

NETWORKS - VLAN

VLAN (Virtual Local Area Network).....	2
VLAN PORT.....	2
VLAN TRUNK.....	2
VLAN TAG.....	2
Le Switch de Niveau 3 (Layer 3 / Multilayer Switch).....	2
Subnetting vs. VLAN.....	3
Avantages et Inconvénients.....	3
Subnetting (Couche 3).....	3
VLAN (Couche 2).....	3

VLAN (Virtual Local Area Network)

C'est une technologie qui permet de découper un commutateur (switch) physique en plusieurs réseaux logiques indépendants.

Limiter les domaines de diffusion (Broadcast) : Sans VLAN, une trame de diffusion (envoyée à tout le monde, comme une requête ARP) est reçue par *toutes* les machines du switch. Avec un VLAN, la diffusion reste bloquée à l'intérieur de ce VLAN.

La Sécurité et la Confidentialité : Les environnements sont isolés. **Une machine d'un VLAN ne peut pas voir les échanges d'un autre VLAN**, bien qu'elles partagent la même infrastructure physique.

La Souplesse : Cela évite de devoir refaire le câblage physique si on veut changer l'organisation du réseau. C'est plus simple que de gérer des routeurs et des sous-réseaux complexes physiquement.

VLAN PORT

L'administrateur réseau qui décide (access) quel port physique du commutateur appartient à quel VLAN. On associe un **numéro de VLAN** à un **numéro de port**.

C'est très sécurisé : Comme l'appartenance au VLAN dépend du *câble* physique branché sur le switch, un utilisateur malin ne peut pas changer de VLAN en trichant sur son adresse IP ou son adresse MAC (Spoofing). S'il est branché sur le port 1, il est dans le VLAN 1, point final.

C'est rigide : Si un utilisateur change de bureau, il se connecte sur une nouvelle prise murale reliée à un autre port du switch (donc potentiellement un autre VLAN). Il perdra ses accès habituels. L'administrateur doit intervenir physiquement ou reconfigurer le switch pour rétablir la connexion au bon réseau.

VLAN TRUNK

Le **Trunk** est un type de connexion spécial configuré sur un port qui permet de transporter **plusieurs VLANs** sur un seul câble physique. C'est un "tuyau" partagé.

VLAN TAG

Le **TAG** (Étiquetage 802.1Q), Il ajoute une **étiquette (Tag)** dans l'en-tête de la trame Ethernet. Cette étiquette contient le **VLAN ID** (sur 12 bits).

Il existe un **VLAN Natif** (généralement le VLAN 1 par défaut). Sur un lien Trunk, les trames qui appartiennent à ce VLAN Natif ne sont **pas taguées**.

Le Switch de Niveau 3 (Layer 3 / Multilayer Switch)

Le Routage Inter-VLAN Contrairement à un Switch L2 qui est bloqué dans son VLAN (il ne regarde que les adresses MAC), le Switch L3 peut lire les **adresses IP**. Il sert de **passerelle par défaut** (Gateway) pour les machines de chaque VLAN.

SVI (Switch Virtual Interface) Au lieu d'avoir des câbles physiques reliés à un routeur, le Switch L3 utilise des interfaces virtuelles internes.

- Pour chaque VLAN, on crée une interface virtuelle (ex: Interface Vlan 10).
- On lui donne une adresse IP (ex: 192.168.1.254).
- Cette IP (192.168.1.254) devient la passerelle pour tous les PC du VLAN 10.

Subnetting vs. VLAN

Attribut	Subnetting (Sous-réseautage)	VLAN (Réseau Local Virtuel)
Couche OSI	Couche 3 (Réseau) (via les adresses IP)	Couche 2 (Liaison de données)
Méthode de Segmentation	Logique (via l'adresse IP et le masque)	Virtuelle/Physique (via le port du commutateur ou l'adresse MAC)
Objectif Principal	Réduire la taille du domaine de diffusion (Broadcast) et optimiser l'utilisation de l'espace d'adressage IP.	Séparer les équipements dans des groupes logiques pour des raisons de sécurité et de gestion du trafic.
Communication Inter-Segment	Nécessite un Routeur (passerelle) pour le trafic entre sous-réseaux différents.	Nécessite un Routeur (pour le routage inter-VLAN) si les VLANs sont associés à des sous-réseaux IP différents.
Impact sur l'IP	Modifie la partie réseau de l'adresse IP (en modifiant le masque).	N'impacte pas l'adresse IP, mais place le trafic dans un "tunnel" ou une étiquette (tag) spécifique.

Avantages et Inconvénients

Chaque méthode a ses propres forces et faiblesses, ce qui justifie souvent leur **utilisation conjointe** dans les infrastructures modernes.

Subnetting (Couche 3)

Avantages	Inconvénients
Optimisation IP : Permet de découper un grand réseau en sous-réseaux plus petits, gaspillant moins d'adresses IP.	Rigidité Physique : Un sous-réseau est souvent lié à une zone géographique (ex: un bâtiment) ou à un routeur.
Filtrage de Trafic : Les routeurs peuvent facilement appliquer des règles de sécurité (ACLs) basées sur les plages IP.	Faible Sécurité Physique : Ne sépare pas physiquement le trafic sur un même commutateur (Layer 2).
Gestion du Broadcast : Réduit la taille des domaines de diffusion.	Complexité de Planification : Le calcul binaire pour le masque (CIDR) et les plages demande une bonne maîtrise.

VLAN (Couche 2)

Avantages	Inconvénients
Flexibilité : Un équipement peut être déplacé physiquement (changer de port de commutateur) tout en restant dans le même VLAN (et le même sous-réseau IP).	Nécessite des équipements coûteux : Requier des commutateurs de couche 2 ou 3 administrables, gérant la norme IEEE 802.1Q (tagging).
Sécurité : Isole complètement le trafic entre groupes (ex: Séparer les serveurs des postes utilisateurs), même s'ils sont sur le même commutateur.	Complexité de Configuration : Le <i>tagging</i> des ports et le routage inter-VLAN doivent être configurés avec précision.
Réduction du Broadcast : Chaque VLAN est un domaine de diffusion séparé.	Problèmes de Compatibilité : Les anciens équipements non administrables ou non compatibles 802.1Q ne peuvent pas être intégrés.