Rapport Technique SAÉ 1.02 : S’initier aux réseaux informatiques

MAMMAD Shemseddine

Sommaire :

Une entreprise est en phase d'expansion et a recruté un nouvel employé pour concevoir un réseau local adapté à ses besoins. Cependant, la documentation réseau n'a pas été tenue à jour depuis plusieurs années, ce qui complique les évolutions nécessaires.

Problématique :

- Absence de documentation complète et récente du réseau existant.
- Les configurations des switchs, bien que sauvegardées sur un serveur TFTP par l'ancien administrateur réseau, doivent être récupérées et analysées.
- Nécessité d'identifier les erreurs potentielles et de documenter tous les aspects du réseau pour assurer sa pérennité.

Mission confiée :

- Concevoir une documentation exhaustive du réseau incluant :
    - La topologie du réseau.
    - Les adresses IP utilisées.
    - Les VLANs configurés.
    - Les configurations des équipements réseau.
    - L'identification des erreurs ou des incohérences existantes.
- S'appuyer sur les configurations existantes pour éviter de repartir de zéro et garantir un réseau évolutif.

Partie Théorique :

1. Compétences mobilisées :

Pour mener à bien ce projet, plusieurs ressources et compétences acquises au cours de la formation sont mises à contribution :

- **Principes et architecture des réseaux (R1.02)** :
  Permet l'analyse et la collecte des informations sur l'infrastructure réseau existante, notamment grâce à l'examen des trames disponibles.
- **Fondamentaux réseaux (R1.01B)** :
  Utilisés pour réaliser des simulations de base et configurer les éléments essentiels du réseau.
- **Réseaux locaux et équipements actifs (R1.03)** :
  Crucial pour les configurations avancées des switches, avec une attention particulière sur :
  - La mise en place des connexions SSH.
  - La configuration approfondie des VLANs.
- **Systèmes d'exploitation (R1.08)** :
  Essentiel pour l'intégration et la configuration des machines Ubuntu dans l'environnement réseau.
- **Systèmes numériques (R1.06) et électroniques (R1.04)** :
  Garantis pour l'installation physique optimale du réseau.

2. Approche complémentaire :

Une étude approfondie de la documentation technique est réalisée afin d'identifier des solutions adaptées pour le nouveau switch, en explorant des options innovantes et pertinentes.

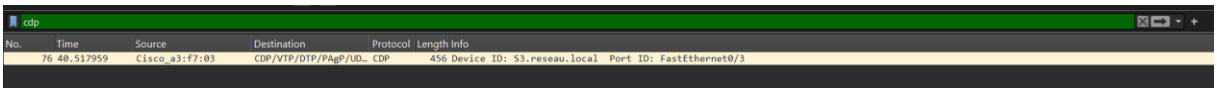
3. Première phase d'analyse :

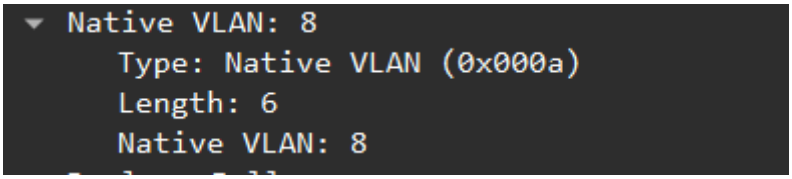
Un état des lieux précis de la configuration actuelle du réseau a été entrepris, notamment à travers :

- Une analyse détaillée des trames réseau disponibles.
- Un focus particulier sur la configuration du switch 3.

Objectif final :
Concevoir un réseau fonctionnel et évolutif tout en consolidant les bases techniques et la documentation pour garantir la pérennité des installations.

En étudiant une des trames réseaux du switch s3





Nous pouvons voir que nous devons nous connecter au port 3 qui est dans le vlan 8 du switch s3

Fonctionnement du Tracert avec le TTL :
Le protocole traceroute utilise le mécanisme du TTL (*Time To Live*) pour analyser le chemin pris par un paquet à travers le réseau jusqu'à sa destination. Voici les étapes principales :

1. **Détermination du nombre de routeurs sur la route :**
    - Le tracert envoie des paquets successifs avec un TTL initial croissant (commençant à 1).
    - À chaque routeur traversé, le TTL est décrémenté de 1.
2. **Comportement à l'expiration du TTL :**
    - Lorsque le TTL atteint 0, le paquet est supprimé par le routeur.
    - Une réponse ICMP (*Time Exceeded*) est renvoyée à l'expéditeur, indiquant le routeur où le TTL a expiré.
3. **Arrivée à destination :**
    - Une fois que le paquet atteint sa destination, une réponse ICMP (*Echo Reply* ou équivalent) est renvoyée, marquant la fin du tracert.

Rôle du TTL :
Le TTL empêche les paquets de circuler indéfiniment dans le réseau, en garantissant qu'ils seront supprimés après un certain nombre de sauts (routeurs). Cela limite les erreurs potentielles et le gaspillage de ressources réseau.

Interprétation des résultats :

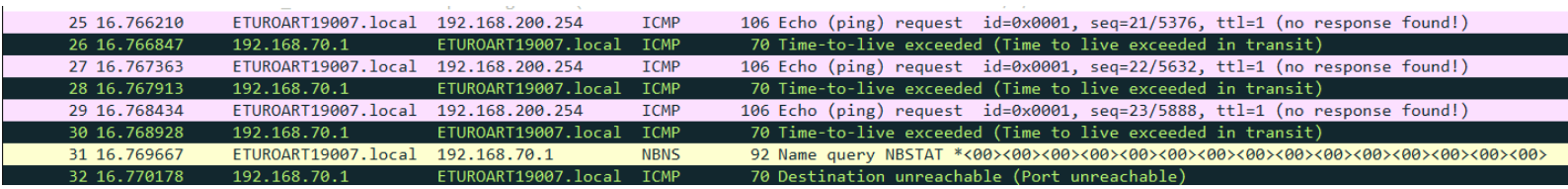
- **Réponse ICMP reçue :** Cela indique un routeur ou la destination finale.
- **Absence de réponse pendant le tracert :** Cela signifie que le TTL était trop court pour atteindre le prochain routeur ou que des restrictions (comme des pare-feu) empêchent la génération de réponses ICMP.

Conclusion :
L'analyse des résultats du tracert permet de cartographier les routeurs traversés, d'identifier les points de défaillance éventuels et de vérifier les performances du réseau sur le chemin vers la destination.

Dans cet exemple précis, le message **"TTL exceeded in transit"** indique clairement que le TTL initialement défini dans le paquet a atteint 0 après être passé par un routeur. Cela signifie que :

1. Le paquet a été reçu par un routeur, qui a décrémenté le TTL de 1.
2. Une fois le TTL à 0, le routeur a supprimé le paquet conformément aux règles du protocole IP.
3. En réponse, ce routeur a généré un message ICMP **Time Exceeded** pour signaler que le paquet ne pouvait pas être transmis plus loin.

Dans cet exemple, on observe également que le routeur ayant généré cette



réponse à l'adresse **192.168.70.1**, ce qui permet de l'identifier comme un des nœuds du chemin suivi par le paquet.

Avec un TTL de **127**, le paquet peut traverser plusieurs routeurs sans être supprimé, ce qui résout le problème rencontré avec un TTL de 1. Le paquet

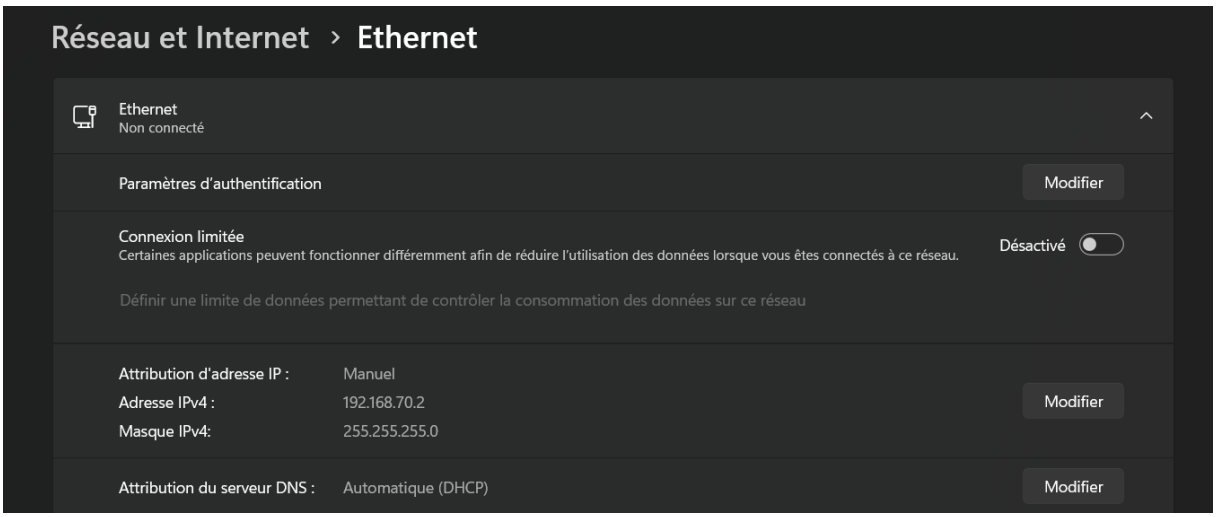
```
51 22.317490    ETUROART19007.local  192.168.200.254      ICMP     106 Echo (ping) request  id=0x0001, seq=24/6144, ttl=2 (reply in 52)
52 22.318738    192.168.200.254      ETUROART19007.local  ICMP     106 Echo (ping) reply    id=0x0001, seq=24/6144, ttl=127 (request in 51)
53 22.319533    ETUROART19007.local  192.168.200.254      ICMP     106 Echo (ping) request  id=0x0001, seq=25/6400, ttl=2 (reply in 54)
54 22.321741    192.168.200.254      ETUROART19007.local  ICMP     106 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=127 (request in 53)
55 22.323022    ETUROART19007.local  192.168.200.254      ICMP     106 Echo (ping) request  id=0x0001, seq=26/6656, ttl=2 (reply in 56)
56 22.325161    192.168.200.254      ETUROART19007.local  ICMP     106 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=127 (request in 55)
```

atteint maintenant la destination **192.168.200.254** sans erreur, car le TTL est suffisamment élevé pour couvrir tous les sauts nécessaires.

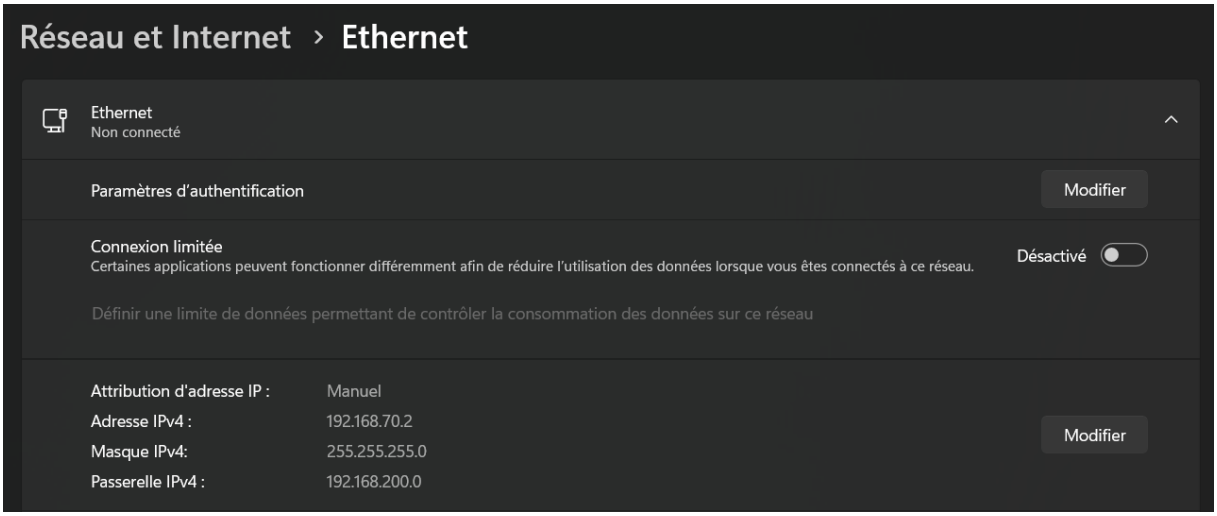
Pour récupérer la configuration du switch **S3**, vous devez suivre ces étapes :

1. **Connecter le PC au port 3 du switch S3** :
   Le PC doit être connecté à ce port pour pouvoir accéder à la configuration du switch.
2. **Configurer l'adresse IP du PC** :
   L'adresse IP du PC doit être configurée pour être dans le même sous-réseau que l'adresse IP du switch ou le routeur auquel il est connecté, en prenant soin de spécifier l'adresse IP qui a émis la requête **tracert**.

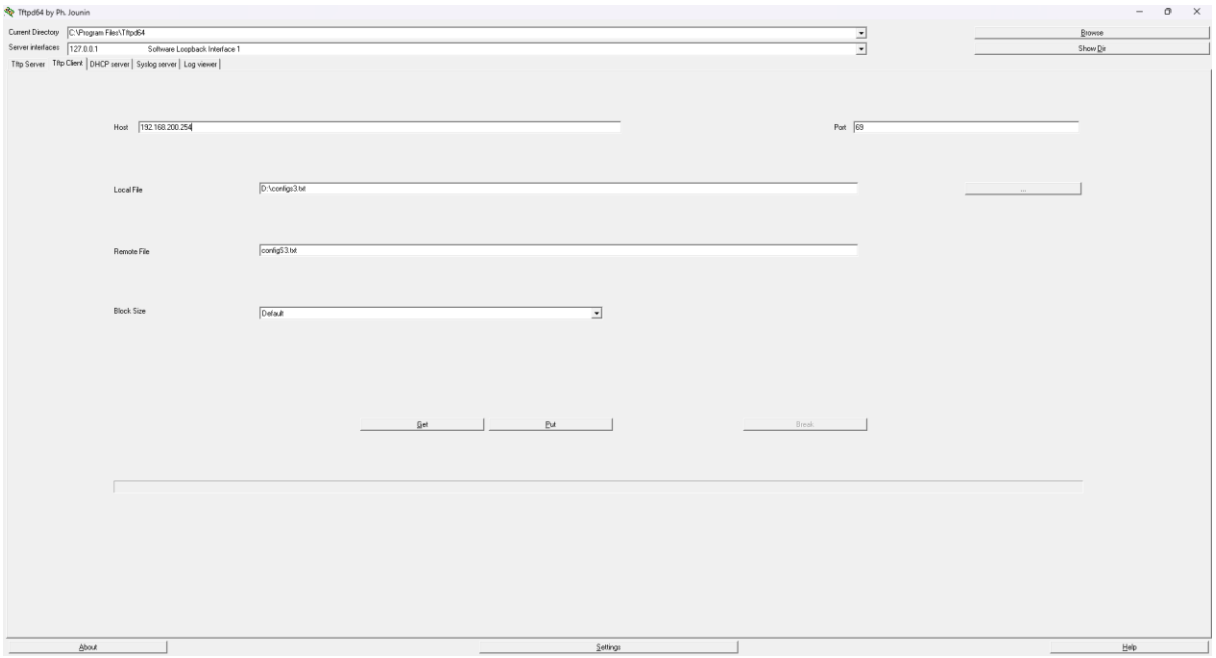
```
Protocol Version 4, Src: ETUROART19007.local (192.168.70.2), Dst: 192.168.200.254 (192.168.200.254)
```



Pour pouvoir récupérer la configuration nous devons pouvoir ping le serveur tftp. Pour cela nous allons ajouter une passerelle.



A la suite de ce ping réussi à l'aide du logiciel tftp64



Après avoir réalisé l'analyse des trames réseau, nous pouvons débuter l'étude des configurations nécessaires pour le **switch 3**. En passant par le **VLAN 8**, deux éléments clés doivent être identifiés :

1. **Un port en trunk avec le VLAN 150 en native :**
   Ce port doit permettre le transport de plusieurs VLANs, avec le **VLAN 150** configuré comme VLAN natif pour gérer le trafic non étiqueté.
2. **Un port avec le VLAN 8 pour établir la connexion avec le serveur TFTP :**
   Ce port est essentiel pour permettre la communication entre le serveur TFTP et le reste du réseau via le **VLAN 8**.

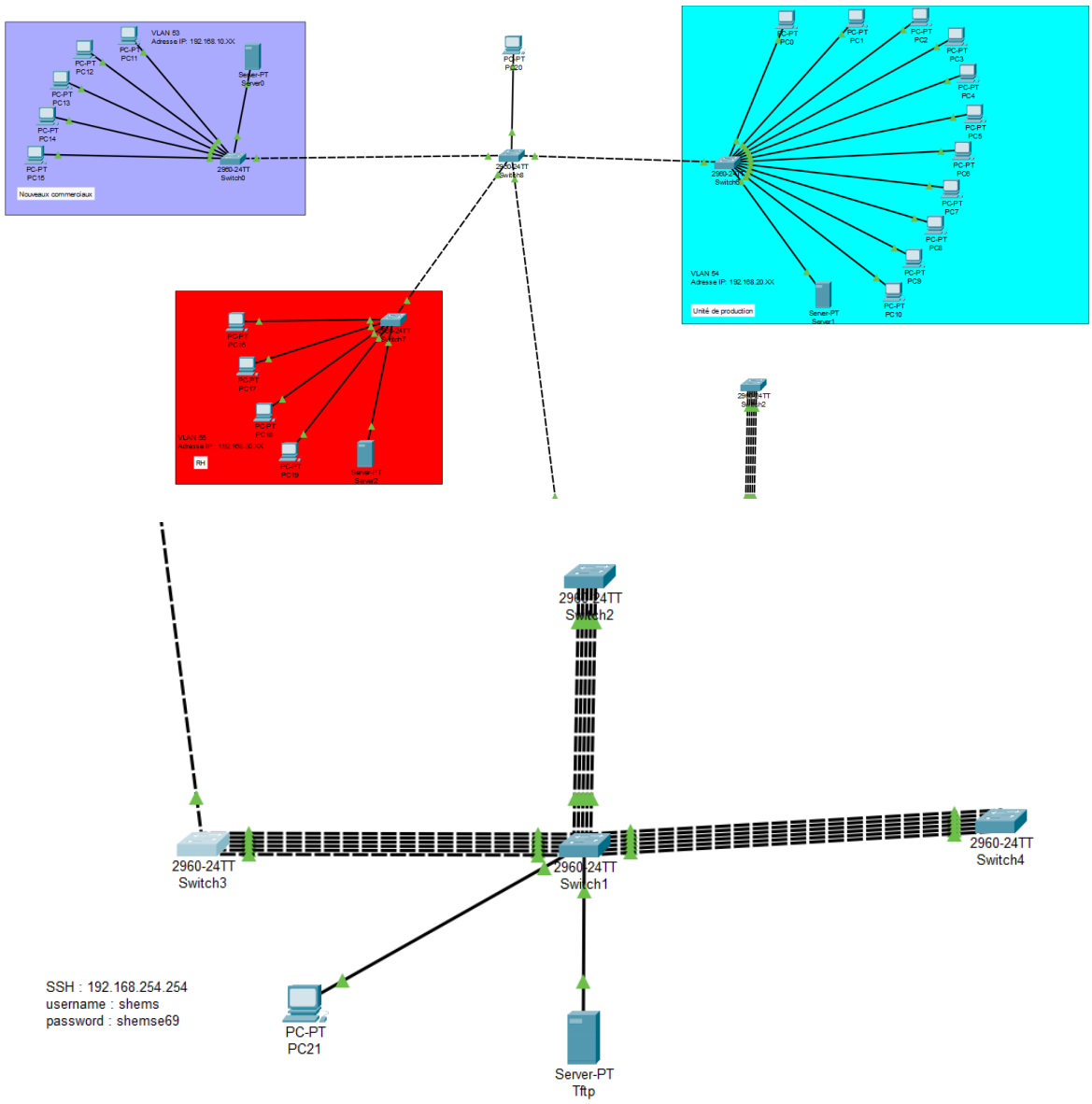
Lors de l'analyse, l'**interface 13** a été identifiée comme répondant à tous ces critères. En plus de transporter le **VLAN 8** pour la connexion au serveur TFTP et le **VLAN 150** en native, elle propose également trois VLANs supplémentaires, ce qui offre une flexibilité pour les configurations futures.

Cette interface regroupe donc les paramètres nécessaires pour l'interconnexion et l'évolution du réseau, facilitant à la fois la gestion actuelle et les configurations à venir.

```
interface fa0/13
switchport mode trunk
switchport trunk allowed vlan 8,53,54,55,150
switchport trunk native vlan 150
no sh
```

```
interface fa0/24
switchport mode trunk
switchport trunk allowed vlan 1-150
switchport trunk native vlan 150
no sh
```

Simulations réalisées



Pour la partie topologie, nous avons réalisé une configuration sur **Packet Tracer** afin d'intégrer un **nouveau LAN** à l'infrastructure existante. Sur l'image de la topologie, nous pouvons observer la configuration complète, incluant à la fois la baie initiale et le nouveau LAN ajouté.

Détails des choix réalisés :

1. **Choix du port sur le switch S3 :**
    - Nous avons sélectionné le port **fa0/13** sur le switch **S3**, car il offre une interface en **mode trunk** avec le **VLAN 150 configuré comme natif**.

- Ce port supporte également **trois VLANs consécutifs**, qui sont essentiels pour la configuration des différents LANs nécessaires à l'évolution de l'infrastructure.

2. **Configuration du nouveau switch :**
    - Le port **fa0/24** du switch nouvellement installé a été configuré comme une copie exacte du port **fa0/13** sur le switch S3.
    - Cette duplication garantit la continuité des paramètres réseau, notamment pour le **trunk**, le VLAN natif, et les VLANs supplémentaires.

La nouvelle configuration assure une intégration optimale entre l'infrastructure existante et le nouveau LAN, tout en conservant une structure cohérente et évolutive pour les futures extensions. Les choix réalisés, notamment au niveau des ports et des VLANs, garantissent une communication fluide entre les éléments du réseau.

```
S3#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      150
Fa0/24      on           802.1q         trunking      150

Port        Vlans allowed on trunk
Fa0/13      8,53-55,150
Fa0/24      1-150

Port        Vlans allowed and active in management domain
Fa0/13      8,150
Fa0/24      1,7,8,9,10,11,150

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      8,150
Fa0/24      1,7,8,9,10,11,150
```

Attribution des VLANs dans la Nouvelle Configuration

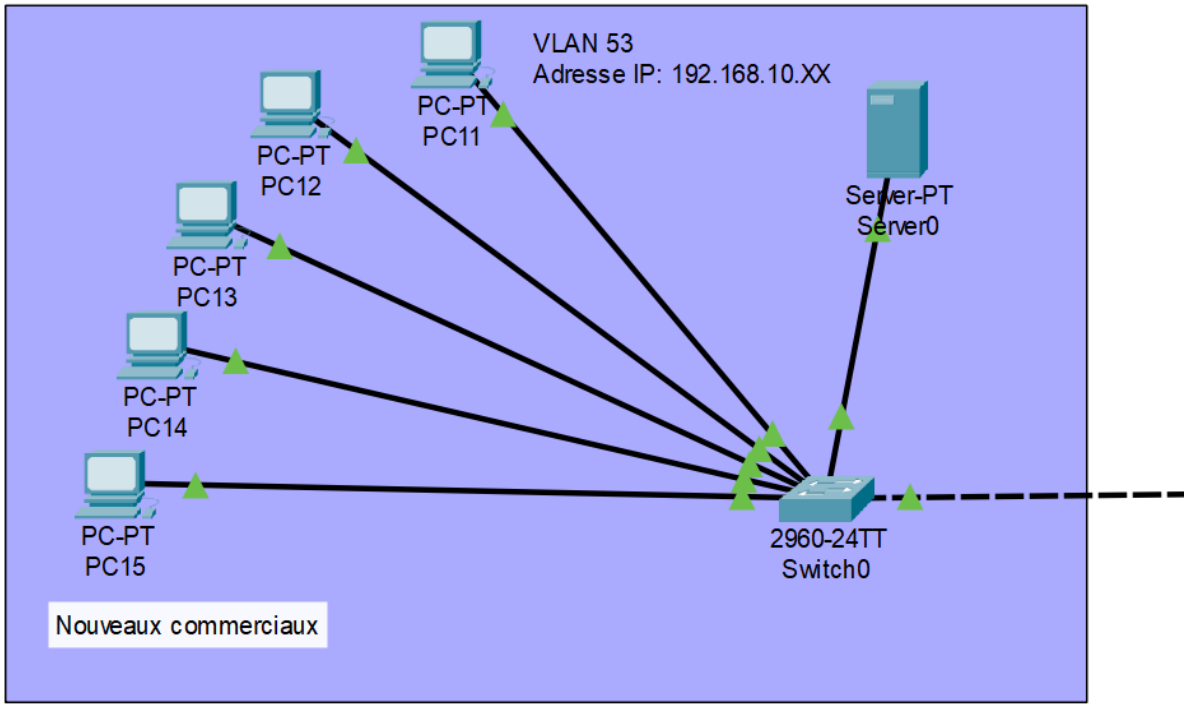
Les **VLANs** utilisés pour la configuration du nouveau LAN sont directement hérités du port **fa0/13** du switch **S3**, qui est en **mode trunk** et transporte plusieurs VLANs. Voici comment les VLANs ont été attribués :

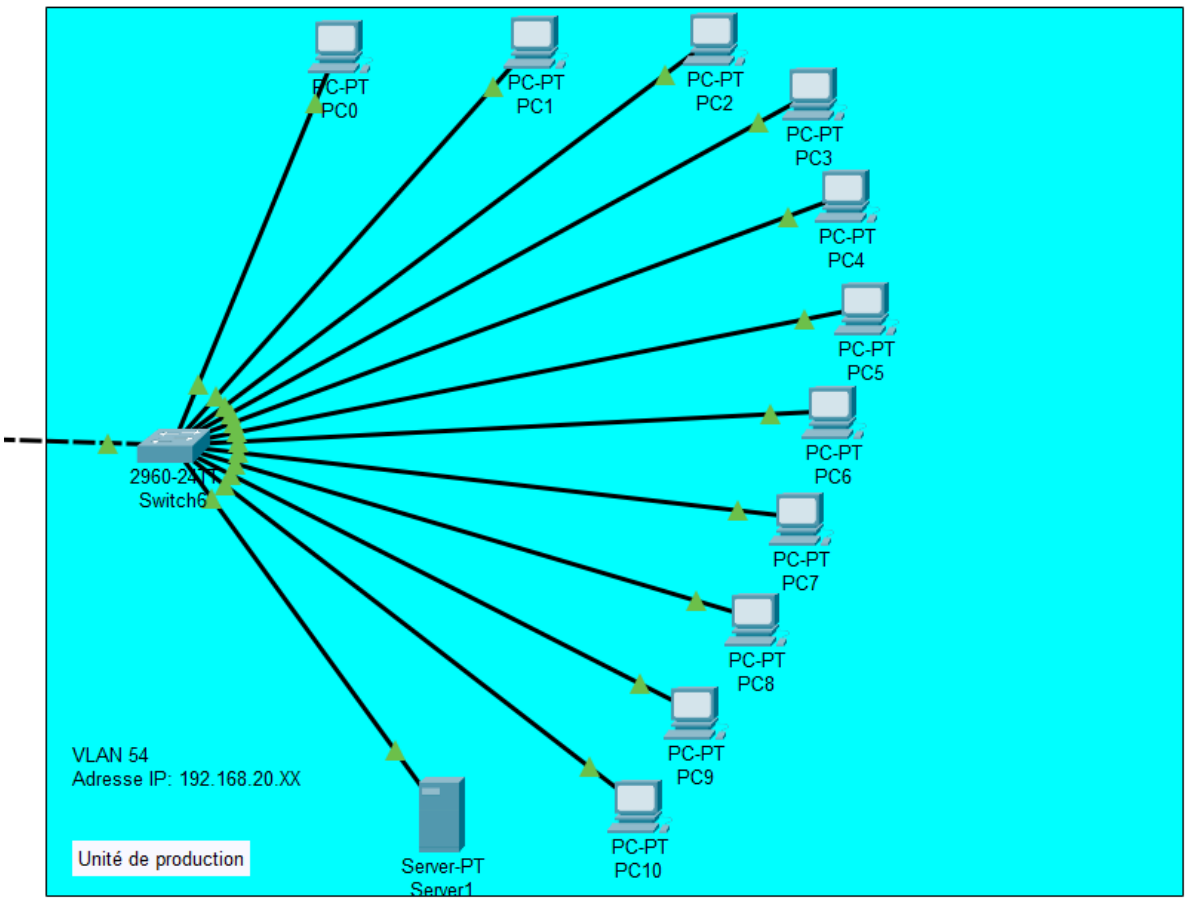
1. **VLAN 54** : Assigné à l'**unité de production**.
    - Ce VLAN est dédié aux équipements et utilisateurs liés à la production, assurant une isolation et une gestion spécifique du trafic pour cette unité.
2. **VLAN 53** : Réservé aux **nouveaux commerciaux**.
    - Il regroupe les postes et équipements des commerciaux récemment ajoutés, garantissant un réseau segmenté pour leurs besoins.
3. **VLAN 55** : Alloué aux **ressources humaines (RH)**.
    - Ce VLAN offre une séparation pour le trafic des RH, renforçant la sécurité et la gestion de leurs données.

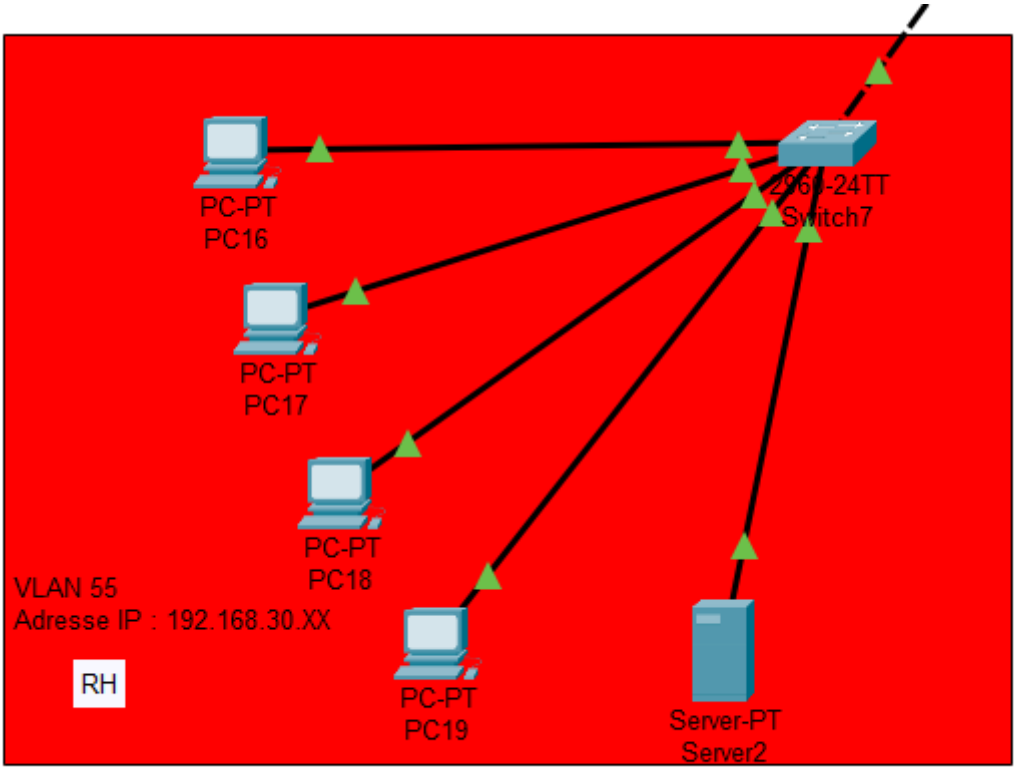
Grâce à cette répartition, chaque département ou groupe bénéficie de son propre VLAN, permettant :

- Une meilleure isolation du trafic réseau.
- Une gestion plus simple des permissions et des politiques de sécurité.
- Une organisation claire et évolutive pour les futures modifications.

Cette configuration garantit que le nouveau LAN est intégré harmonieusement à l'infrastructure existante tout en respectant les besoins spécifiques des différents services.


VLAN 53
Adresse IP: 192.168.10.XX
PC-PT
PC11
PC-PT
PC12
PC-PT
PC13
PC-PT
PC14
PC-PT
PC15
Server-PT
Server0
2960-24TT
Switch0
Nouveaux commerciaux


PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
PC-PT
PC6
PC-PT
PC7
PC-PT
PC8
PC-PT
PC9
PC-PT
PC10
2960-24TT
Switch6
VLAN 54
Adresse IP: 192.168.20.XX
Unité de production
Server-PT
Server1



L'intégration d'un **serveur DHCP** dans notre infrastructure permet d'automatiser la configuration des adresses IP. Cela présente plusieurs avantages majeurs :

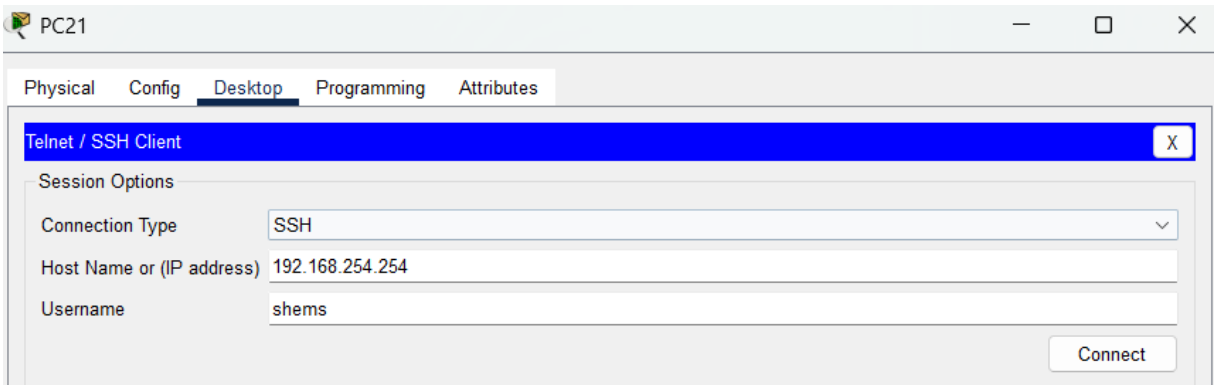
1. **Suppression de la configuration manuelle** :
   Les appareils connectés au réseau reçoivent automatiquement une adresse IP, un masque de sous-réseau, une passerelle par défaut et les adresses des serveurs DNS. Cela élimine le besoin de régler ces paramètres manuellement pour chaque appareil.
2. **Facilité de connexion pour les nouveaux appareils** :
   Lorsqu'un nouvel appareil est ajouté au réseau, il obtient instantanément une adresse IP valide sans nécessiter d'intervention externe. Cela simplifie le déploiement et améliore l'efficacité.
3. **Gestion centralisée** :
   Le serveur DHCP centralise la gestion des adresses IP, réduisant ainsi les erreurs liées aux configurations manuelles et évitant les conflits d'adresses IP.

Pour renforcer la sécurité et permettre une gestion à distance du **switch nouvellement installé**, le service **SSH** a été configuré. Voici les détails :

1. **Fonctionnalité du SSH** :
    - Le service **SSH** est opérationnel et permet d'accéder à la configuration du switch via une connexion sécurisée.
2. **Accès depuis le réseau** :
    - SSH est accessible à partir d'un **ordinateur connecté au port 18** du switch **S1**. Ce port appartient au **VLAN 150**, garantissant que l'accès est isolé dans un segment réseau sécurisé.
3. **Sécurité renforcée** :
    - Un mot de passe sécurisé a été choisi pour l'accès SSH, protégeant ainsi le switch contre les accès non autorisés.
    - La configuration inclut probablement des pratiques sécurisées comme la désactivation de Telnet pour privilégier SSH, le choix d'algorithmes de chiffrement robustes, et l'utilisation d'utilisateurs spécifiques pour les connexions.

Avantages :

- La gestion à distance est désormais sécurisée et centralisée.
- Le VLAN 150, dédié au management, garantit que seul le trafic autorisé peut accéder au switch via SSH.
- Cette configuration prépare le réseau pour une maintenance et une gestion efficace, sans compromis sur la sécurité.



Commandes qui ont permis la configuration SSH :

hostname switch-principal

ip domain-name reseau.local

crypto key generate rsa

2048

line vty 0 15

transport input ssh

login local

exit

username shems privilege 15 secret shemse69

ip ssh version 2

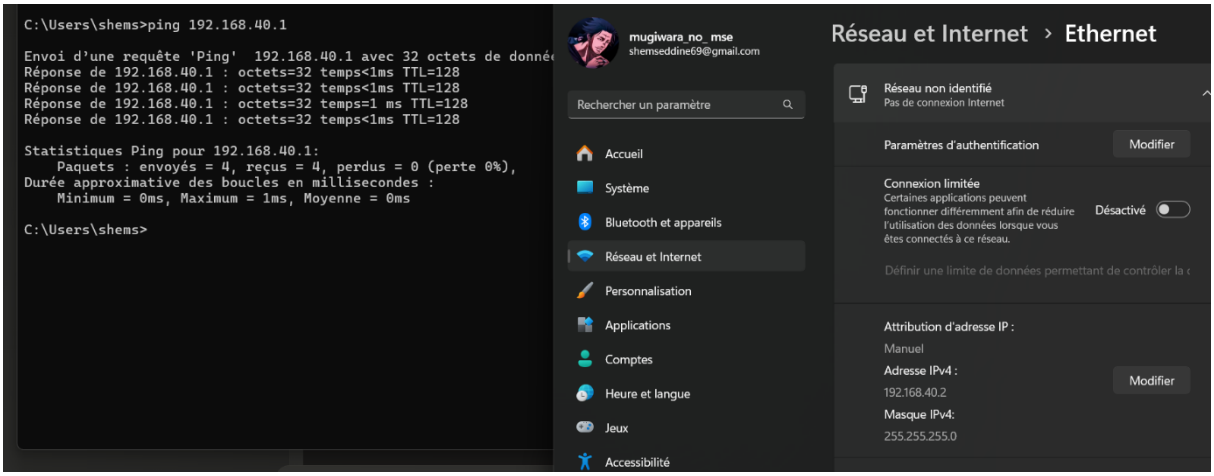
exit

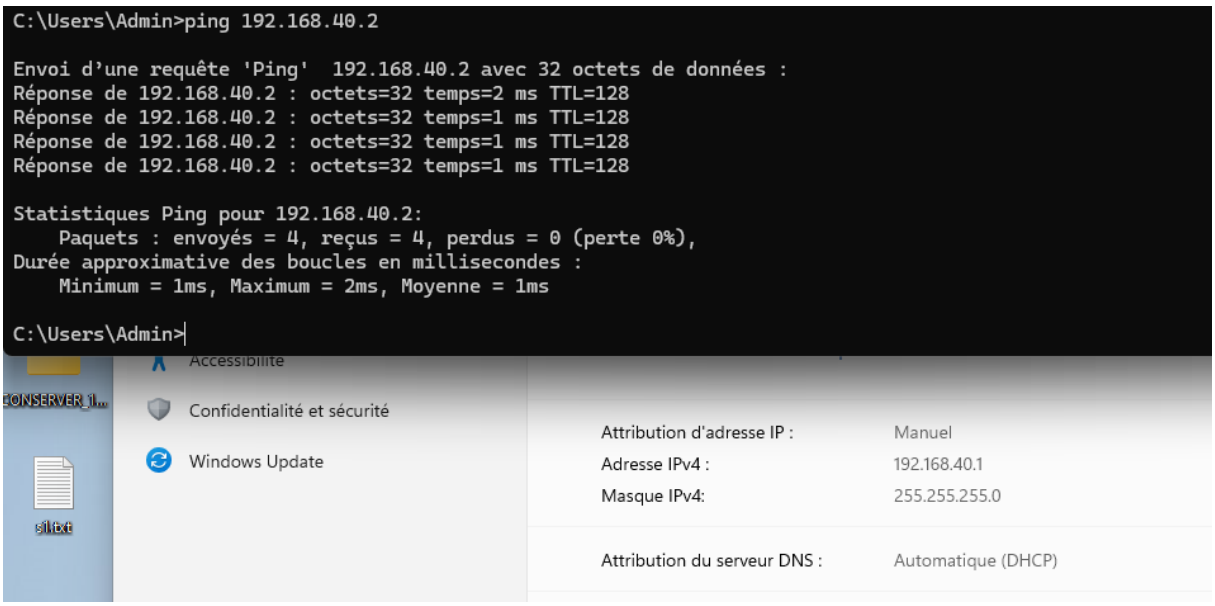
write memory

Résultats et interprétations

Pour vérifier la connectivité au sein du même VLAN, nous avons réalisé un test en utilisant deux ordinateurs : un PC portable et un PC de l'IUT. Ces deux appareils ont été placés dans le même VLAN, leur permettant de partager le même domaine de diffusion. Les adresses IP ont été configurées de manière à être compatibles avec le sous-réseau de ce VLAN.

Ensuite, un **ping** a été effectué entre les deux ordinateurs. Ce test a confirmé que la communication entre les deux PC était fonctionnelle, sans perte de paquets.





Ensuite, nous avons testé la connectivité entre deux machines virtuelles installées sur les mêmes appareils utilisés précédemment, à savoir le PC

portable et le PC de l'IUT. Ces machines virtuelles ont également été configurées pour être dans le même VLAN, tout comme les appareils physiques.

Un **ping** a été effectué entre les deux machines virtuelles. Ce test a permis de vérifier que la communication réseau fonctionnait correctement entre elles, confirmant ainsi que la configuration réseau du VLAN est bien opérationnelle, non seulement pour les appareils physiques mais aussi pour les machines virtuelles hébergées sur ces derniers.

Ce test valide également l'intégration des machines virtuelles dans l'infrastructure réseau existante et leur compatibilité avec la segmentation en VLAN.