

ROUTEUR

Objectif général

Assurer la gestion réseau de plusieurs VLAN, distribuer les adresses IP via DHCP, effectuer du routage inter-VLAN et fournir un accès Internet via NAT.

1. Architecture IP & VLAN

VLAN configurés

VLAN	Sous-interface	Réseau	Passerelle
VLAN 24	Gi0/1.24	192.168.24.0/24	192.168.24.254
VLAN 100	Gi0/1.100	192.168.100.0/24	192.168.100.254
VLAN 200	Gi0/1.200	192.168.101.0/24	192.168.101.254
VLAN 300	Gi0/1.300	192.168.102.0/24	192.168.102.254
VLAN 24 (autre lien)	Gi0/2.24	172.17.4.0/24	172.17.4.254

2. Services DHCP

Pools DHCP configurés

- **vlan100 → 192.168.100.0/24**
- **vlan200 → 192.168.101.0/24**
- **vlan300 → 192.168.102.0/24**
- **vlan24 → 172.17.4.0/24**
- **Plages exclues**

Pour éviter de distribuer les IP réservées :

192.168.24.1–20 • 192.168.100.1–20 • 192.168.101.1–20 • 192.168.102.1–20 • 172.17.4.2

3. Interfaces principales

Vers Internet

Gi0/0

- IP : 172.16.1.244/24
- NAT **outside**

Vers le switch (Trunk 802.1Q)

Gi0/1

- NAT **inside**
- Sous-interfaces pour VLAN 24,100,200,300

Deuxième trunk

Gi0/2.24

- VLAN 24 sur un autre lien trunk

4. NAT & Routage

NAT Overload configuré

Permet aux VLAN internes d'accéder à Internet via l'IP publique :

```
ip nat inside source list 10 interface Gi0/0 overload
```

ACL 10 autorise :

- 192.168.24.0/24
- 192.168.100.0/24
- 192.168.101.0/24
- 192.168.102.0/24
- 172.17.4.0/24

Route par défaut

```
ip route 0.0.0.0 0.0.0.0 172.16.1.254
```

(Passerelle du réseau opérateur)

5. Autres éléments

Accès

- SSH version 2 activé
- Console et VTY ouverts sans mot de passe (à sécuriser)

SWITCH

1. VLAN et Affectation des Ports

VLAN 100 (Accès utilisateur 1)

Ports : Fa0/1 → Fa0/12

Mode : access

VLAN 200 (Accès utilisateur 2)

Ports : Fa0/13 → Fa0/23

Mode : access

VLAN 300 (Native / Trunk)

Port Trunk : Fa0/24

- Native VLAN : 300
- VLAN autorisés : 100, 200, 300
- `switchport nonegotiate`
- `spanning-tree portfast trunk`

2. Interfaces VLAN (SVI)

Présentes mais pas utilisées pour le routage (seul le routeur effectue le routage inter-VLAN).

- Vlan1 : 192.168.1.2/24
- Vlan2 : 192.168.2.2/24
- Vlan100/200/300 : sans IP (Simple présence pour spanning-tree))

3. Spanning-Tree

- Mode : PVST
- **spanning-tree portfast** sur VLAN 100 & 200
- Port Trunk : PortFast activé

4. Services

- HTTP & HTTPS activés (à désactiver en production)
- Certificat auto-signé configuré (PKI)

5. Architecture Résumée

- VLAN 100 = utilisateurs
- VLAN 200 = utilisateurs
- VLAN 300 = native VLAN pour le trunk avec le routeur
- Fa0/24 = Trunk principal vers le routeur (Gi0/1)