

**Université Paris-Est Créteil**  
**Faculté de Droit - IUT de Sénart-Fontainebleau**  
**2016/2017**  
**Deuxième semestre – Première année**  
**Master Droit du Numérique – Informatique et Droit**  
**Réseau et normes**

**PREMIÈRE SESSION – Mercredi 19 avril 2017**  
**Corrigé**

- 1°) Cette trame de  $23 \times 16 + 3 = 371$  octets provient d'une interface Ethernet donc commence par un en-tête Ethernet (sans préambule ni CRC).

Analyse de l'en-tête Ethernet.-

- Les six premiers octets donnent l'adresse MAC du destinataire : 10:bf:48:4c:b6:a3.
- Les six octets suivants donnent l'adresse MAC de l'expéditeur : 00:24:d4:ac:22:a9. Les adresses MAC sont donc échangées par rapport à la requête, ce qui est normal.
- les deux octets suivants, 08 00h, soit 2048 donne le type, donc IP, certainement IPv4.

Analyse de l'en-tête IPv4.- Puisque le type Ethernet est IP, cet en-tête est suivi d'un en-tête IP, certainement IPv4 :

- Le premier demi-octet, 4, donne la version d'IP. Il s'agit bien d'IPv4.
- Le second demi-octet, 5, donne la longueur de l'en-tête IP en mots de 4 octets. On a donc 20 octets, soit le minimum pour un en-tête IPv4. Il n'y a pas d'options.
- L'octet suivant donne le type de service. Il est nul, ce qui est habituel pour une extrémité.
- Les deux octets suivants, 0x01 65, donnent la longueur du paquet, soit 357 octets. Avec les 14 octets de l'en-tête Ethernet, on retrouve bien les 371 octets de la trame ; il n'y a donc rien d'autre que le paquet IPv4 comme données de la trame.
- Les deux octets suivants, 0x65 78, donnent l'identificateur du paquet, sur lequel il n'y a rien de plus à dire puisqu'il est choisi presque au hasard.

- Les deux octets suivants, 0x40 00, représentent deux champs :
  - Les premiers bits 010b sont des drapeaux : le premier est « réservé » donc sa valeur nulle n'est pas étonnante ; le second DF, qui est levé, indique que le paquet originel ne doit pas être fragmenté ; le dernier MF, qui n'est pas levé, indique qu'il n'y a pas de fragment qui suit, ce qui est normal puisque le paquet originel ne devait pas être fragmenté.
  - Les treize derniers bits donnent le décalage par rapport au paquet originel. Il est nul, ce qui est normal puisque le paquet originel ne devait pas être fragmenté. Le paquet originel n'a donc effectivement pas été fragmenté.
- L'octet suivant 0x3f, donne la durée de vie, c'est-à-dire le nombre de sauts que peut traverser le paquet avant d'être écarté : la valeur 63 montre qu'il a traversé un certain nombre de sauts avant de nous parvenir.
 

Le plus probable est que le TTL était à l'origine à 64 et qu'il n'est passé que par un seul saut.
- L'octet suivant, 06h, donne le « protocole » : il s'agit ici de TCP.
- Les deux octets suivants donnent la somme de contrôle, 61 09h. Nous y reviendrons à la question 2.
- Les quatre octets suivants, 4e c0 63 77h, donnent l'adresse IP de l'expéditeur : 78.192.99.119.
- Les quatre octets suivants, c0 a8 01 32h, donnent l'adresse IP du destinataire : 192.168.1.50. Il s'agit d'une adresse IP privée, certainement attribuée dynamiquement par la box.

Analyse de l'en-tête TCP.- Puisque le protocole IP est TCP, l'en-tête IPv4 est suivi d'un en-tête TCP :

- Les deux premiers octets, 00 50h, donnent le port de l'expéditeur. Il s'agit d'un port bien connu : 80 pour un service HTTP.
- Les deux octets suivants, 0xf5 07, donnent le port du destinataire. Il est supérieur à 2 048, il s'agit donc certainement d'un port client attribué de façon pseudo-aléatoire par le module TCP du client.
- Les 4 octets suivants, 0x1a a6 ad 67, donnent le numéro de séquence.
- Les 4 octets suivants, 0xc7 23 9a a1, donnent le numéro d'accusé de réception.
- Les deux octets suivants, 50 18h, représentent deux champs :
  - Le demi-octet suivant, 5h, donne la longueur de l'en-tête TCP en mots de 4 octets. On a donc 20 octets, ce qui est la taille minimum. Il n'y a donc pas d'options.

– Les 12 bits suivants, 0000 0001 1000b, sont des drapeaux : les six premiers sont à l’origine réservés, donc nuls ; le drapeau urgent URG n’est pas levé ; le drapeau d’accusé de réception ACK est levé, ce qui indique qu’il faut prendre en compte le numéro d’accusé de réception ; le drapeau PuSH est levé, c’est donc la fin du message, qu’il faudra envoyer à l’application ; les drapeaux ReSeT, SYn et FIN ne sont pas levés.

- Les deux octets suivants, 03 5ch, donnent la taille de la fenêtre : 860, donc le débit n’est pas élevé.
- Les deux octets suivants, 5c fch, donnent la somme de contrôle.
- Les deux octets suivants, 00 00h, donnent la valeur du pointeur urgent, qui est nul, ce qui est normal puisque le drapeau urgent n’est pas levé.

Analyse du message HTTP.- Nous sommes arrivés à la fin des 20 octets de l’en-tête TCP, la suite est donc constituée du message HTTP.

En s’aidant de la fenêtre ASCII de l’éditeur hexadécimal, on trouve le message HTTP suivant :

```
HTTP/1.1 200 OK\r\n
Date: Wed, 05 Apr 2017 08:20:31 GMT\r\n
Server: Apache\r\n
Last-Modified: Wed, 05 Apr 2017 08:16:29 GMT\r\n
ETag: "4d68001-2f-263f140"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 47\r\n
Keep-Alive: timeout=15, max=94\r\n
Connection: Keep-Alive\r\n
Content-Type: text/plain\r\n
\r\n
```

Bravo ! Vous êtes arrivés à la fin de la trame.

Il s’agit d’une réponse.

- 2°) Calculons la somme de contrôle de l’en-tête IP :

```
45 00 : 0100 0101 0000 0000
01 65 : 0000 0001 0110 0101
-----
          0100 0110 0110 0101
65 78 : 0110 0101 0111 1000
-----
          1010 1011 1101 1101
40 00 : 0100 0000 0000 0000
-----
          1110 1011 1101 1101
3f 06 : 0011 1111 0000 0110
-----
          0010 1010 1110 0011
+ 0000 0000 0000 0001
-----
```

```

          0010 1010 1110 0100
4e c0 : 0100 1110 1100 0000
          -----
          0111 1001 1010 0100
63 77 : 0110 0011 0111 0111
          -----
          1101 1101 0001 1011
c0 a8 : 1100 0000 1010 1000
          -----
          1001 1101 1100 0011
+ 0000 0000 0000 0001
          -----
          1001 1101 1100 0100
01 32 : 0000 0001 0011 0010
          -----
          1001 1110 1111 0110

```

Le complément à 1 est 0110 0001 0000 1001b = 0x61 09. On retrouve bien la somme de contrôle.

- 3°) En consultant le fichier OUI.txt.