

CCNA09 - VLANs et Trunking

Nº ID	DS-242
≡ Compétence(s)	
≡ Type	

1. Introduction aux VLANs

Dans un réseau classique sans VLAN, tous les équipements connectés à un switch appartiennent au **même domaine de broadcast**. Cela signifie que :

- tous les broadcasts sont diffusés à tous les ports
- la sécurité est limitée
- la performance diminue lorsque le réseau grandit

Les VLANs permettent de **segmenter logiquement un réseau**, même si les équipements sont branchés sur le même switch physique.

Un VLAN crée une séparation **logique**, indépendante du câblage.

2. Fonctionnement et intérêts des VLANs

Définition

Un **VLAN (Virtual Local Area Network)** est un réseau local virtuel qui permet de regrouper des équipements selon un critère logique :

- service (administration, RH, étudiants...)
- fonction
- niveau de sécurité

Chaque VLAN correspond à :

- un **domaine de broadcast distinct**
- généralement **un sous-réseau IP**

Intérêts des VLANs

Les VLANs permettent :

- de réduire les broadcasts
- d'améliorer la sécurité
- de mieux organiser le réseau
- de faciliter l'administration
- de préparer le routage inter-VLAN

Sans routage inter-VLAN, **deux VLANs ne peuvent pas communiquer entre eux**, même s'ils sont sur le même switch.

3. Ports access et ports trunk

Port access

Un **port access** :

- appartient à **un seul VLAN**
- est utilisé pour connecter des équipements finaux (PC, imprimantes...)
- ne transporte pas d'information de VLAN dans la trame

Un PC branché sur un port access **ignore totalement l'existence des VLANs**.

Port trunk

Un **port trunk** :

- transporte **plusieurs VLANs simultanément**
- est utilisé pour relier :
 - deux switches
 - un switch et un routeur
 - un switch et un switch L3

Pour distinguer les VLANs sur un trunk, on utilise une **encapsulation VLAN**.

4. Encapsulation ISL et 802.1Q

ISL (Inter-Switch Link)

- protocole propriétaire Cisco
- encapsule entièrement la trame Ethernet
- ajoute environ 30 octets
- **obsolète et non utilisé aujourd'hui**

802.1Q (dot1Q)

- standard IEEE
- utilisé sur tous les équipements modernes
- ajoute **un tag de 4 octets** dans la trame Ethernet
- compatible multi-constructeurs

Le tag 802.1Q contient notamment :

- l'identifiant du VLAN (VLAN ID de 1 à 4094)
- des informations de priorité (QoS)

VLAN natif

- le VLAN natif est **non tagué** sur un lien trunk
- par défaut, il s'agit du **VLAN 1**
- une mauvaise configuration du VLAN natif peut provoquer des failles de sécurité

5. Routage inter-VLAN

Par défaut, les VLANs sont **isolés**.

Pour permettre la communication entre VLANs, il faut mettre en place un **routage inter-VLAN**.

Deux méthodes existent :

1. Utiliser un **switch de niveau 3 (L3)**

2. Utiliser un **routeur avec un switch L2** (Router-on-a-Stick)

6. Commandes essentielles VLAN et trunk

Création d'un VLAN

```
Switch(config)# vlan 10
Switch(config-vlan)# name Admin
```

Associer un port à un VLAN (mode access)

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

Configuration d'un lien trunk

```
Switch(config)# interface FastEthernet0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20
```

Sur les équipements récents, l'encapsulation dot1Q est implicite.

7. Routage inter-VLAN avec un switch L3 (SVI)

Un **switch L3** permet de router directement entre VLANs grâce aux **SVI (Switched Virtual Interfaces)**.

Chaque VLAN possède une interface logique avec une adresse IP servant de passerelle.

Création d'une interface VLAN

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

```
Switch(config-if)# no shutdown
```

```
Switch(config)# interface vlan 20
```

```
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
```

```
Switch(config-if)# no shutdown
```

Activation du routage

```
Switch(config)# ip routing
```

```
SwitchA>enable
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#interface vlan 10
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SwitchA(config-if)#ip address 192.168.10.1 255.255.255.0
SwitchA(config-if)#shutdown
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
SwitchA(config-if)#no shutdown
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SwitchA(config-if)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SwitchA(config-if)#ip address 192.168.20.1 255.255.255.0
SwitchA(config-if)#shutdown
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
```

```
SwitchA(config-if)#no shutdown
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SwitchA(config-if)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SwitchA(config-if)#ip address 192.168.20.1 255.255.255.0
SwitchA(config-if)#shutdown
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
SwitchA(config-if)#no shutdown
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SwitchA(config-if)#exit
SwitchA(config)#ip routing
SwitchA(config)#exit
%SYS-5-CONFIG-I: Configured from console by console
SwitchA#write
Building configuration...
[OK]
SwitchA#
```

8. Routage inter-VLAN avec un switch L2 et un routeur (Router-on-a-Stick)

Cette méthode est utilisée lorsque :

- le switch est de niveau 2
- le routage est assuré par un routeur

Le principe :

- un **trunk** relie le switch au routeur

- le routeur utilise des **sous-interfaces**
- chaque sous-interface correspond à un VLAN

Configuration des sous-interfaces sur le routeur

```
Router(config)# interface GigabitEthernet0/0.100
Router(config-subif)# encapsulation dot1Q 100
Router(config-subif)# ip address 192.168.100.1 255.255.255.0
```

```
Router(config)# interface GigabitEthernet0/0.200
Router(config-subif)# encapsulation dot1Q 200
Router(config-subif)# ip address 192.168.200.1 255.255.255.0
```

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# no shutdown
```

9. Vérifications et bonnes pratiques

Vérification des VLANs

```
show vlan brief
```

```
SwitchA(config-if)#exit
SwitchA(config)#ip routing
SwitchA(config)#exit
SwitchA#
#SYS-5-COMFIG-1: Configured from console by console

SwitchA#write
Building configuration...
[OK]
SwitchA#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Gig0/1, Gig0/2

10   Admin                  active    Fa0/1
20   RM                     active    Fa0/2

1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trinet-default        active

SwitchA#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
-----
Fa0/24    on        802.1q          trunking    1

Port      Vlans allowed on trunk
Fa0/24    10,20

Port      Vlans allowed and active in management domain
Fa0/24    10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    10,20

SwitchA#
```

```
SwitchB#enable
SwitchB#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Gig0/1, Gig0/2

10   Admin                  active    Fa0/1
20   RM                     active    Fa0/2

1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trinet-default        active

SwitchB#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
-----
Fa0/24    on        802.1q          trunking    1

Port      Vlans allowed on trunk
Fa0/24    10,20

Port      Vlans allowed and active in management domain
Fa0/24    10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    10,20

SwitchB#
```

Vérification du trunk

show interfaces trunk

Vérification côté routeur

show ip interface brief

Bonnes pratiques CCNA :

- toujours vérifier après configuration
- documenter les VLANs
- limiter les VLANs autorisés sur les trunks
- éviter l'utilisation du VLAN 1 pour les utilisateurs

10. Exercice de compréhension

Objectif

Mettre en place :

- deux VLANs
- un lien trunk
- un routage inter-VLAN

Travail demandé

- créer les VLANs
- associer les ports
- configurer le trunk
- configurer le routage
- vérifier la connectivité entre les machines

Commandes à maîtriser absolument pour le CCNA

- vlan
- switchport mode access
- switchport access vlan
- switchport mode trunk
- encapsulation dot1Q
- ip routing
- show vlan brief
- show interfaces trunk
- show ip interface brief