Exercice 1 : Question de cours

1. De quelle couche du modèle TCP/IP fait parti le protocole IP ? Quel est son rôle ?
2. Comment le protocole IP détermine-t-il le destinataire ?
3. Dans quoi est encapsulé un paquet IP ?
4. Quelle est la taille de l'en-tête d'un paquet IP ?
5. Quelle est la particularité du champ IHL ?
6. Quel est le rôle du champ "LEN" ?
7. Quel est le rôle du champ "TTL" ?
8. Quel est le rôle du champ "PROTOCOL" ?

Exercice 2 : Décodage de trame

On a représenté ci-dessous le résultat d'une capture par le logiciel wireshark de trames Ethernet (ni le préambule, ni le FCS ne sont représentés).

Trame 1

```
0000  00 12 17 41 c2 c7 00 1a  73 24 44 89 08 00 45 00     ..A.... s$D...E.
0010  01 bb da c2 40 00 3c 06 fc 9d d5 e4 00 2a 3e 93     ....@.<......*>.
0020  51 3b 00 50 04 85 87 c7 14 d5 00 12 b0 cb 50 19     Q;.P..........P.
0030  19 20 95 45 00 00 3e 20 0a 3c 74 64 20 77 69 64     . .E..> .<td wid
0040  74 86 3d 22 33 30 25 22 20 20 68 65 69 67 68 74     th="30%" height
```

Trame 2

```
0000  00 1a 73 24 44 89 00 12  17 41 c2 c7 08 00 45 00     ..s$D... .A....E.
0010  00 3c 00 29 00 00 96 01  a0 dd c0 a8 01 01 c0 a8     .<.)....  ........
0020  01 69 00 00 55 56 00 01  00 05 61 62 63 64 65 66     .i..UV.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76     ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                      wabcdefg hi
```

Pour chacune de ces trames,

1. Entourer en rouge, les octets composant la trame Ethernet.

   Extrayez :

   - l'adresse MAC SOURCE
   - L'adresse MAC Destination
   - Le contenu du champ type de protocole. En déduire le protocole encapsulé dans la trame

2. Entourer en vert les octets composant le paquet IP contenu dans la trame Ethernet

   Extrayez :

   - La version du protocole
   - La longueur de l'entête
   - La valeur du champ TOS
   - La longueur totale du datagramme IP
   - L'identifiant affecté au datagramme
   - La valeur des champs DF, MF et fragment offset. En déduire si datagramme est fragmenté.
   - La valeur du champ TTL
   - Le contenu du champ protocole. En déduire le protocole encapsulé dans le paquet IP.
   - Les adresses IP source et destination.

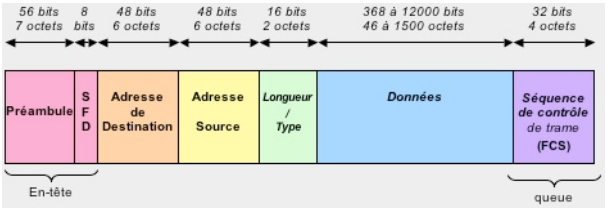
3. Entourer en bleu, les octets correspondant au message ICMP encapsulé dans le datagramme IP.

   Extrayez:

   - La valeur du champ type et du champ code. En déduire la nature du message ICMP.
   - Le contenu du champ de donnée du message ICMP.

ANNEXES

Entête Ethernet



Préambule : permet de synchroniser l'envoi.
SFD : indique à la carte réceptrice que le début de la trame va commencer.
Adresse destination : adresse MAC (Medium Access Control) de l'adaptateur destinataire.

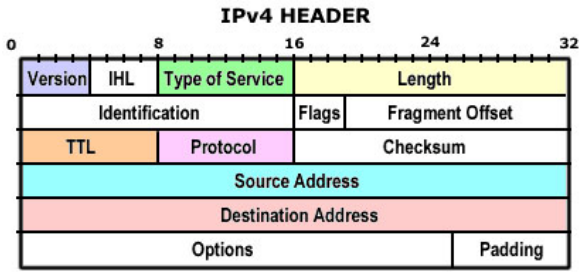
- Les trois premiers octets désignent le constructeur.
- Les trois derniers octets désignent le numéro d'identifiant de la carte.

Adresse source : adresse MAC (Medium Access Control) de l'adaptateur émetteur.
Ether Type : type de protocole

- 0x6000 - DEC
- 0x0609 - DEC
- 0x0600 - XNS
- 0x0800 - IPv4
- 0x0806 - ARP
- 0x8019 - Domain
- 0x8035 - RARP
- 0x809B - AppleTalk
- 0x86DD - IPv6

Données : entre 46 et 1500 octets et contient les données de la couche 3. Si la taille des données est inférieure à 46 octets, alors elle devra être complétée avec des octets de bourrage (padding).
FCS : séquence de contrôle de trame.

Entête IP



Version : *numéro de version du protocole IP*

- 04 - IP V4
- 05 - ST Datagram Mode
- 06 - IP V6

IHL (Internet header lengh) : longueur de l'entête IP

Service : gestion d'une qualité de service traitée (Priorité, Délai, Débit, Fiabilité, ...)

Longueur totale : longueur du paquet incluant l'entête IP et les Data
Identification : identification pour reconstituer les différents fragments
Flags : état de la fragmentation. Voici le détail des différents bits constituant ce champ.

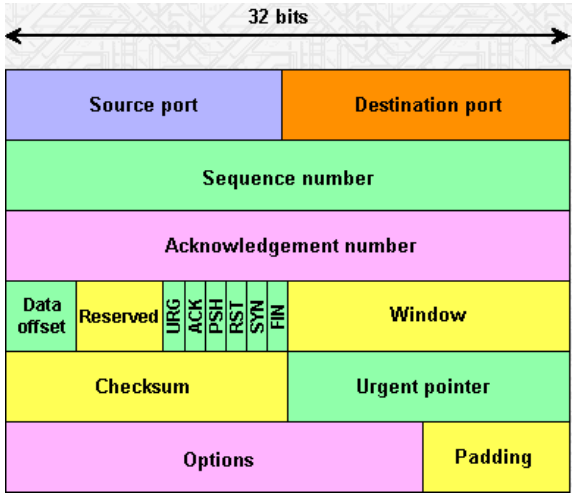
- DF :Don't Fragment
- MF :More Fragments
- le troisième bit indique s'il le fragment est le dernier

Position fragment : indique la position du fragment par rapport à la première trame
TTL (Time To Live) : indique la durée de vie maximale du paquet
Protocole : représente le type de Data

- 01 - 00001 - ICMP
- 02 - 00010 - IGMP
- 06 - 00110 - TCP
- 17 - 10001 - UDP

Checksum : représente la validité du paquet de la couche 3
Adresse IP source : adresse IP source ou de réponse
Adresse IP destination : adresse IP destination
Options : optionnel
Bourrage : permet de combler le champ option

Entête TCP



Port source : port relatif à l'application sur la machine source.
Port destination : port relatif à l'application sur la machine de destination.
Numéro de séquence : numéro du paquet
Numéro de l'accusé de réception : acquittement pour les paquets reçus
Offset : indique donc où les données commencent
Réservé : pour des besoins futur
Flags :

- URG : champ Pointeur de donnée urgente est utilisé.
- ACK : numéro de séquence pour les acquittements est valide.
- PSH :indique au récepteur de délivrer les données à l'application
- RST : demande la réinitialisation de la connexion.
- SYN : indique la synchronisation des numéros de séquence.
- FIN : indique fin de transmission.

Fenêtre : nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.
Checksum : validité du paquet de la couche 4 TCP.
Pointeur de donnée urgente : position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence.
Options : optionnel
Bourrage : permet de combler le champ option