# TP3 : ICMP - TCP - UDP

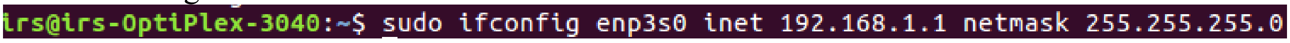
## CAUMES Clément (PC1) – LAMMAMRA Aicha (PC2) – MTALSI MERIMI Mehdi (PC3) – RAMAROSON Andritsalama (PC4)

### Exercice 1-2

1) On va faire la configuration suivante :

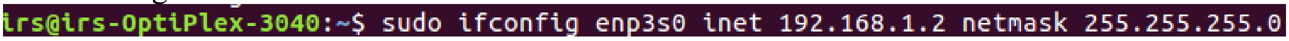
- Le sous réseau 192.168.1.0 sera composé du PC de Clément (PC1) et celui d'Aicha (PC2) qui seront connectés à l'aide d'un concentrateur 1.
- Le sous réseau 192.168.2.0 sera composé du PC de Mehdi (PC3) et celui de Andritsalama (PC4) qui seront connectés avec un concentrateur 2.
- Les deux concentrateurs seront connectés par un routeur.

Clément configure  l'adresse IP et le mask du PC1 :



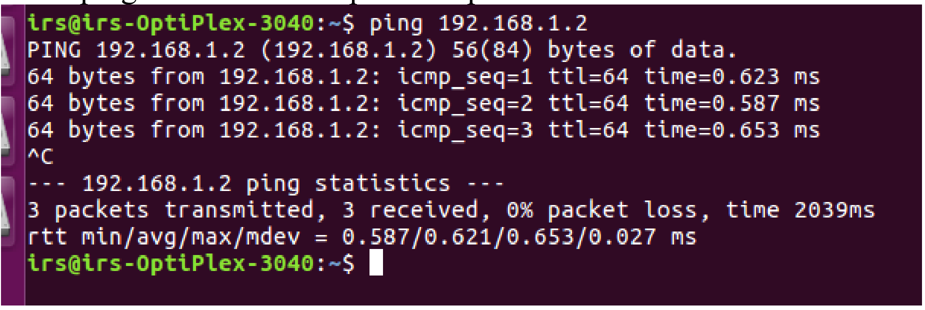
```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.1.1 netmask 255.255.255.0
```

Aicha configure l'adresse IP et le mask du PC2 :



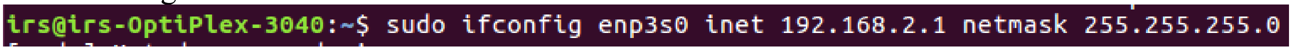
```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.1.2 netmask 255.255.255.0
```

On peut envoyer un ping du PC1 au PC2 par exemple :



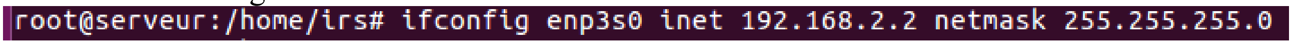
```
irs@irs-OptiPlex-3040:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.623 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.587 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.653 ms
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.587/0.621/0.653/0.027 ms
irs@irs-OptiPlex-3040:~$ 
```

Mehdi configure l'adresse IP et le mask du PC3 :



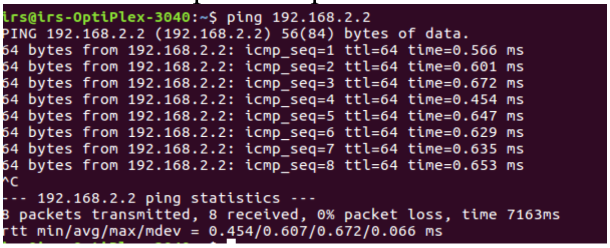
```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.2.1 netmask 255.255.255.0
```

Andritsalama configure l'adresse IP et le mask du PC4 :



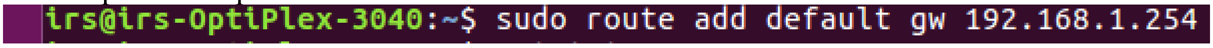
```
root@serveur:/home/irs# ifconfig enp3s0 inet 192.168.2.2 netmask 255.255.255.0
```

On peut envoyer un ping du PC3 au PC4 par exemple :



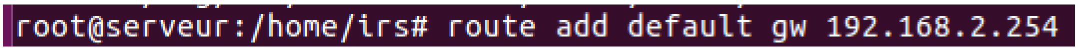
```
irs@irs-OptiPlex-3040:~$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.566 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=0.672 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=64 time=0.454 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=64 time=0.647 ms
64 bytes from 192.168.2.2: icmp_seq=6 ttl=64 time=0.629 ms
64 bytes from 192.168.2.2: icmp_seq=7 ttl=64 time=0.635 ms
64 bytes from 192.168.2.2: icmp_seq=8 ttl=64 time=0.653 ms
^C
--- 192.168.2.2 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7163ms
rtt min/avg/max/mdev = 0.454/0.607/0.672/0.066 ms
```

2) On insère la ligne de la passerelle par défaut :
La passerelle par défaut du sous réseau 192.168.1.0 sera 192.168.1.254 :



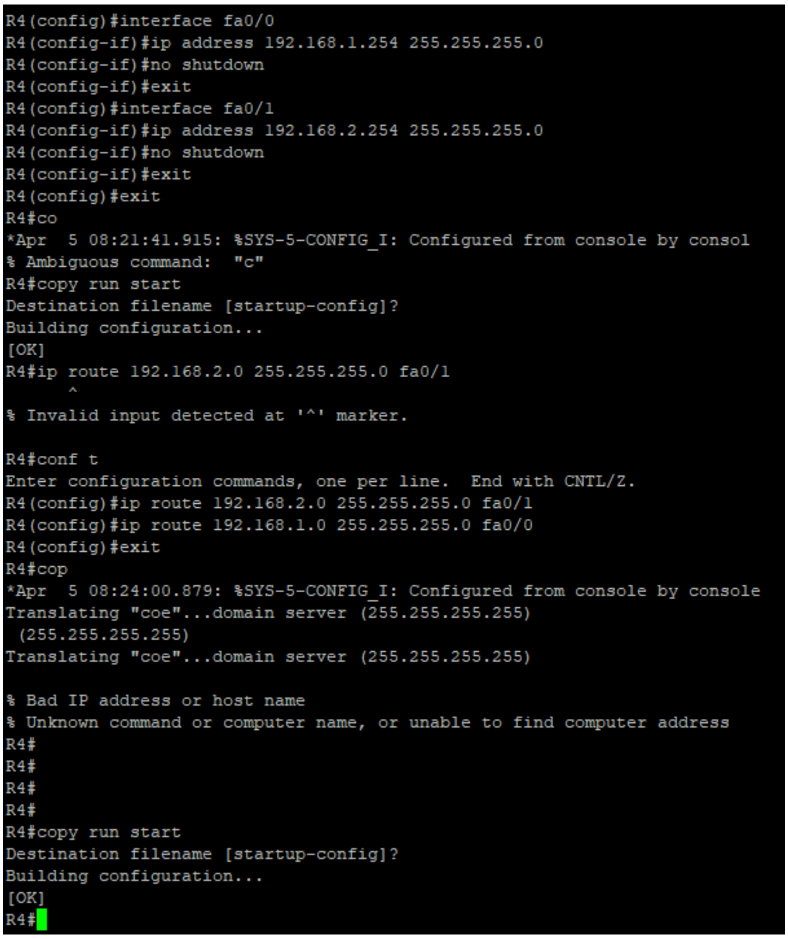
```
irs@irs-OptiPlex-3040:~$ sudo route add default gw 192.168.1.254
```

La passerelle par défaut du sous réseau 192.168.2.0 sera 192.168.2.254 :



```
root@serveur:/home/irs# route add default gw 192.168.2.254
```

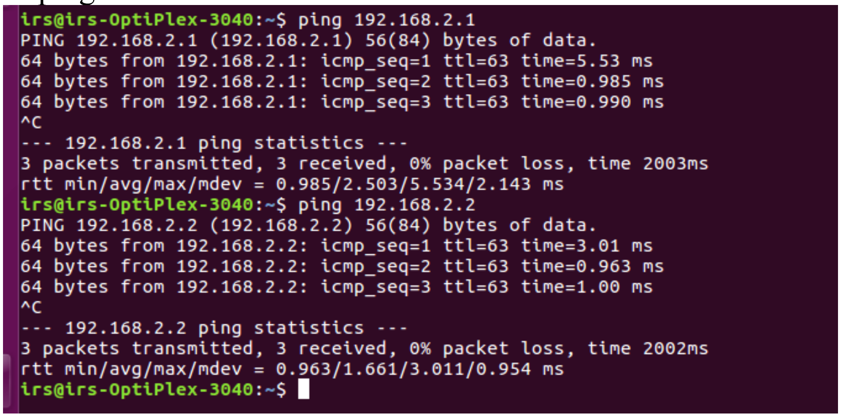
3) Pour réussir à envoyer un ping entre les deux sous réseaux, il faut configurer le routeur :



```
R4(config)#interface fa0/0
R4(config-if)#ip address 192.168.1.254 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface fa0/1
R4(config-if)#ip address 192.168.2.254 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#exit
R4#co
*Apr  5 08:21:41.915: %SYS-5-CONFIG_I: Configured from console by consol
% Ambiguous command:  "c"
R4#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R4#ip route 192.168.2.0 255.255.255.0 fa0/1
      ^
% Invalid input detected at '^' marker.

R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip route 192.168.2.0 255.255.255.0 fa0/1
R4(config)#ip route 192.168.1.0 255.255.255.0 fa0/0
R4(config)#exit
R4#cop
*Apr  5 08:24:00.879: %SYS-5-CONFIG_I: Configured from console by console
Translating "coe"...domain server (255.255.255.255)
 (255.255.255.255)
Translating "coe"...domain server (255.255.255.255)

% Bad IP address or host name
% Unknown command or computer name, or unable to find computer address
R4#
R4#
R4#
R4#
R4#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R4#
```

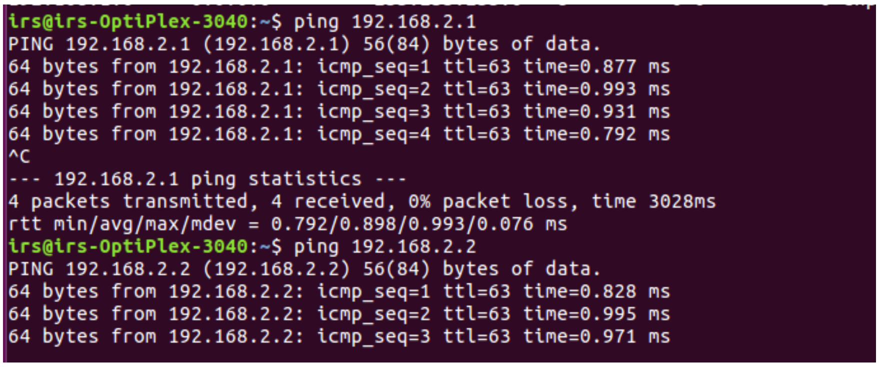
Pour cela, on connecte le réseau 192.168.1.0 à l'interface fa0/0 d'adresse IP 192.168.1.254. On connecte le réseau 192.168.2.0 à l'interface fa0/1 d'adresse IP 192.168.2.254.

On peut maintenant ping PC1 vers PC3 et PC4 :



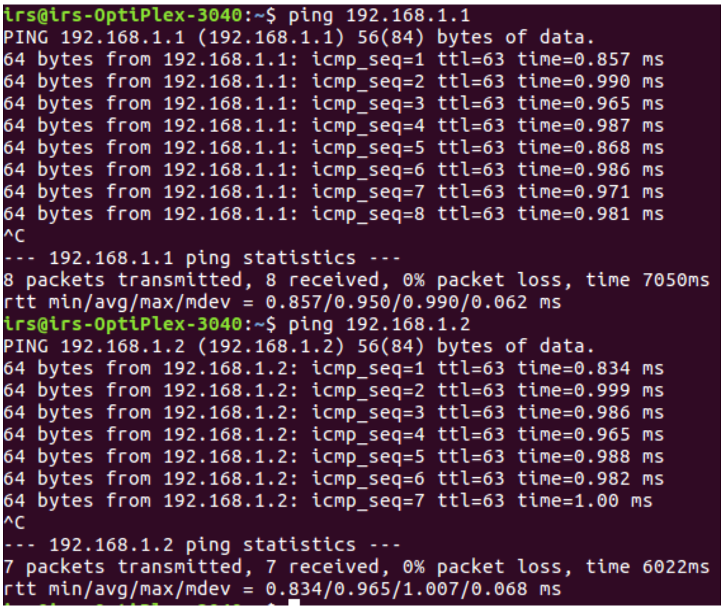
```
irs@irs-OptiPlex-3040:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=5.53 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=0.985 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=0.990 ms
^C
--- 192.168.2.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.985/2.503/5.534/2.143 ms
irs@irs-OptiPlex-3040:~$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=3.01 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=0.963 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=1.00 ms
^C
--- 192.168.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.963/1.661/3.011/0.954 ms
irs@irs-OptiPlex-3040:~$
```

On peut ping PC2 vers PC3 et PC4 :



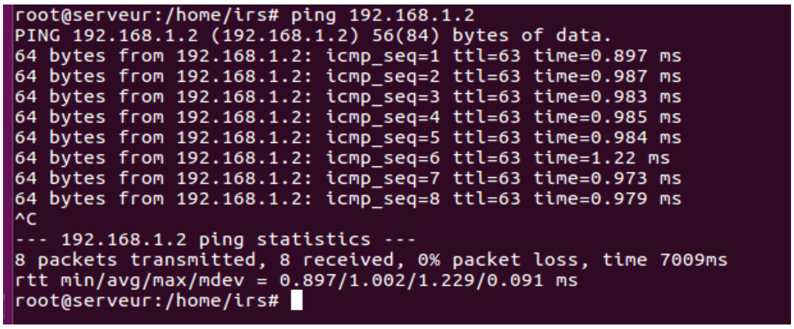
```
irs@irs-OptiPlex-3040:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=0.877 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=0.993 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=0.931 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=0.792 ms
^C
--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3028ms
rtt min/avg/max/mdev = 0.792/0.898/0.993/0.076 ms
irs@irs-OptiPlex-3040:~$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=0.828 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=0.995 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=0.971 ms
```

On peut ping PC3 vers PC1 et PC2 :



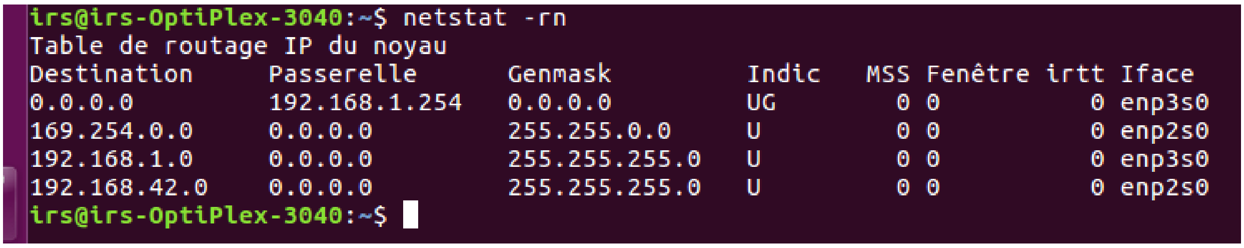
```
irs@irs-OptiPlex-3040:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=0.857 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=0.990 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=0.965 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=0.987 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=63 time=0.868 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=63 time=0.986 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=63 time=0.971 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=63 time=0.981 ms
^C
--- 192.168.1.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7050ms
rtt min/avg/max/mdev = 0.857/0.950/0.990/0.062 ms
irs@irs-OptiPlex-3040:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.834 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=0.999 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=0.986 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=0.965 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=63 time=0.988 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=63 time=0.982 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=63 time=1.00 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6022ms
rtt min/avg/max/mdev = 0.834/0.965/1.007/0.068 ms
```

On peut ping PC4 vers PC1 et PC2 :



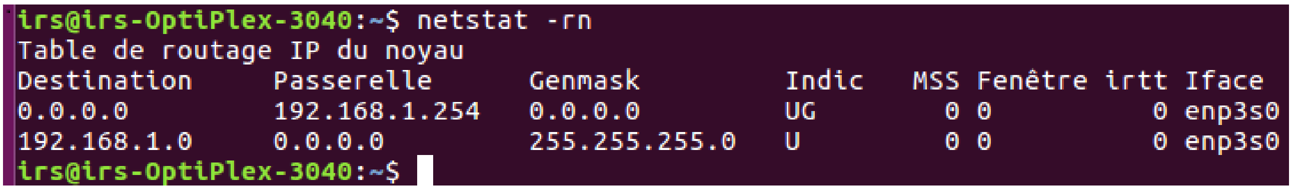
```
root@serveur:/home/irs# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.897 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=0.987 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=0.983 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=0.985 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=63 time=0.984 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=63 time=1.22 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=63 time=0.973 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=63 time=0.979 ms
^C
--- 192.168.1.2 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7009ms
rtt min/avg/max/mdev = 0.897/1.002/1.229/0.091 ms
root@serveur:/home/irs# 
```

4) On obtient donc les tables de routage suivantes :
Pour le PC1 :



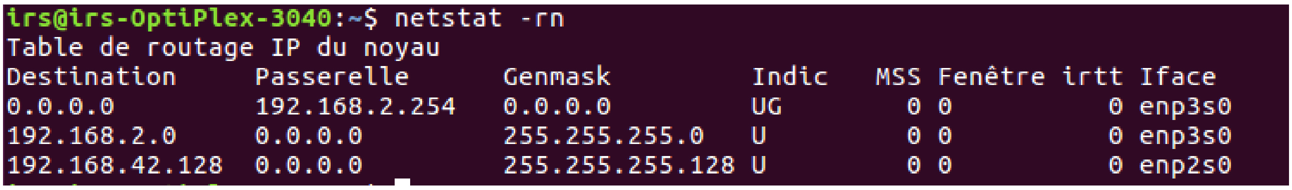
```
irs@irs-OptiPlex-3040:~$ netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
0.0.0.0         192.168.1.254   0.0.0.0         UG        0 0          0 enp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 enp2s0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 enp3s0
192.168.42.0    0.0.0.0         255.255.255.0   U         0 0          0 enp2s0
irs@irs-OptiPlex-3040:~$ 
```

Pour le PC2 :



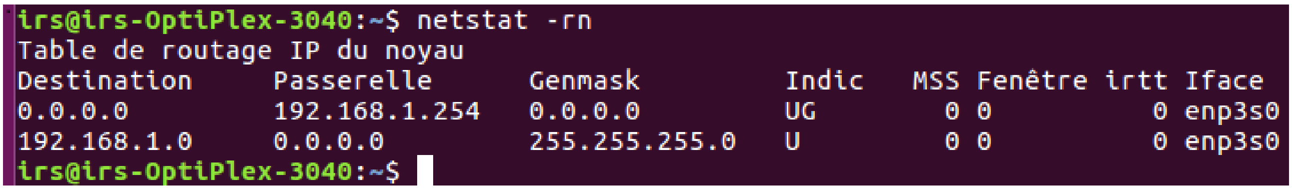
```
irs@irs-OptiPlex-3040:~$ netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
0.0.0.0         192.168.1.254   0.0.0.0         UG        0 0          0 enp3s0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 enp3s0
irs@irs-OptiPlex-3040:~$ 
```

Pour le PC3 :



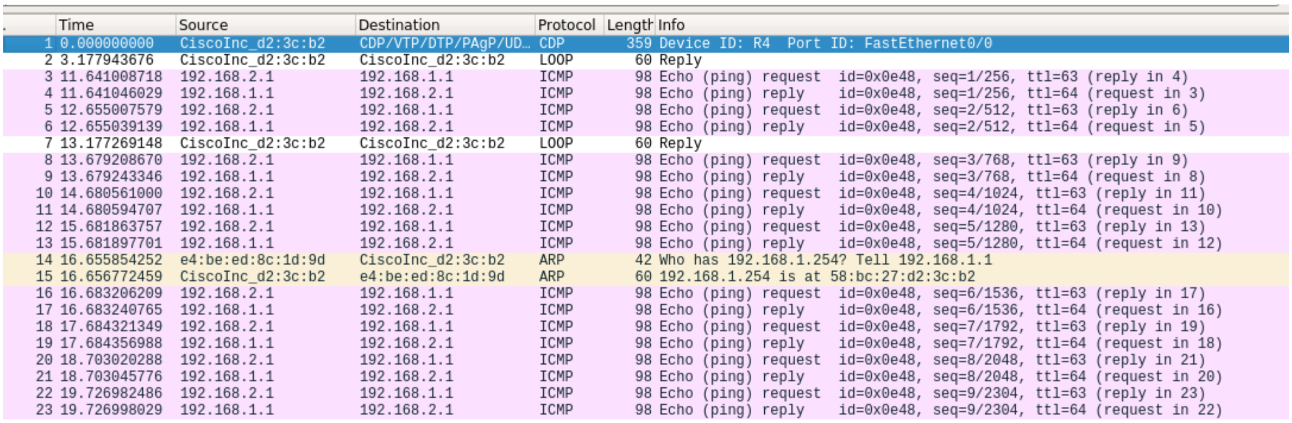
```
irs@irs-OptiPlex-3040:~$ netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
0.0.0.0         192.168.2.254   0.0.0.0         UG        0 0          0 enp3s0
192.168.2.0     0.0.0.0         255.255.255.0   U         0 0          0 enp3s0
192.168.42.128  0.0.0.0         255.255.255.128 U         0 0          0 enp2s0
```

Pour le PC4 :



```
irs@irs-OptiPlex-3040:~$ netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
0.0.0.0         192.168.1.254   0.0.0.0         UG        0 0          0 enp3s0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 enp3s0
irs@irs-OptiPlex-3040:~$
```

5)

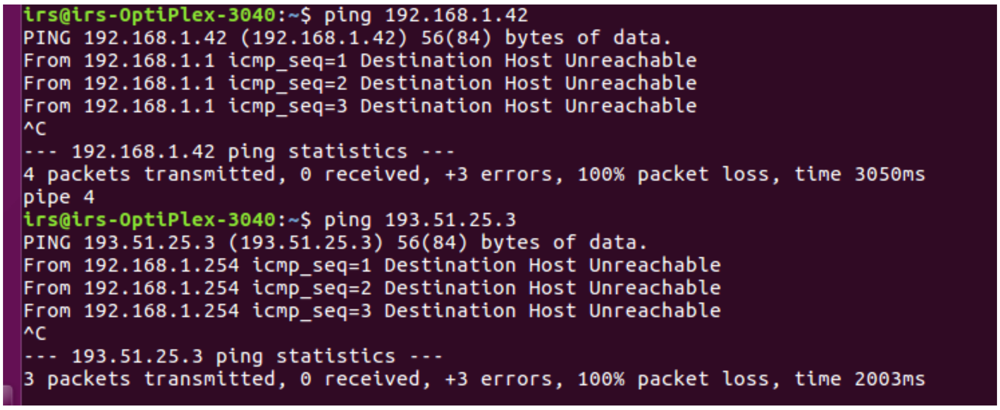


```
    Time           Source               Destination          Protocol Length Info
  1 0.000000000    CiscoInc_d2:3c:b2    CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/0
  2 3.177943676    CiscoInc_d2:3c:b2    CiscoInc_d2:3c:b2    LOOP       60 Reply
  3 11.641008718   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=1/256, ttl=63 (reply in 4)
  4 11.641046029   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=1/256, ttl=64 (request in 3)
  5 12.655007579   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=2/512, ttl=63 (reply in 6)
  6 12.655039139   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=2/512, ttl=64 (request in 5)
  7 13.177269148   CiscoInc_d2:3c:b2    CiscoInc_d2:3c:b2    LOOP       60 Reply
  8 13.679208670   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=3/768, ttl=63 (reply in 9)
  9 13.679243346   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=3/768, ttl=64 (request in 8)
 10 14.680561000   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=4/1024, ttl=63 (reply in 11)
 11 14.680594707   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=4/1024, ttl=64 (request in 10)
 12 15.681863757   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=5/1280, ttl=63 (reply in 13)
 13 15.681897701   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=5/1280, ttl=64 (request in 12)
 14 16.655854252   e4:be:ed:8c:1d:9d    CiscoInc_d2:3c:b2    ARP        42 Who has 192.168.1.254? Tell 192.168.1.1
 15 16.656772459   CiscoInc_d2:3c:b2    e4:be:ed:8c:1d:9d    ARP        60 192.168.1.254 is at 58:bc:27:d2:3c:b2
 16 16.683206209   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=6/1536, ttl=63 (reply in 17)
 17 16.683240765   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=6/1536, ttl=64 (request in 16)
 18 17.684321349   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=7/1792, ttl=63 (reply in 19)
 19 17.684356988   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=7/1792, ttl=64 (request in 18)
 20 18.703020288   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=8/2048, ttl=63 (reply in 21)
 21 18.703045776   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=8/2048, ttl=64 (request in 20)
 22 19.726982486   192.168.2.1          192.168.1.1          ICMP       98 Echo (ping) request  id=0x0e48, seq=9/2304, ttl=63 (reply in 23)
 23 19.726998029   192.168.1.1          192.168.2.1          ICMP       98 Echo (ping) reply    id=0x0e48, seq=9/2304, ttl=64 (request in 22)
```

On remarque que les trames transitées sont des trames ICMP. Sur cet exemple, le PC2 envoie des pings au PC1.

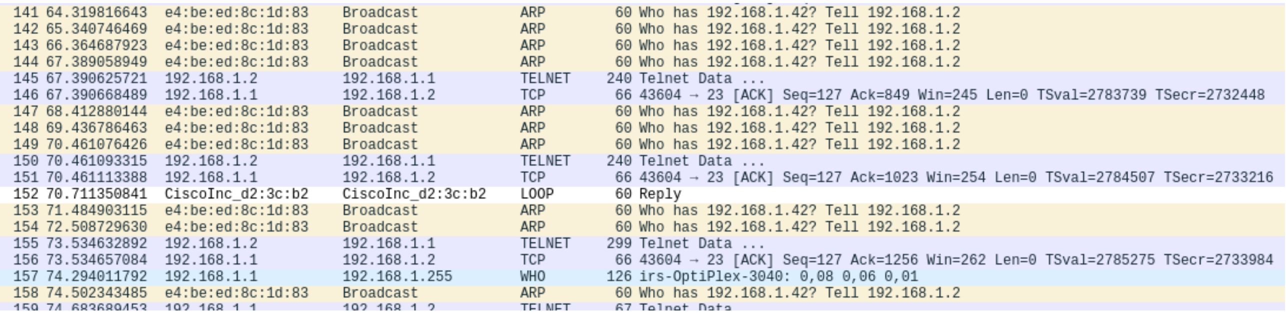
## Exercice 3

On va envoyer des pings à deux adresses IP qui ne sont pas dans notre réseau (ici l'exemple est pour PC1) :



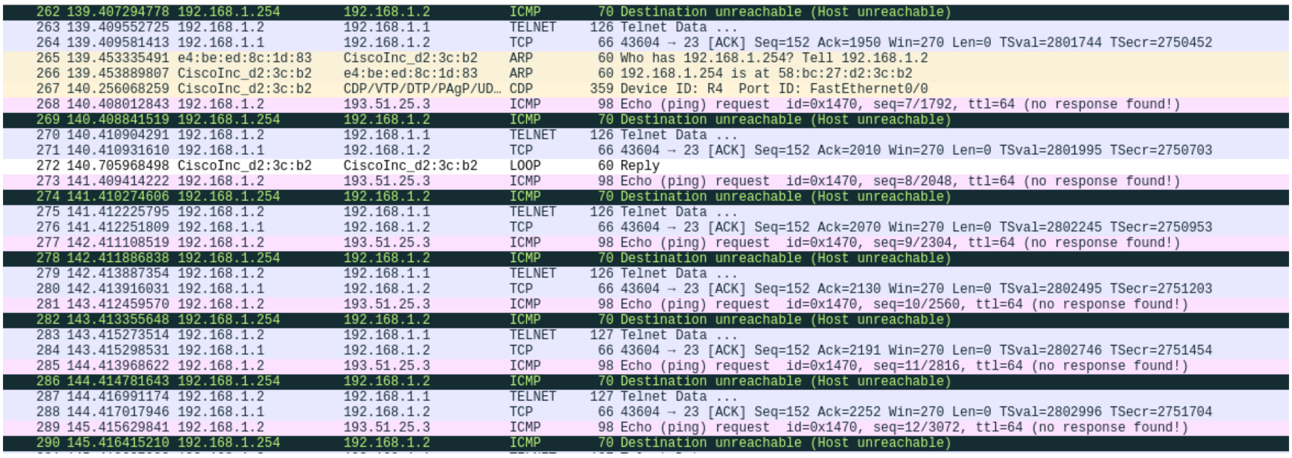
```
irs@irs-OptiPlex-3040:~$ ping 192.168.1.42
PING 192.168.1.42 (192.168.1.42) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.1.42 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3050ms
pipe 4
irs@irs-OptiPlex-3040:~$ ping 193.51.25.3
PING 193.51.25.3 (193.51.25.3) 56(84) bytes of data.
From 192.168.1.254 icmp_seq=1 Destination Host Unreachable
From 192.168.1.254 icmp_seq=2 Destination Host Unreachable
From 192.168.1.254 icmp_seq=3 Destination Host Unreachable
^C
--- 193.51.25.3 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2003ms
```

On remarque ainsi que le temps est nettement supérieur pour l'IP « host down» car le ping devient une trame ARP afin de connaître l'adresse physique de l'hôte possiblement appartenant au réseau (192.168.1.42) :



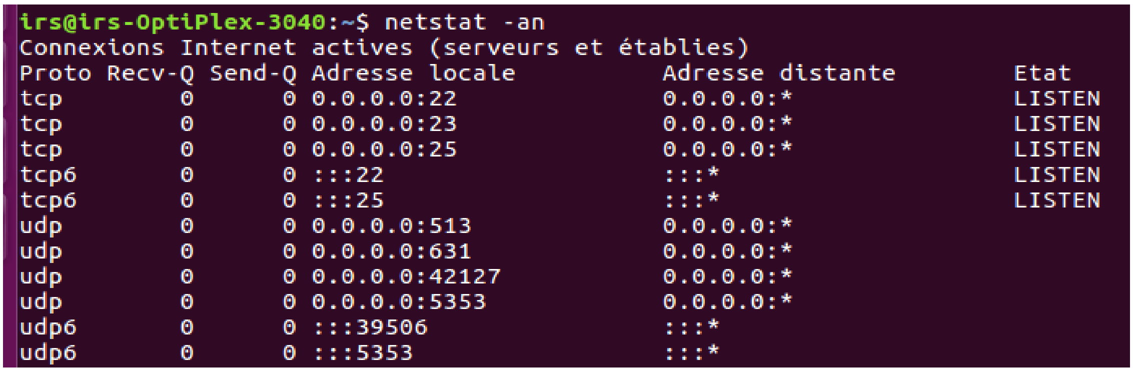
```
141 64.319816643  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
142 65.340746469  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
143 66.364687923  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
144 67.389058949  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
145 67.390625721  192.168.1.2          192.168.1.1          TELNET    240 Telnet Data ...
146 67.390668489  192.168.1.1          192.168.1.2          TCP        66 43604 → 23 [ACK] Seq=127 Ack=849 Win=245 Len=0 TSval=2783739 TSecr=2732448
147 68.412880144  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
148 69.436786463  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
149 70.461076426  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
150 70.461093315  192.168.1.2          192.168.1.1          TELNET    240 Telnet Data ...
151 70.461113388  192.168.1.1          192.168.1.2          TCP        66 43604 → 23 [ACK] Seq=127 Ack=1023 Win=254 Len=0 TSval=2784507 TSecr=2733216
152 70.711350841  CiscoInc_d2:3c:b2    CiscoInc_d2:3c:b2    LOOP       60 Reply
153 71.484903115  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
154 72.508729630  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
155 73.534632892  192.168.1.2          192.168.1.1          TELNET    299 Telnet Data ...
156 73.534657084  192.168.1.1          192.168.1.2          TCP        66 43604 → 23 [ACK] Seq=127 Ack=1256 Win=262 Len=0 TSval=2785275 TSecr=2733984
157 74.294011792  192.168.1.1          192.168.1.255        WHO       126 irs-OptiPlex-3040: 0,08 0,06 0,01
158 74.502343485  e4:be:ed:8c:1d:83    Broadcast            ARP        60 Who has 192.168.1.42? Tell 192.168.1.2
159 74.683689453  192.168.1.1          192.168.1.2          TELNET     67 Telnet Data
```

Pour la machine inatteignable 193.51.25.3, elle n'appartient pas au réseau. C'est la raison pour laquelle on voit des paquets ICMP transiter :

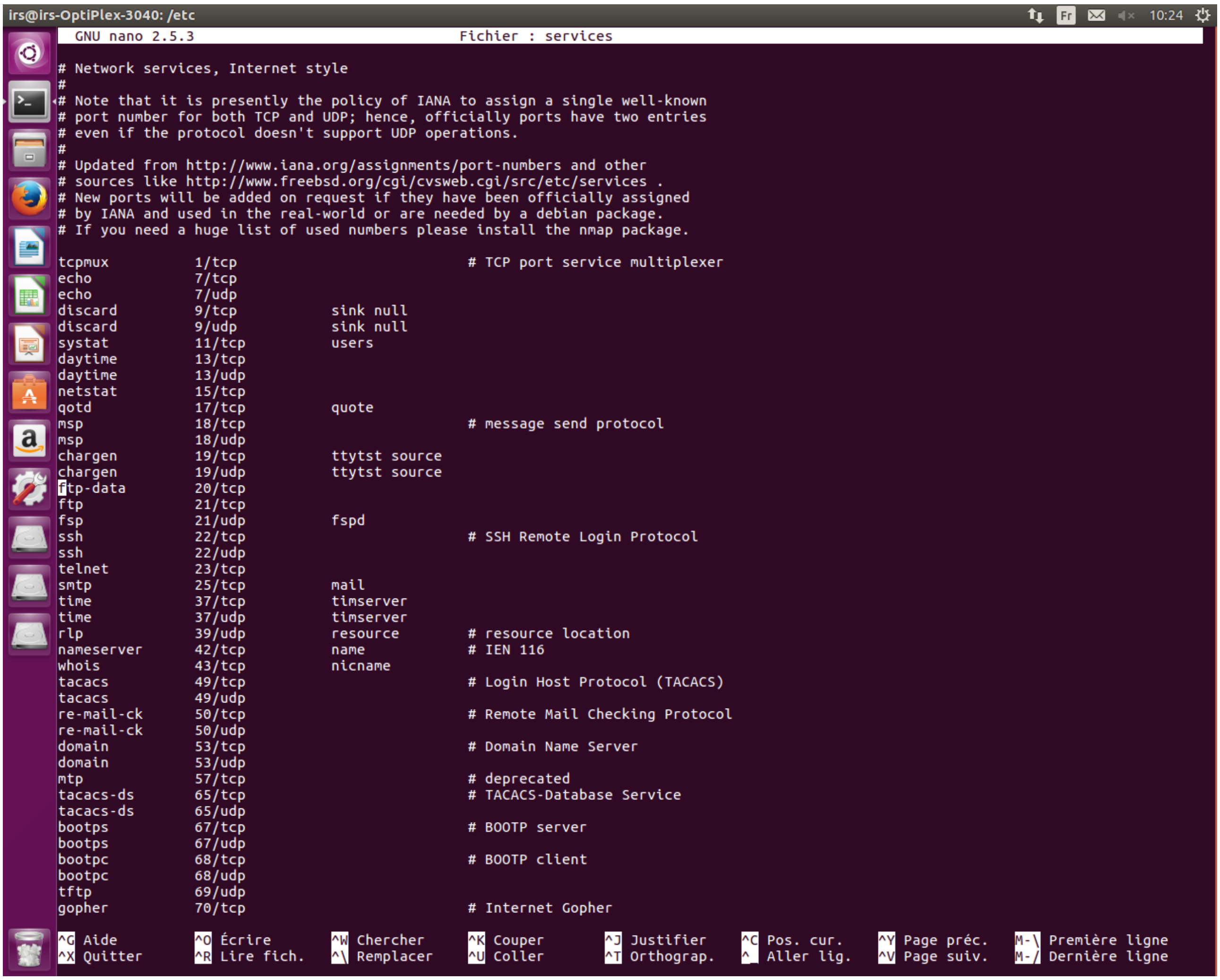


```
262 139.407294778 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
263 139.409552725 192.168.1.2         192.168.1.1         TELNET    126 Telnet Data ...
264 139.409581413 192.168.1.1         192.168.1.2         TCP        66 43604 → 23 [ACK] Seq=152 Ack=1950 Win=270 Len=0 TSval=2801744 TSecr=2750452
265 139.453335491 e4:be:ed:8c:1d:83   CiscoInc_d2:3c:b2   ARP        60 Who has 192.168.1.254? Tell 192.168.1.2
266 139.453889807 CiscoInc_d2:3c:b2   e4:be:ed:8c:1d:83   ARP        60 192.168.1.254 is at 58:bc:27:d2:3c:b2
267 140.256068259 CiscoInc_d2:3c:b2   CDP/VTP/DTP/PAgP/UD… CDP      359 Device ID: R4  Port ID: FastEthernet0/0
268 140.408012843 192.168.1.2         193.51.25.3         ICMP       98 Echo (ping) request  id=0x1470, seq=7/1792, ttl=64 (no response found!)
269 140.408841519 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
270 140.410904291 192.168.1.2         192.168.1.1         TELNET    126 Telnet Data ...
271 140.410931610 192.168.1.1         192.168.1.2         TCP        66 43604 → 23 [ACK] Seq=152 Ack=2010 Win=270 Len=0 TSval=2801995 TSecr=2750703
272 140.705968498 CiscoInc_d2:3c:b2   CiscoInc_d2:3c:b2   LOOP       60 Reply
273 141.409414222 192.168.1.2         193.51.25.3         ICMP       98 Echo (ping) request  id=0x1470, seq=8/2048, ttl=64 (no response found!)
274 141.410274606 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
275 141.412225795 192.168.1.2         192.168.1.1         TELNET    126 Telnet Data ...
276 141.412251809 192.168.1.1         192.168.1.2         TCP        66 43604 → 23 [ACK] Seq=152 Ack=2070 Win=270 Len=0 TSval=2802245 TSecr=2750953
277 142.411108519 192.168.1.2         193.51.25.3         ICMP       98 Echo (ping) request  id=0x1470, seq=9/2304, ttl=64 (no response found!)
278 142.411886838 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
279 142.413887354 192.168.1.2         192.168.1.1         TELNET    126 Telnet Data ...
280 142.413916031 192.168.1.1         192.168.1.2         TCP        66 43604 → 23 [ACK] Seq=152 Ack=2130 Win=270 Len=0 TSval=2802495 TSecr=2751203
281 143.412459570 192.168.1.2         193.51.25.3         ICMP       98 Echo (ping) request  id=0x1470, seq=10/2560, ttl=64 (no response found!)
282 143.413355648 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
283 143.415273514 192.168.1.2         192.168.1.1         TELNET    127 Telnet Data ...
284 143.415298531 192.168.1.1         192.168.1.2         TCP        66 43604 → 23 [ACK] Seq=152 Ack=2191 Win=270 Len=0 TSval=2802746 TSecr=2751454
285 144.413968622 192.168.1.2         193.51.25.3         ICMP       98 Echo (ping) request  id=0x1470, seq=11/2816, ttl=64 (no response found!)
286 144.414781643 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
287 144.416991174 192.168.1.2         192.168.1.1         TELNET    127 Telnet Data ...
288 144.417017946 192.168.1.1         192.168.1.2         TCP        66 43604 → 23 [ACK] Seq=152 Ack=2252 Win=270 Len=0 TSval=2802996 TSecr=2751704
289 145.415629841 192.168.1.2         193.51.25.3         ICMP       98 Echo (ping) request  id=0x1470, seq=12/3072, ttl=64 (no response found!)
290 145.416415210 192.168.1.254       192.168.1.2         ICMP       70 Destination unreachable (Host unreachable)
```

## Exercice 4



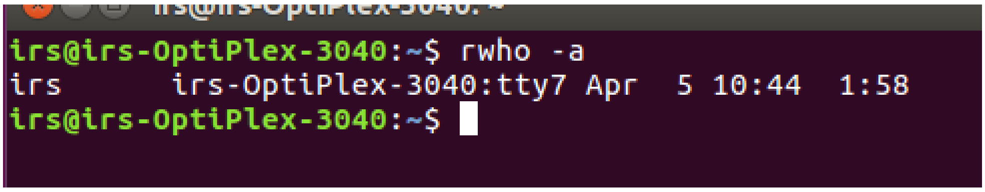
```
irs@irs-OptiPlex-3040:~$ netstat -an
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::25                   :::*                    LISTEN
udp        0      0 0.0.0.0:513             0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:42127           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp6       0      0 :::39506                :::*
udp6       0      0 :::5353                 :::*
```



```
  GNU nano 2.5.3                     Fichier : services

# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp
domain          53/tcp                          # Domain Name Server
domain          53/udp
mtp             57/tcp                          # deprecated
tacacs-ds       65/tcp                          # TACACS-Database Service
tacacs-ds       65/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher

^G Aide        ^O Écrire      ^W Chercher    ^K Couper      ^J Justifier   ^C Pos. cur.   ^Y Page préc.  M-\ Première ligne
^X Quitter     ^R Lire fich.  ^\ Remplacer   ^U Coller      ^T Orthograp.  ^_ Aller lig.  ^V Page suiv.  M-/ Dernière ligne
```

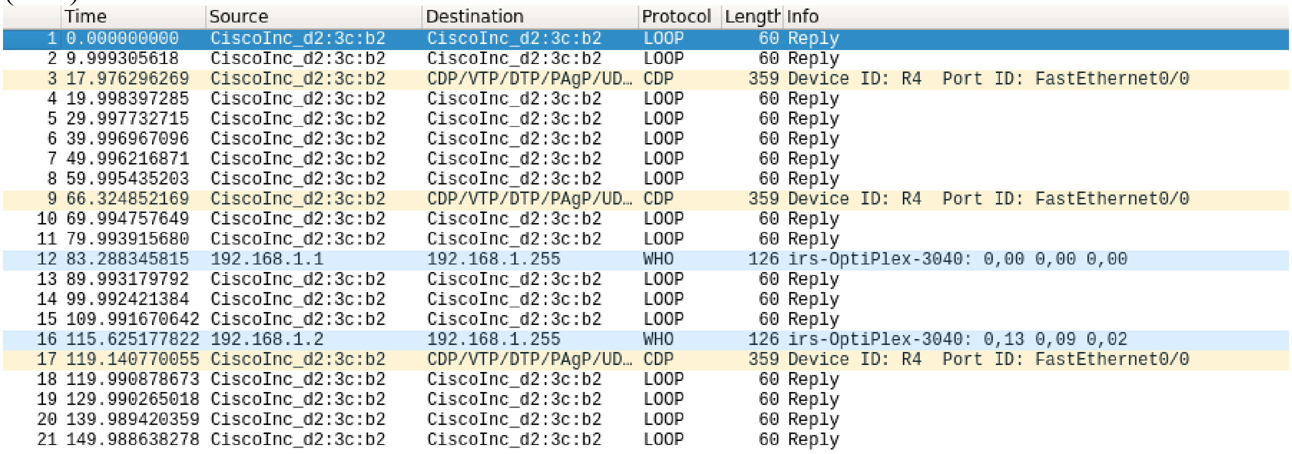
Les services TCP tournants sur nos machines sont les services 22, 23 et 25.
Le service 22 correspond au service ssh.
Le service 23 correspond au service telnet.
Le service 25 correspond au service smtp.

## Exercice 5



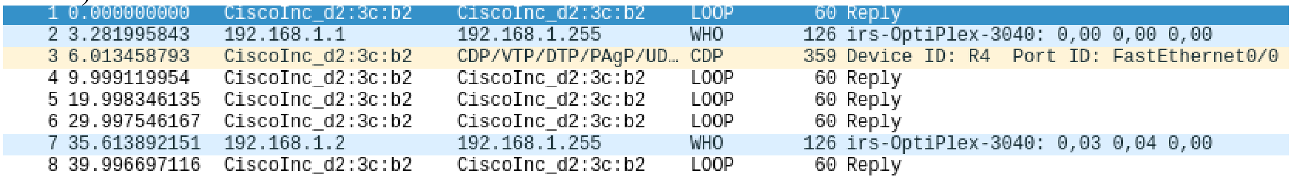
```
irs@irs-OptiPlex-3040:~$ rwho -a
irs      irs-OptiPlex-3040:tty7 Apr  5 10:44   1:58
irs@irs-OptiPlex-3040:~$ 
```

On démarre chacun wireshark et on peut voir le protocole WHO permettant de voir les hôtes sur le même réseau.
Sur le PC1, on voit que les machines de son réseau sont 192.168.1.1 (lui-même) et 192.168.1.2 (PC2) :



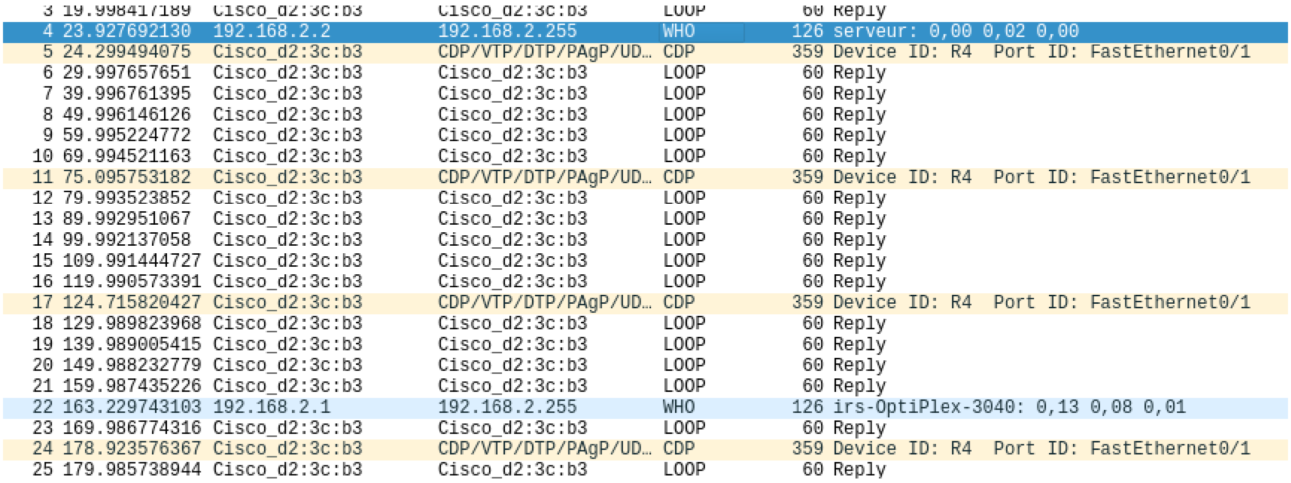
```
     Time          Source             Destination          Protocol Length Info
   1 0.000000000   CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   2 9.999305618   CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   3 17.976296269  CiscoInc_d2:3c:b2  CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/0
   4 19.998397285  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   5 29.997732715  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   6 39.996967096  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   7 49.996216871  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   8 59.995435203  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   9 66.324852169  CiscoInc_d2:3c:b2  CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/0
  10 69.994757649  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  11 79.993915680  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  12 83.288345815  192.168.1.1        192.168.1.255        WHO       126 irs-OptiPlex-3040: 0,00 0,00 0,00
  13 89.993179792  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  14 99.992421384  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  15 109.991670642 CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  16 115.625177822 192.168.1.2        192.168.1.255        WHO       126 irs-OptiPlex-3040: 0,13 0,09 0,02
  17 119.140770055 CiscoInc_d2:3c:b2  CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/0
  18 119.990878673 CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  19 129.990265018 CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  20 139.989420359 CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
  21 149.988638278 CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
```

Sur le PC2, on voit que les machines de son réseau sont 192.168.1.1 (PC1) et 192.168.1.2 (lui-même) :



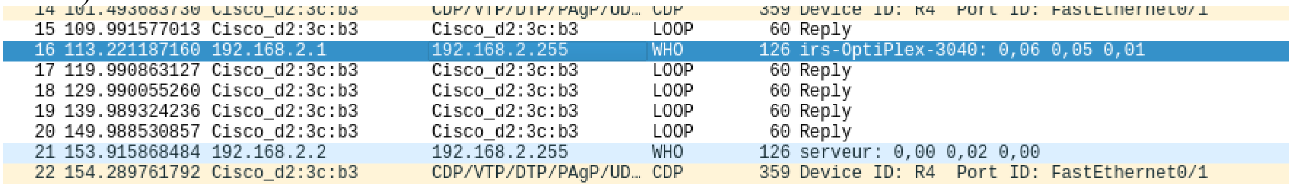
```
   1 0.000000000   CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   2 3.281995843   192.168.1.1        192.168.1.255        WHO       126 irs-OptiPlex-3040: 0,00 0,00 0,00
   3 6.013458793   CiscoInc_d2:3c:b2  CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/0
   4 9.999119954   CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   5 19.998346135  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   6 29.997546167  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
   7 35.613892151  192.168.1.2        192.168.1.255        WHO       126 irs-OptiPlex-3040: 0,03 0,04 0,00
   8 39.996697116  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2    LOOP       60 Reply
```

Sur le PC3, on voit que les machines de son réseau sont 192.168.2.1 (lui-même) et 192.168.2.2 (PC4) :



```
   3 19.998417189  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
   4 23.927692130  192.168.2.2        192.168.2.255        WHO       126 serveur: 0,00 0,02 0,00
   5 24.299494075  Cisco_d2:3c:b3     CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/1
   6 29.997657651  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
   7 39.996761395  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
   8 49.996146126  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
   9 59.995224772  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  10 69.994521163  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  11 75.095753182  Cisco_d2:3c:b3     CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/1
  12 79.993523852  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  13 89.992951067  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  14 99.992137058  Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  15 109.991444727 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  16 119.990573391 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  17 124.715820427 Cisco_d2:3c:b3     CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/1
  18 129.989823968 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  19 139.989005415 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  20 149.988232779 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  21 159.987435226 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  22 163.229743103 192.168.2.1        192.168.2.255        WHO       126 irs-OptiPlex-3040: 0,13 0,08 0,01
  23 169.986774316 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
  24 178.923576367 Cisco_d2:3c:b3     CDP/VTP/DTP/PAgP/UD… CDP       359 Device ID: R4  Port ID: FastEthernet0/1
  25 179.985738944 Cisco_d2:3c:b3     Cisco_d2:3c:b3       LOOP       60 Reply
```

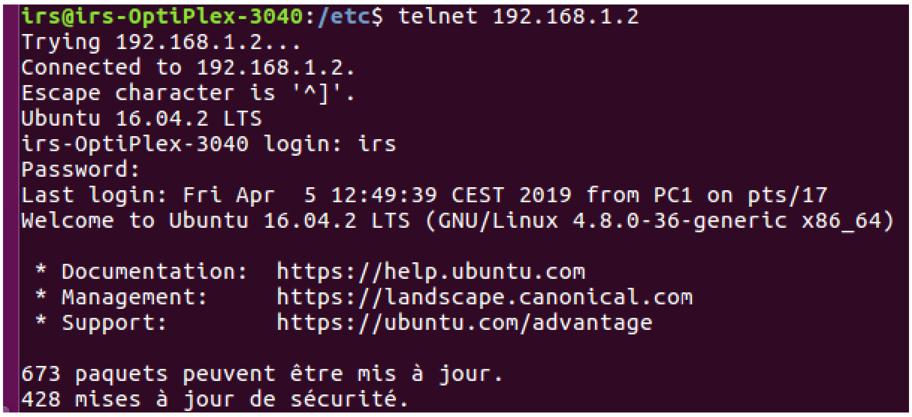
Sur le PC4, on voit que les machines de son réseau sont 192.168.2.1 (PC3) et 192.168.2.2 (lui-même) :



```
 14 101.493683730 Cisco_d2:3c:b3  CDP/VTP/DTP/PAgP/UD… CDP   359 Device ID: R4  Port ID: FastEthernet0/1
 15 109.991577013 Cisco_d2:3c:b3  Cisco_d2:3c:b3       LOOP   60 Reply
 16 113.221187160 192.168.2.1     192.168.2.255        WHO   126 irs-OptiPlex-3040: 0,06 0,05 0,01
 17 119.990863127 Cisco_d2:3c:b3  Cisco_d2:3c:b3       LOOP   60 Reply
 18 129.990055260 Cisco_d2:3c:b3  Cisco_d2:3c:b3       LOOP   60 Reply
 19 139.989324236 Cisco_d2:3c:b3  Cisco_d2:3c:b3       LOOP   60 Reply
 20 149.988530857 Cisco_d2:3c:b3  Cisco_d2:3c:b3       LOOP   60 Reply
 21 153.915868484 192.168.2.2     192.168.2.255        WHO   126 serveur: 0,00 0,02 0,00
 22 154.289761792 Cisco_d2:3c:b3  CDP/VTP/DTP/PAgP/UD… CDP   359 Device ID: R4  Port ID: FastEthernet0/1
```

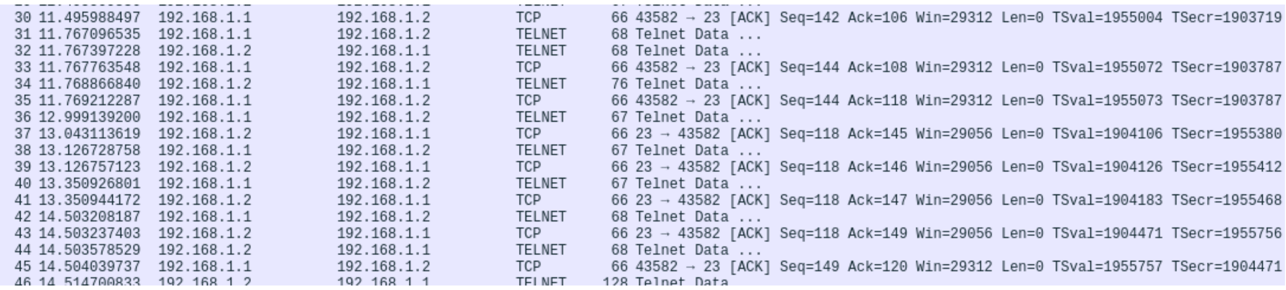
## Exercice 6

PC1/3 déclenche une session Telnet sur PC2/4 :

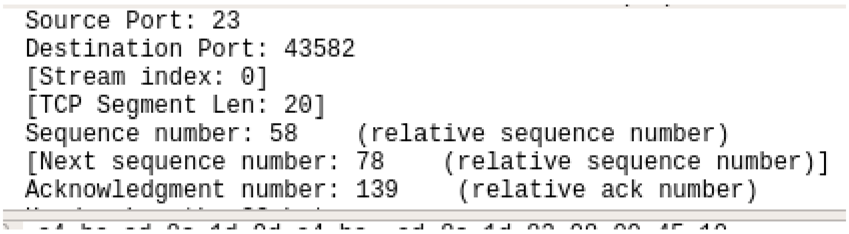


```
irs@irs-OptiPlex-3040:/etc$ telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
irs-OptiPlex-3040 login: irs
Password:
Last login: Fri Apr  5 12:49:39 CEST 2019 from PC1 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

673 paquets peuvent être mis à jour.
428 mises à jour de sécurité.
```

PC2/4 déclenche Wireshark et voit les trames TELNET et TCP (retour) :



```
30 11.495988497  192.168.1.1    192.168.1.2    TCP       66 43582 → 23 [ACK] Seq=142 Ack=106 Win=29312 Len=0 TSval=1955004 TSecr=1903719
31 11.767096535  192.168.1.1    192.168.1.2    TELNET    68 Telnet Data ...
32 11.767397228  192.168.1.2    192.168.1.1    TELNET    68 Telnet Data ...
33 11.767763548  192.168.1.1    192.168.1.2    TCP       66 43582 → 23 [ACK] Seq=144 Ack=108 Win=29312 Len=0 TSval=1955072 TSecr=1903787
34 11.768866840  192.168.1.2    192.168.1.1    TELNET    76 Telnet Data ...
35 11.769212287  192.168.1.1    192.168.1.2    TCP       66 43582 → 23 [ACK] Seq=144 Ack=118 Win=29312 Len=0 TSval=1955073 TSecr=1903787
36 12.999139200  192.168.1.1    192.168.1.2    TELNET    67 Telnet Data ...
37 13.043113619  192.168.1.2    192.168.1.1    TCP       66 23 → 43582 [ACK] Seq=118 Ack=145 Win=29056 Len=0 TSval=1904106 TSecr=1955380
38 13.126728758  192.168.1.1    192.168.1.2    TELNET    67 Telnet Data ...
39 13.126757123  192.168.1.2    192.168.1.1    TCP       66 23 → 43582 [ACK] Seq=118 Ack=146 Win=29056 Len=0 TSval=1904126 TSecr=1955412
40 13.350926801  192.168.1.1    192.168.1.2    TELNET    67 Telnet Data ...
41 13.350944172  192.168.1.2    192.168.1.1    TCP       66 23 → 43582 [ACK] Seq=118 Ack=147 Win=29056 Len=0 TSval=1904183 TSecr=1955468
42 14.503208187  192.168.1.1    192.168.1.2    TELNET    68 Telnet Data ...
43 14.503237403  192.168.1.2    192.168.1.1    TCP       66 23 → 43582 [ACK] Seq=118 Ack=149 Win=29056 Len=0 TSval=1904471 TSecr=1955756
44 14.503578529  192.168.1.2    192.168.1.1    TELNET    68 Telnet Data ...
45 14.504039737  192.168.1.1    192.168.1.2    TCP       66 43582 → 23 [ACK] Seq=149 Ack=120 Win=29312 Len=0 TSval=1955757 TSecr=1904471
46 14.514700833  192.168.1.2    192.168.1.1    TELNET   128 Telnet Data
```

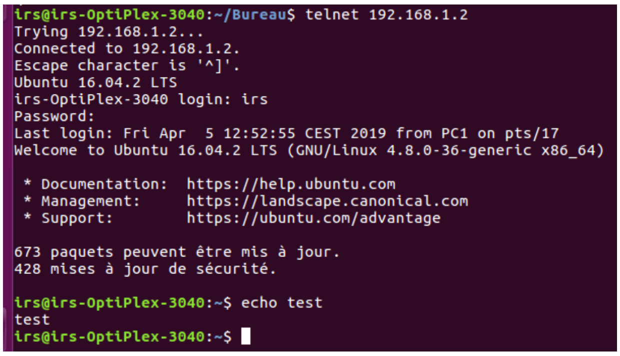


```
Source Port: 23
Destination Port: 43582
[Stream index: 0]
[TCP Segment Len: 20]
Sequence number: 58    (relative sequence number)
[Next sequence number: 78    (relative sequence number)]
Acknowledgment number: 139    (relative ack number)
```

On remarque que le port utilisé est le port 23 (source) et le port 43582 (pour la destination).

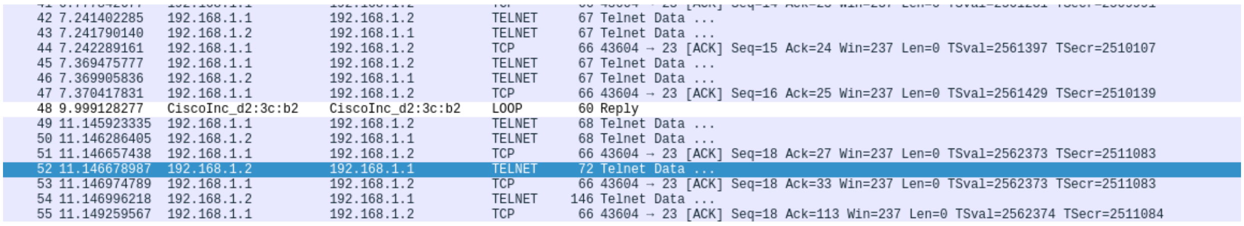
## Exercice 7

1) - Le PC1 déclenche une session telnet sur PC2 et fait « echo test ».



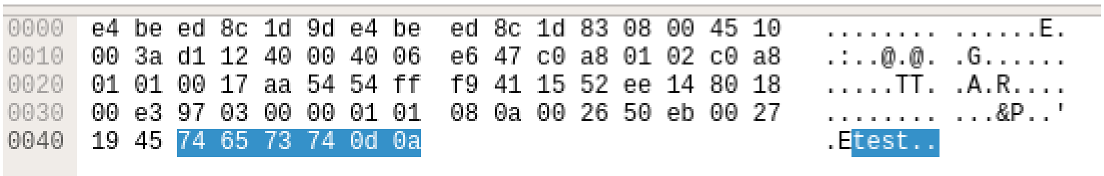
```
irs@irs-OptiPlex-3040:~/Bureau$ telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
irs-OptiPlex-3040 login: irs
Password:
Last login: Fri Apr  5 12:52:55 CEST 2019 from PC1 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

673 paquets peuvent être mis à jour.
428 mises à jour de sécurité.

irs@irs-OptiPlex-3040:~$ echo test
test
irs@irs-OptiPlex-3040:~$
```

PC2 voit sur Wireshark les trames TELNET :



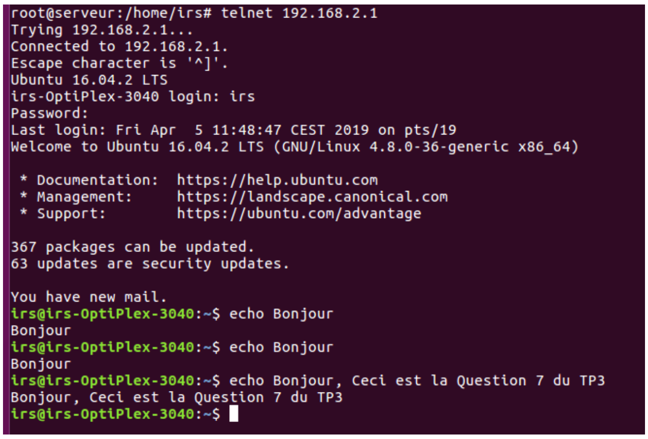
```
42 7.241402285   192.168.1.1       192.168.1.2       TELNET    67 Telnet Data ...
43 7.241790140   192.168.1.2       192.168.1.1       TELNET    67 Telnet Data ...
44 7.242289161   192.168.1.1       192.168.1.2       TCP       66 43604 → 23 [ACK] Seq=15 Ack=24 Win=237 Len=0 TSval=2561397 TSecr=2510107
45 7.369475777   192.168.1.1       192.168.1.2       TELNET    67 Telnet Data ...
46 7.369905836   192.168.1.2       192.168.1.1       TELNET    67 Telnet Data ...
47 7.370417831   192.168.1.1       192.168.1.2       TCP       66 43604 → 23 [ACK] Seq=16 Ack=25 Win=237 Len=0 TSval=2561429 TSecr=2510139
48 9.999128277   CiscoInc_d2:3c:b2 CiscoInc_d2:3c:b2 LOOP      60 Reply
49 11.145923335  192.168.1.1       192.168.1.2       TELNET    68 Telnet Data ...
50 11.146286405  192.168.1.2       192.168.1.1       TELNET    68 Telnet Data ...
51 11.146657438  192.168.1.1       192.168.1.2       TCP       66 43604 → 23 [ACK] Seq=18 Ack=27 Win=237 Len=0 TSval=2562373 TSecr=2511083
52 11.146678987  192.168.1.2       192.168.1.1       TELNET    72 Telnet Data ...
53 11.146974789  192.168.1.1       192.168.1.2       TCP       66 43604 → 23 [ACK] Seq=18 Ack=33 Win=237 Len=0 TSval=2562373 TSecr=2511083
54 11.146996218  192.168.1.2       192.168.1.1       TELNET   146 Telnet Data ...
55 11.149259567  192.168.1.1       192.168.1.2       TCP       66 43604 → 23 [ACK] Seq=18 Ack=113 Win=237 Len=0 TSval=2562374 TSecr=2511084
```

On peut voir sur la trame en surbrillance le détail de la trame dans la partie DATA :



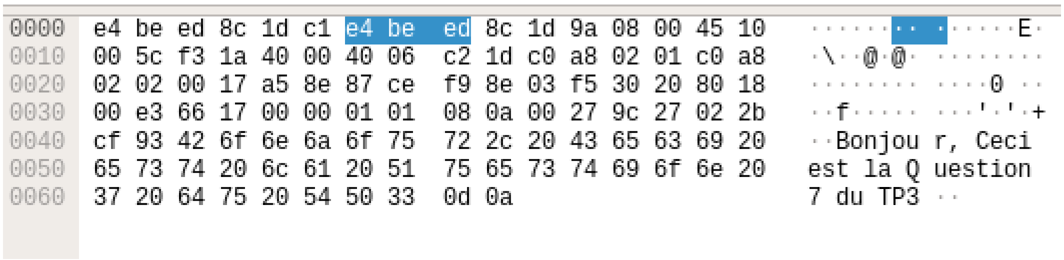
```
0000  e4 be ed 8c 1d 9d e4 be  ed 8c 1d 83 08 00 45 10   ........ ......E.
0010  00 3a d1 12 40 00 40 06  e6 47 c0 a8 01 02 c0 a8   .:..@.@. .G......
0020  01 01 00 17 aa 54 54 ff  f9 41 15 52 ee 14 80 18   .....TT. .A.R....
0030  00 e3 97 03 00 00 01 01  08 0a 00 26 50 eb 00 27   ........ ...&P..'
0040  19 45 74 65 73 74 0d 0a                            .Etest..
```

- On fait de même pour le PC4 qui fait :



```
root@serveur:/home/irs# telnet 192.168.2.1
Trying 192.168.2.1...
Connected to 192.168.2.1.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
irs-OptiPlex-3040 login: irs
Password:
Last login: Fri Apr  5 11:48:47 CEST 2019 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

367 packages can be updated.
63 updates are security updates.

You have new mail.
irs@irs-OptiPlex-3040:~$ echo Bonjour
Bonjour
irs@irs-OptiPlex-3040:~$ echo Bonjour
Bonjour
irs@irs-OptiPlex-3040:~$ echo Bonjour, Ceci est la Question 7 du TP3
Bonjour, Ceci est la Question 7 du TP3
irs@irs-OptiPlex-3040:~$
```

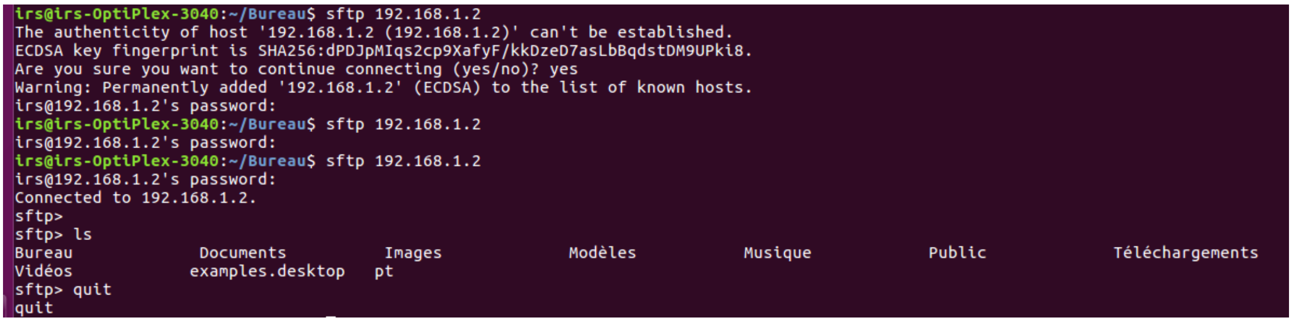
Le PC3 observe sur Wireshark et obtient une trame :



```
0000  e4 be ed 8c 1d c1 e4 be  ed 8c 1d 9a 08 00 45 10   ········ ······E·
0010  00 5c f3 1a 40 00 40 06  c2 1d c0 a8 02 01 c0 a8   ·\··@·@· ········
0020  02 02 00 17 a5 8e 87 ce  f9 8e 03 f5 30 20 80 18   ········ ····0 ··
0030  00 e3 66 17 00 00 01 01  08 0a 00 27 9c 27 02 2b   ··f····· ···'·'·+
0040  cf 93 42 6f 6e 6a 6f 75  72 2c 20 43 65 63 69 20   ··Bonjou r, Ceci
0050  65 73 74 20 6c 61 20 51  75 65 73 74 69 6f 6e 20   est la Q uestion
0060  37 20 64 75 20 54 50 33  0d 0a                     7 du TP3 ··
```

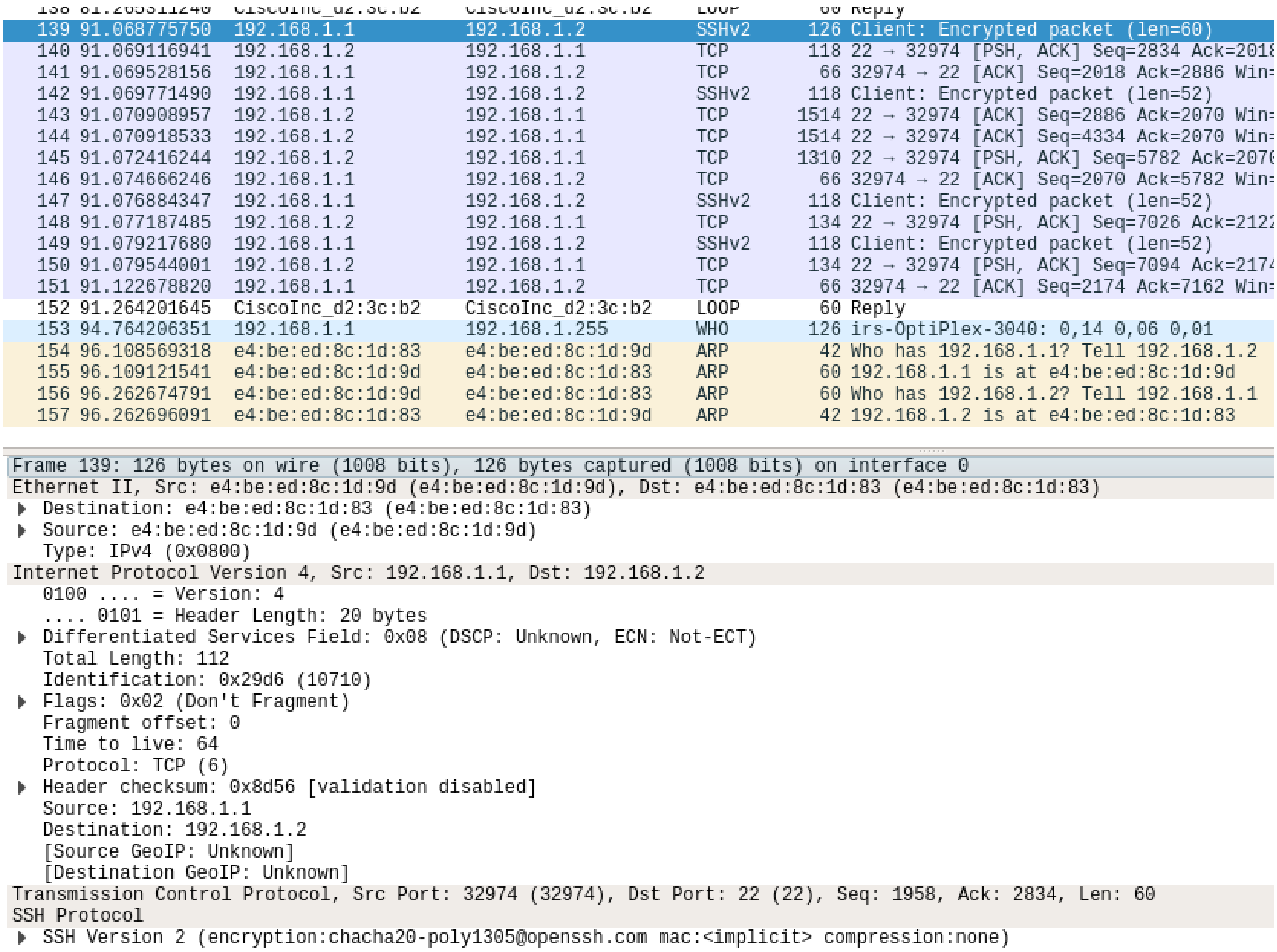
On remarque que les données ne sont pas chiffrées.

2) Pour FTP, PC1 se connecte à PC2 :



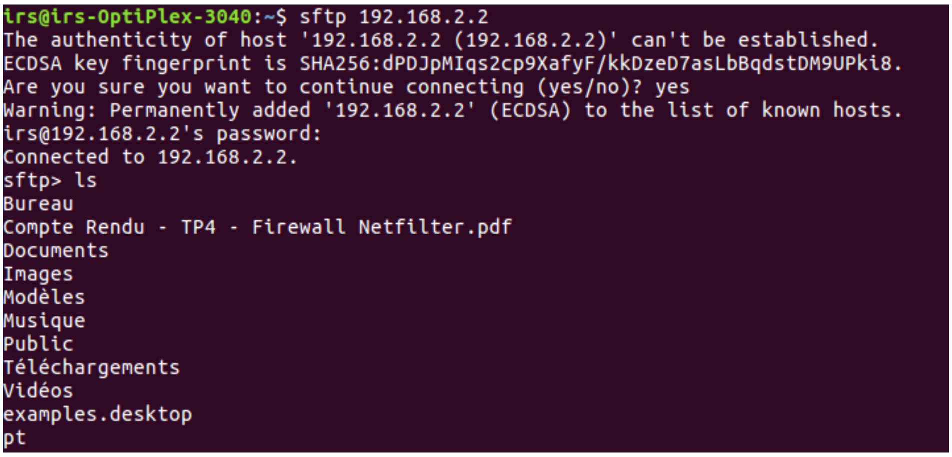
```
irs@irs-OptiPlex-3040:~/Bureau$ sftp 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
ECDSA key fingerprint is SHA256:dPDJpMIqs2cp9XafyF/kkDzeD7asLbBqdstDM9UPki8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.2' (ECDSA) to the list of known hosts.
irs@192.168.1.2's password:
irs@irs-OptiPlex-3040:~/Bureau$ sftp 192.168.1.2
irs@192.168.1.2's password:
irs@irs-OptiPlex-3040:~/Bureau$ sftp 192.168.1.2
irs@192.168.1.2's password:
Connected to 192.168.1.2.
sftp>
sftp> ls
Bureau                  Documents               Images                  Modèles                 Musique                 Public                  Téléchargements
Vidéos                 examples.desktop        pt
sftp> quit
quit
```

Et on obtient des trames SSH/SSHv2 dont les données sont chiffrées.

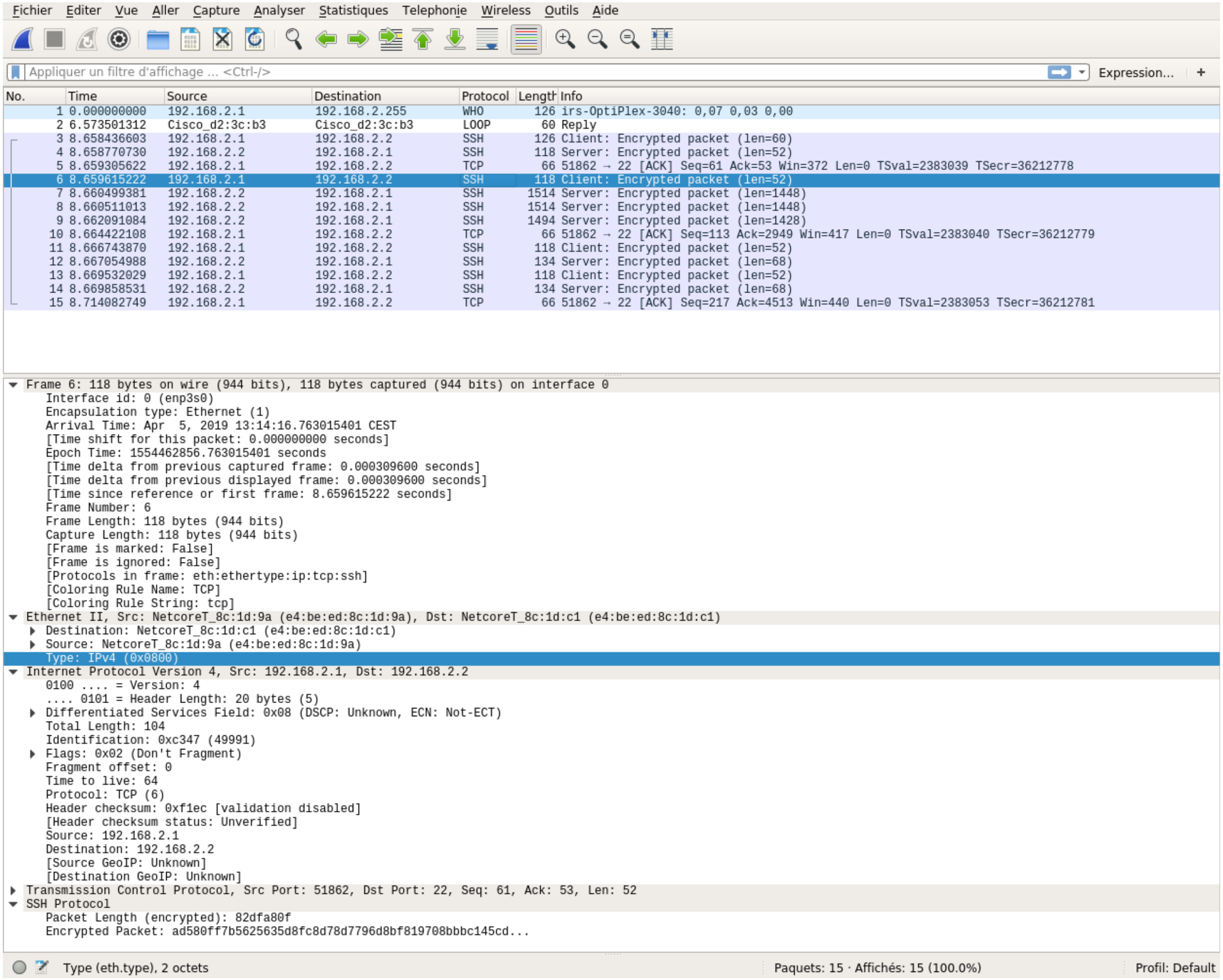


```
 138 81.205311240  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2  LOOP      60 Reply
 139 91.068775750  192.168.1.1        192.168.1.2        SSHv2    126 Client: Encrypted packet (len=60)
 140 91.069116941  192.168.1.2        192.168.1.1        TCP      118 22 → 32974 [PSH, ACK] Seq=2834 Ack=2018
 141 91.069528156  192.168.1.1        192.168.1.2        TCP       66 32974 → 22 [ACK] Seq=2018 Ack=2886 Win=
 142 91.069771490  192.168.1.1        192.168.1.2        SSHv2    118 Client: Encrypted packet (len=52)
 143 91.070908957  192.168.1.2        192.168.1.1        TCP     1514 22 → 32974 [ACK] Seq=2886 Ack=2070 Win=
 144 91.070918533  192.168.1.2        192.168.1.1        TCP     1514 22 → 32974 [ACK] Seq=4334 Ack=2070 Win=
 145 91.072416244  192.168.1.2        192.168.1.1        TCP     1310 22 → 32974 [PSH, ACK] Seq=5782 Ack=2070
 146 91.074666246  192.168.1.1        192.168.1.2        TCP       66 32974 → 22 [ACK] Seq=2070 Ack=5782 Win=
 147 91.076884347  192.168.1.1        192.168.1.2        SSHv2    118 Client: Encrypted packet (len=52)
 148 91.077187485  192.168.1.2        192.168.1.1        TCP      134 22 → 32974 [PSH, ACK] Seq=7026 Ack=2122
 149 91.079217680  192.168.1.1        192.168.1.2        SSHv2    118 Client: Encrypted packet (len=52)
 150 91.079544001  192.168.1.2        192.168.1.1        TCP      134 22 → 32974 [PSH, ACK] Seq=7094 Ack=2174
 151 91.122678820  192.168.1.1        192.168.1.2        TCP       66 32974 → 22 [ACK] Seq=2174 Ack=7162 Win=
 152 91.264201645  CiscoInc_d2:3c:b2  CiscoInc_d2:3c:b2  LOOP      60 Reply
 153 94.764206351  192.168.1.1        192.168.1.255      WHO      126 irs-OptiPlex-3040: 0,14 0,06 0,01
 154 96.108569318  e4:be:ed:8c:1d:83  e4:be:ed:8c:1d:9d  ARP       42 Who has 192.168.1.1? Tell 192.168.1.2
 155 96.109121541  e4:be:ed:8c:1d:9d  e4:be:ed:8c:1d:83  ARP       60 192.168.1.1 is at e4:be:ed:8c:1d:9d
 156 96.262674791  e4:be:ed:8c:1d:9d  e4:be:ed:8c:1d:83  ARP       60 Who has 192.168.1.2? Tell 192.168.1.1
 157 96.262696091  e4:be:ed:8c:1d:83  e4:be:ed:8c:1d:9d  ARP       42 192.168.1.2 is at e4:be:ed:8c:1d:83

Frame 139: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
Ethernet II, Src: e4:be:ed:8c:1d:9d (e4:be:ed:8c:1d:9d), Dst: e4:be:ed:8c:1d:83 (e4:be:ed:8c:1d:83)
 ▸ Destination: e4:be:ed:8c:1d:83 (e4:be:ed:8c:1d:83)
 ▸ Source: e4:be:ed:8c:1d:9d (e4:be:ed:8c:1d:9d)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes
 ▸ Differentiated Services Field: 0x08 (DSCP: Unknown, ECN: Not-ECT)
   Total Length: 112
   Identification: 0x29d6 (10710)
 ▸ Flags: 0x02 (Don't Fragment)
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (6)
 ▸ Header checksum: 0x8d56 [validation disabled]
   Source: 192.168.1.1
   Destination: 192.168.1.2
   [Source GeoIP: Unknown]
   [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 32974 (32974), Dst Port: 22 (22), Seq: 1958, Ack: 2834, Len: 60
SSH Protocol
 ▸ SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)
```

On fait de même entre PC3 et PC4 :



```
irs@irs-OptiPlex-3040:~$ sftp 192.168.2.2
The authenticity of host '192.168.2.2 (192.168.2.2)' can't be established.
ECDSA key fingerprint is SHA256:dPDJpMIqs2cp9XafyF/kkDzeD7asLbBqdstDM9UPki8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.2' (ECDSA) to the list of known hosts.
irs@192.168.2.2's password:
Connected to 192.168.2.2.
sftp> ls
Bureau
Compte Rendu - TP4 - Firewall Netfilter.pdf
Documents
Images
Modèles
Musique
Public
Téléchargements
Vidéos
examples.desktop
pt
```



```
No.      Time         Source            Destination       Protocol Length Info
       1 0.000000000  192.168.2.1       192.168.2.255     WHO       126 irs-OptiPlex-3040: 0,07 0,03 0,00
       2 6.573501312  Cisco_d2:3c:b3    Cisco_d2:3c:b3    LOOP       60 Reply
       3 8.658436603  192.168.2.1       192.168.2.2       SSH       126 Client: Encrypted packet (len=60)
       4 8.658770730  192.168.2.2       192.168.2.1       SSH       118 Server: Encrypted packet (len=52)
       5 8.659305622  192.168.2.1       192.168.2.2       TCP        66 51862 → 22 [ACK] Seq=61 Ack=53 Win=372 Len=0 TSval=2383039 TSecr=36212778
       6 8.659615222  192.168.2.1       192.168.2.2       SSH       118 Client: Encrypted packet (len=52)
       7 8.660499381  192.168.2.2       192.168.2.1       SSH      1514 Server: Encrypted packet (len=1448)
       8 8.660511013  192.168.2.2       192.168.2.1       SSH      1514 Server: Encrypted packet (len=1448)
       9 8.662091084  192.168.2.2       192.168.2.1       SSH      1494 Server: Encrypted packet (len=1428)
      10 8.664422108  192.168.2.1       192.168.2.2       TCP        66 51862 → 22 [ACK] Seq=113 Ack=2949 Win=417 Len=0 TSval=2383040 TSecr=36212779
      11 8.666743870  192.168.2.1       192.168.2.2       SSH       118 Client: Encrypted packet (len=52)
      12 8.667054988  192.168.2.2       192.168.2.1       SSH       134 Server: Encrypted packet (len=68)
      13 8.669532029  192.168.2.1       192.168.2.2       SSH       118 Client: Encrypted packet (len=52)
      14 8.669858531  192.168.2.2       192.168.2.1       SSH       134 Server: Encrypted packet (len=68)
      15 8.714082749  192.168.2.1       192.168.2.2       TCP        66 51862 → 22 [ACK] Seq=217 Ack=4513 Win=440 Len=0 TSval=2383053 TSecr=36212781
```

```
▼ Frame 6: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
     Interface id: 0 (enp3s0)
     Encapsulation type: Ethernet (1)
     Arrival Time: Apr  5, 2019 13:14:16.763015401 CEST
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1554462856.763015401 seconds
     [Time delta from previous captured frame: 0.000309600 seconds]
     [Time delta from previous displayed frame: 0.000309600 seconds]
     [Time since reference or first frame: 8.659615222 seconds]
     Frame Number: 6
     Frame Length: 118 bytes (944 bits)
     Capture Length: 118 bytes (944 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp:ssh]
     [Coloring Rule Name: TCP]
     [Coloring Rule String: tcp]
▼ Ethernet II, Src: NetcoreT_8c:1d:9a (e4:be:ed:8c:1d:9a), Dst: NetcoreT_8c:1d:c1 (e4:be:ed:8c:1d:c1)
   ▶ Destination: NetcoreT_8c:1d:c1 (e4:be:ed:8c:1d:c1)
   ▶ Source: NetcoreT_8c:1d:9a (e4:be:ed:8c:1d:9a)
     Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.2
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▶ Differentiated Services Field: 0x08 (DSCP: Unknown, ECN: Not-ECT)
     Total Length: 104
     Identification: 0xc347 (49991)
   ▶ Flags: 0x02 (Don't Fragment)
     Fragment offset: 0
     Time to live: 64
     Protocol: TCP (6)
     Header checksum: 0xf1ec [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.2.1
     Destination: 192.168.2.2
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▶ Transmission Control Protocol, Src Port: 51862, Dst Port: 22, Seq: 61, Ack: 53, Len: 52
▼ SSH Protocol
     Packet Length (encrypted): 82dfa80f
     Encrypted Packet: ad580ff7b5625635d8fc8d78d7796d8bf819708bbbc145cd...
```

```
Type (eth.type), 2 octets          Paquets: 15 · Affichés: 15 (100.0%)          Profil: Default
```