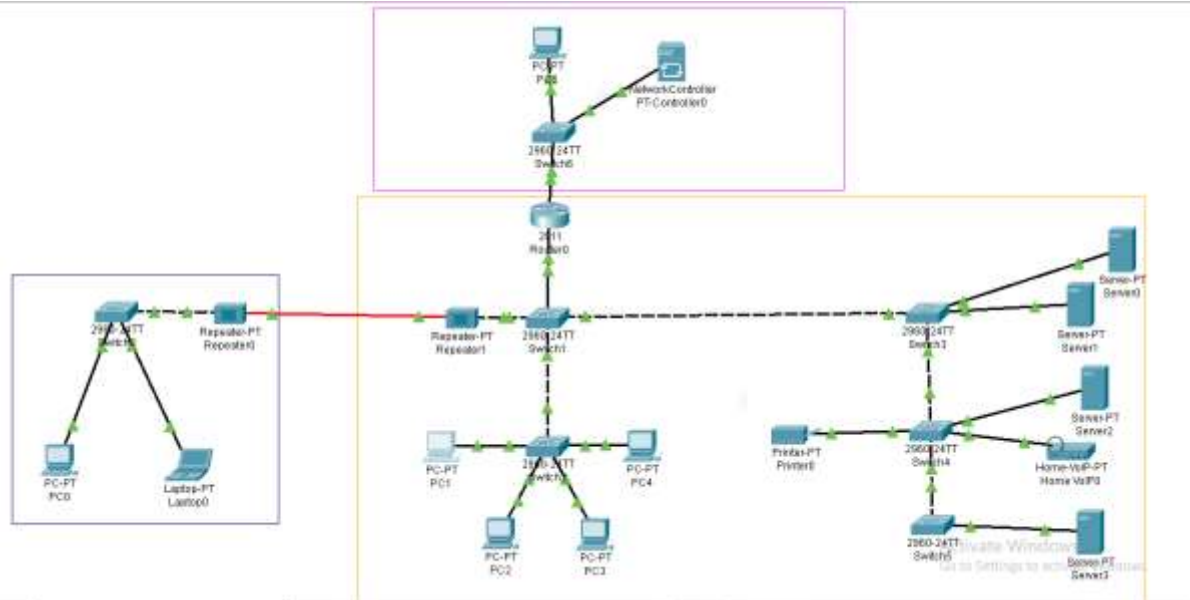
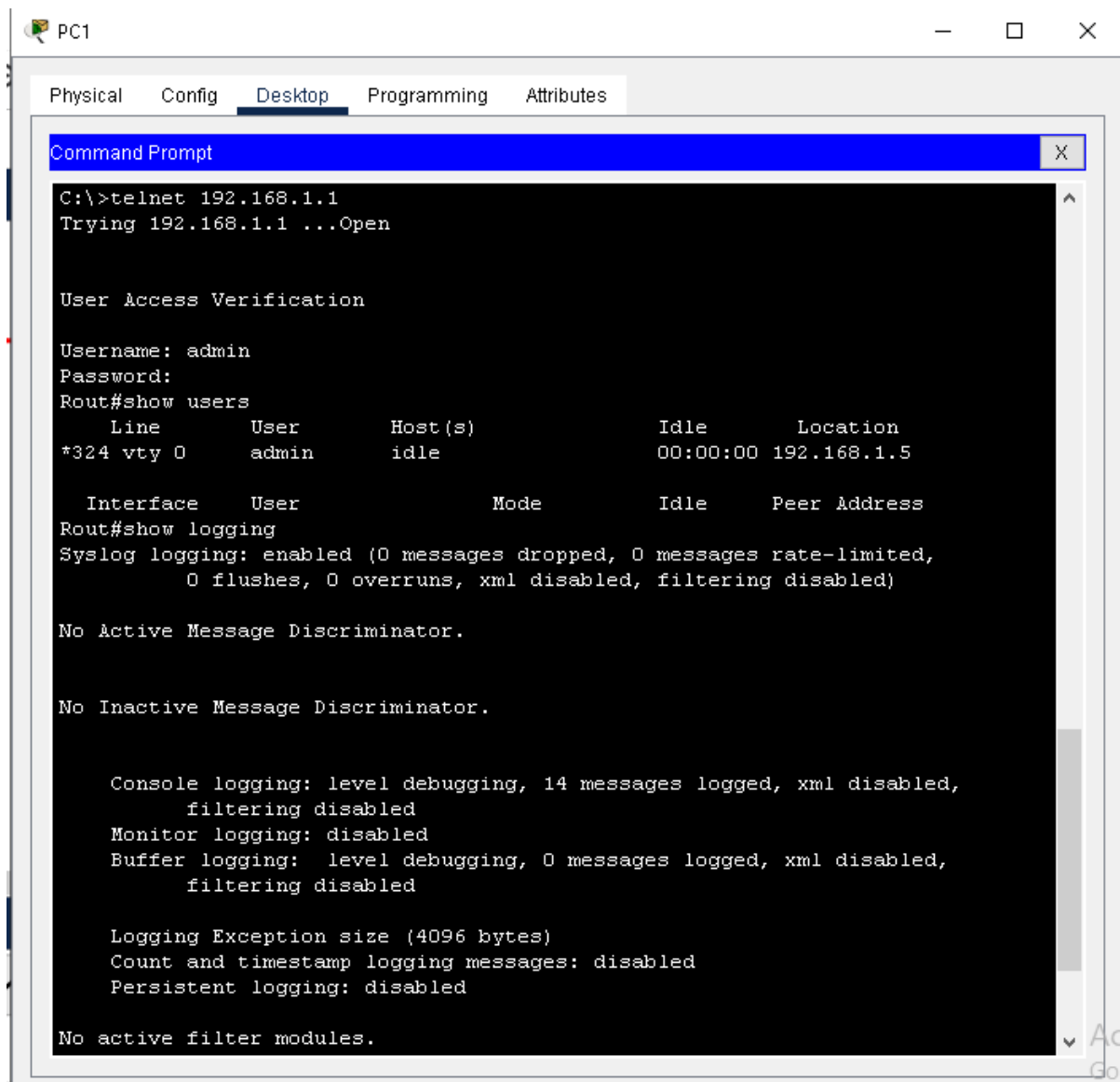


Topologie



Configuration Telnet (partie non sécurisée)

Tester l'accès Telnet :



The screenshot shows a PC1 window with a 'Desktop' tab selected. Inside is a 'Command Prompt' window. The user has executed the command 'telnet 192.168.1.1'. The output shows a successful connection to a router. The user 'admin' has logged in. The router prompt is 'Rout#'. The user has entered the command 'show users', which displays a table of active users. The user has then entered 'show logging', which displays various logging configurations. The output is as follows:

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification
Username: admin
Password:
Rout#show users
      Line      User      Host(s)      Idle      Location
*324 vty 0      admin      idle         00:00:00  192.168.1.5

      Interface      User      Mode      Idle      Peer Address
Rout#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, 14 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.
```

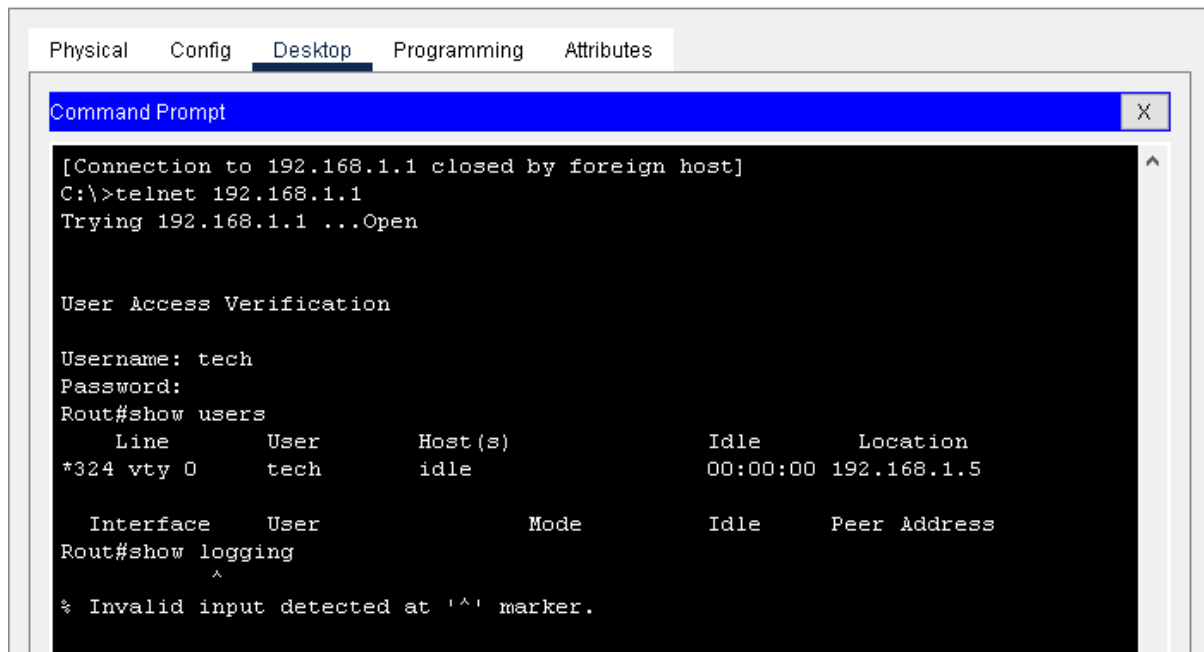


This block shows the continuation of the Telnet session output from the previous screenshot. The user has entered the command 'show login failures', which displays the login failure statistics. The output is as follows:

```
No active filter modules.

ESM: 0 messages dropped
      Trap logging: level informational, 14 message lines logged
Log Buffer (64000 bytes):
Rout#show login failures
*** No logged failed login attempts with the device.***

Rout#
```



```
[Connection to 192.168.1.1 closed by foreign host]
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Username: tech
Password:
Rout#show users
      Line      User      Host(s)      Idle      Location
*324 vty 0      tech      idle        00:00:00  192.168.1.5

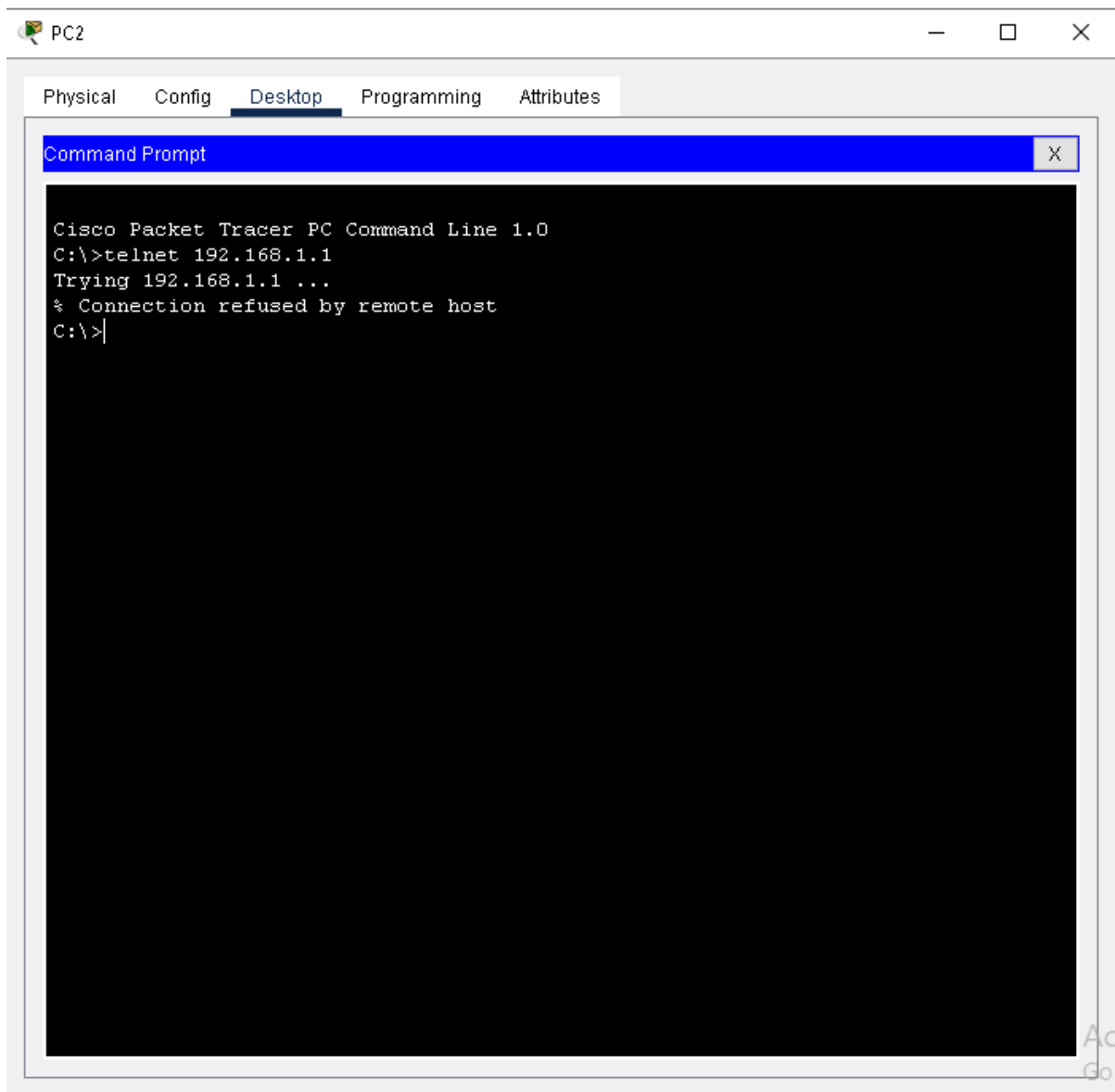
      Interface  User      Mode      Idle      Peer Address
Rout#show logging
      ^
% Invalid input detected at '^' marker.
```

```
[Connection to 192.168.1.1 closed by foreign host]
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

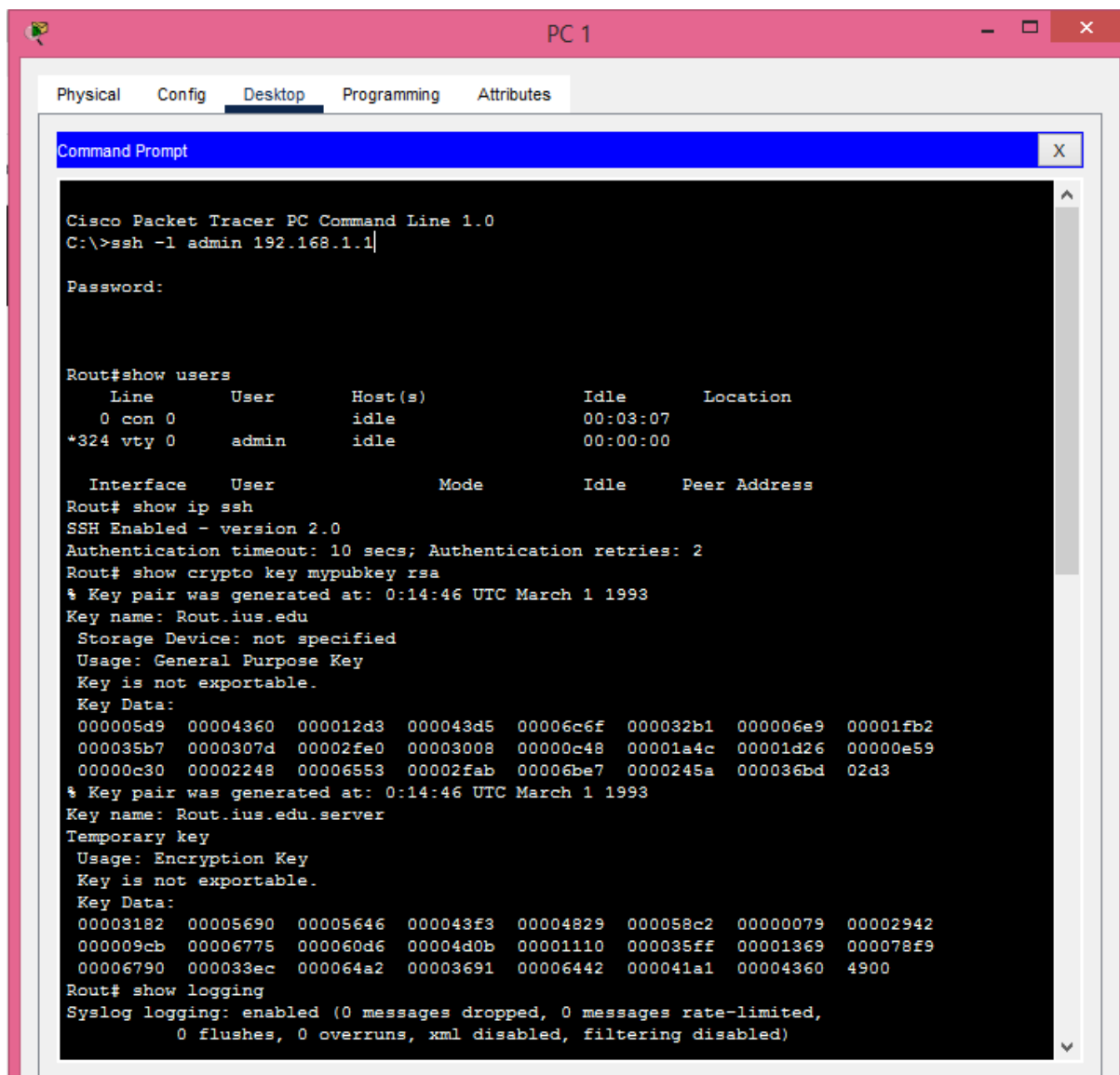
Username: guest
Password:
Rout>show users
      Line      User      Host(s)      Idle      Location
*324 vty 0      guest     idle        00:00:00  192.168.1.5

      Interface  User      Mode      Idle      Peer Address
Rout>show logging
      ^
% Invalid input detected at '^' marker.
```



Configuration SSH (partie sécurisée)

Tester l'accès SSH :



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC 1. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.1.1

Password:

Rout#show users
      Line        User       Host(s)      Idle       Location
  0 con 0
*324 vty 0      admin      idle         00:03:07
                                00:00:00

      Interface    User              Mode        Idle       Peer Address
Rout# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 10 secs; Authentication retries: 2
Rout# show crypto key mypubkey rsa
% Key pair was generated at: 0:14:46 UTC March 1 1993
Key name: Rout.ius.edu
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
000005d9 00004360 000012d3 000043d5 00006c6f 000032b1 000006e9 00001fb2
000035b7 0000307d 00002fa0 00003008 00000c48 00001a4c 00001d26 00000e59
00000c30 00002248 00006553 00002fab 00006be7 0000245a 000036bd 02d3
% Key pair was generated at: 0:14:46 UTC March 1 1993
Key name: Rout.ius.edu.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00003182 00005690 00005646 000043f3 00004829 000058c2 00000079 00002942
000009cb 00006775 000060d6 00004d0b 00001110 000035ff 00001369 000078f9
00006790 000033ec 000064a2 00003691 00006442 000041a1 00004360 4900
Rout# 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, 10 messages logged, xml disabled,
filtering disabled
Monitor logging: disabled
Buffer logging: disabled, 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

Trap logging: level informational, 10 message lines logged

Rout#

Rout#exit

