

COMPTE-RENDU TP1 RÉSEAU

Couches réseau, capture et DNS

Exercice 2 : Capture et filtrage

1) En faisant la commande `habibah@ummhahibah:~$ ping univ-rouen.fr -c5` j'obtiens la capture ci-dessous :

No.	Time	Source	Destination	Protocol	Length	Info
10.000000000	192.168.0.15	192.168.0.254	DNS	84	Standard query 0xe49b AAAA univ-rouen.fr OPT	
20.029746822	192.168.0.254	192.168.0.15	DNS	138	Standard query response 0xe49b AAAA univ-rouen.fr SOA nommay.univ-rouen.fr OPT	
30.031034350	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (reply in 4)	
40.059412393	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256, ttl=52 (request in 3)	
51.033062511	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=2/512, ttl=64 (reply in 6)	
61.061349829	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=2/512, ttl=52 (request in 5)	
72.034721495	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=3/768, ttl=64 (reply in 8)	
82.062214313	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=3/768, ttl=52 (request in 7)	
93.036496972	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=4/1024, ttl=64 (reply in 10)	
103.065076555	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=4/1024, ttl=52 (request in 9)	
113.085909720	fe80::6aa3:78ff:fe0...	ff02::1:ff55:8a27	ICMPv6	86	Neighbor Solicitation for 2a01:e0a:41f:a770:a2e2:5d8f:c855:8a27 from 68:a3:78:05:3b:1f	
123.085977903	2a01:e0a:41f:a770:a...	fe80::6aa3:78ff:fe0...	ICMPv6	86	Neighbor Advertisement 2a01:e0a:41f:a770:a2e2:5d8f:c855:8a27 (sol, ovr) is at e4:a7:a0:d9:c4:39	
134.038455529	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=5/1280, ttl=64 (reply in 14)	
144.066130353	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=5/1280, ttl=52 (request in 13)	
155.152089423	IntelCor_d9:c4:39	FreeboxS_05:3b:1f	ARP	42	Who has 192.168.0.254? Tell 192.168.0.15	
165.154227280	FreeboxS_05:3b:1f	IntelCor_d9:c4:39	ARP	42	Who has 192.168.0.15? Tell 192.168.0.254	
175.154227571	FreeboxS_05:3b:1f	IntelCor_d9:c4:39	ARP	42	192.168.0.254 is at 68:a3:78:05:3b:1f	
185.154262933	IntelCor_d9:c4:39	FreeboxS_05:3b:1f	ARP	42	192.168.0.15 is at e4:a7:a0:d9:c4:39	

Les protocoles capturés sont :

- DNS, correspond à la couche application du modèle OSI
- ICMP, correspond à la couche réseau du modèle OSI
- ICMPv6, correspond à la couche réseau du modèle OSI
- ARP, correspond à la couche réseau du modèle OSI

2) Les différents protocoles identifiés sont :

- IPv4, couche réseau du modèle OSI
- UDP, couche transport du modèle OSI
- DNS, couche applicative du modèle OSI

3) Les paquets correspondants au ping nous donne comme information :

- l'adresse IP de destination / de source
- la longueur du paquet en octet
- les protocoles
- les informations sur le contenu des paquets
- combien de temps après la capture le paquet a été capturé

4) Dans mon cas la résolution de nom est nommay.univ-rouen.fr. J'ai trouvé cette information dans le paquet DNS.

```
Domain Name System (response)
  Transaction ID: 0xe49b
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 1
  Queries
    univ-rouen.fr: type AAAA, class IN
  Authoritative nameservers
    univ-rouen.fr: type SOA, class IN, mname nommay.univ-rouen.fr
```

5) En définissant comme filtre ICMP les paquets de ping, j'obtiens, la capture ci-dessous :

No.	Time	Source	Destination	Protocol	Length	Info
3	0.031034350	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (reply in 4)
4	0.059412393	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256, ttl=52 (request in 3)
5	1.033062511	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=2/512, ttl=64 (reply in 6)
6	1.061349829	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=2/512, ttl=52 (request in 5)
7	2.034721495	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=3/768, ttl=64 (reply in 8)
8	2.062214313	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=3/768, ttl=52 (request in 7)
9	3.036496972	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=4/1024, ttl=64 (reply in 10)
10	3.065076555	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=4/1024, ttl=52 (request in 9)
13	4.038455529	192.168.0.15	193.52.152.49	ICMP	98	Echo (ping) request id=0x0002, seq=5/1280, ttl=64 (reply in 14)
14	4.066130353	193.52.152.49	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0002, seq=5/1280, ttl=52 (request in 13)

Et on peut remarquer que :

- dans la barre de filtre il y a icmp qui apparaît dans un fond vert
- il n'y a que les protocoles icmp affichés
- on voit les adresses sources et destinataires

6) En refaisant un ping mais sur l'adresse IP 172.16.3.1

```
habibah@ummhbabah:~$ ping 172.16.3.1 -c5
PING 172.16.3.1 (172.16.3.1) 56(84) bytes of data.

--- statistiques ping 172.16.3.1 ---
5 paquets transmis, 0 reçus, 100 % paquets perdus, temps 4093 ms
```

On obtient la capture suivantes :

No.	Time	Source	Destination	Protocol	Length	Info
320	3.316127923	192.168.0.15	172.16.3.1	ICMP	98	Echo (ping) request id=0x0004, seq=1/256, ttl=64 (no response found!)
473	4.337490548	192.168.0.15	172.16.3.1	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=64 (no response found!)
636	5.361471880	192.168.0.15	172.16.3.1	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=64 (no response found!)
792	6.389432644	192.168.0.15	172.16.3.1	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (no response found!)
940	7.409490364	192.168.0.15	172.16.3.1	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280, ttl=64 (no response found!)

Je constate que la destination ne réponds pas et que dans les colonnes source on a toujours la même adresse IP 192.168.0.15 et dans la colonne destination on a la même adresse 172.16.3.1. Il n'y a pas d'échange effectué.

7) Cette fois-ci dans la barre de filtre il y a **ip.dst == 193.52.152.49**

8) En remplaçant ip.dst par ip.addr, on revient au résultat de la question 6)

Exercice 3 : DNS

4) La commande permet d'afficher le contenu du fichier. namserver indique les serveurs DNS du système.

5)

```
habibah@ummhabibah:~$ dig www.univ-rouen.fr

; <<>> DiG 9.16.1-Ubuntu <<>> www.univ-rouen.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52450
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.univ-rouen.fr.                IN      A

;; ANSWER SECTION:
www.univ-rouen.fr.                600     IN      CNAME   woel.univ-rouen.fr.
woel.univ-rouen.fr.              1020    IN      A       193.52.152.49

;; Query time: 31 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: jeu. févr. 02 21:46:59 CET 2023
;; MSG SIZE rcvd: 81
```

On obtient 2 réponses : et on se rends compte que univ-rouen.fr n'est pas le vrai nom de domaine de l'université, c'est en faite un alias de woel.univ-rouen.fr et woel.univ-rouen.fr correspond à une adresse machine.

2 réponses

www.univ-rouen.fr
woel.univ-rouen.fr

Type

CNAME
A

woel.univ-rouen.fr
adIPv4

Adresse machine

synonyme

6)

```
umm-habibah@ummhabibah:~$ dig mail.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65280
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mail.google.com.                IN      A

;; ANSWER SECTION:
mail.google.com.                34      IN      A       142.250.179.101

;; Query time: 367 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: ven. janv. 27 18:34:22 CET 2023
;; MSG SIZE rcvd: 60
```

```

umm-habibah@ummhabibah:~$ dig drive.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> drive.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30580
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;drive.google.com.                IN      A

;; ANSWER SECTION:
drive.google.com.                262     IN      A      142.250.74.238

;; Query time: 567 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: ven. janv. 27 18:36:07 CET 2023
;; MSG SIZE rcvd: 61

```

drive.google.com et mail.google.com sont de même type, ce sont des adresses machines, ce ne sont pas des alias. Pour un nom de domaine qui n'existe pas, en faisant la commande **dig mail.google.azert**, ce qu'il va changer est dans le header. En effet, au lieu d'avoir l'attribut NOERROR dans le champs status on aura l'attribut NXDOMAIN.

7) et 9) La commande **dig www.univ-rouen.fr +trace** nous permet d'avoir l'ordre des serveurs interrogés dans un service DNS. On part de la racine pour arriver jusqu'à l'adresse complète. On choisit en premier une adresse racine, par exemple a, et à partir de cette adresse on fait un appel à dig sur une autre adresse jusqu'à ce qu'on ait dans les réponses une adresse avec un type A.

Voici un exemple itérative de requête DNS :

```

dig @a.root-serveur.net NS fr +norecurse
dig @g.ext.nic.fr. univ-rouen.fr +norecurse
dig @ns.crihan.fr. univ-rouen.fr +norecurse

```

```

.          9257      IN      NS      b.root-servers.net.
.          9257      IN      NS      l.root-servers.net.
.          9257      IN      NS      g.root-servers.net.
.          9257      IN      NS      a.root-servers.net.
.          9257      IN      NS      h.root-servers.net.
.          9257      IN      NS      f.root-servers.net.
.          9257      IN      NS      m.root-servers.net.
.          9257      IN      NS      c.root-servers.net.
.          9257      IN      NS      k.root-servers.net.
.          9257      IN      NS      e.root-servers.net.
.          9257      IN      NS      d.root-servers.net.
.          9257      IN      NS      i.root-servers.net.
.          9257      IN      NS      j.root-servers.net.
;; Received 262 bytes from 127.0.0.53#53(127.0.0.53) in 660 ms

```

8) Pour savoir la durée de vie de chaque enregistrement il faut faire la commande **dig SOA univ-rouen.fr** et regarder le dernier argument

```

;; ANSWER SECTION:
univ-rouen.fr.      3600      IN      SOA      nommay.univ-rouen.fr. postmaster.univ-rouen.fr. 2014126150 1200 3600 1209600 3600

```

D'après cette commande la durée de vie est de 3600s. Cette valeur sert à savoir la durée maximal de univ-rouen.fr dans les serveurs secondaires

10) **dig mx** permet de savoir quels sont les serveurs de messagerie utilisé par un nom de domaine. Par exemple pour le nom de domaine univ-rouen.fr, le nom du serveur de courrier du domaine est smtp.univ-rouen.fr.