M2102-2 Architecture des réseaux, DUT Info S2

Correction TD : couche IP

Pour toute question ou besoin de précision, n'hésitez pas à utiliser le forum ou m'envoyer un mail. (remi.watrigant@univ-lyon1.fr).

Exercice :

Essayez des **`traceroute`** vers les serveurs suivants :

- Un serveur français de Google : www.google.fr
- Un serveur coréen de Google : www.google.kr
- Le site web de l'Université Royal Holloway de Londres : www.royalholloway.ac.uk
- Le site web de l'Université Lyon 1 : www.univ-lyon1.fr

Regardez les points communs de ces **`traceroute`**, les différences, et tentez de comprendre les informations affichées.

Traceroute permet de voir les routeurs parcourus par des paquets IP. Il donne une liste de routeurs (on parlera de « sauts », car les paquets vont de routeur en routeur).

Le cas des serveurs de Google est un peu particulier. Il se peut que 2 traceroute vers la même adresse à 2 moments différents donnent des résultats différents. Par exemple, chez moi, un premier traceroute vers l'adresse coréenne me donne 12 sauts, et un second m'en donne 10. Google possède des serveurs dans de nombreuses régions du monde, et procède à de « l'équilibre de charge » pour répartir les connexions. Ainsi, même si on pense accéder à « l'interface coréenne » du moteur de recherche, on est peut-être sur un serveur en Europe…

Pour les autres en revanche, le traceroute est censé moins varier. Celui vers l'université anglaise me donne 15 sauts :

```
remi@remi-XPS-13-9360:~$ traceroute www.royalholloway.ac.uk
traceroute to www.royalholloway.ac.uk (134.219.220.117), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  3.286 ms  3.229 ms  3.179 ms
 2  10.113.64.1 (10.113.64.1)  14.011 ms  14.028 ms  13.991 ms
 3  eps1rj-ge-1-1-5.200.numericable.net (213.245.253.81)  17.186 ms  22.795 ms  23.236 ms
 4  * * ip-65.net-80-236-3.static.numericable.fr (80.236.3.65)  33.181 ms
 5  prs-b7-link.telia.net (62.115.55.45)  28.486 ms  28.386 ms  28.375 ms
 6  prs-bb3-link.telia.net (62.115.113.182)  40.673 ms  34.798 ms *
 7  * ldn-bb3-link.telia.net (62.115.134.93)  24.498 ms  29.879 ms
 8  ldn-b4-link.telia.net (62.115.134.139)  29.250 ms ldn-b4-link.telia.net (62.115.134.135)  27.102 ms
41.374 ms
 9  jisc-ic-345131-ldn-b4.c.telia.net (62.115.175.131)  29.019 ms  26.435 ms  26.345 ms
10  ae24.londhx-sbr1.ja.net (146.97.35.197)  26.270 ms  25.992 ms  25.197 ms
11  ae29.londpg-sbr2.ja.net (146.97.33.2)  29.372 ms  29.311 ms  24.809 ms
12  ae26.londpg-ban1.ja.net (146.97.35.234)  29.484 ms  29.405 ms  27.037 ms
13  royal-holloway-and-bedford-new-college.ja.net (146.97.139.186)  28.025 ms  27.954 ms  28.021 ms
14  * * *
15  tip-134-219-220-117.rhul.ac.uk (134.219.220.117)  28.193 ms *  31.159 ms
```

à chaque saut, on a le nom du serveur puis son adresse IP entre parenthèses, puis 3 temps de latence (en ms), car à chaque fois traceroute envoie 3 requêtes. Certaines fois, il y a des étoiles, on verra

pourquoi plus tard. Le 1er routeur est ma box, les 3 suivants appartiennent vraisemblablement à Numericable, car mon fournisseur d'accès internet est SFR qui utilise le réseau Numéricable. Ensuite ce sont d'autres entreprises.

Pour le serveur de l'université de Lyon, je n'obtiens que des étoiles après 9 sauts, on verra pourquoi à la prochaine question. En principe, après des sauts sur des routeurs de votre fournisseur d'accès internet, vous tombez sur des routeurs du réseau « Renater » qui relie toutes les universités françaises.

Dans tous les cas, les 4-5 premiers routeurs seront très certainement toujours les mêmes quelle que soit la destination, ce seront ceux de votre fournisseur d'accès à internet (FAI) : vos paquets utiliseront le même chemin pour « sortir » du réseau de votre FAI.

Question 1 :
Que signifient les étoiles dans certains résultats de **`traceroute`** ? Pour le dernier exemple (www.univ-lyon1.fr), le traceroute n'aboutit pas : pourquoi ? Essayez de lancer un ping vers ce dernier : que se passe-t-il ? Pourquoi?)

Sous Windows, traceroute envoie par défaut des messages ICMP (comme des pings), et certains routeurs sont paramétrés pour ne pas répondre aux pings (en utilisant un pare-feu, « firewall »), probablement car leurs administrateurs jugent que cela enduira une charge de travail inutile, ou bien pour empêcher une attaque par « déni de service » (DoS). C'est le cas du serveur web de l'université : un ping n'aboutit pas.
Sous Linux, traceroute utilise par défaut le protocole UDP. Dans le cas du serveur de l'université, il le bloque également, donc j'obtiens des étoiles (en fait traceroute va utiliser UDP avec un « numéro de port » généralement jamais utilisé par les utilisations « standards » du serveur web, et c'est ce numéro de port qui sera bloqué sur le serveur). En revanche je peux paramétrer pour utiliser TCP, et là il veut bien me répondre :

```
remi@remi-XPS-13-9360:~$ traceroute -T www.univ-lyon1.fr
traceroute to www.univ-lyon1.fr (134.214.126.72), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  2.443 ms  2.458 ms  2.458 ms
 2  10.113.64.1 (10.113.64.1)  8.735 ms  13.316 ms  13.290 ms
 3  eps1rj-ge-1-1-5.200.numericable.net (213.245.253.81)  13.303 ms  13.292 ms  13.286 ms
 4  172.19.132.146 (172.19.132.146)  25.982 ms  21.945 ms  21.917 ms
 5  ip-58.net-80-236-0.static.numericable.fr (80.236.0.58)  20.956 ms  20.926 ms  21.200 ms
 6  * * *
 7  30.12.6.109.rev.sfr.net (109.6.12.30)  26.789 ms  24.783 ms  24.748 ms
 8  renater.peers.lyonix.net (77.95.71.17)  21.214 ms  21.158 ms  24.700 ms
 9  lyres-vl143-te1-5-lyon2-rtr-021.noc.renater.fr (193.51.183.253)  24.693 ms  24.679 ms  24.859
ms
10  * * *
11  * * *
12  ksup.univ-lyon1.fr (134.214.126.72)  22.443 ms  22.274 ms  22.386 ms
```

On voit néanmoins que les routeurs aux sauts 6, 10 et 11 ne me répondent pas : leur « firewall » les empêche de me répondre (en revanche ils font quand même leur boulot : ils transmettent ces paquets aux autres routeurs, donc on peut suivre la fin de la route).

Les sites web des universités/organismes français bloquent souvent les paquets de traceroute. Pour certaines ce n'est pas le cas. J'ai trouvé par exemple celui de l'INRIA Sophia Antipolis www-sop.inria.fr (ce n'est pas une faute de frappe, c'est bien www-sop au début, et pas www.sop). En

principe, un traceroute utilisant ICMP (donc celui par défaut de Windows, ou bien en utilisant l'option -I sous Linux) fonctionnera sur celui-ci :

```
remi@remi-XPS-13-9360:~$ traceroute -I www-sop.inria.fr
traceroute to www-sop.inria.fr (138.96.0.39), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.704 ms  1.693 ms  1.690 ms
 2  10.113.64.1 (10.113.64.1)  8.282 ms  8.215 ms  12.929 ms
 3  eps1rj-ge-1-1-5.200.numericable.net (213.245.253.81)  12.991 ms  12.994 ms  12.995 ms
 4  172.19.132.146 (172.19.132.146)  28.646 ms  28.654 ms  28.649 ms
 5  renater.par.franceix.net (37.49.236.19)  20.812 ms  20.813 ms  20.729 ms
 6  te2-2-lyon2-rtr-021.noc.renater.fr (193.51.177.43)  27.892 ms  24.780 ms  24.742 ms
 7  193.51.180.103 (193.51.180.103)  24.924 ms  22.889 ms  26.741 ms
 8  193.51.180.119 (193.51.180.119)  25.749 ms  25.823 ms  25.825 ms
 9  te0-2-0-0-ren-nr-sophia-rtr-091.noc.renater.fr (193.51.177.21)  26.605 ms  23.596 ms  23.828
ms
10  inria-gi8-2-sophia-rtr-021.noc.renater.fr (193.51.181.137)  23.398 ms  22.274 ms  27.540 ms
11  193.48.223.19 (193.48.223.19)  27.549 ms  27.385 ms  22.469 ms
12  193.48.223.26 (193.48.223.26)  24.365 ms  27.108 ms  26.611 ms
13  www-sop.inria.fr (138.96.0.39)  26.624 ms  32.417 ms  32.185 ms
```

Là on voit bien les routeurs de Renater dans la deuxième moitié de la route.

Question 2 :

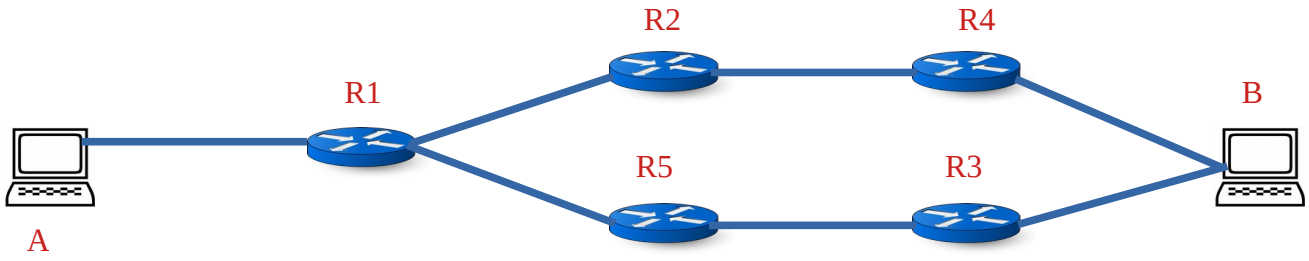
Comment fait **`traceroute`** pour afficher les adresses des routeurs ? Indice : re-visionnez l'exemple des pings à la fin de la vidéo du cours 2.

Traceroute envoie des messages ICMP (ou UDP, selon le système d'exploitation et les options) vers la machine que vous lui avez indiquée, encapsulés dans des paquets IP ayant des valeurs de TTL croissantes : 0, 1, 2, .. jusqu'à une certaine limite qui est souvent 30 par défaut. Rappelez-vous qu'un routeur qui transmet un paquet à un autre routeur va décroître son champ TTL, et si celui-ci est 0 quand il le reçoit, alors il ne le transmet pas au destinataire, mais envoie un message ICMP d'erreur (TTL exceeded) à l'émetteur. Ainsi :
- un paquet avec un TTL de 0 ira à votre box, mais celle-ci vous renverra immédiatement un ICMP TTL exceeded
- un paquet avec un TTL de 1 ira à votre box, celle-ci transmettra au prochain routeur ce message avec un TTL de 0, donc ce routeur vous envoie un ICMP TTL exceeded. Vous connaissez ainsi l'adresse IP de ce routeur
… ainsi de suite jusqu'à l'adresse que vous voulez atteindre.

Question 3 :

Traceroute ne donne qu'une idée du chemin emprunté, mais on ne peut pas vraiment être sûr que c'est le bon tout le temps. Pourquoi ? Donnez un exemple de situation où le chemin donné peut être incorrect. Par exemple, un exemple où le programme va donner comme liste de routeurs R1, R2, R3 pour un chemin de A à B, alors que R2 et R3 ne sont même pas reliés ensemble.

Imaginons le cas suivant :



Supposons que A lance un traceroute vers B, et supposons que les tables de routages font en sorte que le plus court chemin de A vers B passe par R1, R2 et R4 (on peut éventuellement rajouter des routeurs entre R3 et B pour qu'on soit sûr que cela soit le cas). Résumons ce qui se passe :

- A envoie un paquet à B avec TTL de 0. Il arrive à R1 qui lui renvoie un ICMP TTL exceeded
- A envoie un paquet à B avec TTL de 1. Il passe par R1 qui décrémente le TTL, puis arrive à R2 avec donc un TTL de 0 qui lui renvoie un ICMP TTL exceeded
- Supposons maintenant que le routeur R2 tombe en panne ! Ainsi la nouvelle route de A vers B passe maintenant par R1, R5 puis R3.
- A envoie un paquet à B avec un TTL de 2. Il arrive à R1 qui décrémente le TTL, puis passe par R5 qui décrémente le TTL, et arrive enfin à R3 avec un TTL de 0, qui renvoie donc à B un ICMP TTL exceeded.
- A envoie un paquet à B avec un TTL de 3. Il arrive à R1 qui décrémente le TTL, puis passe par R5 et R3 qui décémentent ce TTL, et le paquet arrive enfin à B.

Si on résume, le traceroute de la machine A affichera les résultats suivants (qui correspondent aux ICMP TTL exceeded reçus) :
1. R1
2. R2
3. R3
4. B

On a donc l'impression que le chemin est A – R1 – R2 – R3 – B, mais ce n'est pas le cas. R2 et R3 ne sont même pas connectés !

Dans un autre cas de figure, plutôt qu'une panne, on pourrait imaginer la situation où R1 fait passer les paquets soit par R2 soit par R5 afin d'équilibrer la charge. On aurait ici aussi un « faux » résultat de traceroute.

Ainsi, traceroute ne donne qu'une idée du chemin emprunté. Souvent il n'y a pas de panne ni d'équilibrage de charge, la route donnée est donc probablement correcte, mais pas tout le temps !