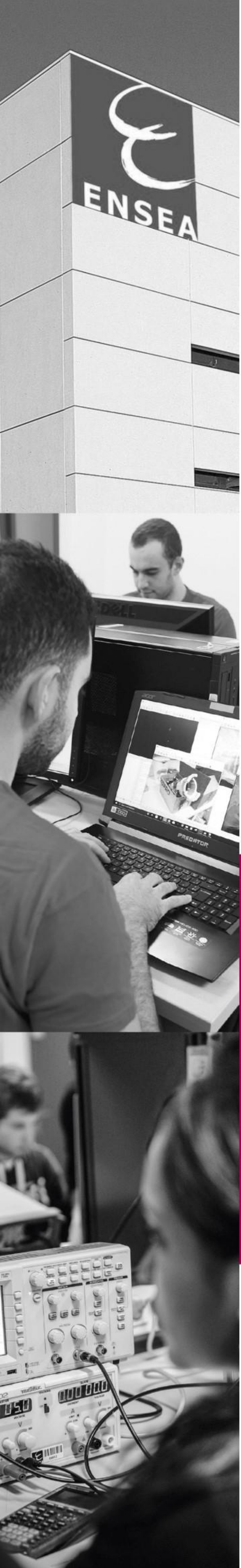
Document de travail



Architecture & Protocols

Lab 1

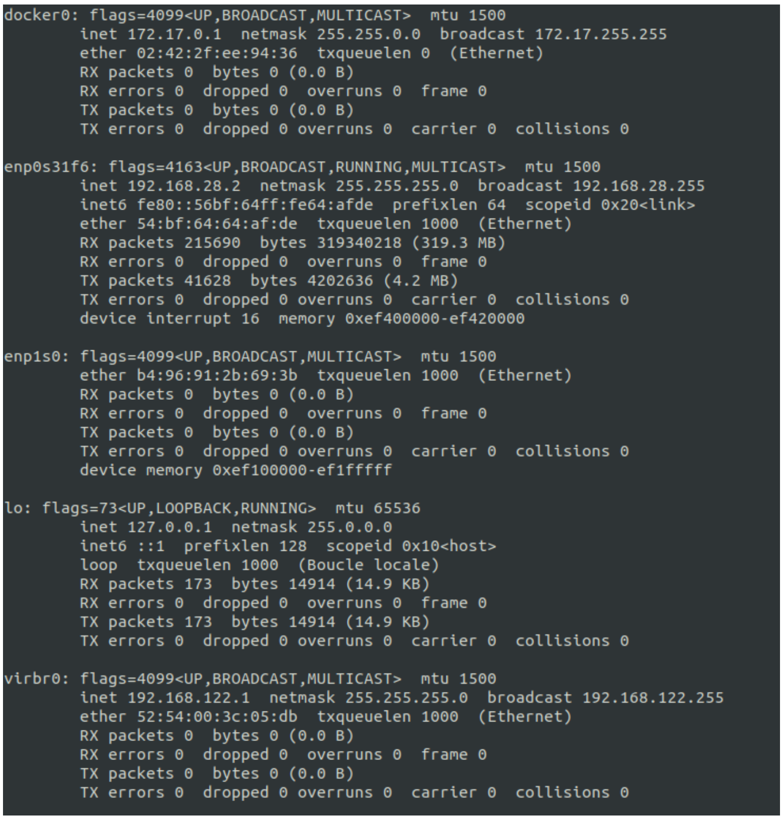
Report of the Lab

3ème année - RTS

PETIT Alexandre
Arthur LAUMY

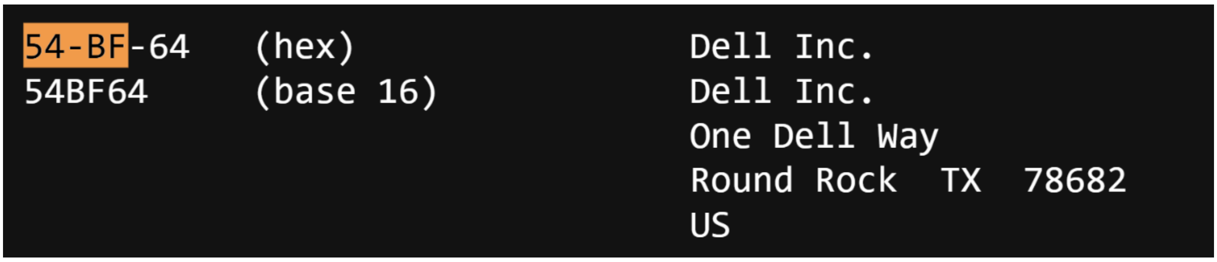
TP1 REPORT

I – Basic Commands



```
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:2f:ee:94:36  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.28.2  netmask 255.255.255.0  broadcast 192.168.28.255
        inet6 fe80::56bf:64ff:fe64:afde  prefixlen 64  scopeid 0x20<link>
        ether 54:bf:64:64:af:de  txqueuelen 1000  (Ethernet)
        RX packets 215690  bytes 319340218 (319.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41628  bytes 4202636 (4.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xef400000-ef420000

enp1s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b4:96:91:2b:69:3b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xef100000-ef1fffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Boucle locale)
        RX packets 173  bytes 14914 (14.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 173  bytes 14914 (14.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:3c:05:db  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

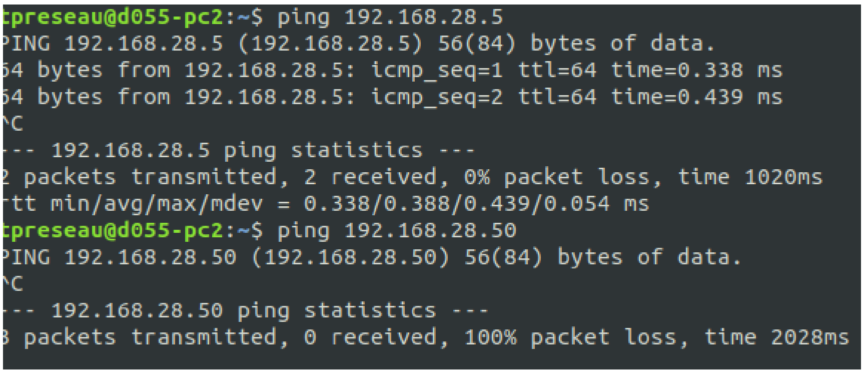
- Number of Interfaces: 5 (plus 2 which are desactivated). We have 3 physical interfaces in this computer: 2 ports Ethernet and one WIFI (wireless).
- We have two enpXsY interfaces and the information which describe them are:
  - Enp0s31f6:
    - Flags: UP/BROADCAST/RUNNING/MULTICAST
    - MTU=1500
    - Ether: 54:bf:64:64:af:de
    - Ipv4: 192.168.28.2
    - Ipv6: fe80: : 56bf: 64ff: fe64: afde
    - Netmask: 255.255.255.0
  - Enp1s0:
    - Flags: UP/BROADCAST/MULTICAST
    - MTU=1500
    - Ether: b4:96:91:2b:69:3b
- We find thanks to the database of OUI that the manufacturer of the network card



```
54-BF-64   (hex)             Dell Inc.
54BF64     (base 16)         Dell Inc.
                             One Dell Way
                             Round Rock  TX  78682
                             US
```

Figure 1 - Extract from the OUI Database

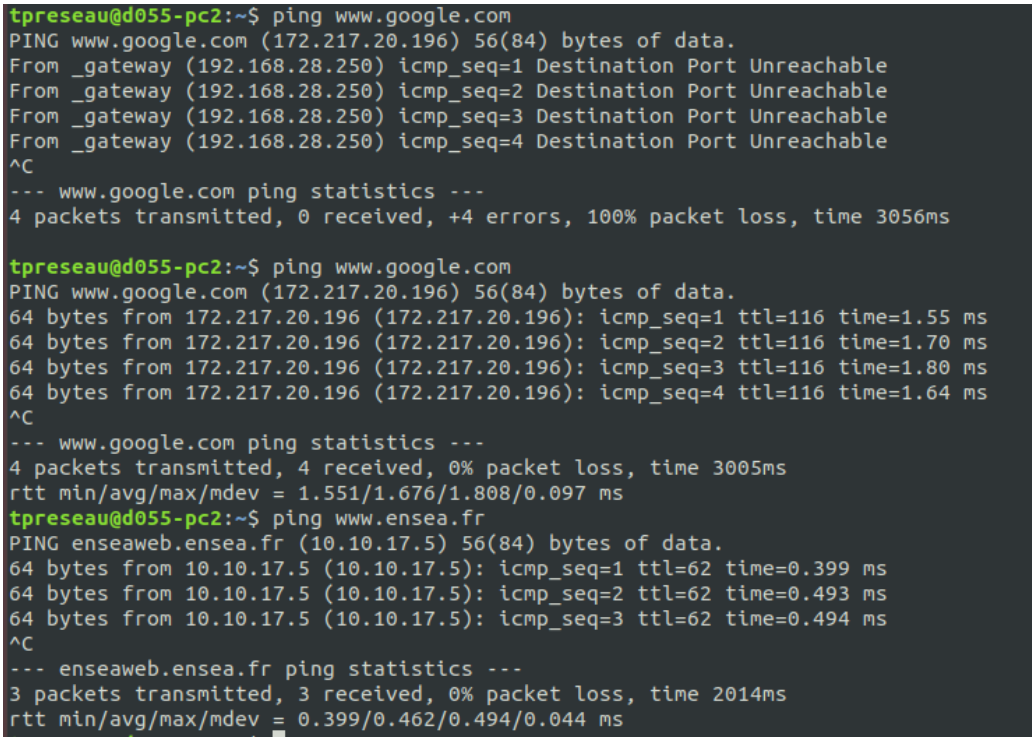
- IPv6 is compatible for the computer because we have this line: fe80: : 56bf: 64ff: fe64: afde and this is the IPv6 address.
- The Network mask is /24 (255.255.255.0), this is a Class C. The Address of the LAN is: 192.168.28.0
- We ping every computer in the room, and we observe that the time is very short because we are in the same LAN. We also try to ping an unattributed address, and we don't have any answer (with the 192.168.28.50 address).



```
tpreseau@d055-pc2:~$ ping 192.168.28.5
PING 192.168.28.5 (192.168.28.5) 56(84) bytes of data.
64 bytes from 192.168.28.5: icmp_seq=1 ttl=64 time=0.338 ms
64 bytes from 192.168.28.5: icmp_seq=2 ttl=64 time=0.439 ms
^C
--- 192.168.28.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.338/0.388/0.439/0.054 ms
tpreseau@d055-pc2:~$ ping 192.168.28.50
PING 192.168.28.50 (192.168.28.50) 56(84) bytes of data.
^C
--- 192.168.28.50 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2028ms
```

Figure 2 - Ping Different computers in the room

- Because the computer was not connected, the ping to www.google.com ended with a destination port unreachable. We observe that the time taken to respond to the ping is longer for google than for ENSEA because we go through many routers to reach google while we go through almost no other routers for ENSEA.



```
tpreseau@d055-pc2:~$ ping www.google.com
PING www.google.com (172.217.20.196) 56(84) bytes of data.
From _gateway (192.168.28.250) icmp_seq=1 Destination Port Unreachable
From _gateway (192.168.28.250) icmp_seq=2 Destination Port Unreachable
From _gateway (192.168.28.250) icmp_seq=3 Destination Port Unreachable
From _gateway (192.168.28.250) icmp_seq=4 Destination Port Unreachable
^C
--- www.google.com ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3056ms

tpreseau@d055-pc2:~$ ping www.google.com
PING www.google.com (172.217.20.196) 56(84) bytes of data.
64 bytes from 172.217.20.196 (172.217.20.196): icmp_seq=1 ttl=116 time=1.55 ms
64 bytes from 172.217.20.196 (172.217.20.196): icmp_seq=2 ttl=116 time=1.70 ms
64 bytes from 172.217.20.196 (172.217.20.196): icmp_seq=3 ttl=116 time=1.80 ms
64 bytes from 172.217.20.196 (172.217.20.196): icmp_seq=4 ttl=116 time=1.64 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.551/1.676/1.808/0.097 ms
tpreseau@d055-pc2:~$ ping www.ensea.fr
PING enseaweb.ensea.fr (10.10.17.5) 56(84) bytes of data.
64 bytes from 10.10.17.5 (10.10.17.5): icmp_seq=1 ttl=62 time=0.399 ms
64 bytes from 10.10.17.5 (10.10.17.5): icmp_seq=2 ttl=62 time=0.493 ms
64 bytes from 10.10.17.5 (10.10.17.5): icmp_seq=3 ttl=62 time=0.494 ms
^C
--- enseaweb.ensea.fr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.399/0.462/0.494/0.044 ms
```

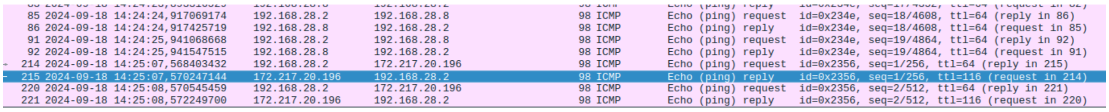
Figure 3 - Ping different websites

- TTL (Time To Live) varies based on the source of the packet. For example, packets sent from www.google.com have a TTL of 116, while those directed from www.ensea.fr have a TTL of 62, and packets from computers in the room typically have a default TTL of 64. As packets traverse routers, their TTL decreases. Therefore, it can be inferred that packets sent to **ensea.fr** pass through two routers before reaching their destination, while packets sent to **google.com** pass through twelve routers. This decrementing mechanism is essential for preventing packets from circulating indefinitely within the network.

II – Capture a Ping

A ping was performed on a computer in the room (with the IP address: 192.168.28.8), and it was observed through Wireshark that the protocol used is ICMP (Internet Control Message Protocol). A ping was indeed detected as there was a request and a response.

Additionally, there is a sequence in the seq part, indicating that the ping is being performed continuously. It was noted that we remain within the same network since the TTL does not decrease, meaning we do not pass through a router. The TTL starts at 64 and remains at 64.



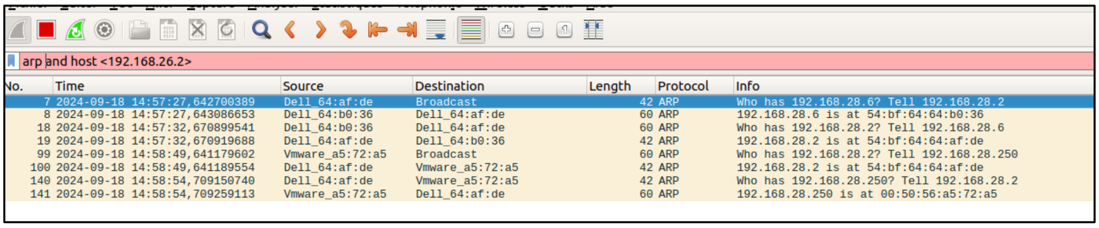
```
 85 2024-09-18 14:24:24,917069174   192.168.28.2     192.168.28.8       98 ICMP    Echo (ping) request  id=0x234e, seq=18/4608, ttl=64 (reply in 86)
 86 2024-09-18 14:24:24,917425719   192.168.28.8     192.168.28.2       98 ICMP    Echo (ping) reply    id=0x234e, seq=18/4608, ttl=64 (request in 85)
 91 2024-09-18 14:24:25,941068668   192.168.28.2     192.168.28.8       98 ICMP    Echo (ping) request  id=0x234e, seq=19/4864, ttl=64 (reply in 92)
 92 2024-09-18 14:24:25,941547515   192.168.28.8     192.168.28.2       98 ICMP    Echo (ping) reply    id=0x234e, seq=19/4864, ttl=64 (request in 91)
214 2024-09-18 14:25:07,568403432   192.168.28.2     172.217.20.196     98 ICMP    Echo (ping) request  id=0x2356, seq=1/256, ttl=64 (reply in 215)
215 2024-09-18 14:25:07,570247144   172.217.20.196   192.168.28.2       98 ICMP    Echo (ping) reply    id=0x2356, seq=1/256, ttl=116 (request in 214)
220 2024-09-18 14:25:08,570545459   192.168.28.2     172.217.20.196     98 ICMP    Echo (ping) request  id=0x2356, seq=2/512, ttl=64 (reply in 221)
221 2024-09-18 14:25:08,572249700   172.217.20.196   192.168.28.2       98 ICMP    Echo (ping) reply    id=0x2356, seq=2/512, ttl=116 (request in 220)
```

Figure 4 - Wireshark capture of a ping

On ping ensuite Google. On observe alors que son adresse IP est 172.217.20.196 et on observe également le ping avec la requete et la réponse. Le TTL est à 116 car on passe par Windows qui possède un TTL de 128. On observe alors que le ping est passé par 12 routeurs avant d'atteindre Google.

A ping was subsequently performed on Google. It was observed that its IP address is **172.217.20.196**, and the ping showed both a request and a response. The TTL was recorded at **116**, indicating that the packet passed through **12 routers** before reaching our computer (default could be 128).

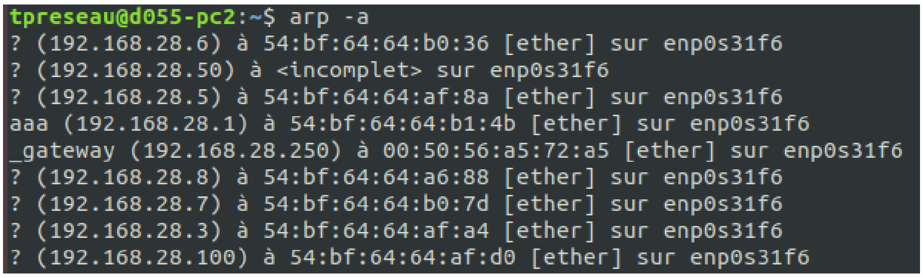
III – ARP Request Capture



arp and host <192.168.26.2>

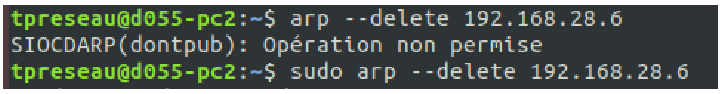
```
No.  Time                           Source             Destination        Length Protocol Info
  7 2024-09-18 14:57:27,642700389   Dell_64:af:de      Broadcast              42 ARP      Who has 192.168.28.6? Tell 192.168.28.2
  8 2024-09-18 14:57:27,643086653   Dell_64:b0:36      Dell_64:af:de          60 ARP      192.168.28.6 is at 54:bf:64:64:b0:36
 18 2024-09-18 14:57:32,670899541   Dell_64:b0:36      Dell_64:af:de          60 ARP      Who has 192.168.28.2? Tell 192.168.28.6
 19 2024-09-18 14:57:32,670919688   Dell_64:af:de      Dell_64:b0:36          42 ARP      192.168.28.2 is at 54:bf:64:64:af:de
 99 2024-09-18 14:58:49,641179602   Vmware_a5:72:a5    Broadcast              60 ARP      Who has 192.168.28.2? Tell 192.168.28.250
100 2024-09-18 14:58:49,641189554   Dell_64:af:de      Vmware_a5:72:a5        42 ARP      192.168.28.2 is at 54:bf:64:64:af:de
140 2024-09-18 14:58:54,709150740   Dell_64:af:de      Vmware_a5:72:a5        42 ARP      Who has 192.168.28.250? Tell 192.168.28.2
141 2024-09-18 14:58:54,709259113   Vmware_a5:72:a5    Dell_64:af:de          60 ARP      192.168.28.250 is at 00:50:56:a5:72:a5
```

Figure 5 - Wireshark capture of an ARP request



```
tpreseau@d055-pc2:~$ arp -a
? (192.168.28.6) à 54:bf:64:64:b0:36 [ether] sur enp0s31f6
? (192.168.28.50) à <incomplet> sur enp0s31f6
? (192.168.28.5) à 54:bf:64:64:af:8a [ether] sur enp0s31f6
aaa (192.168.28.1) à 54:bf:64:64:b1:4b [ether] sur enp0s31f6
_gateway (192.168.28.250) à 00:50:56:a5:72:a5 [ether] sur enp0s31f6
? (192.168.28.8) à 54:bf:64:64:a6:88 [ether] sur enp0s31f6
? (192.168.28.7) à 54:bf:64:64:b0:7d [ether] sur enp0s31f6
? (192.168.28.3) à 54:bf:64:64:af:a4 [ether] sur enp0s31f6
? (192.168.28.100) à 54:bf:64:64:af:d0 [ether] sur enp0s31f6
```

Figure 6 - ARP Table

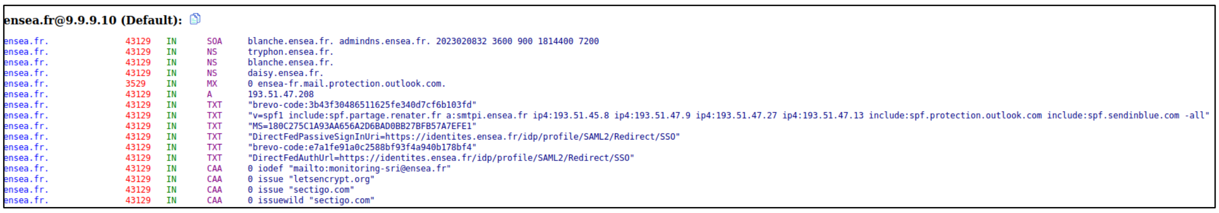


```
tpreseau@d055-pc2:~$ arp --delete 192.168.28.6
SIOCDARP(dontpub): Opération non permise
tpreseau@d055-pc2:~$ sudo arp --delete 192.168.28.6
```

Figure 7 - Delete command

We deleted the line in the ARP table of our computer of 192.168.28.6. Next, we sent a ping and these lines appeared in the capture. The first line is a packet sent to everyone to know who is the IP. The second line is the response from the computer who give back a MAC address so it can be noted in the ARP Table of our computer.

IV – DNS Query Capture



ensea.fr@9.9.9.10 (Default):

```
ensea.fr.          43129   IN      SOA     blanche.ensea.fr. admindns.ensea.fr. 2023020832 3600 900 1814400 7200
ensea.fr.          43129   IN      NS      tryphon.ensea.fr.
ensea.fr.          43129   IN      NS      blanche.ensea.fr.
ensea.fr.          43129   IN      NS      daisy.ensea.fr.
ensea.fr.          3529    IN      MX      0 ensea-fr.mail.protection.outlook.com.
ensea.fr.          43129   IN      A       193.51.47.208
ensea.fr.          43129   IN      TXT     "brevo-code:3b43f30486511625fe340d7cf6b103fd"
ensea.fr.          43129   IN      TXT     "v=spf1 include:spf.partage.renater.fr a:smtpi.ensea.fr ip4:193.51.45.8 ip4:193.51.47.9 ip4:193.51.47.27 ip4:193.51.47.13 include:spf.protection.outlook.com include:spf.sendinblue.com -all"
ensea.fr.          43129   IN      TXT     "MS=180C275C1A93AA656A2D6BAD0BB27BFB57A7EFE1"
ensea.fr.          43129   IN      TXT     "DirectFedPassiveSignInUri=https://identites.ensea.fr/idp/profile/SAML2/Redirect/SSO"
ensea.fr.          43129   IN      TXT     "brevo-code:e7a1fe91a0c2588bf93f4a940b178bf4"
ensea.fr.          43129   IN      TXT     "DirectFedAuthUrl=https://identites.ensea.fr/idp/profile/SAML2/Redirect/SSO"
ensea.fr.          43129   IN      CAA     0 iodef "mailto:monitoring-sri@ensea.fr"
ensea.fr.          43129   IN      CAA     0 issue "letsencrypt.org"
ensea.fr.          43129   IN      CAA     0 issue "sectigo.com"
ensea.fr.          43129   IN      CAA     0 issuewild "sectigo.com"
```

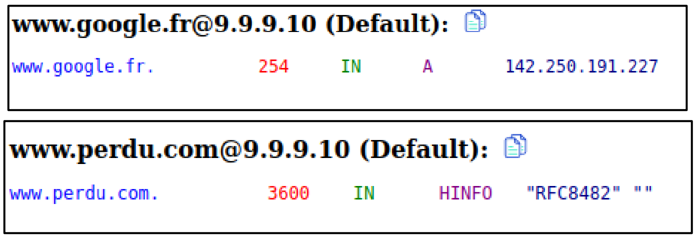
Figure 8 - Dig command

Using the command dig and the website digwebinterface.com, we found the following servers for the ENSEA:

- Blanche
- Tryphon
- Daisy
- Outlook Protection Server for the mails

We can also define:

- A: used for IPv4
- AAAA: Used for IPv6
- MX: Mails
- NS: Name Servers. These servers are responsible for answering to DNS requests.
- SOA: Start of Authority



www.google.fr@9.9.9.10 (Default):

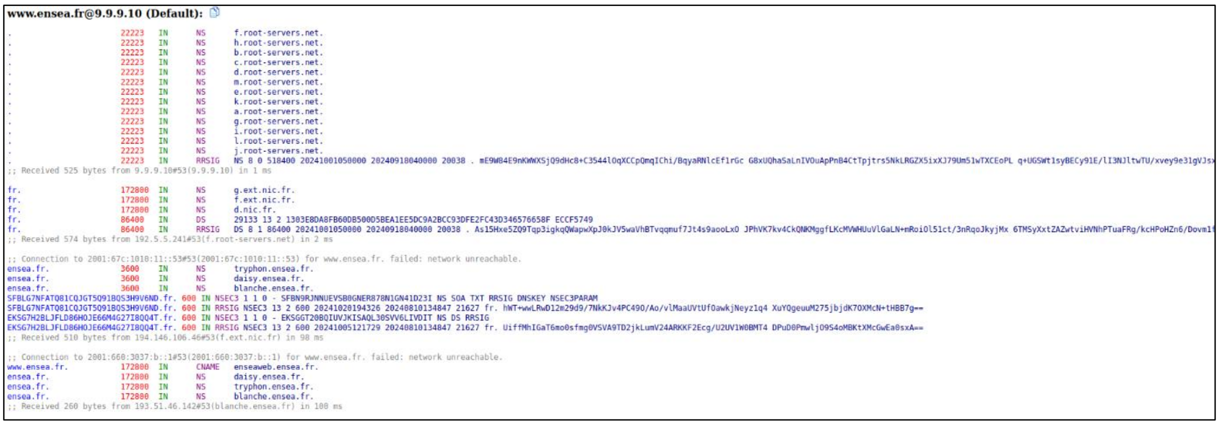
```
www.google.fr.          254     IN      A       142.250.191.227
```

www.perdu.com@9.9.9.10 (Default):

```
www.perdu.com.          3600    IN      HINFO   "RFC8482" ""
```

Figure 9 - Searching web server IP

If we tap the IP 142.250.191.227 in a browser, we can access directly to google.fr.



www.ensea.fr@9.9.9.10 (Default):

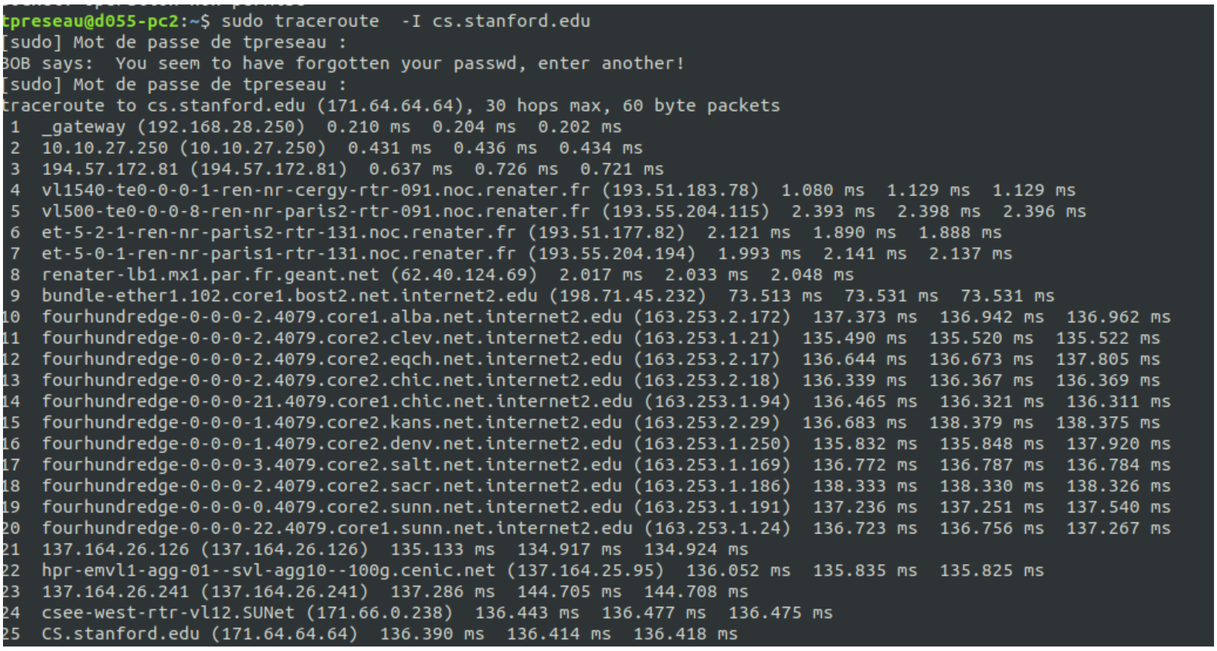
```
.                       22223   IN      NS      f.root-servers.net.
.                       22223   IN      NS      h.root-servers.net.
.                       22223   IN      NS      b.root-servers.net.
.                       22223   IN      NS      c.root-servers.net.
.                       22223   IN      NS      d.root-servers.net.
.                       22223   IN      NS      m.root-servers.net.
.                       22223   IN      NS      e.root-servers.net.
.                       22223   IN      NS      k.root-servers.net.
.                       22223   IN      NS      a.root-servers.net.
.                       22223   IN      NS      g.root-servers.net.
.                       22223   IN      NS      i.root-servers.net.
.                       22223   IN      NS      l.root-servers.net.
.                       22223   IN      NS      j.root-servers.net.
.                       22223   IN      RRSIG   NS 8 0 518400 20241001050000 20240918040000 20038 . mE9W84E9nKWWXSjQ9dHc8+C3544lOqXCCpQmqIChi/BqyaRNlcEf1rGc G8xUQhaSaLnIVOuApPnB4CtTpjtrs5NkLRGZX5ixXJ79Um5lwTXCEoPL q+UGSWt1syBECy91E/lI3NJltwTU/xvey9e31gVJsx
;; Received 525 bytes from 9.9.9.10#53(9.9.9.10) in 1 ms

fr.                     172800  IN      NS      g.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      d.nic.fr.
fr.                     86400   IN      DS      29133 13 2 1303E8DA8FB60DB500D5BEA1EE5DC9A2BCC93DFE2FC43D346576658F ECCF5749
fr.                     86400   IN      RRSIG   DS 8 1 86400 20241001050000 20240918040000 20038 . As15Hxe5ZQ9Tqp3igkqQWapwXpJ0kJV5waVhBTvqqmuf7Jt4s9aooLx0 JPhVK7kv4CkQNKMggfLKcMVWHUuVlGaLN+mRoiOl51ct/3nRqoJkyjMx 6TMSyXxtZAZwtviHVNhPTuaFRg/kcHPoHZn6/Dovm1f
;; Received 574 bytes from 192.5.5.241#53(f.root-servers.net) in 2 ms

;; Connection to 2001:67c:1010:11::53#53(2001:67c:1010:11::53) for www.ensea.fr. failed: network unreachable.
ensea.fr.               3600    IN      NS      tryphon.ensea.fr.
ensea.fr.               3600    IN      NS      daisy.ensea.fr.
ensea.fr.               3600    IN      NS      blanche.ensea.fr.
SFBLG7NFATQ81CQJGT5Q91BQS3H9V6ND.fr. 600 IN NSEC3 1 1 0 - SFBN9RJNNUEVSB0GNER878N1GN41D23I NS SOA TXT RRSIG DNSKEY NSEC3PARAM
SFBLG7NFATQ81CQJGT5Q91BQS3H9V6ND.fr. 600 IN RRSIG NSEC3 13 2 600 20241020194326 20240810134847 21627 fr. hWT+wwLRwD12m29d9/7NkKJv4PC490/Ao/vlMaaUVtUf0awkjNeyz1q4 XuYQgeuuM275jbjdK70XMcN+tHBB7g==
EKSG7H2BLJFLD86HOJE66M4G27I8QQ4T.fr. 600 IN NSEC3 1 1 0 - EKSGGT20BQIUVJKISAQL30SVV6LIVDIT NS DS RRSIG
EKSG7H2BLJFLD86HOJE66M4G27I8QQ4T.fr. 600 IN RRSIG NSEC3 13 2 600 20241005121729 20240810134847 21627 fr. UiffMhIGaT6mo0sfmg0VSVA9TD2jkLumV24ARKKF2Ecg/U2UV1W0BMT4 DPuD0PmwljO9S4oMBKtXMcGwEa0sxA==
;; Received 510 bytes from 194.146.106.46#53(f.ext.nic.fr) in 98 ms

;; Connection to 2001:660:3037:b::1#53(2001:660:3037:b::1) for www.ensea.fr. failed: network unreachable.
www.ensea.fr.           172800  IN      CNAME   enseaweb.ensea.fr.
ensea.fr.               172800  IN      NS      daisy.ensea.fr.
ensea.fr.               172800  IN      NS      tryphon.ensea.fr.
ensea.fr.               172800  IN      NS      blanche.ensea.fr.
;; Received 260 bytes from 193.51.46.142#53(blanche.ensea.fr) in 100 ms
```

Figure 10 - Dig with trace option

With the trace option, we can see the path along all the DNS root servers, where our request is processed. In a first place, the request is handled by a root-servers.net (in this example, g,f or d) and after it's redirected to Names Servers of ENSEA (tryphon, …).

V – Capture traffic generated by traceroute

The utility allows us to see the path taken by the packet when the packet pass through different routers.



```
tpreseau@d055-pc2:~$ sudo traceroute  -I cs.stanford.edu
[sudo] Mot de passe de tpreseau :
3OB says:  You seem to have forgotten your passwd, enter another!
[sudo] Mot de passe de tpreseau :
traceroute to cs.stanford.edu (171.64.64.64), 30 hops max, 60 byte packets
 1  _gateway (192.168.28.250)  0.210 ms  0.204 ms  0.202 ms
 2  10.10.27.250 (10.10.27.250)  0.431 ms  0.436 ms  0.434 ms
 3  194.57.172.81 (194.57.172.81)  0.637 ms  0.726 ms  0.721 ms
 4  vl1540-te0-0-0-1-ren-nr-cergy-rtr-091.noc.renater.fr (193.51.183.78)  1.080 ms  1.129 ms  1.129 ms
 5  vl500-te0-0-0-8-ren-nr-paris2-rtr-091.noc.renater.fr (193.55.204.115)  2.393 ms  2.398 ms  2.396 ms
 6  et-5-2-1-ren-nr-paris2-rtr-131.noc.renater.fr (193.51.177.82)  2.121 ms  1.890 ms  1.888 ms
 7  et-5-0-1-ren-nr-paris1-rtr-131.noc.renater.fr (193.55.204.194)  1.993 ms  2.141 ms  2.137 ms
 8  renater-lb1.mx1.par.fr.geant.net (62.40.124.69)  2.017 ms  2.033 ms  2.048 ms
 9  bundle-ether1.102.core1.bost2.net.internet2.edu (198.71.45.232)  73.513 ms  73.531 ms  73.531 ms
10  fourhundredge-0-0-0-2.4079.core1.alba.net.internet2.edu (163.253.2.172)  137.373 ms  136.942 ms  136.962 ms
11  fourhundredge-0-0-0-2.4079.core2.clev.net.internet2.edu (163.253.1.21)  135.490 ms  135.520 ms  135.522 ms
12  fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu (163.253.2.17)  136.644 ms  136.673 ms  137.805 ms
13  fourhundredge-0-0-0-2.4079.core2.chic.net.internet2.edu (163.253.2.18)  136.339 ms  136.367 ms  136.369 ms
14  fourhundredge-0-0-0-21.4079.core1.chic.net.internet2.edu (163.253.1.94)  136.465 ms  136.321 ms  136.311 ms
15  fourhundredge-0-0-0-1.4079.core2.kans.net.internet2.edu (163.253.2.29)  136.683 ms  138.379 ms  138.375 ms
16  fourhundredge-0-0-0-1.4079.core2.denv.net.internet2.edu (163.253.1.250)  135.832 ms  135.848 ms  137.920 ms
17  fourhundredge-0-0-0-3.4079.core2.salt.net.internet2.edu (163.253.1.169)  136.772 ms  136.787 ms  136.784 ms
18  fourhundredge-0-0-0-2.4079.core2.sacr.net.internet2.edu (163.253.1.186)  138.333 ms  138.330 ms  138.326 ms
19  fourhundredge-0-0-0-0.4079.core2.sunn.net.internet2.edu (163.253.1.191)  137.236 ms  137.251 ms  137.540 ms
20  fourhundredge-0-0-0-22.4079.core1.sunn.net.internet2.edu (163.253.1.24)  136.723 ms  136.756 ms  137.267 ms
21  137.164.26.126 (137.164.26.126)  135.133 ms  134.917 ms  134.924 ms
22  hpr-emvl1-agg-01--svl-agg10--100g.cenic.net (137.164.25.95)  136.052 ms  135.835 ms  135.825 ms
23  137.164.26.241 (137.164.26.241)  137.286 ms  144.705 ms  144.708 ms
24  csee-west-rtr-vl12.SUNet (171.66.0.238)  136.443 ms  136.477 ms  136.475 ms
25  CS.stanford.edu (171.64.64.64)  136.390 ms  136.414 ms  136.418 ms
```

Figure 11 - Traceroute for stanford

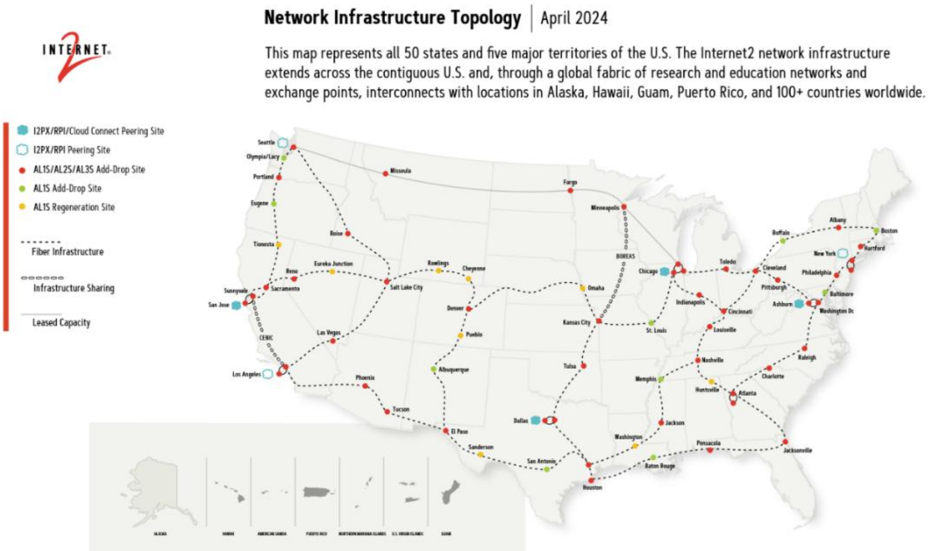
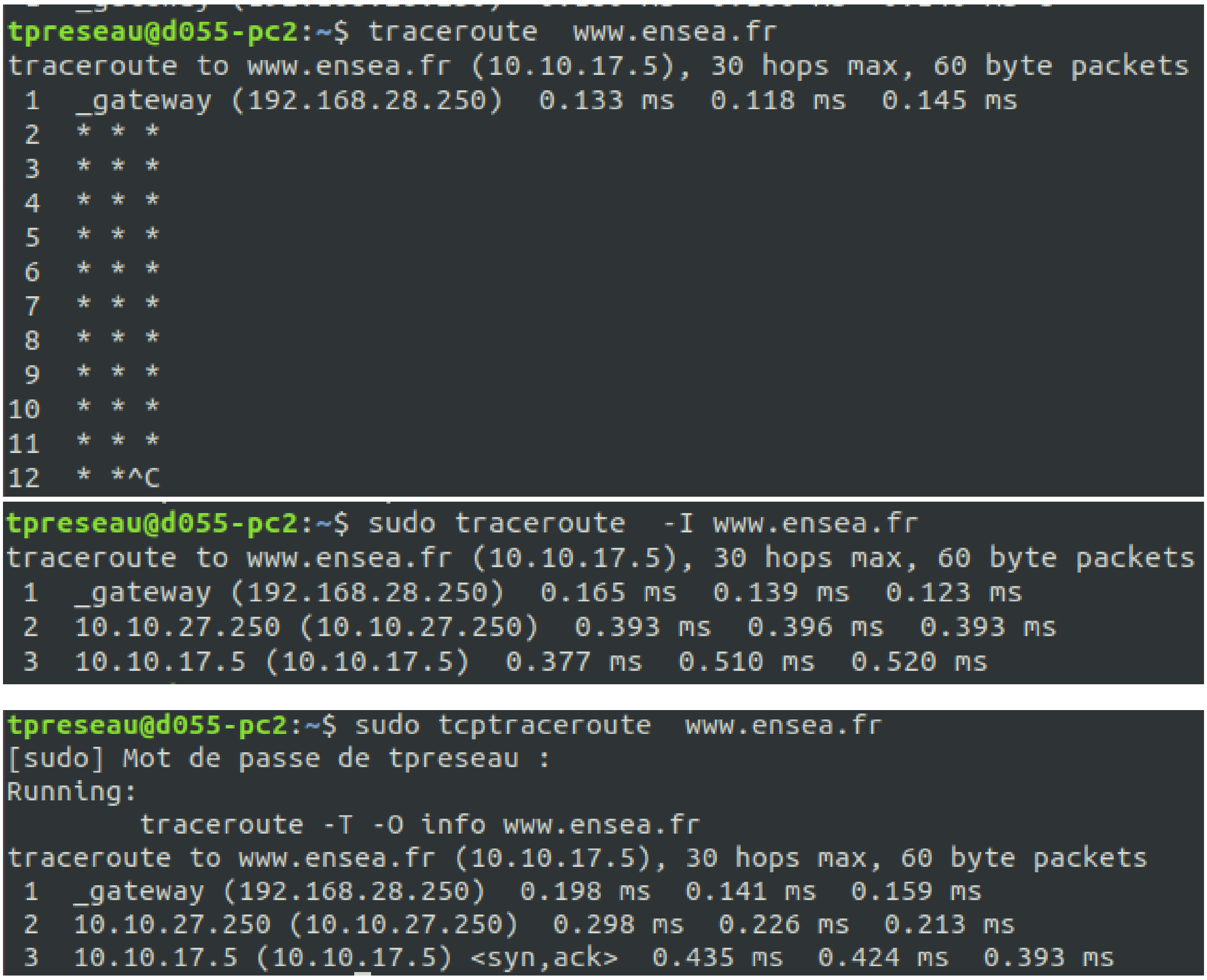


Figure 12 - Map of Internet2

The traceroute shows that the packet first traversed the Renater Network, which is the French Education Network that connects Cergy University. It then passed through the Géant network, which is the pan-European research and education network. After this router, the packet entered the United States, as evidenced by the additional ping time of approximately 70ms. This suggests that the packet likely crossed the Atlantic Ocean at this point.

Using the Internet2 Network Map, we can trace the approximate path the packet took within the US(Cleveland, Salt Lake City, ...).



```
tpreseau@d055-pc2:~$ traceroute  www.ensea.fr
traceroute to www.ensea.fr (10.10.17.5), 30 hops max, 60 byte packets
 1  _gateway (192.168.28.250)  0.133 ms  0.118 ms  0.145 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * *^C
```

```
tpreseau@d055-pc2:~$ sudo traceroute  -I www.ensea.fr
traceroute to www.ensea.fr (10.10.17.5), 30 hops max, 60 byte packets
 1  _gateway (192.168.28.250)  0.165 ms  0.139 ms  0.123 ms
 2  10.10.27.250 (10.10.27.250)  0.393 ms  0.396 ms  0.393 ms
 3  10.10.17.5 (10.10.17.5)  0.377 ms  0.510 ms  0.520 ms
```

```
tpreseau@d055-pc2:~$ sudo tcptraceroute  www.ensea.fr
[sudo] Mot de passe de tpreseau :
Running:
        traceroute -T -O info www.ensea.fr
traceroute to www.ensea.fr (10.10.17.5), 30 hops max, 60 byte packets
 1  _gateway (192.168.28.250)  0.198 ms  0.141 ms  0.159 ms
 2  10.10.27.250 (10.10.27.250)  0.298 ms  0.226 ms  0.213 ms
 3  10.10.17.5 (10.10.17.5) <syn,ack>  0.435 ms  0.424 ms  0.393 ms
```

Figure 13 - Test with different types of command for traceroute

The difference between the different command is that -I option forces the use of ICMP for the traceroute. Therefore, it can't be blocked by the routers whereas traceroute without options can be. However, *** could also be that the router has no name.