Compte-Rendu Traceroute

Table des matières

Analyse de traceroute :

La commande **traceroute** est un outil réseau permettant de déterminer l'acheminement d'un paquet IP ; soit les routeurs par lequel le paquet passe pour arriver jusqu'à sa cible. Voici comment la commande **traceroute** fait pour pouvoir déterminer ce chemin :
Traceroute envoie des trames sondes (3 par défaut) vers une adresse de destination avec un même Time-To-Live (correspond à « temps de vie » en français et commence à 1 par défaut). Cela signifie que, selon le nombre, le paquet pourra aller jusqu'à un certain routeur.

A chaque routeur que la trame sonde traverse, le Time-To-Live diminue de 1. Le premier routeur reçoit donc un paquet contenant un TTL de 1, le TTL est décrémenté, et arrive donc à zéro. Une fois que le Time-To-Live est à zéro, le routeur détruit le paquet et envoie une réponse ICMP "time exceeded", ce qui permet à la machine source de récupérer les informations de celui-ci.

On incrémente donc le TTL jusqu'à ce qu'on reçoive un "port unreachable" qui signifie soit :
        -qu'on a atteint l'hôte recherché
        -qu'on a dépassé le TTL max fixé (par défaut à 30), sans avoir atteint l'hôte recherché

Par défaut, traceroute utilise le protocole UDP, dans l'intervalle de port de 33434 à 33534. Celui-ci permettant de transmettre rapidement de petites quantités de données. Cependant, il est possible de choisir de passer par un protocole TCP ou même ICMP. Cela est pratique lorsque le pare-feu de l'un des routeurs traversé bloque certains protocoles utilisé par traceroute. De plus, si on précise l'option UDP (-U), cela utilisera le protocole UDP mais vers un port de destination particulier (au lieu d'augmenter le port pour chaque sonde). Par défaut le port est 53, celui du dns.

Sans option :

Voici ce que me retourne mon terminal lorsque je fais la commande traceroute sans option, donc par défaut il passera par le protocole UDP :

```
root@osavio:~# traceroute ac-toulouse.fr
traceroute to ac-toulouse.fr (185.75.143.25), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.254)  3.158 ms  3.148 ms  3.250 ms
 2  194.149.169.85 (194.149.169.85)  18.589 ms  18.913 ms  18.792 ms
 3  194.149.166.54 (194.149.166.54)  18.638 ms  21.847 ms  21.736 ms
 4  193.253.13.69 (193.253.13.69)  21.255 ms  21.511 ms  21.446 ms
 5  ae40-0.noidf001.Paris3eArrondissement.francetelecom.net (193.252.98.109)  21.679 ms  21.601 ms  21.182 ms
 6  ae52-0.nridf201.Aubervilliers.francetelecom.net (193.252.98.233)  21.424 ms  19.379 ms  19.596 ms
```

Compte-Rendu Traceroute

```
 7  ae41-0.nrlil101.Villeneuve-dascq.francetelecom.net (193.252.160.217)  22.955 ms  22.908 ms
24.999 ms
 8  lag-1.nolil601.Villeneuve-dascq.francetelecom.net (193.252.100.94)  24.351 ms  24.235 ms
24.219 ms
 9  193.252.227.62 (193.252.227.62)  24.153 ms  24.069 ms  24.017 ms
10  core01-civ_core01-ate.as35625.net (185.39.168.25)  23.958 ms  23.891 ms  23.845 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

On y voit beaucoup d'étoiles, cela est une exception, elle signifie que le routeur n'a pas
renvoyé d'informations.

Voici ci-dessous, ma capture de trame pour la commande ci-dessus :

```
No.   Time          Source          Destination     Protocol Length Info
  4 12.712085443   192.168.1.30    185.75.143.25      UDP     74    33159 → 33434 Len=32

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5534 (21812)
   Flags: 0x0000
   Time to live: 1
   Protocol: UDP (17)
   Header checksum: 0x5a52 [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
 User Datagram Protocol, Src Port: 33159, Dst Port: 33434
```

Compte-Rendu Traceroute

Data (32 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
5	12.712188670	192.168.1.30	185.75.143.25	UDP	74	39776 → 33435 Len=32

Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5535 (21813)
   Flags: 0x0000
   Time to live: 1
   Protocol: UDP (17)
   Header checksum: 0x5a51 [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
User Datagram Protocol, Src Port: 39776, Dst Port: 33435
Data (32 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
6	12.712267429	192.168.1.30	185.75.143.25	UDP	74	43100 → 33436 Len=32

Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5536 (21814)
   Flags: 0x0000
   Time to live: 1
   Protocol: UDP (17)
   Header checksum: 0x5a50 [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
User Datagram Protocol, Src Port: 43100, Dst Port: 33436
Data (32 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
7	12.712317350	192.168.1.30	185.75.143.25	UDP	74	50862 → 33437 Len=32

Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20

Compte-Rendu Traceroute

(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5537 (21815)
   Flags: 0x0000
   Time to live: 2
   Protocol: UDP (17)
   Header checksum: 0x594f [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
User Datagram Protocol, Src Port: 50862, Dst Port: 33437
Data (32 bytes)

. . .

No.   Time   Source   Destination   Protocol Length Info
  162 27.794052971 192.168.1.30   185.75.143.25   UDP   74   38879 → 33520
Len=32

Frame 162: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5ccf (23759)
   Flags: 0x0000
   Time to live: 29
   Protocol: UDP (17)
   Header checksum: 0x36b7 [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
User Datagram Protocol, Src Port: 38879, Dst Port: 33520
Data (32 bytes)

No.   Time   Source   Destination   Protocol Length Info
163 27.794195848 192.168.1.30   185.75.143.25   UDP   74   49412 → 33521
Len=32

Frame 163: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4

Compte-Rendu Traceroute

```
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5cd0 (23760)
    Flags: 0x0000
    Time to live: 30
    Protocol: UDP (17)
    Header checksum: 0x35b6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 49412, Dst Port: 33521
Data (32 bytes)
```

No.	Time	Source	Destination	Protocol	Length	Info
164	27.794308267	192.168.1.30	185.75.143.25	UDP	74	51635 → 33522 Len=32

```
Frame 164: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5cd1 (23761)
    Flags: 0x0000
    Time to live: 30
    Protocol: UDP (17)
    Header checksum: 0x35b5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 51635, Dst Port: 33522
Data (32 bytes)
```

No.	Time	Source	Destination	Protocol	Length	Info
165	27.794420362	192.168.1.30	185.75.143.25	UDP	74	53323 → 33523 Len=32

```
Frame 165: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5cd2 (23762)
    Flags: 0x0000
    Time to live: 30
```

Compte-Rendu Traceroute

```
    Protocol: UDP (17)
    Header checksum: 0x35b4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
  User Datagram Protocol, Src Port: 53323, Dst Port: 33523
```

Cela passe bien en UDP, et on voit bien que le Time to live augmente de 1, après avoir envoyé 3 trames sondes (couleur rouge).

Cependant, nous ne voyons pas la réponse du routeur destination (vert) "port unreachable" car celui-ci comportait une *, ce qui signifie que le routeur n'envoie pas ses informations, donc nous ne pouvons pas le voir dans la capture de trame.

Option -U :

Voici ce que me retourne mon terminal lorsque je fais la commande traceroute avec option UDP, donc vers le port 53 par défaut, celui du dns. :

```
root@osavio:~# traceroute ac-toulouse.fr -U
traceroute to ac-toulouse.fr (185.75.143.25), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.254)  1.791 ms  1.829 ms  1.867 ms
 2  194.149.169.85 (194.149.169.85)  19.390 ms  19.327 ms  19.257 ms
 3  194.149.166.54 (194.149.166.54)  18.812 ms  19.106 ms  19.423 ms
 4  193.253.13.69 (193.253.13.69)  19.370 ms  19.297 ms  19.237 ms
 5  ae40-0.noidf001.Paris3eArrondissement.francetelecom.net (193.252.98.109)  19.152 ms  19.332
ms  19.240 ms
 6  ae52-0.nridf201.Aubervilliers.francetelecom.net (193.252.98.233)  19.137 ms  19.502 ms
18.958 ms
 7  ae41-0.nrlil101.Villeneuve-dascq.francetelecom.net (193.252.160.217)  22.699 ms  24.042 ms
23.483 ms
 8  * * *
 9  193.252.227.62 (193.252.227.62)  25.833 ms  25.662 ms  25.649 ms
10  core01-civ_core01-ate.as35625.net (185.39.168.25)  25.629 ms  25.584 ms  25.537 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Compte-Rendu Traceroute

On y voit encore beaucoup d'étoiles, le routeur n'envoie toujours pas d'informations.

Voici ci-dessous, ma capture de trame pour la commande ci-dessus :

```
No.    Time          Source          Destination      Protocol Length Info
 189 37.761250992  192.168.1.30     185.75.143.25     DNS     74    Unknown operation
 (8) 0x4041[Malformed Packet]


 Frame 189: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
 (70:fc:8f:3f:47:20)
 Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6386 (25478)
    Flags: 0x0000
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x4c00 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
 User Datagram Protocol, Src Port: 57578, Dst Port: 53
 Domain Name System (query)
 [Malformed Packet: DNS]


No.    Time          Source          Destination      Protocol Length Info
 190 37.761390089  192.168.1.30     185.75.143.25     DNS     74    Unknown operation
 (8) 0x4041[Malformed Packet]


 Frame 190: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
 (70:fc:8f:3f:47:20)
 Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6387 (25479)
    Flags: 0x0000
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x4bff [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
```

Compte-Rendu Traceroute

User Datagram Protocol, Src Port: 38498, Dst Port: 53
Domain Name System (query)
[Malformed Packet: DNS]

No.	Time	Source	Destination	Protocol	Length	Info
191	37.761474919	192.168.1.30	185.75.143.25	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]

Frame 191: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20 (70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6388 (25480)
    Flags: 0x0000
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x4bfe [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 40666, Dst Port: 53
Domain Name System (query)
[Malformed Packet: DNS]

No.	Time	Source	Destination	Protocol	Length	Info
192	37.761556197	192.168.1.30	185.75.143.25	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]

Frame 192: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20 (70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6389 (25481)
    Flags: 0x0000
    Time to live: 2
    Protocol: UDP (17)
    Header checksum: 0x4afd [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 54006, Dst Port: 53

Compte-Rendu Traceroute

Domain Name System (query)
[Malformed Packet: DNS]

. . .

No.	Time	Source	Destination	Protocol Length Info
316	52.819106347	192.168.1.30	185.75.143.25	DNS 74 Unknown operation

(8) 0x4041[Malformed Packet]

Frame 316: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6d11 (27921)
    Flags: 0x0000
    Time to live: 29
    Protocol: UDP (17)
    Header checksum: 0x2675 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 45867, Dst Port: 53
Domain Name System (query)
[Malformed Packet: DNS]

No.	Time	Source	Destination	Protocol Length Info
317	52.819420840	192.168.1.30	185.75.143.25	DNS 74 Unknown operation

(8) 0x4041[Malformed Packet]

Frame 317: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6d12 (27922)
    Flags: 0x0000
    Time to live: 30
    Protocol: UDP (17)
    Header checksum: 0x2574 [validation disabled]
    [Header checksum status: Unverified]

Compte-Rendu Traceroute

Source: 192.168.1.30
Destination: 185.75.143.25
User Datagram Protocol, Src Port: 40181, Dst Port: 53
Domain Name System (query)
[Malformed Packet: DNS]

No.	Time	Source	Destination	Protocol	Length	Info
318	52.819729033	192.168.1.30	185.75.143.25	DNS	74	Unknown operation

(8) 0x4041[Malformed Packet]

Frame 318: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6d13 (27923)
    Flags: 0x0000
    Time to live: 30
    Protocol: UDP (17)
    Header checksum: 0x2573 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 41852, Dst Port: 53
Domain Name System (query)
[Malformed Packet: DNS]

No.	Time	Source	Destination	Protocol	Length	Info
319	52.820030170	192.168.1.30	185.75.143.25	DNS	74	Unknown operation

(8) 0x4041[Malformed Packet]

Frame 319: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6d14 (27924)
    Flags: 0x0000
    Time to live: 30
    Protocol: UDP (17)
    Header checksum: 0x2572 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
User Datagram Protocol, Src Port: 51522, Dst Port: 53

Compte-Rendu Traceroute

Domain Name System (query)
[Malformed Packet: DNS]

Cela passe toujours bien en UDP, et on voit bien que le Time to live augmente de 1, après avoir envoyé 3 trames sondes (couleur rouge).

Cependant, nous ne voyons toujours pas la réponse du routeur destination (vert) "port unreachable" car celui-ci comportait une *, ce qui signifie que le routeur n'envoie pas ses infos, donc nous ne pouvons pas le voir dans la capture de trame.

Option -I :

Voici ce que me retourne mon terminal lorsque je fais la commande traceroute avec l'option ICMP (-I) :

```
root@osavio:~# traceroute ac-toulouse.fr -I
traceroute to ac-toulouse.fr (185.75.143.25), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.254)  0.745 ms  23.949 ms  24.180 ms
 2  194.149.169.85 (194.149.169.85)  45.163 ms  45.158 ms  45.188 ms
 3  194.149.166.54 (194.149.166.54)  45.024 ms  45.059 ms  45.055 ms
 4  193.253.13.69 (193.253.13.69)  45.071 ms  45.065 ms  45.060 ms
 5  ae40-0.noidf001.Paris3eArrondissement.francetelecom.net (193.252.98.109)  45.063 ms  45.050 ms  45.045 ms
 6  ae52-0.nridf201.Aubervilliers.francetelecom.net (193.252.98.233)  45.035 ms  19.855 ms 20.027 ms
 7  ae41-0.nrlil101.Villeneuve-dascq.francetelecom.net (193.252.160.217)  38.462 ms  36.013 ms 35.991 ms
 8  lag-1.nolil601.Villeneuve-dascq.francetelecom.net (193.252.100.94)  23.410 ms  23.680 ms 23.669 ms
 9  193.252.227.62 (193.252.227.62)  23.881 ms  24.256 ms  24.243 ms
10  core01-civ_core01-ate.as35625.net (185.39.168.25)  23.491 ms  24.166 ms  24.109 ms
11  MEN-WEBEDU-PROXY01.dedie.ate.info (185.75.143.25)  24.361 ms  24.348 ms  24.194 ms
```

Je reçois bien mes 3 trames sondes, avec toujours comme adresse de destination l'adresse de ac-toulouse.fr :

No.	Time	Source	Destination	Protocol	Length	Info
325	62.556772416	192.168.1.30	185.75.143.25	ICMP	74	Echo (ping) request

id=0x5db9, seq=1/256, ttl=1 (no response found!)

Frame 325: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20 (70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf1d7 (61911)
    Flags: 0x0000
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0xbdbe [validation disabled]
    [Header checksum status: Unverified]

Compte-Rendu Traceroute

Source: 192.168.1.30
Destination: 185.75.143.25
Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Length	Info
326	62.556872426	192.168.1.30	185.75.143.25	ICMP	74	Echo (ping) request

id=0x5db9, seq=2/512, ttl=1 (no response found!)

Frame 326: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20 (70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0xf1d8 (61912)
   Flags: 0x0000
   Time to live: 1
   Protocol: ICMP (1)
   Header checksum: 0xbdbd [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Length	Info
327	62.556895491	192.168.1.30	185.75.143.25	ICMP	74	Echo (ping) request

id=0x5db9, seq=3/768, ttl=1 (no response found!)

Frame 327: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20 (70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0xf1d9 (61913)
   Flags: 0x0000
   Time to live: 1
   Protocol: ICMP (1)
   Header checksum: 0xbdbc [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
Internet Control Message Protocol

Compte-Rendu Traceroute

```
No.    Time          Source            Destination      Protocol Length Info
   328 62.556918064  192.168.1.30      185.75.143.25    ICMP    74    Echo (ping) request
id=0x5db9, seq=4/1024, ttl=2 (no response found!)
```

Frame 328: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf1da (61914)
    Flags: 0x0000
    Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0xbcbb [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
Internet Control Message Protocol

. . .

```
No.    Time          Source            Destination      Protocol Length Info
   376 62.612565945  192.168.1.30      185.75.143.25    ICMP    74    Echo (ping) request
id=0x5db9, seq=30/7680, ttl=10 (no response found!)
```

Frame 376: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf1f9 (61945)
    Flags: 0x0000
    Time to live: 10
    Protocol: ICMP (1)
    Header checksum: 0xb49c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
Internet Control Message Protocol

```
No.    Time          Source            Destination      Protocol Length Info
```

Compte-Rendu Traceroute

377 62.612616695   192.168.1.30   185.75.143.25   ICMP   74   Echo (ping) request
id=0x5db9, seq=31/7936, ttl=11 (reply in 401)

Frame 377: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf1fa (61946)
    Flags: 0x0000
    Time to live: 11
    Protocol: ICMP (1)
    Header checksum: 0xb39b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
Internet Control Message Protocol

No.   Time   Source   Destination   Protocol Length Info
378 62.612661588   192.168.1.30   185.75.143.25   ICMP   74   Echo (ping) request
id=0x5db9, seq=32/8192, ttl=11 (reply in 402)

Frame 378: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf1fb (61947)
    Flags: 0x0000
    Time to live: 11
    Protocol: ICMP (1)
    Header checksum: 0xb39a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
Internet Control Message Protocol

No.   Time   Source   Destination   Protocol Length Info
379 62.612834549   192.168.1.30   185.75.143.25   ICMP   74   Echo (ping) request
id=0x5db9, seq=33/8448, ttl=11 (reply in 403)

Compte-Rendu Traceroute

```
Frame 379: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf1fc (61948)
    Flags: 0x0000
    Time to live: 11
    Protocol: ICMP (1)
    Header checksum: 0xb399 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
Internet Control Message Protocol
```

Mes trames passent donc désormais par le protocole ICMP(jaune), le Time to live augmente toujours de 1, après avoir envoyé 3 trames sondes (couleur rouge).

De plus, nous voyons bien la réponse du routeur destination (vert) "port unreachable" :

```
No.     Time          Source              Destination        Protocol Length Info
392 94.712803736  185.75.143.25       192.168.1.30        ICMP    102   Destination
unreachable (Port unreachable)
```

Option -T :

Voici ce que me retourne mon terminal lorsque je fais la commande traceroute avec l'option TCP (-T) :

```
root@osavio:~# traceroute ac-toulouse.fr -T
traceroute to ac-toulouse.fr (185.75.143.25), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.254)  0.798 ms  26.803 ms  26.903 ms
 2  194.149.169.85 (194.149.169.85)  45.409 ms  45.304 ms  45.257 ms
 3  194.149.166.54 (194.149.166.54)  45.113 ms  45.146 ms  47.352 ms
 4  193.253.13.69 (193.253.13.69)  47.319 ms  47.228 ms  47.173 ms
 5  ae40-0.noidf001.Paris3eArrondissement.francetelecom.net (193.252.98.109)  47.115 ms  47.076
ms  46.974 ms
 6  ae52-0.nridf201.Aubervilliers.francetelecom.net (193.252.98.233)  46.925 ms  18.697 ms
18.749 ms
 7  ae41-0.nrlil101.Villeneuve-dascq.francetelecom.net (193.252.160.217)  25.482 ms  24.290 ms
23.827 ms
 8  * * *
 9  193.252.227.62 (193.252.227.62)  22.838 ms  23.130 ms  23.009 ms
10  core01-civ_core01-ate.as35625.net (185.39.168.25)  23.198 ms  23.491 ms  23.472 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  MEN-WEBEDU-PROXY01.dedie.ate.info (185.75.143.25)  23.436 ms  23.024 ms  23.205 ms
```

Compte-Rendu Traceroute

Je reçois bien mes 3 trames sondes, avec toujours comme adresse de destination l'adresse de ac-toulouse.fr :

```
No.    Time          Source          Destination       Protocol Length Info
   436 81.004647210  192.168.1.30    185.75.143.25      TCP     74    41747 → 80 [SYN]
 Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4


 Frame 436: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
 (70:fc:8f:3f:47:20)
 Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5955 (22869)
    Flags: 0x0000
    Time to live: 1
    Protocol: TCP (6)
    Header checksum: 0x563c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
 Transmission Control Protocol, Src Port: 41747, Dst Port: 80, Seq: 0, Len: 0

No.    Time          Source          Destination       Protocol Length Info
   437 81.004744773  192.168.1.30    185.75.143.25      TCP     74    58585 → 80 [SYN]
 Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4

 Frame 437: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
 (70:fc:8f:3f:47:20)
 Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5956 (22870)
    Flags: 0x0000
    Time to live: 1
    Protocol: TCP (6)
    Header checksum: 0x563b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.30
    Destination: 185.75.143.25
 Transmission Control Protocol, Src Port: 58585, Dst Port: 80, Seq: 0, Len: 0

No.    Time          Source          Destination       Protocol Length Info
   438 81.004815251  192.168.1.30    185.75.143.25      TCP     74    33275 → 80 [SYN]
 Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4
```

Compte-Rendu Traceroute

Frame 438: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5957 (22871)
   Flags: 0x0000
   Time to live: 1
   Protocol: TCP (6)
   Header checksum: 0x563a [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
Transmission Control Protocol, Src Port: 33275, Dst Port: 80, Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
439	81.004898534	192.168.1.30	185.75.143.25	TCP	74	57489 → 80 [SYN]

Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4

Frame 439: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x5958 (22872)
   Flags: 0x0000
   Time to live: 2
   Protocol: TCP (6)
   Header checksum: 0x5539 [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.30
   Destination: 185.75.143.25
Transmission Control Protocol, Src Port: 57489, Dst Port: 80, Seq: 0, Len: 0

. . .

No.	Time	Source	Destination	Protocol	Length	Info
508	81.087050080	192.168.1.30	185.75.143.25	TCP	74	52665 → 80 [SYN]

Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4

Frame 508: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25

Compte-Rendu Traceroute

```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x5988 (22920)
  Flags: 0x0000
  Time to live: 14
  Protocol: TCP (6)
  Header checksum: 0x4909 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.30
  Destination: 185.75.143.25
Transmission Control Protocol, Src Port: 52665, Dst Port: 80, Seq: 0, Len: 0
```

```
No.    Time          Source            Destination        Protocol Length Info
   509 81.087191108  192.168.1.30      185.75.143.25       TCP      74    59869 → 80 [SYN]
Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4
```

```
Frame 509: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x5989 (22921)
  Flags: 0x0000
  Time to live: 15
  Protocol: TCP (6)
  Header checksum: 0x4808 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.30
  Destination: 185.75.143.25
Transmission Control Protocol, Src Port: 59869, Dst Port: 80, Seq: 0, Len: 0
```

```
No.    Time          Source            Destination        Protocol Length Info
   512 81.110952595  192.168.1.30      185.75.143.25       TCP      74    53045 → 80 [SYN]
Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4
```

```
Frame 512: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x598d (22925)
```

Compte-Rendu Traceroute

```
Flags: 0x0000
Time to live: 15
Protocol: TCP (6)
Header checksum: 0x4804 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.30
Destination: 185.75.143.25
Transmission Control Protocol, Src Port: 53045, Dst Port: 80, Seq: 0, Len: 0


No.   Time         Source           Destination       Protocol Length Info
  515 81.134199710   192.168.1.30    185.75.143.25     TCP      74     57779 → 80 [SYN]
Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3837575513 TSecr=0 WS=4


Frame 515: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_6e:62:a4 (70:77:81:6e:62:a4), Dst: FreeboxS_3f:47:20
(70:fc:8f:3f:47:20)
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 185.75.143.25
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x5991 (22929)
  Flags: 0x0000
  Time to live: 15
  Protocol: TCP (6)
  Header checksum: 0x4800 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.30
  Destination: 185.75.143.25
Transmission Control Protocol, Src Port: 57779, Dst Port: 80, Seq: 0, Len: 0
```

Cela passe bien en TCP (jaune), et on voit bien que le Time to live augmente de 1, après avoir envoyé 3 trames sondes (couleur rouge).

De plus, comme avec l'option ICMP, nous voyons bien la réponse du routeur destination (vert) "port unreachable" :

```
No.   Time         Source           Destination       Protocol Length Info
  392 94.712803736   185.75.143.25   192.168.1.30      ICMP     102    Destination
unreachable (Port unreachable)
```

Time to live exceeded :

```
No.   Time         Source           Destination       Protocol Length Info
   17 12.712803736   192.168.1.254   192.168.1.30      ICMP     102    Time-to-live exceeded
  (Time to live exceeded in transit)
```

On peut donc voir que l'adresse bleu est bien la même sur la capture de trame et sur toutes les commandes traceroute, le premier routeur nous envoie donc bien une réponse ICMP "time exceeded" lorsque le ttl arrive à 0. De plus, il y en a pour toutes les autres

Compte-Rendu Traceroute

adresses, mais j'ai décidé de mettre que cet exemple car il regroupe toutes mes captures ci-dessus.

Nous remarquons bien à travers ces exemples que l'adresse de destination ne change jamais, cependant, nous n'y accédons que dans un second temps. Néanmoins, l'adresse qui nous répond avec le message "time exceeded" est bien celle du routeur sur lequel le ttl s'est arrêté.

De plus, on remarque bien que selon le protocole, nous avons des réponses différentes, le fait de tester avec plusieurs protocoles est donc utile pour avoir le plus de résultats possibles.