Université Paris-Est Créteil
Faculté de Droit - IUT de Sénart-Fontainebleau
2017/2018
Deuxième semestre – Première année
Master Droit du Numérique – Informatique et Droit
Réseau et normes

PREMIÈRE SESSION – Mardi 24 avril 2018
Corrigé

- 1^o) Cette trame de 19x16 + 13 = 317 octets provient d'une interface Ethernet donc commence par un en-tête Ethernet (sans préambule).

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 deux octets suivants, 08 00h, soit 2048 donne le type Ethernet, 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 2f, donnent la longueur du paquet, soit 303 octets. Avec les 14 octets de l'ent-tête Ethernet, on retrouve bien les 317 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, 0xf5 05, donnent l'identificateur du paquet, sur lequel il n'y a rien de plus à dire puisqu'il est choisi presqu'au hasard.

- Les deux octets suivants, 0x40 00, représentent deux champs :
  - Les trois 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 sui 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 0x2d, donne la durée de vie, c'est-à dire le nombre de sauts que peut traverser le paquet avant d'être écarté : la valeur 45 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 est passé que par 19 sauts.
- L'octet suivant, 06h, donne le « protocole » : il s'agit ici de TCP.
- Les deux octets suivants donnent la somme de contrôle, 0x78 ad. Nous y reviendrons à la question 2.
- Les quatre octets suivants, 0x58 d4 c4 67h, donnent l'adresse IP de l'expéditeur : 88.212.196.103.
- Les quatre octets suivants, 0xc0 a8 01 32, 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, 0xca 34, donnent le port du destinataire. Il est supérieur à 2 048, il s'agit donc certainement d'un port client attribué de façon presqu'aléatoire par le module TCP du client.
- Les 4 octets suivants, 0x7b e4 92 e8, donnent le numéro de séquence.
- Les 4 octets suivants, 0xc19 ee 1c 8f, donnent le numéro d'accusé de réception.
- Les deux octets suivants, 50 18h, représentent deux champs :
  - Le demi-octet suivant, 5h, donne la longeur 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, 02 23h, donnent la taille de la fenêtre : 547, donc le débit n'est pas élevé.
- Les deux octets suivants, 0x27 4b, donnent la somme de contrôle TCP, dont nous ne occuperons pas ici.
- Les deux derniers octets, 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:  Tue, 10 Apr 2018 11:32:02 GMT\r\n
Server:  OW/0.8c\r\n
Connection:  Close\r\n
Content-Type:  image/gif\r\n
Content-Length:  43\r\n
Expires:  Sun, 09 Apr 2017 21:00:00 GMT\r\n
Pragma:  no-cache\r\n
Cache-control:  no-cache\r\n
\r\n
GIF89a...
```

Il s'agit d'une réponse.

- 2^o) Calculons la somme de contrôle de l'en-tête IP :

```
45 00 :  0100 0101 0000 0000
01 2f :  0000 0001 0010 1111
         -------------------
         0100 0110 0010 1111
f5 05 :  1111 0101 0000 0101
         -------------------
         0011 1011 0011 0100
       + 0000 0000 0000 0001
         -------------------
         0011 1011 0011 0101
40 00 :  0100 0000 0000 0000
         -------------------
         0111 1011 0011 0101
2d 06 :  0010 1101 0000 0110
         -------------------
```

```
          1010 1000 0011 1011
58 d4 :   0101 1000 1101 0100
          -------------------
          0000 0001 0000 1111
        + 0000 0000 0000 0001
          -------------------
          0000 0001 0001 0000
c4 67 :   1100 0100 0110 0111
          -------------------
          1100 0101 0111 0111
c0 a8 :   1100 0000 1010 1000
          -------------------
          1000 0110 0001 1111
        + 0000 0000 0000 0001
          -------------------
          1000 0110 0010 0000
01 32 :   0000 0001 0011 0010
          -------------------
          1000 0111 0101 0010
```

Le complément à 1 est 0111 1000 1010 1101b = 0x78 ad. On retrouve bien la somme de contrôle.

- 3^o) En consultant le fichier OUI.txt.