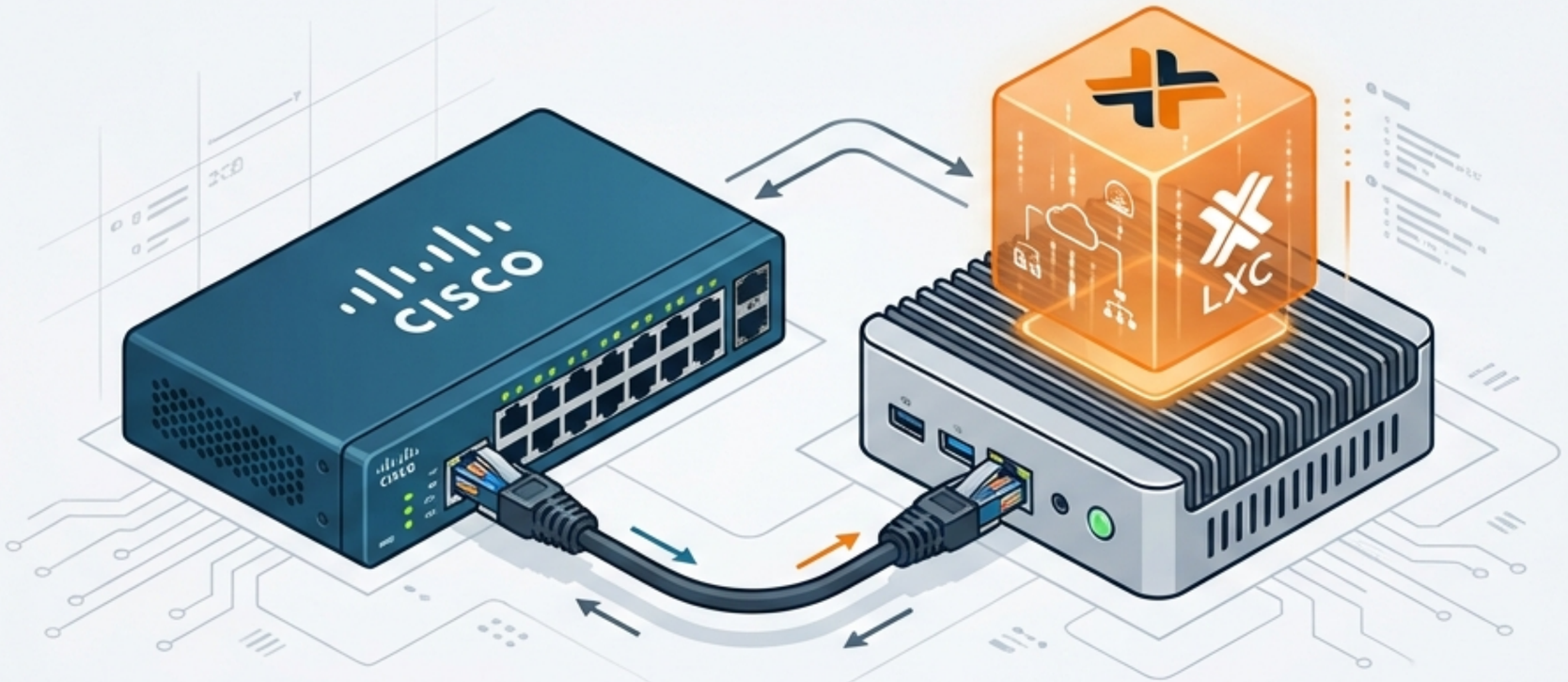
Mise en place de VLANs Dynamiques (802.1X)

Guide de configuration : Cisco Catalyst + FreeRADIUS sous Proxmox LXC

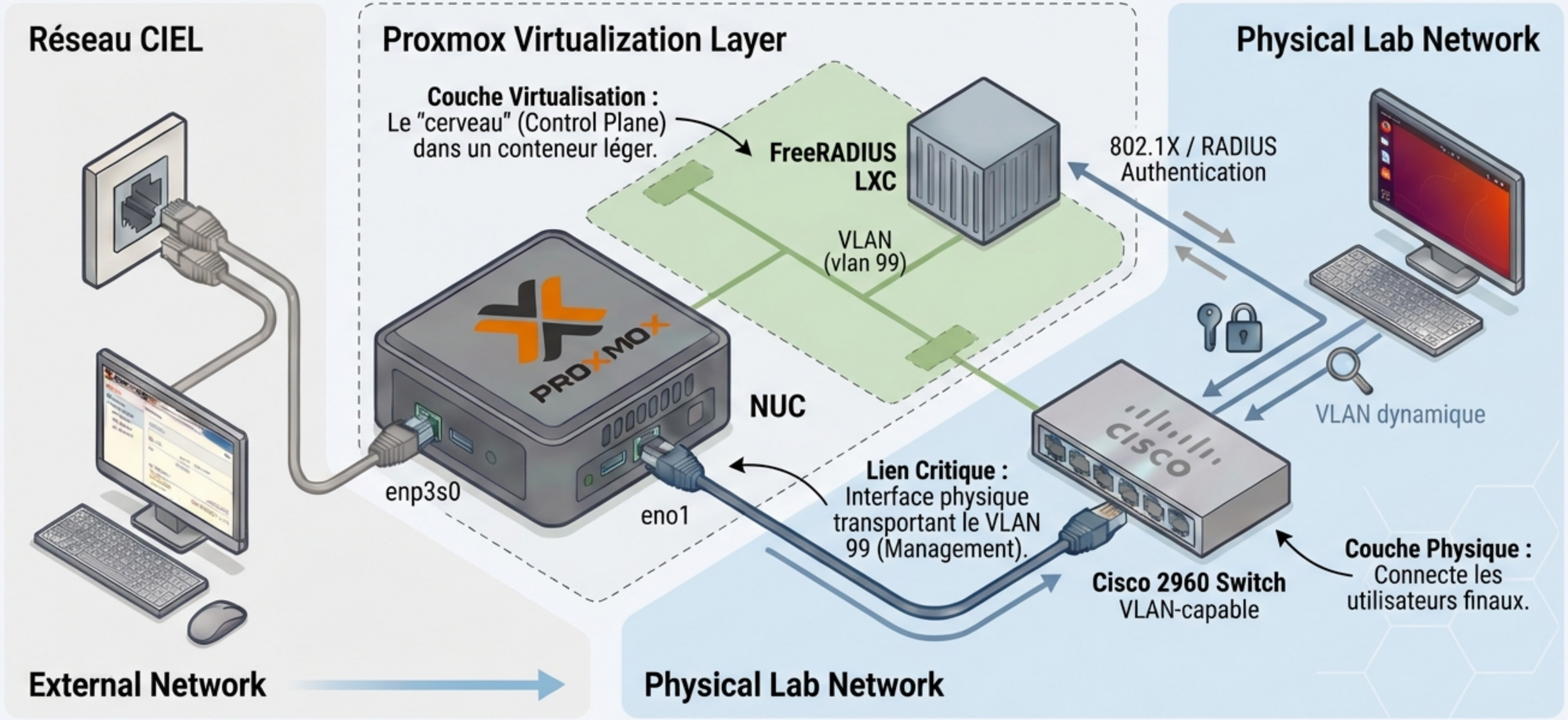


Objectif : Authentifier les utilisateurs et assigner dynamiquement les VLANs (10 Étudiants / 20 Professeurs).

Protocole : Standard IEEE 802.1X / RADIUS.

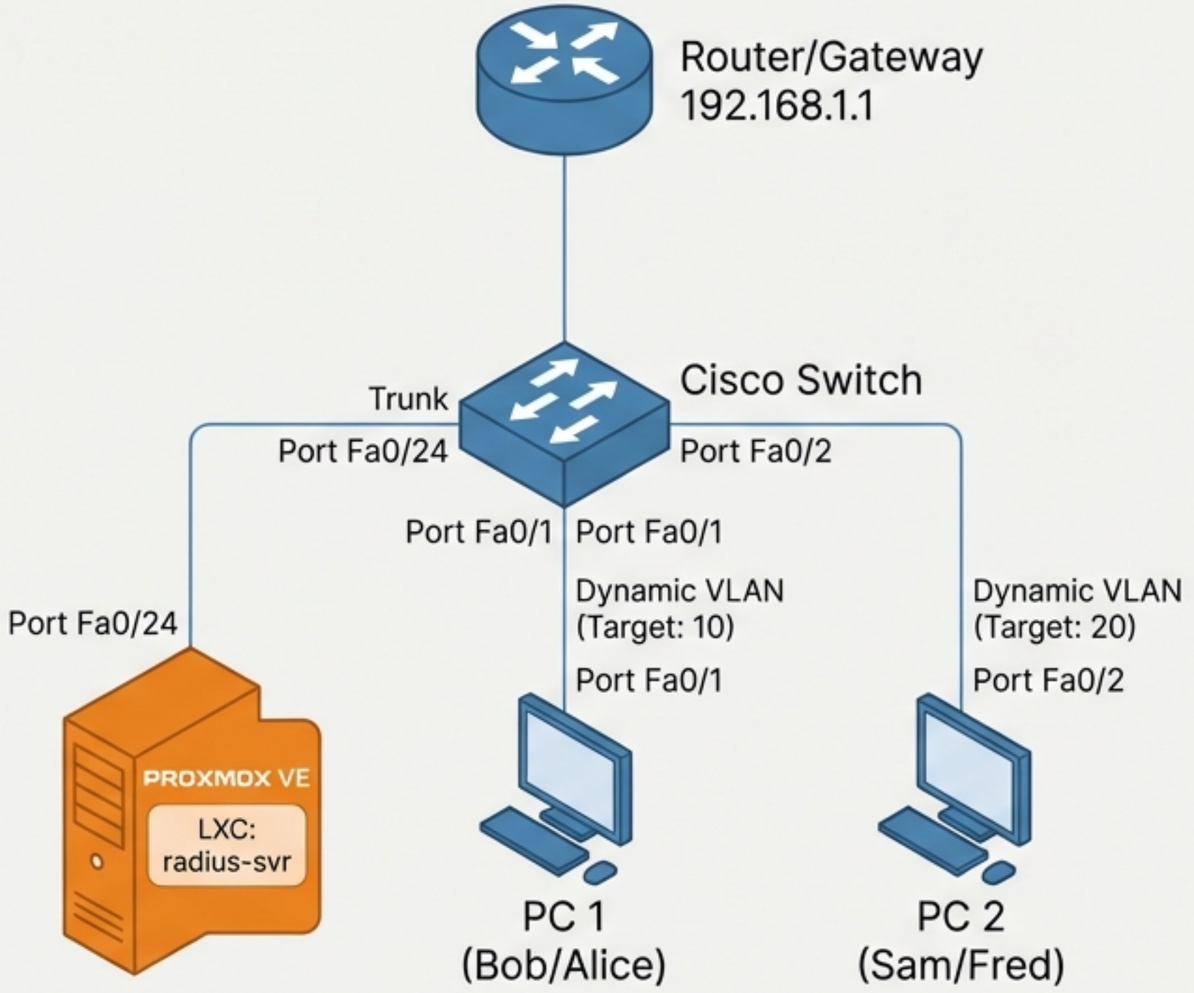
Infrastructure : Hybride (Switch Physique + Conteneur LXC Virtualisé).

Architecture Physique et Virtuelle



enp3s0: External Network Interface **eno1:** Lab Network Interface **LXC:** Linux Container **VLAN:** Virtual LAN **802.1X:** Network Access (

Topologie Logique et Plan d'Adressage

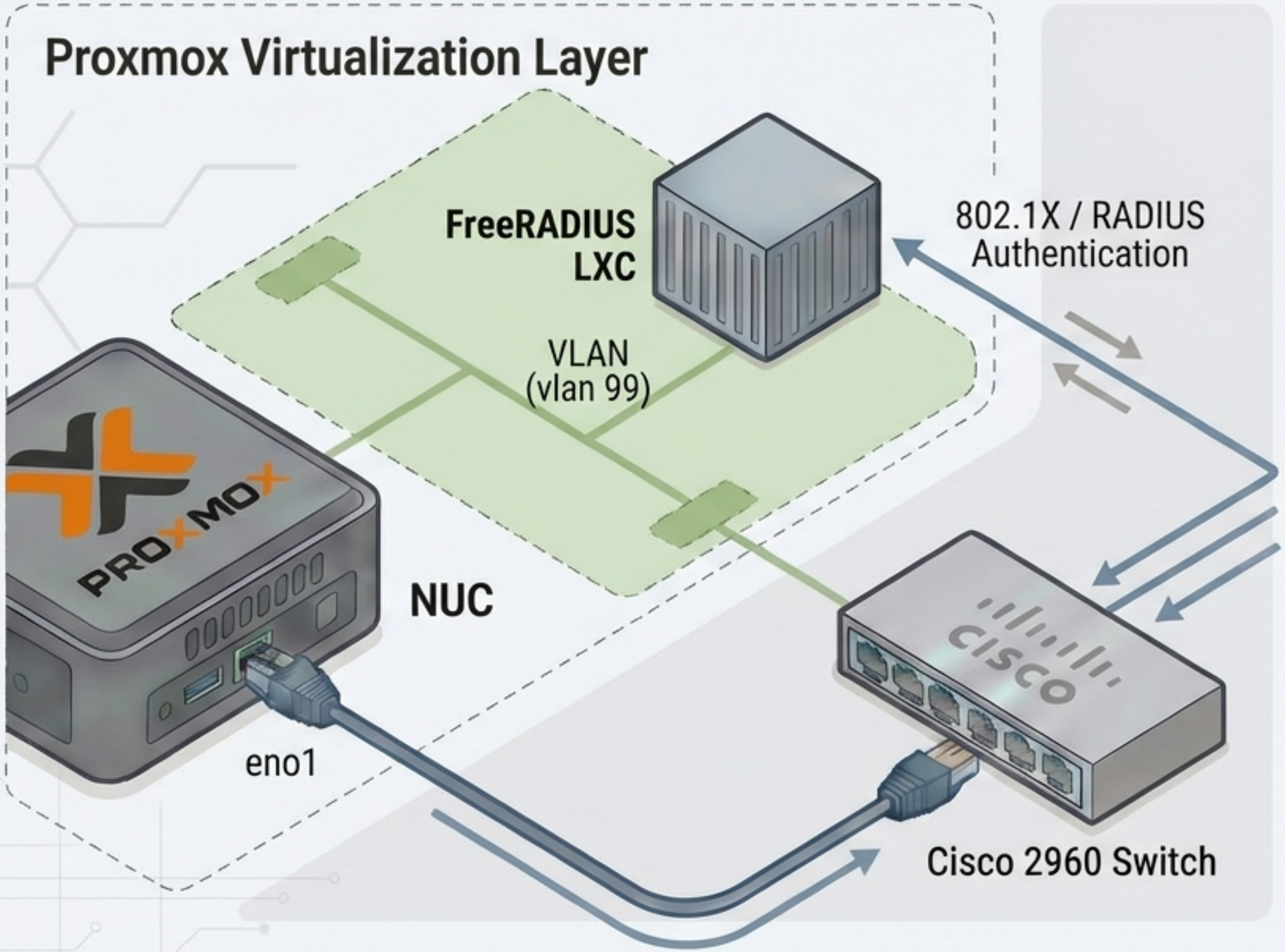


VLAN ID	Nom	Rôle	Sous-réseau
10	STUDENT	Utilisateurs (Bob, Alice)	Non routé (L2)
20	TEACHER	Utilisateurs (Sam, Fred)	Non routé (L2)
99	MGMT	Infrastructure	192.168.1.0/24

Configuration IP

```
Switch (SVI Vlan99): 192.168.1.50
RADIUS (LXC):        192.168.1.10
```

Le Cœur de l'Authentification : FreeRADIUS sur Proxmox



1. Infrastructure

NUC Intel exécutant Proxmox VE.

2. Service

Conteneur LXC exécutant le service FreeRADIUS.

3. Rôle

Reçoit les demandes d'accès du switch Cisco, vérifie les identifiants (User/Password), et renvoie les attributs d'autorisation (ex: ID du VLAN dynamique).

4. Flux Réseau

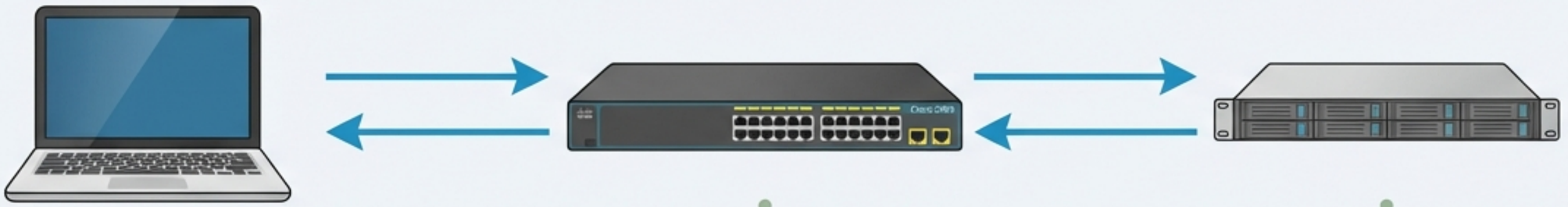
Le trafic RADIUS transite par l'interface physique 'eno1' vers le switch.

Le Mécanisme d'Authentification (802.1x Flow)

Supplicant
(PC Client)

Authentificateur
(Cisco 2960)

Serveur d'Authentification
(RADIUS)



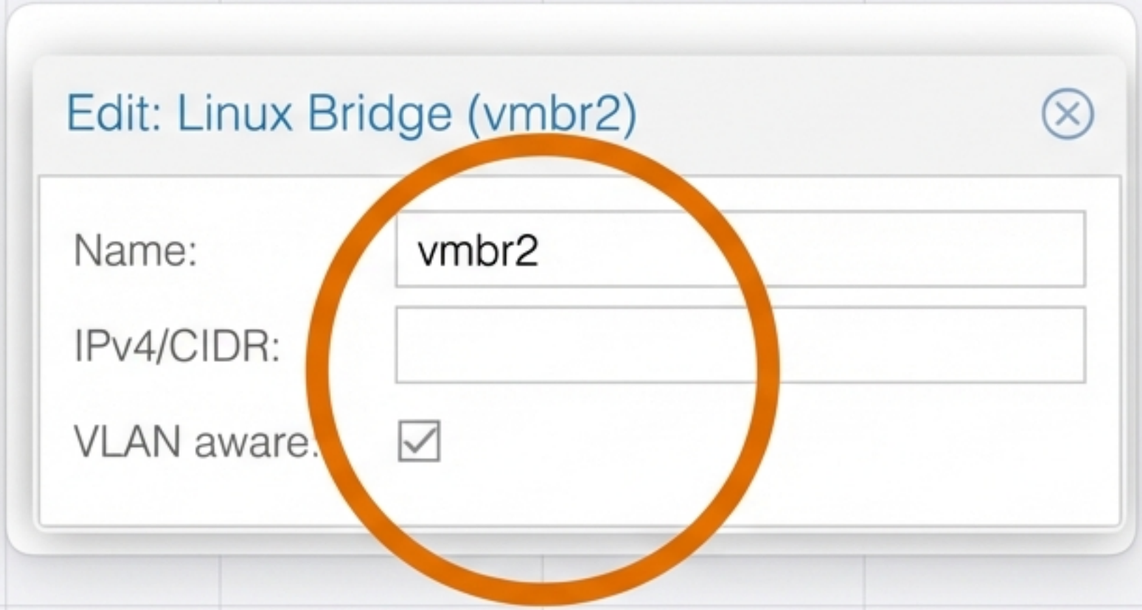
Tente de se connecter au port physique. L'accès est bloqué par défaut (Unauthorized State).

Intercepte la demande EAP, encapsule les identifiants dans des paquets RADIUS et les transmet au serveur.

Valide l'identité et autorise le switch à ouvrir le port et à assigner le VLAN approprié.

cisco

Préparation du Réseau Hôte (Proxmox)



Le Pont Linux (vmbr2)

Configuration spéciale : Ce pont agit comme un 'tuyau' transparent de niveau 2.

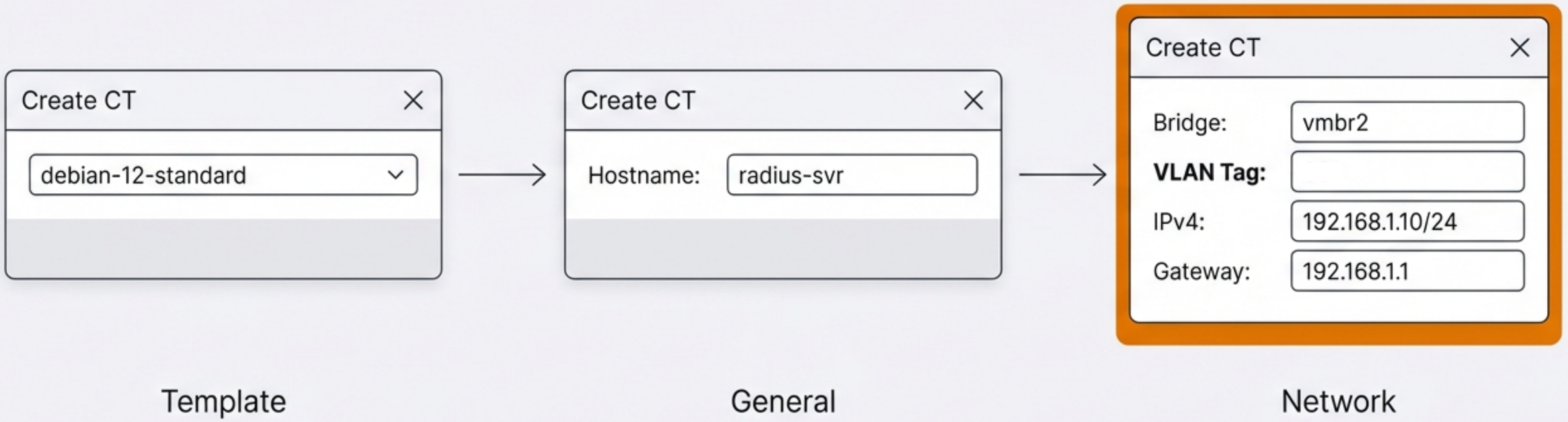
Pourquoi pas d'IP ?

Nous ne mettons PAS d'adresse IP sur vmbr2. Son seul but est de transporter les trames taguées (802.1Q) vers le conteneur sans interagir avec l'hôte Proxmox.

VLAN Aware

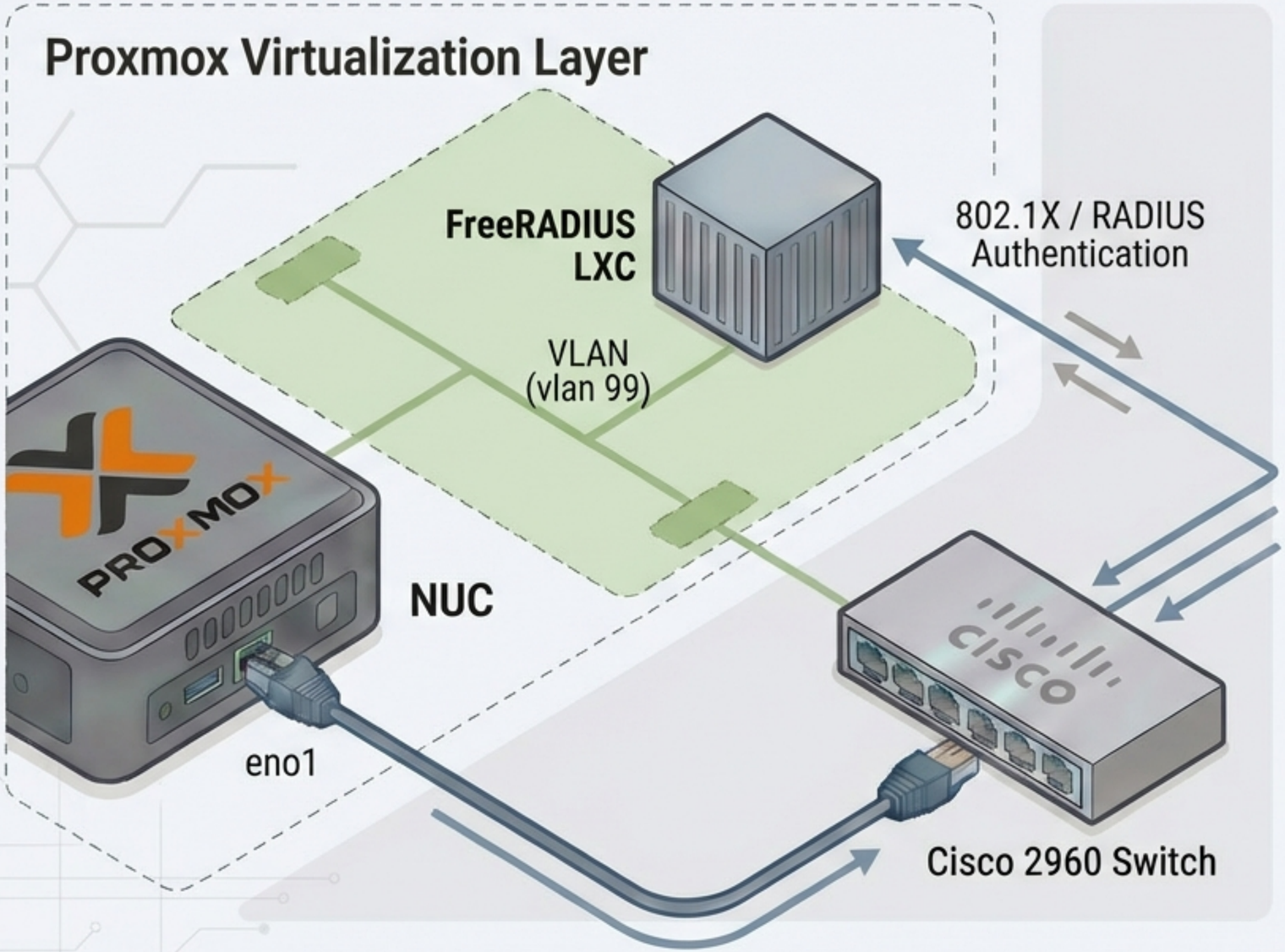
Indispensable pour préserver les tags VLAN (notamment le 99) entrants sur l'interface physique.

Déploiement du Conteneur FreeRADIUS (LXC)



Le Tag 99 place l'interface virtuelle directement dans le VLAN de Management. Architecture légère et performante.

Le Cœur de l'Authentification : FreeRADIUS sur Proxmox



1. Infrastructure

NUC Intel exécutant Proxmox VE.

2. Service

Conteneur LXC exécutant le service FreeRADIUS.

3. Rôle

Reçoit les demandes d'accès du switch Cisco, vérifie les identifiants (User/Password), et renvoie les attributs d'autorisation (ex: ID du VLAN dynamique).

4. Flux Réseau

Le trafic RADIUS transite par l'interface physique 'eno1' vers le switch.

Installation des Services FreeRADIUS

root@radius-svr

```
# 1. Mise à jour des paquets
apt update && apt upgrade -y

# 2. Installation du serveur et des outils de test
apt install freeradius freeradius-utils -y

# 3. Vérification du service
systemctl status freeradius
root@radius-svr:~# _
```

Packages requis

- **freeradius** : Le serveur d'authentification.
- **freeradius-utils** : Contient la commande 'radtest', indispensable pour le diagnostic.

Configuration FreeRADIUS : Déclaration du Client

Fichier : /etc/freeradius/3.0/clients.conf

```
client switch_cisco {
    ipaddr = 192.168.1.50 # IP de Management du Switch
    secret = SECRET123    # Clé partagée (PSK)
    nas_type = cisco
}
```

Doit correspondre à l'interface Vlan99 du switch.

Zone Critique : Ce mot de passe doit être identique côté Cisco.

Configuration FreeRADIUS : Utilisateurs et Attributs VLAN

Fichier : /etc/freeradius/3.0/users

VLAN 10 - Étudiants

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

VLAN 20 - Professeurs

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

Important : Appliquer les changements `systemctl restart freeradius`

Correction Critique : Transmission des attributs (PEAP)

Fichier : /etc/freeradius/3.0/mods-enabled/eap

Par défaut, FreeRADIUS ne sort pas les numéros de VLAN du tunnel chiffré PEAP. Le switch reçoit "OK" mais ne sait pas quel VLAN utiliser.

Une défaut ne sort port pas les numéros de VLAN du tunnel chiffré PEAP. switch reçoit ‘OK’ changez ‘OK’ mais ne pas quel VLAN utiliser.

INDISPENSABLE

```
peap {
    # ...
    default_eap_type = mschapv2
    copy_request_to_tunnel = yes
    use_tunneled_reply = yes  <-- CHANGEZ 'no' EN 'yes'
    # ...
}
```

Action : Redémarrez le service immédiatement.

Validation Locale (Test radtest)

Commande de Test

```
radtest bob passbob 127.0.0.1 0 testing123
```

Résultat Attendu

```
Sent Access-Request Id 212...
Received Access-Accept Id 212...
    Tunnel-Type:0 = VLAN
    Tunnel-Private-Group-Id:0 = '10'
```

Si ce test échoue, vérifiez les fichiers 'users' et 'clients.conf' avant de configurer le switch.

Switch Cisco : Configuration de Base et VLANs

Phase 1 : Adressage et Layer 2

Cisco CLI

```
Switch# conf t

! Configuration de l'interface de Management
Switch(config)# interface Vlan1
Switch(config-if)# ip address 192.168.1.50 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Activation AAA et VLANs
Switch(config)# aaa new-model
Switch(config)# vlan 10
Switch(config-vlan)# name student
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name teacher
```

Note : Utilisation du Vlan1 par défaut pour le management (IP .50).

Switch Cisco : Liaison AAA et Serveur RADIUS

Phase 2 : Le Cerveau

Cisco CLI

```
! Groupes AAA
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius

! Paramètres Serveur
Switch(config)# radius-server host 192.168.1.10 auth-port 1812
acct-port 1813 key SECRET123
Switch(config)# radius-server timeout 5
Switch(config)# radius-server retransmit 3
Switch(config)# radius-server deadtime 10

! Activation Globale
Switch(config)# dot1x system-auth-control
```

Switch Cisco : Configuration des Interfaces

Phase 3 : Uplink vs Client

Uplink vers Serveur (Fa0/24)

Cisco CLI

```
Switch(config)# interface fa 0/24
Switch(config-if)# switchport mode access
```

Port Utilisateur (Fa0/1)

Cisco CLI

```
Switch(config)# interface fa 0/1
Switch(config-if)# description PC_UTILISATEUR
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
```

Vérification et Diagnostic (Côté Switch)

Cisco CLI

```
Switch# show authentication sessions interface Fa0/1
Interface: FastEthernet0/1
  MAC Address: 0011.2233.4455
  User-Name: bob
  Status: Authz Success
  Domain: DATA
  Operational VLAN: 10
```

Status 'Unauthorized' ? Vérifiez le Secret partagé et la connectivité vers 192.168.1.10.

Vérification Finale et Diagnostic

```
show authentication sessions interface Fa0/1
Interface: FastEthernet0/1
MAC Address: 0011.2233.4455
User-Name:   bob
Status:      Authz Success
Method:      dot1x
```

```
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, Fa0/13, Fa0/8, Fa0/14,
                                               Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19,
                                               Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1,
                                               Gi0/2
10  STUDENT                           active   Fa0/1
20  TEACHER                           active   Fa0/2
```

Le port Fa0/1 a basculé automatiquement dans le VLAN 10 après l'authentification de Bob.

Validation Technique (Côté Switch)

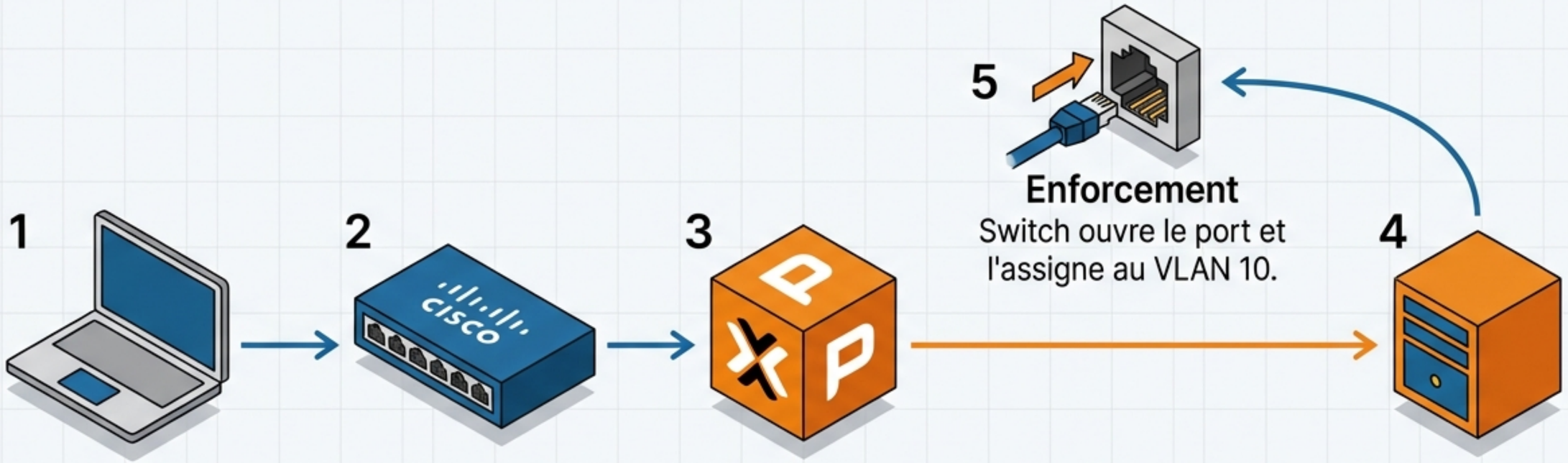
```
Switch# show dot1x all
Sysauthcontrol              : Enabled
Dot1x Protocol Version      : 3
Dot1x Protocol Prokemmme    : Enabled
Dot1x Protocol Data         : Enabled
```

```
Switch# show authentication sessions interface Fa0/1
Interface   : FastEthernet0/1
Status      : Authz Success
Method      : dot1x
UserName    : etudiant_ciel
```

Vérifiez que 'Sysauthcontrol' est bien à **Enabled**. C'est la preuve que la commande critique a été acceptée.

'Authz Success' confirme que le serveur RADIUS a validé les accès.

Résumé du Flux d'Authentification



Supplicant
Envoie identifiants (Bob/Pass).

Authenticator
Encapsule EAP dans RADIUS -> 192.168.1.10.

Transport
Passe le trafic via Vlan99.

RADIUS Server
Vérifie 'users', renvoie 'Access-Accept' + 'VLAN:10'.

Succès : Intégration transparente physique/virtuel.