LAFORGE RT1
Samuel

TP2 M1104

Table des matières

1) ICMP et Ping

1) Pour cette question je lance wireshark, je met un filtre pour ne garder que ce que mon ordinateur envoi et je ping plusieurs sites différents.

2) Ici on voit bien que les 10 paquets ont été envoyés et reçus pour la machine de mon voisin :

```
test@214-4:~$ ping 10.214.3.1 -c 10
PING 10.214.3.1 (10.214.3.1) 56(84) bytes of data.
64 bytes from 10.214.3.1: icmp_seq=1 ttl=64 time=0.412 ms
64 bytes from 10.214.3.1: icmp_seq=2 ttl=64 time=0.378 ms
64 bytes from 10.214.3.1: icmp_seq=3 ttl=64 time=0.368 ms
64 bytes from 10.214.3.1: icmp_seq=4 ttl=64 time=0.403 ms
64 bytes from 10.214.3.1: icmp_seq=5 ttl=64 time=0.417 ms
64 bytes from 10.214.3.1: icmp_seq=6 ttl=64 time=0.243 ms
64 bytes from 10.214.3.1: icmp_seq=7 ttl=64 time=0.357 ms
64 bytes from 10.214.3.1: icmp_seq=8 ttl=64 time=0.326 ms
64 bytes from 10.214.3.1: icmp_seq=9 ttl=64 time=0.395 ms
64 bytes from 10.214.3.1: icmp_seq=10 ttl=64 time=0.382 ms
--- 10.214.3.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9221ms
```

Ici on voit bien que les 10 paquets ont été envoyés et reçus pour pour le site www.lirmm.fr :

```
test@214-4:~$ ping www.lirmm.fr -c 10
PING pluton.lirmm.fr (193.49.104.251) 56(84) bytes of data.
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=1 ttl=55 time=14.0 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=2 ttl=55 time=12.4 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=3 ttl=55 time=7.77 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=4 ttl=55 time=13.0 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=5 ttl=55 time=13.5 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=6 ttl=55 time=9.38 ms
```

TP2 M1104

```
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=7 ttl=55 time=4.33 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=8 ttl=55 time=29.6 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=9 ttl=55 time=16.8 ms
64 bytes from pluton.lirmm.fr (193.49.104.251): icmp_seq=10 ttl=55 time=3.83 ms
--- pluton.lirmm.fr ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
```

Ici on voit bien que les 10 paquets ont été envoyés et reçus pour pour le site www.google.com :

```
test@214-4:~$ ping www.google.com -c 10
PING www.google.com (172.217.19.132) 56(84) bytes of data.
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=1 ttl=54 time=10.8 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=2 ttl=54 time=12.5 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=3 ttl=54 time=9.56 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=4 ttl=54 time=11.1 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=5 ttl=54 time=9.16 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=6 ttl=54 time=22.6 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=7 ttl=54 time=6.86 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=8 ttl=54 time=5.98 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=9 ttl=54 time=27.0 ms
64 bytes from par03s12-in-f132.1e100.net (172.217.19.132): icmp_seq=10 ttl=54 time=10.4
ms
--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
```

Ici on voit bien que les 10 paquets ont été envoyés et reçus pour pour le site www.nasa.gov :

```
test@214-4:~$ ping www.nasa.gov -c 10
PING iznasa.hs.llnwd.net (178.79.242.47) 56(84) bytes of data.
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=1 ttl=49 time=45.6
ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=2 ttl=49 time=46.2
ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=3 ttl=49 time=45.0
ms
```

TP2 M1104

```
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=4 ttl=49 time=44.8 ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=5 ttl=49 time=61.9 ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=6 ttl=49 time=45.1 ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=7 ttl=49 time=45.1 ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=8 ttl=49 time=44.8 ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=9 ttl=49 time=45.0 ms
64 bytes from https-178-79-242-47.fra.llnw.net (178.79.242.47): icmp_seq=10 ttl=49 time=44.8 ms

--- iznasa.hs.llnwd.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
```

En regardant les temps de transmission de chacun des paquets vers les sites on en déduit que le temps moyen pour l'envoi de 10 paquets est de 9000ms

3) Pour chaque machine on a 20 échanges qui ont lieu (10 pour l'envoi et 10 pour la réception). Pour le premier message envoyé à chaque adresse distante le protocole utilisé est l'ICMP. Son numéro de protocole est le numéro 1.

4) Adresse IP :

- Ma machine : 10.214.4.1

- Machine de mon voisin : 10.214.3.1

- Machine de www.lirmm.fr : 193.49.104.251

- Machine de www.google.com : 172.217.19.132

- Machine de www.nasa.gov : 178.79.242.47

5) Il y a des paquets ICMP qui n'ont pas de numéros de port destination ni source car ils sont inconnus.

6) Les autres champs qu'un paquets ICMP possède sont le type, le code, le jour de l'envoi…

2 octets soit 16 bits sont utilisés pour le cheeksum, le numéro de séquence et le champ d'identification.

TP2 M1104

2) Utilisation de traceroute

1) J'installe le mtr dans mon terminal grâce à la commande apt-get install mtr. Ensuite j'utilise la commande mtr Nom_Du_Site pour déterminer les routes utilisées pour accéder aux adresses.

Pour accéder au site www.lirmm.fr je passe par les routes suivantes :

```
10.214.255.254 ; GW.iutbeziers.fr ; 10.3.7.25 ; 193.55.200.8 ; r3lr5-tel-6-montpellier-rtr-021.noc.renater.fr ; deux routes quon ne connaît pas ; gate-e.lirmm.fr ; cs-lirmm.lirm.fr ; pluton.lirmm.fr
```

Pour accéder au site www.free.fr je passe par les routes suivantes :

```
10.214.255.254 ; GW.iutbeziers.fr ; 10.3.7.25 ; 193.55.200.8 ; xe1-0-3-marseille1-rtr-131.noc.renater.fr ; te0-6-0-2-lyon1-rtr-001.noc.renater.fr ; xe0-0-9-paris1-rtr-131.noc.renater.fr ; aub-6k-1.routers.proxad.net ; une route inconnue ; bzn-9k-4-be1004.intf.routers.proxad.net ; une autre route inconnue ; bzn-9k-2.sys.routers.proxad.net ; www.free.fr
```

Pour accéder au site www.google.com je passe par les routes suivantes :

```
10.214.255.254 ; GW.iutbeziers.fr ; 10.3.7.25 ; 193.55.200.8 ; xe0-0-3-marseille1-rtr-131.noc.renater.fr ; te1-1-marseille2-rtr-021.noc.renater.fr ; 72.14.218.132 ; 108.170.252.241 ; 66.249.95.43 ; par03s12-in-f132.1e100.net
```

Pour accéder au site www.nasa.gov je passe par les routes suivantes :

```
10.214.255.254 ; GW.iutbeziers.fr ; 10.3.7.25 ; 193.55.200.8 ; xe1-0-3-marseille1-rtr-131.noc.renater.fr ; 193.51.180.10 ; renater-ias-geant-gw.gen.ch.geant.net ; ae1.mx1.fra.de.geant.net ; une route inconnue ; vl2014.dr02.fra1.llnw.net ; https-178-79-242-47.fra.llnw.net
```

2) L'adresse www.i3S.unice.fr/I3S n'existe pas

Le serveur de l'adresse www.irit.fr se situe à Toulouse

```
root@214-4 : /home/test
# traceroute www.irit.fr
traceroute to www.irit.fr (141.115.28.2), 30 hops max, 60 byte packets
 1  gateway (10.214.255.254)  2.340 ms  2.688 ms  3.084 ms
 2  GW.iutbeziers.fr (194.199.227.254)  1.509 ms  1.522 ms  1.661 ms
 3  10.3.7.25 (10.3.7.25)  3.920 ms  3.452 ms  5.948 ms
 4  * * *
 5  te4-2-toulouse-rtr-021.noc.renater.fr (193.51.177.225)  5.921 ms  5.904 ms  5.900 ms
 6  remip-2000-te1-3-toulouse-rtr-021.noc.renater.fr (193.51.181.177)  5.880 ms  5.903 ms  5.907 ms
```

TP2 M1104

Le serveur de l'adresse www.irisa.fr se situe à Rennes

```
root@214-4 : /home/test
# traceroute www.irisa.fr
traceroute to www.irisa.fr (131.254.254.30), 30 hops max, 60 byte packets
 1  gateway (10.214.255.254)  2.509 ms  2.879 ms  3.302 ms
 2  GW.iutbeziers.fr (194.199.227.254)  1.425 ms  1.427 ms  1.683 ms
 3  10.3.7.25 (10.3.7.25)  6.002 ms  5.998 ms  5.959 ms
 4  * * *
 5  te4-2-toulouse-rtr-021.noc.renater.fr (193.51.177.225)  15.656 ms  15.630 ms  15.840 ms
 6  te4-1-bordeaux-rtr-021.noc.renater.fr (193.51.177.37)  15.093 ms  15.264 ms  15.248 ms
 7  te0-0-0-3-lyon1-rtr-001.noc.renater.fr (193.51.177.41)  13.492 ms  13.583 ms  13.843 ms
 8  * * *
 9  irisa-rennes-gi8-7-rennes-rtr-021.noc.renater.fr (193.51.181.169)  16.889 ms  15.007 ms
14.958 ms
```

Le serveur de l'adresse www.lifl.fr se situe à Lille

```
root@214-4 : /home/test
# traceroute www.lifl.fr
traceroute to www.lifl.fr (193.48.186.120), 30 hops max, 60 byte packets
 1  gateway (10.214.255.254)  6.649 ms  7.021 ms  7.420 ms
 2  GW.iutbeziers.fr (194.199.227.254)  1.381 ms  1.383 ms  1.198 ms
 3  10.3.7.25 (10.3.7.25)  3.194 ms  3.160 ms  3.177 ms
 4  * * *
 5  xe1-0-3-marseille1-rtr-131.noc.renater.fr (193.51.177.18)  18.888 ms  19.012 ms  18.872 ms
 6  193.51.180.12 (193.51.180.12)  18.833 ms  19.584 ms 193.51.180.10 (193.51.180.10)
19.475 ms
 7  193.51.180.62 (193.51.180.62)  14.807 ms 193.51.180.60 (193.51.180.60)  14.912 ms xe0-
0-9-paris1-rtr-131.noc.renater.fr (193.51.177.38)  15.074 ms
 8  * * *
 9  noropale-vl340-gi8-3-lille-rtr-021.noc.renater.fr (193.51.183.89)  18.086 ms  18.384 ms
18.651 ms
```

Toutes les routes commencent du même point et passent de routeurs en routeurs. Les routes commencent sur les routeurs de l'iut et ensuite partent dans des directions qui ne sont pas les

mêmes. En comparant mes résultats par rapport à l'infrastructure générale du réseau Renater je vois que les routes utilisées correspondent.

3) Je lance wireshark, je met des filtres et je lance la capture des paquets et sur le terminal je fais un traceroute d'un site situé en France.

4) Je sélectionne le premier message Requête ICMP et je vois que mon adresse IP est : 10.214.7.1

5) Dans l'en-tête du paquet IP la valeur du champ protocole de niveau supérieur est de 17 (UDP)

6) La taille totale du datagramme Ip est de 65 000 octets. 20 octets sont présents dans l'en-tête ip. La partie utile varie en fonction des données transmises.

7) Dans le premier cas (50 octets) le paquet n'est pas fragmenté mais dans le deuxième cas (2000 octets) le paquet est fragmenté. Pour savoir si un paquet est fragmenté il faut connaître sa taille (80 octets). Si la taille est dépassée alors le paquet sera fragmenté. La paquet ICMP réserve les champs de 31 à 62 bits (3ème octet) pour l'identification du fragment et les flags et offset.

9) En faisant un traceroute je peux identifier le routeur le plus proche de ma machine auquel le paquet est passé.

```
test@214-7:~$ traceroute www.google.fr
traceroute to www.google.fr (216.58.205.131), 30 hops max, 60 byte packets
 1  gateway (10.214.255.254)  2.291 ms  2.667 ms  3.066 ms
 2  GW.iutbeziers.fr (194.199.227.254)  1.904 ms  1.448 ms  1.860 ms
 3  10.3.7.25 (10.3.7.25)  25.082 ms  25.097 ms  25.092 ms
 4  * * *
 5  xe0-0-3-marseille1-rtr-131.noc.renater.fr (193.51.177.236)  29.065 ms  29.061 ms  29.046 ms
 6  te2-6-marseille2-rtr-021.noc.renater.fr (193.51.177.213)  30.723 ms  29.322 ms  28.901 ms
 7  72.14.218.132 (72.14.218.132)  27.135 ms  30.733 ms  30.983 ms
 8  108.170.252.242 (108.170.252.242)  28.126 ms  27.920 ms  27.881 ms
 9  209.85.253.104 (209.85.253.104)  29.124 ms 72.14.238.20 (72.14.238.20)  31.967 ms 209.85.253.104 (209.85.253.104)  28.413 ms
10  64.233.175.50 (64.233.175.50)  33.428 ms 108.170.245.81 (108.170.245.81)  33.444 ms 209.85.142.220 (209.85.142.220)  32.437 ms
11  108.170.245.65 (108.170.245.65)  33.672 ms  33.665 ms 216.239.42.13 (216.239.42.13)  32.911 ms
12  216.239.42.15 (216.239.42.15)  32.119 ms  32.610 ms  32.697 ms
13  mil04s27-in-f3.1e100.net (216.58.205.131)  32.648 ms  33.210 ms  32.701 ms
```

TP2 M1104

10) Ici on peut le voir avec la capture sur wireshark

No.	Time	Source	Destination	Protocol	Length	Info
29	2.061979117	194.199.227.254	10.214.7.1	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

11)