

COMPTE-RENDU TP9 RÉSEAU

Routage et résolution ARP

Pour ce TP voici mon adresse IP et le filtre sur Wireshark et arp or icmp

```
ouattumm@inf-36-13:~$ hostname -I
192.168.36.13
```

Exercice 1 :

4)

Current filter: arp						
No.	Time	Source	Destination	Protocol	Length	Info
44	6.224309736	Dell_6a:7f:9c	Broadcast	ARP	60	ARP Announcement for 192.168.36.5
48	6.244097407	Dell_6a:7f:9c	Broadcast	ARP	60	Who has 192.168.36.254? Tell 192.168.36.5
77	8.224782613	Dell_6a:7f:9c	Broadcast	ARP	60	ARP Announcement for 192.168.36.5
95	10.225476610	Dell_6a:7f:9c	Broadcast	ARP	60	ARP Announcement for 192.168.36.5
194	21.472198735	Dell_4a:87:f6	Broadcast	ARP	60	Who has 192.168.36.11? Tell 192.168.36.254
222	26.298832756	Dell_6a:c7:01	Broadcast	ARP	60	ARP Announcement for 192.168.36.16
225	26.328596814	Dell_6a:c7:01	Broadcast	ARP	60	Who has 192.168.36.254? Tell 192.168.36.16
268	28.299478299	Dell_6a:c7:01	Broadcast	ARP	60	ARP Announcement for 192.168.36.16
288	30.128874888	Dell_6a:c7:01	Broadcast	ARP	60	ARP Announcement for 192.168.36.16
317	31.389629030	Dell_e0:3d:b3	Broadcast	ARP	60	Who has 192.168.36.13? Tell 192.168.36.11
318	31.389676022	Dell_6a:7e:a3	Dell_e0:3d:b3	ARP	42	192.168.36.13 is at a4:bb:6d:6a:7e:a3
355	38.069993263	Dell_6a:7f:b2	Broadcast	ARP	60	ARP Announcement for 192.168.36.3
856	58.096029127	Dell_6a:7f:b2	Broadcast	ARP	60	Who has 192.168.36.254? Tell 192.168.36.3
861	58.140850268	Dell_e0:3d:b3	Broadcast	ARP	60	Who has 192.168.36.18? Tell 192.168.36.11
892	60.070690030	Dell_6a:7f:b2	Broadcast	ARP	60	ARP Announcement for 192.168.36.3
907	62.070712678	Dell_6a:7f:b2	Broadcast	ARP	60	ARP Announcement for 192.168.36.3

Envoie d'une demande d'une machine qui a l'adresse IP 192.168.36.11, pour une résolution d'adresse IP pour connaître l'adresse physique de la machine qui a l'adresse IP 192.168.36.13. La machine a reçu une réponse.

Quand les machines sont dans le même réseau local, il y a un paquet ARP qui part en mode broadcast et qui demande à toutes les machines qui à cette adresse IP. Les machines demandent une résolution d'adresse sur une adresse IP et en même temps sur son adresse. Si il y a une réponse la machine sait qu'une autre machine a pris son IP.

5) Avec la commande **ping -w 60 192.168.36.5** j'envoie une demande ARP pour connaître l'adresse physique de l'IP passée en paramètre. Elle envoie pendant 60 secondes des paquets de demande d'écho (ICMP) en continu. Et j'obtiens la capture suivante :

19	2.031398528	Dell_6a:7e:a3	Dell_6a:7f:9c	ARP	42	Who has 192.168.36.5? Tell 192.168.36.13
20	2.032446440	Dell_6a:7f:9c	Dell_6a:7e:a3	ARP	60	192.168.36.5 is at a4:bb:6d:6a:7f:9c
24	2.842743447	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=7/1792, ttl=64
25	2.844023920	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=7/1792, ttl=64
30	3.844253461	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=8/2048, ttl=64
31	3.845434733	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=8/2048, ttl=64
40	4.845700449	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=9/2304, ttl=64
41	4.846761913	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64
46	5.847275569	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=10/2560, ttl=64
47	5.848699850	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64
55	6.848954150	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=11/2816, ttl=64
56	6.850004368	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64
61	7.850527799	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=12/3072, ttl=64
62	7.851976276	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=12/3072, ttl=64
67	8.852186174	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=13/3328, ttl=64
68	8.853609286	192.168.36.5	192.168.36.13	ICMP	98	Echo (ping) reply id=0x0001, seq=13/3328, ttl=64
73	9.853905110	192.168.36.13	192.168.36.5	ICMP	98	Echo (ping) request id=0x0001, seq=14/3584, ttl=64

6) Ce qui se passe quand tente de faire un ping sur une IP qui n'existe pas, c'est qu'on va envoyer une demande ARP sans jamais avoir de réponse. Au niveau de la réponse on va recevoir un timeout. Et au niveau de ICMP on a l'erreur : « Destination Host Unreachable ».

```

ouattumm@inf-36-13:~$ ping -w 60 192.168.36.170
PING 192.168.36.170 (192.168.36.170) 56(84) bytes of data.
From 192.168.36.13 icmp_seq=1 Destination Host Unreachable
From 192.168.36.13 icmp_seq=2 Destination Host Unreachable
From 192.168.36.13 icmp_seq=3 Destination Host Unreachable

--- 192.168.36.170 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3076ms
pipe 4
ouattumm@inf-36-13:~$

```

De plus, on peut remarquer que c'est ma machine qui réponds à ma machine.

1	0.000000000	Dell_6a:82:b9	ARP	62	Who has 192.168.36.155? Tell 192.168.36.7
2	0.777948506	Dell_6a:7e:a3	ARP	44	Who has 192.168.36.170? Tell 192.168.36.13
3	1.011460231	Dell_6a:82:b9	ARP	62	Who has 192.168.36.155? Tell 192.168.36.7
4	1.784253837	Dell_6a:7e:a3	ARP	44	Who has 192.168.36.170? Tell 192.168.36.13
5	2.035283920	Dell_6a:82:b9	ARP	62	Who has 192.168.36.155? Tell 192.168.36.7
6	2.808238872	Dell_6a:7e:a3	ARP	44	Who has 192.168.36.170? Tell 192.168.36.13
7	3.059500529	Dell_6a:82:b9	ARP	62	Who has 192.168.36.155? Tell 192.168.36.7
8	3.822272907	Dell_6a:7e:a3	ARP	44	Who has 192.168.36.170? Tell 192.168.36.13
9	3.832272907	192.168.36.13	ICMP	128	Destination unreachable (Host unreachable)
10	3.832282088	192.168.36.13	ICMP	128	Destination unreachable (Host unreachable)
11	3.832288121	192.168.36.13	ICMP	128	Destination unreachable (Host unreachable)
12	4.000000000	Dell_6a:82:b9	ARP	62	Who has 192.168.36.155? Tell 192.168.36.7
13	4.856221420	Dell_6a:7e:a3	ARP	44	Who has 192.168.36.170? Tell 192.168.36.13
14	5.107274181	Dell_6a:82:b9	ARP	62	Who has 192.168.36.155? Tell 192.168.36.7
15	5.879903889	Dell_6a:7e:a3	ARP	44	Who has 192.168.36.170? Tell 192.168.36.13
16	6.903930713	192.168.36.13	ICMP	128	Destination unreachable (Host unreachable)
17	8.117582365	fe80::b52e:e167:6c8... ff02::fb	MDNS	394	Standard query 0x0000 PTR _ftp._tcp.local,
18	8.117582665	192.168.36.16	MDNS	374	Standard query 0x0000 PTR _ftp._tcp.local,

7) Comme c'est une adresse IP externe il va demander l'adresse du routeur. Le routeur sait qu'elle est la passerelle car il l'a connaît par défaut. Avec l'adresse de la passerelle, il va dire quelle est l'adresse MAC de la machine qui a telle adresse IP (ici sncf.fr) et le routeur va envoyer au bon réseau. L'autre routeur qui est dans l'autre sous réseau va re dispatcher le message en disant qui a l'adresse IP (IP de destination)

```

umm-habibah@ummhabibah:~$ ping -D sncf.fr
PING sncf.fr (99.83.160.166) 56(84) bytes of data.
[1680364221.244782] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=1 ttl=123 time=28.8 ms
[1680364222.006268] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=2 ttl=123 time=26.3 ms
[1680364223.009027] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=3 ttl=123 time=28.2 ms
[1680364224.009365] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=4 ttl=123 time=28.0 ms
[1680364225.010205] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=5 ttl=123 time=28.4 ms
[1680364226.011303] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=6 ttl=123 time=28.7 ms
[1680364227.011587] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=7 ttl=123 time=27.9 ms
[1680364228.010149] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=8 ttl=123 time=26.1 ms
[1680364229.012705] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=9 ttl=123 time=28.5 ms
[1680364230.013478] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=10 ttl=123 time=28.3 ms
[1680364231.011030] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=11 ttl=123 time=25.1 ms
[1680364232.014894] 64 bytes from a4c1c7cf05ecf6b65.awsglobalaccelerator.com (99.83.160.166): icmp_seq=12 ttl=123 time=28.5 ms
^C

```

En revanche pour voir le nombre de saut, la commande **ping -R sncf.fr** ou **ping -R univ-rouen.fr** ne fonctionne pas.

8) En faisant un ping sur l'adresse 10.1.2.3. Le routeur c'est que l'adresse est à l'extérieur. Comme le routeur n'a pas dans sa table de routage l'adresse, il ne peut pas l'atteindre, donc il va répondre que l'adresse de destination n'est pas joignable via ICMP.

```

umm-habibah@ummhabibah:~$ ping -w 60 10.1.2.3
PING 10.1.2.3 (10.1.2.3) 56(84) bytes of data.

--- 10.1.2.3 ping statistics ---
59 packets transmitted, 0 received, 100% packet loss, time 59370ms

```


Exercice 2 :

5) En faisant la commande **tracert -I www.univ-rouen.fr**, j'obtiens la liste de chaque saut qui sont effectués entre la source (mon PC) et la destination (le site de l'université).

```
umm-habibah@ummhabibah:~$ tracert -I www.univ-rouen.fr
tracert to www.univ-rouen.fr (193.52.152.49), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.254) 0.976 ms 1.157 ms 2.161 ms
 2 * station9.multimania.isdnet.net (194.149.174.106) 27.239 ms *
 3 * * *
 4 193.51.187.208 (193.51.187.208) 45.621 ms 46.026 ms 46.004 ms
 5 et-2-0-2-ren-nr-paris1-rtr-131.noc.renater.fr (193.55.204.192) 45.988 ms 45.963 ms 45.950 ms
 6 te0-0-0-8-ren-nr-rouen-rtr-091.noc.renater.fr (193.55.204.228) 45.923 ms 35.990 ms 36.608 ms
 7 syrhamo-vl3201-te4-3-rouen-rtr-021.noc.renater.fr (193.51.184.129) 36.573 ms 25.454 ms 26.472 ms
 8 * * *
 9 * * *
10 193.51.187.208 (193.51.187.208) 35.716 ms 36.514 ms 37.157 ms
11 woel.univ-rouen.fr (193.52.152.49) 32.379 ms 27.092 ms 26.552 ms
12 woel.univ-rouen.fr (193.52.152.49) 27.184 ms 28.493 ms 27.150 ms
13 woel.univ-rouen.fr (193.52.152.49) 29.145 ms 30.336 ms 27.176 ms
umm-habibah@ummhabibah:~$
```

Il y a la liste de chaque saut effectué, entre la source et la destination et le temps moyen aller-retour. Le saut 13 indique qu'on a atteint la destination, c'est-à-dire le serveur de l'université

3) En faisant la même commande mais avec wireshark en appliquant le filtre ICMP, voici ce que j'obtiens comme résultat : **je n'ai mis que la partie intéressante**

65 0.102616217	193.52.152.49	192.168.0.15	ICMP	102Time-to-live exceeded (Time to live exceeded in transit)
66 0.102777182	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=38/9728, ttl=13 (reply in 81)
67 0.103989529	193.52.152.49	192.168.0.15	ICMP	102Time-to-live exceeded (Time to live exceeded in transit)
68 0.104152216	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=39/9984, ttl=13 (reply in 82)
69 0.111611940	193.52.152.49	192.168.0.15	ICMP	102Time-to-live exceeded (Time to live exceeded in transit)
70 0.111795519	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=40/10240, ttl=14 (reply in 84)
73 0.120031772	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=41/10496, ttl=14 (reply in 85)
74 0.124000648	193.52.152.49	192.168.0.15	ICMP	70Time-to-live exceeded (Time to live exceeded in transit)
75 0.124195855	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=42/10752, ttl=14 (reply in 86)
76 0.126846393	193.52.152.49	192.168.0.15	ICMP	70Time-to-live exceeded (Time to live exceeded in transit)
77 0.127037822	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=43/11008, ttl=15 (reply in 87)
78 0.127915983	193.52.152.49	192.168.0.15	ICMP	70Time-to-live exceeded (Time to live exceeded in transit)
79 0.128120162	192.168.0.15	193.52.152.49	ICMP	74Echo (ping) request id=0x0002, seq=44/11264, ttl=15 (reply in 88)
80 0.129391489	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=37/9472, ttl=52 (request in 64)
81 0.129756650	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=38/9728, ttl=52 (request in 66)
82 0.131117511	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=39/9984, ttl=52 (request in 68)
84 0.138557914	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=40/10240, ttl=52 (request in 70)
85 0.145958864	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=41/10496, ttl=52 (request in 73)
86 0.151338403	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=42/10752, ttl=52 (request in 75)
87 0.152275831	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=43/11008, ttl=52 (request in 77)
88 0.155024211	193.52.152.49	192.168.0.15	ICMP	74Echo (ping) reply id=0x0002, seq=44/11264, ttl=52 (request in 79)

Le message de réponse d'écho ICMP est envoyé de l'université à mon PC pour ttl=52. La source a envoyé la requête dns au routeur pour la recherche dns www.univ-rouen.fr. Le routeur a envoyé la réponse à la source.

Exercice 3 :

1)

Nom	Réseau	IP
Poste de travail 1	10.0.3.0	10.0.3.25
Poste de travail 2	10.0.3.0	10.0.3.26
Routeur utilisateur	10.0.3.0	10.0.3.1
Routeur serveur	192.168.80.0	192.168.80.1
Serveur mail.l3info	192.168.80.0	192.168.80.15

Serveur ns.l3info.net	192.168.80.0	192.168.80.5
Serveur www.l3info.net	192.168.80.0	192.168.80.10
