

# BTS SIO - E5

## Situation professionnelle n°3

**Initier un environnement virtuel avec un routeur un switch et un vlan 3 avec une machine virtuel linux et un vlan 2 une machine Windows server**

03/04/2026

Description :

La configuration d'un environnement virtuel est une étape clé dans la gestion des infrastructures informatiques modernes. Cette mission vise à maîtriser un environnement virtuel via un switch Cisco de niveau 2 en utilisant aussi un routeur afin de sécuriser le réseau et pouvoir accéder à internet via le NAT relié par un câble Ethernet à un branchement au WAN.

Contexte :

Cette mission s'inscrit dans le cadre du déploiement et de la gestion d'un environnement réseau virtuel et permettre le transfert de fichier d'un Windows server à une machine linux au sein de l'entreprise avec samba et le protocole FTP ainsi qu'un bridge. Elle consiste à configurer une architecture réseau virtualisé simple comprenant un switch Cisco de niveau 2, un routeur Cisco, deux machines virtuels (windows server et linux) et un poste de travail. L'objectif est d'assurer la communication entre les 2 machines virtuels, valider la connectivité IP ainsi que l'accès au réseau via le port wan ainsi que de permettre un transfert de fichier du windows server au linux.

| NOM                | DATE       | TAMPON |
|--------------------|------------|--------|
| CHERIF SOULEYMANE  | 03/04/2026 |        |
| BERDJEGHLOUL BILAL | 03/04/2026 |        |
| PETIT GABIN        | 03/04/2026 |        |
| DOUSSAINT THEODORE | 03/04/2026 |        |

# SOMMAIRE :

|                                                    |       |
|----------------------------------------------------|-------|
| 1. Objectif de la mission                          | 3     |
| 1.1. Objectif principal                            |       |
| 1.2 Matériel réseau                                |       |
| 1.3 Vérification des ports wan                     | 4     |
| 1.4 Schéma du projet réalisé                       |       |
| 1.5 Simulation sur Cisco Packet Tracer             | 5     |
| 1.6 Outils et logiciels                            |       |
| 2. Mise en œuvre (PARTIE RESEAU)                   | 6     |
| 2.1 Branchement des équipements                    |       |
| 2.2 Configuration du switch                        | 7-8   |
| 2.3 Configuration du routeur                       | 9     |
| 2.4 Paramétrage IP du Windows server et DNS, ADDS  | 9-11  |
| Paramétrage IP du Debian (machine linux)           | 11-12 |
| 2.5 Vérification et test                           | 12    |
| 3. Deuxième partie de la mission (PARTIE SYSTEME)  | 13    |
| 3.1 Installation et configuration de Samba sur...  | 13-14 |
| 3.2 Transfert de fichier du windows server a linux |       |
| 3.3 Bilan                                          |       |
| 3.4 Rôles                                          |       |

# OBJECTIF DE LA MISSION :

## 1.1 Objectif principal :

Initier un environnement virtuel local, configurer un réseau local avec Vlan windows server et debian avec un pont pour leur permettre de communiquer entre eux, ainsi qu'un routeur et un switch pour leur permettre de se connecter à internet.

## 1.2 Matériel réseau :

- Switch Cisco choisi pour sa capacité à faire communiquer efficacement plusieurs VLAN et offrir une configuration accessible pour les étudiants et pour sa capacité à gérer le routage.

- Routeur Cisco choisi pour sa capacité à gérer efficacement plusieurs VLAN, et offrir une configuration accessible et pour sa capacité à gérer le routage afin de distribuer internet de manière sécurisée à l'environnement.

Configurations des VLANs :

- Un VLAN2 (contenant le Windows server) et un VLAN 3 (contenant la machine linux) pour séparer les zones du réseau en fonction des besoins fonctionnels.

Adresses IP :

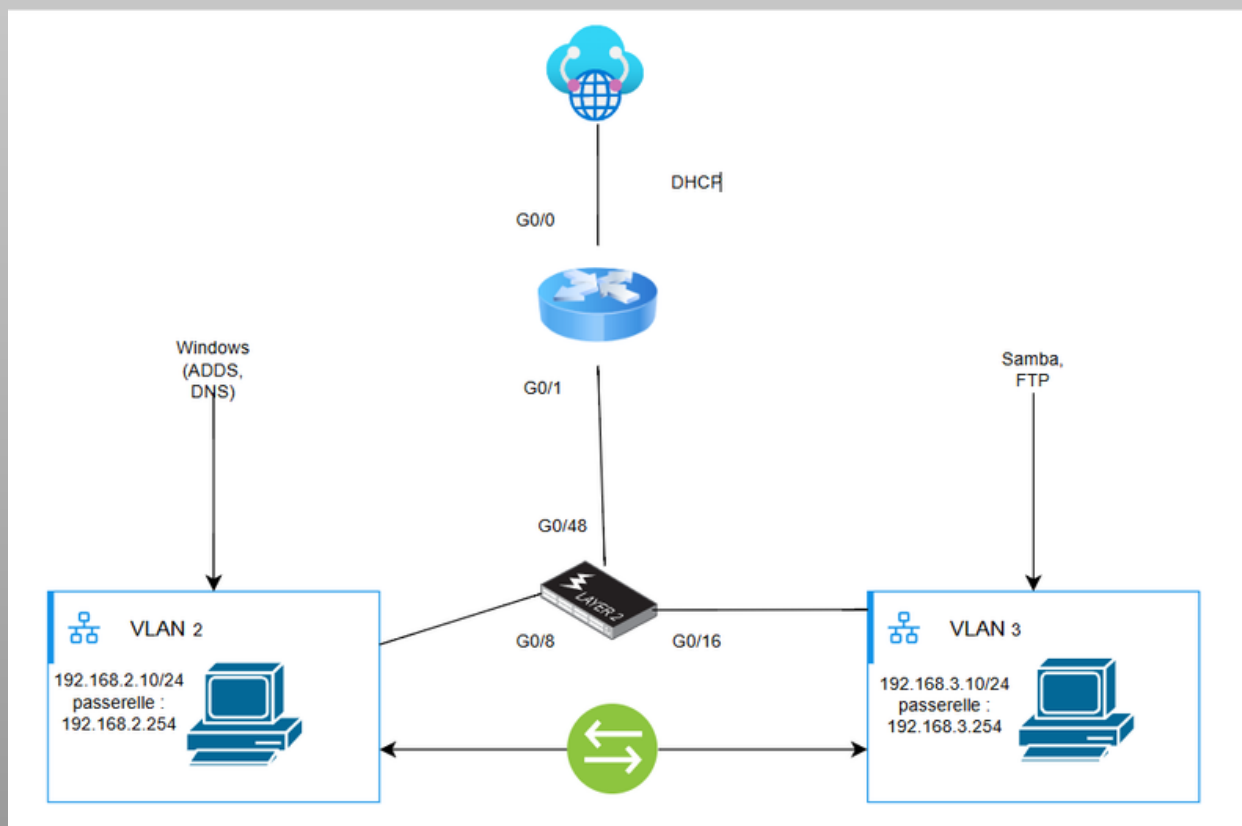
- Plages IP privées choisies en classe C (192.168.3.10/24, 192.168.2.10/24, et le wan 172.16.15 (qui est de classe B) conformes aux bonnes pratiques pour réseaux locaux.

- Passerelles configurées sur les sous-interfaces correspondant aux VLAN.

## 1.3 Vérification de la prise WAN :

Avant toute configuration, on vérifie que la prise WAN disponible en salle est active. Pour cela, on branche un câble Ethernet directement entre le port WAN du routeur et la prise murale. On vérifie la présence du signal de deux façons : soit visuellement en observant que le voyant du port s'allume sur le routeur (lumière verte fixe ou clignotante), soit logiciellement en entrant dans la configuration du routeur et en vérifiant que l'interface GigabitEthernet 0/0 obtient bien une adresse IP via DHCP avec la commande `show ip interface brief`. Si une IP est attribuée automatiquement sur cette interface, la prise WAN est fonctionnelle et on peut continuer.

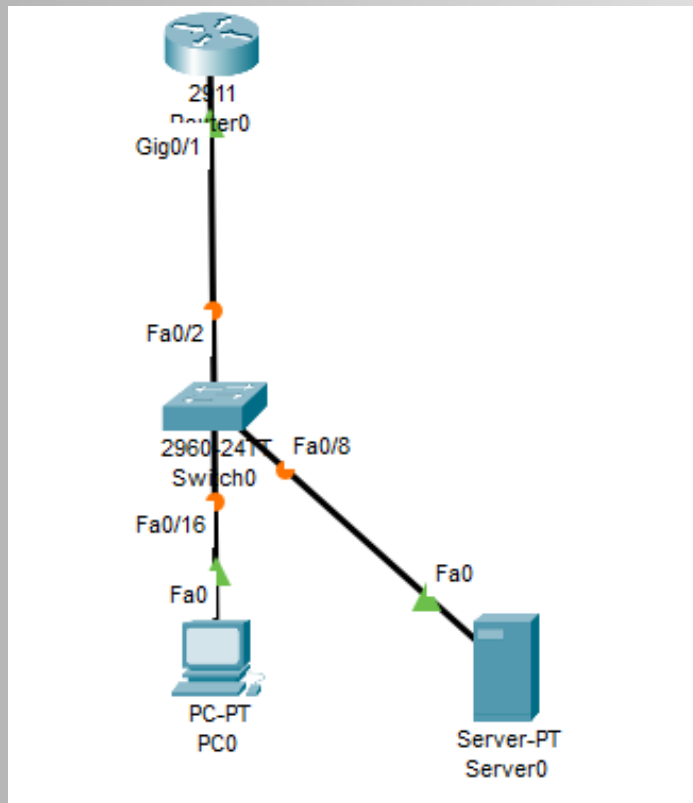
## 1.4 Schéma de la mission :



## 1.5 Simulation sur Cisco Packet Tracer

On simule ensuite la configuration sur Cisco Packet Tracer avant de la déployer sur le vrai matériel, ce qui permet de détecter les erreurs de configuration sans risquer de bloquer le réseau réel.

Répartition des tâches pour cette phase :



## 1.6 Outils et logiciels :

- 1 switch de niveau 2
- 2 PC
- 1 câble console
- 4 câbles ethernet
- 1 router
- PuTTY (pour la configuration)
- Draw.io (schéma)
- VMware workstation (pour la virtualisation)
- Samba et FTP (pour le transfert de fichiers)

# MISE EN OEUVRE :

## Etapes de configurations :

### 2.1. Branchement des équipements

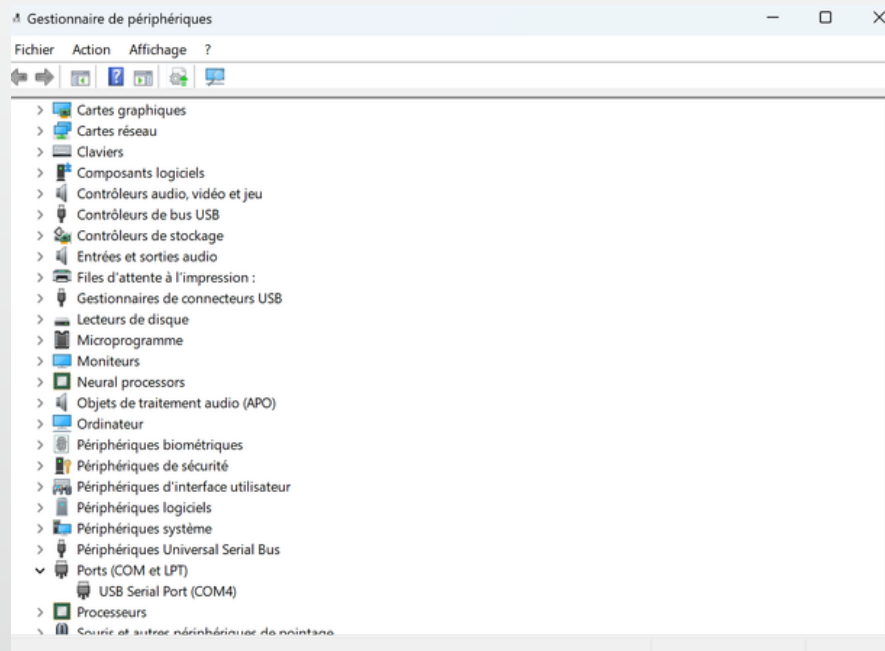
- 
- Connecter un câble Ethernet entre le switch (g0/8) et le vlan 2
- Connecter un câble Ethernet entre le switch (g0/16) et le vlan 3
- Connecter un câble Ethernet entre le routeur (g0/0) et le port wan.
- Brancher un câble entre le routeur (g0/1) et le switch (g0/48)
- Brancher le câble console du switch au PC

On vérifie que tous les voyants des ports sont allumés avant de commencer la configuration.

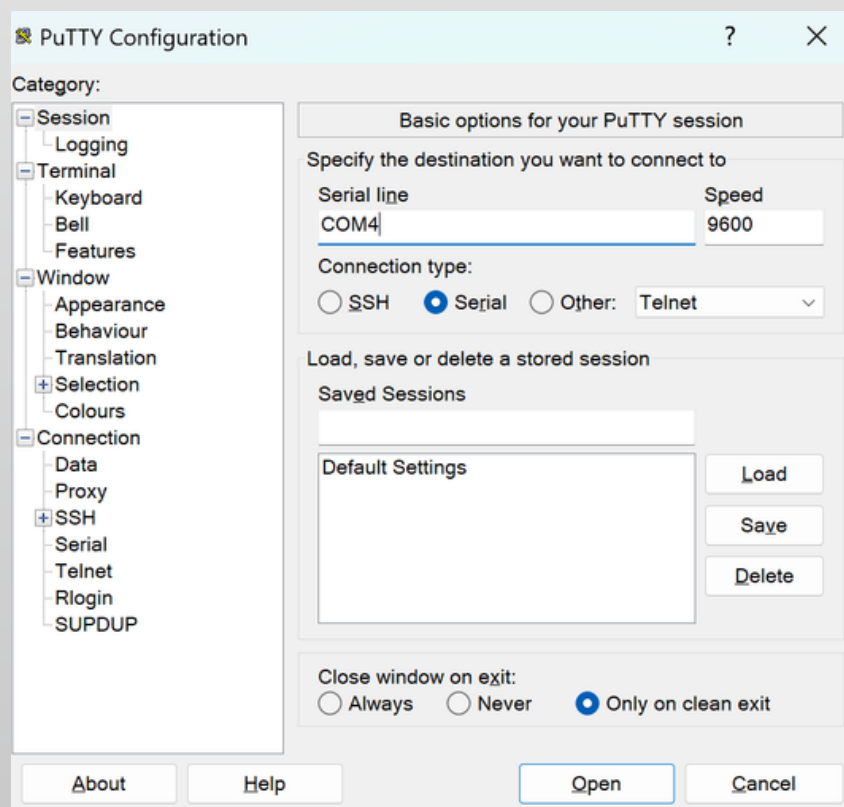
## 2.2 Connexion au switch

- Identifier le port USB (ex: COM4) via le gestionnaire de périphériques (1)
- Ouvrir Putty en mode Série, indiquer le port COM4 (2)

(1)



(2)



### 3. Configuration du switch

- Accéder au terminal Putty et configurer le switch L3 avec les commandes suivantes :

```
!sw0
enable
configure terminal

vlan 2
  name VLAN_WindowsServer
vlan 3
  name VLAN_Debian

interface g0/8
  switchport mode access
  switchport access vlan 2
  no shutdown

interface g0/16
  switchport mode access
  switchport access vlan 3
  no shutdown

interface g0/48
sw tr enc dot1Q
  switchport mode trunk
  switchport trunk allowed vlan 2,3
  no shutdown

end
write memory
```

- Fin de la configuration du switch.

## 2.3 Configuration du routeur :

```
!R0
enable
configure terminal

# Interface WAN (connectée à la box/internet)
interface gigabitEthernet 0/0
  ip address dhcp
  no shutdown
  ip nat outside

# Interface vers le switch (trunk)
interface gigabitEthernet 0/1
  no shutdown
  ip nat inside

# Sous-interface VLAN 2 → Windows Server
interface gigabitEthernet 0/1.2
  encapsulation dot1Q 2
  ip address 192.168.2.254 255.255.255.0
  ip nat inside

# Sous-interface VLAN 3 → Debian
interface gigabitEthernet 0/1.3
  encapsulation dot1Q 3
  ip address 192.168.3.254 255.255.255.0
  ip nat inside

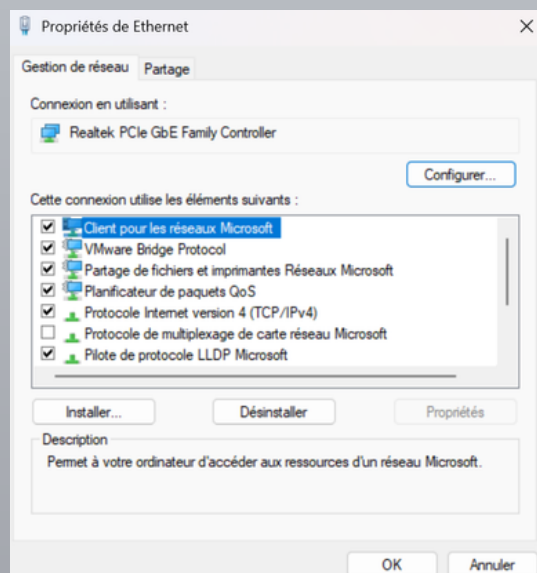
# NAT : permettre aux VLANs d'accéder à internet
ip nat inside source list 1 interface gigabitEthernet 0/0 overload
access-list 1 permit 192.168.0.0 0.0.255.255

end
write memory
```

- Fin de la configuration du routeur.

## 2.4. Paramétrage des adresses IP des machines

- Ouvrir les propriétés du réseau Ethernet (Windows R + ncpa.cpl)



- Configurer sur le windows server :  
Adresse IP : 192.168.2.10 / Masque : 255.255.255.0 /  
Passerelle : 192.168.10.254 / DNS : 8.8.8.8

## **Installation du DNS et du ADDS :**

Afin d'installer DNS et ADDS dans le windows serveur il faut, dans la VM, aller dans "gérer dans l'interface" et sélectionner DNS et ADDS :

Une fois les rôles installés et le serveur promu en contrôleur de domaine, on vérifie depuis le cmd que le domaine est bien actif : `echo %userdomain%` Retourne BILAL — confirme que le serveur fait bien partie du domaine `bilal.local`. `nslookup bilal.local` Retourne l'IP 192.168.2.10 — confirme que le serveur DNS répond correctement et résout le nom de domaine vers l'adresse du Windows Server.

L'objectif est de promouvoir Windows Server en contrôleur de domaine pour centraliser l'authentification du réseau et assurer la résolution de noms.

Depuis le Gestionnaire de serveur, on clique sur "Ajouter des rôles et fonctionnalités" et on installe les rôles Active Directory Domain Services (ADDS) et DNS. Ces deux rôles sont liés : ADDS gère l'annuaire et les comptes utilisateurs, DNS permet la résolution des noms de domaine au sein du réseau.

Une fois l'installation terminée, on clique sur la notification qui apparaît dans le gestionnaire pour "Promouvoir ce serveur en contrôleur de domaine". On choisit de créer une nouvelle forêt avec le nom de domaine `tp.local`. On définit un mot de passe de restauration des services d'annuaire (DSRM), on laisse les options par défaut et on finalise l'installation. Le serveur redémarre automatiquement.

Après redémarrage, le serveur gère le domaine `tp.local` et le service DNS est actif sur 192.168.2.10. Les machines du réseau peuvent pointer leur DNS vers cette adresse pour résoudre les noms du domaine.

```

Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

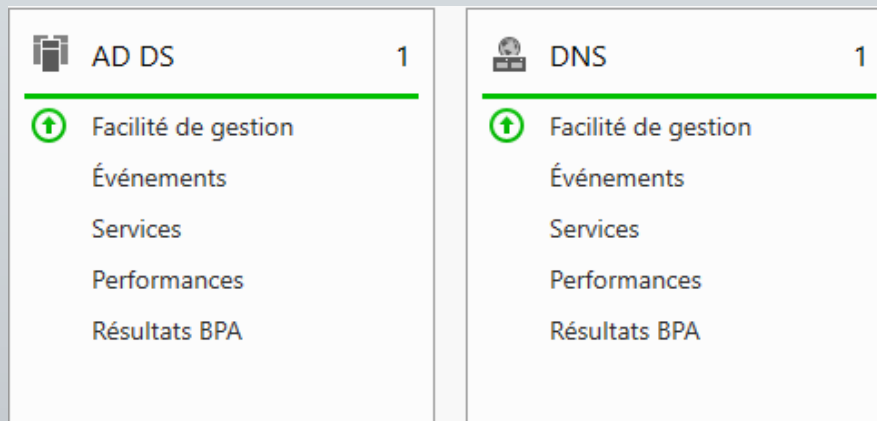
C:\Users\Administrateur>echo %userdomain%
BILAL

C:\Users\Administrateur>nslookup bilal.local
Serveur : WIN-7B3LDP1VN4L.bilal.local
Address: 192.168.2.10

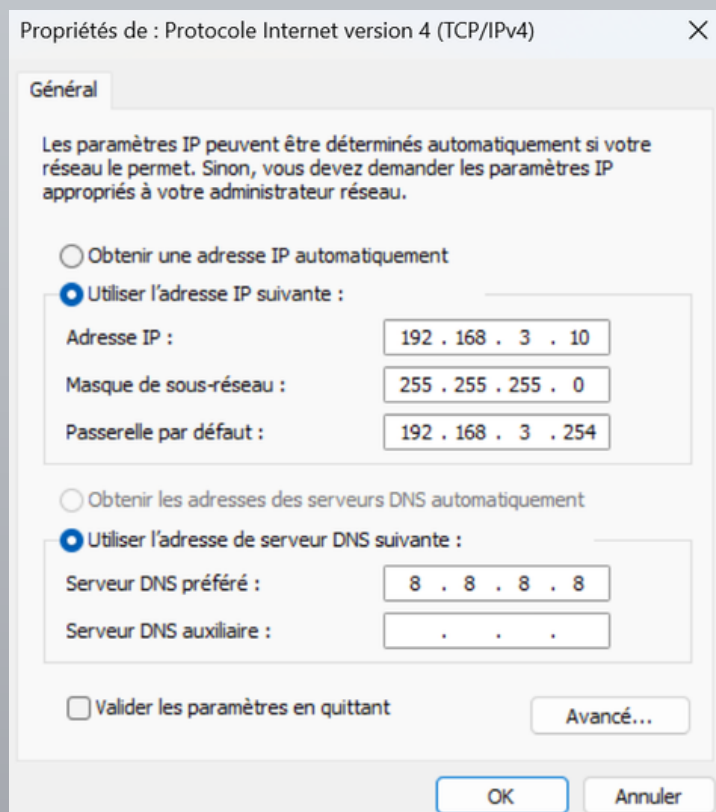
Nom : bilal.local
Address: 192.168.2.10

C:\Users\Administrateur>_

```



- Sur debian : L'adresse IP : 192.168.3.10 / Masque : 255.255.255.0 / Passerelle : 192.168.3.254/ DNS : 8.8.8.8



## 2.5 Vérifier la connectivité par ping : ping 192.168.2.10 et ping 192.168.3.10

```
Ping statistics for 192.168.2.10:  
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Cisco Packet Tracer SERVER Command Line 1.0  
C:\>ping 192.168.3.10
```

```
Pinging 192.168.3.10 with 32 bytes of data:
```

```
Reply from 192.168.3.10: bytes=32 time=6ms TTL=127  
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127  
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127  
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 192.168.3.10:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

```
C:\>|
```

## Résultats et vérification

Chaque test de ping doit indiquer une réponse permettant d'attester que la configuration du routage inter-VLAN est fonctionnelle. Les adresses sont validées si la réponse est correcte et le taux de perte est minimal.

# Seconde Partie de la mission:

## Objectif principal :

Permettre au windows server de partager des fichiers au debian avec Samba et FTP.

## MISE EN OEUVRE :

### 3.1 Configuration de Samba sur Debian :

On commence par ouvrir le fichier de configuration principal de Samba pour y ajouter notre partage :

```
nano /etc/samba/smb.conf
```

On y ajoute le bloc suivant qui définit le partage nommé partagDebian, pointant vers le dossier /partagegab, accessible uniquement à l'utilisateur gabvlan3 avec les droits d'écriture :

```
[partagDebian]
```

```
path = /partagegab
```

```
browseable = yes
```

```
writable = yes
```

```
guest ok = no
```

```
valid users = gabvlan3
```

```
create mask = 0770
```

```
directory mask = 0770
```

On crée ensuite le dossier qui sera partagé sur le réseau :

```
mkdir -p /partagegab
```

On crée l'utilisateur Linux qui servira à s'authentifier sur le partage :

```
useradd -m gabvlan3
```

```
passwd gabvlan3
```

On l'enregistre ensuite dans la base Samba avec son propre mot de passe SMB, car Samba gère ses mots de passe indépendamment de Linux :

```
smbpasswd -a gabvlan3
```

On attribue la propriété du dossier à cet utilisateur pour qu'il puisse y lire et écrire, puis on applique les bonnes permissions :

```
chown -R gabvlan3:gabvlan3 /partagegab
```

```
chmod -R 770 /partagegab
```

On vérifie que la configuration ne contient pas d'erreurs, puis on redémarre le service pour appliquer les changements :

```
testparm
```

```
systemctl restart smbd
```

Depuis Windows Server, on accède au partage via l'explorateur de fichiers en tapant l'adresse suivante dans la barre d'adresse :

```
\\192.168.3.10\partagDebian
```

On s'authentifie avec le compte gabvlan3 et son mot de passe.

## 3.2 Configuration FTP (vsftpd) :

Le service vsftpd est déjà installé sur la Debian. On vérifie et adapte sa configuration dans le fichier suivant pour s'assurer que les utilisateurs locaux peuvent se connecter et sont confinés dans leur dossier :

```
nano /etc/vsftpd.conf
```

Les paramètres clés activés sont `local_enable=YES` pour autoriser les comptes Linux, `chroot_local_user=YES` pour isoler chaque utilisateur dans son dossier, et `local_root=/ftp` qui définit le dossier racine FTP.

On crée ensuite la structure de dossiers : le dossier /ftp doit appartenir à root (obligation de vsftpd en mode chroot), et on crée un sous-dossier propre à gabvlan3 où il pourra déposer ses fichiers :

```
chown root:root /ftp && chmod 755 /ftp
```

```
mkdir -p /ftp/gabvlan3
```

```
chown gabvlan3:gabvlan3 /ftp/gabvlan3
```

On redémarre le service pour appliquer la configuration :

```
systemctl restart vsftpd
```

Sur Windows Server, on installe FileZilla Client depuis [filezilla-project.org](http://filezilla-project.org). On se connecte avec les paramètres suivants : hôte 192.168.3.10, port 21, identifiant gabvlan3. Une fois connecté, le dossier /ftp/gabvlan3 apparaît dans FileZilla et le transfert de fichiers est possible dans les deux sens.

### 3.3

## BILAN :

Cette mission nous a permis de bien comprendre comment déployer un environnement virtualisé comprenant un routeur (accès WAN/Internet), un switch manageable avec segmentation VLAN, et un bridge dédié assurant la communication inter-VLAN. En suivant cette procédure, nous avons pu vérifier que le VLAN 2 et le VLAN 3 pouvaient échanger des données sans problème via le bridge, comme l'ont montré les tests de transfert de fichiers réussis entre le Windows Server et la machine Linux Debian. Ce travail montre à quel point une bonne segmentation réseau est essentielle, tout comme un plan d'adressage IP clair et une configuration rigoureuse des équipements virtualisés. De plus, nous avons appris à déployer et configurer des services critiques en entreprise tels que le DNS, l'Active Directory, Samba et le FTP. En somme, cette mission est une étape importante pour maîtriser les bases des infrastructures réseau et systèmes modernes, et elle ouvre la porte à des configurations plus avancées, notamment l'intégration de ces services dans des environnements d'entreprise plus complexes.

### 3.4 Répartition des tâches :

Bilal et Théodore : Schéma Draw.io, plan d'adressage, simulation packet tracer, configuration du switch et du routeur

Souleymane et Gabin et Théodore : Rédaction du plan écrit, vérification de la cohérence des adressages IPs et du partage Samba.