Thibaut LEFRANCOIS D2

> Adresse IP : 10.192.51.94 Adresse @MAC : 08:00:27:17:51:94 Nom de la machine : vmsparc04.univ-lr.fr

Question 1 : Prise en main de Wireshark

1. Analyse globale

Capture en mode espion de l'expérimentation demandée : `ping -c4 impll304.univ-lr.fr`.

a. 20 premières lignes affichées :

```
No.     Time        Source              Destination         Protocol Length Info
    1 0.000000000   Dell_1c:51:d8       Broadcast           ARP      60  Who has
10.192.150.99? Tell 10.192.0.250
    2 0.073420404   10.192.0.250        224.0.0.18          VRRP     70
Announcement (v2)
    3 0.318028735   ::                  ff02::16            ICMPv6   130
Multicast Listener Report Message v2
    4 0.318800127   ::                  ff02::fb            ICMPv6   90
Multicast Listener Query
    5 0.869226330   Dell_1c:51:d8       Broadcast           ARP      60  Who has
10.192.150.241? Tell 10.192.0.250
    6 1.150021705   HewlettP_aa:0a:a5   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x805b
    7 1.317956584   ::                  ff02::16            ICMPv6   130
Multicast Listener Report Message v2
    8 1.330831619   ::                  ff02::fb            ICMPv6   90
Multicast Listener Query
    9 1.669406656   10.192.51.94        10.192.50.49        ICMP     98  Echo
(ping) request  id=0x16a0, seq=1/256, ttl=64 (reply in 10)
    10 1.671314840  10.192.50.49        10.192.51.94        ICMP     98  Echo
(ping) reply    id=0x16a0, seq=1/256, ttl=60 (request in 9)
    11 2.083606282  10.192.0.250        224.0.0.18          VRRP     70
Announcement (v2)
    12 2.671516315  10.192.51.94        10.192.50.49        ICMP     98  Echo
(ping) request  id=0x16a0, seq=2/512, ttl=64 (reply in 13)
    13 2.673145446  10.192.50.49        10.192.51.94        ICMP     98  Echo
(ping) reply    id=0x16a0, seq=2/512, ttl=60 (request in 12)
    14 3.145220855  0.0.0.0             255.255.255.255     DHCP     342 DHCP
Discover - Transaction ID 0xafae220b
    15 3.149882617  HewlettP_aa:0a:a5   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x805b
    16 3.643568389  Dell_ea:c3:fa       Broadcast           ARP      60  Who has
10.192.55.44? Tell 10.192.51.120
    17 3.673765970  10.192.51.94        10.192.50.49        ICMP     98  Echo
(ping) request  id=0x16a0, seq=3/768, ttl=64 (reply in 18)
    18 3.675716653  10.192.50.49        10.192.51.94        ICMP     98  Echo
(ping) reply    id=0x16a0, seq=3/768, ttl=60 (request in 17)
    19 4.093090335  10.192.0.250        224.0.0.18          VRRP     70
```

```
Announcement (v2)
    20 4.567279447  fe80::3c35:219c:5d2e:5feb ff02::fb              MDNS    107
Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local,
"QM" question
    21 4.623569551  Dell_ea:c3:fa       Broadcast           ARP     60  Who has
10.192.55.44? Tell 10.192.51.120
    22 4.675930851  10.192.51.94        10.192.50.49        ICMP    98  Echo
(ping) request  id=0x16a0, seq=4/1024, ttl=64 (reply in 23)
```

b. Les protocoles de niveau haut capturés sont : ARP / VRRP / ICMPv6 / ICMP / DHCP / MDNS / STP.

c. Le protocole communément utilisé dans toutes les trames au niveau de la couche liaison de données est le protocole Ethernet. Il est du niveau bas car il est le plus proche de la couche physique.

---

2. Filtrage

a. J'ai utilisé le filtre `eth.addr == 08:00:27:17:51:94` pour ne garder que les trames de la machine à l'aide de mon adresse MAC

b. Voici les trames filtrées destinées à ma machine sans détails des protocoles encapsulés ni le contenu hexadécimal :

```
No.     Time        Source              Destination         Protocol Length Info
    9 1.669406656   10.192.51.94        10.192.50.49        ICMP    98  Echo
(ping) request  id=0x16a0, seq=1/256, ttl=64 (reply in 10)
    10 1.671314840  10.192.50.49        10.192.51.94        ICMP    98  Echo
(ping) reply    id=0x16a0, seq=1/256, ttl=60 (request in 9)
    12 2.671516315  10.192.51.94        10.192.50.49        ICMP    98  Echo
(ping) request  id=0x16a0, seq=2/512, ttl=64 (reply in 13)
    13 2.673145446  10.192.50.49        10.192.51.94        ICMP    98  Echo
(ping) reply    id=0x16a0, seq=2/512, ttl=60 (request in 12)
    17 3.673765970  10.192.51.94        10.192.50.49        ICMP    98  Echo
(ping) request  id=0x16a0, seq=3/768, ttl=64 (reply in 18)
    18 3.675716653  10.192.50.49        10.192.51.94        ICMP    98  Echo
(ping) reply    id=0x16a0, seq=3/768, ttl=60 (request in 17)
    22 4.675930851  10.192.51.94        10.192.50.49        ICMP    98  Echo
(ping) request  id=0x16a0, seq=4/1024, ttl=64 (reply in 23)
    23 4.677614655  10.192.50.49        10.192.51.94        ICMP    98  Echo
(ping) reply    id=0x16a0, seq=4/1024, ttl=60 (request in 22)
```

c. Malheuresement le test a été fait plusieurs fois et je n'ai donc qu'un protocole qui reste affiché qui est : ICMP (ping).

---

3. Récupération d'information

a-b-c. A l'aide de wireshark, j'ai analysé les détails d'une trame "reply", toujours à l'aide du filtre `eth.addr == 08:00:27:17:51:94` et retrouve à l'aide des protocoles, l'adresse IP et l'adresse MAC de la machine ainsi que de l'imprimante :

```
Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src (l'adresse MAC l'imprimante) (00:10:83:53:e0:e2), Dst (mon
adresse Mac) (08:00:27:17:51:94)
Internet Protocol Version 4, Src (l'adresse IP de l'imprimante) (10.192.50.49),
Dst (mon adresse IP) (10.192.51.94)
Internet Control Message Protocol
```

L'adresse MAC de la machine est donc `08:00:27:17:51:94` et l'adresse IP est `10.192.51.94`.

d. Je pense que le champ de contrôle d'erreur du niveau de la couche liaison de données n'est pas toujours présenté par Wireshark car il peut être calculé et vérifié en interne par le matériel de réseau (par exemple, une carte réseau) avant que les données ne soient transmises à la couche logicielle.

Question 2

1. Analyse globale

Capture en mode espion de l'expérimentation demandée (lancé la page) : `http://serverrx.univ-lr.fr/`.

```
No.     Time        Source              Destination         Protocol Length Info
    1 0.000000000   10.192.51.94        10.1.30.18          TCP      105 54852 →
3128 [PSH, ACK] Seq=110074633 Ack=1058401821 Win=501 Len=39 TSval=1459626635
TSecr=2069227191
    2 0.056267620   10.1.30.18          10.192.51.94        TCP      105 3128 →
54852 [PSH, ACK] Seq=1058401821 Ack=110074672 Win=147 Len=39 TSval=2069228466
TSecr=1459626635
    3 0.056287156   10.192.51.94        10.1.30.18          TCP      66  54852 →
3128 [ACK] Seq=110074672 Ack=1058401860 Win=501 Len=0 TSval=1459626691
TSecr=2069228466
    4 0.064617575   10.192.51.94        34.107.221.82       TCP      74  33942 → 80
[SYN] Seq=240844166 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1420220023 TSecr=0
WS=128
    5 0.297489366   10.192.100.2        10.192.255.255      NBNS     92  Name query
NB KIOSKL02<1c>
    6 0.317157540   10.192.51.94        34.107.221.82       TCP      74  33944 → 80
[SYN] Seq=1197311654 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1420220275 TSecr=0
WS=128
    7 0.761195674   10.192.0.250        224.0.0.18          VRRP     70
Announcement (v2)
    8 0.831122155   HewlettP_aa:0a:a5   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x805b
    9 1.058215763   10.192.51.94        10.2.40.230         DNS      90  Standard
query 0x01e7 A serverrx.univ-lr.fr OPT
    10 1.058341140  10.192.51.94        10.2.40.230         DNS      90  Standard
query 0xa059 AAAA serverrx.univ-lr.fr OPT
    11 1.063433334  10.192.51.94        34.107.221.82       TCP      74  33942 → 80
[SYN] Seq=240844166 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1420221021 TSecr=0
WS=128
    12 1.092400575  10.2.40.230         10.192.51.94        DNS      106 Standard
```

```
query response 0x01e7 A serverrx.univ-lr.fr A 10.192.50.253 OPT
    13 1.092422511  10.2.40.230         10.192.51.94        DNS     143 Standard
query response 0xa059 AAAA serverrx.univ-lr.fr SOA middas.univ-lr.fr OPT
    14 1.092969595  PcsCompu_17:51:94   Broadcast           ARP     42  Who has
10.192.50.253? Tell 10.192.51.94
    15 1.093182797  10.192.100.2        10.192.255.255      NBNS    92  Name query
NB KIOSKL02<1c>
    16 1.093439356  HewlettP_05:05:ba   PcsCompu_17:51:94   ARP     60
10.192.50.253 is at 00:1f:29:05:05:ba
    17 1.093447091  10.192.51.94        10.192.50.253       TCP     74  39948 → 80
[SYN] Seq=2003138522 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3886404408 TSecr=0
WS=128
    18 1.093741816  10.192.50.253       10.192.51.94        TCP     74  80 → 39948
[SYN, ACK] Seq=3618063222 Ack=2003138523 Win=28960 Len=0 MSS=1460 SACK_PERM=1
TSval=773916104 TSecr=3886404408 WS=128
    19 1.093772620  10.192.51.94        10.192.50.253       TCP     66  39948 → 80
[ACK] Seq=2003138523 Ack=3618063223 Win=64256 Len=0 TSval=3886404409
TSecr=773916104
    20 1.094021767  10.192.51.94        10.192.50.253       HTTP    425 GET /
HTTP/1.1
    21 1.094345377  10.192.50.253       10.192.51.94        TCP     66  80 → 39948
[ACK] Seq=3618063223 Ack=2003138882 Win=30080 Len=0 TSval=773916104
TSecr=3886404409
    22 1.094549766  10.192.50.253       10.192.51.94        HTTP    1514
HTTP/1.1 200 OK  (text/html)
    23 1.094556516  10.192.51.94        10.192.50.253       TCP     66  39948 → 80
[ACK] Seq=2003138882 Ack=3618064671 Win=64128 Len=0 TSval=3886404410
TSecr=773916104
    24 1.094573095  10.192.50.253       10.192.51.94        HTTP    1037
Continuation
    25 1.094577507  10.192.51.94        10.192.50.253       TCP     66  39948 → 80
[ACK] Seq=2003138882 Ack=3618065642 Win=63488 Len=0 TSval=3886404410
TSecr=773916104
    26 1.094580645  10.192.50.253       10.192.51.94        TCP     66  80 → 39948
[FIN, ACK] Seq=3618065642 Ack=2003138882 Win=30080 Len=0 TSval=773916104
TSecr=3886404409
    27 1.094840424  10.192.51.94        10.192.50.253       TCP     66  39948 → 80
[FIN, ACK] Seq=2003138882 Ack=3618065643 Win=64128 Len=0 TSval=3886404410
TSecr=773916104
    28 1.095131388  10.192.50.253       10.192.51.94        TCP     66  80 → 39948
[ACK] Seq=3618065643 Ack=2003138883 Win=30080 Len=0 TSval=773916104
TSecr=3886404410
    29 1.319799640  10.192.51.94        34.107.221.82       TCP     74  33944 → 80
[SYN] Seq=1197311654 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1420221278 TSecr=0
WS=128
    30 1.376242183  10.192.51.94        10.192.50.253       TCP     74  39950 → 80
[SYN] Seq=2479527617 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3886404691 TSecr=0
WS=128
    31 1.376547773  10.192.50.253       10.192.51.94        TCP     74  80 → 39950
[SYN, ACK] Seq=1308100622 Ack=2479527618 Win=28960 Len=0 MSS=1460 SACK_PERM=1
TSval=773916175 TSecr=3886404691 WS=128
    32 1.376570972  10.192.51.94        10.192.50.253       TCP     66  39950 → 80
[ACK] Seq=2479527618 Ack=1308100623 Win=64256 Len=0 TSval=3886404692
TSecr=773916175
```

```
    33 1.376648457  10.192.51.94        10.192.50.253       HTTP    346 GET
/favicon.ico HTTP/1.1
    34 1.376903440  10.192.50.253       10.192.51.94        TCP     66  80 → 39950
[ACK] Seq=1308100623 Ack=2479527898 Win=30080 Len=0 TSval=773916175
TSecr=3886404692
    35 1.377048276  10.192.50.253       10.192.51.94        HTTP    336 HTTP/1.1
404 Not Found  (text/html)
    36 1.377053844  10.192.51.94        10.192.50.253       TCP     66  39950 → 80
[ACK] Seq=2479527898 Ack=1308100893 Win=64128 Len=0 TSval=3886404692
TSecr=773916175
    37 1.377132913  10.192.50.253       10.192.51.94        TCP     66  80 → 39950
[FIN, ACK] Seq=1308100893 Ack=2479527898 Win=30080 Len=0 TSval=773916175
TSecr=3886404692
    38 1.379266277  10.192.51.94        10.192.50.253       TCP     66  39950 → 80
[FIN, ACK] Seq=2479527898 Ack=1308100894 Win=64128 Len=0 TSval=3886404694
TSecr=773916175
    39 1.379586633  10.192.50.253       10.192.51.94        TCP     66  80 → 39950
[ACK] Seq=1308100894 Ack=2479527899 Win=30080 Len=0 TSval=773916176
TSecr=3886404694
```

a. Les protocoles de niveau haut capturés sont : TCP / NBNS / VRRP / DNS / HTTP / ARP

b. Le protocole utilisé pour envoyer la requête et recevoir la réponse entre le navigateur et le serveur web est le protocole HTTP.

c. Le protocole qui a encapsulé le protocole précédent (la requête de votre navigateur et la réponse du serveur Web) est le protocole TCP.

d. Le filtre qui permet d'isoler les trames transportant le protocole de la question précédente est : `tcp.port == 80` (port 80 car c'est le port utilisé par le protocole HTTP).

e. En observant les trames correspondants à la requête GET du navigateur, on peut voir que l'adresse MAC du serveur Web est `00:1f:29:05:05:ba` et son adresse IP est `10.192.53`

f. Voici liste des trames affichées après filtrage sans détails des protocoles encapsulés ni le contenu hexadécimal :

```
No.     Time           Source                Destination           Protocol Length
Info
      4 0.064617575    10.192.51.94          34.107.221.82         TCP      74
33942 → 80 [SYN] Seq=240844166 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TSval=1420220023 TSecr=0 WS=128
      6 0.317157540    10.192.51.94          34.107.221.82         TCP      74
33944 → 80 [SYN] Seq=1197311654 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TSval=1420220275 TSecr=0 WS=128
     11 1.063433334    10.192.51.94          34.107.221.82         TCP      74
33942 → 80 [SYN] Seq=240844166 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TSval=1420221021 TSecr=0 WS=128
     17 1.093447091    10.192.51.94          10.192.50.253         TCP      74
39948 → 80 [SYN] Seq=2003138522 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TSval=3886404408 TSecr=0 WS=128
```

```
     18 1.093741816    10.192.50.253         10.192.51.94          TCP      74
80 → 39948 [SYN, ACK] Seq=3618063222 Ack=2003138523 Win=28960 Len=0 MSS=1460
SACK_PERM=1 TSval=773916104 TSecr=3886404408 WS=128
     19 1.093772620    10.192.51.94          10.192.50.253         TCP      66
39948 → 80 [ACK] Seq=2003138523 Ack=3618063223 Win=64256 Len=0 TSval=3886404409
TSecr=773916104
     20 1.094021767    10.192.51.94          10.192.50.253         HTTP     425
GET / HTTP/1.1
     21 1.094345377    10.192.50.253         10.192.51.94          TCP      66
80 → 39948 [ACK] Seq=3618063223 Ack=2003138882 Win=30080 Len=0 TSval=773916104
TSecr=3886404409
     22 1.094549766    10.192.50.253         10.192.51.94          HTTP     1514
HTTP/1.1 200 OK  (text/html)
     23 1.094556516    10.192.51.94          10.192.50.253         TCP      66
39948 → 80 [ACK] Seq=2003138882 Ack=3618064671 Win=64128 Len=0 TSval=3886404410
TSecr=773916104
     24 1.094573095    10.192.50.253         10.192.51.94          HTTP     1037
Continuation
     25 1.094577507    10.192.51.94          10.192.50.253         TCP      66
39948 → 80 [ACK] Seq=2003138882 Ack=3618065642 Win=63488 Len=0 TSval=3886404410
TSecr=773916104
     26 1.094580645    10.192.50.253         10.192.51.94          TCP      66
80 → 39948 [FIN, ACK] Seq=3618065642 Ack=2003138882 Win=30080 Len=0
TSval=773916104 TSecr=3886404409
     27 1.094840424    10.192.51.94          10.192.50.253         TCP      66
39948 → 80 [FIN, ACK] Seq=2003138882 Ack=3618065643 Win=64128 Len=0
TSval=3886404410 TSecr=773916104
     28 1.095131388    10.192.50.253         10.192.51.94          TCP      66
80 → 39948 [ACK] Seq=3618065643 Ack=2003138883 Win=30080 Len=0 TSval=773916104
TSecr=3886404410
     29 1.319799640    10.192.51.94          34.107.221.82         TCP      74
33944 → 80 [SYN] Seq=1197311654 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TSval=1420221278 TSecr=0 WS=128
     30 1.376242183    10.192.51.94          10.192.50.253         TCP      74
39950 → 80 [SYN] Seq=2479527617 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TSval=3886404691 TSecr=0 WS=128
     31 1.376547773    10.192.50.253         10.192.51.94          TCP      74
80 → 39950 [SYN, ACK] Seq=1308100622 Ack=2479527618 Win=28960 Len=0 MSS=1460
SACK_PERM=1 TSval=773916175 TSecr=3886404691 WS=128
     32 1.376570972    10.192.51.94          10.192.50.253         TCP      66
39950 → 80 [ACK] Seq=2479527618 Ack=1308100623 Win=64256 Len=0 TSval=3886404692
TSecr=773916175
     33 1.376648457    10.192.51.94          10.192.50.253         HTTP     346
GET /favicon.ico HTTP/1.1
     34 1.376903440    10.192.50.253         10.192.51.94          TCP      66
80 → 39950 [ACK] Seq=1308100623 Ack=2479527898 Win=30080 Len=0 TSval=773916175
TSecr=3886404692
     35 1.377048276    10.192.50.253         10.192.51.94          HTTP     336
HTTP/1.1 404 Not Found  (text/html)
     36 1.377053844    10.192.51.94          10.192.50.253         TCP      66
39950 → 80 [ACK] Seq=2479527898 Ack=1308100893 Win=64128 Len=0 TSval=3886404692
TSecr=773916175
     37 1.377132913    10.192.50.253         10.192.51.94          TCP      66
80 → 39950 [FIN, ACK] Seq=1308100893 Ack=2479527898 Win=30080 Len=0
```

```
TSval=773916175 TSecr=3886404692
     38 1.379266277    10.192.51.94          10.192.50.253         TCP      66
39950 → 80 [FIN, ACK] Seq=2479527898 Ack=1308100894 Win=64128 Len=0
TSval=3886404694 TSecr=773916175
     39 1.379586633    10.192.50.253         10.192.51.94          TCP      66
80 → 39950 [ACK] Seq=1308100894 Ack=2479527899 Win=30080 Len=0 TSval=773916176
TSecr=3886404694
```

---

2. Analyse fine

a. 2 trames ont transporté la réponse du serveur hormis celle indiquant l'erreur 404. Les voici :

```
No.     Time           Source                Destination           Protocol Length
Info
22 1.094549766    10.192.50.253         10.192.51.94          HTTP     1514
HTTP/1.1 200 OK  (text/html)
24 1.094573095    10.192.50.253         10.192.51.94          HTTP     1037
Continuation
```

b. La taille de la page web récupérée est de 1514 octets (ligne 22). On l'obtient en regardant la taille de la requête HTTP (ligne 22).

c. La requête envoyée au serveur Web est : `GET / HTTP/1.1`

d. Les 3 premières directives de la requête Web sont : `GET`: indique que la requête est une requête de type GET. `/` : indique que la requête est faite à la racine du serveur. `HTTP/1.1` : indique que le protocole HTTP utilisé est la version 1.1.

Et leur rôle respectif : `User-agent` : indique le nom et la version du navigateur ou de l'outil qui a envoyé la requête. `Accept` : indique le type de contenu que le navigateur accepte comme réponse. `Accept-Language` : indique la langue préférée du navigateur pour la réponse.

e. Voici le détail des protocoles encapsulés dans la première trame de la réponse du serveur :

```
No.     Time           Source                Destination           Protocol Length
Info
17      2.495117236    10.192.50.253         10.192.51.97          HTTP     1514
HTTP/1.1 200 OK  (text/html)

Frame 17: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on
interface 0
Ethernet II, Src: HewlettP_05:05:ba (00:1f:29:05:05:ba), Dst: PcsCompu_17:51:97
(08:00:27:17:51:97)
Internet Protocol Version 4, Src: 10.192.50.253, Dst: 10.192.51.97
Transmission Control Protocol, Src Port: 80, Dst Port: 52500, Seq: 459502056, Ack:
3002954047, Len: 1448
Hypertext Transfer Protocol
Line-based text data: text/html (33 lines)
```

Question 3 : Protocole ARP

> Séance 2 Adresse IP : 10.192.51.33 Adresse @MAC : 08:00:27:17:51:13 Nom de la machine : vmarm003.univ-lr.fr

1. Le protocole ARP permet de résoudre une adresse IP en une adresse MAC. Il fonctionne en envoyant une requête ARP à tous les hôtes du réseau. Si l'hôte reçoit la requête, il répond avec son adresse MAC. Si l'hôte ne reçoit pas la requête, il ne répond pas.

2.a. Voici le contenu du cache ARP de ma machine physique :

```
admin@archi000:~$ arp -a
silo192.univ-lr.fr (10.192.51.253) at 3a:83:99:00:f7:d7 [ether] on enp0s3
_gateway (10.192.0.255) at 00:00:5e:00:01:0a [ether] on enp0s3
```

Et suite à la commande `arp 10.192.51.34` qui est ma machine voisine, on a une réponse tel que `10.192.51.34 (10.192.51.34) -- no entry` ce qui vérifie qu'elle ne se trouve pas dans le cache.

Pour retrouver ensuite la machine voisine dans mon cache avec la commande `arp -a`, j'ai juste eu à exécuter un ping vers l'adresse IP 10.192.51.34 et refaire la commande `arp -a`.

2.b. Voici le résultat de la capture dans Wireshark après avoir exécuté le `ping -c3` sur l'@IP de la machine voisine :

```
No.     Time        Source              Destination         Protocol Length Info
    1 0.000000000   10.192.0.250        224.0.0.18          VRRP    70
Announcement (v2)
    2 0.476870078   HewlettP_aa:0a:6b   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x8095
    3 0.907660121   ::                  ff02::16            ICMPv6   130
Multicast Listener Report Message v2
    4 0.908644378   ::                  ff02::fb            ICMPv6   90
Multicast Listener Query
    5 1.115998561   fe80::82c1:6eff:feff:316c ff02::fb               MDNS    336
Standard query 0x0000 TXT hp LaserJet 4200 (0001E66F79FB)._ipp._tcp.local, "QM"
question TXT HP Officejet Pro X476dw MFP [CE0225]._ipps._tcp.local, "QM" question
TXT Kyocera TASKalfa 3212i._ipps._tcp.local, "QM" question TXT HP LaserJet MFP
M426fdn (11EF6C) (Fax) @ asylum._ipps._tcp.local, "QM" question TXT HP ENVY Photo
6200 series @ crista05._ipps._tcp.local, "QM" question TXT print.univ-lr.fr @
crista05._ipps._tcp.local, "QM" question
    6 1.443484028   fe80::b474:4f4f:dd7f:5339 ff02::fb               MDNS    107
Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local,
"QM" question
    7 1.612845799   10.192.51.33        224.0.0.251         MDNS    87  Standard
query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM"
question
```

```
    8 1.695387253   ::                  ff02::16            ICMPv6   130
Multicast Listener Report Message v2
    9 1.910114645   ::                  ff02::fb            ICMPv6   90
Multicast Listener Query
    10 2.010175030  10.192.0.250        224.0.0.18          VRRP     70
Announcement (v2)
    11 2.476953202  HewlettP_aa:0a:6b   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x8095
    12 3.057365540  Dell_1c:51:d8       Broadcast           ARP      60  Who has
10.192.150.205? Tell 10.192.0.250
    13 4.020241435  10.192.0.250        224.0.0.18          VRRP     70
Announcement (v2)
```

2.c. J'ai effectivement une trame utilisant le protocole ARP qui est envoyée à la machine cible. C'esr la trame numéro 12 :

```
No.     Time        Source              Destination         Protocol Length Info
12 3.057365540  Dell_1c:51:d8       Broadcast           ARP      60  Who has
10.192.150.205? Tell 10.192.0.250
```

Lorsque notre ordinateur envoie un paquet IP à une adresse IP donnée, il envoie également une requête ARP pour demander l'adresse MAC correspondante à cette adresse et c'est pour cela que dans la capture Wireshark après l'exécution de la commande ping, on voit une trame ARP qui est envoyée à la machine cible.

2.d. Voici le résultat de la capture dans Wireshark après avoir exécuté le `ping -c3` sur l'@IP de ma machine physique :

```
No.     Time        Source              Destination         Protocol Length Info
    1 0.000000000   PcsCompu_17:51:33   Broadcast           ARP      42  Who has
10.192.51.34? Tell 10.192.51.33
    2 0.001385710   PcsCompu_17:51:34   PcsCompu_17:51:33   ARP      60
10.192.51.34 is at 08:00:27:17:51:34
    3 0.001397907   10.192.51.33        10.192.51.34        ICMP     98  Echo
(ping) request  id=0x099e, seq=1/256, ttl=64 (reply in 4)
    4 0.002698860   10.192.51.34        10.192.51.33        ICMP     98  Echo
(ping) reply    id=0x099e, seq=1/256, ttl=64 (request in 3)
    5 0.067048738   HewlettP_aa:0a:6b   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x8095
    6 0.410043172   fe80::46a8:42ff:fe03:98a2 ff02::2               ICMPv6   70
Router Solicitation from 44:a8:42:03:98:a2
    7 0.725588940   10.192.0.250        224.0.0.18          VRRP     70
Announcement (v2)
    8 1.002500530   10.192.51.33        10.192.51.34        ICMP     98  Echo
(ping) request  id=0x099e, seq=2/512, ttl=64 (reply in 9)
    9 1.004067759   10.192.51.34        10.192.51.33        ICMP     98  Echo
(ping) reply    id=0x099e, seq=2/512, ttl=64 (request in 8)
    10 1.045564301  fe80::ce48:3aff:fef6:106b ff02::1:fffb:6823     ICMPv6   86
Neighbor Solicitation for fe80::146f:52a0:bbfb:6823 from cc:48:3a:f6:10:6b
    11 1.964706120  0.0.0.0             255.255.255.255     DHCP     342 DHCP
```

```
Discover - Transaction ID 0xc1b55c7c
    12 2.003813414  10.192.51.33        10.192.51.34        ICMP    98  Echo
(ping) request  id=0x099e, seq=3/768, ttl=64 (reply in 13)
    13 2.005274846  10.192.51.34        10.192.51.33        ICMP    98  Echo
(ping) reply    id=0x099e, seq=3/768, ttl=64 (request in 12)
    14 2.066950274  HewlettP_aa:0a:6b   Spanning-tree-(for-bridges)_00 STP
119 MST. Root = 0/0/00:1f:fe:7e:ac:00  Cost = 25000  Port = 0x8095
    15 2.735943222  10.192.0.250        224.0.0.18          VRRP    70
Announcement (v2)
    16 3.061950607  fe80::ce48:3aff:fef6:106b ff02::1:fffb:6823     ICMPv6   86
Neighbor Solicitation for fe80::146f:52a0:bbfb:6823 from cc:48:3a:f6:10:6b
    17 3.157106111  fe80::4ed9:8fff:fee3:e2fa ff02::1:ff1e:958a     ICMPv6   86
Neighbor Solicitation for fe80::186f:44de:681e:958a from 4c:d9:8f:e3:e2:fa
```

On remarque qu'il y a ici 2 trames utilisant le protocol ARP :

```
    1 0.000000000   PcsCompu_17:51:33   Broadcast           ARP     42  Who has
10.192.51.34? Tell 10.192.51.33
    2 0.001385710   PcsCompu_17:51:34   PcsCompu_17:51:33   ARP     60
10.192.51.34 is at 08:00:27:17:51:34
```

---

4. Voici la pile de protocole observé sur la capture du ping de la machine voisine sur WireShark :

```
Frame 12 : 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
0
Ethernet II, Src: Dell_1c:51:d8 (24:6e:96:1c:51:d8), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

---

5. Voici le contenu des champs ARP de la première trame ARP capturée avec les détails :

```
No.     Time        Source              Destination         Protocol Length Info
    12 3.057365540  Dell_1c:51:d8       Broadcast           ARP     60  Who has
10.192.150.205? Tell 10.192.0.250

Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
    Interface id: 0 (enp0s3)
        Interface name: enp0s3
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  8, 2023 11:44:15.680933734 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1678272255.680933734 seconds
    [Time delta from previous captured frame: 0.580412338 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
```

```
    [Time since reference or first frame: 3.057365540 seconds]
    Frame Number: 12
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: Dell_1c:51:d8 (24:6e:96:1c:51:d8), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
        Address: Broadcast (ff:ff:ff:ff:ff:ff)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this
is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address
(multicast/broadcast)
    Source: Dell_1c:51:d8 (24:6e:96:1c:51:d8)
        Address: Dell_1c:51:d8 (24:6e:96:1c:51:d8)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Dell_1c:51:d8 (24:6e:96:1c:51:d8)
    Sender IP address: 10.192.0.250
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.192.150.205
```

Question 4 : ICMP

1. Le protocole ICMP (Internet Control Message Protocol) est un protocole réseau qui est utilisé pour communiquer des informations de contrôle et de diagnostic sur l'état de la communication réseau entre des ordinateurs connectés à Internet. Il est parfois utilisé pour tester la connectivité entre deux machines, signaler des erreurs de routage ou de livraison de paquets et plus encore.

2.a. Le message indique que le destinataire de l'IP (Internet Protocol) ne peut être atteint car le réseau de destination est inaccessible. Ce message est généralement renvoyé par un routeur ou une passerelle lorsqu'il ne peut pas atteindre la destination finale.

```
Type : 11 (Time Exceeded)
Code : 0 (TTL expired in transit)
```

2.b. Le message indique qu'un paquet envoyé à une adresse IP de destination spécifique ne peut pas être livré car la destination est hors ligne ou inaccessible.

```
Type : 3 (Destination Unreachable)
Code : 0 (Network unreachable)
```

2.c. Le message indique qu'un paquet envoyé à une adresse IP de destination spécifique ne peut pas être livré car la destination est inaccessible en raison d'un filtrage administratif

```
Type : 3 (Destination Unreachable)
Code : 1 (Host unreachable)
```

2.d. Le message indique qu'un paquet envoyé à une adresse IP de destination spécifique ne peut pas être livré car le délai de vie du paquet a expiré

```
Type : 3 (Destination Unreachable)
Code : 3 (Port unreachable)
```

2.e. Le message indique qu'un paquet envoyé à une adresse IP de destination spécifique a été bloqué par une règle de filtrage de paquets qui interdit la communication avec cette destination en raison de raisons administratives.

```
Type : 3 (Destination Unreachable)
Code : 9 (Communication administratively prohibited)
```

2.f.

```
Type : 11 (Time Exceeded)
Code : 0 (TTL expired in transit)
```

3.

```
No.     Time           Source                Destination         Protocol Length
Info
    7 1.801987748      10.192.50.253         10.192.51.33        ICMP     102
Redirect            (Redirect for host)
    16 9.349205658     10.192.51.33          10.2.40.230         ICMP     98
Echo (ping) request  id=0x0f69, seq=1/256, ttl=1 (no response found!)
```

```
    17 9.349800022     10.192.50.253        10.192.51.34         ICMP     126
Time-to-live exceeded (Time to live exceeded in transit)
    51 17.354522639    10.192.50.253        10.192.51.33         ICMP     102
Destination unreachable (Network unreachable)
    94 29.364914256    10.192.50.253        10.192.51.33         ICMP     102
Destination unreachable (Host unreachable)
    96 29.365041127    10.192.50.253        10.192.51.33         ICMP     102
Destination unreachable (Host unreachable)
    106 32.365320206   10.192.50.253        10.192.51.33         ICMP     102
Destination unreachable (Host unreachable)
    125 40.297386951   10.192.50.253        10.192.51.33         ICMP     102
Destination unreachable (Port unreachable)
    143 47.937635202   10.192.50.253        10.192.51.33         ICMP     102
Destination unreachable (Network administratively prohibited)
    169 60.702882721   10.192.51.33         10.2.40.230          ICMP     98
Echo (ping) request  id=0x0f76, seq=1/256, ttl=1 (no response found!)
    170 60.703188346   10.192.50.253        10.192.51.33         ICMP     126
Time-to-live exceeded (Time to live exceeded in transit)
```

---

5. La pile de protocole pour la question 2.a est la suivante : Ethernet II -> IPv4 -> ICMP -> Echo (ping) request.

Question 5 : TELNET

1) Telnet est un protocole de communication utilisé pour établir une connexion distante à un serveur ou à un équipement réseau. Il permet aux utilisateurs de se connecter à un système distant et d'exécuter des commandes à distance comme s'ils étaient physiquement présents. Les deux rôles principaux de Telnet sont d'offrir un accès à distance à des systèmes informatiques et d'administrer des équipements réseau à distance.

2.a) Après capture de l'éxperience et filtrage des trames via le filtre `telnet`, on obtiens un total de 55 trames du protocole TELNET.

2.b) En regardant les trames capturées, on peut voir que Telnet envoie les commandes en utilisant des caractères ASCII pour les commandes et les réponses. Ces caractères sont affichés en texte clair dans Wireshark.

2.c) En ce qui concerne la sécurité, Telnet est considéré comme peu sûr car il transmet toutes les informations, y compris les noms d'utilisateur et les mots de passe, en texte clair. Il est préférable d'utiliser SSH pour une communication à distance plus sécurisée.

---

3) 10 premières trames TELNET :

```
No.     Time           Source                Destination           Protocol Length
Info
      8 6.926698718    10.192.51.33          10.192.50.253         TELNET   93
Telnet Data ...
     11 6.932477288    10.192.50.253         10.192.51.33          TELNET   78
```

```
Telnet Data ...
     13 6.933008146    10.192.50.253         10.192.51.33          TELNET   105
Telnet Data ...
     15 6.933341710    10.192.51.33          10.192.50.253         TELNET   153
Telnet Data ...
     16 6.934025838    10.192.50.253         10.192.51.33          TELNET   69
Telnet Data ...
     18 6.934151341    10.192.51.33          10.192.50.253         TELNET   69
Telnet Data ...
     19 6.934701984    10.192.50.253         10.192.51.33          TELNET   69
Telnet Data ...
     21 6.935089276    10.192.51.33          10.192.50.253         TELNET   69
Telnet Data ...
     22 6.935203200    10.192.50.253         10.192.51.33          TELNET   85
Telnet Data ...
     24 6.941681123    10.192.50.253         10.192.51.33          TELNET   82
Telnet Data ...
```