Table des matières

1) Commande Traceroute :

La commande traceroute donne les IP des routeurs qu'il a traversé pour aller à un point de ping. Il joue sur le TTL (couche 3) : trame IP. Il peut envoyer des paquets de type UDP, TCP ou bien ICMP. Par défaut il envoi des paquets UDP.

Le TTL (Time To Leave) permet de limiter le nombre de bonds entre chaque routeurs. Pour traceroute le TTL par défaut est de 1.

1.1) Comment fonctionne traceroute (source : wikipedia)

Les paquets IP sont acheminés vers la destination en passant d'un routeur à un autre. Chaque routeur examine sa table de routage pour déterminer le routeur suivant. Traceroute va permettre d'identifier les routeurs empruntés, indiquer le délai entre chacun des routeurs et les éventuelles pertes de paquets. Ces informations seront utiles pour diagnostiquer des problèmes de routage, comme des boucles, pour déterminer s'il y a de la congestion ou un autre problème sur un des liens vers la destination.

Le principe de fonctionnement de Traceroute consiste à envoyer des paquets UDP (certaines versions peuvent aussi utiliser TCP ou bien ICMP *ECHO Request*) avec un paramètre Time-To-Live (TTL) de plus en plus grand (en commençant à 1). Chaque routeur qui reçoit un paquet IP en décrémente le TTL avant de le transmettre. Lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur *Time to live exceeded* vers la source. Traceroute découvre ainsi les routeurs de proche en proche.

Une fois le paquet sonde arrivé à sa destination finale, traceroute cesse de recevoir des TTL exceeded, et reçoit un paquet réponse ayant pour adresse IP source celle de l'interface de l'équipement sondé à travers laquelle est émis le paquet ICMP. Traceroute essaie volontairement de contacter un port invalide, donc le paquet réponse est normalement de type ICMP Port Unreachable. Si la machine destination avait par hasard un programme écoutant sur ce port, le comportement n'est pas certain et dépend du programme.

Il existe cependant un certain nombre d'éléments qui peuvent compliquer l'interprétation du résultat :

- le chemin suivi par les paquets peut être asymétrique et traceroute ne montre que l'aller ;
- le chemin suivi peut être radicalement différent depuis un autre point, même proche géographiquement ;
- les routeurs émettent le paquet ICMP avec l'adresse source de l'interface utilisée pour vous joindre, ce n'est pas forcément l'interface par laquelle votre paquet sonde est passé ;
- les routeurs ne traitent pas nécessairement les paquets ICMP en transit de la même façon que le trafic de données. Les temps de réponse en cours de route peuvent ne pas refléter ceux que l'on observerait au niveau du trafic applicatif. Ce sera particulièrement le cas si le réseau fait usage de qualité de service et que le trafic sur certains liens approche la congestion.
- la création du paquet ICMP « TTL exceeded » est une opération complexe qui sollicite le CPU du routeur, alors que le trafic est habituellement traité au niveau du matériel spécialisé. Il se peut qu'un délai supplémentaire soit observé si le CPU est occupé à d'autres tâches plus essentielles (gestion des tables de routage, traitement des requêtes de gestion du réseau), alors que ce délai n'a pas d'effet sur le trafic de transit du routeur.
- un routeur peut ne pas répondre aux requêtes ICMP. Dans ce cas, on voit généralement des signes astérisques (*) sur les nœuds intermédiaires qui ne répondent pas aux requêtes ICMP. Il se peut aussi que, pour des raisons de performance, le routeur limite le nombre de paquets ICMP généré par unité de temps, ce qui cause l'apparition d'étoiles sur le parcours, qui ne sont cependant pas le symptôme d'un problème.
- l'adresse IP de la réponse ICMP TTL Exceeded peut être privée (RFC 1918), et donc bloquée en cas de transit par Internet, ou impossible à identifier.

1.2) Exemples d’utilisations

Prenons deux exemples différents. Le premier exemple est un traceroute vers google.com. On peut voir que les paquets passent par 10 routeurs. On peut voir l’adresse IP des routeurs par lesquels passent les paquets et le temps de parcours. On voit aussi le nom de domaine qui est traversé. Les étoiles sur le routeurs n°4 veulent dire que le routeur n’a donné aucunes informations car la commande traceroute utilise des ports particuliers pour envoyer les paquets (il commence au port 34334) et certains routeurs sont configurés pour ne pas répondre à ces ports.

```
test@213-15 : ~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.213.255.254 (10.213.255.254)  3.443 ms  3.707 ms  4.122 ms
 2  GW.iutbeziers.fr (194.199.227.254)  1.199 ms  1.358 ms  1.567 ms
```

```
3  10.3.7.25 (10.3.7.25)  3.132 ms  3.276 ms  3.115 ms
4  * * *
5  xe0-0-3-marseille1-rtr-131.noc.renater.fr (193.51.177.236)  6.134 ms  6.136 ms  6.115 ms
6  te1-1-marseille2-rtr-021.noc.renater.fr (193.51.177.185)  12.039 ms te2-6-marseille2-rtr-021.noc.renater.fr (193.51.177.213)  5.508 ms  5.403 ms
7  72.14.218.132 (72.14.218.132)  8.628 ms  5.844 ms  5.753 ms
8  74.125.244.225 (74.125.244.225)  6.703 ms  6.451 ms  6.877 ms
9  172.253.67.157 (172.253.67.157)  6.827 ms 66.249.95.43 (66.249.95.43)  6.736 ms 172.253.67.153 (172.253.67.153)  6.677 ms
10  dns.google (8.8.8.8)  5.641 ms  5.630 ms  6.111 ms
```

Maintenant prenons un deuxième exemple avec l'IUT :

```
test@213-15 : ~$ traceroute www.iutbeziers.fr
traceroute to www.iutbeziers.fr (194.199.227.80), 30 hops max, 60 byte packets
1  10.213.255.254 (10.213.255.254)  4.979 ms  5.269 ms  5.662 ms
2  www.iutbeziers.fr (194.199.227.80)  0.914 ms  1.149 ms  1.474 ms
```

Cette fois comme nous nous situons déjà dans l'IUT nous avons moins de routeurs à traverser.

2) Quelques commandes intéressantes de traceroute

La commande « traceroute -I » permet d'envoyer des paquets de type ICMP

La commande « traceroute -T » permet d'envoyer des paquets de type TCP

La commande « traceroute -U » permet d'envoyer des paquets de type UDP

La commande « traceroute -f » permet de définir avec quel TTL on commence

La commande « traceroute -m » permet de définir le maximum de TTL

La commande « traceroute -n » permet de supprimer les noms de domaine

La commande « traceroute -A » permet de lister tous les AS par lesquels passent les paquets

3) Application de traceroute

3.1) Message UDP

Filtres utilisés :

- Affichage : ip.addr == 10.213.15.1

No.	Time	Source	Destination	Protocol	Length	Info
3	0.364652542	10.213.15.1	8.8.8.8	UDP	74	38303 → 33434 Len=32

No.	Time	Source	Destination	Protocol	Length	Info
4	0.364714799	10.213.15.1	8.8.8.8	UDP	74	33594 → 33435 Len=32

User Datagram Protocol, Src Port: 33594, Dst Port: 33435

Source Port: 33594

Destination Port: 33435

[Expert Info (Chat/Sequence): Possible traceroute: hop #1, attempt #1]

No.	Time	Source	Destination	Protocol	Length	Info
5	0.364746561	10.213.15.1	8.8.8.8	UDP	74	34096 → 33436 Len=32

No.	Time	Source	Destination	Protocol	Length	Info
6	0.364775120	10.213.15.1	8.8.8.8	UDP	74	33124 → 33437 Len=32

No.	Time	Source	Destination	Protocol	Length	Info
7	0.364804432	10.213.15.1	8.8.8.8	UDP	74	38012 → 33438 Len=32

No.	Time	Source	Destination	Protocol	Length	Info
8	0.364832914	10.213.15.1	8.8.8.8	UDP	74	52556 → 33439 Len=32

En vert on peut voir à quel TTL et à quel routeur correspond la trame

En rouge on peut voir le port de la source et de la destination

En bleu on peut voir le type de paquet envoyé

Ces trames correspondent aux 2 premiers routeurs qui sont traversés. Traceroute envoi par défaut 3 paquets.

3.2) Message d'erreur «TTL exceeded»(paquets ICMP)

No. Time Source Destination Protocol Length Info

19 0.365966414 194.199.227.254 10.213.15.1 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

...

Time to live: 254

Protocol: ICMP (1)

Source: 194.199.227.254

Destination: 10.213.15.1

...

Time to live: 1

[Expert Info (Note/Sequence): "Time To Live" only 1]

Protocol: UDP (17)

Header checksum: 0x75c0 [validation disabled]

[Header checksum status: Unverified]

Source: 10.213.15.1

Destination: 8.8.8.8

User Datagram Protocol, Src Port: 33124, Dst Port: 33437

Source Port: 33124

Destination Port: 33437

[Expert Info (Chat/Sequence): Possible traceroute: hop #1, attempt #3]

Length: 40

Checksum: 0x50b5 [unverified]

[Checksum Status: Unverified]

[Stream index: 4]

No. Time Source Destination Protocol Length Info

20 0.366154889 194.199.227.254 10.213.15.1 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

```
    Identification: 0xe3e8 (58344)
    Flags: 0x0000
    Time to live: 254
    Protocol: ICMP (1)
    Source: 194.199.227.254
    Destination: 10.213.15.1
Internet Control Message Protocol
      Identification: 0x8e10 (36368)
      Flags: 0x0000
      Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
      Protocol: UDP (17)
      Header checksum: 0x75bf [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.213.15.1
      Destination: 8.8.8.8
    User Datagram Protocol, Src Port: 38012, Dst Port: 33438
      Source Port: 38012
      Destination Port: 33438
        [Expert Info (Chat/Sequence): Possible traceroute: hop #2, attempt #1]
      Length: 40
      Checksum: 0x3d9c [unverified]
      [Checksum Status: Unverified]
      [Stream index: 5]
```

En rouge on peut voir que le protocole utilisé pour envoyer le message d'erreur est de l'ICMP (Internet Control Message Protocol). L'ICMP

En vert on peut voir l'adresse IP de destination du message. On voit ici que le message est destiné à ma machine ce qui veut dire que c'est le routeur qui renvoi l'erreur.

En bleu on peut voir que le premier routeur traversé renvoi un message d'erreur au troisième paquet qu'il a reçu

3.3) Autres messages d'erreur «port unreachable»

No. Time Source Destination Protocol Length Info

63 6.012296711 172.217.18.36 10.213.15.1 ICMP 70 Destination unreachable (Port unreachable)

...

Time to live: 54

Protocol: ICMP (1)

Header checksum: 0xabf2 [validation disabled]

[Header checksum status: Unverified]

Source: 172.217.18.36

Destination: 10.213.15.1

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

64 6.012547283 172.217.18.36 10.213.15.1 ICMP 70 Destination unreachable (Port unreachable)

...

Time to live: 54

Protocol: ICMP (1)

Header checksum: 0xabf2 [validation disabled]

[Header checksum status: Unverified]

Source: 172.217.18.36

Destination: 10.213.15.1

Internet Control Message Protocol

Dans notre cas le message d'erreur port unreachable veut dire que les paquets sont bien arrivés à la destination finale. Il existe 2 types de cas où l'on peut avoir ce message d'erreur :

- Le premier est quand le paquet arrive à la destination finale

-Le second cas est quand la destination finale se situe plus loin que le nombre de sauts maximal que fait la commande