VIPD** (VLAN Protocol ID) il identifie le format 802.1 p/Q, sa valeur est fixée à **0x8100**.
- Le champ **priorité** (User Priority) : les 3 bits permettent de définir **8 niveaux de priorité**.
- Le bit **CFI** (Canonical Format Identifier) pour les réseaux **Ethernet = 0** et pour **Token Ring = 1**.
- Le champ **VID** (VLAN Identifier) sur **12 bits**, identifie le VLAN destination.



ROUTAGE INTER-VLAN

Introduction

- Les VLAN sont associés à des réseaux individuels. Ainsi, les unités réseau dans des VLAN différents ne peuvent pas communiquer directement sans l'intervention d'une unité de roulage de couche 3.
- Un routeur (ou un *Switch L3*) est nécessaire pour acheminer le trafic entre les VLAN. Sans unité de routage, le trafic entre VLAN est impossible.



ROUTAGE INTER-VLAN

Séparation des interfaces physiques en sous-interfaces

- Lorsque le nombre de VLAN augmente sur un réseau, l'approche physique consistant à utiliser une interface de routeur par VLAN devient vite limitée en termes d'évolutivité.
- Les réseaux contenant plusieurs VLAN doivent utiliser le mécanisme d'agrégation de VLAN pour affecter plusieurs VLAN à une interface physique de routeur unique.
- Chaque sous-interface logique (lignes en pointillé) prend en charge un VLAN et dispose d'une adresse IP affectée.

