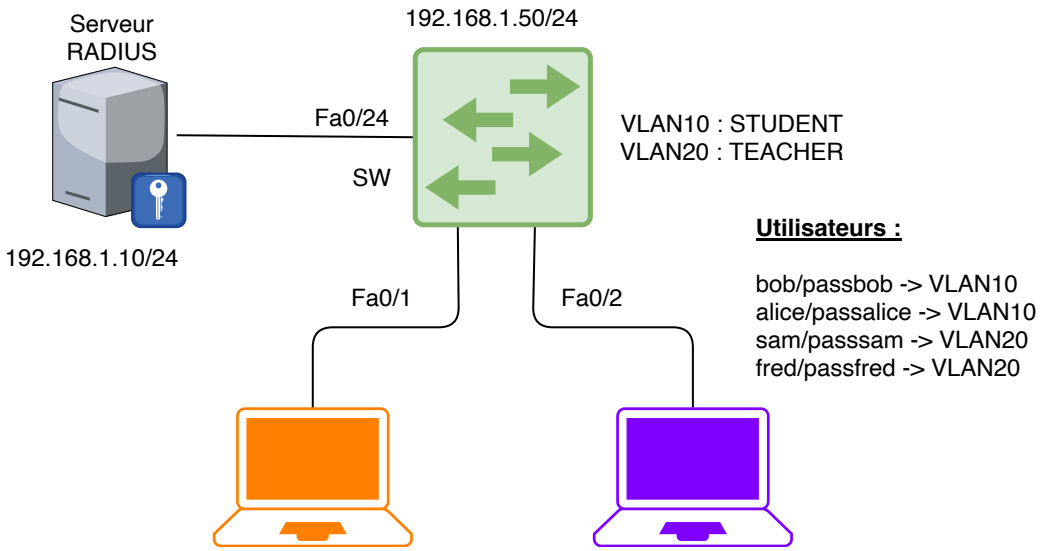
VLAN dynamique avec RADIUS

Topologie

1. Topologie utilisée



Topologie cohérente avec ton schéma, **en ajoutant explicitement un VLAN 99 pour le management** :

- Un **serveur RADIUS** (VM/CT sur Proxmox)
  - IP : `192.168.1.10/24`
  - VLAN : **99 (MGMT)**
- Un **switch Cisco**
  - IP de management : `192.168.1.50/24`
  - VLAN : **99 (MGMT)**
- Deux VLANs utilisateurs :
  - **VLAN 10 : STUDENT**
  - **VLAN 20 : TEACHER**
- Deux PC connectés au switch :
  - **Fa0/1** : PC étudiant (orange) → doit aller en VLAN 10
  - **Fa0/2** : PC professeur (violet) → doit aller en VLAN 20
- Port **Fa0/24** : vers le serveur RADIUS, en **access VLAN 99**

Utilisateurs demandés :

- `bob / passbob` → VLAN 10 (STUDENT)
- `alice / passalice` → VLAN 10 (STUDENT)
- `sam / passsam` → VLAN 20 (TEACHER)
- `fred / passfred` → VLAN 20 (TEACHER)

Réseau de management : `192.168.1.0/24` transporté sur **VLAN 99**.

2. Configuration du switch Cisco

2.1. Création des VLANs

```
! VLANs utilisateurs + VLAN de management
vlan 10
 name STUDENT
vlan 20
 name TEACHER
vlan 99
 name MGMT
```

2.2. Adresse IP de management du switch (VLAN 99)

```
! Interface SVI de management sur VLAN 99
interface Vlan99
 ip address 192.168.1.50 255.255.255.0
 no shutdown

! Passerelle par défaut du switch (routeur/firewall du réseau)
ip default-gateway 192.168.1.1
```

> Le routeur ou firewall relié quelque part au VLAN 99 doit avoir l'IP `192.168.1.1/24`.

2.3. Port vers le serveur RADIUS : Fa0/24 (VLAN 99)

On relie le serveur RADIUS au switch sur **Fa0/24**, dans **VLAN 99**.

```
interface FastEthernet0/24
 description Vers_Serveur_RADIUS_192.168.1.10
 switchport mode access
 switchport access vlan 99
 spanning-tree portfast
```

La carte réseau de la VM/CT RADIUS doit être configurée en :

- IP : `192.168.1.10`
- Masque : `255.255.255.0`
- Passerelle : `192.168.1.1` (optionnel selon ton besoin de sortie Internet)

2.4. Configuration RADIUS / AAA / 802.1X

```
! Activation du modèle AAA
aaa new-model
```

```
! Authentification 802.1X par défaut : via RADIUS
aaa authentication dot1x default group radius

! Autorisation réseau (prise en compte des attributs RADIUS, dont les
VLAN)
aaa authorization network default group radius

! Déclaration du serveur RADIUS (VM Proxmox)
radius-server host 192.168.1.10 auth-port 1812 acct-port 1813 key
SECRET123
radius-server timeout 5
radius-server retransmit 3
radius-server deadtime 10

! Activation globale de 802.1X sur le switch
dot1x system-auth-control
```

2.5. Ports utilisateurs (Fa0/1 et Fa0/2) – VLAN dynamique

Les ports **Fa0/1** et **Fa0/2** servent aux PC utilisateurs.
Ils sont contrôlés par RADIUS, qui décide de :

- VLAN 10 pour les comptes étudiants (bob, alice)
- VLAN 20 pour les comptes enseignants (sam, fred)

Pour simplifier, on applique la même configuration à **tous les ports utilisateurs** (Fa0/1 à Fa0/23).

```
interface range FastEthernet0/1 - 23
 description PORTS_UTILISATEURS
 switchport mode access

 ! Le port est contrôlé par 802.1X / RADIUS
 authentication port-control auto
 dot1x pae authenticator

 ! Méthode de secours : MAC Authentication Bypass (MAB)
 mab

 ! Si 802.1X échoue -> passer à MAB
 authentication event fail action next-method

 ! Si le serveur RADIUS est DOWN -> autoriser le port dans le VLAN 10
(VLAN de secours)
 authentication event server dead action authorize vlan 10

 ! Quand le serveur revient -> relancer une authentification
 authentication event server alive action reinitialize

 ! Port utilisateur : pas d'attente STP
 spanning-tree portfast
```

> Remarque importante :
> On **ne configure PAS** de `switchport access vlan 10` ou `20` sur ces ports.
> Le VLAN est **donné dynamiquement** par le serveur RADIUS via l'attribut `Tunnel-Private-Group-ID`.

3. Configuration FreeRADIUS sur la VM Proxmox (192.168.1.10)

3.1. Installation rapide (Debian/Ubuntu)

```
sudo apt update
sudo apt install freeradius freeradius-utils
```

Fichiers clés :

- `/etc/freeradius/3.0/clients.conf` → déclaration des clients RADIUS (ici le switch Cisco)
- `/etc/freeradius/3.0/users` → définition des utilisateurs et de leurs VLANs

3.2. Déclarer le switch dans `clients.conf`

```
client switch_cisco {
    ipaddr = 192.168.1.50        # IP de management du switch (VLAN 99)
    secret = SECRET123
    nas_type = cisco
}
```

3.3. Définir les comptes utilisateurs dans `users`

Conformément à ton schéma :

- `bob`, `alice` → VLAN 10 (STUDENT)
- `sam`, `fred` → VLAN 20 (TEACHER)

```
bob   Cleartext-Password := "passbob"
      Tunnel-Type := VLAN,
      Tunnel-Medium-Type := IEEE-802,
      Tunnel-Private-Group-ID := "10"

alice Cleartext-Password := "passalice"
      Tunnel-Type := VLAN,
      Tunnel-Medium-Type := IEEE-802,
      Tunnel-Private-Group-ID := "10"

sam   Cleartext-Password := "passsam"
      Tunnel-Type := VLAN,
      Tunnel-Medium-Type := IEEE-802,
      Tunnel-Private-Group-ID := "20"
```

```
fred  Cleartext-Password := "passfred"
      Tunnel-Type := VLAN,
      Tunnel-Medium-Type := IEEE-802,
      Tunnel-Private-Group-ID := "20"
```

Redémarrer FreeRADIUS :

```
sudo systemctl restart freeradius
```

3.4. Test RADIUS local (optionnel mais conseillé)

Depuis la VM RADIUS :

```
radtest bob passbob 127.0.0.1 0 SECRET123
```

Tu dois voir un `Access-Accept` avec les attributs `Tunnel-Private-Group-ID = 10`.

Même chose pour les autres comptes :

```
radtest alice passalice 127.0.0.1 0 SECRET123
radtest sam passsam 127.0.0.1 0 SECRET123
radtest fred passfred 127.0.0.1 0 SECRET123
```

4. Vérifications sur le switch

4.1. État des sessions d'authentification

```
show authentication sessions
show authentication sessions interface FastEthernet0/1
show dot1x interface FastEthernet0/1 details
```

Tu dois voir, par exemple :

- `bob` ou `alice` authentifié sur Fa0/1 ou Fa0/2 → VLAN 10
- `sam` ou `fred` authentifié → VLAN 20

4.2. Table MAC et VLANs

```
show mac address-table dynamic
show vlan brief
```

Les ports devraient apparaître dans :

- VLAN 10 pour les comptes étudiants
- VLAN 20 pour les comptes enseignants

5. Résumé pédagogique

- Le **VLAN 99** est explicitement le **VLAN de management** (switch + serveur RADIUS) dans le réseau `192.168.1.0/24`.
- Les **VLANs 10 et 20** sont réservés aux utilisateurs, et **ne portent pas d'IP sur le switch** (switch purement L2 pour ces VLANs).
- Le serveur **FreeRADIUS** décide dans quel VLAN placer chaque port en fonction de l'utilisateur, grâce aux attributs RADIUS :
  - `Tunnel-Type = VLAN`
  - `Tunnel-Medium-Type = IEEE-802`
  - `Tunnel-Private-Group-ID = "10"` ou `"20"`