R&T1 R2 TD5

Analyse de trame Ethernet

1. Analyse de trames : démarrage de lr1-09.

La machine lr1-09 est mise sous tension. Pendant la phase d'initialisation de l'interface réseau, un analyseur de trames relève les trames (sans les préambules) échangées vers ou à partir de cette machine.

L'objectif est d'analyser les 4 trames (quasi) consécutives relevées, et d'en déduire les opérations réalisées par lr1-09 durant cette phase.

On relève sur les machines du réseau les informations suivantes :

Machine	***Adresse MAC***	***Adresse IP***
lr1- 09	000B6A-341749	???
Iut-gtr2	000B6A-BC65AF	172.31.25.9
Passerelle	???	172.17.16.1
Serveur DNS Panoramix	???	172.31.23.10

1.1 Trame N°1

- Analyser cette trame à l'aide du document fourni en annexe, en faisant apparaître les protocoles associés à chacun des niveaux.

```
0000  ff ff ff ff ff ff 00 0b 6a 34 17 49 08 00 45 10   ........j4.I..E.
0010  01 48 00 00 00 00 10 11 a9 96 00 00 00 00 ff ff   .H..............
0020  ff ff 00 44 00 43 01 34 51 ee 01 01 06 00 0f 09   ...D.C.4Q.......
0030  c2 4a 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .J..............
0040  00 00 00 00 00 00 00 0b 6a 34 17 49 00 00 00 00   ........j4.I....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
          ..................................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110  00 00 00 00 00 00 63 82 53 63 35 01 03 32 04 ac   ......c.Sc5..2..
0120  1f 19 13 37 07 01 1c 02 03 0f 06 0c ff 00 00 00   ...7............
0130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0150  00 00 00 00 00 00                                 ......
```

1.2 Trame N°2

- Analyser cette trame à l'aide du document fourni en annexe, en faisant apparaître les protocoles associés à chacun des niveaux.

```
0000  00 0b 6a 34 17 49 00 0b 6a bc 65 af 08 00 45 10   ..j4.I..j.e...E.
0010  01 48 00 00 00 00 10 11 1f 3b ac 1f 19 09 ac 1f   .H.......;......
0020  19 13 00 43 00 44 01 34 7f b6 02 01 06 00 0f 09   ...C.D.4........
0030  c2 4a 00 00 00 00 00 00 00 00 ac 1f 19 13 ac 1f   .J..............
0040  19 09 00 00 00 00 00 0b 6a 34 17 49 00 00 00 00   ........j4.I....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
            ..................................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110  00 00 00 00 00 00 63 82 53 63 35 01 05 36 04 ac   ......c.Sc5..6..
0120  1f 19 09 33 04 00 01 51 80 01 04 ff ff f0 00 03   ...3...Q........
0130  04 ac 1f 10 01 0f 0e 75 6e 69 76 2d 61 72 74 6f   .......univ-arto
0140  69 73 2e 66 72 06 08 ac 1f 17 0a c1 31 3e 09 ff   is.fr.......1>..
0150  00 00 00 00 00 00                                 ......
```

1.3 Trame N°3

- Analyser cette trame à l'aide du document fourni en annexe, en faisant apparaître les protocoles associés à chacun des niveaux.

```
0000  ff ff ff ff ff ff 00 0b 6a 34 17 49 08 06 00 01   ........j4.I....
0010  08 00 06 04 00 01 00 0b 6a 34 17 49 ac 1f 19 13   ........j4.I....
0020  00 00 00 00 00 00 ac 1f 19 09 ff ff ff ff ff ff   ................
0030  ff ff ff ff ff ff ff ff ff ff ff ff               ............
```

1.4 Trame N°4

- Analyser cette trame à l'aide du document fourni en annexe, en faisant apparaître les protocoles associés à chacun des niveaux.

```
0000  00 0b 6a 34 17 49 00 0b 6a bc 65 af 08 06 00 01   ..j4.I..j.e.....
0010  08 00 06 04 00 02 00 0b 6a bc 65 af ac 1f 19 09   ........j.e.....
0020  00 0b 6a 34 17 49 ac 1f 19 13 00 00 00 00 00 00   ..j4.I..........
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

1.5 Synthèse

Résumer en quelques mots les opérations réalisées par lr1-09 lors de la phase d'initialisation de son interface réseau.

2. Analyse de trames ethernet de connexion FTP

Deux trames Ethernet ont été récupérées sur le réseau de l'EUDIL par le logiciel tcpdump. Dans le cas présent seuls les 68 octets suivant le préambule ont été mémorisés. Vous devez analyser chaque trame. Il vous est autant demandé une analyse syntaxique (énumérer les valeurs des champs des protocoles) qu'une analyse sémantique (pourquoi telle valeur dans tel champ). Prenez cet exercice comme un travail de détective : il faut trouver l'origine des trames, leur destination, leur cheminement, leur raison d'exister, etc.

Première trame :

00 00 0c 03 a9 38 08 00 20 19 c2 9f 08 00 45 00 00 2c 3b e1 40 00
ff 06 a2 9a 86 ce 3c 05 c1 33 19 49 8f 50 00 15 f2 ee d4 b4 00 00
00 00 60 02 22 38 81 95 00 00 02 04 05 b4

Seconde trame :

00 00 0c 03 a9 38 08 00 20 19 c2 9f 08 00 45 00 00 42 3b e8 40 00
ff 06 a2 7d 86 ce 3c 05 c1 33 19 49 8f 50 00 15 f2 ee d4 ce 2a 8d
8e 65 50 18 23 98 51 19 00 00 50 4f 52 54 20 31 33 34 2c 32 30 36
2c 36

Pour cette trame il est rappelé que le code ascii (en hexadécimal) de 'A' est 41, celui de 'O' est 30 et celui de ',' est 2c.

Annexes (à titre d'information) :

```
eudilmac01.univ-lillel.fr      (134.206.60.210) at 0:0:89:6:43:be
pceudil9.univ-lillel.fr        (134.206.60.130) at 0:60:8c:71:b8:8f
cisco4000-eth1.univ-lille1.fr  (134.206.3.2) at 0:0:c:3:a9:38
eudilmac03.univ-lillel.fr      (134.206.60.212) at 0:0:89:6:43:be
eudilserv.eudil.univ-lillel.fr (134.206.60.5) at 8:0:20:19:c2:9f
eudilmac06.univ-lillel.fr      (134.206.60.215) at 0:0:89:6:43:be
lailp2pc5.univ-lillel.fr       (134.206.24.25) at 0:a0:24:36:39:7b
eudilsginfo.univ-lillel.fr     (134.206.60.202) at 0:0:89:6:43:be
eudil14.eudil.univ-lillel.fr   (134.206.60.58) at 8:0:20:3:b4:e9
pceudil2.univ-lillel.fr        (134.206.60.10) at 8:0:9:4f:ca:d1
```