Les VLANs et le routage inter-VLAN

Cours rédigé par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

1. Qu'est-ce qu'un VLAN ?

Un VLAN (Virtual Local Area Network) est une segmentation logique d'un réseau physique. Il permet de regrouper des équipements dans un même domaine de broadcast, indépendamment de leur emplacement physique.

Sans VLAN, tous les équipements d'un switch partagent le même domaine de broadcast : une trame broadcast envoyée par un poste est reçue par tous les autres.

Avec les VLANs, on découpe ce domaine en plusieurs segments isolés. Un poste en VLAN 10 ne peut pas communiquer directement avec un poste en VLAN 20, même s'ils sont branchés sur le même switch physique.

Pourquoi segmenter ?

- **Sécurité** — isoler les services sensibles (serveurs, administration) du reste du réseau
- **Performance** — réduire la taille des domaines de broadcast
- **Organisation** — regrouper les équipements par fonction (RH, Informatique, Serveurs…)

2. Types de ports

Type	Rôle	Trafic
Access	Connecte un équipement terminal (PC, imprimante)	Non taggué — appartient à un seul VLAN
Trunk	Relie deux switches ou un switch à un routeur	Taggué 802.1Q — transporte plusieurs VLANs

Le standard **802.1Q** est le protocole utilisé pour taguer les trames sur un lien trunk. Il ajoute un champ de 4 octets dans l'en-tête Ethernet contenant l'identifiant du VLAN (VID).

Le **VLAN natif** est le seul VLAN dont les trames ne sont pas taggées sur un trunk. Par convention on lui attribue souvent un VLAN dédié (ex: VLAN 99) différent du VLAN 1 par défaut pour des raisons de sécurité.

3. Maquette de référence

La maquette suivante sera utilisée pour tous les exemples de cette page :

```
         [PC-RH]      [PC-IT]      [Serveur]
            |            |            |
         Fa0/1         Fa0/2         Fa0/3
            |            |            |
         +-------------------------------------+
         |          SW-CORE                    |
         |                           Gi0/1 (trunk)|
         +-------------------------------------+
                                     |
                                Gi0/0 (trunk)
                                     |
                               +---------------+
                               |    ROUTEUR    |
                               +---------------+

VLANs :
  VLAN 10 — USERS     → 192.168.10.0/24  (PC-RH sur Fa0/1)
  VLAN 20 — IT        → 192.168.20.0/24  (PC-IT sur Fa0/2)
  VLAN 30 — SERVEURS  → 192.168.30.0/24  (Serveur sur Fa0/3)
  VLAN 99 — NATIF     → non routé
```

4. Configuration des VLANs sur le switch

Créer les VLANs

```
SW-CORE# configure terminal

SW-CORE(config)# vlan 10
SW-CORE(config-vlan)# name USERS
SW-CORE(config)# vlan 20
SW-CORE(config-vlan)# name IT
SW-CORE(config)# vlan 30
SW-CORE(config-vlan)# name SERVEURS
SW-CORE(config)# vlan 99
SW-CORE(config-vlan)# name NATIF
```

Assigner les ports en mode access

```
SW-CORE(config)# interface FastEthernet0/1
```

```
SW-CORE(config-if)# switchport mode access
SW-CORE(config-if)# switchport access vlan 10
SW-CORE(config-if)# description PC-RH

SW-CORE(config)# interface FastEthernet0/2
SW-CORE(config-if)# switchport mode access
SW-CORE(config-if)# switchport access vlan 20
SW-CORE(config-if)# description PC-IT

SW-CORE(config)# interface FastEthernet0/3
SW-CORE(config-if)# switchport mode access
SW-CORE(config-if)# switchport access vlan 30
SW-CORE(config-if)# description Serveur
```

Configurer le port trunk vers le routeur

```
SW-CORE(config)# interface GigabitEthernet0/1
SW-CORE(config-if)# switchport mode trunk
SW-CORE(config-if)# switchport trunk allowed vlan 10,20,30,99
SW-CORE(config-if)# switchport trunk native vlan 99
SW-CORE(config-if)# description Trunk-vers-Routeur
```



Dans une topologie multi-switches, **chaque switch traversé par le trafic d'un VLAN doit avoir ce VLAN déclaré dans sa table locale**, même s'il ne possède aucun port access dans ce VLAN. Un switch qui ne connaît pas un VLAN supprimera les trames taggées correspondantes, même sur un lien trunk.

Exemple : si VLAN 30 doit transiter de SW1 vers SW3 en passant par SW2, les trois switches doivent avoir `vlan 30` configuré, et les liens trunk entre eux doivent autoriser ce VLAN avec `switchport trunk allowed vlan 30`.

La solution pour éviter de configurer manuellement chaque switch est d'utiliser le **VTP** (voir Mémo Cisco — section VTP).

5. Le routage inter-VLAN

Par défaut, deux VLANs différents ne peuvent pas communiquer entre eux — ils sont isolés au niveau L2. Pour permettre cette communication, il faut un équipement de **niveau 3** : un routeur ou un switch L3.

Il existe deux méthodes principales :

Méthode	Matériel	Avantages	Inconvénients
Router-on-a-Stick	Routeur + 1 interface trunk	Simple, peu de matériel	Goulot d'étranglement sur l'interface
Switch L3 (SVI)	Switch L3	Performances élevées, pas de routeur externe	Matériel plus coûteux

6. Router-on-a-Stick

Une seule interface physique du routeur est connectée au switch en mode trunk. On crée des **sous-interfaces** (une par VLAN) qui serviront de passerelle par défaut.

Configuration du routeur

```
ROUTEUR(config)# interface GigabitEthernet0/0
ROUTEUR(config-if)# no shutdown
ROUTEUR(config-if)# description Trunk-vers-Switch

ROUTEUR(config)# interface GigabitEthernet0/0.10
ROUTEUR(config-subif)# encapsulation dot1Q 10
ROUTEUR(config-subif)# ip address 192.168.10.1 255.255.255.0
ROUTEUR(config-subif)# description Gateway-VLAN10-USERS

ROUTEUR(config)# interface GigabitEthernet0/0.20
ROUTEUR(config-subif)# encapsulation dot1Q 20
ROUTEUR(config-subif)# ip address 192.168.20.1 255.255.255.0
ROUTEUR(config-subif)# description Gateway-VLAN20-IT

ROUTEUR(config)# interface GigabitEthernet0/0.30
ROUTEUR(config-subif)# encapsulation dot1Q 30
ROUTEUR(config-subif)# ip address 192.168.30.1 255.255.255.0
ROUTEUR(config-subif)# description Gateway-VLAN30-SERVEURS

ROUTEUR(config)# interface GigabitEthernet0/0.99
ROUTEUR(config-subif)# encapsulation dot1Q 99 native
ROUTEUR(config-subif)# description VLAN-Natif
```

Configuration des postes clients

Chaque PC doit avoir comme passerelle par défaut l'adresse IP de la sous-interface correspondant à son VLAN :

Équipement	IP	Masque	Passerelle
PC-RH (VLAN 10)	192.168.10.10	255.255.255.0	192.168.10.1
PC-IT (VLAN 20)	192.168.20.10	255.255.255.0	192.168.20.1
Serveur (VLAN 30)	192.168.30.10	255.255.255.0	192.168.30.1

7. Switch L3 (SVI)

Sur un switch L3, on active le routage IP et on crée des **SVI** (Switched Virtual Interface) — une interface virtuelle par VLAN qui sert de passerelle.

```
SW-CORE(config)# ip routing                          ! Active le routage IP

SW-CORE(config)# interface vlan 10
SW-CORE(config-if)# ip address 192.168.10.1 255.255.255.0
```

```
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# description Gateway-VLAN10

SW-CORE(config)# interface vlan 20
SW-CORE(config-if)# ip address 192.168.20.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# description Gateway-VLAN20

SW-CORE(config)# interface vlan 30
SW-CORE(config-if)# ip address 192.168.30.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# description Gateway-VLAN30
```

8. Vérification

```
show vlan brief                           ! Liste des VLANs et ports associés
show interfaces trunk                     ! Liens trunk actifs et VLANs
transportés
show ip route                             ! Table de routage (routeur ou
switch L3)
show interfaces vlan 10                   ! État d'une SVI

ping 192.168.20.10 source vlan 10         ! Test de routage inter-VLAN depuis
le switch
```

9. Points clés à retenir

- Un port **access** appartient à un seul VLAN, les trames ne sont pas taggées
- Un port **trunk** transporte plusieurs VLANs avec le tag 802.1Q
- Le **VLAN natif** ne doit pas être le VLAN 1 (sécurité)
- Sans routage, deux VLANs sont complètement isolés
- Le **Router-on-a-Stick** est simple mais limité en bande passante
- Le **switch L3 avec SVI** est plus performant pour les environnements de production

10. SVI, routes de retour et filtrage

Une SVI configurée n'est pas nécessairement opérationnelle : vérifier le VLAN, les ports actifs associés et le lien montant. Le VLAN Bastion de l'exemple utilise 192.168.3.208/29, avec la passerelle 192.168.3.214.

Le routage inter-VLAN sur un switch L3 peut permettre un échange sans traverser le pare-feu. La création d'un VLAN dédié ne suffit donc pas à imposer le passage par un bastion : appliquer le filtrage sur le chemin réel.

```
show ip interface brief
show interfaces trunk
```

```
show ip route
show access-lists
```

Contrôler également les routes de retour sur le pare-feu. Voir IPv4 et VLSM et Bastion Guacamole.

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:cisco:cours:cours_vlans

Last update: **2026/10/18 01:23**