

ING2 - GI

TD 2 : Réseau local

A l'aide d'un logiciel "sniffer" (tcpdump, wireshark...), nous écoutons les paquets entrants et sortants de notre interface réseau.

```

0000  ff ff ff ff ff ff 00 15 00 3a f7 14 08 00 45 10  .....:....E.
0010  01 48 00 00 00 00 40 11 79 96 00 00 00 00 ff ff  .H....@.y.....
0020  ff ff 00 44 00 43 01 34 89 f2 01 01 06 00 c8 dc  ...D.C.4.....
[...]

0000  00 15 00 3a f7 14 00 04 75 c9 4d 97 08 00 45 10  ...:.... u.M...E.
0010  01 48 00 00 00 00 40 11 f7 ac c0 a8 00 02 c0 a8  .H....@. ....
0020  00 96 00 43 00 44 01 34 36 13 02 01 06 00 c8 dc  ...C.D.4 6.....
[...]

0000  ff ff ff ff ff ff 00 15 00 3a f7 14 08 00 45 10  ..... :....E.
0010  01 48 00 00 00 00 40 11 79 96 00 00 00 00 ff ff  .H....@. y.....
0020  ff ff 00 44 00 43 01 34 d8 fb 01 01 06 00 c8 dc  ...D.C.4 .....
[...]

0000  00 15 00 3a f7 14 00 04 75 c9 4d 97 08 00 45 10  ...:.... u.M...E.
0010  01 48 00 00 00 00 40 11 f7 ac c0 a8 00 02 c0 a8  .H....@. ....
0020  00 96 00 43 00 44 01 34 33 13 02 01 06 00 c8 dc  ...C.D.4 3.....
[...]

0000  ff ff ff ff ff ff 00 15 00 3a f7 14 08 06 00 01  ..... :.....
0010  08 00 06 04 00 01 00 15 00 3a f7 14 c0 a8 00 96  ..... :.....
0020  00 00 00 00 00 00 c0 a8 00 03  ..... ..
0000  00 15 00 3a f7 14 00 04 75 c9 4d 97 08 06 00 01  ...:.... u.M.....
0010  08 00 06 04 00 02 00 04 75 c9 4d 97 c0 a8 00 03  ..... u.M.....
0020  00 15 00 3a f7 14 c0 a8 00 96  ..... ..

0000  00 04 75 c9 4d 97 00 15 00 3a f7 14 08 00 45 00  ..u.M... :....E.
0010  00 3b 0c f0 40 00 40 11 ab d8 c0 a8 00 96 c0 a8  .;.@.@. ....
0020  00 03 81 36 00 35 00 27 a9 98 2c 0b 01 00 00 01  ...6.5.' ..,.....
0030  00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  .....w ww.googl
0040  65 02 66 72 00 00 01 00 01  ..... e.fr.... .

0000  00 15 00 3a f7 14 00 04 75 c9 4d 97 08 00 45 00  ...:.... u.M...E.
0010  02 0e 00 00 40 00 40 11 b6 f5 c0 a8 00 03 c0 a8  ....@.@. ....
0020  00 96 00 35 81 36 01 fa ef 66 2c 0b 81 80 00 01  ...5.6.. .f,.....
0030  00 05 00 0d 00 0a 03 77 77 77 06 67 6f 6f 67 6c  .....w ww.googl

0000  ff ff ff ff ff ff 00 15 00 3a f7 14 08 06 00 01  ..... :.....
0010  08 00 06 04 00 01 00 15 00 3a f7 14 c0 a8 00 96  ..... :.....
0020  00 00 00 00 00 00 c0 a8 00 01  ..... ..

```

```

0000 00 15 00 3a f7 14 00 04 75 c9 4d 97 08 06 00 01  ....:.... u.M.....
0010 08 00 06 04 00 02 00 04 75 c9 4d 97 c0 a8 00 01  ..... u.M.....
0020 00 15 00 3a f7 14 c0 a8 00 96  ....:.... ..

0000 00 04 75 c9 4d 97 00 15 00 3a f7 14 08 00 45 00  ..u.M... :.....E.
0010 00 54 00 00 40 00 40 01 d9 0e c0 a8 00 96 42 f9  .T..@.@. ....B.
0020 5d 63 08 00 ef 9d 07 1a 00 01 06 6d 97 46 71 90  ]c..... ...m.Fq.
0030 07 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... .. !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,- ./012345
0060 36 37

0000 00 15 00 3a f7 14 00 04 75 c9 4d 97 08 00 45 00  ....:.... u.M...E.
0010 00 54 00 00 40 00 f3 01 26 0e 42 f9 5d 63 c0 a8  .T..@... &.B.]c..
0020 00 96 00 00 f7 9d 07 1a 00 01 06 6d 97 46 71 90  ..... ...m.Fq.
0030 07 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... .. !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,- ./012345
0060 36 37

```

Note: Chaque bloc représente une trame, mais seuls les 38 premiers octets de chaque trame sont affichés.

Déduire de cette trace la décomposition des paquets (à l'aide des annexes ci-dessous) et répondre aux questions suivantes :

1. Quelles sont les adresses MAC /IP de la station, du serveur DHCP, du DNS, du correspondant et de la passerelle ?
2. Que se déroule-t-il exactement ? Expliquer à l'aide d'un chronogramme les différents échanges.