FACULTE DES SCIENCES ET TECHNOLOGIES

Sciences Informatiques

TD N^{o} 7 : Réseau I

Blomy ANTOINE

Licence 3

Sous la direction du professeur :

Ismaël SAINT-AMOUR

05 janvier 2025

I- Description des résultats de la tâche et objectifs du TD

Dans le cadre du cours Réseaux I, ce travail dirigé (TD 7) porte sur la configuration et l'utilisation des services d'accès distant Telnet et SSH sur des équipements Cisco, à l'aide du logiciel Cisco Packet Tracer.

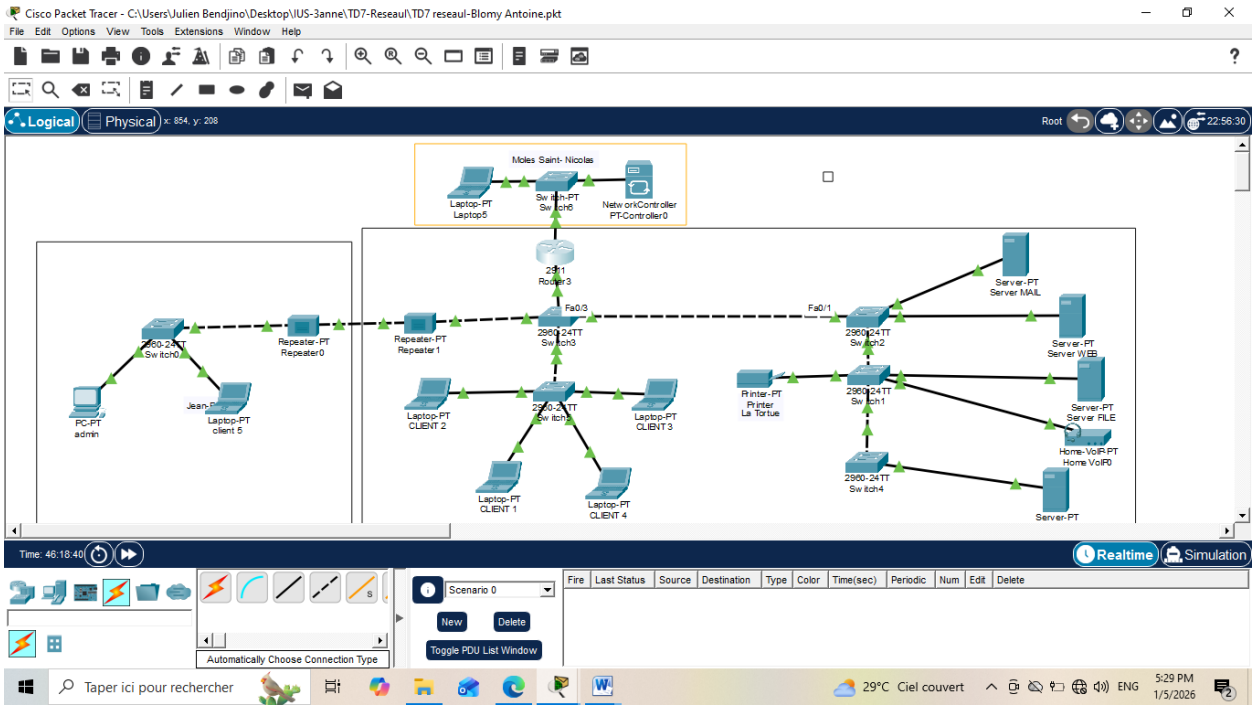
L'objectif principal de ce TD est de permettre à l'étudiant de comprendre les mécanismes d'administration à distance des équipements réseau, tout en mettant en évidence les différences fondamentales entre une connexion non sécurisée (Telnet) et une connexion sécurisée (SSH).

Au cours de ce travail, il est question de configurer plusieurs niveaux d'utilisateurs avec des privilèges distincts, de restreindre l'accès aux équipements par des listes de contrôle d'accès (ACL), d'activer la journalisation des connexions, ainsi que de mettre en place des mécanismes de protection contre les attaques par force brute.

Ce TD vise également à sensibiliser l'étudiant à l'importance de la sécurité des réseaux et aux bonnes pratiques à adopter dans un environnement de production.

Résultats des exécutions des commandes

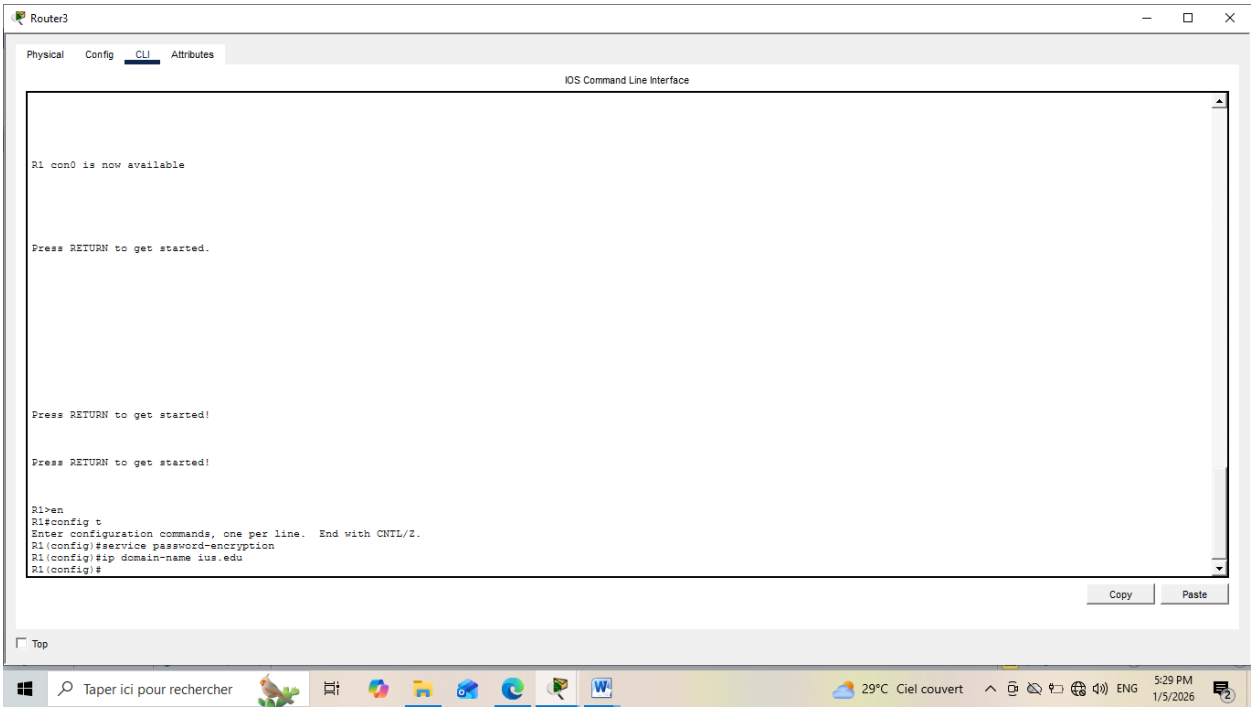
1- Reproduction de la topologie 1 en configurant les services DHCP afin d'attribuer automatiquement les adresses IP aux dispositifs du réseau.



PARTIE A – TELNET (NON SÉCURISÉ)

1) Configuration globale

```
R1(config)# hostname R1
R1(config)# service password-encryption
R1(config)# ip domain-name ius.edu
```



2) Création des utilisateurs (1,5 15 privileges)

Administrateur 15 privileges;

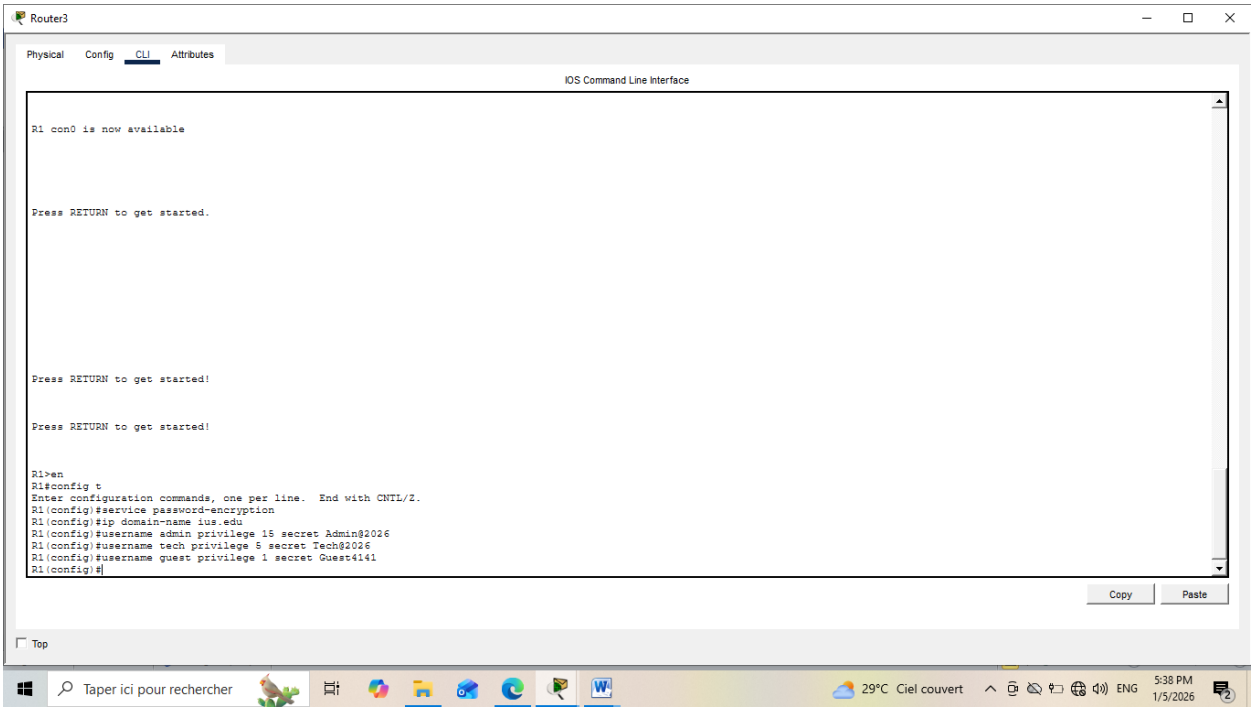
```
R1(config)# username admin privilege 15 secret Admin@2026
```

Technician 5 privileges;

```
R1(config)# username tech privilege 5 secret Tech@2026
```

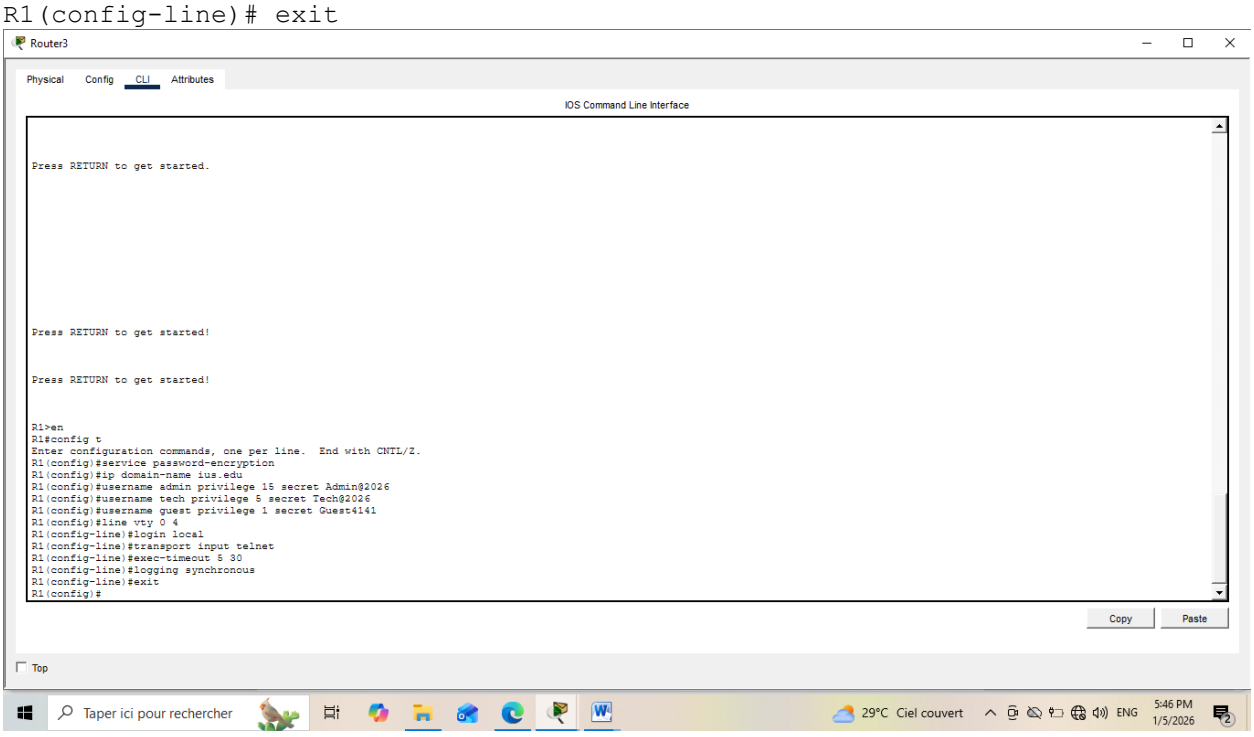
Utilisateur 1 privilege

```
R1(config)# username guest privilege 1 secret Guest4141
```



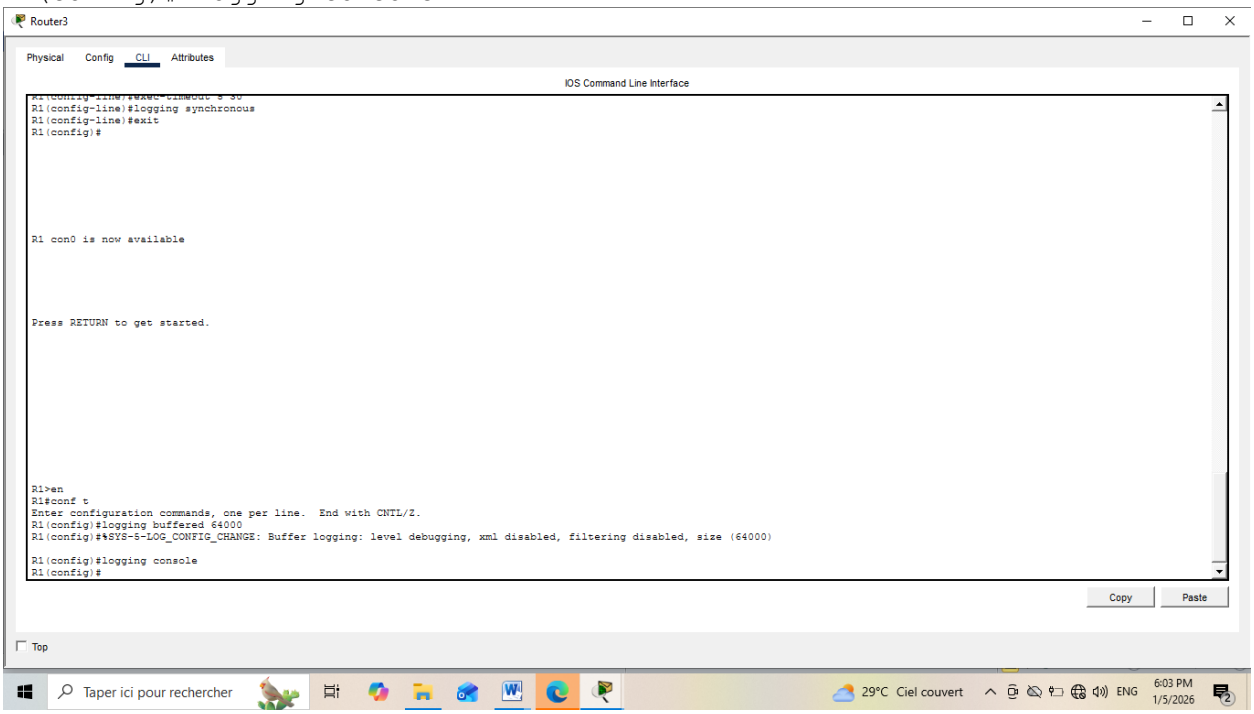
3- Activation Telnet sur les lignes VTY.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# password telnet123
R1(config-line)# exec-timeout 5 30
R1(config-line)# logging synchronous
R1(config-line)# exit
```



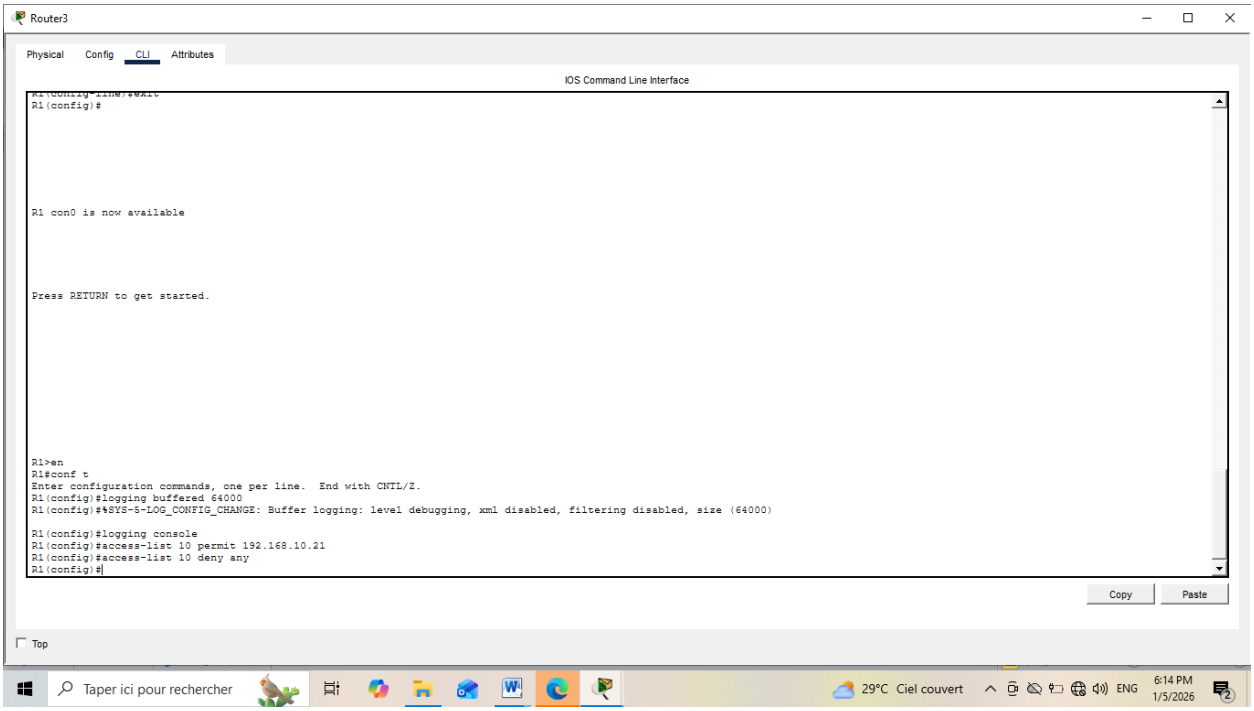
4- journalisation

```
R1(config)# logging buffered 64000
R1(config)# logging console
```



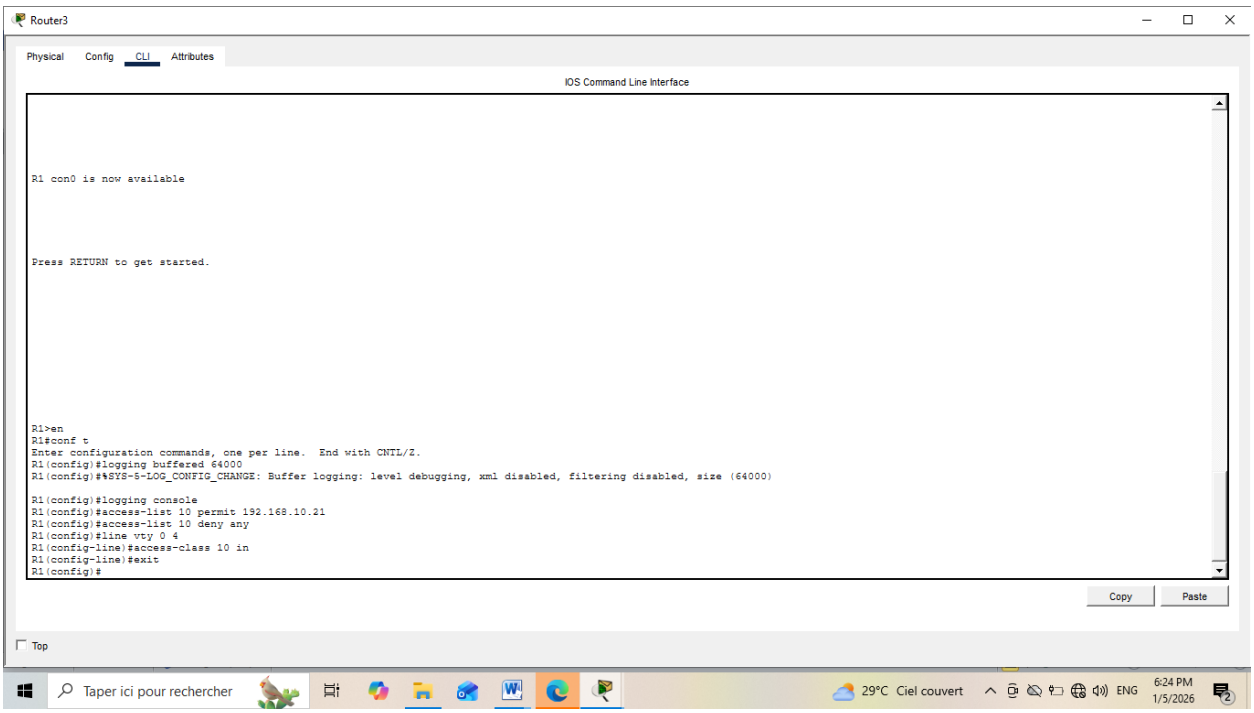
5- Autorisation uniquement PC1, PC2 doit échouer

```
R1(config)# access-list 10 permit 192.168.10.21  (admin)
R1(config)# access-list 10 deny any
```



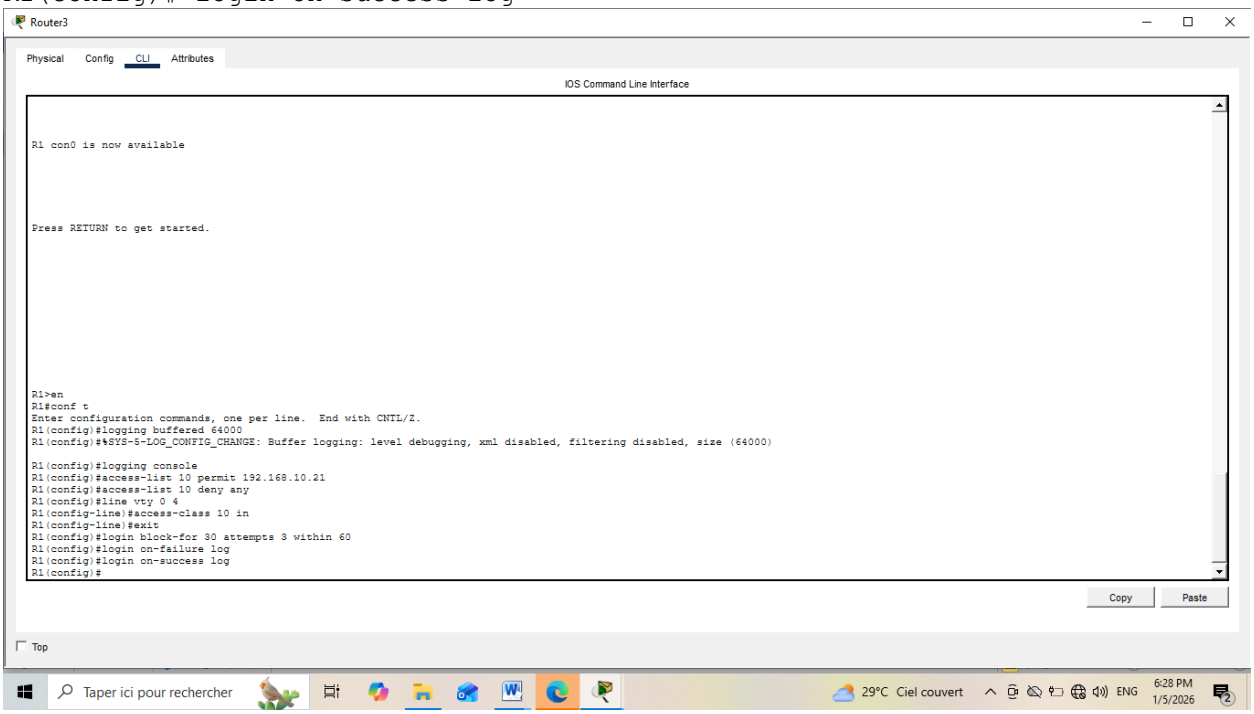
Application de l'ACL

```
R1(config)# line vty 0 4
R1(config-line)# access-class 10 in
R1(config-line)# exit
```



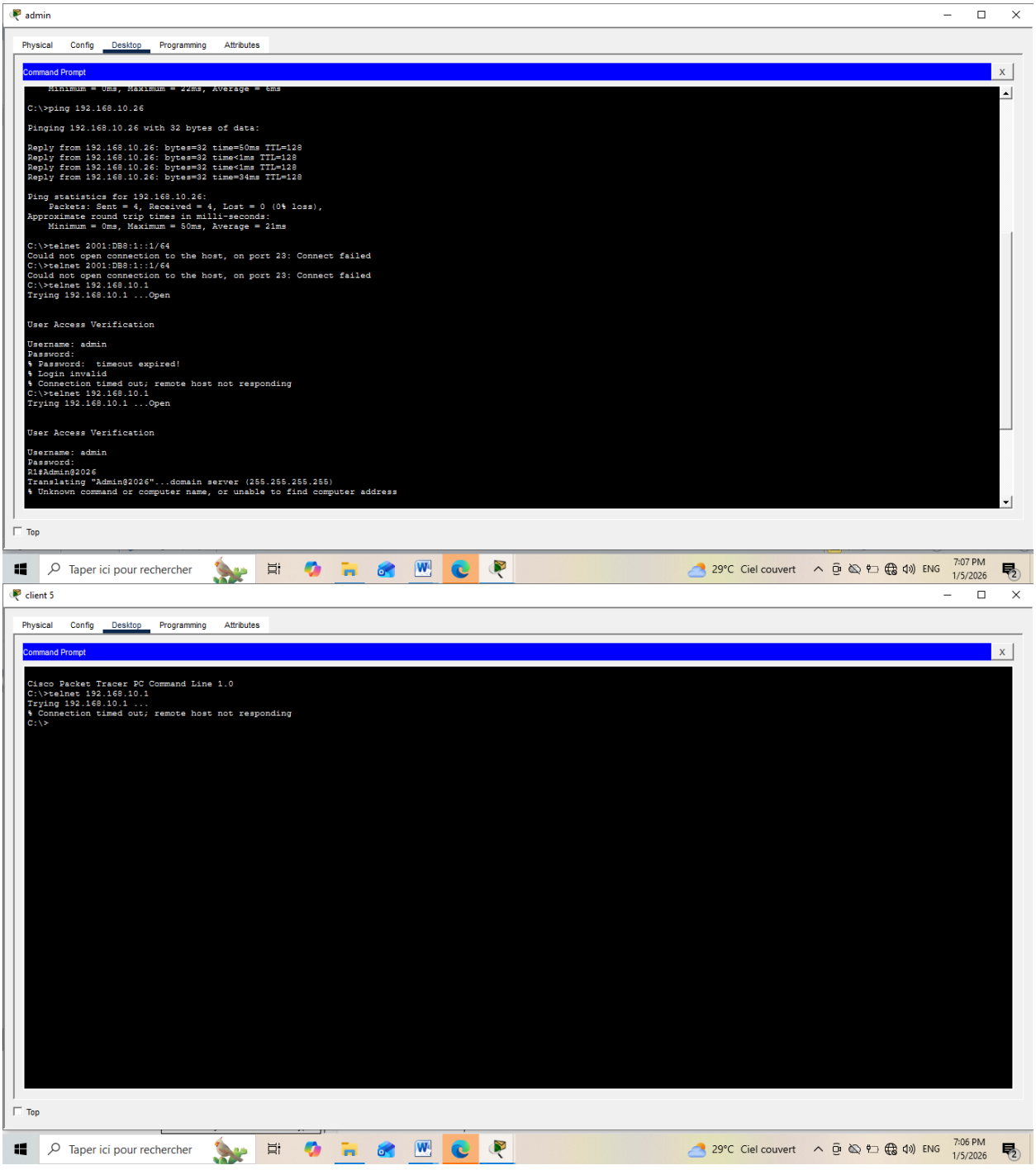
6- protection contre brute-force

```
R1(config)# login block-for 30 attempts 3 within 60
R1(config)# login on-failure log
R1(config)# login on-success log
```



Tests Telnet

```
admin> telnet 192.168.10.1(ip du routeur)
login: admin
password: Admin@2026
```


admin
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Minimum = 0ms, Maximum = 22ms, Average = 6ms
C:\>ping 192.168.10.26
Pinging 192.168.10.26 with 32 bytes of data:
Reply from 192.168.10.26: bytes=32 time=50ms TTL=128
Reply from 192.168.10.26: bytes=32 time<1ms TTL=128
Reply from 192.168.10.26: bytes=32 time<1ms TTL=128
Reply from 192.168.10.26: bytes=32 time=34ms TTL=128
Ping statistics for 192.168.10.26:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 50ms, Average = 21ms
C:\>telnet 2001:DB8:1::1/64
Could not open connection to the host, on port 23: Connect failed
C:\>telnet 2001:DB8:1::1/64
Could not open connection to the host, on port 23: Connect failed
C:\>telnet 192.168.10.1
Trying 192.168.10.1 ...Open
User Access Verification
Username: admin
Password:
% Password: timeout expired!
% Login invalid
% Connection timed out; remote host not responding
C:\>telnet 192.168.10.1
Trying 192.168.10.1 ...Open
User Access Verification
Username: admin
Password:
R1#Admin@2026
Translating "Admin@2026"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Top
Taper ici pour rechercher
29°C Ciel couvert
ENG
7:07 PM
1/5/2026
client 5
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.10.1
Trying 192.168.10.1 ...
% Connection timed out; remote host not responding
C:\>
Top
Taper ici pour rechercher
29°C Ciel couvert
ENG
7:06 PM
1/5/2026

1. Pourquoi Telnet est-il non sécurisé ?

Parce que telnet transmet **toutes les données en clair**.

2. Quelles informations transitent en clair ?

- Nom d'utilisateur
- Mot de passe
- Commandes tapées
- Résultats

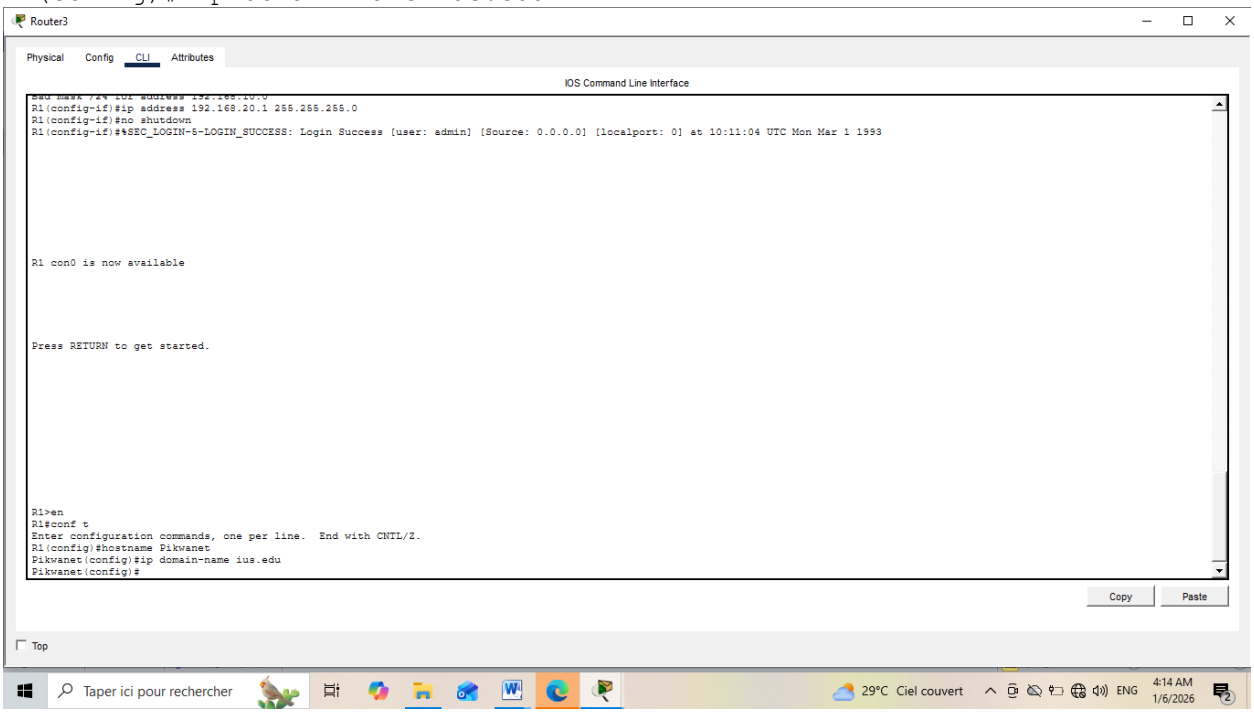
3. Pourquoi éviter Telnet en production ?

- Facilement interceptable (sniffing)
- Aucune confidentialité
- Vulnérable aux attaques MITM

PARTIE B-SSH SECURISEE

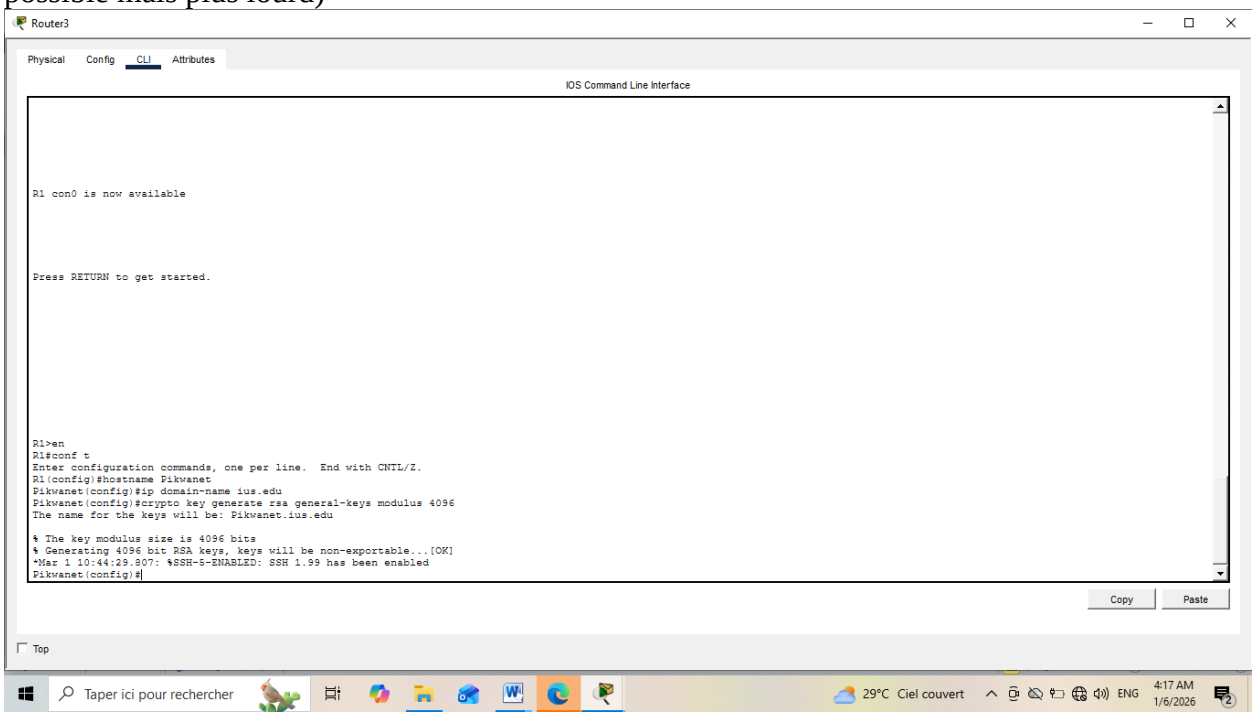
1) Definition d'un nom hote et nom de domaine

```
R1(config)# hostname Pikwanet
R1(config)# ip domain-name ius.edu
```



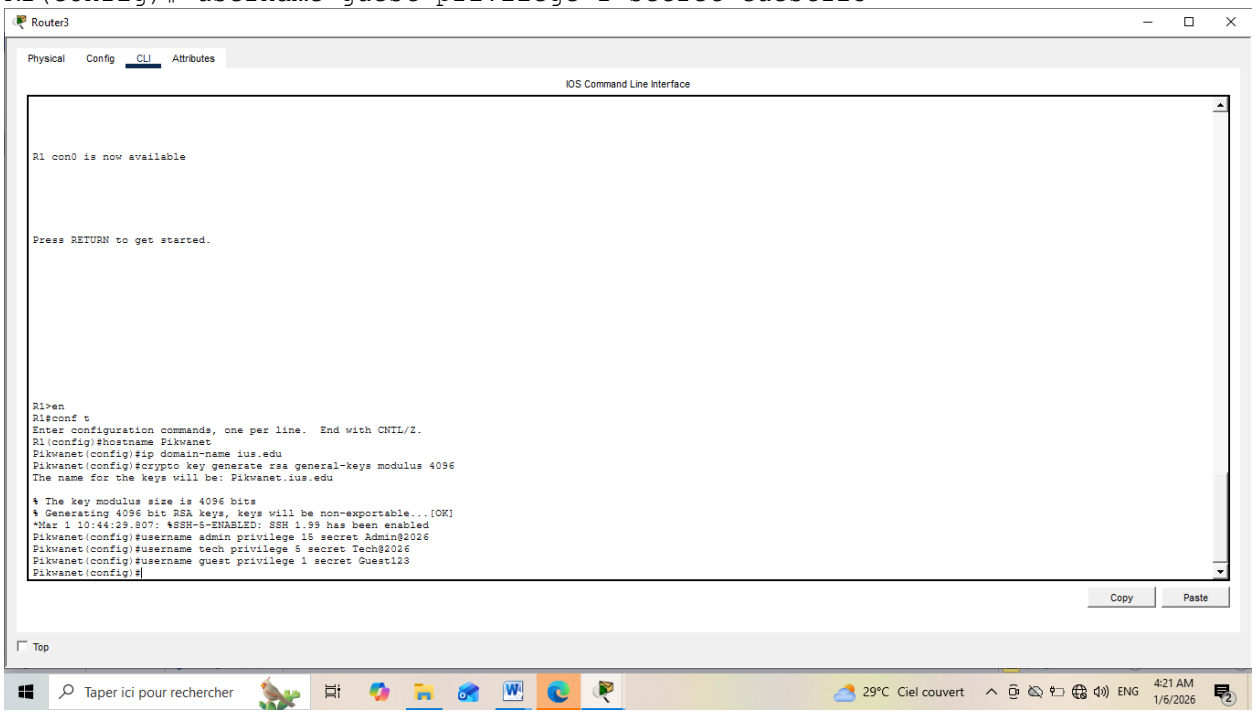
2- Génération d'une clé RSA (2048 bits minimum).

`R1(config)# crypto key generate rsa general-keys modulus 4096` (4096 possible mais plus lourd)



3- Comptes utilisateurs

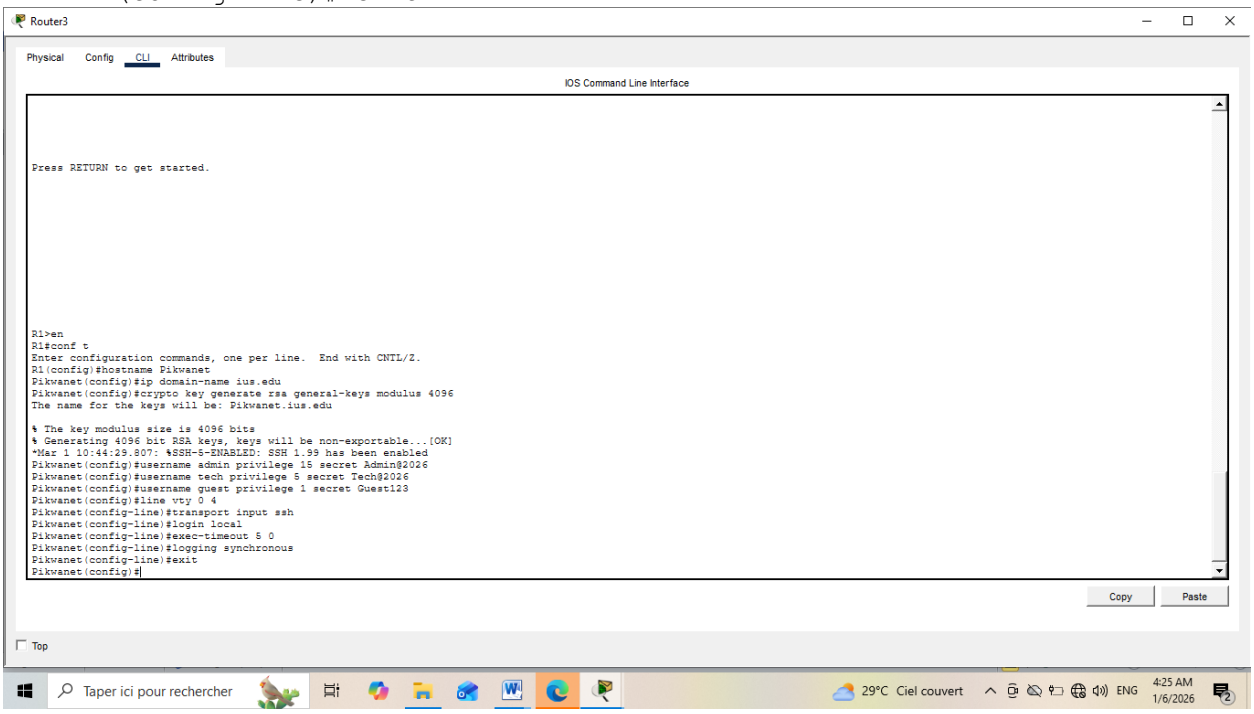
```
R1(config)# username admin privilege 15 secret Admin@2026
R1(config)# username tech privilege 5 secret Tech@2026
R1(config)# username guest privilege 1 secret Guest123
```



4- Activation SSH uniquement

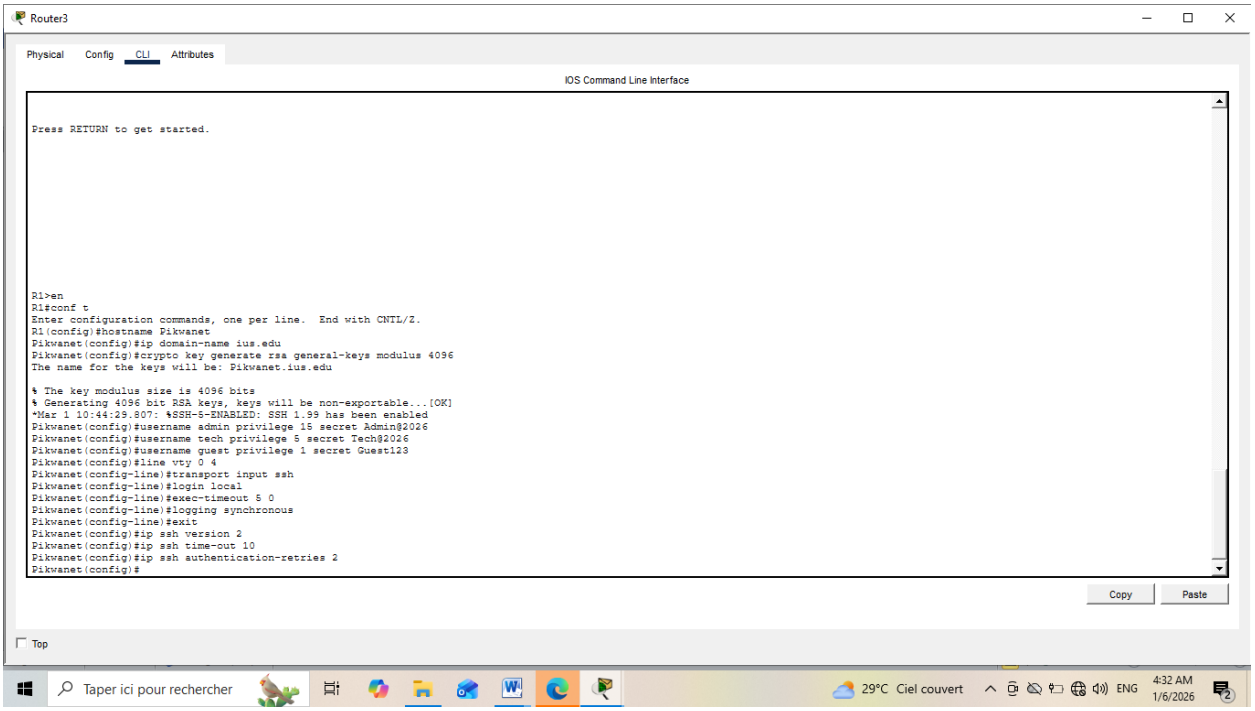
```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config-line)# exit
```



5- Activation de SSH et durcissement

```
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 10
R1(config)# ip ssh authentication-retries 2
```

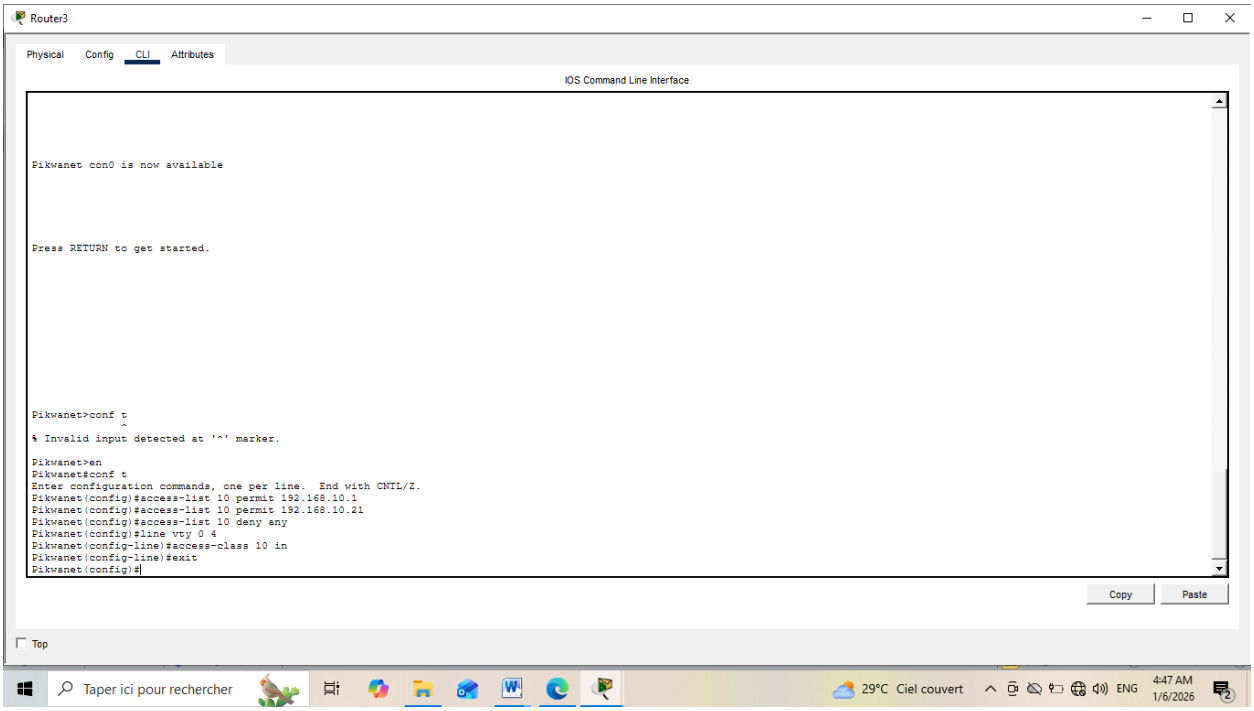


5. Désactivation Telnet

ACL SSH (PC1 uniquement)

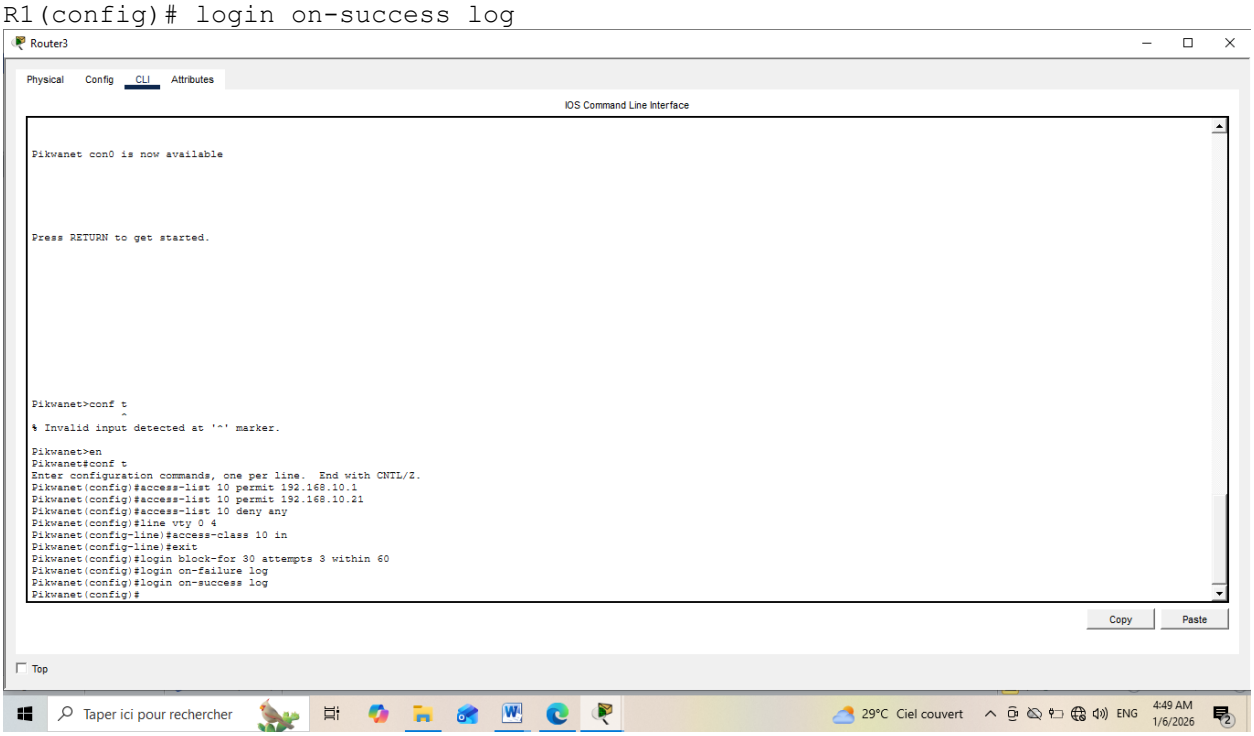
```
R1(config)# access-list 10 permit 192.168.10.21
R1(config)# access-list 10 deny any

R1(config)# line vty 0 4
R1(config-line)# access-class 10 in
R1(config-line)# exit
```



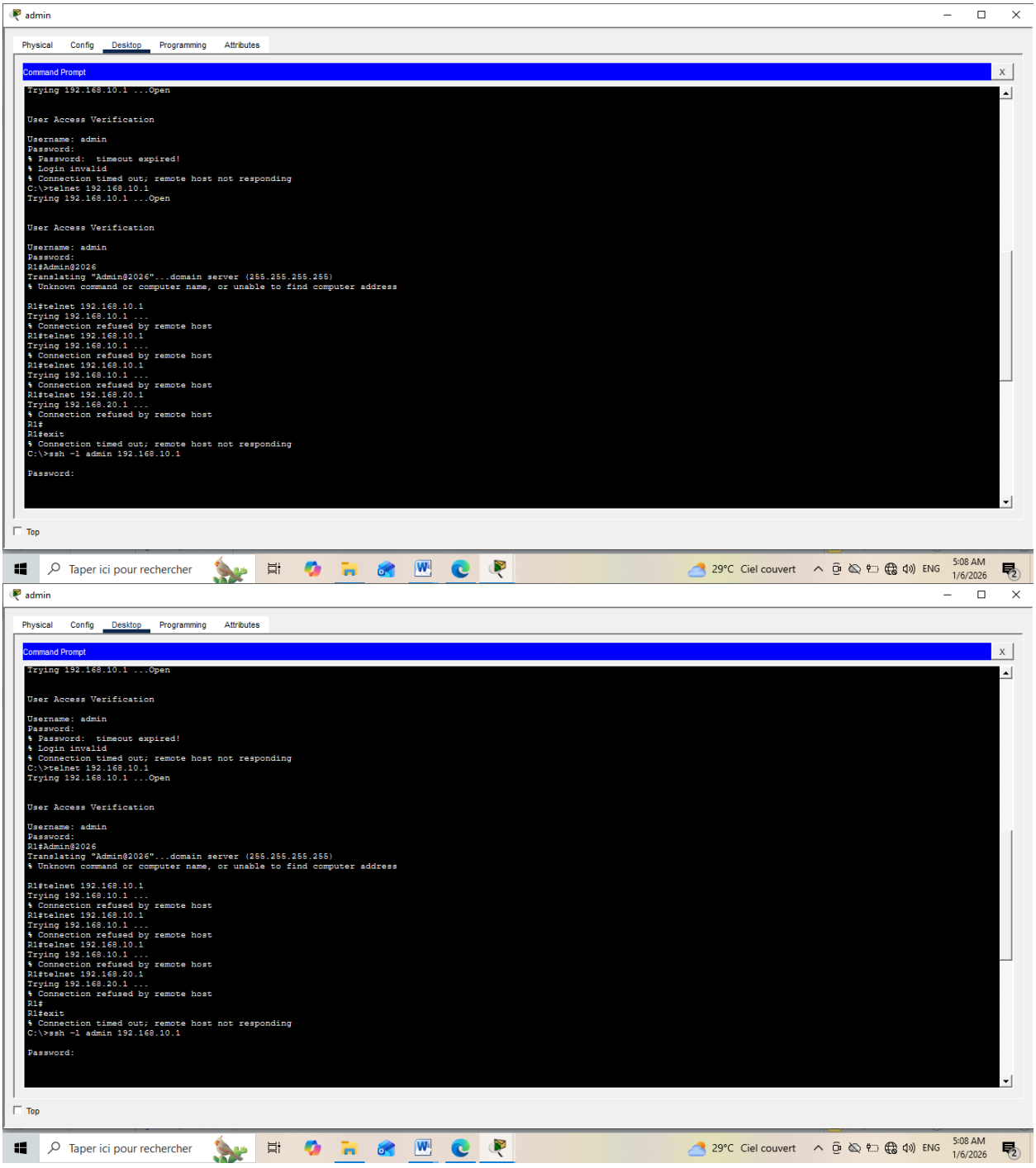
Protection brute-force

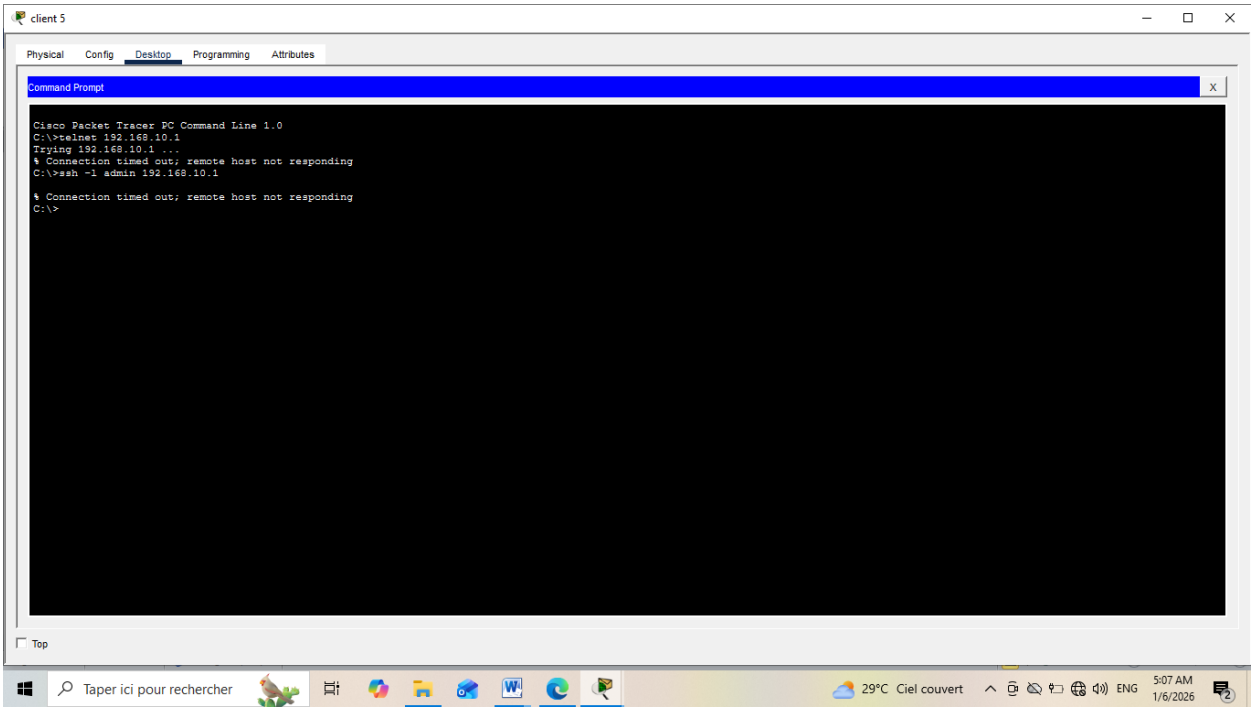
```
R1(config)# login block-for 30 attempts 3 within 60
R1(config)# login on-failure log
R1(config)# login on-success log
```



Teste de l'acces SSH

```
Admin> ssh -l admin 192.168.10.1
Admin> ssh -l tech 192.168.10.1
```





Réponse aux questions

1. Différence SSH v1 / SSH v2

Pour comprendre la différence entre les deux versions, je propose une illustration dans le tableau ci-contre.

SSH v1	SSH v2
Obsolète	Sécurisé
Failles connues	Chiffrement fort
Non recommandé	Obligatoire

2. Pourquoi RSA 1024 bits est déconseillé ?

Parce qu'il est facilement cassable aujourd'hui. Il est insuffisant face aux capacités de calcul modernes.

3. Que se passe-t-il sans domaine local ?

Dans le domaine local, il est impossible de générer les clés RSA, donc SSH ne fonctionne pas.

En conclusion on peut dire que :

1. Telnet est simple mais **dangereux**
2. SSH assure :
    a. chiffrement,
    b. authentification sécurisée,
    c. contrôle d'accès,
    d. traçabilité

Conclusion

L'issue de ce travail dirigé, il ressort que la configuration des services Telnet et SSH permet une meilleure compréhension de l'administration distante des équipements réseau Cisco. La mise en œuvre de Telnet a permis de constater ses nombreuses failles de sécurité, notamment la transmission des identifiants et des données en clair, ce qui le rend fortement déconseillé dans les environnements réels.

Ce travail a également permis de se familiariser avec la supervision des sessions actives et la journalisation des connexions réussies ou échouées.

En conclusion, les objectifs du TD ont été atteints avec succès. Malgré quelques difficultés techniques rencontrées lors de la configuration initiale (génération des clés RSA, ACL ou restrictions d'accès), celles-ci ont été résolues grâce à une analyse méthodique des commandes et des messages du système. Ce TD a renforcé nos compétences pratiques en **sécurité réseau** et en **administration des équipements Cisco**, compétences indispensables pour tout futur administrateur réseau.