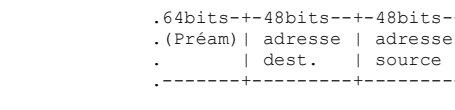
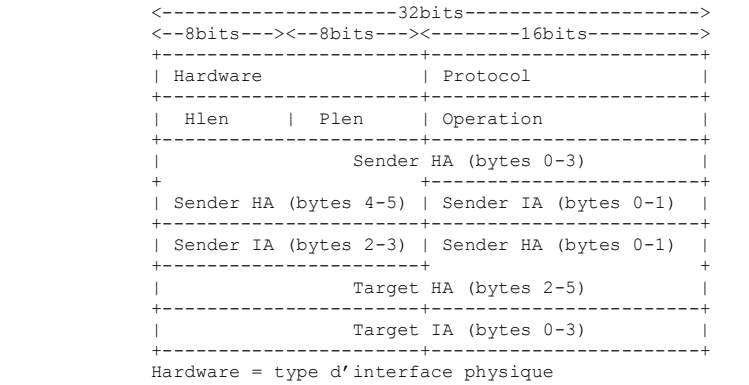
Annexe

Structure d'une trame Ethernet



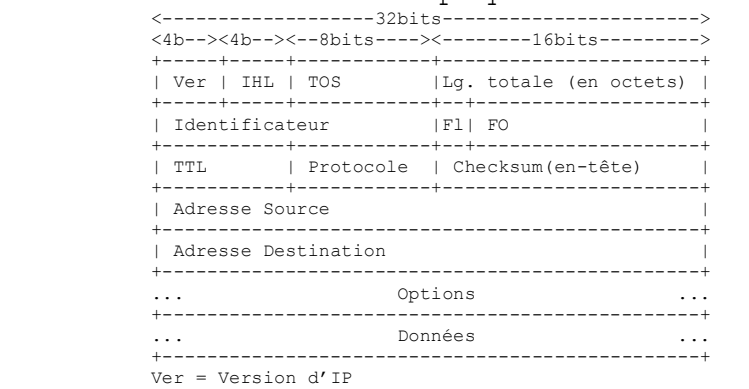
Quelques types : 0x0800 = DoD Internet (IP)
0x0806 = ARP
0x8035 = RARP

Structure d'un paquet ARP



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

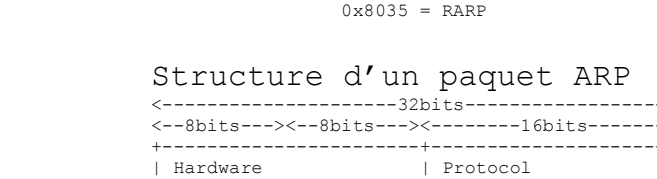
Structure d'un paquet IP



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



Structure d'un segment TCP

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

...