

## Annexe 1

---

00 07 cb c5 ff 95 9c f3 87 ba f3 ea 08 00 45 00  
00 40 2f cc 40 00 40 06 4f 3e c0 a8 00 0d 84 e3  
76 15 c1 36 00 16 07 ef 5d c8 00 00 00 00 b0 02  
ff ff 7f b2 00 00 02 04 05 b4 01 03 03 05 01 01  
08 0a 26 d1 ad c7 00 00 00 00 04 02 00 00

9c f3 87 ba f3 ea 00 07 cb c5 ff 95 08 00 45 00  
00 3c 00 00 40 00 31 06 8e 0e 84 e3 76 15 c0 a8  
00 0d 00 16 c1 36 fd 89 50 f3 07 Ef 5d c9 a0 12  
16 a0 70 b2 00 00 02 04 05 b4 04 02 08 0a 06 4e  
b4 86 26 d1 ad c7 01 03 03 07

.



## Annexe 2

### Structure d'une trame Ethernet

```
.64bits--+48bits--+48bits--+16b--+ - - - +32b--.
.(Préam)| adresse | adresse |type| données | (CRC).
.      | dest.   | source  |   |         |         |
.-----+-----+-----+-----+-----+-----+-----.
```

Quelques types : 0x0800 = DoD Internet (IP)  
0x0806 = ARP  
0x8035 = RARP

### Structure d'un paquet ARP

```
<-----32bits----->
<--8bits--><--8bits--><-----16bits----->
+-----+-----+-----+-----+-----+-----+
| Hardware | Protocol |                               |
+-----+-----+-----+-----+-----+-----+
| Hlen     | Plen     | Operation |                               |
+-----+-----+-----+-----+-----+-----+
|                               | Sender HA (bytes 0-3) |
+-----+-----+-----+-----+-----+-----+
| Sender HA (bytes 4-5) | Sender IA (bytes 0-1) |
+-----+-----+-----+-----+-----+-----+
| Sender IA (bytes 2-3) | Sender HA (bytes 0-1) |
+-----+-----+-----+-----+-----+-----+
|                               | Target HA (bytes 2-5) |
+-----+-----+-----+-----+-----+-----+
|                               | Target IA (bytes 0-3) |
+-----+-----+-----+-----+-----+-----+

```

Hardware = type d'interface physique

ex : 0x0001 pour Ethernet

Protocol = type de protocole pour lequel une requête a été émise

ex : 0x0800 pour IP

Hlen = lg de l'adresse physique (en octets)

Plen = lg de l'adresse protocolaire (en octets)

Operation = type d'opération à effectuer par le récepteur

ex : 0x0001 pour une requête ARP

0x0002 pour une réponse ARP

Sender HA = adresse physique (Ethernet) de l'émetteur

Sender IA = adresse protocolaire (IP) de l'émetteur

Target HA = adresse physique (Ethernet) du récepteur

Target IA = adresse protocolaire (IP) du récepteur

### Structure d'un paquet IP

```
<-----32bits----->
<4b--><4b--><--8bits--><-----16bits----->
+-----+-----+-----+-----+-----+-----+
| Ver | IHL | TOS |                               |Lg. totale (en octets) |
+-----+-----+-----+-----+-----+-----+
| Identificateur | Fl | FO |                               |
+-----+-----+-----+-----+-----+-----+
| TTL | Protocole | Checksum(en-tête) |                               |
+-----+-----+-----+-----+-----+-----+
| Adresse Source |                               |
+-----+-----+-----+-----+-----+-----+
| Adresse Destination |                               |
+-----+-----+-----+-----+-----+-----+
|                               | Options |                               |
+-----+-----+-----+-----+-----+-----+
|                               | Données |                               |
+-----+-----+-----+-----+-----+-----+

```

Ver = Version d'IP

IHL = Longueur de l'en-tête IP (en mots de 4 octets)

TOS = Type de service (zéro généralement)

Fl (3 premiers bits) = Bits pour la fragmentation

\* 1er = réservé

\* 2ème = DF (Ne pas fragmenter)

\* 3ème = MF (Fragment suivant existe)

FO (13 bits suivants) = Position relative du fragment

dans le datagramme initial (déplacement exprimé en mots de 8 octets (seuls un datagramme complet ou un premier fragment peuvent avoir ce champ à 0)

TTL = Durée de vie restante

Protocole = protocole transporté

ex : 1 = ICMP

2 = IGMP

6 = TCP

8 = EGP  
11 = GLOUPS  
17 = UDP  
89 = OSPF

### Structure d'un message UDP

```
<-----32bits----->
+-----+-----+-----+-----+-----+-----+
| Port Source | Port Destination |
+-----+-----+-----+-----+-----+-----+
| Longueur | Checksum (msg) |
+-----+-----+-----+-----+-----+-----+
|                               | Données |                               |
+-----+-----+-----+-----+-----+-----+

```

### Structure d'un segment TCP

```
<-----32bits----->
<4b--> <-6bits--><-----16bits----->
+-----+-----+-----+-----+-----+-----+
| Port Source | Port Destination |
+-----+-----+-----+-----+-----+-----+
| Numéro de Séquence |
+-----+-----+-----+-----+-----+-----+
| Numéro d'Acquittement |
+-----+-----+-----+-----+-----+-----+
| THL | Flags | Taille Fenêtre |
+-----+-----+-----+-----+-----+-----+
| Checksum (msg) | Pointeur d'urgence |
+-----+-----+-----+-----+-----+-----+
|                               | Options |                               |
+-----+-----+-----+-----+-----+-----+
|                               | Données |                               |
+-----+-----+-----+-----+-----+-----+

```

THL = Longueur de l'entête TCP sur 4 bits (en mots de 4 octets)

Flags = indicateur codé sur 6 bits, de gauche à droite

- \* 1er = URG (Données urgentes)
- \* 2ème = ACK (Acquittement)
- \* 3ème = PSH (Données immédiates)
- \* 4ème = RST (Réinitialisation)
- \* 5ème = SYN (Synchronisation)
- \* 6ème = FIN

Options = suite d'options codées sur

\* un seul octet :

00 = Fin des options

01 = NOP (pas d'opération)

\* plusieurs octets, avec un codage TLV

T = un octet pour le type de l'option

2 Négociation de la taille max. du segment

3 Adaptation de la taille de la fenêtre

4 Autorisation des acquittements sélectifs

8 Estampilles temporelles

L = un octet pour la taille totale de l'option

V = valeur de l'option (sur L-2 octets)

### Services associés aux ports

ftp-data	20/tcp
ftp	21/tcp
ssh	22/tcp
telnet	23/tcp
smtp	25/tcp
dns	53/udp
www	80/tcp
pop-3	110/tcp
imap	143/tcp
bgp	179/tcp
snmp	161/udp
...	

