



Réseaux 2

Soumis au chargé de cours : Ismaël SAINT AMOUR

Préparé par : Jameson DOMINIQUE

Date : 28 Mai 2025

Projet 1 : Étude et Mise en Œuvre des Protocoles Telnet et SSH

avec GNS3 et Cisco Packet Tracer

Objectif du Projet

Ce projet vise à :

1. Comparer et analyser les protocoles Telnet et SSH en termes de fonctionnement, sécurité, et applications.
2. Configurer et sécuriser des connexions à distance sur des équipements réseau en utilisant ces protocoles.
3. Expérimenter les vulnérabilités de Telnet et comprendre l'importance de SSH en tant que protocole sécurisé.

Livrables du Projet

1. Diagramme de topologie réseau : Schéma de la topologie utilisée pour les tests.
2. Rapport technique : Comparaison des protocoles Telnet et SSH, avec une analyse de la sécurité.
3. Configuration réseau : Scripts ou fichiers de configuration pour chaque appareil utilisé dans le projet.
4. Capture de paquets : Exemple de paquets Telnet non chiffrés et paquets SSH chiffrés.
5. Présentation : Résumé des résultats du projet pour présentation en classe.

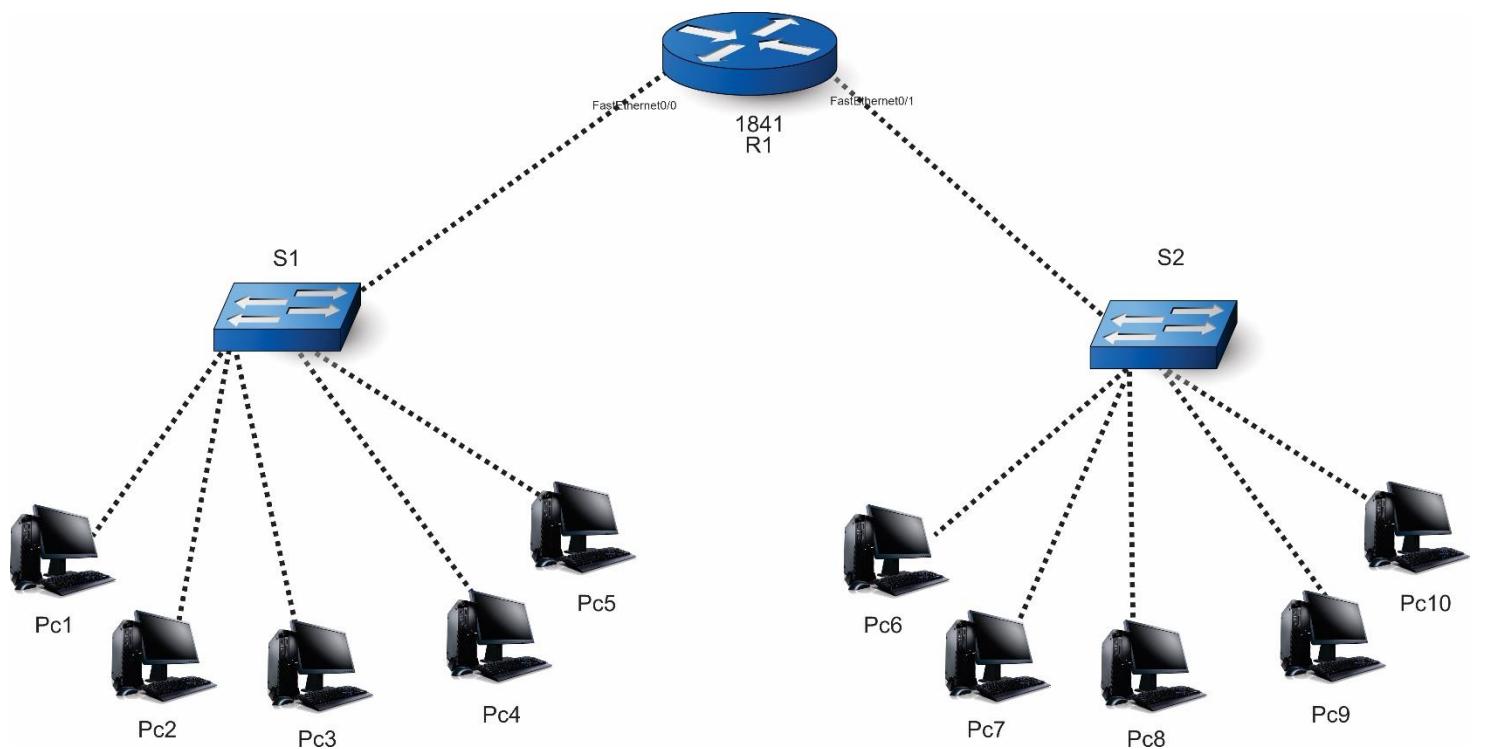
Évaluation du Projet

Les critères d'évaluation incluent :

1. La précision de la configuration des appareils pour Telnet et SSH.
2. L'analyse de sécurité : capacité à identifier les vulnérabilités de Telnet et à démontrer la sécurité de SSH.
3. La qualité du rapport : Le rapport doit inclure des captures d'écran des configurations, des captures de paquets (si possible), une comparaison détaillée et des recommandations.
4. Présentation orale : Résumer les principaux résultats et démontrer la configuration dans Packet Tracer, en expliquant l'importance de la sécurité réseau.

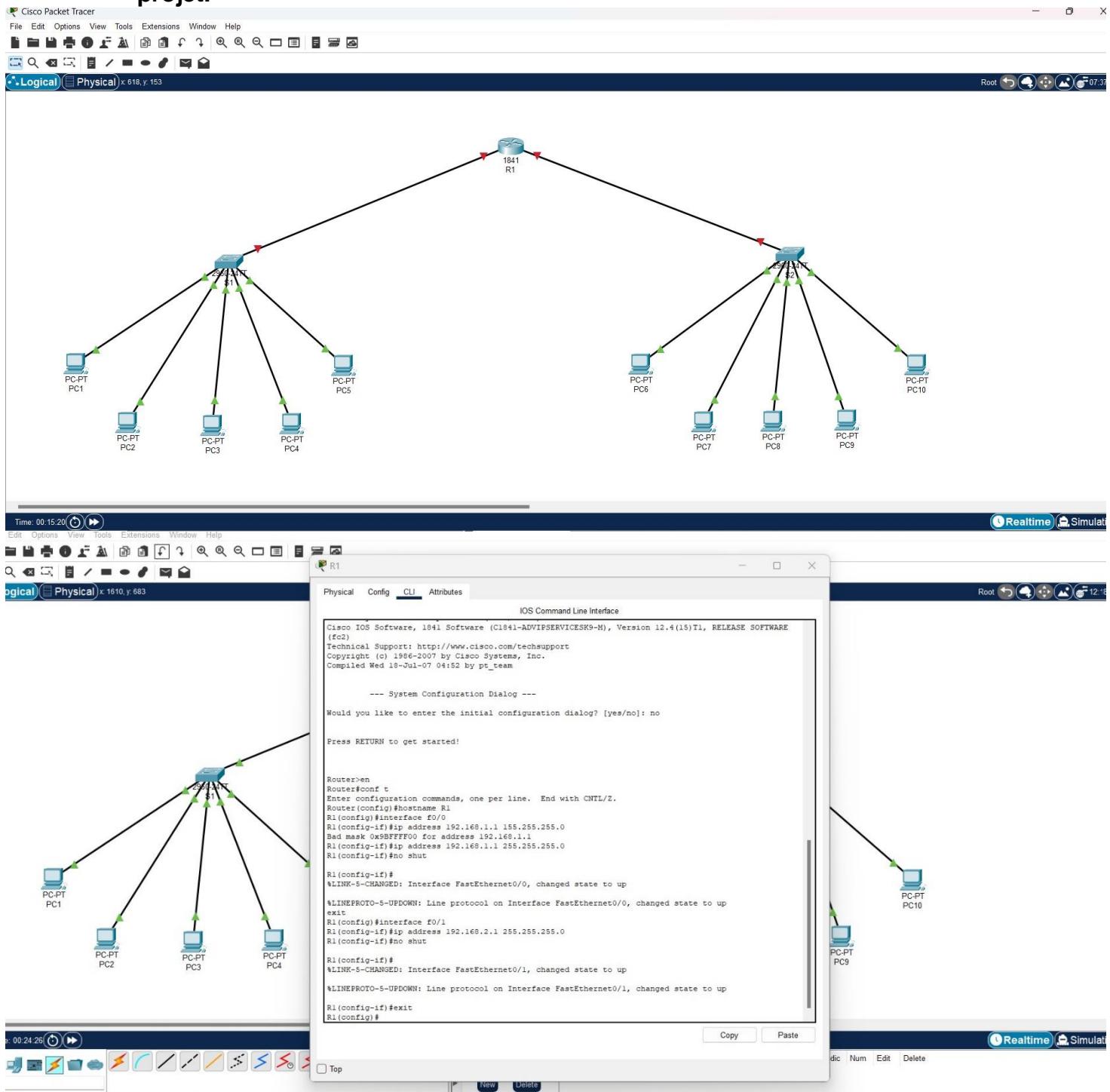
Pour Cisco Packet Tracer

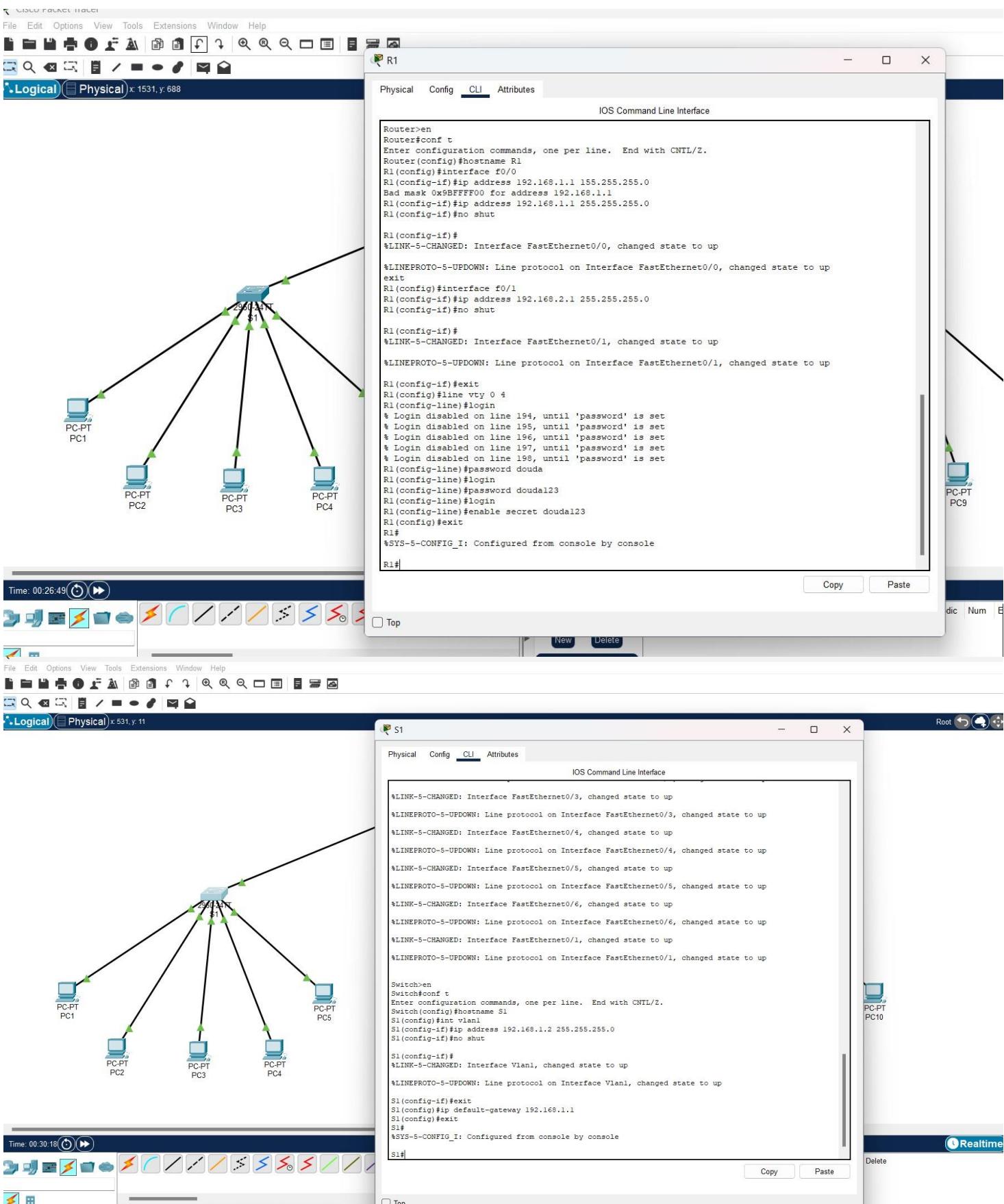
- **Diagramme de topologie réseau.**



• Configuration réseau.

Scripts ou fichiers de configuration pour chaque appareil utilisé dans le projet.





File Edit Options View Tools Extensions Window Help

Logical Physical x 1355, y 285 Root

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#int vlan1
S2(config)#ip add 192.168.2.2 255.255.255.0
S2(config)#no shut

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#ip default-gateway 192.168.2.1
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#
```

Copy Paste

Time: 00:32:04

PC-PT PC10 Delete

PC1

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

DHCP Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

Automatic Static

IPv6 Address: FE80::240:BFF:FEAE:5493

Link Local Address:

Default Gateway:

DNS Server:

802.1X

Use 802.1X Security

Authentication: MD5

Username:

Password:

PC-PT PC10 Delete

Realtime

PC2

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

DHCP

Static

IPv4 Address 192.168.1.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

Automatic

Static

IPv6 Address FE80::209:7CFF:FEC2:A285

Link Local Address

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication MD5

Username

Password

PC-PT PC10

Realtime Delete

PC3

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

DHCP

Static

IPv4 Address 192.168.1.12

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

Automatic

Static

IPv6 Address FE80::2E0:F7FF:FE3D:5C24

Link Local Address

Default Gateway

DNS Server

802.1X

Use 802.1X Security

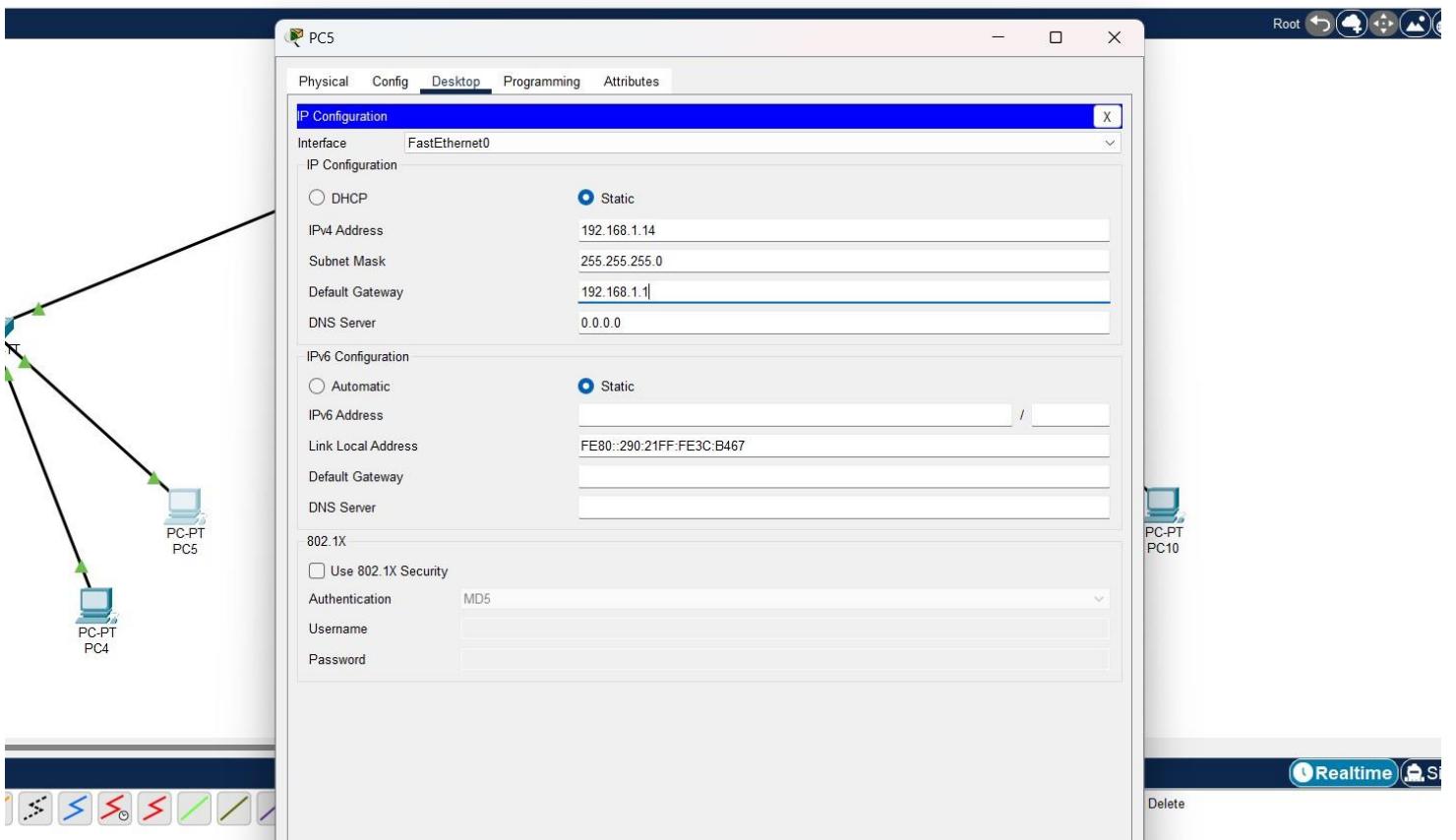
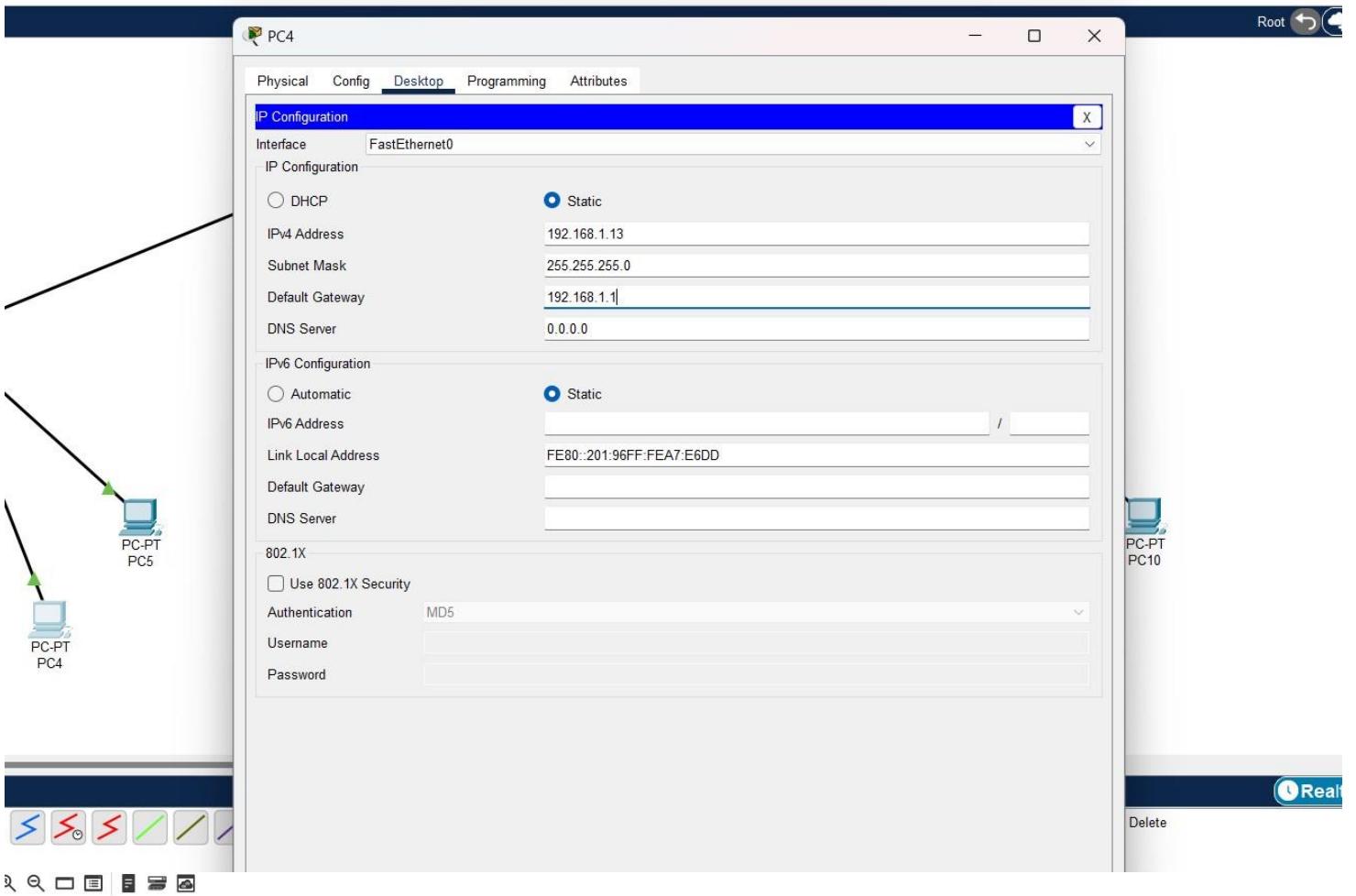
Authentication MD5

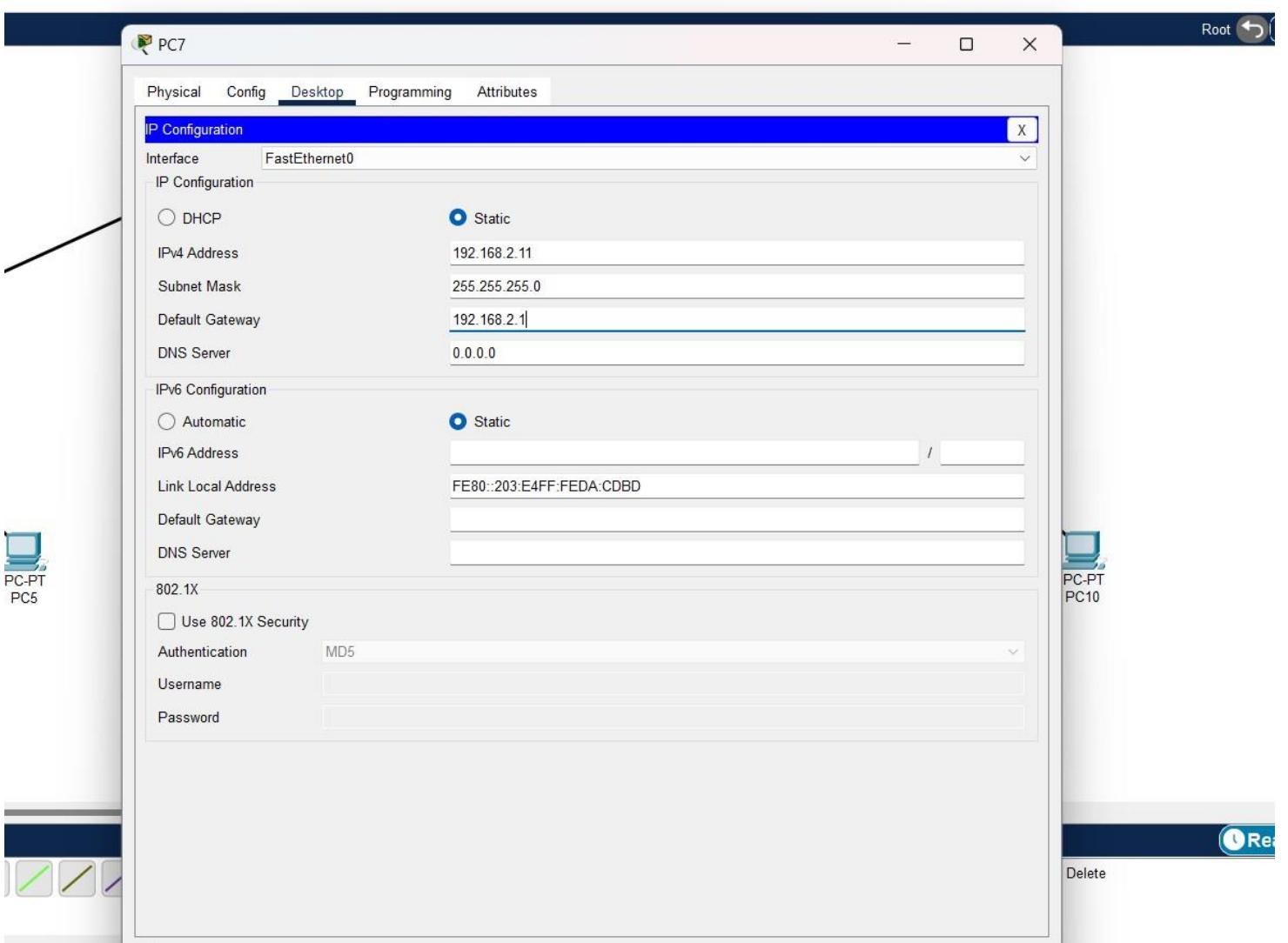
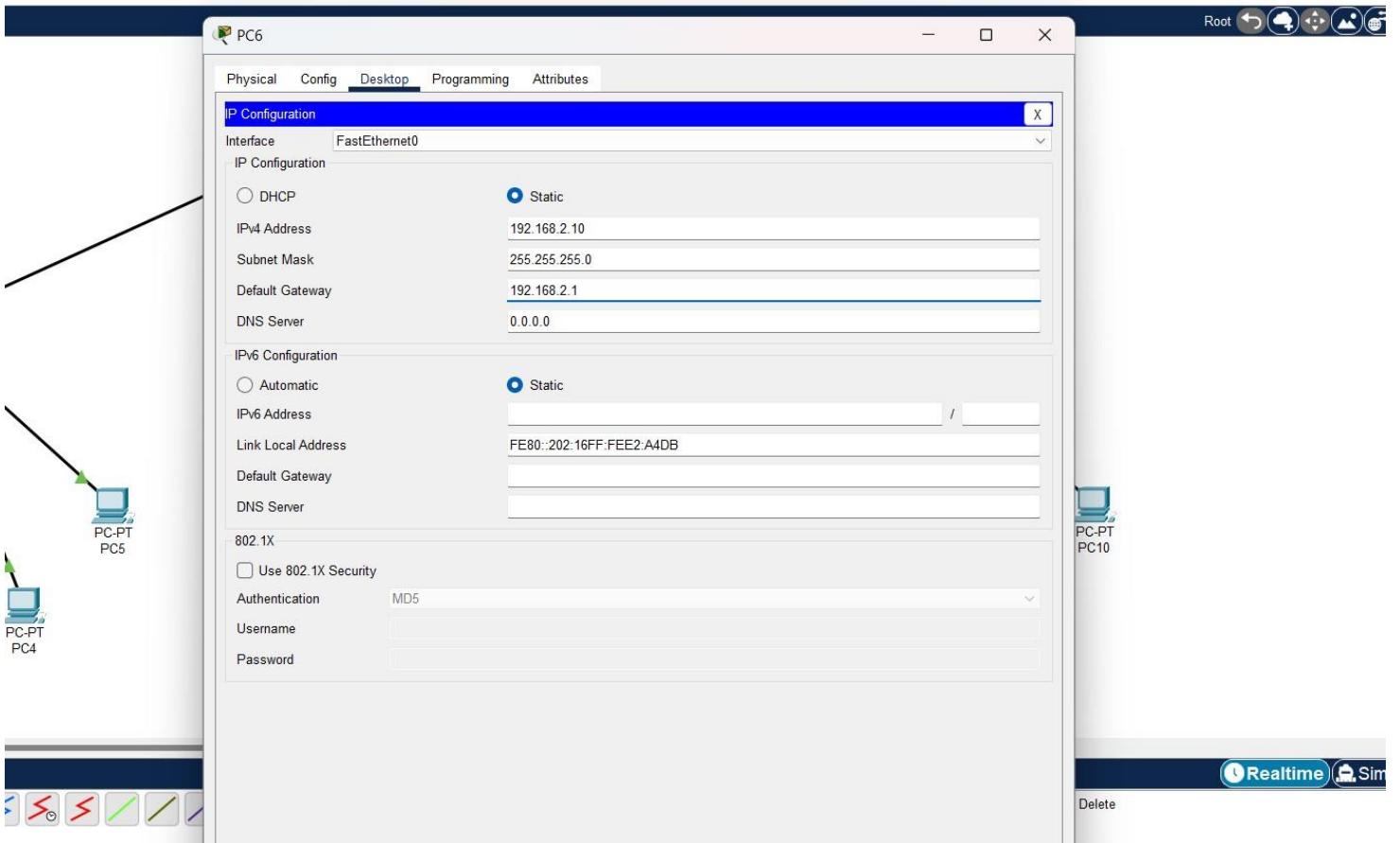
Username

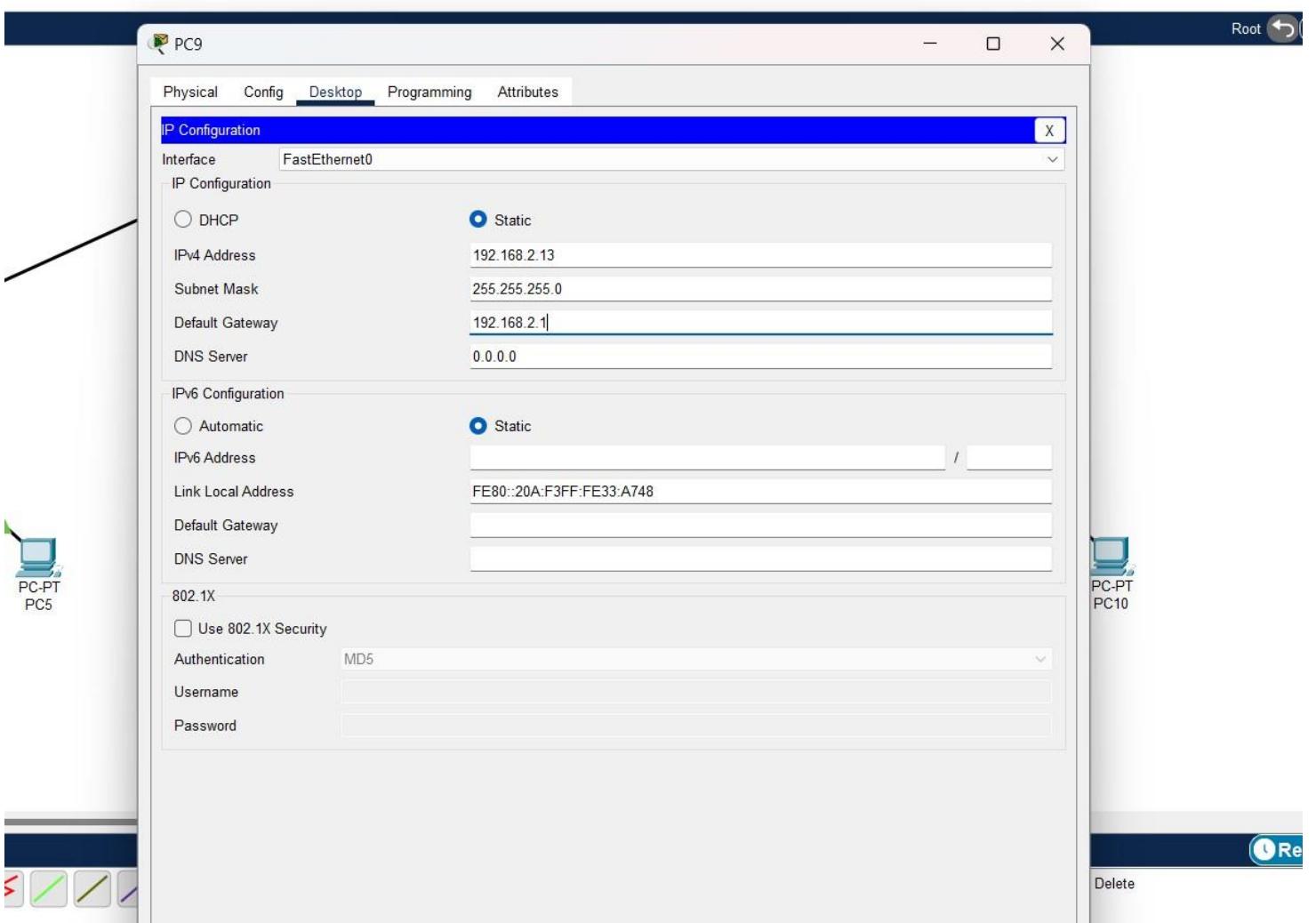
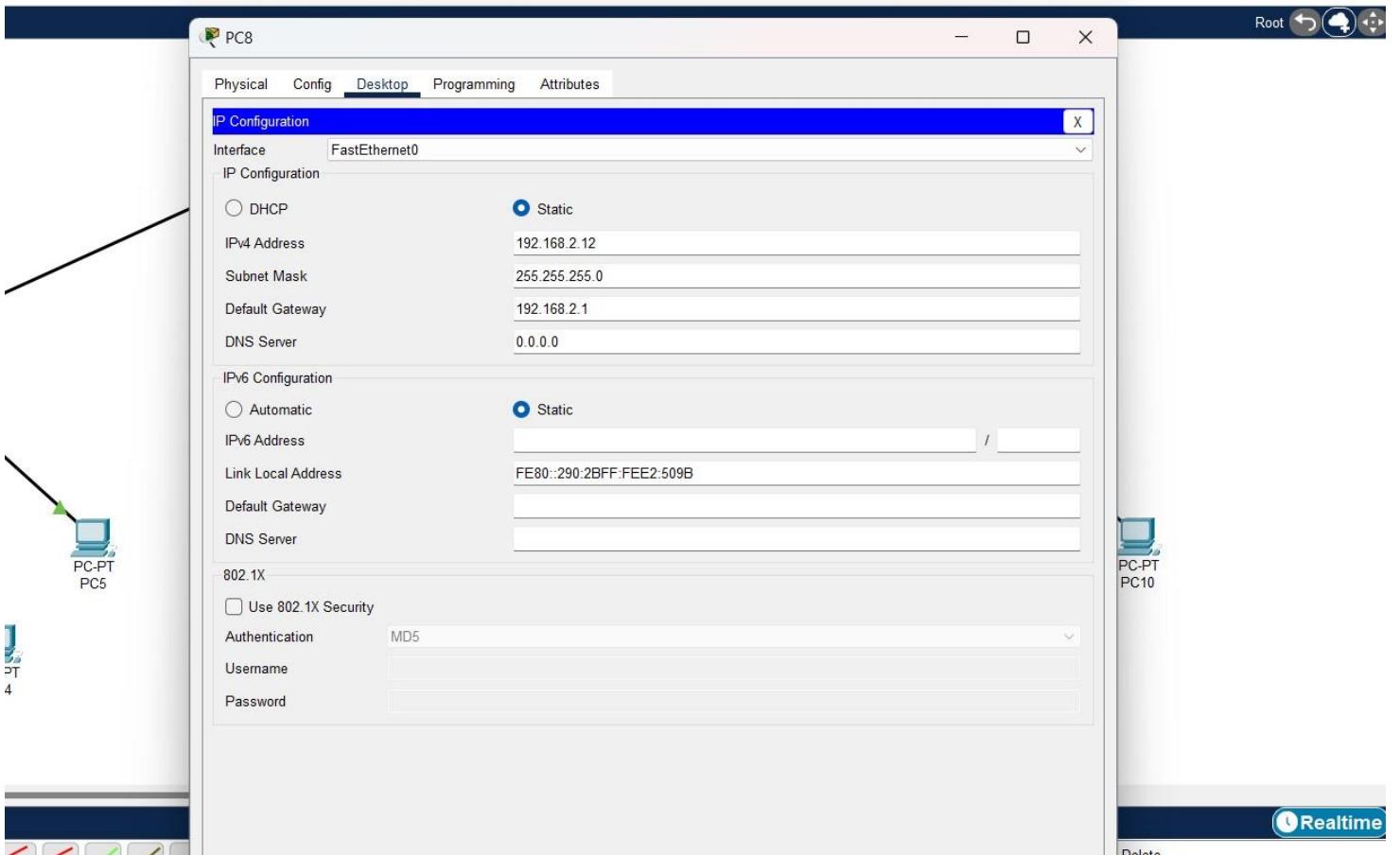
Password

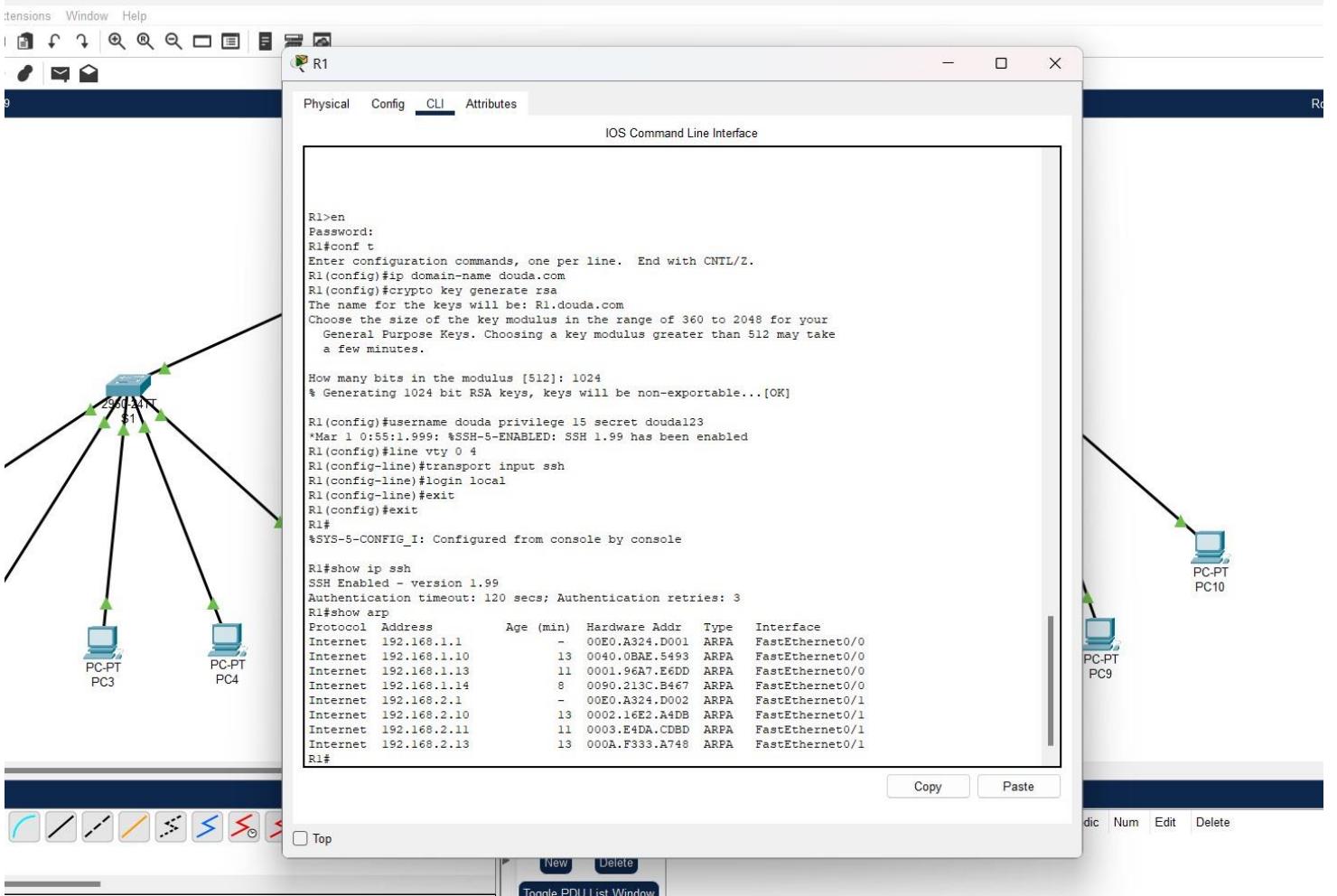
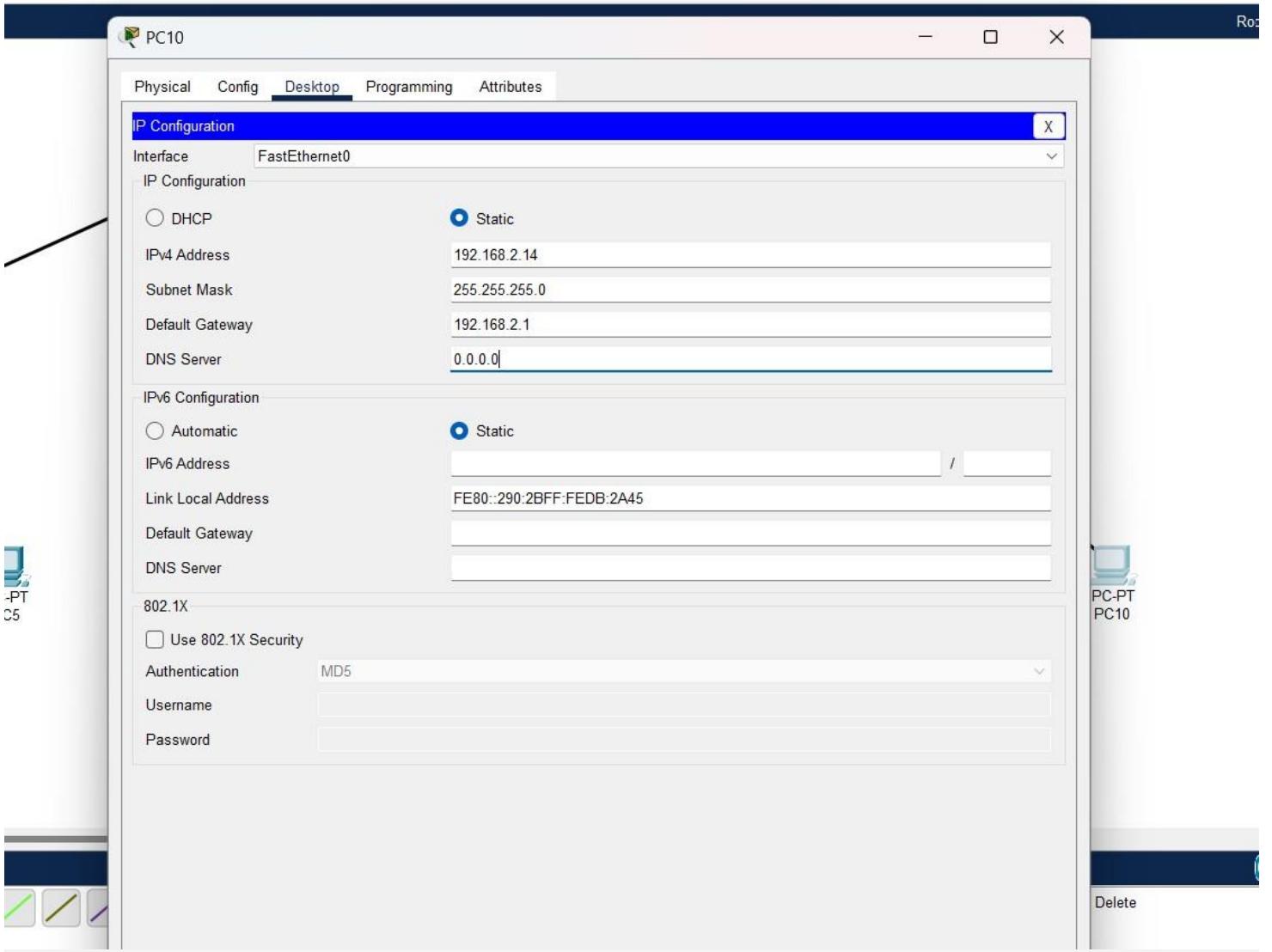
PC-PT PC10

Realtime Delete

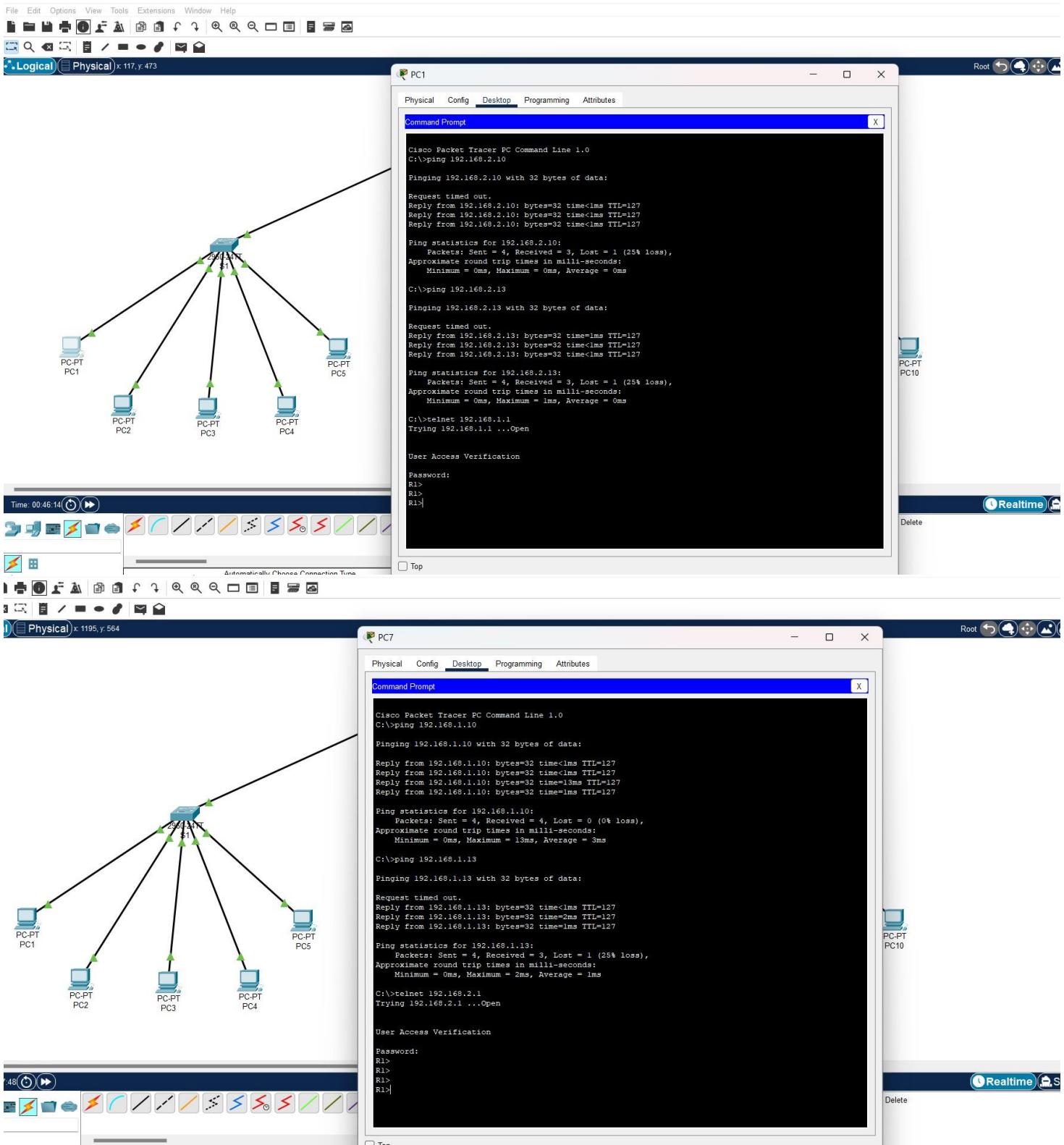


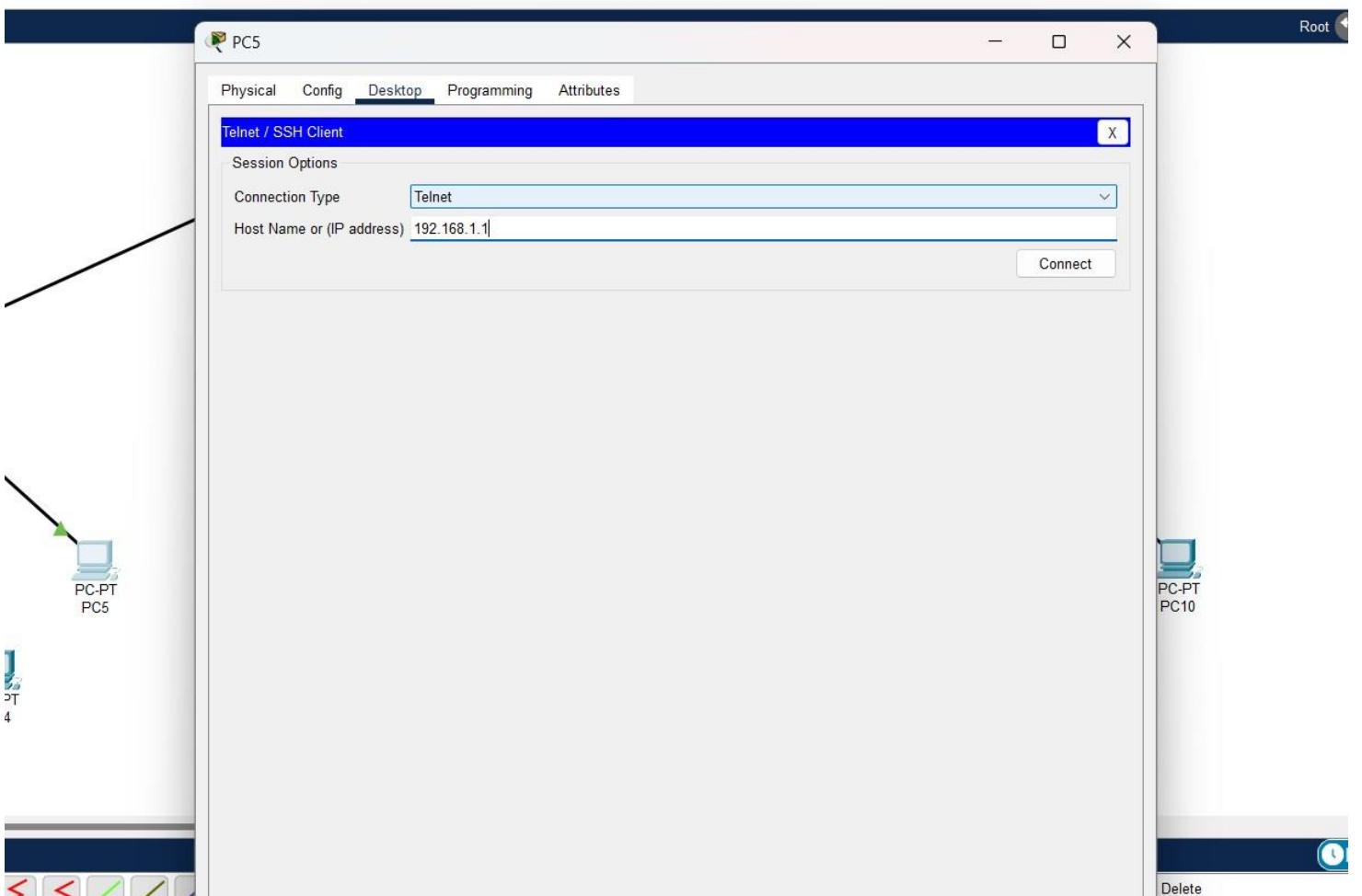
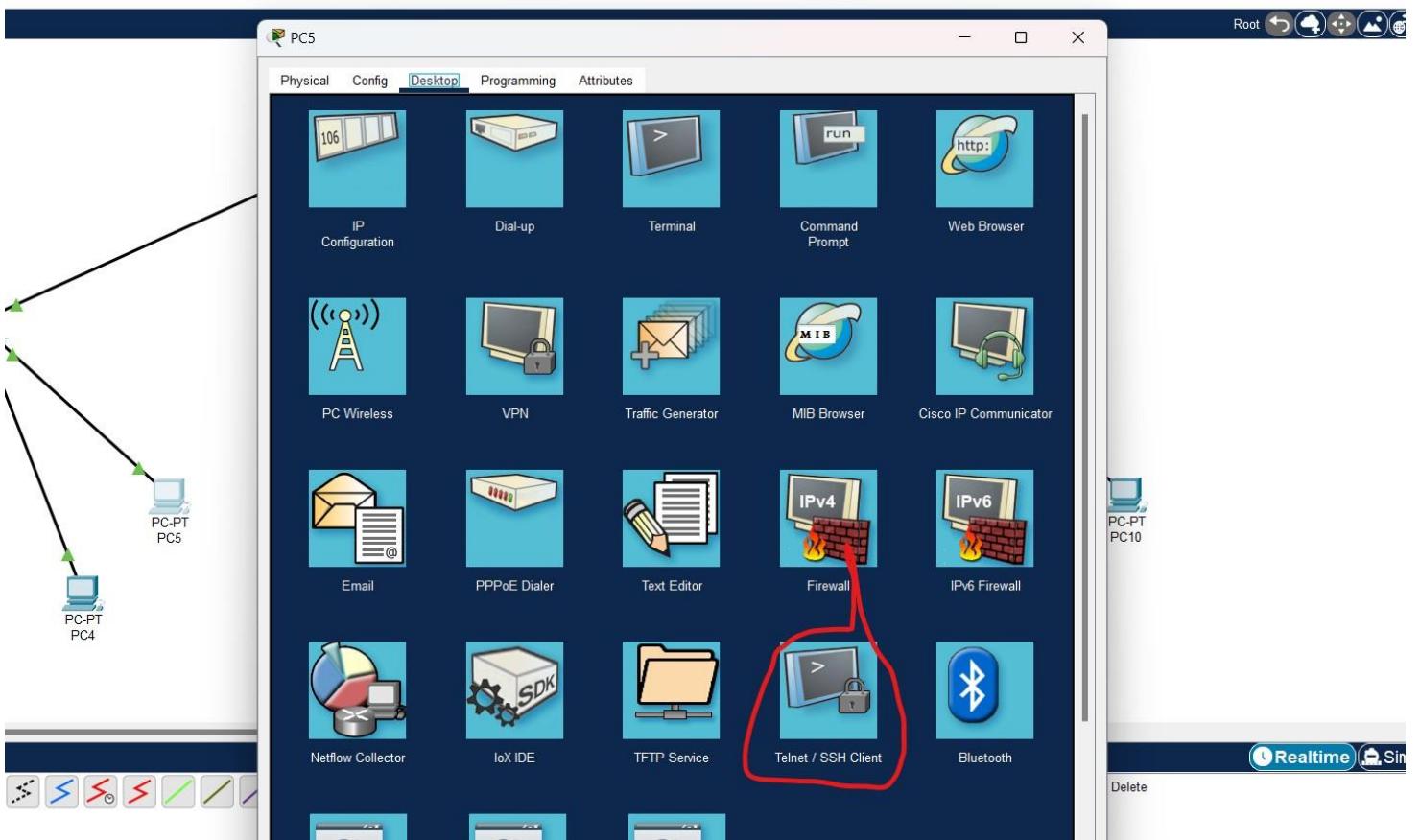


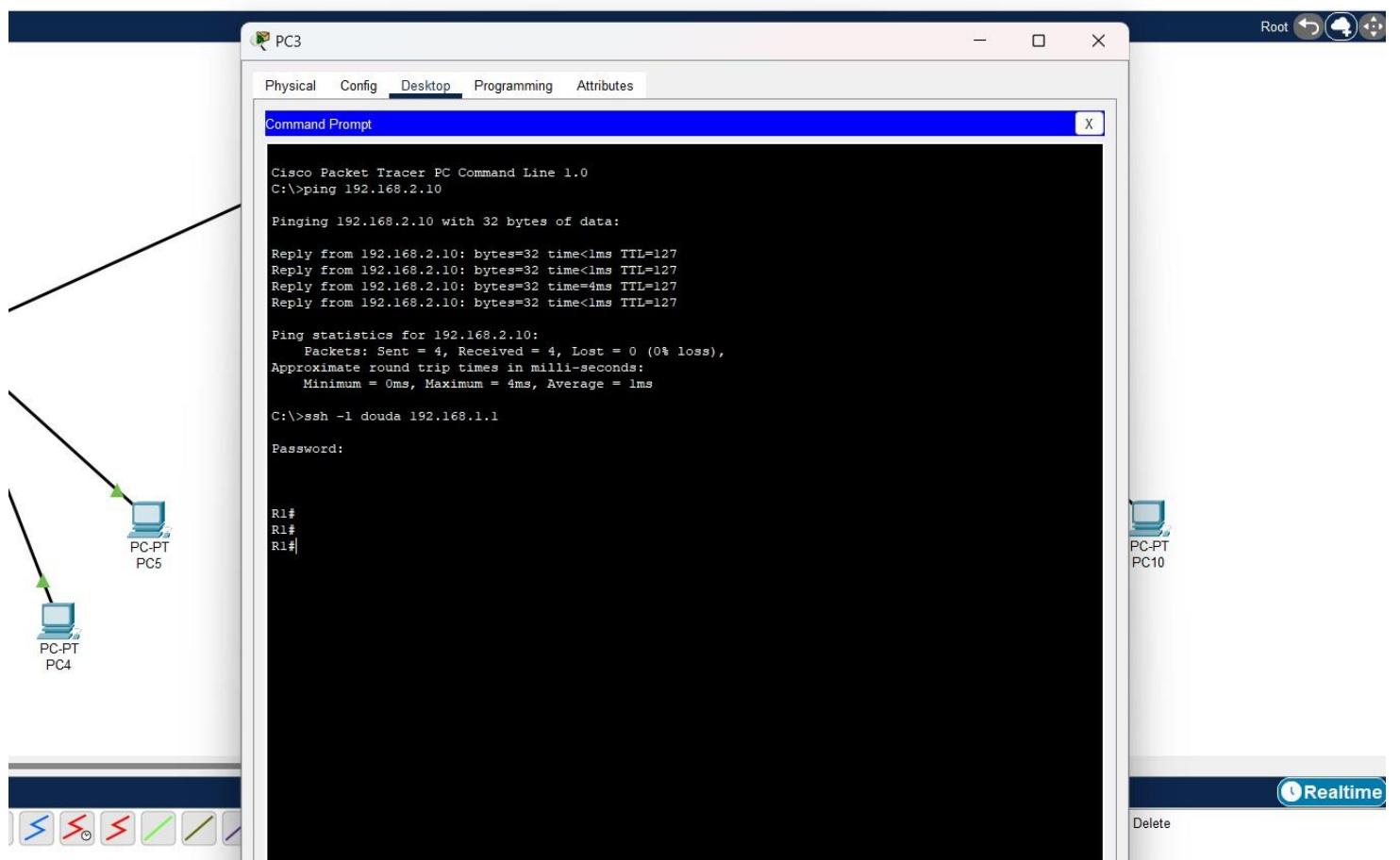
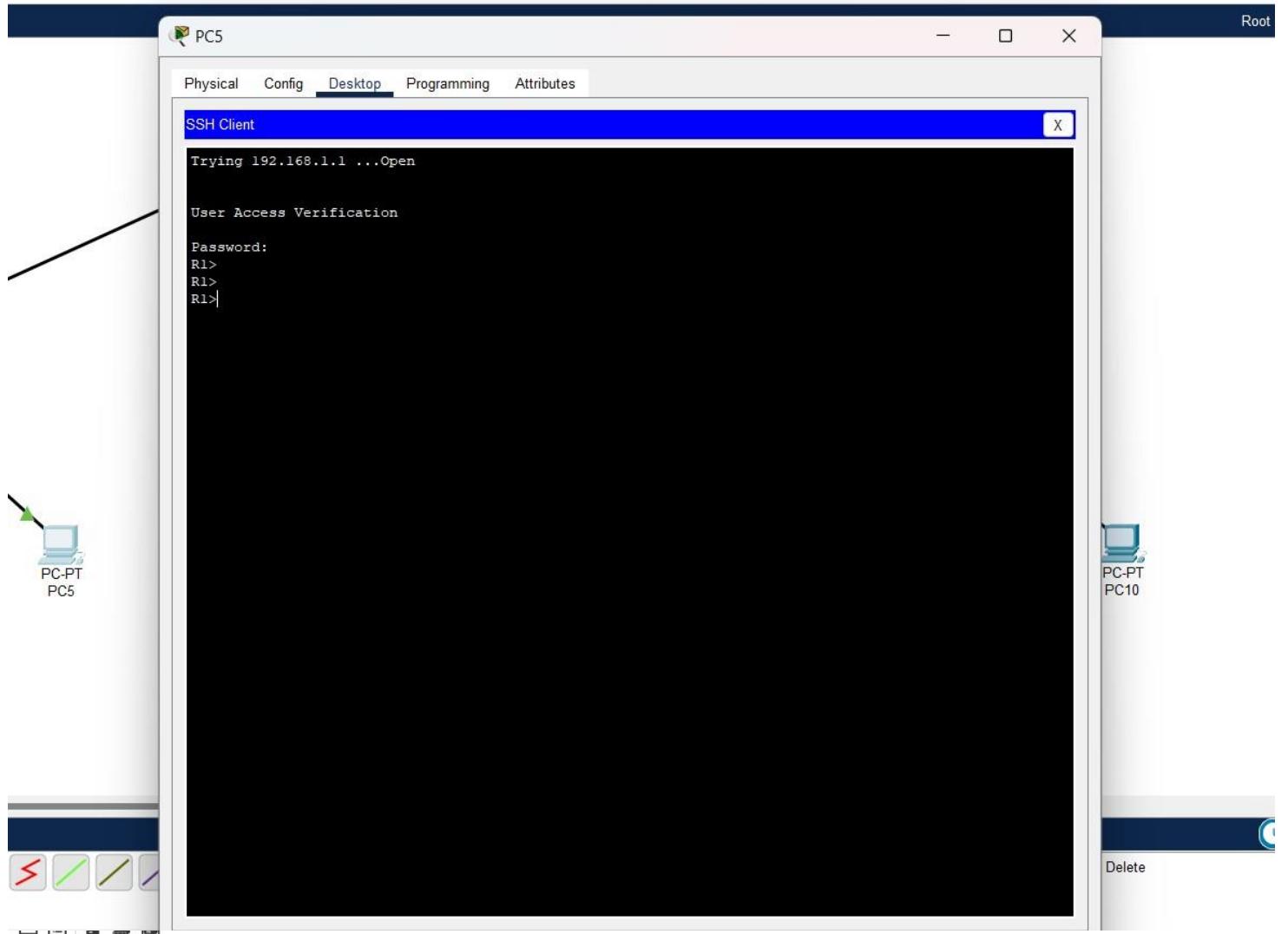


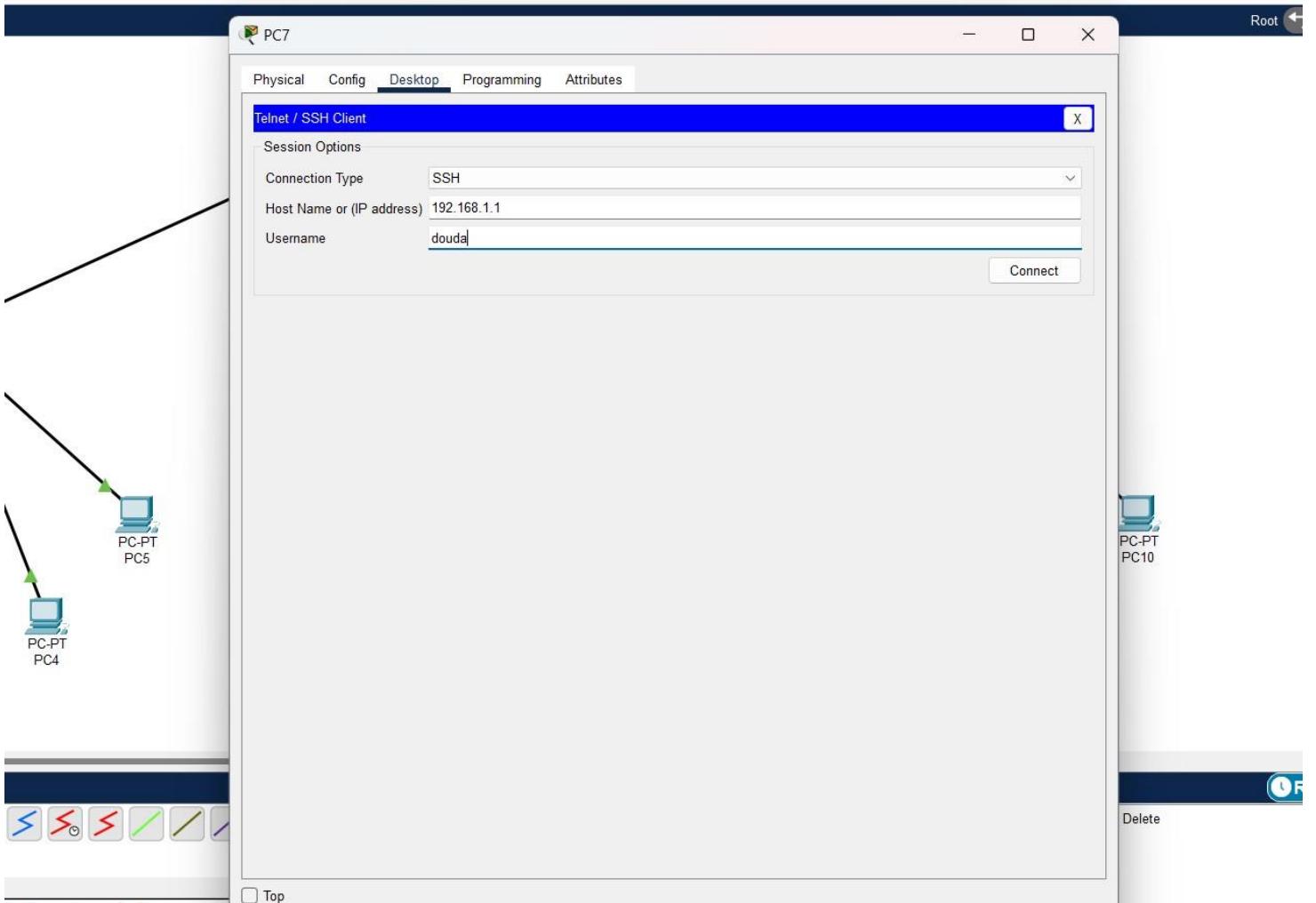


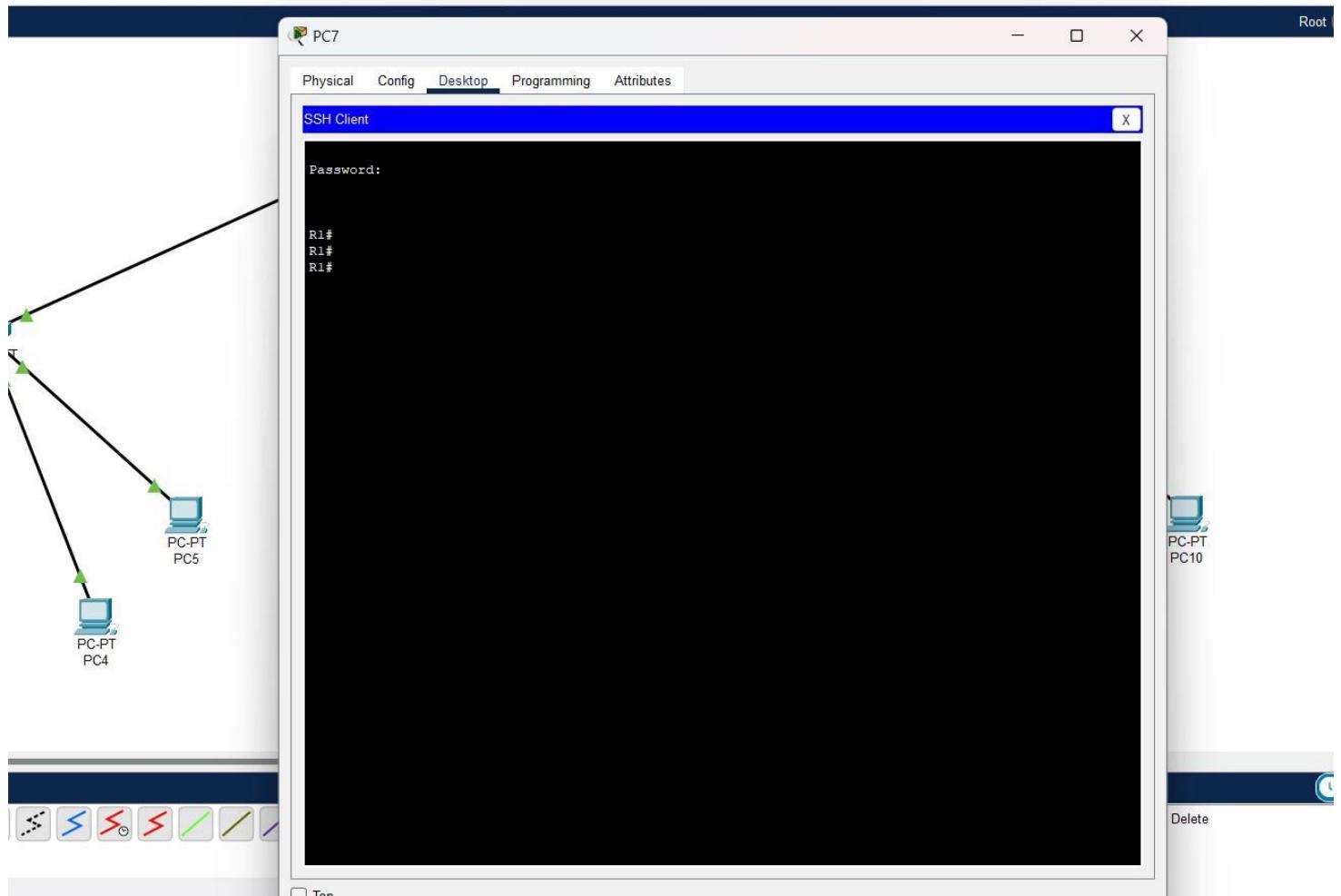
• Tests et Observations sur Cisco Packet Tracer





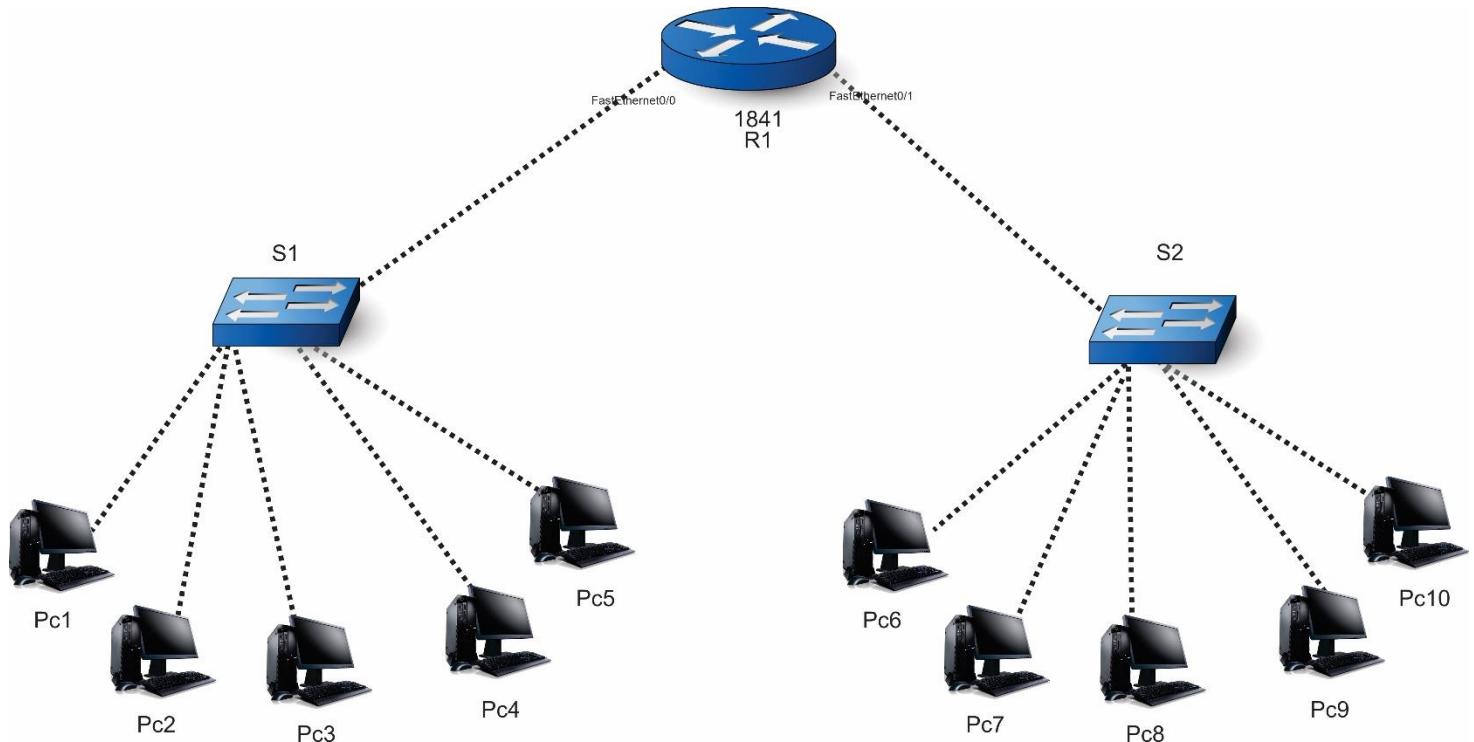




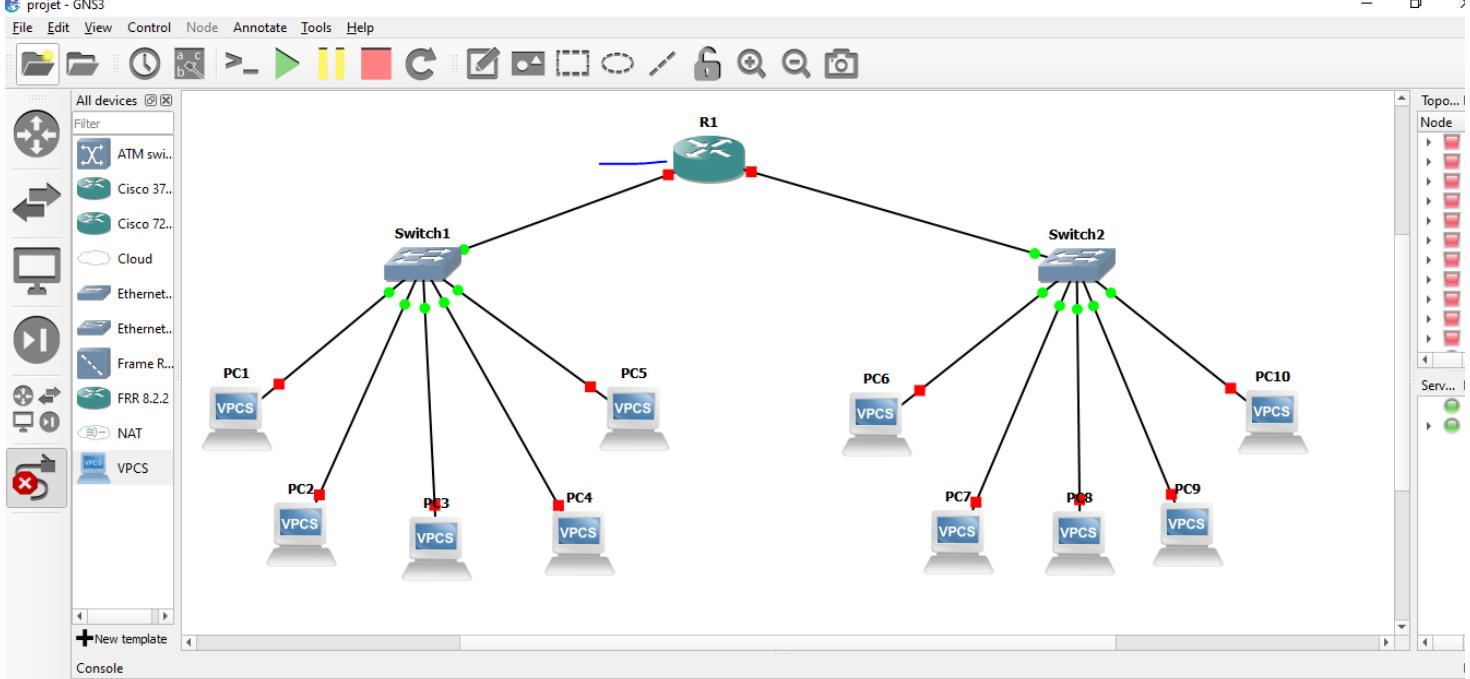
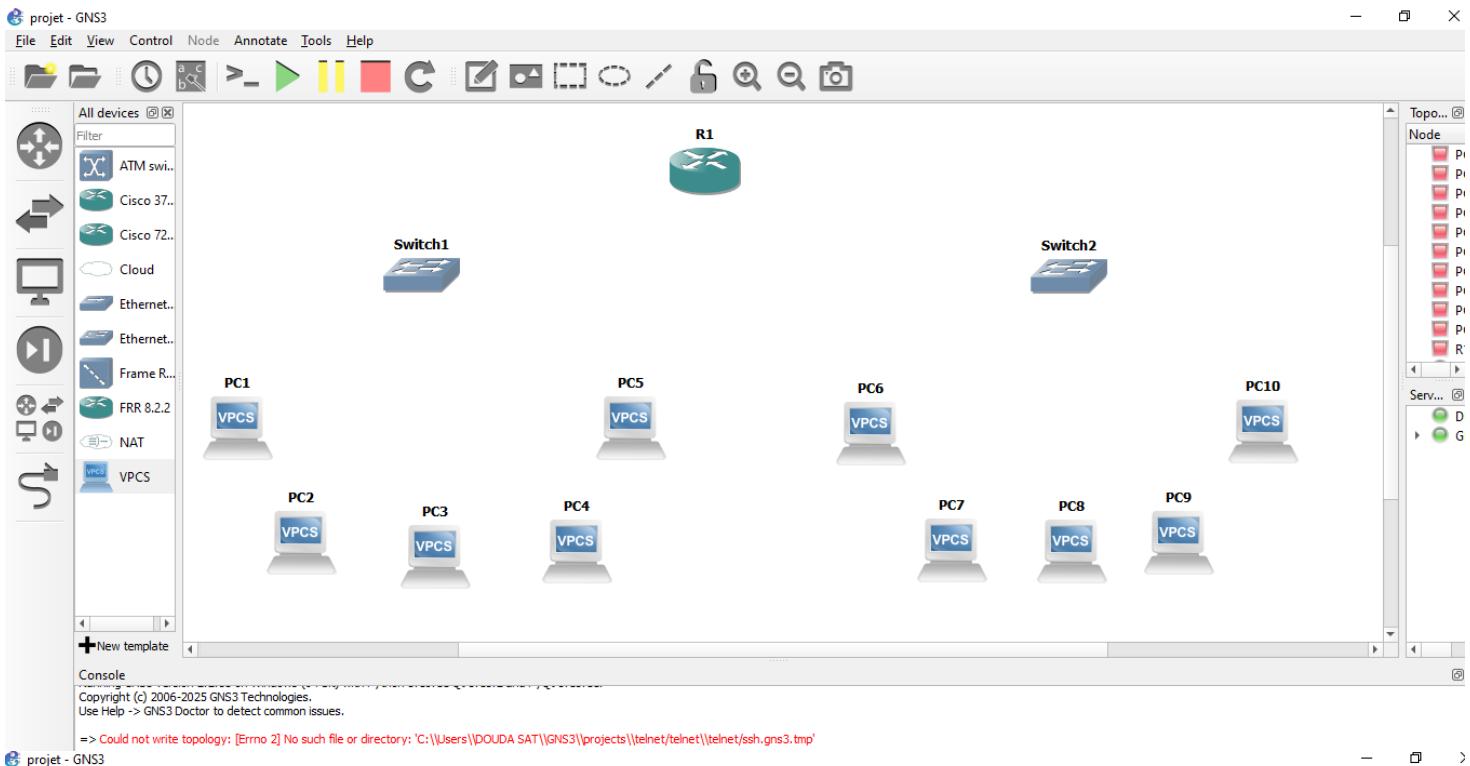


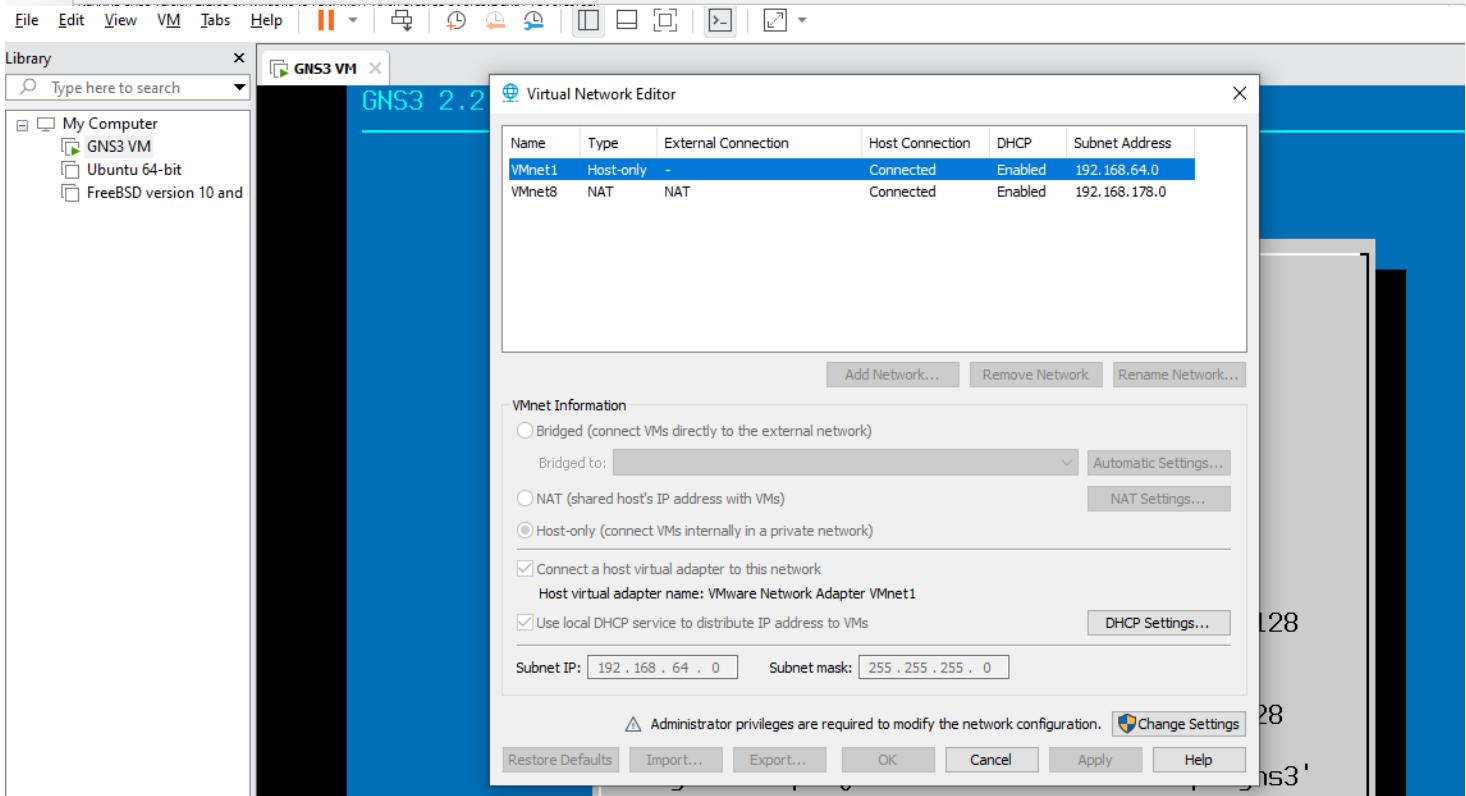
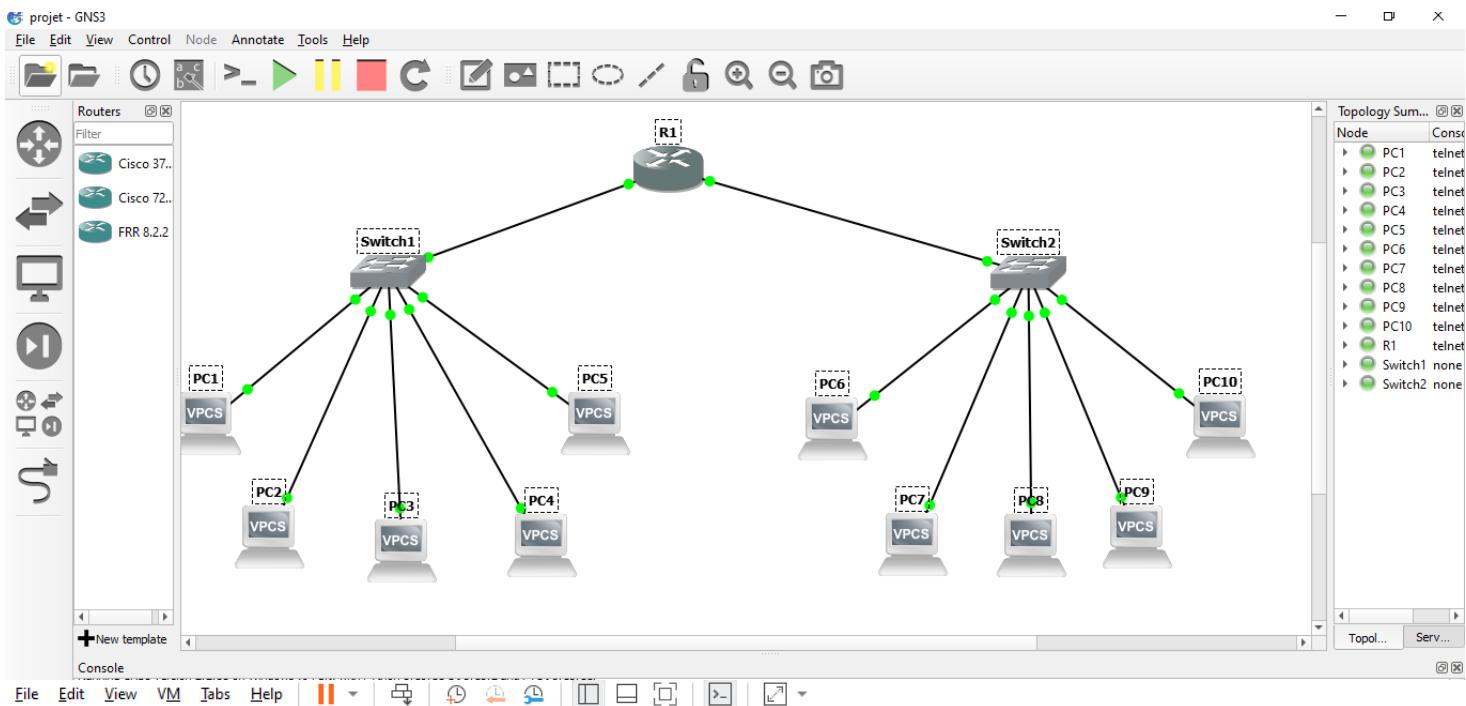
Pour GNS3

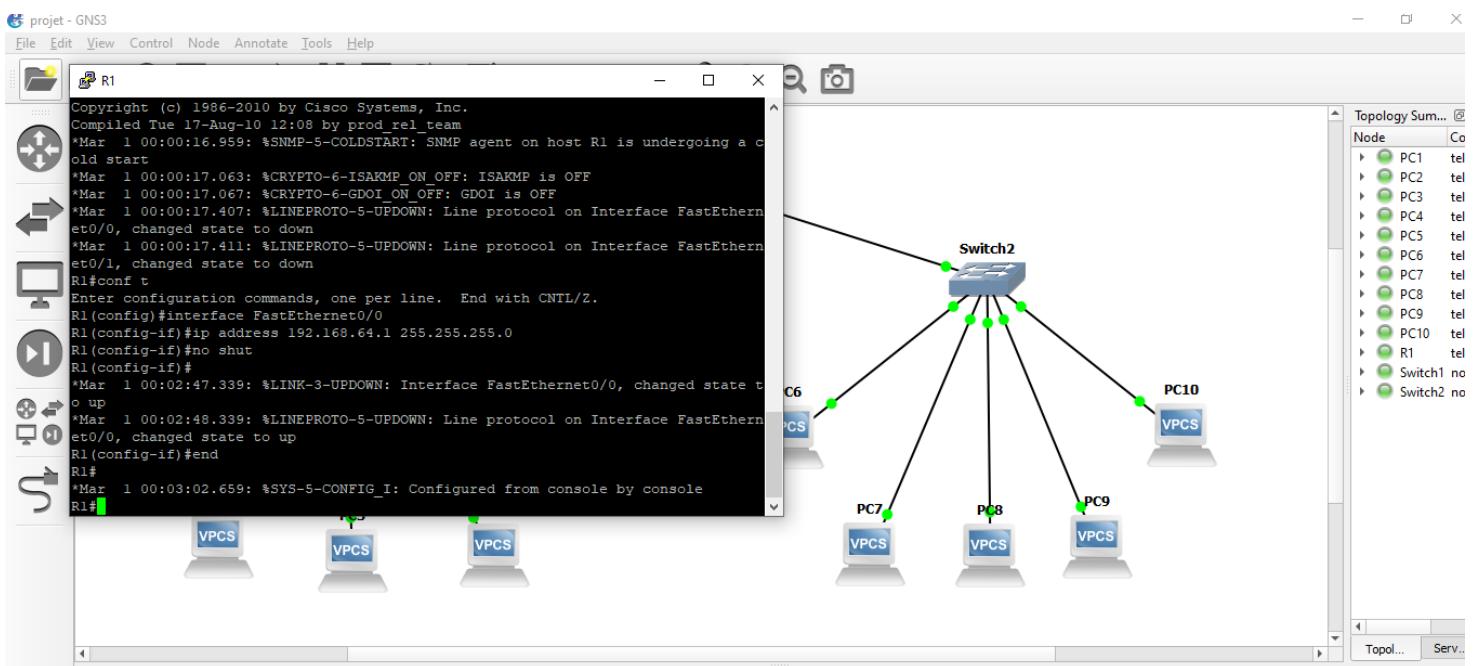
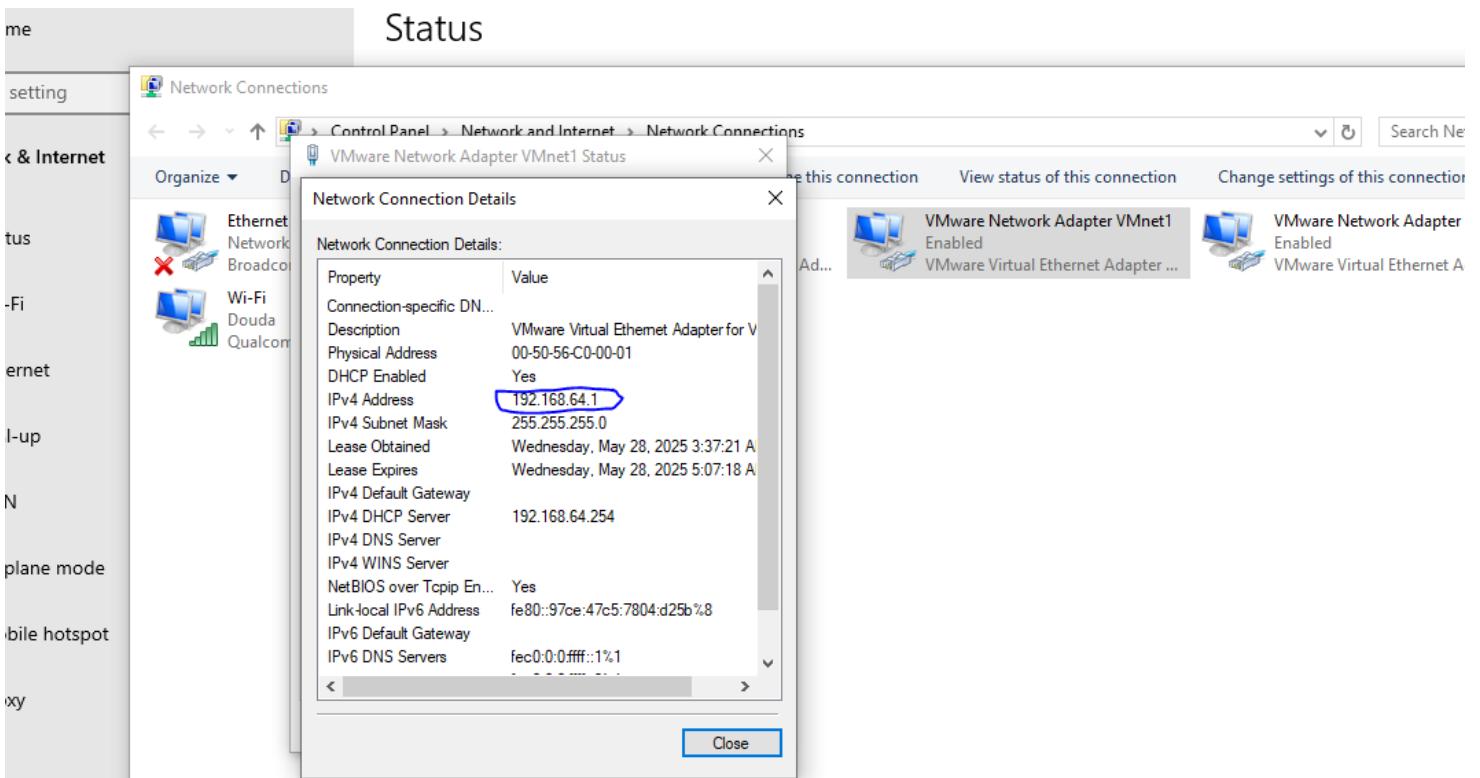
- **Diagramme de topologie réseau.**

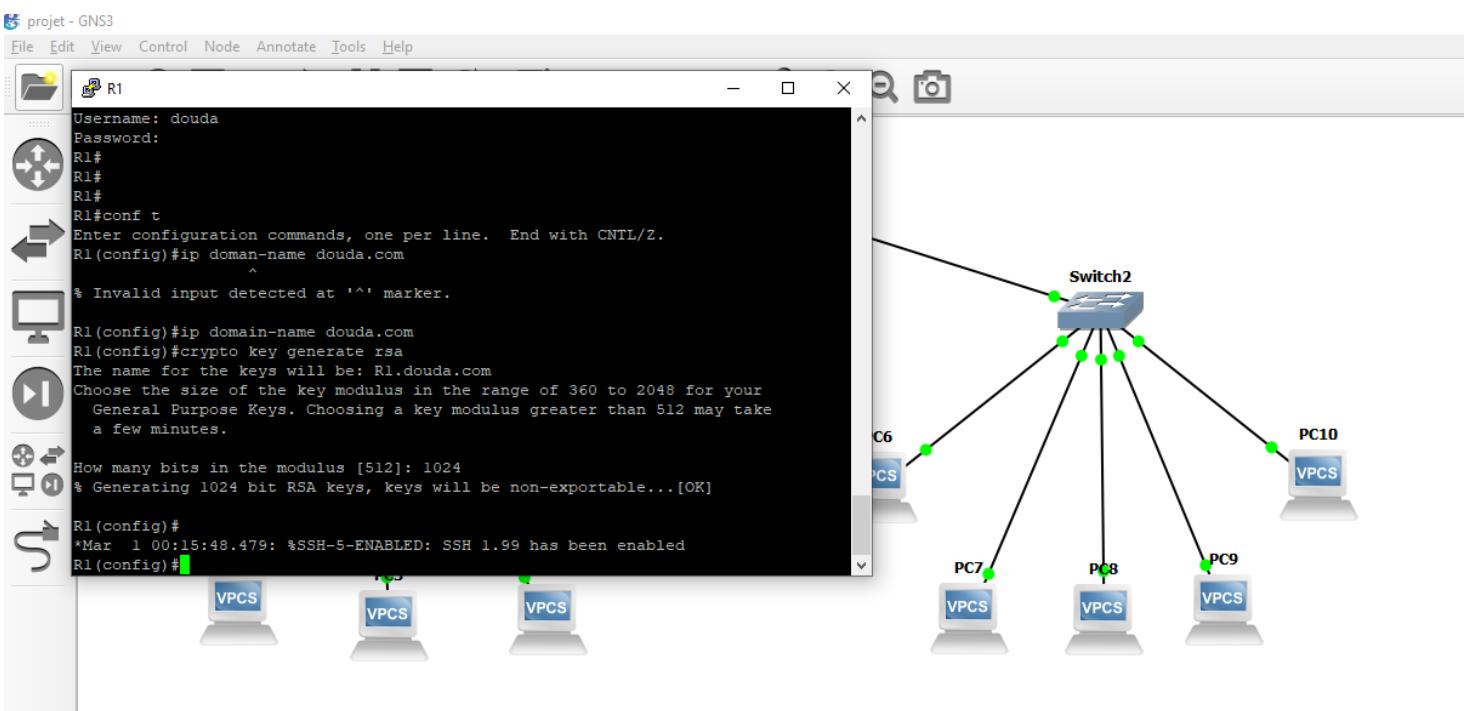
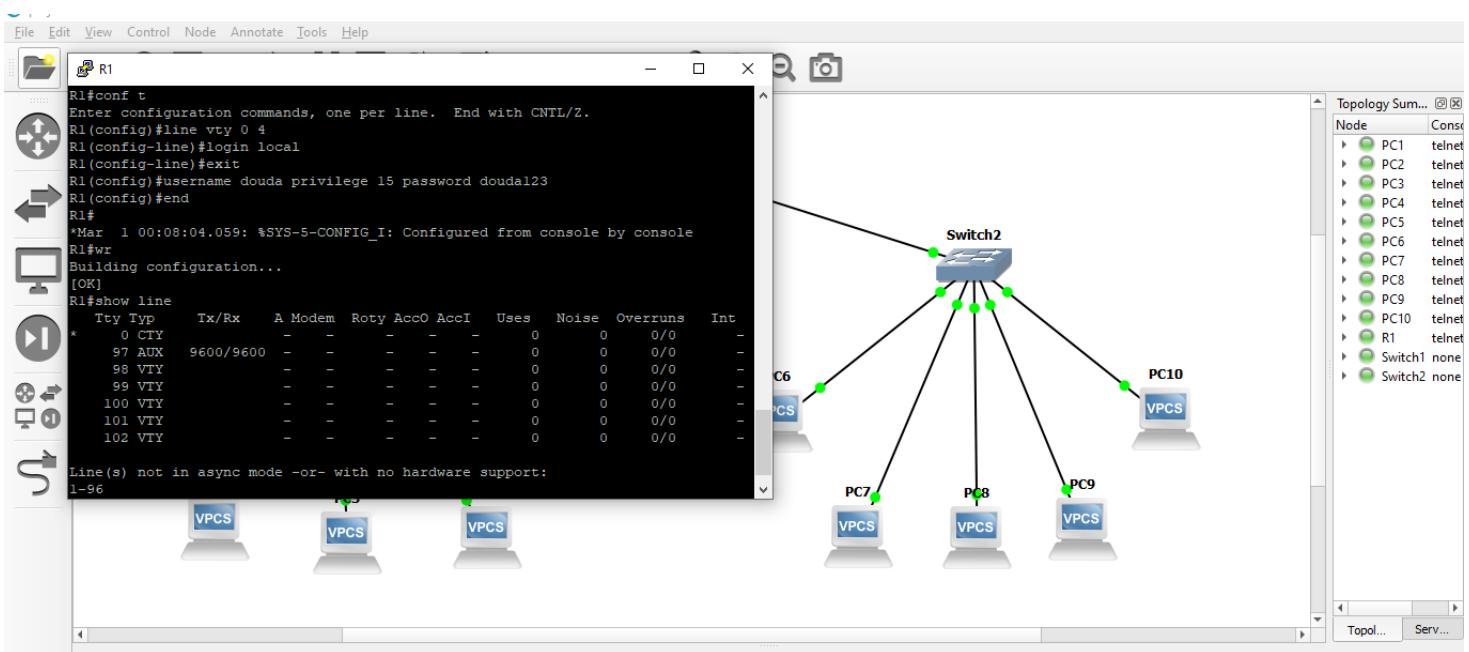
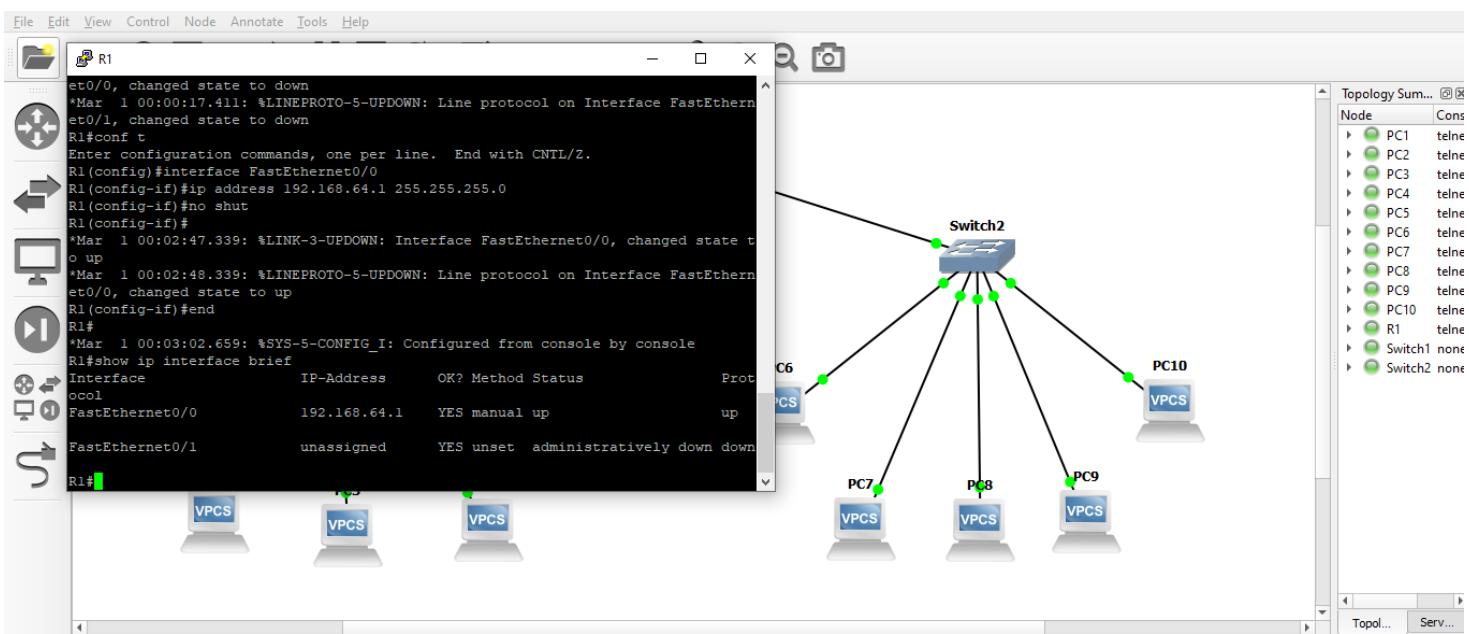


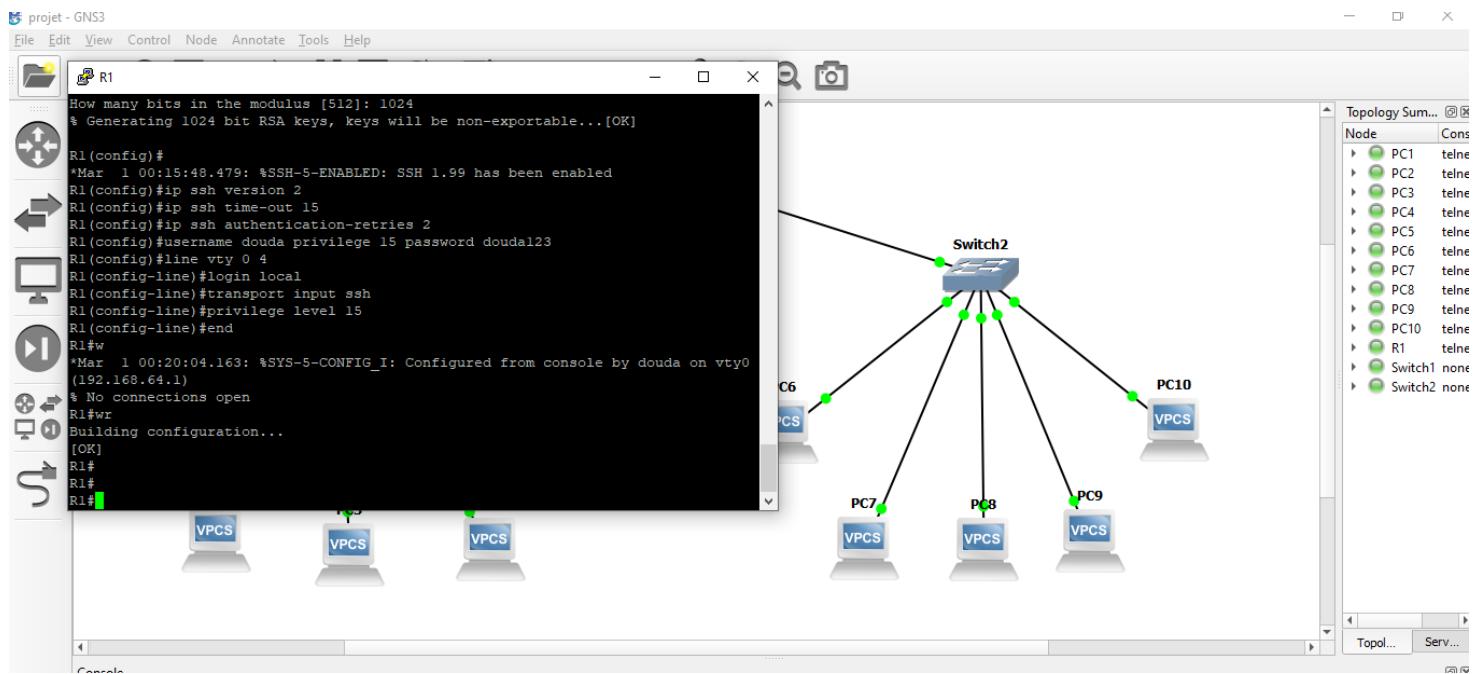
- Configuration réseau.



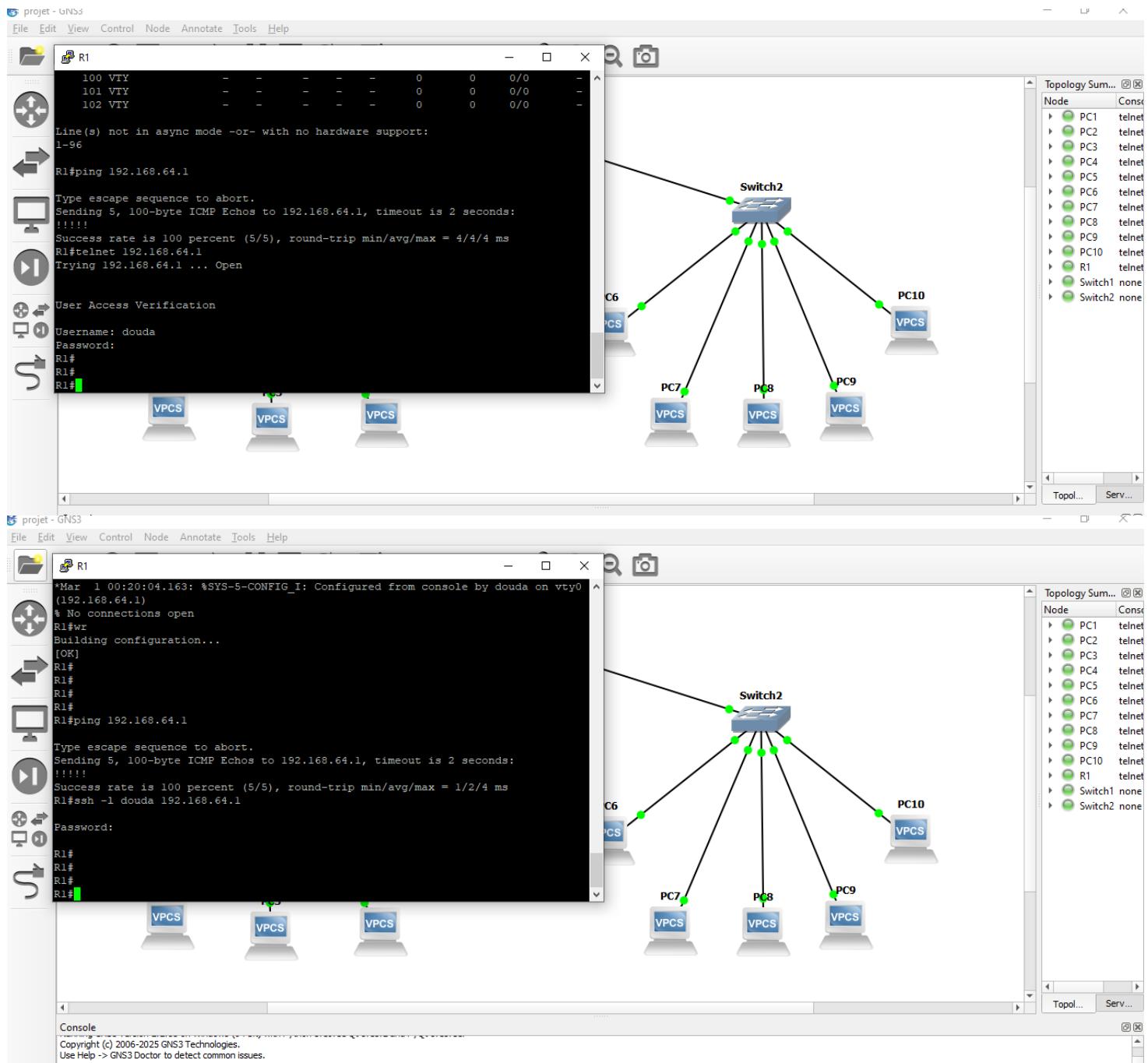








- **Tests et Observations sur GNS3**



- **Analyse des Protocoles**

Telnet est un protocole de communication qui permet aux utilisateurs de se connecter à des équipements réseau via une interface en ligne de commande. Il fonctionne sur le port 23 et est largement utilisé pour la gestion à distance des routeurs, commutateurs et serveurs.

Avantages :

- Simplicité d'utilisation : Telnet est facile à configurer et à utiliser, ce qui le rend accessible même aux utilisateurs moins expérimentés.
- Large compatibilité : Étant un protocole ancien, il est pris en charge par presque tous les équipements réseau et systèmes d'exploitation.
- Rapidité : Les connexions Telnet sont généralement rapides, car elles n'impliquent pas de processus de chiffrement.

Inconvénients :

- Sécurité faible : Telnet transmet les données en clair, ce qui signifie que les informations sensibles (comme les mots de passe) peuvent être interceptées par des attaquants.
- Absence de chiffrement : L'absence de mécanismes de sécurité rend Telnet vulnérable aux attaques de type "man-in-the-middle".
- Non adapté aux environnements sensibles : En raison de ses failles de sécurité, Telnet n'est pas recommandé pour les réseaux où la sécurité est une priorité.

Cas d'utilisation :

- Utilisé principalement dans des environnements de test ou de développement où la sécurité n'est pas une préoccupation majeure.
- Peut être utilisé pour des équipements anciens ou dans des situations où des alternatives sécurisées ne sont pas disponibles.

SSH est un protocole de communication sécurisé qui permet l'accès à distance aux équipements réseau. Il fonctionne sur le port 22 et utilise des mécanismes de chiffrement pour protéger les données échangées.

Avantages :

- Sécurité élevée : SSH chiffre toutes les données échangées, ce qui protège les informations sensibles contre l'interception.
- Authentification forte : SSH prend en charge l'authentification par clé publique, offrant une

sécurité supplémentaire par rapport aux mots de passe.

- Fonctionnalités avancées : SSH offre des fonctionnalités telles que le transfert de fichiers sécurisé (SCP, SFTP) et le tunneling, permettant des connexions sécurisées à d'autres services.

Inconvénients :

- Complexité : La configuration de SSH peut être plus complexe que celle de Telnet, surtout pour les utilisateurs novices.
- Légère latence : En raison du chiffrement, les connexions SSH peuvent être légèrement plus lentes que celles de Telnet, bien que cela soit souvent négligeable.
- Compatibilité : Bien que largement supporté, certains équipements très anciens peuvent ne pas prendre en charge SSH.

Cas d'utilisation :

- Utilisé dans des environnements de production où la sécurité est primordiale, comme les serveurs web, les bases de données et les équipements réseau critiques.
- Recommandé pour toute gestion à distance d'équipements où des informations sensibles sont échangées.

Comparaison des protocoles Telnet et SSH, avec une analyse de la sécurité.

Caractéristique	Telnet	SSH
Chiffrement	Extrêmement faible	Très élevée
Authentification	Non	Oui
Vitesse	Simple (risqué)	Multiple (sécurisé)
Configuration	Rapide	Légèrement plus lent
	Simple	Plus complexe
Cas d'utilisation	Environnements non sensibles	Environnements sensibles et critiques

SSH est le standard pour l'administration à distance sécurisée. C'est plus complexe, mais la sécurité est primordiale, surtout dans le monde actuel. On ne prend pas de risques inutiles avec des données sensibles.

- **Conclusion**

En conclusion, bien que Telnet et SSH soient tous deux des protocoles d'accès à distance, SSH est clairement le choix privilégié pour la plupart des applications modernes en raison de ses fonctionnalités de sécurité avancées. Telnet peut encore avoir sa place dans des scénarios spécifiques, mais son utilisation devrait être limitée aux environnements où la sécurité n'est pas une préoccupation. En tant qu'étudiant, il est essentiel de comprendre ces différences pour faire des choix éclairés lors de la gestion des réseaux.