Les VLAN

Introduction

Le protocole Ethernet, mis en place par l'IEEE, est un protocole de couche de liaison de données (Network access) de la suite TCP/IP qui décrit comment les machines, connectées à un réseau, formatent et transmettent les données afin que les autres machines du même réseau local (LAN) les reconnaissent et les traitent.
Généralement, on désigne par Ethernet la technologie filaire qui permet à deux machines connectées à l'aide d'un câble RJ45 (câble Ethernet) de communiquer dans un réseau local (LAN) en utilisant le protocole Ethernet.

Le protocole Ethernet définit la trame (frame) comme unité de transmission .Une trame comprend outre les données (charge utile) :

- Les adresses MAC de la source et du destinataire;
- Le marquage VLAN et certaines informations sur la qualité de service
- Les informations de correction d'erreurs survenues en cours de transmission

Avant l'arrivée du switch, la technologie Ethernet utilisait le hub qui présentait un inconvénient majeur : lorsqu'une trame arrive sur un port du hub, elle est diffusée sur tous les autres ports. Le message envoyé à un destinataire donné se répand sur tout le réseau.

L'utilisation du switch a permis de surmonter cet inconvénient. En effet, de par son fonctionnement, un switch ne transmet les trames que vers le port où est connectée la machine destinataire (sauf pour des trames de diffusions).De plus, si un switch de 12 ports est connecté par câble à un autre switch de 8 ports, par exemple, l'ensemble se comporte comme un seul switch de 18 ports (12 + 8 = 20 – 2 (pour la connexion)).

Cependant, pour des raisons de sécurité, on est parfois amené à séparer les abonnés d'un switch en plusieurs groupes en fonction du type de services par exemple. Une solution serait de faire des réseaux physiquement indépendants et donc d'utiliser plusieurs switchs (Un switch par groupe).Toutefois, cette solution est coûteuse et encombrante surtout quand il s'agit de groupes éloignés géographiquement. Une alternative à cette solution est d'utiliser un même switch tout en réalisant virtuellement l'indépendance des différents groupes. La technologie VLAN offre cette possibilité en permettant à l'administrateur réseau de définir logiquement dans le même réseau, des groupes indépendants appelés **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork).

Définition : Un **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork) est un réseau local virtuel. C'est une fonctionnalité qui permet de séparer des ports d'un switch pour former des réseaux différents. Les machines, connectées à des ports d'un même switch mais séparés en

différents groupes, ne peuvent pas communiquer ensemble. Tout se passe comme si l'on a coupé un switch en plusieurs morceaux formant chacun un switch.

La séparation des ports du switch en différents groupes, formant chacun un réseau virtuel, est effectuée par l'administrateur réseau à travers une interface web d'administration du switch. L'administrateur réseau déclare que des ports d'un switch appartiennent à un VLAN donné. Seules les machines d'un même VLAN peuvent communiquer ensemble. Les machines appartenant à des VLAN différents, ne peuvent pas communiquer ensemble. C'est la technologie VLAN par port.

L'association d'un VLAN à un port se fait par une table d'association. Il faut donc déclarer les VLANs sur le matériel. Prenons l'exemple illustré par la figure 1.

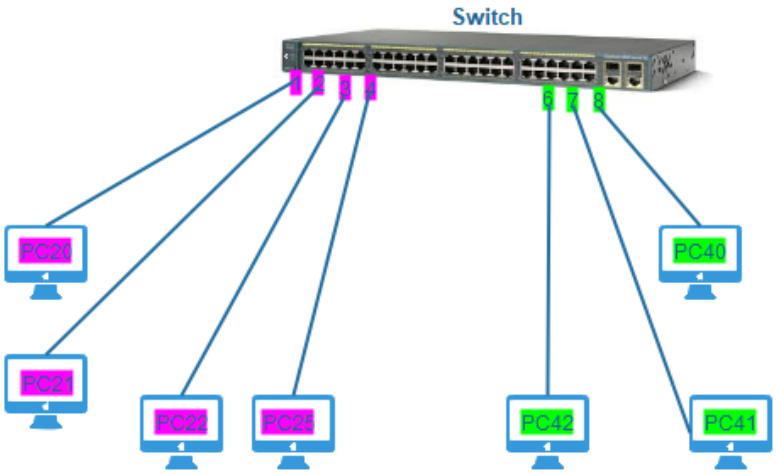

Figure 1: **VLAN** (Virtual Local Area Network)

Supposons que l'on désire grouper les machines PC20, PC21, Pc22 et PC25 connectées aux ports 1,2,3 et 4 (en rouge dans la figure) dans le VLAN 1 et les machines PC40, PC42,et PC42 aux ports 6,7et 8 (en vert dans la figure) dans le VLAN 2. Pour ce faire, on va simplement configurer le switch comme indiqué dans le tableau de la figure 2.

1	1
2	1
3	1
4	1
6	2
7	2
8	2

Figure 2

PVID (Port VLAN Identifier) : Dans le cas de la technologie de VLAN par port, le PVID d'un port de switch est l'identifiant Vlan qui est associé à la trame entrante sur le switch par ce port. Le PVID permet donc de savoir dans quel VLAN se situe ce port sachant qu'un port ne peut avoir qu'un seul PVID.

Différents types de VLAN

VLAN par défaut: Chaque port est associé à un identifiant de VLAN. Par défaut, chaque port est associé au PVID 1, soit le VLAN 1. Lors de la mise en œuvre des VLAN sur un matériel au moins un VLAN doit être définit, d'où la nécessité du VLAN par défaut.

VLAN utilisateur : Ce sont les VLANs qui sont déclarés pour une utilisation courante.

VLAN de management : C'est le VLAN utilisé par les équipements réseaux pour échanger leurs trames de contrôle et de management (OSPF, RIP, Spanning-Tree, etc). C'est aussi le VLAN utilisé par l'administrateur pour se connecter sur les équipements afin de les administrer. Généralement le VLAN de management par défaut est le VLAN 1.

VLAN natif : la notion de VLAN natif entre en compte dans le cas d'association de VLAN par port. Cela correspond au PVID sur port trunk. Ainsi lorsqu'un trame non taggué arrive sur un port trunk, elle sera associé à un VLAN en fonction du PVID du port. On dit alors que la trame est associé au VLAN natif du port

Trame Tagged et trame Untagged:

Une trame Ethernet peut être « tagguée » avec un numéro et ainsi être identifiée dans un VLAN. Si un appareil peut ajouter le numéro à une trame, le port auquel il est connecté devra être Tagged de son n° de VLAN. Lorsque celui communiquera avec le Switch, il ajoutera un identifiant dans la trame et le Switch pourra alors reconnaître l'appartenance à son VLAN et rediriger correctement le trafic. Si l'identifiant n'est pas reconnu, le trafic est supprimé.

Inversement, un ordinateur qui ne sait pas « tagguer » une trame devra être connectée à un port du Switch configuré en Untagged. C'est le switch qui identifiera ces trames et les renverra à d'autres ports identifiés sur le même VLAN.

Technologie VLAN par port

Dans la technologie VLAN par port, On définit les VLANs membres sur un port de type**:**

- **Access ou untagged:** Un port de type Access est configuré lorsqu'un seul VLAN transite par ce port et qu'il véhicule du trafic Untagged. Ce type de configuration est utilisé pour connecter une machine qui n'est pas en mesure d'identifier les paquets Ethernets (Un PC par exemple).
- **Hybrid :** Un port de type Hybrid, autorise le trafic Untagged et Tagged de plusieurs VLANs.
- **Trunk** : Un port de type Trunk transporte le trafic en VLAN Tagged à l'exception du PVID qui sera Untagged. Ce type de port est utilisé pour interconnecter des switchs.
- **Par défaut**, le type de port est configuré en **Access et sur le VLAN 1.**