Vallée Estéban & Zaimi Souhir — Document de validation d’AP4 — Campus Carlo Acutis
BTS SIO 1

Atelier Professionnel 4 - Segmentation du réseau

Sommaire

A.1 Réalisation du schéma réseau

Concevoir le schéma réseau logique de votre solution répondant au cahier des charges. Vous pourrez utiliser les outils tels que Visio ou Packet Tracer ou tout autre outil de conception.
Le réseau est segmenté en 8 VLANs répartis sur 3 étages :

- 2ème étage : VLAN 20 (Direction-DSI), VLAN 300 (Serveurs) avec le contrôleur de domaine hébergeant Active Directory, NextCloud et le service TFTP, ainsi qu'une salle de réunion en VLAN 150
- 1er étage : VLAN 10 (Réseau & Système), VLAN 30 (Administratif)
- RDC : VLAN 40 (Commercial), VLAN 50 (Développement), VLAN 200 (Démonstration) et une salle de réunion en VLAN 150 (Visiteurs)

Chaque étage dispose d'un switch Catalyst 2960 relié à la baie centrale. Un routeur Cisco 2911 assure le routage InterVLAN. Des points d'accès Wifi sont placés dans chaque salle de réunion pour le VLAN Visiteurs. Chaque VLAN dispose d'un poste client pour la validation des tests.

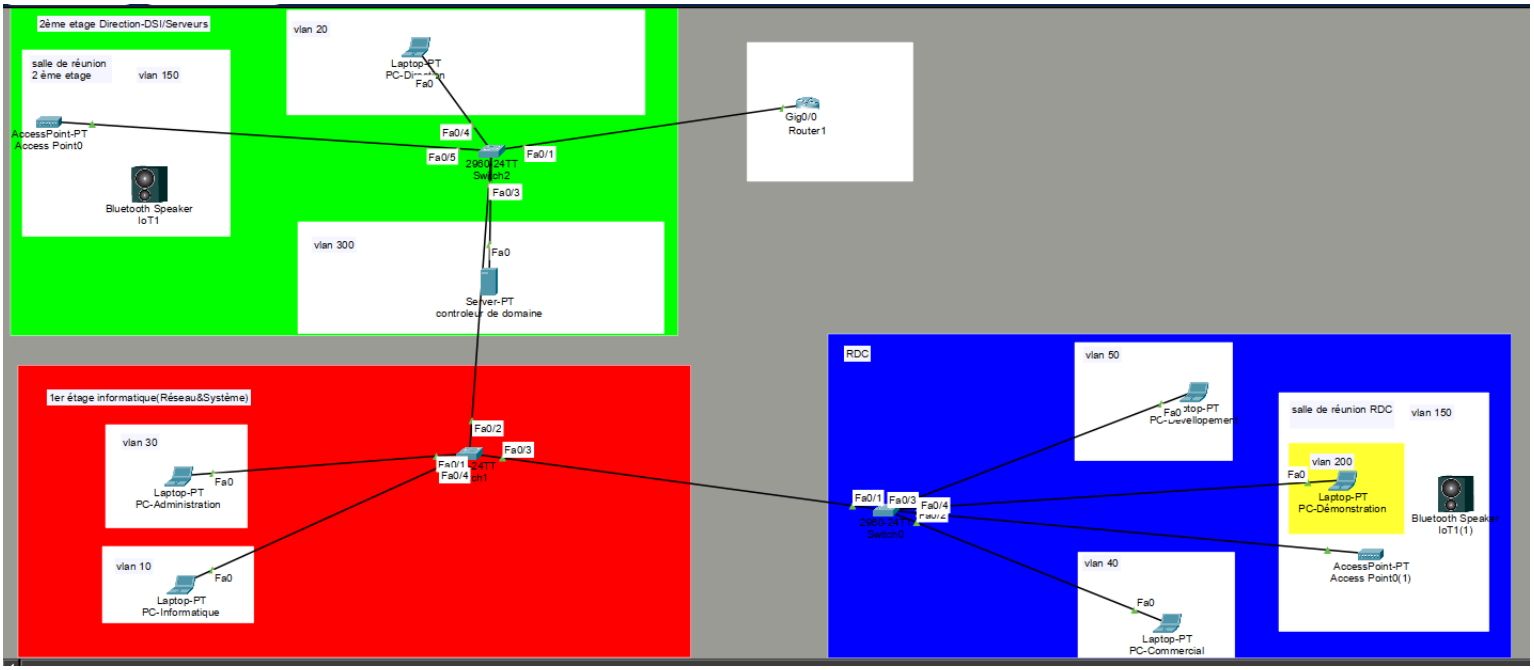


Schéma réseau de notre AP réalisé sur Cisco Packet Tracer

A.2 Mise en place de l’accès distant SSH

Dans le cadre du projet, il était nécessaire de permettre l’administration à distance des équipements réseau. Pour cela, le protocole SSH a été mis en place, car il permet une connexion sécurisée contrairement à Telnet, qui transmet les informations en clair.

La configuration a été réalisée directement sur le routeur. Dans un premier temps, un nom de domaine a été défini afin de pouvoir générer les clés de chiffrement nécessaires au fonctionnement de SSH. Ensuite, des clés RSA ont été créées pour sécuriser les échanges.

```
Switch(config)#hos
Switch(config)#hostname SwitchE2
SwitchE2(config)#ip domai
SwitchE2(config)#ip domain-n
SwitchE2(config)#ip domain-name mdl4.local
SwitchE2(config)#crypto k
SwitchE2(config)#crypto key gen
```

```
SwitchE2(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SwitchE2.mdl4.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 7 seconds)
```

```
SwitchE2(config)#line vty 0 4
SwitchE2(config-line)#login local
SwitchE2(config-line)#tran
SwitchE2(config-line)#transport ss
SwitchE2(config-line)#transport input ssh
SwitchE2(config-line)#
```

Liste des commandes effectuées pour mettre en place le SSH

Un compte administrateur a été configuré afin de permettre l'authentification lors de la connexion. L'accès aux lignes VTY a ensuite été paramétré pour n'autoriser que les connexions en SSH, ce qui permet de bloquer totalement l'utilisation de Telnet.

Afin de respecter le cahier des charges, l'accès à l'administration à distance a été restreint uniquement aux machines du VLAN Réseau & Système. Une règle spécifique a également été ajoutée pour bloquer l'accès au stagiaire disposant de l'adresse IP 192.168.10.1. Cette restriction a été mise en place grâce à une ACL appliquée sur les lignes VTY.

Des tests ont ensuite été réalisés afin de vérifier le bon fonctionnement du dispositif. La connexion SSH fonctionne correctement depuis un poste autorisé, tandis qu'elle est refusée pour les machines non autorisées, notamment celle du stagiaire.

Cette configuration permet donc de sécuriser efficacement l'accès aux équipements réseau tout en respectant les contraintes de sécurité imposées dans le projet.

A.3 Création des Vlan

Paramétrer individuellement les différents switches en respectant le cahier des charges et les informations de nommage fournies :

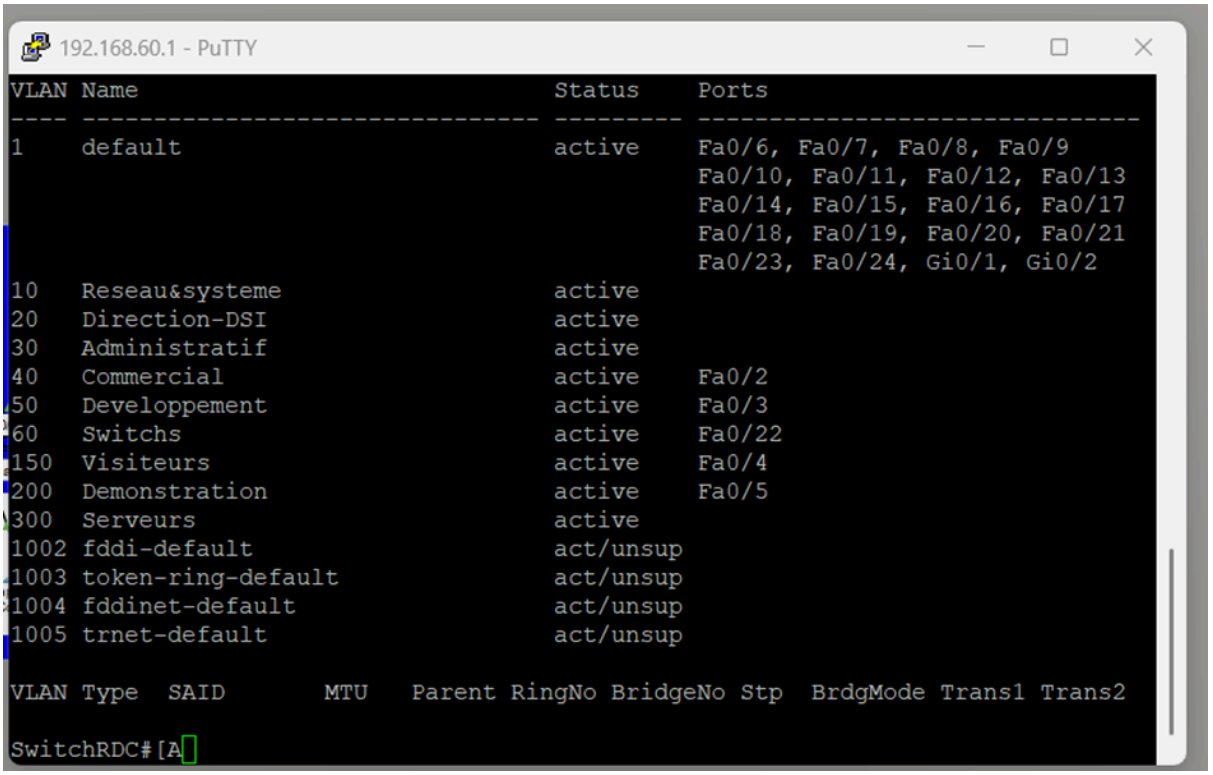
Dans notre infrastructure, le switch du 2ème étage a été configuré en tant que serveur VTP, tandis que les deux autres switchs (dont le switch RDC) jouent le rôle de clients VTP.

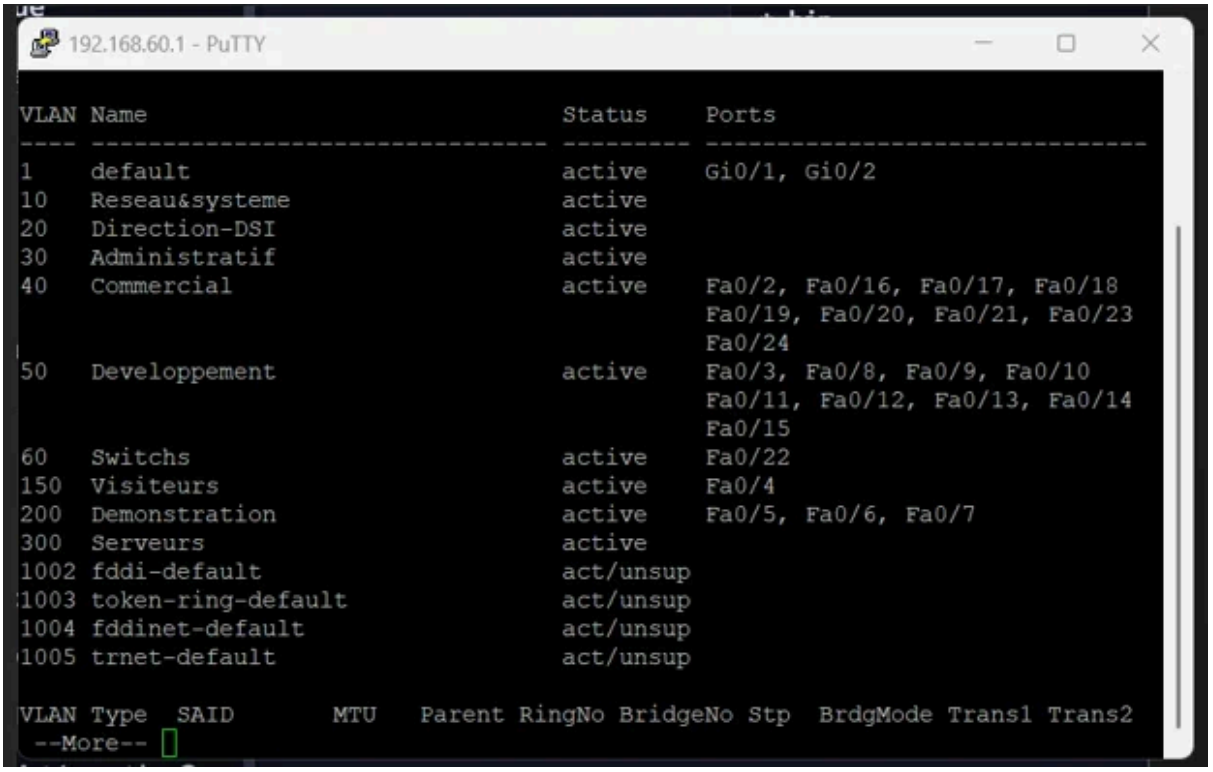
VLANs créés sur le switch serveur (2ème étage) :
• VLAN 10 – Réseau & Système
• VLAN 20 – Direction DSI
• VLAN 30 – Administratif
• VLAN 40 – Commercial
• VLAN 50 – Développement
• VLAN 60 – Switchs
• VLAN 150 – Visiteurs
• VLAN 200 – Démonstration
• VLAN 300 – Serveurs

Le mode trunk a été activé sur les liens entre les switches afin que les VLANs soient propagés automatiquement vers les switches clients via le protocole VTP.

Domaine VTP configuré : groupe4.local

Assignation des ports : une fois les VLANs propagés sur les switches clients, nous avons assigné les ports de chaque switch au VLAN correspondant en suivant le schéma réseau défini en amont. Chaque port a ainsi été placé dans le bon VLAN selon l'équipement ou le service qui y est connecté.





On peut constater que les VLANs ont bien été reçus et que les ports sont correctement assignés (ex : VLAN 40 Commercial sur Fa0/2, Fa0/16–Fa0/24 ; VLAN 50 Développement sur Fa0/3, Fa0/8–Fa0/15 ; VLAN 200 Démonstration sur Fa0/5–Fa0/7, etc.).

Grâce à cette configuration, les switches clients reçoivent automatiquement la liste des VLANs sans avoir besoin de les recréer manuellement.

A.4 Routage InterVlan

Assurer la communication des différents services autorisés vers le serveur :

Configuration Inter-VLAN – Routeur
Pour permettre la communication entre les différents VLANs, nous avons configuré le routage inter-VLAN directement sur le routeur. Pour chaque VLAN, on crée une sous-interface sur l'interface GigabitEthernet0/0 ex : interface GigabitEthernet0/0.10 , puis on y applique l'encapsulation dot1Q avec le numéro du VLAN correspondant, et enfin on lui assigne une adresse IP qui servira de passerelle par défaut pour les machines de ce VLAN.
Sous-interfaces configurées :
• Gi0/0.10 – VLAN 10 (Réseau & Système) → 192.168.10.254 /24
• Gi0/0.20 – VLAN 20 (Direction DSI) → 192.168.20.254 /24
• Gi0/0.30 – VLAN 30 (Administratif) → 192.168.30.254 /24
• Gi0/0.40 – VLAN 40 (Commercial) → 192.168.40.254 /24
• Gi0/0.50 – VLAN 50 (Développement) → 192.168.50.254 /24
• Gi0/0.60 – VLAN 60 (Switchs) → 192.168.60.254 /24
• Gi0/0.150 – VLAN 150 (Visiteurs) → 192.168.150.254 /24
• Gi0/0.200 – VLAN 200 (Démonstration) → 192.168.200.254 /24
• Gi0/0.300 – VLAN 300 (Serveurs) → 172.18.0.254 /24
Chaque sous-interface fait office de passerelle par défaut (gateway) pour les machines du VLAN correspondant, permettant ainsi la communication entre les VLANs via le routeur.

```
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
!
interface GigabitEthernet0/0.23
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.254 255.255.255.0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.254 255.255.255.0
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.254 255.255.255.0
!
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.254 255.255.255.0
!
interface GigabitEthernet0/0.150
 encapsulation dot1Q 150
 ip address 192.168.150.254 255.255.255.0
!
interface GigabitEthernet0/0.200
 encapsulation dot1Q 200
 ip address 192.168.200.254 255.255.255.0
!
interface GigabitEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.18.0.254 255.255.0.0
!
```

A.5 Tests & Rapport de Tests

Élaborer et réaliser l’ensemble des tests nécessaires à la validation de la solution proposée.

Nous avons réalisé l'ensemble des tests permettant de valider notre infrastructure réseau :

- Création des VLANs & propagation VTP : les VLANs sont bien présents sur les 3 switches grâce au protocole VTP (domaine groupe4.local)

- SSH : un VLAN dédié à l'administration a été créé (VLAN 60 – Switchs). La connexion SSH fonctionne sur le port 22 via PuTTY (192.168.60.1), réservée au VLAN 10 (Réseau & Système).

- Routage inter-VLAN : nous avons testé la connectivité depuis 5 VLANs différents (VLAN 10, 30, 50, 150, 200) vers le serveur. Les pings passent correctement, confirmant que le routage inter-VLAN est fonctionnel.

- Sauvegardes TFTP : les configurations du routeur et des 3 switches ont bien été sauvegardées sur le serveur TFTP.

- ACL : les règles d'accès ont été configurées sur le routeur (ACL 100 à 104). Les tests de blocage sont à compléter.

Notre rapport de test est disponible dès la page suivant :

BTS SIO – Établissement Saint-Adjutor

AP4 – Segmentation du réseau

RAPPORT DE TESTS

Groupe 4 – Semestre 2 – 2025/2026

Domaine VTP : groupe4.local

Date : 10/04/2026

1. Création des VLANs

Les VLANs ont été créés sur le switch du 2ème étage configuré en mode serveur VTP. Les deux autres switches (étage 1 et RDC) sont configurés en mode client VTP et reçoivent automatiquement les VLANs via le trunk.

Le domaine VTP configuré est : groupe4.local

La capture ci-dessous est issue du switch RDC (client VTP). Elle confirme que les VLANs ont bien été propagés depuis le switch serveur vers les switches clients. Les trois switches disposent de la même liste de VLANs grâce au protocole VTP. Les ports ont été assignés à chaque VLAN conformément au schéma réseau.

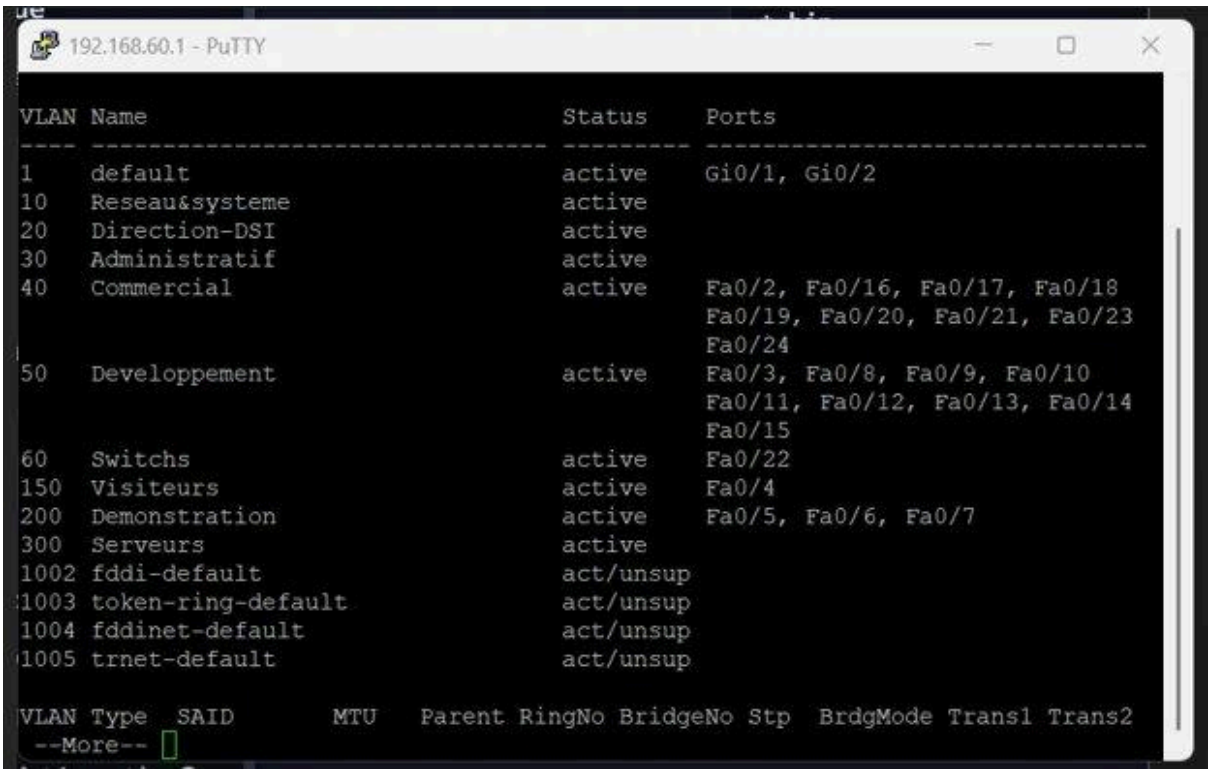


Figure 1 – VLANs propagés sur le switch RDC (client VTP) avec ports assignés

Résultat : Les VLANs sont bien présents sur les trois switches grâce à la propagation VTP. Les ports ont été assignés à chaque VLAN conformément au schéma réseau.

2. Test SSH – Administration à distance

Un VLAN dédié à l'administration a été créé : le VLAN 60 (Switchs), avec la passerelle 192.168.60.254. Le SSH a été configuré sur le port 22 sur l'ensemble des équipements d'interconnexion. La connexion SSH est autorisée uniquement depuis le VLAN 10 (Réseau & Système), à l'exception du stagiaire (192.168.10.1).

Pour se connecter, on utilise PuTTY en renseignant l'adresse IP de l'équipement (ici 192.168.60.1) et le port 22. La capture ci-dessous confirme que la connexion SSH est active et fonctionnelle.

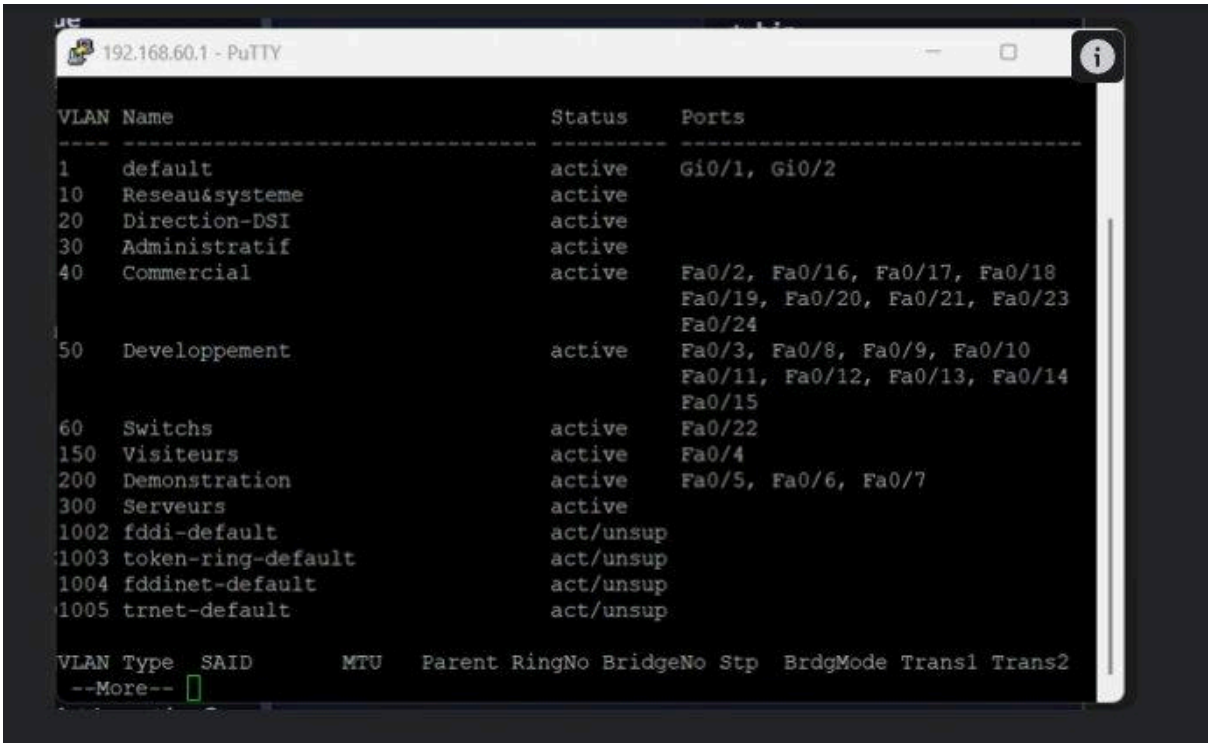


Figure 2 – Connexion SSH via PuTTY sur le VLAN 60 (port 22) – switch serveur 192.168.60.1

Résultat : ✅ La connexion SSH est opérationnelle sur le port 22 via le VLAN 60.

3. Test du routage inter-VLAN

Pour valider le routage inter-VLAN, nous avons testé la connectivité depuis différents VLANs vers le serveur (172.18.40.2) en déplaçant le poste sur différents ports du switch. Chaque branchement sur un nouveau port attribue automatiquement l'IP du VLAN correspondant.

3.1 Tableau récapitulatif des tests

Test	VLAN	IP machine	Ping serveur	Résultat
Ping vers serveur	VLAN 150 – Visiteurs	192.168.150.8	172.18.40.2	**OK**
Ping vers serveur	VLAN 30 – Administratif	192.168.30.8	172.18.40.2	**OK**
Ping vers serveur	VLAN 10 – Réseau&Sys.	192.168.10.8	172.18.40.2	**OK**
Ping vers serveur	VLAN 50 – Développement	192.168.50.8	172.18.40.2	**OK**
Ping vers serveur	VLAN 200 – Démonstration	192.168.200.5	172.18.40.2	**OK**

3.2 Captures des tests par VLAN

VLAN 150 – Visiteurs (192.168.150.8)

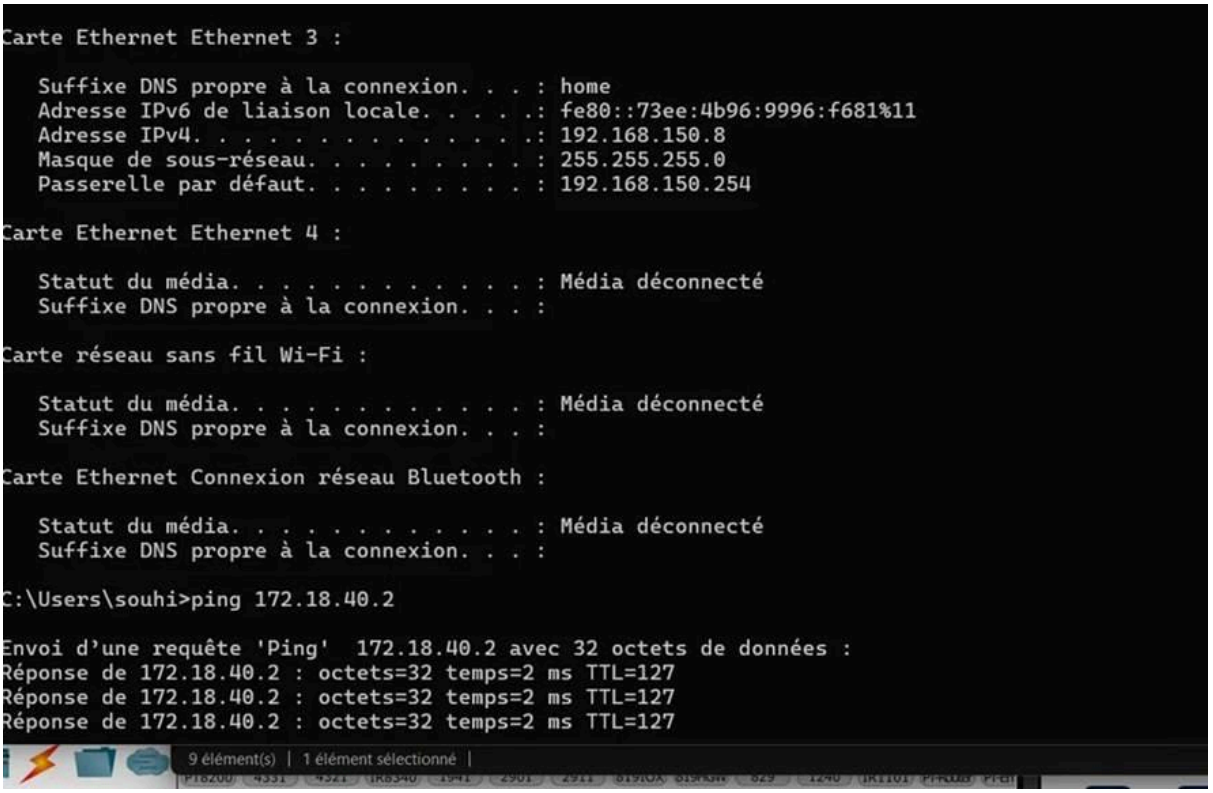


Figure 5 – Ping depuis VLAN 150 Visiteurs vers 172.18.40.2

VLAN 30 – Administratif (192.168.30.8)

Figure 6 – Ping depuis VLAN 30 Administratif vers 172.18.40.2

VLAN 10 – Réseau & Système (192.168.10.8)

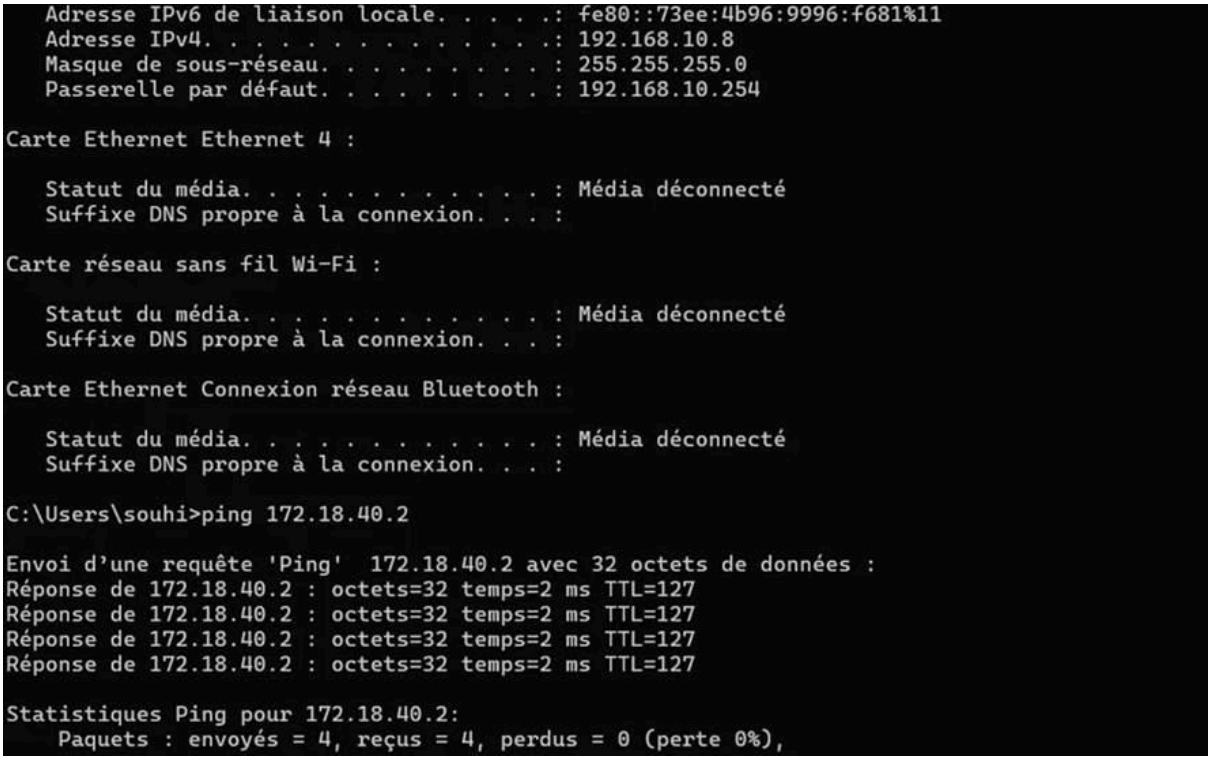


Figure 7 – Ping depuis VLAN 10 Réseau & Système vers 172.18.40.2

VLAN 50 – Développement (192.168.50.8)

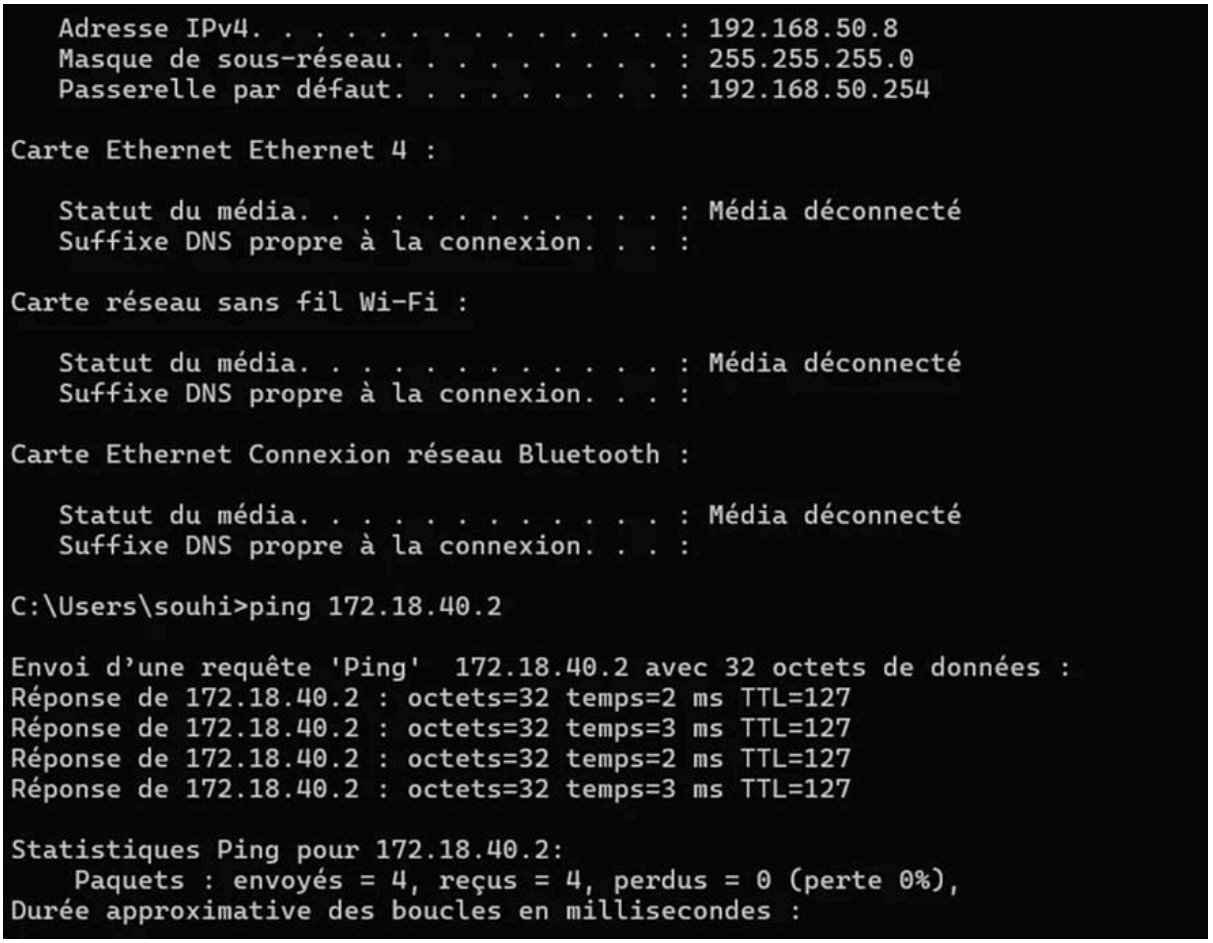


Figure 8 – Ping depuis VLAN 50 Développement vers 172.18.40.2

VLAN 200 – Démonstration (192.168.200.5)

Figure 9 – Ping depuis VLAN 200 Démonstration vers 172.18.40.2

Résultat : Le routage inter-VLAN est fonctionnel. Chaque VLAN peut communiquer avec le serveur via le routeur.

4. Sauvegardes TFTP

Les configurations de l'ensemble des équipements ont été sauvegardées sur le serveur TFTP. Le dossier de sauvegarde contient les fichiers suivants :

- routeur – configuration du routeur Cisco
- switch etage 1 – configuration du switch étage 1
- switch etage 2 – configuration du switch étage 2 (serveur VTP)
- switch etage rdc – configuration du switch RDC

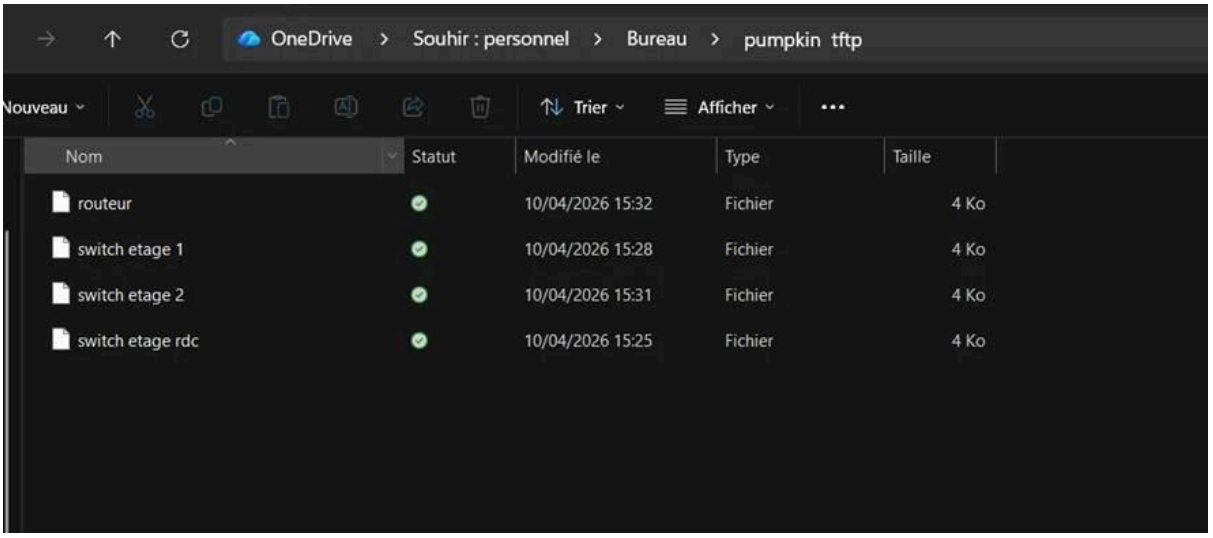


Figure 10 – Fichiers de sauvegarde TFTP (routeur + 3 switches)

Résultat : Les sauvegardes des 4 équipements sont bien présentes sur le serveur TFTP.

5. Règles d'accès – ACL

Les ACL (Access Control Lists) étendues ont été configurées sur le routeur afin de respecter les règles d'accès définies dans le cahier des charges.

5.1 ACL configurées

```
Routeur-MDL(config-ext-nacl)#do show access-list
Extended IP access list 100
    10 deny tcp host 192.168.10.42 192.168.60.0 0.0.0.255 eq 22
    20 permit tcp 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255 eq 22
    30 permit tcp any any (4 matches)
Extended IP access list 101
    10 deny ip 192.168.200.0 0.0.0.255 host 172.18.255.254
    20 permit ip any host 172.18.255.254
Extended IP access list 102
    10 deny ip host 192.168.40.1 host 172.18.40.4
    20 permit ip 192.168.40.0 0.0.0.255 host 172.18.40.4
    30 permit ip 192.168.50.0 0.0.0.255 host 172.18.40.4
    40 deny ip any host 172.18.40.4
Extended IP access list 103
    10 deny ip 192.168.150.0 0.0.0.255 host 172.18.40.2
    20 deny ip 192.168.200.0 0.0.0.255 host 172.18.40.2
    30 permit ip any host 172.18.40.2
Extended IP access list 104
    3 deny ip host 192.168.10.1 any
    5 permit ip 192.168.10.0 0.0.0.255 host 172.18.40.7
    20 permit ip 192.168.10.0 0.0.0.255 host 172.18.40.4 (14 matches)
    30 deny ip any host 172.18.40.4
    40 permit ip any any (159 matches)
Routeur-MDL(config-ext-nacl)#
```

Figure 11 – Configuration des ACL sur le routeur (show access-list)

5.2 Détail des règles

ACL	Règle	Objectif

100	Deny SSH stagiaire (192.168.10.42), permit SSH VLAN 10 → VLAN 60	Administration SSH réservée au VLAN Réseau & Système
101	Deny VLAN Démonstration → Active Directory, permit les autres	Bloquer l'accès AD depuis VLAN 200
102	Deny alternant (192.168.40.1), permit VLAN 40 et 50 → NextCloud	NextCloud accessible uniquement depuis Commercial et Développement
103	Deny VLAN 150 et 200 → TFTP (172.18.40.2), permit le reste	TFTP accessible uniquement depuis VLAN 10
104	Deny stagiaire (192.168.10.1), permit VLAN 10 → TFTP et NextCloud	Bloquer le stagiaire de VLAN 10

Note : Les ACL sont configurées et appliquées sur les sous-interfaces du routeur. Les captures de validation des blocages n'ont pas pu être réalisées lors de la séance.

6. Bilan des tests

Fonctionnalité	Statut	Remarque
Création des VLANs + propagation VTP	**OK**	Validé sur les 3 switches
Assignation des ports selon schéma réseau	**OK**	Ports assignés correctement
SSH – Administration à distance	**OK**	Connexion PuTTY fonctionnelle
Routage inter-VLAN	**OK**	Ping OK depuis 5 VLANs différents
Sauvegardes TFTP	**OK**	4 fichiers sauvegardés
ACL – Règles d'accès	**Partiel**	ACL configurées, tests de blocage à compléter

A.6 Réalisation des ACL

Réalisation des règles d'accès aux différentes zones

Les ACL vont permettrent de filtrer les flux réseau entre les différents VLAN afin de respecter les règles de sécurité définies dans le cahier des charges. Elles sont appliquées sur les interfaces du routeur pour contrôler les communications entrantes et sortantes. Nous avons décidé de travailler avec des ACLs étendues semblant mieux respecter le cahier des charges imposé.

Chaque ACL va avoir un but spécifique, voici le détail des ACLs :

- ACL 100 : **Accès SSH**

  Cette ACL permet de sécuriser l'administration à distance des équipements en SSH.

  - Refus de l'accès SSH pour l'hôte 192.168.10.42
  - Autorisation du réseau 192.168.10.0/24 vers le réseau serveur (port 22)
  - Autorisation implicite du reste du trafic

- ACL 101 : Cette ACL bloque l'accès au serveur Active Directory depuis le VLAN Démonstration (192.168.200.0/24), conformément au cahier des charges. Les autres accès sont autorisés.

- ACL 102 : Cette ACL autorise uniquement les VLAN Commercial (192.168.40.0/24) et Développement (192.168.50.0/24) à accéder au serveur NextCloud (172.18.40.4). Tous les autres accès sont refusés.

- ACL 103 : Cette ACL bloque certains VLAN (150 et 200) vers une machine spécifique (172.18.40.2), puis autorise le reste du trafic.

- ACL 104 : Cette ACL :
  - Refuse l'accès au serveur pour le stagiaire (192.168.10.1)
  - Autorise le VLAN Réseau & Système
  - Applique les règles d'accès aux serveurs spécifiques
  - Autorise le reste du trafic (règle finale)

Ces ACL permettent de sécuriser l’infrastructure en respectant le cloisonnement des VLAN et les contraintes du cahier des charges, notamment pour les accès aux serveurs critiques.

Liste de nos ACLs appliquées sur notre routeur afin de sécuriser notre maquette.

```
Routeur-MDL(config-ext-nacl)#do show access-list
Extended IP access list 100
    10 deny tcp host 192.168.10.42 192.168.60.0 0.0.0.255 eq 22
    20 permit tcp 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255 eq 22
    30 permit tcp any any (4 matches)
Extended IP access list 101
    10 deny ip 192.168.200.0 0.0.0.255 host 172.18.255.254
    20 permit ip any host 172.18.255.254
Extended IP access list 102
    10 deny ip host 192.168.40.1 host 172.18.40.4
    20 permit ip 192.168.40.0 0.0.0.255 host 172.18.40.4
    30 permit ip 192.168.50.0 0.0.0.255 host 172.18.40.4
    40 deny ip any host 172.18.40.4
Extended IP access list 103
    10 deny ip 192.168.150.0 0.0.0.255 host 172.18.40.2
    20 deny ip 192.168.200.0 0.0.0.255 host 172.18.40.2
    30 permit ip any host 172.18.40.2
Extended IP access list 104
    3 deny ip host 192.168.10.1 any
    5 permit ip 192.168.10.0 0.0.0.255 host 172.18.40.7
    20 permit ip 192.168.10.0 0.0.0.255 host 172.18.40.4 (14 matches)
    30 deny ip any host 172.18.40.4
    40 permit ip any any (159 matches)
Routeur-MDL(config-ext-nacl)#
```

A.7 Sauvegarde

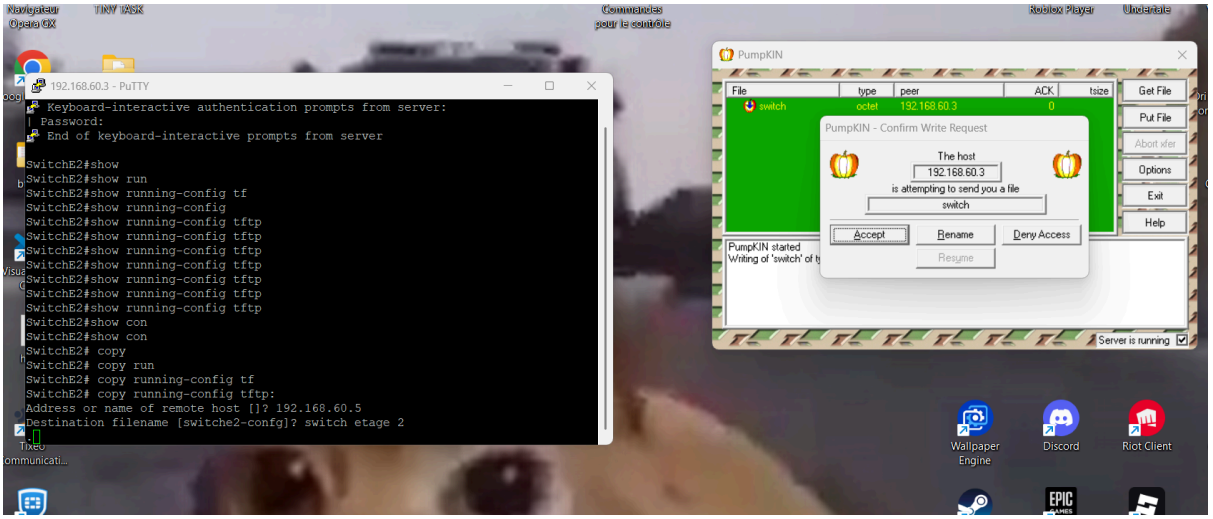
Réaliser l'ensemble des sauvegardes nécessaires

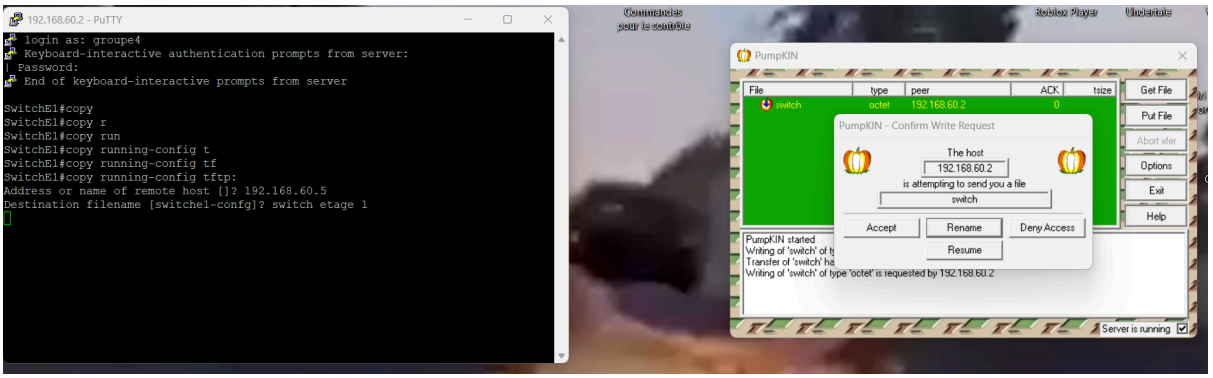
Les sauvegardes des configuration des 3 switchs et du routeur seront envoyées sur le poste d'une des deux personnes du groupe, se situant dans une vlan ayant accès au switch, ici la vlan 60 des switchs.

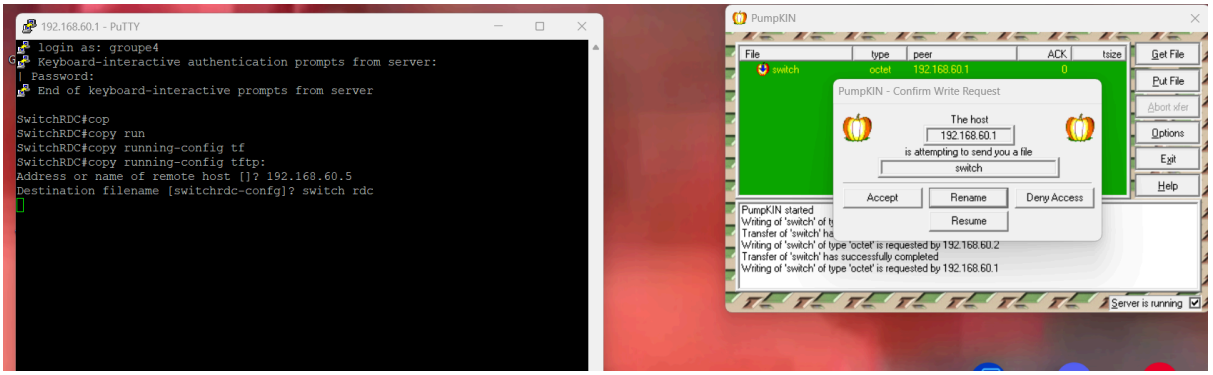
Nous avons décidé d'utiliser l'outil Pumpkin installé sur nos postes afin de réaliser l'ensemble de ces sauvegardes.

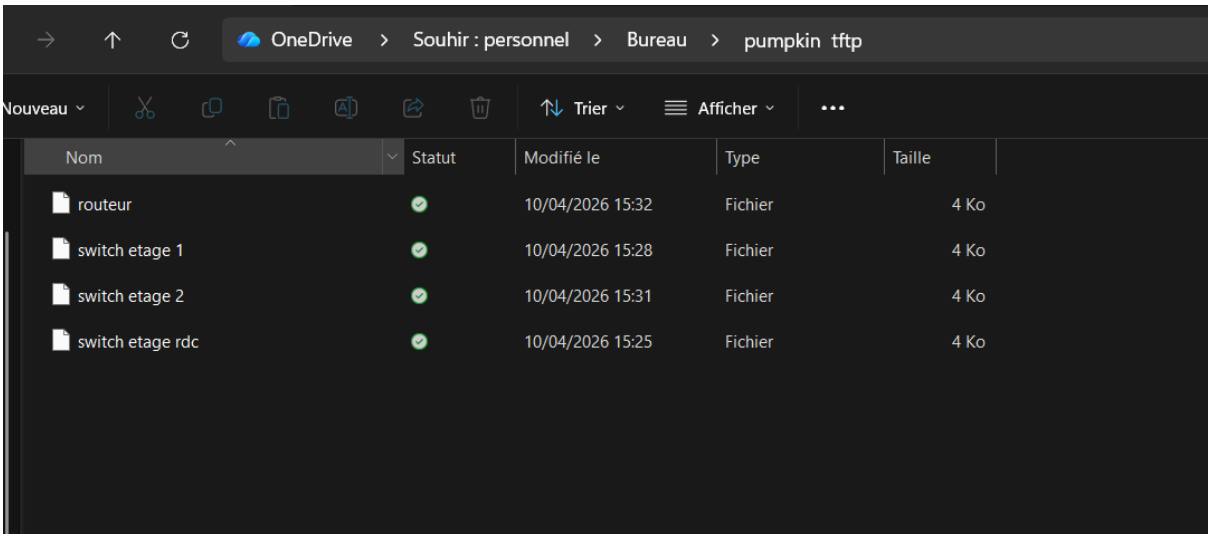
Pour ce faire, nous avons utilisé la commande copy et nous avons envoyé la running config sur notre poste via son IPv4

Voici l'ensemble des sauvegardes effectués ainsi que le dossier contenant ces sauvegardes:






192.168.60.1 - PuTTY
login as: groupe4
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
SwitchRDC#cop
SwitchRDC#copy run
SwitchRDC#copy running-config tf
SwitchRDC#copy running-config tftp:
Address or name of remote host []? 192.168.60.5
Destination filename [switchrdc-confg]? switch rdc
PumpKIN
File
type
peer
ACK
tsize
switch
octet
192.168.60.1
0
Get File
Put File
Abort xfer
Options
Exit
Help
PumpKIN - Confirm Write Request
The host
192.168.60.1
is attempting to send you a file
switch
Accept
Rename
Deny Access
Resume
PumpKIN started
Transfer of 'switch' has successfully completed
Writing of 'switch' of type 'octet' is requested by 192.168.60.1
Server is running


OneDrive
Souhir : personnel
Bureau
pumpkin tftp
Nouveau
Trier
Afficher
Nom
Statut
Modifié le
Type
Taille
routeur
10/04/2026 15:32
Fichier
4 Ko
switch etage 1
10/04/2026 15:28
Fichier
4 Ko
switch etage 2
10/04/2026 15:31
Fichier
4 Ko
switch etage rdc
10/04/2026 15:25
Fichier
4 Ko