

Configuration du VLAN

Introduction :

Dans l'entreprise SmartTech, notre organisation du réseau repose sur une **architecture VLAN** (Virtual Local Area Network) afin de segmenter logiquement les différents zones (LAN, DMZ, Service Auth, ToIP, etc.). Cela permet une meilleure sécurité, une gestion plus fine du trafic, et une évolutivité accrue du réseau.

Pour permettre cette segmentation tout en assurant la communication entre les VLANs, la solution retenue est le **Router-on-a-Stick** : une seule interface physique du routeur est subdivisée en plusieurs **sous-interfaces** (une par VLAN), chacune configurée avec un identifiant VLAN via l'encapsulation **802.1Q**.

Configuration :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#no sh
R1(config-if)#in
*Mar  1 00:01:18.771: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:01:19.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R1(config-if)#int fa0/0.10
R1(config-subif)#encaps
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#
*Mar  1 00:01:57.059: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
```

```

R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#int fa0/0.20
R1(config-subif)#encaps
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#int fa0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#int fa0/0.50
R1(config-subif)#encapsulation dot1Q 50
R1(config-subif)#ip add 192.168.50.1 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#int fa0/0.100
R1(config-subif)#encapsulation dot1Q 100
R1(config-subif)#ip add 192.168.100.1 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#int fa0/0.200
R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#no sh

```

Le routeur R1 est configuré pour permettre la communication entre plusieurs VLANs en utilisant une seule interface physique (FastEthernet0/0) avec plusieurs sous-interfaces.

Cette configuration permet au routeur de servir de passerelle pour 6 VLANs différents, permettant ainsi la communication inter-VLAN. Chaque sous-interface agit comme la passerelle par défaut pour son VLAN respectif, avec une adresse IP dans le réseau correspondant (192.168.X.1 où X est le numéro du VLAN).

Port	VLAN	Type	EtherType
0	1	dot1q	
1	10	access	
2	20	access	
3	30	access	
4	50	access	
5	100	access	
6	200	access	

Port 0 :

- VLAN 1 (VLAN par défaut)
- Type : **dot1q** (trunk)
- Ce port est connecté au routeur pour le trafic inter-VLAN

Raison principale : Le port 0 doit transporter le trafic de **TOUS les VLANs** vers le routeur

Fonctionnement :

- Il reçoit des trames de différents VLANs (10, 20, 30, 50, 100, 200)

- Il doit "étiqueter" chaque trame avec son numéro de VLAN
- Le routeur pourra ainsi identifier à quel VLAN appartient chaque trame
- **Exemple** : Une trame du VLAN 10 sera taguée "VLAN 10" avant d'être envoyée au routeur

Ports 1-6 :

- VLANs : 10, 20, 30, 50, 100, 200
- Type : **access**
- Chaque port est assigné à un VLAN spécifique

Raison principale : Chaque port ne gère qu'**UN SEUL VLAN**

Fonctionnement :

- Port 1 → uniquement VLAN 10
- Port 2 → uniquement VLAN 20
- Port 3 → uniquement VLAN 30
- etc.

Pourquoi pas de tag ?

- Les équipements finaux (PC, imprimantes) ne comprennent pas les tags VLAN
- Le switch ajoute automatiquement le tag approprié quand la trame entre dans le switch
- Le switch retire le tag quand la trame sort vers l'équipement final

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
C    192.168.10.0/24 is directly connected, FastEthernet0/0.10
C    192.168.200.0/24 is directly connected, FastEthernet0/0.200
C    192.168.20.0/24 is directly connected, FastEthernet0/0.20
C    192.168.50.0/24 is directly connected, FastEthernet0/0.50
C    192.168.100.0/24 is directly connected, FastEthernet0/0.100
```

Explication des termes techniques

dot1q (802.1Q)

- **Définition** : Protocole standard IEEE pour le VLAN tagging
- **Fonction** : Ajoute un tag de 4 octets dans les trames Ethernet pour identifier le VLAN
- **Usage** : Utilisé sur les liens trunk pour transporter le trafic de plusieurs VLANs
- **Dans cette config** : Le port 0 du switch utilise dot1q pour envoyer le trafic tagué vers le routeur

Access

- **Définition** : Mode de port qui appartient à un seul VLAN
- **Fonction** : Les trames ne sont pas taguées, le port traite uniquement le trafic d'un VLAN spécifique
- **Usage** : Connecte les équipements finaux (PC, imprimantes, etc.)
- **Dans cette config** : Les ports 1-6 sont en mode access, chacun dédié à un VLAN

Architecture réseau complète

1. **Switch** : Sépare le trafic en VLANs et envoie tout via le port trunk (dot1q) vers le routeur
2. **Routeur** : Reçoit le trafic tagué et route entre les VLANs grâce aux sous-interfaces
3. **Communication** : Les équipements de VLANs différents peuvent communiquer via le routeur