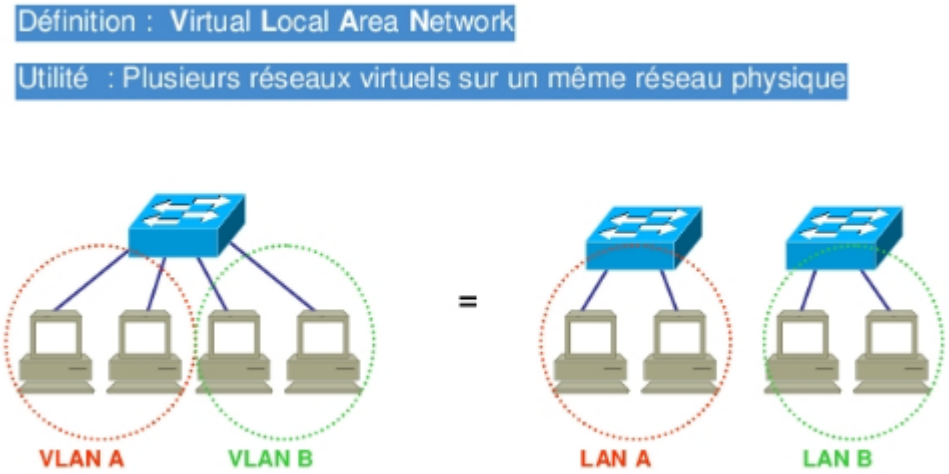
LES VLAN

Le principe

Un VLAN (Virtual LAN) ou réseau virtuel s'apparente à un regroupement d'équipements indépendamment de la localisation géographique sur le réseau. Ces équipements pourront communiquer comme si ils étaient sur le même segment. Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN.

Les VLAN n'ont été réalisables qu'avec l'apparition des commutateurs. Auparavant, pour constituer des domaines de diffusion, il était nécessaire de créer autant de réseaux physiques, reliés par l'intermédiaire de routeurs, solution contraignante car elle était fortement liée à la localisation géographique des stations. En ce sens, les vlan ont révolutionné le concept de segmentation des réseaux. Ils permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques.



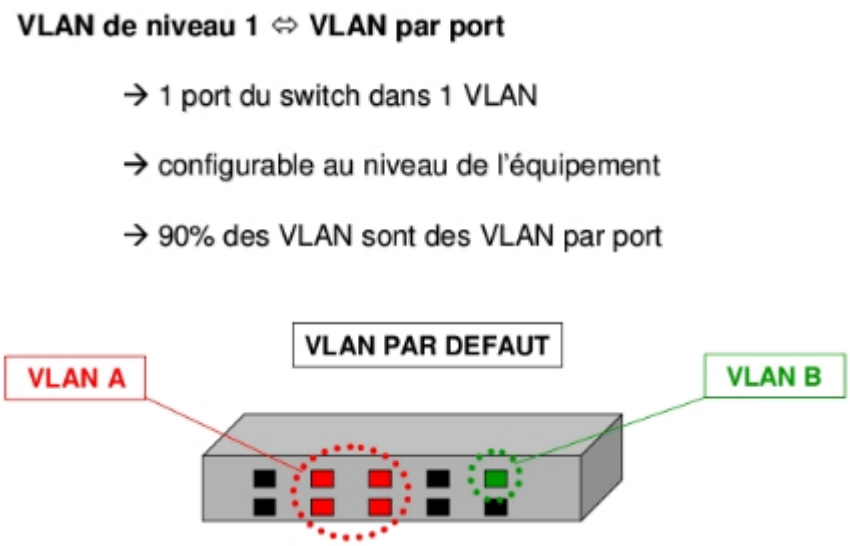
Les types de VLAN

Il existe plusieurs méthodes de construction des VLAN :

- par port
- par adresse IEEE (adresse MAC)
- par sous-réseau

VLAN par port

Un VLAN par port, aussi appelé VLAN de niveau 1 (pour physique), est obtenu en associant chaque port du commutateur à un VLAN particulier. C'est une solution simple, qui a été rapidement mise en oeuvre par les constructeurs.



Les premières implémentations ne permettaient pas de créer un même VLAN sur plusieurs commutateurs. Depuis une nouvelle génération de commutateurs permet de réaliser d'un tel VLAN, grace à l'échange d'informations entre les commutateurs et au marquage des trames. Les VLAN par port manquent de souplesse. Tout déplacement d'une station nécessite une reconfiguration des ports. De plus, toutes les stations reliées sur un port par l'intermédiaire d'un concentrateur, appartiennent au même VLAN.

VLAN par adresse IEEE (par adresse MAC)

Un VLAN par adresse IEEE, ou VLAN de niveau 2 est constitué en associant les adresses MAC des stations à chaque VLAN.

Le switch gère une table de ce type :

ADRESSE MAC	N° VLAN
...	...

L'intérêt de ce type de VLAN est surtout l'indépendance vis à vis de la localisation. La station peut être déplacée sur le réseau physique, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN. Les VLAN par adresse MAC sont très adaptés à l'utilisation de stations portables. La configuration peut s'avérer rapidement fastidieuse puisqu'elle nécessite de renseigner une table de correspondance avec toutes les adresses du réseau. Cette table doit aussi être partagée par tous les commutateurs, ce qui peut engendrer un trafic supplémentaire sur le réseau. Cette solution reste peu utilisée car elle manque de souplesse.

VLAN par sous-réseau (routage inter-vlan)

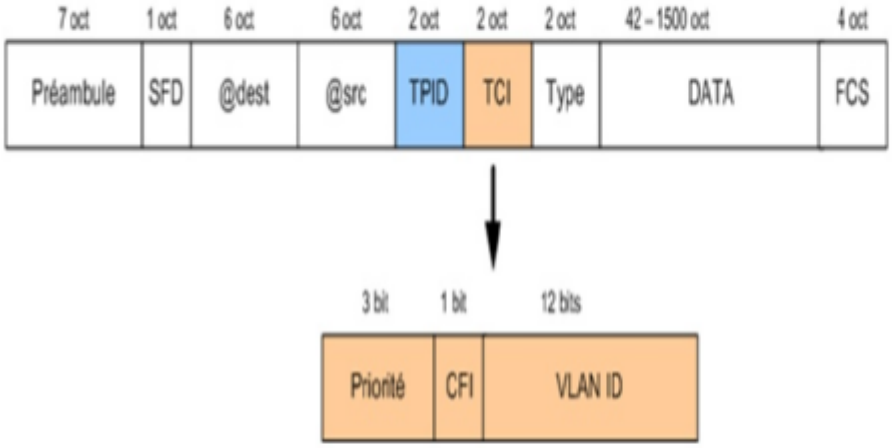
Un chapitre sera dédié au routage inter-vlan. Egalement appelé VLAN de niveau 3 et variante des précédents, un VLAN par sous-réseau utilise les adresses IP sources des datagrammes émis. Un réseau virtuel est associé à chaque sous-réseau IP. Dans ce cas, les commutateurs apprennent automatiquement la configuration des VLAN et il est possible de changer une station de place sans reconfiguration des VLAN. Cette solution est l'une des plus intéressantes, malgré une légère dégradation des performances de la commutation dûe à l'analyse des informations de niveau réseau (niveau 3).

Le marquage

Le marquage permet de reconnaître le VLAN d'origine d'une trame. Il peut être implicite, c'est-à-dire que l'appartenance à tel ou tel VLAN peut être déduite des informations contenues dans la trame (adresse IEEE, protocole, sous-réseau IP) ou par son origine (port). Il peut être explicite, dans ce cas qu'une information souvent un numéro de VLAN est insérée dans la trame. La définition de VLAN à travers plusieurs commutateurs se complique. Tout dépend du type de VLAN. Plusieurs solutions constructeurs ont été proposées telle que InterSwitch Link Protocol de Cisco, toutes incompatibles entre elles. Pour cette raison, l'IEEE a défini une norme de définition des VLAN sous la référence 802.1Q.

La Trame 802.1Q

La norme 802.1Q rajoute deux champs à l'entête de protocole de niveau 2 (Ethernet ou Token-Ring) appelés tag. Voici l'exemple d'une trame Ethernet pour laquelle les champs TPID et TCI ont été ajoutés :



Le champ TPID détermine le type du tag, 0x8100 pour 802.1Q, ce champ est utilisé pour prévoir des évolutions futures afin de pouvoir utiliser le principe du tagging pour différentes fonctionnalités.

Le champ TCI se décline en plusieurs éléments :

- Priorité: niveaux de priorité définis par l'IEEE 802.1P. Ce champ permet de réaliser une priorisation des flux. Le champ étant sur trois bits il est possible de déterminer 7 niveaux de priorité.

- CFI: Ce bit permet de déterminer si le tag s'applique à une trame de type Ethernet ou Token-Ring.

- VID: VLAN identifier. C'est l'identifiant du VLAN. L'appartenance d'une trame à un VLAN se fait grâce à cet identifiant. Le champ étant sur 12 bits, il est donc possible de déclarer jusqu'à 4096 VLANs.

Les avantages

Les réseaux virtuels amènent beaucoup d'avantages :

- réduction de la diffusion du trafic (les trames de broadcast ne traversent pas les Vlan)
- création de groupes de travail indépendamment de l'infrastructure physique
  - séparation des flux de trafic en fonction de leur nature (données, voix/vidéo)
  - contrôle des échanges inter-VLAN

  Les messages de diffusion (broadcast) sont limités à l'intérieur de chaque VLAN. Ainsi les broadcasts d'un serveur peuvent être limités aux clients de ce serveur.

  Des groupes de stations peuvent être réalisés sans remettre en cause l'architecture physique du réseau. De plus, un membre de ce groupe peut se déplacer sans changer de réseau virtuel. Dans le cas de VLAN par adresse IEEE ou par sous-réseau IP, il n'y a pas de reconfiguration des commutateurs. Les échanges inter-VLAN se réalisent tout comme des échanges inter-réseaux, c'est-à-dire au travers de routeurs. Il est par conséquent possible de mettre en oeuvre un filtrage du trafic échangés entre les VLAN.