6 ANNEXE - FORMATS DES DATAGRAMMES DE DIFFERENTS PROTOCOLES

6.1 C'EST QUOI UN RFC ?

Les *Request For Comments* (RFC), sont une série numérotée de documents officiels décrivant les aspects techniques d'internet, ou de différents matériels informatiques (routeurs, serveur DHCP, etc.). Donc, la description, le principe de fonctionnement, le format de datagramme, etc. de chaque protocole est décrit par un document RFC. Ainsi, si on veut savoir plus de détail sur un protocole, il suffit de consulter son RFC. Le tableau suivant donne un exemple de quelques RFC.

RFC	Le protocole décrit
RFC 791	Protocole IP
RFC 793	Protocole TCP
RFC 826	Protocole ARP
RFC 145	Protocole HTTP
RFC 894	Ethernet

6.2 TECHNOLOGIE ETHERNET

Ethernet est la technologie de niveau liaison du modèle OSI la plus répandue et la plus utilisée actuellement dans les réseaux LAN. Elle a été normalisée par IEEE (Ethernet I) et ensuite par ISO (Ethernet II). L'unité de donnée protocolaire (PDU) d'Ethernet est la « Trame ». Selon la normalisation, il existe deux formats de ce protocole, à savoir la trame IEEE 802.3 ou Ethernet I (de IEEE) et la trame Ethernet II (de ISO). Les deux formats sont légèrement différents.

6.2.1 Format de la trame Ethernet II

8 oct.	6 oct.	6 oct.	2 oct.	46 à 1500 oct.	4 oct.
Préambule	Adresse Destination	Adresse Source	Ethernet Type	Données	CRC

- ***Préambule (8 octets)***
  C'est une suite de 8 octets contenant des 1 et des 0 en alternance sauf les deux derniers bits sont à 1, c.-à-d. 10101010…11). Il désigne le début de la trame et permet aux récepteurs de se synchroniser.
- ***Adresse Destination (6 octets)***
  L'adresse MAC de l'interface Ethernet destinatrice de la trame. Elle est constituée de 6 octets en hexadécimal séparés par des « :", ex. 08:00:07:5C:10:0A. Noter que les trois types de communication sont possibles :
  - Unicast (un destinataire unique - celui qui possède cette @ MAC)
  - Multicast (un groupe de destinataires - Ce sont des adresses dont le bit de poids faible du premier octet est 1, par exemple : 01:00:5E:00:00:01).
  - Broadcast (diffusion générale) c'est l'adresse ff:ff:ff:ff:ff:ff qui correspond à toutes les interfaces Ethernet actives sur un réseau Ethernet.
- ***Adresse Source (6 octets)***
  Adresse MAC de l'interface Ethernet émettrice de la trame.

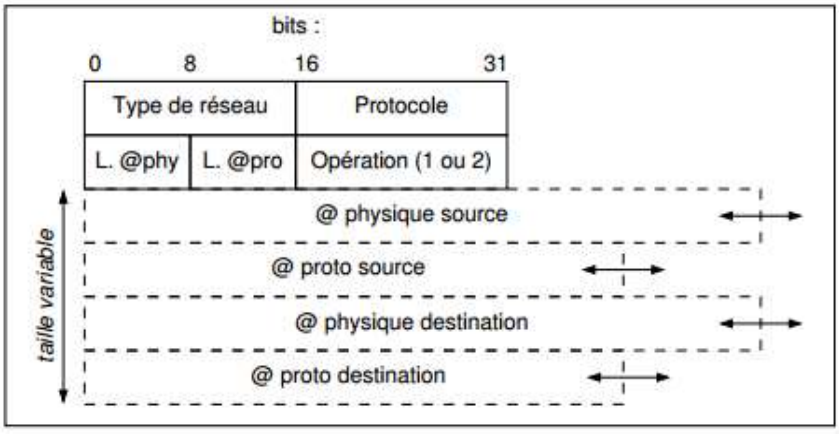
- ***Type de trame - EtherType (2 octets)***
  Indique quel protocole de la couche supérieure est concerné par le message. Quelques types courants (en hexadécimal) sont :
  - 0x0800 : IPv4 (Internet Protocol version 4).
  - 0x0805 : X.25 niveau 3
  - 0x0806: ARP (Address Resolution Protocol)
  - 0x8035 : RARP (Reverse ARP)
  - 0x86DD : IPv6 (Internet Protocol version 6)
  - 0x880B: PPP (Point-to-Point Protocol)
  - 0x8847: MPLS (Multi-Protocol Label Switching)

- ***Données (46 à 1500 octets)***
  Les données véhiculées par la trame. Sur la station destinatrice de la trame, ces octets seront communiqués à l'entité (protocole) indiquée par le champ « EtherType ». Notons que la taille minimale des données est 46 octets. Des octets de bourrage (padding) à 0, sont utilisés pour compléter des données dont la taille est inférieure à 46 octets. La taille minimale de 46 octets est exigée pour le bon fonctionnement du protocole CSMA/CD.
- ***CRC (Cyclic Redundancy Code)***
  Il permet de s'assurer que la trame a été correctement transmise. Le polynôme générateur utilisé est de degré 32.

6.3 PROTOCOLE ARP

Le protocole ARP, pour *Address Resolution Protocol* est décrit par le RFC 826. C'est un protocole situé entre la couche liaison de données et la couche réseau. Il est utilisé pour résoudre le problème d'adresse où un protocole de la couche réseau qui veut envoyer un message à une destination et ne dispose que de son adresse IP, ARP lui permet d'obtenir l'adresse physique de cette destination.

6.3.1 Format du datagramme ARP



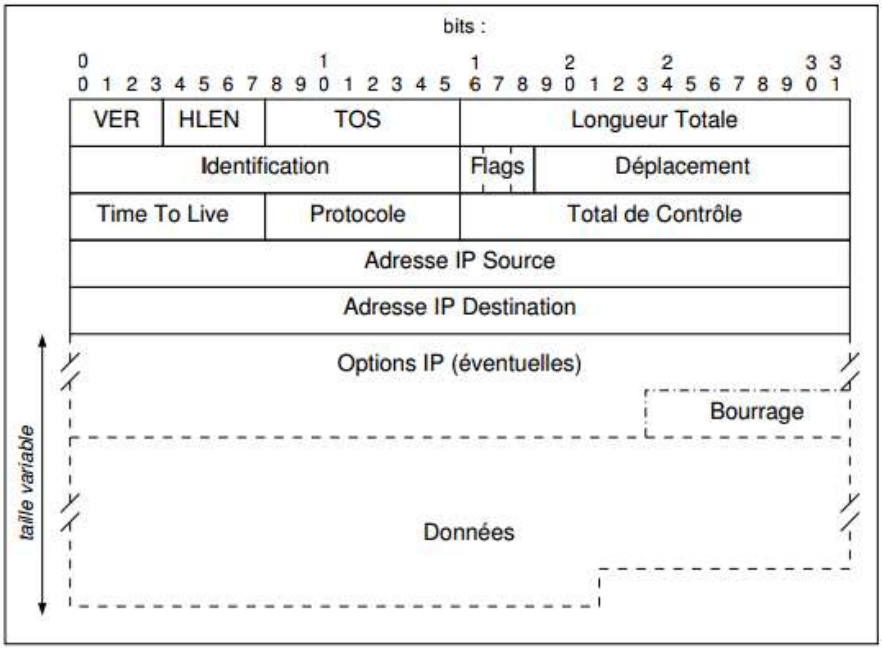
- ***Type de réseau (16 bits)***
  Il indique le type de réseau physique utilisé, ex. pour un réseau Ethernet → « Type de réseau » = 1. Pour les autres types de réseaux, les différentes valeurs possibles pour ce champ sont recensées dans la RFC 1700.
- ***Protocole (16 bits)***
  Il indique le protocole de la couche 3 qui utilise ARP. Pour le protocole IP par exemple ce champ vaut 0x0800. Les différentes valeurs possibles pour ce champ sont recensées dans la RFC 1700.

- ***Longueur de l'adresse physique - L. @phy (8 bits)***
  Il indique le nombre d'octets de l'adresse physique (source et destination) de ce type de réseau. Pour Ethernet, les adresses physiques sont codées sur 6 octets.
- ***Longueur de l'adresse logique - L. @pro (8 bits)***
  Il indique le nombre d'octets de l'adresse logique (source et destination) utilisée par le protocole indiqué dans le champ « Protocole ». Pour IPv4, c'est 4, pour IPv6 c'est 16.
- ***Opération (16 bits)***
  Il indique l'objet (la fonction) du message échangé. Il vaut 1 pour une requête ARP ; 2 pour une réponse ARP.
- ***@physique source (taille variable)***
  Il contient l'adresse physique de l'émetteur. Pour Ethernet, il contient l'@MAC de l'émetteur.
- ***@proto source (taille variable)***
  Il contient l'adresse logique de l'émetteur si connue, ou « 0 » (pour une requête RARP). Dans la spécification TCP/IP, ce champ contient l'adresse IP de source.
- ***@physique destination (taille variable)***
  Il contient l'adresse physique du destinataire, ou « 0 » si inconnue (c'est le cas d'une requête ARP). Pour un réseau Ethernet, il contient l'@MAC du destinataire.
- ***@proto destination (taille variable)***
  Il contient l'adresse logique du destinataire, ou « 0 » si inconnue.

6.4 PROTOCOLE IP

IP (Internet Protocol) est un protocole de niveau réseau dont l'objectif principal est l'interconnexion de réseaux hétérogènes.

6.4.1 Format du paquet IP



- ***VER (4 bits)***
  Il indique la version du protocole IP utilisé. La version actuelle est 4 (soit « 0100 »).

- ***HLEN ou IHL (4 bits)***
  C'est ***I**nternet **H**eader **L**ength*. Cette valeur est à multiplier par 4 pour connaître le nombre d'octets constituant l'en-tête. L'en-tête correspond à la partie du paquet du début jusqu'au « Données ». Le champ IHL permet de savoir s'il y a des options (si le champ « Options » n'est pas nul) et où commencent les données. Sa valeur peut varier de 5 (soit 20 octets d'entête) à 15 (60 octets d'entête), qui s'explique par la présence ou non d'options.
- ***TOS - Type of Service (8 bits)***
  Il indique la qualité du service (priorité, délai, etc.) demandée pour ce paquet.
- ***Longueur Totale (16 bits)***
  Il donne la taille totale en octets du paquet incluant l'entête IP. Ainsi, un paquet ne peut pas excéder ($2^{16} - 1$) octets. Cependant, les paquets IP sont généralement limités à la taille maximale de la trame de données au niveau de la couche liaison, par exemple si la machine est connectée à un réseau Ethernet, elle pourra envoyer un paquet qui entre dans le champ « Données » de la trame qui est limité à 1500 octets. Si le paquet IP est de taille supérieure à ce que le réseau peut transmettre, appelée *Maximum Transfer Unit* (MTU) du réseau, il sera fragmenté par le routeur en des paquets de petite taille, qui pourront être transmis. La taille de chaque sous paquet est égale à la taille des données qu'ils transportent plus la longueur de l'en-tête indiquée dans le champ HLEN. Le paquet d'origine sera reconstitué par le destinataire.
- ***Identification (16 bits)***
  C'est un numéro identifiant le paquet de façon non ambiguë par rapport à sa source. Il permet de rassembler les fragments d'un même paquet pour le reconstituer.
- **Flags (3 bits)**
  Indicateurs de fragmentation. Il se compose des bits suivants :
  - *Reserved (bit 0)* : ce premier bit est inutilisé et il est à « 0 ».
  - *DF - Don't Fragment* : ce deuxième bit indique si la fragmentation est autorisée (s'il est positionné à « 0 ») ou non (s'il est positionné à « 1 »). Si un paquet devant être fragmenté possède le flag DF à 1, il sera détruit, et le routeur envoie un message ICMP « destination inaccessible ».
  - *MF – More Fragments* : si positionné à « 1 », il indique que le paquet est une partie (fragment) du paquet d'origine, et ce n'est pas le dernier fragment. S'il est à « 0 », il indique que c'est le dernier fragment du paquet d'origine.
- ***Déplacement - Offset (13 bits)***
  Il est utilisé seulement dans le cas d'une fragmentation. En multipliant sa valeur par 8, on obtient la position, dans le paquet d'origine, du premier octet de données de ce paquet. Il vaut « 0 » si le paquet n'est pas fragmenté, ou si c'est le premier fragment. Un paquet est non fragmenté lorsque le bit MF et le champ Déplacement sont à « 0 ».
- ***TTL - Time To Live (8 bits)***
  Il fixe la durée de vie du paquet. Il représente la limite du nombre de routeurs pouvant être traversés jusqu'à la destination. Il a pour objectif d'éliminer un paquet qui n'est pas arrivé à destination dans le délai (fragment perdu ou trop retardé). Tout routeur devant transmettre le paquet va décrémenter sa durée de vie de 1 (équivalent à 1 saut).
- ***Proto - Protocole (8 bits)***
  Il indique à quel protocole il faut remettre les données transportées dans ce paquet. Par exemple (en décimal) : « 0 » → IP, « 1 » →ICMP, « 6 » →TCP, « 17 » →UDP.
- ***Checksum (16 bits)***
  Il permet de contrôler l'intégrité de l'entête (sans les données). Si le Checksum calculé par le destinataire est différent de celui figurant dans le paquet, celui-ci sera détruit.
- ***Adresse IP Source (32 bits)***
  Il identifie l'adresse IP de l'émetteur du paquet.
- ***Adresse IP Destination (32 bits)***

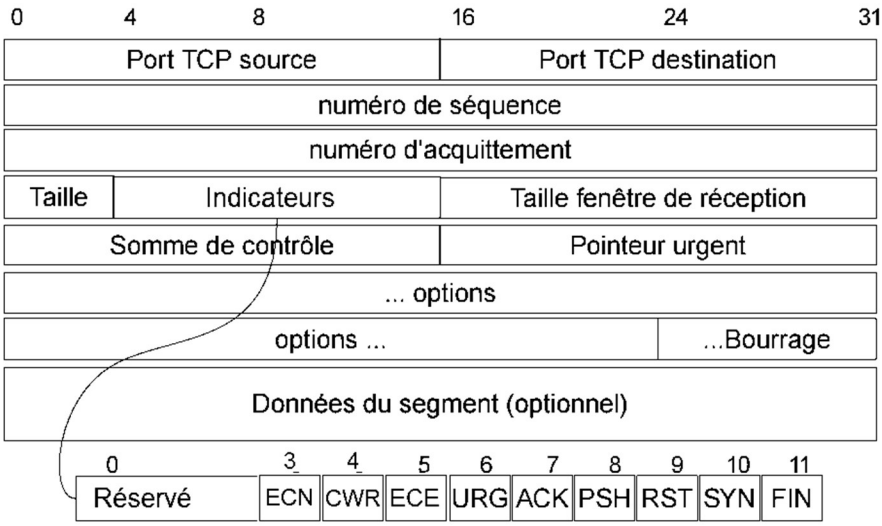
Il identifie l'adresse IP du destinataire du paquet.

- ***Options (taille variable)***
  Il a une taille entre 0 et 40 octets. Il permet de gérer des options : enregistrement d'une route suivie par un paquet, routage stricte définie par la source, etc.
- ***Bourrage (Taille variable)***
  Il a une taille entre 0 et 7 octets. Il n'est présent que pour compléter la taille des options jusqu'à un multiple de 4 octets, parce que la taille de l'en-tête est HLEN × 4 octets.
- ***Données (taille variable)***
  Il contient les données véhiculées par le paquet. Sur la station destinatrice du paquet, ces octets seront communiqués à l'entité (protocole) indiquée par le champ Protocole si le Checksum est confirmé. La taille maximale de ce champ est 65535 moins la longueur de l'en-tête.

6.5 PROTOCOLE TCP

Transmission Control Protocol (TCP) est un protocole de la couche transport. C'est un protocole fiable et fonctionne en mode connecté.

6.5.1 Format du segment TCP



- ***Port TCP source***
  Le numéro du port source.
- ***Port destination.***
  Le numéro du port de destination.
- ***Numéro de séquence***
  Le numéro de séquence du premier octet de ce segment.
- ***Numéro d'acquittement***
  Le numéro de séquence du prochain octet attendu.
- ***Taille***
  La longueur de l'en-tête en mots de 32 bits (les options font partie de l'en-tête)
- ***Indicateurs ou Flags***
  - *Réservé* : réservé pour un usage futur.
  - *ECN/NS* : Il signale la présence de congestion.
  - *CWR - Congestion Window Reduced* : il indique qu'un paquet avec ECE a été reçu et que la congestion a été traitée.
  - *ECE (ECN-Echo)* : si SYN=1, il indique la capacité de gestion ECN, sinon il indique une congestion signalée par IP.

- *URG* : il signale la présence de données urgentes.
- *ACK* : il signale que le paquet est un accusé de réception (Acknowledgement)
- *PSH (Push)* : il indique le cas des données à envoyer tout de suite.
- *RST (Reset)* : Il signale une rupture anormale de la connexion.
- *SYN* : il demande la synchronisation ou l'établissement de connexion.
- *FIN* : il demande la fin de la connexion.

- ***Taille fenêtre de réception***
  Il indique le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception.
- ***Somme de contrôle***
  C'est la somme de contrôle calculée sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP).
- ***Pointeur urgent***
  Sa position est relative des dernières données urgentes.
- ***Options*** (facultatives)
- ***Bourrage***
  Des données de remplissage (des zéros ajoutés) pour aligner les champs suivants du paquet sur 32 bits, si nécessaire.
- ***Données***
  La séquence d'octets transmise par l'application.

7 CONCLUSION GENERALE

L'objectif principal de ce support était de bien mettre sur les rails l'étudiant débutant dans le domaine de l'étude des réseaux informatiques, car un bon démarrage lui permettra de continuer le chemin dans ce domaine avec une base solide. Pour cela, nous nous somme focalisés, dans ce support, sur deux points principaux :

- Faire apprendre à analyser des réseaux réels en utilisant des logiciels appelés renifleurs comme le Wireshark. Ceci permet aux étudiants de voir comment s'effectue réellement l'échange de donnée entre les équipements d'un réseau.
- Faire apprendre à analyser les réseaux par simulation en utilisant des simulateurs comme Packet Tracer de Cisco. Ceci donne la possibilité à l'étudiant d'étudier même les réseaux dont il ne peut pas construire lui-même (un réseau WAN, un réseau privée d'entreprise, etc.).

En se basant sur ces deux points, le support assure, tout au long des TP présentés, l'étude de différents concepts de base sur les réseaux, à savoir, l'encapsulation, l'adressage, le routage, etc.

Ce support résume l'essentiel à savoir pour comprendre, par la pratique, le processus de communication dans un réseau informatique. Il s'intéresse principalement aux fonctionnalités des trois premières couches du modèle OSI, à savoir les couches orientées transmission. Les différents TP qu'il recouvre assurent l'étude et la compréhension de l'échange de données entre les équipements d'un réseau, ainsi que la compréhension du passage de la donnée entre les couches. En effet, il permet de bien percevoir l'aspect complémentaire des couches dans le sens où chaque couche fournit, à travers des protocoles, ses services à la couche supérieure et utilise ceux de la couche inférieure. Ceci est assuré par l'analyse de différent champs de chaque protocole encapsulé dans une trame Ethernet rencontré surtout dans les premiers TP.

Le travail demandé à la fin de chaque TP est fait de telle sorte qu'il soit compréhensible et facile à réaliser par l'étudiant tout seul. Cependant, sa présence est indispensable pour la bonne conduite des TP avec l'aide de l'instructeur.