Annexe

Décodage des trames Ethernet

Adresse destination (6 octets)	Adresse source (6 octets)	Type (2 octets)	Information (46 à 1500 octets)	Code correcteur (4 octets)

Cette structure est une première peau. À l'intérieur du champ « Information » se trouve aussi une structure représentant une unité de donnée de protocole de réseau NPDU (Network Protocol Data Unit). Lorsqu'il y a moins de 46 octets de données, ce champ est complété par des octets de bourrage pour atteindre sa taille minimale.

Le champ « Type » vous renseigne sur la manière de lire le contenu du champ « Information ». Ce contenu quand c'est un NPDU est un paquet. Ce paquet peut être

– un paquet IP si « Type » = 08 00

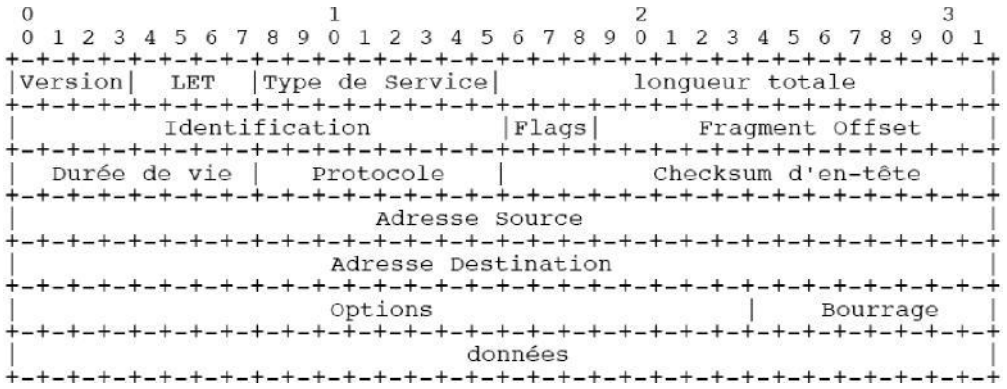
– un paquet ARP si « Type » = 08 06

Souvent le code correcteur n'est pas affiché lors des captures des trames.

Décodage de paquets IP

Un paquet IP (*Internet Protocol*) est composé : d'une entête et d'un contenu (données). **NPDU**

(paquet) du protocole IP



Notez que chaque marque indique une position bit.

– **Version** : 4 bits - format d'entêté

– **LET** ou Longueur d'En-Tête : 4 bits - taille de l'entête en nombre de mots de 32 bits. La valeur la plus courante est 5. Soit 5*4 = 20 octets.

– Type de Service : 8 bits - qualité de service

– **Longueur Totale** : 16 bits - longueur totale du paquet entête + données. Elle est exprimée en octets – Identification : 16 bits - numéro d'identification servant au réassemblage des paquets

– Flags : 3 bits (Bit 0: réservé, doit être laissé à zéro ; Bit 1: (AF) 0 = Fragmentation possible, 1 = Non fractionnable ; Bit 2: (DF) 0 = Dernier fragment, 1 = Fragment intermédiaire)

– Position relative : 13 bits - situation du fragment dans le paquet

– Durée de vie : 8 bits - temps maximal que le paquet peut rester dans le réseau (si 0, paquet détruit)

– **Protocole** : 8 bits - indique quel protocole de niveau supérieur est utilisé dans la section données du paquet qui suit l'entête ci-dessus. Vaut 1 si ICMP, 17 si UDP, 6 si TCP

Checksum d'en-tête : 16 bits - code de contrôle d'erreur pour l'entête

Adresse source : 32 bits - adresse IP de la machine source

Adresse destination : 32 bits - adresse IP de la machine destination

Options : variable

Bourrage : variable - n'existe que pour assurer à l'en-tête une taille totale multiple de 4 octets. Le bourrage se fait par des octets à zéro.

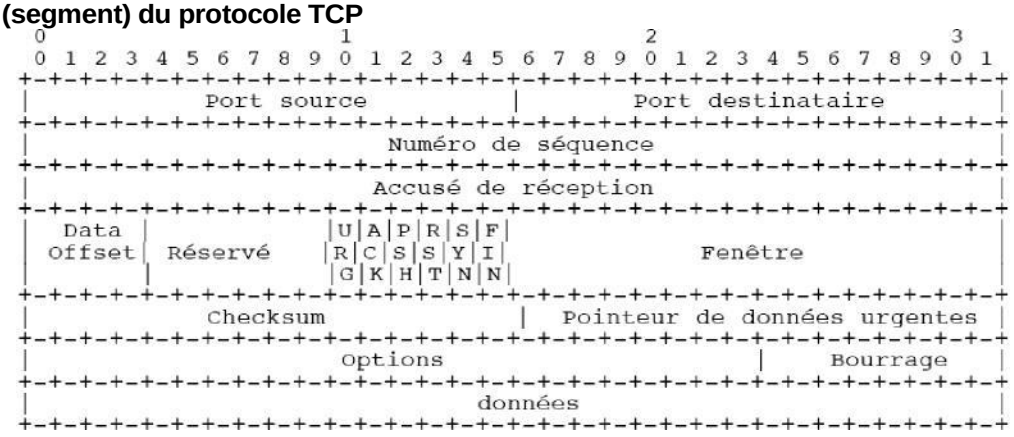
Annexe

L'information (données) contenue dans le paquet IP est aussi une structure. Cette dernière est définie de la manière suivante : une entête et une information. Mais elle peut être de plusieurs types : c'est une donnée de protocole de transfert (TPDU : Transfert Protocol Data Unit) du protocole TCP (*Transfert Control Protocol*), du protocole UDP (*User Datagram Protocol*) ou d'un autre protocole de niveau 4.

Décodage de segment TCP

Un segment TCP est également composé d'un entête et d'un contenu (non représenté ci-dessous).

TPDU (segment) du protocole TCP



Notez qu'une case représente une position bit.

Port source : 16 bits - peut définir le format du contenu du segment (protocole supérieur)
Port Destinataire : 16 bits - peut définir le format du contenu du segment (protocole supérieur)
Numéro de séquence : 32 bits - numéro du premier octet de données par rapport au début de la transmission (sauf si SYN est marqué). Si SYN est marqué, le numéro de séquence est le numéro de séquence initial (ISN) et le premier octet à pour numéro ISN+1).
Accusé de réception: 32 bits - si ACK est marqué ce champ contient le numéro de séquence du prochain octet que le récepteur s'attend à recevoir. Une fois la connexion établie, ce champ est toujours renseigné.
Data Offset : 4 bits - longueur entête en multiples de 32 bits
Réservé : 6 bits
Bits de contrôle : 6 bits (de gauche à droite):
URG: Pointeur de données urgentes significatif
ACK: Accusé de réception significatif
PSH: Fonction Push
RST: Réinitialisation de la connexion
SYN: Synchronisation des numéros de séquence
FIN: Fin de transmission
Fenêtre: 16 bits
Checksum: 16 bits
Pointeur de données urgentes: 16 bits
Options: variable
Bourrage (padding): variable. Les octets de bourrage terminent l'en-tête TCP de sorte que le nombre d'octet de celle-ci soit toujours multiple de 4 octets (32 bits) et de sorte que l'offset de données marqué dans l'en-tête corresponde bien au début des donnes applicatives.

L' information (données) contenue dans le segment TCP peut aussi être une structure avec une entête et des données appartenant à protocole tel que : HTTP, FTP,....

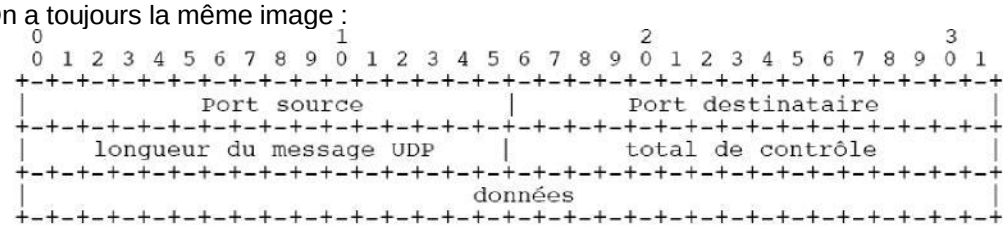
Autres exemples de NPDU et TPDU

NPDU ARP (protocole de contrôle) et TPDU UDP (protocole de transport sans garantie)

TPDU (segment) du protocole UDP

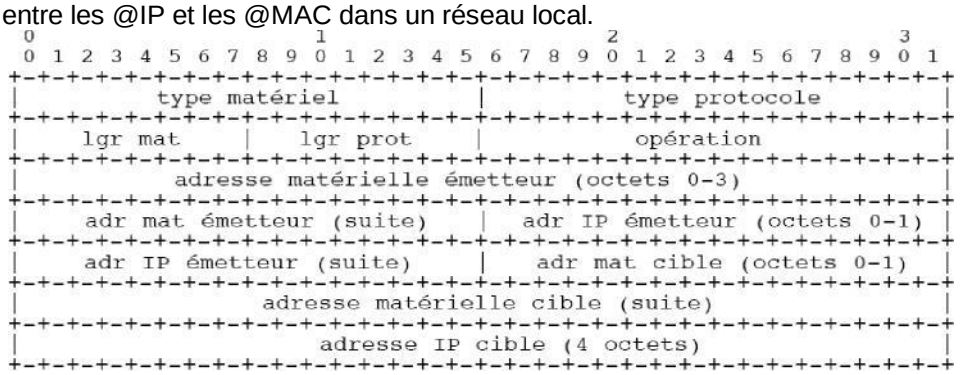
Annexe

Un segment UDP (*User Datagram Protocol*) est composé d'une entête et d'un contenu qui est l'information à transmettre. On a toujours la même image :



NPDU (paquet) du protocole ARP

ARP (*Address Resolution Protocol*) est un protocole de contrôle de niveau 3, il permet de faire la correspondance entre les @IP et les @MAC dans un réseau local.



– type matériel : type du protocole de la couche liaison de données, si 0001 alors Ethernet – type protocole : type du protocole de la couche réseau, si 0800 alors IP
– lgr mat : longueur des adresses physiques (au niveau liaison de données) en octets – lgr prot : longueur des adresses de la couche réseau en octets
– opération : 1 demande ARP, 2 réponse ARP, 3 demande RARP, 4 réponse RARP – adresse matérielle émetteur = @MAC de l'émetteur du paquet ARP
– adresse IP émetteur = @IP de l'émetteur du paquet ARP
– adresse matérielle cible = @MAC du destinataire du paquet ARP
– adresse IP cible = @IP du destinataire du paquet ARP