AU 2020/2021
TD Réseaux Informatiques
Responsable H. AKSASSE

TD 1

Exercice 1 : Analyse d'une trame Ethernet
On donne dans les figures ci-dessous les formats de la trame Ethernet et de paquet IP

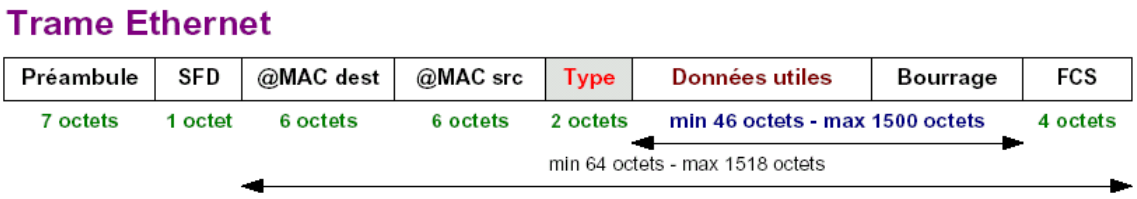


Figure 1 : Format d'une trame Ethernet

EtherType	Protocole
0x0800	IPv4
0x0806	ARP
0x8035	RARP
0x86DD	IPv6

Figure 2 : Exemples de valeurs du champ EtherType

Paquet IP

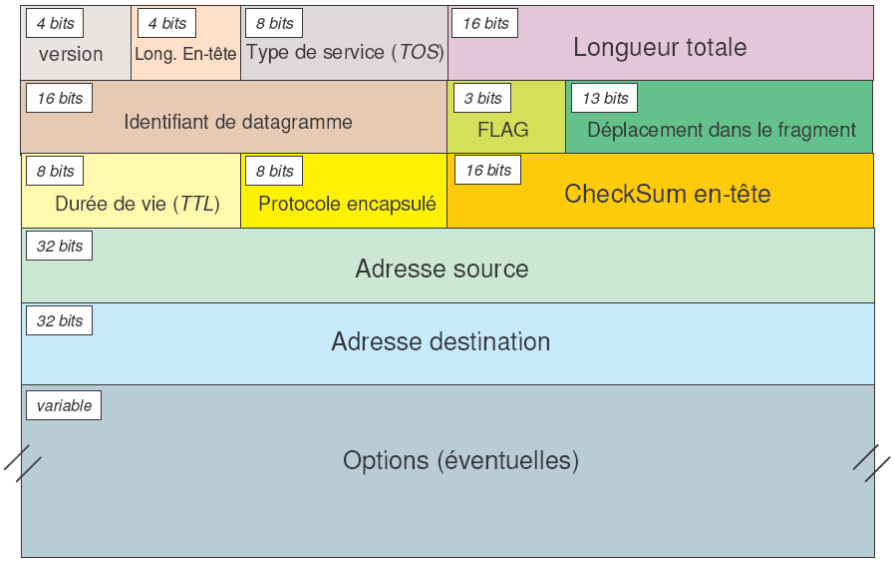


Figure 3 : Format d'un paquet IP

Exploiter la trame Ethernet ci-dessous et donner toutes les informations que vous pouvez en extraire.
AA AA AA AA AA AA AA AB 00 A0 00 00 8D 20 00 40 95 AA A4 3D 08 00 45 00 00 48 2F B1 00 00 40 11 C6 F7 84 E3 3D 17 84 E3 3D 1F 06 58 00 A1 00 34 39 4F 30 82 00 28 02 01 00 04 06 70 75 62 6C 69 63 A0 1B 02 01 01 02 01 00 02 01 00 30 10 30 82 00 0C 06 08 2B 06 01 02 01 01 05 00 05 00 15 A7 5C 89

R

AA AA AA AA AA AA AA : préambule 7 octets de 10101010 =AA en hexadécimal
AB = SFD
00 A0 00 00 8D 20 = @ MAC destination
00 40 95 AA A4 3D= @ MAC source
08 00 = type ➡ le protocole de la couche supérieur est IP

[45 00 00 48 2F B1 00 00 40 11 C6 F7 84 E3 3D 17 84 E3 3D 1F 06 58 00 A1 00 34 39 4F 30 82 00 28 02 01 00 04 06 70 75 62 6C 69 63 A0 1B 02 01 01 02 01 00 02 01 00 30 10 30 82 00 0C 06 08 2B 06 01 02 01 01 05 00 05 00] = Data ➡ les données constituent le paquet IP, et le 45 de début c'est pour la version 4 d'IP.

15 A7 5C 89 = FCS

Exercice 2

On considère la trace suivante, obtenue par l'analyseur de protocoles Ethereal installé sur la machine émettrice de la première trame Ethernet (les trames sont données sans préambule, ni SFD):

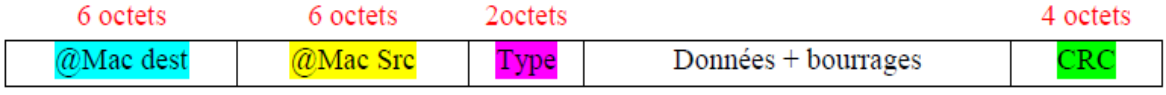
Frame Number : 1
00 0A B7 A3 4A 00
00 01 02 6F 5E 9B
08 00
45 00 00 28
00 00 40 00
40 01 82 AE
84 E3 3D 17
C2 C7
49 0A 08 00 75 DA 9C 7A 00 00 D4 45 A6 3A 62 2A
09 00 FF FF FF FF 00 00 00 00 00 00 DF 4F 54 A0

Frame Number : 2
00 01 02 6f 5E 9B 00 0A B7 A3 4A 00 08 00
45 00 00 28
D0 92 00 00
3A 01 5A BD
C2 C7 49 0A
84 E3 3D 17
00 00 7D DA 9C 7A 00 00 D4 45 A6 3A 62 2A
09 00 FF FF FF FF 00 00 00 00 00 00 FF 00 6C E3

1. Quelle est l'adresse IP de la machine ayant initié l'échange ? Quelle est sa classe d'adresse ?

R

Les trames sont données sans Préambule ni SFD, alors elles sont sous la forme:



Frame Number : 1

00 0a b7 a3 4a 00 00 01 02 6f 5e 9b 08 00 45 00
00 28 00 00 40 00 40 01 82 ae 84 e3 3d 17 c2 c7
49 0a 08 00 75 da 9c 7a 00 00 d4 45 a6 3a 62 2a
09 00 ff ff ff ff 00 00 00 00 00 00 df 4f 54 a0

L'adresse IP de la machine ayant initié l'échange est le quatrième mot de 32 bits dans le champ donné de la trame 1 (IP Scr dans l'entête du paquet IP). Ce mot est donné par : 84 E3 3D 17 (en hexadécimal)

Par suite : IP = 132.227.61.23, elle est de la classe B.

(Ecrire chaque chiffre Hex sur 4 bits, par exemple : 84Hex= (1000 0100)2= 132)

2. Quelle est « l'adresse physique » de la machine ayant initié l'échange ?

R

L'adresse physique de la machine ayant initié l'échange est : 00 01 02 6F 5E 9B

3. Quelle est l'adresse IP de la machine ayant répondu ? Quelle est sa classe d'adresse ?

R

L'adresse IP de la machine ayant répondu est l'adresse IP qui se trouve dans le champ IP Scr du 2ème paquet

```
Frame Number : 2

00 01 02 6f 5e 9b 00 0a b7 a3 4a 00 08 00 45 00
00 28 d0 92 00 00 3a 01 5a db c2 c7 49 0a 84 e3
3d 17 00 00 7d da 9c 7a 00 00 d4 45 a6 3a 62 2a
09 00 ff ff ff ff 00 00 00 00 00 00 ff 00 6c e3
```

@IP Scr = C2 C7 49 0A ➡ @IP Scr = 194.199.73.10, elle est de la classe C.

4. Quelle est « l'adresse physique » de la machine ayant répondu ?

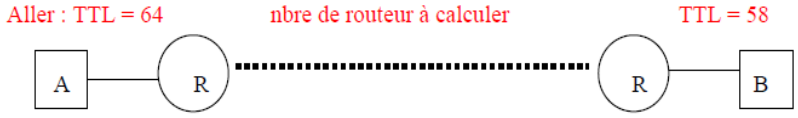
R

L'adresse physique de la machine ayant répondu est : 00 0A B7 A3 4A 00 (adresse mac du routeur puisque la classe B et classe C ne sont pas du même réseau.)

5. En supposant que la route de retour coïncide avec la route de l'aller, combien de routeurs séparent la machine source de la machine destination ?

R

Route aller = route retour
Même valeur par défaut de la TTL
TTLdépart = 40 en Hexa, 1er octets de 3ème mots de 32 bits dans le champ donné de la trame 1, qui vaut en décimal 64.
TTLarrivée= 3A en Hexa, 1er octets de 3ème mots de 32 bits dans le champ donné de la trame 2, qui vaut en décimal 58.



Nombre de routeurs = TTL (départ) – TTL (arrivée)
= 64 – 58 = 6 routeurs.

Exercice 3

On considère les trames suivantes, obtenues par l'outil de capture de trames Wireshark (les trames sont données sans préambule, ni SFD) :

a-

74 46 A0 7B EE 18 DC 4A 3E 78 D2 D7 08 06
00 01 08 00 06 04 00 02 DC 4A 3E 78 D2 D7 32 32 00 0E
74 46 A0 7B EE 18 32 32 00 8E

Extraire les adresses physiques source et destination ? (MAC Dest : 74 46 A0 7B EE 18) (MAC SRC: DC 4A 3E 78 D2 D7)

1.
2. Quel est le type du protocole de la couche supérieure (couche 3)? (ARP)

b-

74 46 A0 7B EE 18 DC 4A 3E 78 D2 D7 08 00 45 00
00 3C 21 8B 00 00 80 01 B4 36 32 32 00 0E 32 32
00 8E

1. Quel est l'adresse IP de la machine ayant initié l'échange ? Quelle est sa classe d'adresse ?
   Réponse : 50.50.0.14 classe : A
2. Quelle est « l'adresse physique » de la machine ayant initié l'échange ?
   Réponse : DC:4A:3E:78:D2:D7
3. Quel est l'adresse IP de la machine ayant répondu ? Quelle est sa classe d'adresse ?
   Réponse : 50.50.0.142 Classe :A
4. Quelle est « l'adresse physique » de la machine ayant répondu ?
   Réponse : 74:46:A0:7B:EE:18
5. Quel est le type du protocole des couches supérieures ?
   Réponse :IPV4/ICMP