Faculté : Sciences Informatique

Nom & Prénom : Louis Dochlie

TD N°7– Reseaux

Niveau : L3

Date : Le/15/12/25

Travaux Dirigés

A. Configuration Telnet (partie non sécurisée)

1. Configurer le nom, la protection globale et le domaine local.

2. Créer des utilisateurs (privilège 1,5,15).

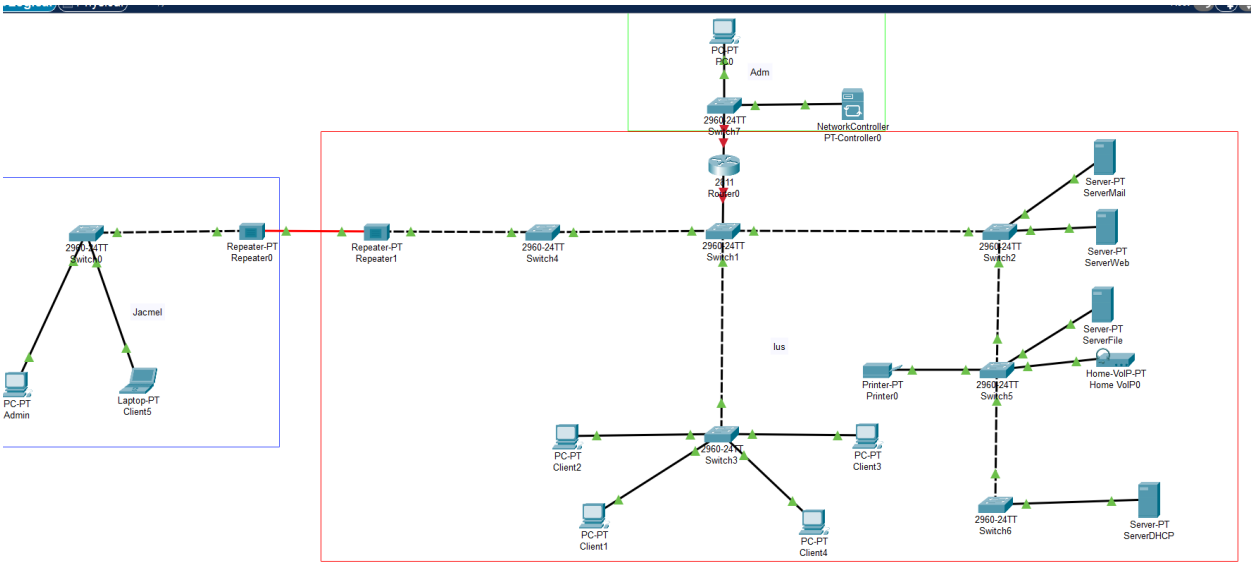
3. Activer Telnet sur les lignes VTY.

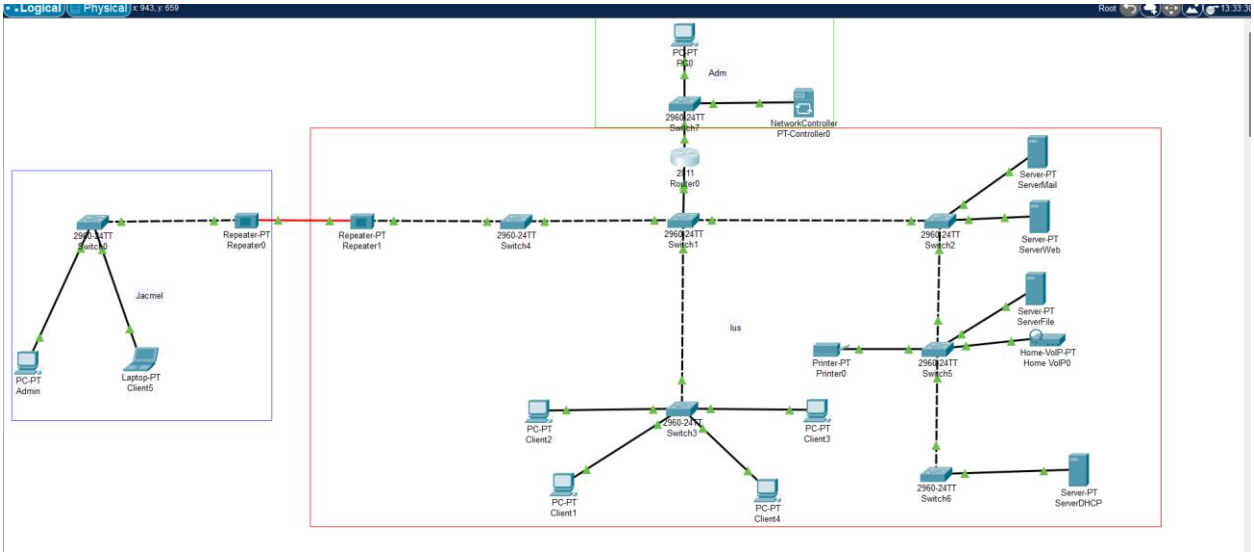
4. Configurer un mot de passe de ligne.

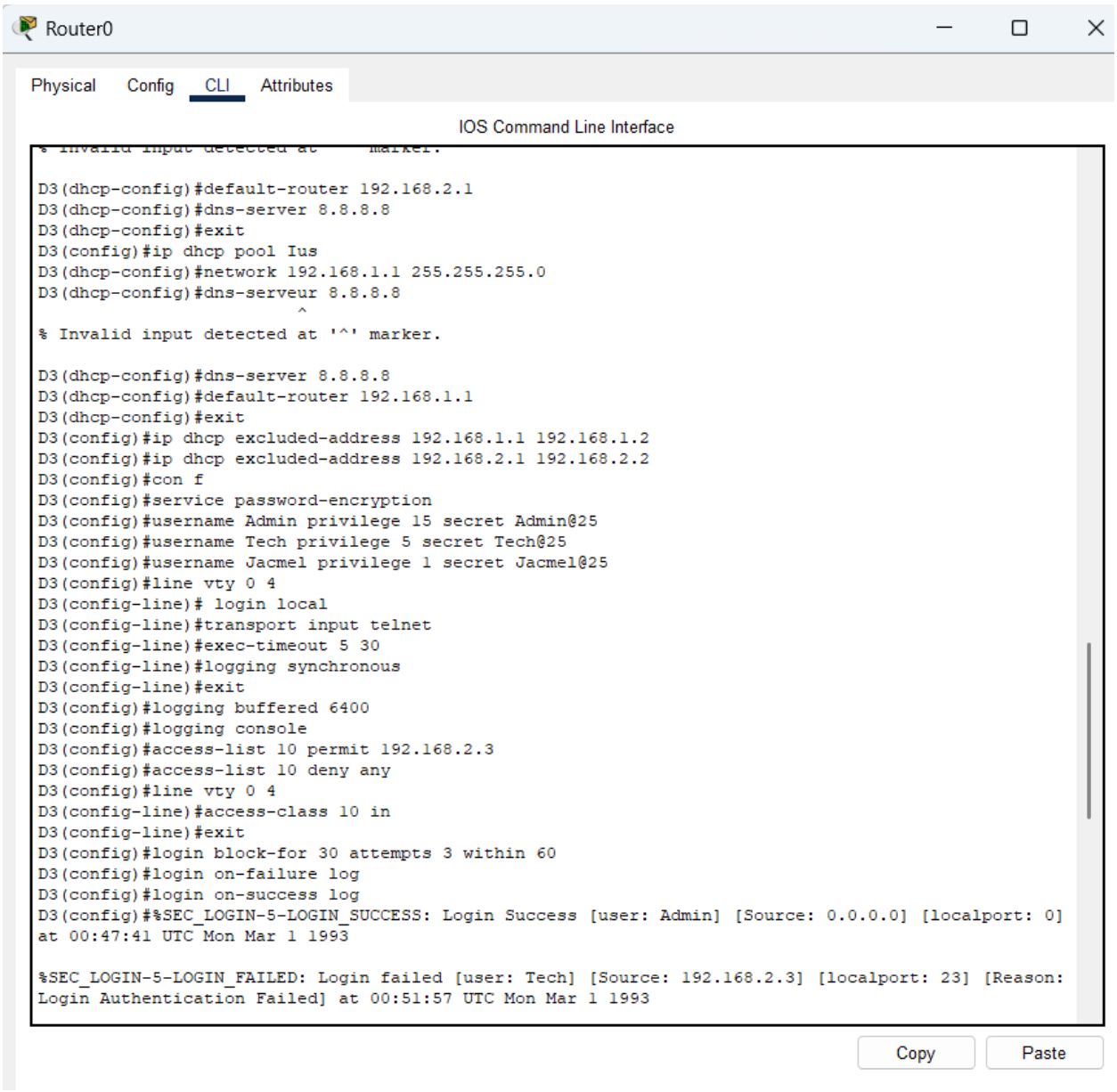
5. Tester l'accès Telnet :

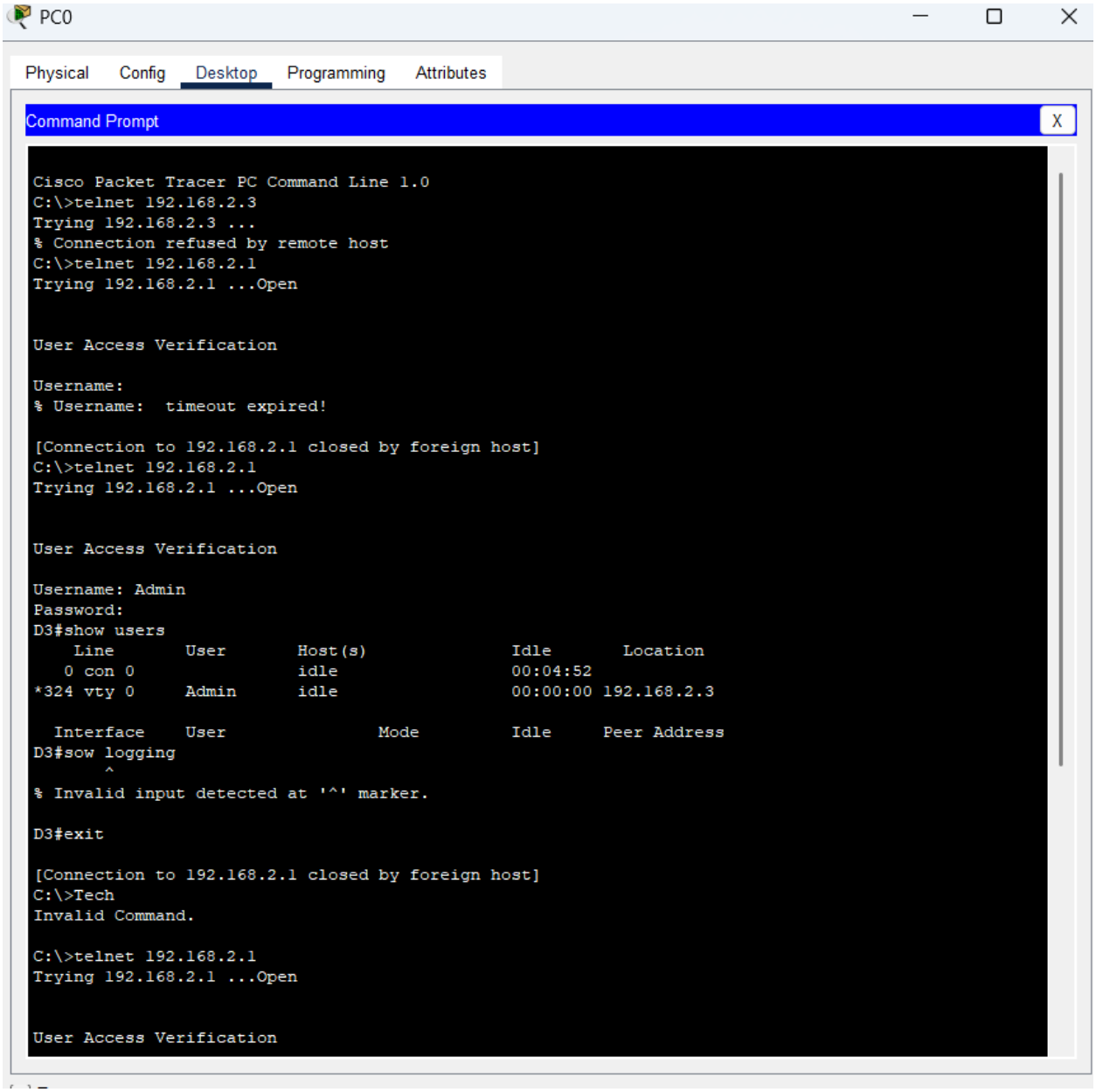
Depuis PC1 → doit fonctionner

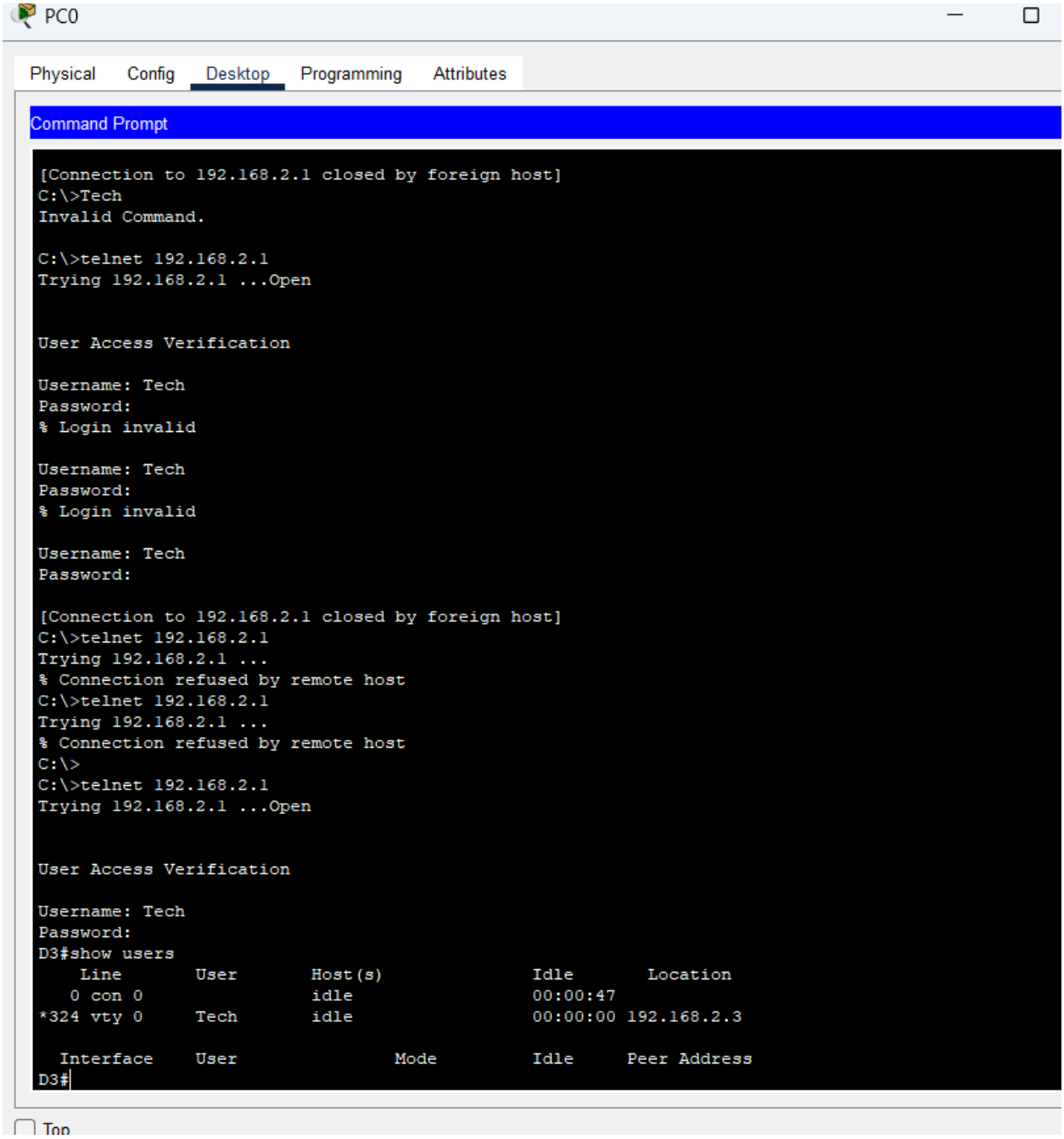
Depuis PC2 → doit échouer

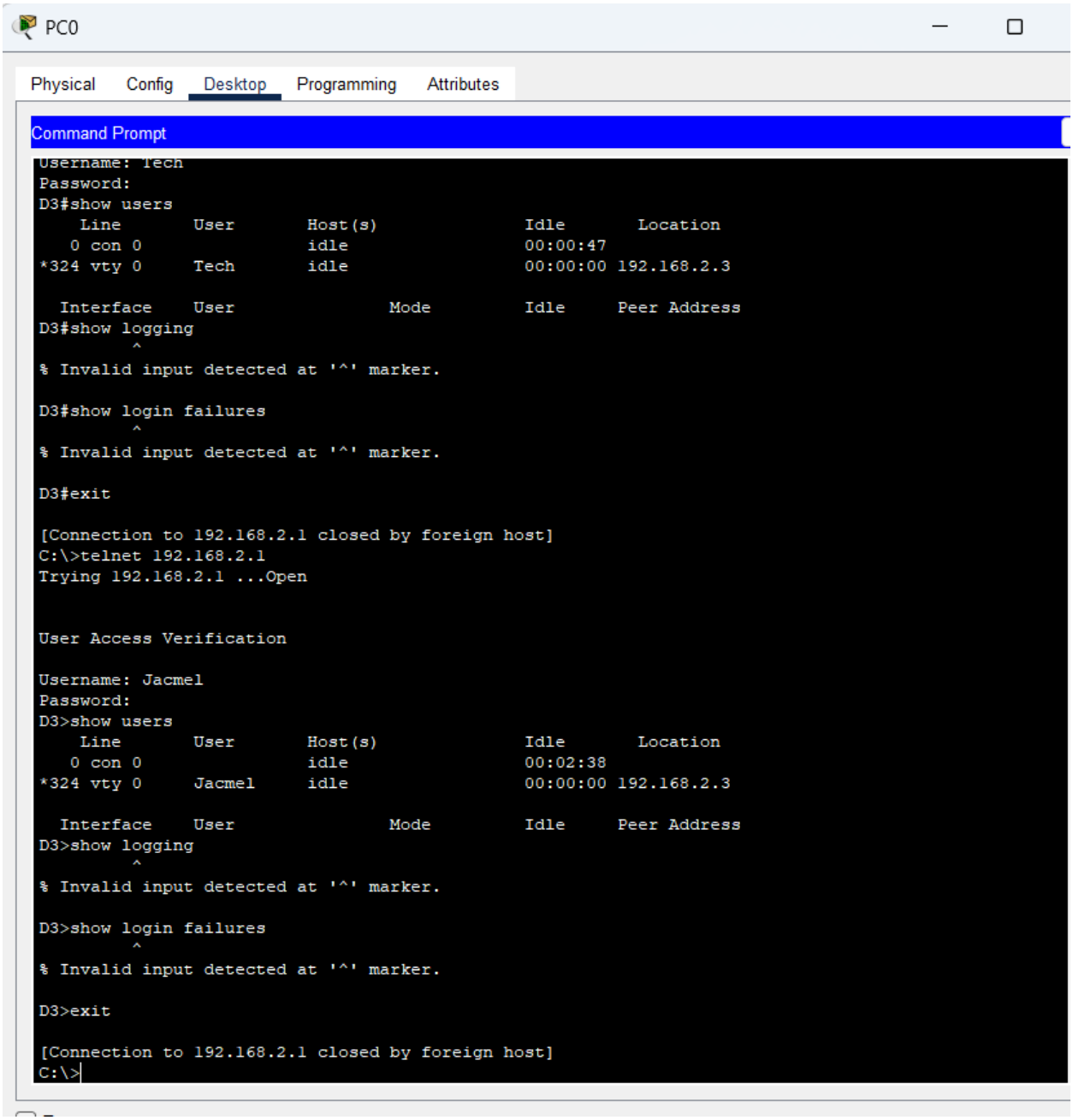


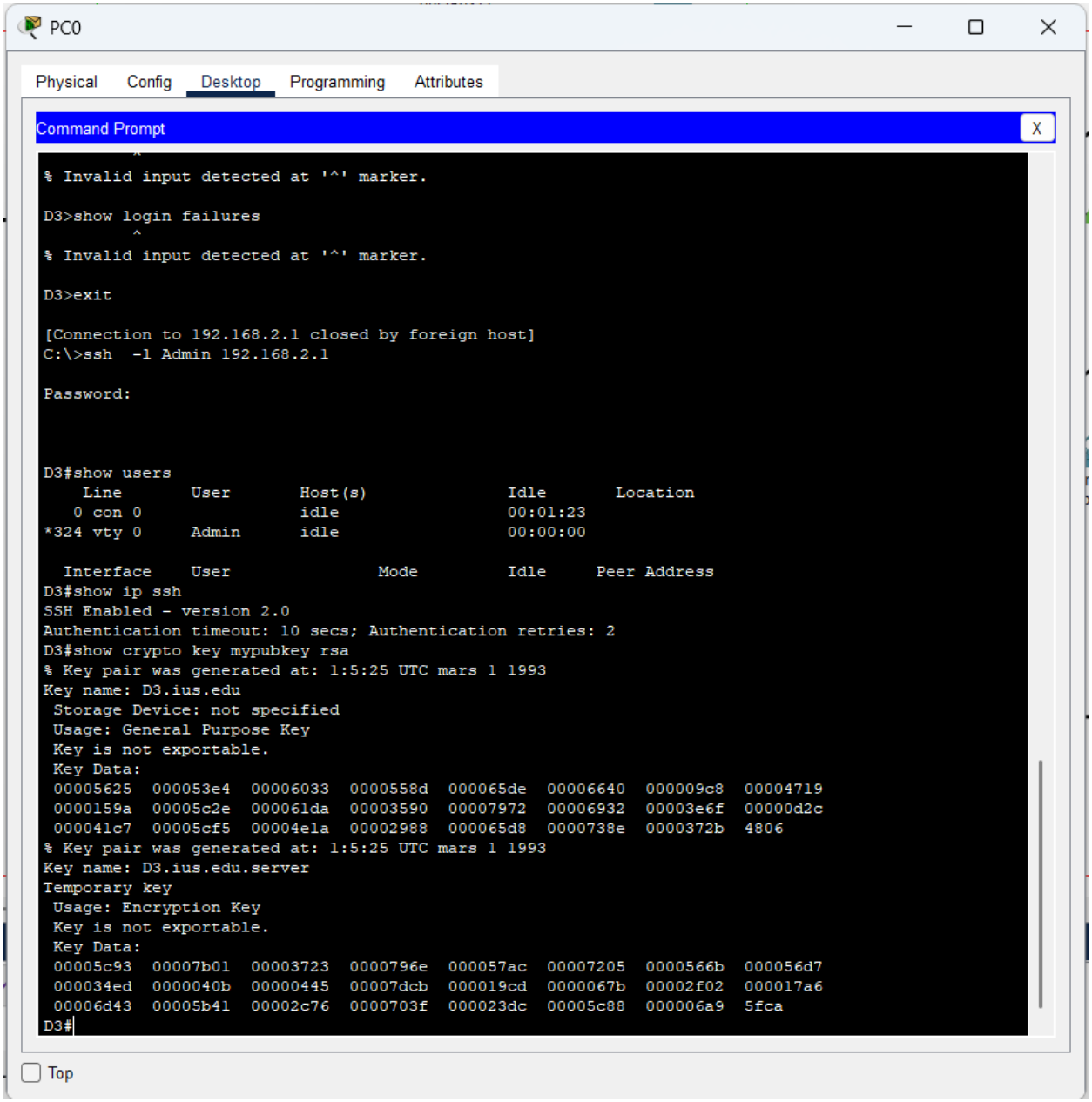

Logical
Physical
Root
PC-PT
Adm
2960-24TT
Switch7
NetworkController
PT-Controller0
2811
Router0
Server-PT
ServerMail
Server-PT
ServerWeb
2960-24TT
Switch2
2960-24TT
Switch1
2960-24TT
Switch4
Repeater-PT
Repeater1
Repeater-PT
Repeater0
2960-24TT
Switch0
Jacmel
PC-PT
Admin
Laptop-PT
Client5
Ius
Server-PT
ServerFile
Home-VoIP-PT
Home VoIP0
Printer-PT
Printer0
2960-24TT
Switch5
PC-PT
Client2
2960-24TT
Switch3
PC-PT
Client3
PC-PT
Client1
PC-PT
Client4
2960-24TT
Switch6
Server-PT
ServerDHCP

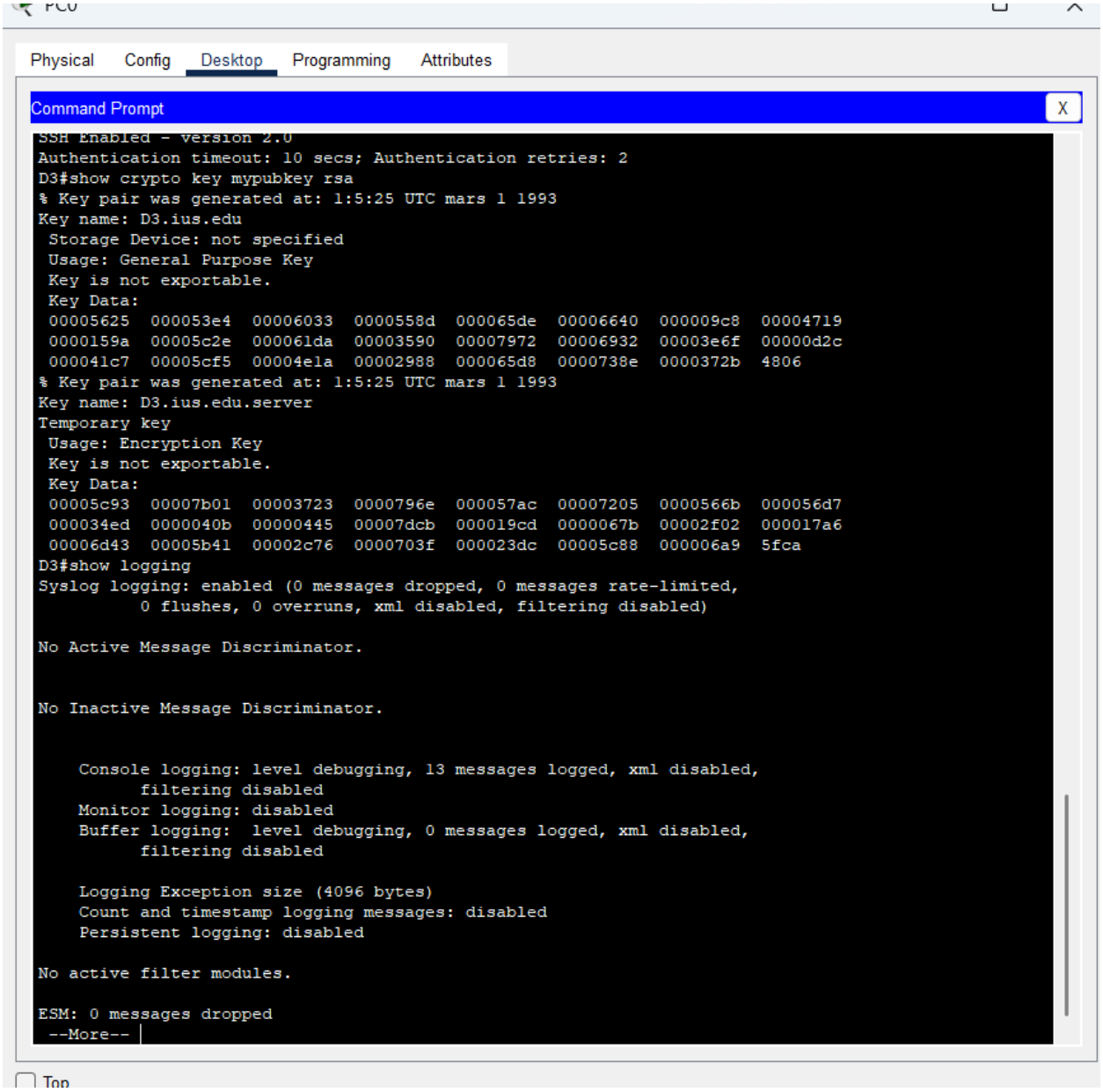

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
D3(dhcp-config)#default-router 192.168.2.1
D3(dhcp-config)#dns-server 8.8.8.8
D3(dhcp-config)#exit
D3(config)#ip dhcp pool Ius
D3(dhcp-config)#network 192.168.1.1 255.255.255.0
D3(dhcp-config)#dns-serveur 8.8.8.8
^
% Invalid input detected at '^' marker.
D3(dhcp-config)#dns-server 8.8.8.8
D3(dhcp-config)#default-router 192.168.1.1
D3(dhcp-config)#exit
D3(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2
D3(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.2
D3(config)#con f
D3(config)#service password-encryption
D3(config)#username Admin privilege 15 secret Admin@25
D3(config)#username Tech privilege 5 secret Tech@25
D3(config)#username Jacmel privilege 1 secret Jacmel@25
D3(config)#line vty 0 4
D3(config-line)# login local
D3(config-line)#transport input telnet
D3(config-line)#exec-timeout 5 30
D3(config-line)#logging synchronous
D3(config-line)#exit
D3(config)#logging buffered 6400
D3(config)#logging console
D3(config)#access-list 10 permit 192.168.2.3
D3(config)#access-list 10 deny any
D3(config)#line vty 0 4
D3(config-line)#access-class 10 in
D3(config-line)#exit
D3(config)#login block-for 30 attempts 3 within 60
D3(config)#login on-failure log
D3(config)#login on-success log
D3(config)#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin] [Source: 0.0.0.0] [localport: 0] at 00:47:41 UTC Mon Mar 1 1993
%SEC_LOGIN-5-LOGIN_FAILED: Login failed [user: Tech] [Source: 192.168.2.3] [localport: 23] [Reason: Login Authentication Failed] at 00:51:57 UTC Mon Mar 1 1993
Copy
Paste

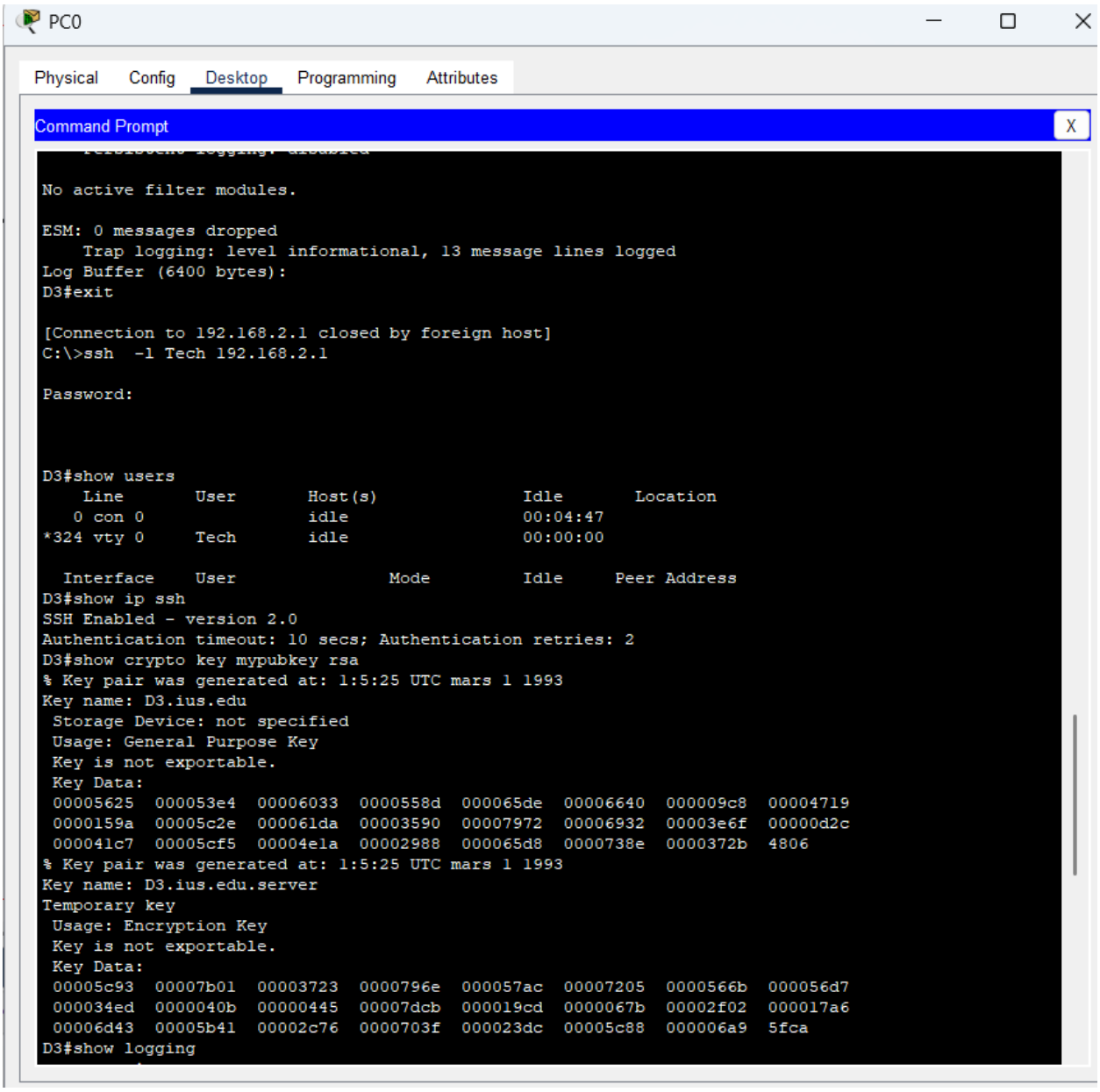

PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.2.3
Trying 192.168.2.3 ...
% Connection refused by remote host
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification
Username:
% Username: timeout expired!
[Connection to 192.168.2.1 closed by foreign host]
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification
Username: Admin
Password:
D3#show users
Line User Host(s) Idle Location
0 con 0 idle 00:04:52
*324 vty 0 Admin idle 00:00:00 192.168.2.3
Interface User Mode Idle Peer Address
D3#sow logging
^
% Invalid input detected at '^' marker.
D3#exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>Tech
Invalid Command.
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification

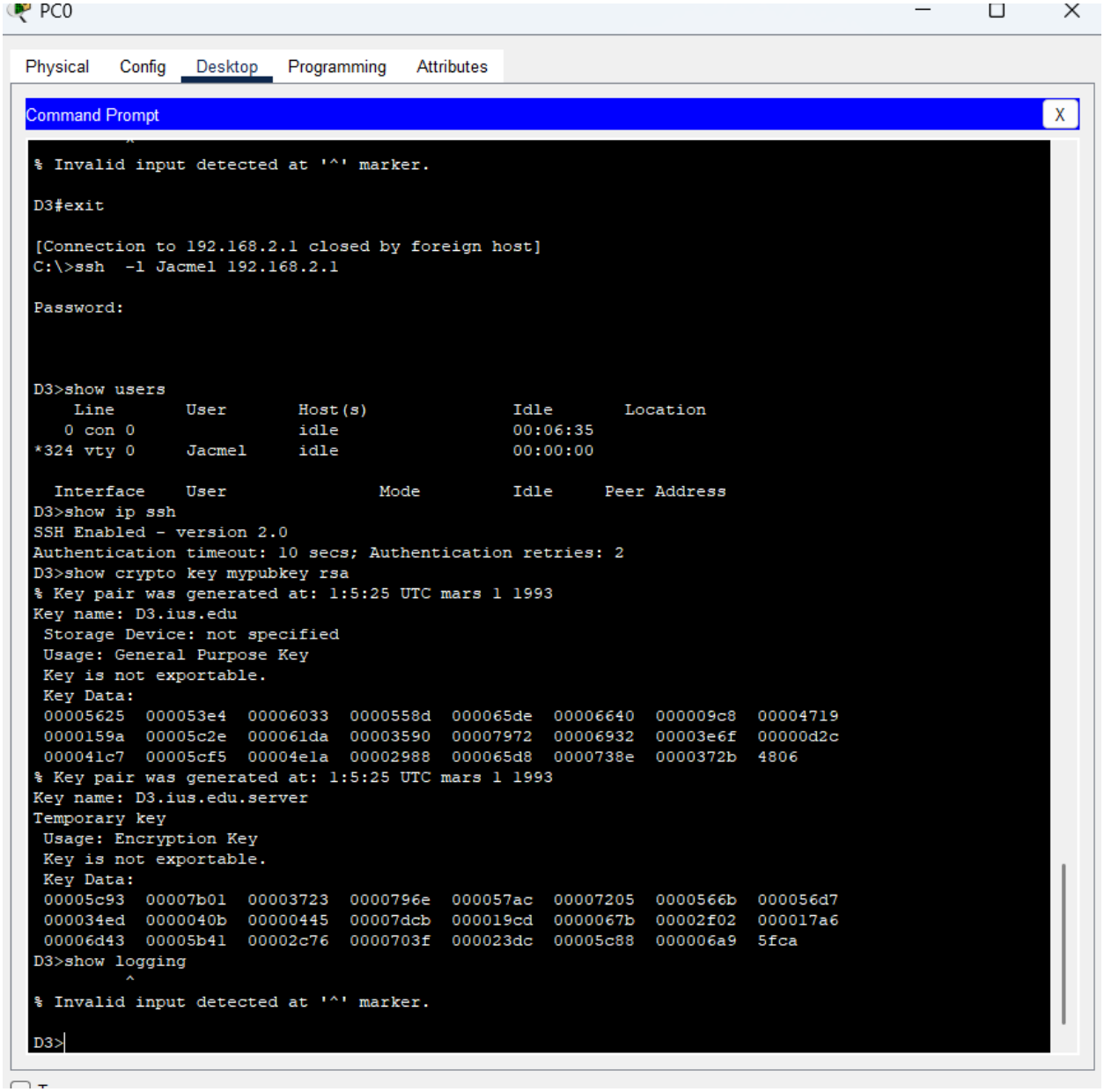

PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
[Connection to 192.168.2.1 closed by foreign host]
C:\>Tech
Invalid Command.
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification
Username: Tech
Password:
% Login invalid
Username: Tech
Password:
% Login invalid
Username: Tech
Password:
[Connection to 192.168.2.1 closed by foreign host]
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...
% Connection refused by remote host
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...
% Connection refused by remote host
C:\>
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification
Username: Tech
Password:
D3#show users
Line User Host(s) Idle Location
0 con 0 idle 00:00:47
*324 vty 0 Tech idle 00:00:00 192.168.2.3
Interface User Mode Idle Peer Address
D3#
Top


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Username: Tech
Password:
D3#show users
Line User Host(s) Idle Location
0 con 0 idle 00:00:47
*324 vty 0 Tech idle 00:00:00 192.168.2.3
Interface User Mode Idle Peer Address
D3#show logging
^
% Invalid input detected at '^' marker.
D3#show login failures
^
% Invalid input detected at '^' marker.
D3#exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification
Username: Jacmel
Password:
D3>show users
Line User Host(s) Idle Location
0 con 0 idle 00:02:38
*324 vty 0 Jacmel idle 00:00:00 192.168.2.3
Interface User Mode Idle Peer Address
D3>show logging
^
% Invalid input detected at '^' marker.
D3>show login failures
^
% Invalid input detected at '^' marker.
D3>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
% Invalid input detected at '^' marker.
D3>show login failures
^
% Invalid input detected at '^' marker.
D3>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l Admin 192.168.2.1
Password:
D3#show users
Line User Host(s) Idle Location
0 con 0 idle 00:01:23
*324 vty 0 Admin idle 00:00:00
Interface User Mode Idle Peer Address
D3#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 10 secs; Authentication retries: 2
D3#show crypto key mypubkey rsa
% Key pair was generated at: 1:5:25 UTC mars 1 1993
Key name: D3.ius.edu
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00005625 000053e4 00006033 0000558d 000065de 00006640 000009c8 00004719
0000159a 00005c2e 00006lda 00003590 00007972 00006932 00003e6f 00000d2c
000041c7 00005cf5 00004ela 00002988 000065d8 0000738e 0000372b 4806
% Key pair was generated at: 1:5:25 UTC mars 1 1993
Key name: D3.ius.edu.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00005c93 00007b01 00003723 0000796e 000057ac 00007205 0000566b 000056d7
000034ed 0000040b 00000445 00007dcb 000019cd 0000067b 00002f02 000017a6
00006d43 00005b41 00002c76 0000703f 000023dc 00005c88 000006a9 5fca
D3#
Top


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
SSH Enabled - version 2.0
Authentication timeout: 10 secs; Authentication retries: 2
D3#show crypto key mypubkey rsa
% Key pair was generated at: 1:5:25 UTC mars 1 1993
Key name: D3.ius.edu
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00005625 000053e4 00006033 0000558d 000065de 00006640 000009c8 00004719
0000159a 00005c2e 00006lda 00003590 00007972 00006932 00003e6f 00000d2c
000041c7 00005cf5 00004ela 00002988 000065d8 0000738e 0000372b 4806
% Key pair was generated at: 1:5:25 UTC mars 1 1993
Key name: D3.ius.edu.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00005c93 00007b01 00003723 0000796e 000057ac 00007205 0000566b 000056d7
000034ed 0000040b 00000445 00007dcb 000019cd 0000067b 00002f02 000017a6
00006d43 00005b41 00002c76 0000703f 000023dc 00005c88 000006a9 5fca
D3#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 13 messages logged, xml disabled,
filtering disabled
Monitor logging: disabled
Buffer logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
--More--
Top


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 13 message lines logged
Log Buffer (6400 bytes):
D3#exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l Tech 192.168.2.1
Password:
D3#show users
Line User Host(s) Idle Location
0 con 0 idle 00:04:47
*324 vty 0 Tech idle 00:00:00
Interface User Mode Idle Peer Address
D3#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 10 secs; Authentication retries: 2
D3#show crypto key mypubkey rsa
% Key pair was generated at: 1:5:25 UTC mars 1 1993
Key name: D3.ius.edu
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00005625 000053e4 00006033 0000558d 000065de 00006640 000009c8 00004719
0000159a 00005c2e 000061da 00003590 00007972 00006932 00003e6f 00000d2c
000041c7 00005cf5 00004e1a 00002988 000065d8 0000738e 0000372b 4806
% Key pair was generated at: 1:5:25 UTC mars 1 1993
Key name: D3.ius.edu.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00005c93 00007b01 00003723 0000796e 000057ac 00007205 0000566b 000056d7
000034ed 0000040b 00000445 00007dcb 000019cd 0000067b 00002f02 000017a6
00006d43 00005b41 00002c76 0000703f 000023dc 00005c88 000006a9 5fca
D3#show logging



Questions :A

1. Pourquoi Telnet est-il considéré comme non sécurisé ?

   Telnet est considéré comme non sécurisé car il transmet toutes les données, y compris les identifiants noms d'utilisateur et mots de passe, sans chiffrement, ce qui les rend vulnérables à l'interception par des pirates qui peuvent les lire facilement sur le réseau. Il n'offre aucune authentification robuste, permettant l'usurpation d'identité, et est obsolète, remplacé par des protocoles sécurisés comme SSH qui chiffrent les communications

2. Quelles informations transitent en clair ?

   Les informations qui transitent en clair sont celles qui ne sont pas chiffrées et peuvent être lues directement par n'importe qui interceptant le trafic, incluant des données personnelles nom, email, des informations de connexion mots de passe, identifiants, des historiques de navigation, des données de localisation, et parfois des informations financières (numéros de carte bancaire) si le site n'utilise pas HTTPS. Il s'agit principalement de données sensibles non protégées, contrairement aux données chiffrées HTTPS, VPN qui sont illisibles sans la clé de déchiffrement.

3. Pourquoi est-il déconseillé d'utiliser Telnet en production

Il est fortement déconseillé d'utiliser Telnet en production car il transmet toutes les données, y compris les mots de passe et les informations sensibles, sur le réseau, sans aucune forme de chiffrement, rendant les communications vulnérables à l'interception (écoute clandestine) et à la falsification par des pirates via des outils comme Wireshark. Pour une connexion distante sécurisée, il faut utiliser des alternatives chiffrées comme SSH Secure Shell, qui crypte tout le trafic, protégeant ainsi les identifiants et les données transmises.

Questions :B

1. Quelle différence entre SSH v1 et SSH v2 ?

   La différence entre SSHv1 et SSH v2

   SSH (Secure Shell) est un protocole de communication sécurisée. SSH v2 (1996) a été développé pour corriger les vulnérabilités structurelles de SSH v1 (1995).

   SSH v1 utilise des mécanismes de chiffrement plus faibles et souffre de vulnérabilités connues (notamment des failles dans l'intégrité des données) tandis que **SSH v2** introduit des algorithmes de chiffrement modernes (AES, 3DES, etc.), une meilleure vérification d'intégrité et une séparation claire des couches du protocole, ce qui le rend beaucoup plus robuste.

   En résume **SSH v1** : ancien, vulnérable, non recommandé.

   SSH v2 : sécurisé, modulaire, supporte des algorithmes modernes, et est le standard actuel.

2. Pourquoi RSA 1024 bits n’est plus recommandé ?

   Le RSA avec une clé de **1024 bits** n'est plus recommandé aujourd'hui principalement en raison des avancées de la puissance de calcul et des attaques cryptographiques qui rendent le cassage de la clé possible ou économiquement réalisable.

   La Vulnérabilité aux attaques par factorisation

   La sécurité de RSA repose sur la difficulté de factoriser de grands nombres (produit de deux nombres premiers.

   Avec l’augmentation de la puissance de calcul notamment grâce aux ordinateurs quantiques et aux progrès en algorithmes de factorisation comme l’algorithme de Shor, 1024 bits est désormais considéré comme trop faible.

   Des attaques pratiques ont démontré qu’il est possible de casser une clé RSA 1024 bits avec des ressources suffisantes.

   RSA 1024 bits est obsolète car il n’offre plus un niveau de sécurité suffisant face aux menaces actuelles et futures. Il est recommandé d’utiliser RSA 2048 bits ou plus, ou de migrer vers des algorithmes post-quantiques si nécessaire.

3. Que se passe-t-il si on désactive le domaine local ?

   La désactivation ou le retrait d'un ordinateur du domaine local entraîne un certain nombre de changements et de conséquences importantes.

   Le point clé est que l'ordinateur passe d'un état de gestion centralisée à un état de gestion locale et autonome.

   Les utilisateurs ne peuvent plus se connecter à l'ordinateur en utilisant leurs identifiants de domaine nom d'utilisateur et mot de passe centralisés.

   L'ordinateur ne peut plus vérifier les identités auprès du Contrôleur de Domaine .

   La désactivation du domaine local est une action qui rend la machine isolée en termes de gestion et d'authentification. C'est une démarche courante pour transformer un poste de travail d'entreprise en un poste de travail autonome.

En conclusion J'ai eu beaucoup de mal à m'adapter à l'exercice, il paraissait vraiment compliqué. Mais en réalité, lorsque je l'ai terminé, j'ai vu qu'il était vraiment facile, et cela m'a aidé à bien comprendre l'exercice. C'était une très belle expérience, et malgré tous les problèmes que j'ai rencontrés, j'ai fini par tout résoudre et trouver une bonne solution pour chaque élément. J'ai réussi la tâche correctement, étape par étape. Après ça, je suis devenu content, et j'ai beaucoup appris avec ce travail. Et je souhaite aller encore plus loin.

L’objectif de ce TD est de :

1. Activer Telnet en mode sécurisé
2. Créer plusieurs niveaux d’utilisateurs
3. Restreindre l’accès Telnet via ACL
4. Journaliser les connexions
5. Mettre en place une bannière légale
6. Tester Telnet depuis plusieurs VLAN
7. Superviser les sessions actives
8. Configurer timeouts et protections
9. Configurer SSH avec clés RSA 2048/4096 bits
10. Mettre en place différents niveaux d’utilisateurs (privilèges 1, 5, 15)
11. Restreindre l’accès SSH via ACL
12. Activer SSH version 2 (obligatoire)
13. Configurer des timers de sécurité
14. Activer protection contre brute-force
15. Journaliser tentatives réussies/échouées
16. Superviser sessions SSH actives
17. Durcir l’équipement