« Réseaux : modèles, protocoles, et applications »

Sujet de TD n°6 : analyse de trafic TCP

On a intercepté sur un réseau local des paquets IP échangés entre deux stations de travail. La trame Ethernet encapsulant le premier de ces paquets (qui lui-même encapsule un segment TCP) est représentée ci-dessous.

```
00 1d e0 29 00 ef 90 4c e5 44 b4 e2 08 00 45 10
00 2c 62 ac 40 00 40 06 af b8 c0 a8 d3 07 c0 a8
d3 fe ba 86 00 17 3b 68 bb 9d 00 00 00 00 60 02
16 d0 a7 5b 00 00 02 04 05 b4
```

a) Décomposez les différents champs de chaque structure (trame, paquet, segment).

b) Vérifiez le total de contrôle du segment TCP. Ce total de contrôle est-il correct ?

c) De quel type de segment TCP s'agit-il ?

En réaction à la transmission du segment TCP précédent, on voit passer sur le réseau local les deux paquets IP suivants :

```
45 00 00 2c 00 00 40 00 40 06 12 75 c0 a8 d3 fe
c0 a8 d3 07 00 17 ba 86 e4 7c b2 95 3b 68 bb 9e
60 12 39 08 28 76 00 00 02 04 05 b4

45 10 00 28 62 ad 40 00 40 06 af bb c0 a8 d3 07
c0 a8 d3 fe ba 86 00 17 3b 68 bb 9e e4 7c b2 96
50 10 16 d0 27 f5 00 00
```

d) À quelle phase d'une session TCP correspond l'échange des trois paquets IP (et segments TCP) précédents ?

e) Que peut-on déduire, en analysant ces segments TCP, de la taille des tampons de réception alloués de part et d'autre pour gérer cette session TCP ?

f) Quelle est la taille maximale des segments TCP pouvant être émis au cours de cette session TCP ?

Dans le cadre de cette même session TCP, le centième segment intercepté sur le réseau est encapsulé dans le paquet IP suivant :

```
45 10 00 28 62 e7 40 00 40 06 af 81 c0 a8 d3 07
c0 a8 d3 fe ba 86 00 17 3b 68 bc 06 e4 7c b5 da
50 10 1d 50 1d c9 00 00
```

g) Que peut-on en déduire quant au nombre d'octets de données échangés dans chaque sens depuis le début de la session TCP, et quant à la taille des fenêtres d'anticipation à ce stade de la session ?

On intercepte à présent les paquets IP suivants :

```
45 10 00 28 aa 96 40 00 40 06 67 d2 c0 a8 d3 fe
c0 a8 d3 07 00 17 ba 86 e4 7c b5 e2 3b 68 bc 07
50 11 39 08 28 72 00 00

45 10 00 28 62 ea 40 00 40 06 af 7e c0 a8 d3 07
c0 a8 d3 fe ba 86 00 17 3b 68 bc 07 e4 7c b5 e3
50 11 1d 50 1d be 00 00

45 10 00 28 aa 97 40 00 40 06 67 d1 c0 a8 d3 fe
c0 a8 d3 07 00 17 ba 86 e4 7c b5 e3 3b 68 bc 08
50 10 39 08 28 72 00 00
```

h) Que peut-on déduire des segments TCP transportés dans ces paquets ?