

SI 5**BTS Services Informatiques
aux Organisations
1^{ère} année****Chapitre 3 :****Les échanges dans le monde TCP-IP****Objectifs :**

Maîtriser le modèle TCP/IP, l'ensemble de ses protocoles, leur fonctionnement et leurs échanges.

Plan :

1. La couche Accès au réseau.
 - 1.1. Les protocoles réseau.
 - 1.2. L'adressage des correspondants.
 - 1.3. L'entête Ethernet.
2. La couche Internet
 - 2.1. le protocole IP.
 - 2.2. Les protocoles ARP et RARP.
 - 2.3. Le protocole ICMP.
3. La couche Hôte à hôte.
 - 3.1. TCP.
 - 3.2. UDP.
 - 3.3. Les ports de la couche Transport.

Ressources :

<http://www.frameip.com>

1. La couche Accès au réseau.

1.1. Les protocoles réseau.

La couche accès réseau est composée de protocoles réseaux qui ont en charge l'envoi de façon correcte des trames et l'adressage vers le ou les bons destinataires.

On y retrouve alors les protocoles suivants (liste non exhaustive) :

- IEEE 802.3 : Ethernet
- IEEE 802.4 : Apple Talk (obsolète)
- IEEE 802.5 : Token Ring

- IEEE 802.11 : Réseaux sans fils (WIFI, FSO)
- IEEE 802.15 : Réseaux WPAN (Bluetooth)
- IEEE 802.16 : Réseaux BLR (WiMax)

Par défaut, les réseaux IEEE 802.11 ont leurs propres caractéristiques techniques de transmission. Pour communiquer avec les autres éléments d'un réseau local, ils utilisent un pont, et exploitent le protocole réseau de base : Ethernet le plus souvent, encore parfois Token Ring.

1.2. L'adressage des correspondants.

Comme nous l'avons déjà vu, le travail de la couche Accès au réseau, est de renseigner les adresses physiques de l'émetteur et du destinataire.

Cette dernière fait m'objet d'une découverte grâce au protocole ARP et stockées dans la table ARP du poste.

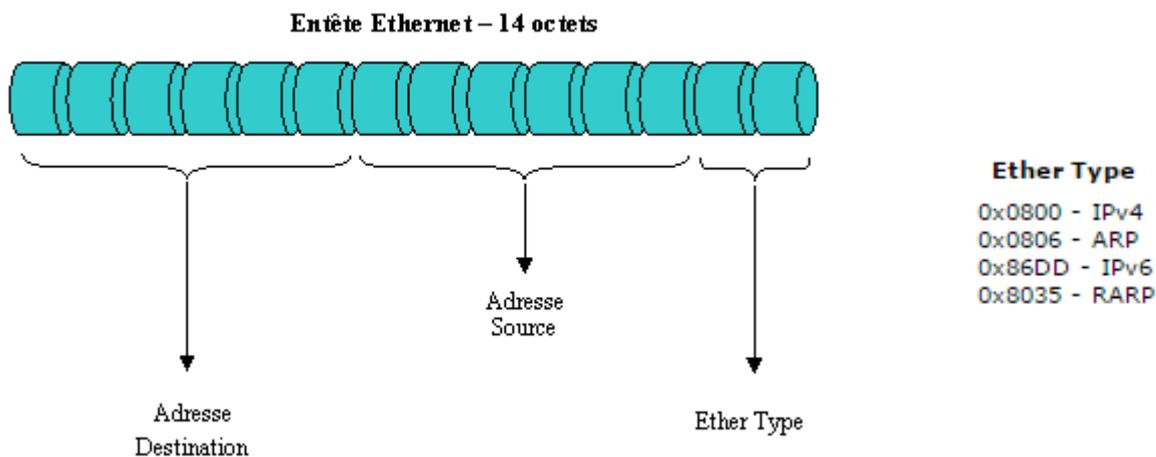
L'adresse physique d'une interface réseau est son adresse MAC, codée sur 6 octets.

La partie OUI (Organizationally Unique Identifier) est destinée à identifier les fabricants.

Les adresses physiques sont également parfois appelées adresse **Ethernet**, **UAA** (Universally Administered Address), **BIA** (Burned-In Address), **MAC-48** ou **EUI-48**.

Enfin, à noter qu'il existe un format d'adresses physiques, nommé EUI-64, dans lequel l'OUI a une taille de 5 octets. Elle est utilisée actuellement dans les adresses auto-attribuées d'IPv6, pour les périphériques FireWire, ...

1.3. L'entête Ethernet.

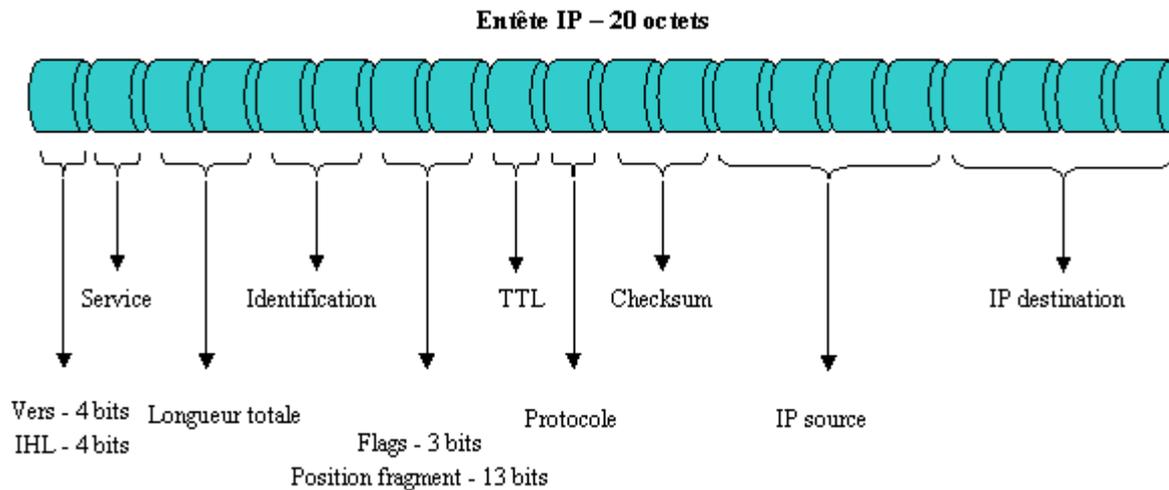


2. La couche Internet

2.1. le protocole IP.

IP (Internet Protocol, Protocole Internet) est un protocole qui se **charge de l'adressage des paquets**. Ainsi, c'est ce protocole qui est en charge de compléter l'entête Internet de d'y préciser, entre autre, les adresses IP expéditeur et destinataire.

Entête IPv4 :



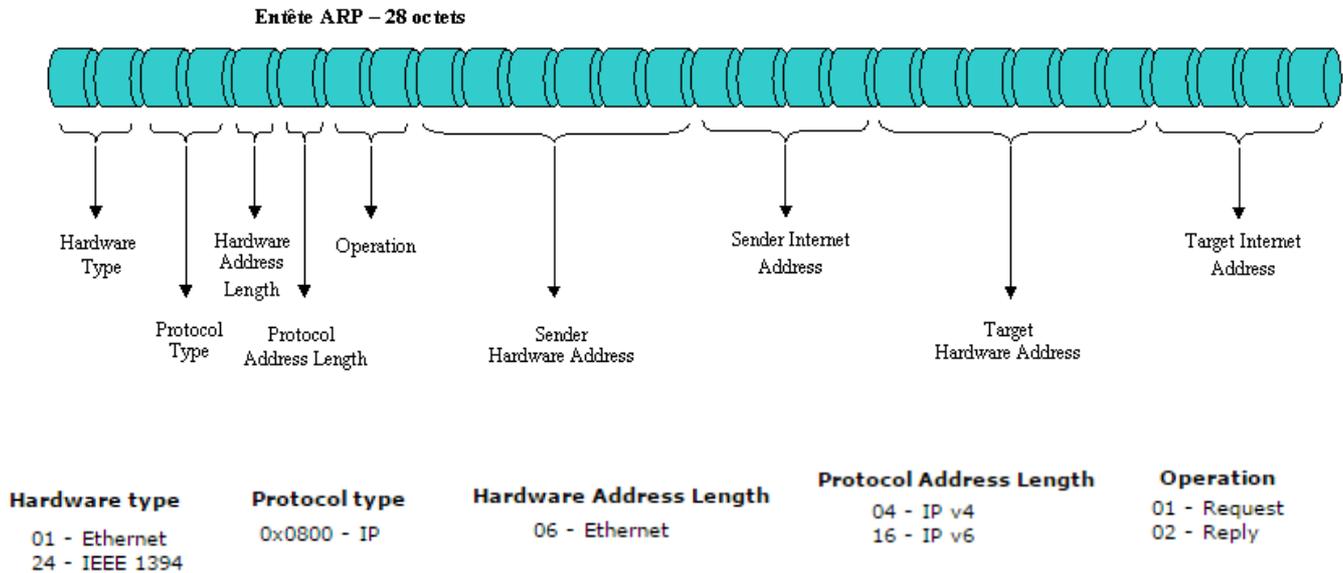
Vers	04 - IP V4 06 - IP V6
IHL	Longueur de l'entête IP, exprimé par bloc de 4 octets Valeur par défaut : 5 (soit 5*4=20 octets)
Service	Permet de spécifier les valeurs nécessaire à la mise en œuvre de la qualité de Service QoS
Longueur totale	Longueur totale du paquet, incluant l'entête et les données.
Identification	Identifiant du message envoyé.
Flags	Permet de savoir si le message a fait l'objet d'une fragmentation, et si c'est le cas, s'il s'agit ou non du dernier fragment.
Position fragment	Si le message est fragmenté, chaque fragment reçoit un identifiant permettant de reconstituer le message initial.
TTL	Représente la durée de vie en seconde du paquet. Si le TTL arrive à 0, alors l'équipement qui possède le paquet, le détruira. Cette durée de vie est décrétementée uniquement au sein des routeurs, avec un minimum de 1 à chaque routeur.
Protocole	01 - ICMP 06 - TCP 17 - UDP
Checksum	Valeur de contrôle de l'intégrité de l'entête Internet
Adresse IP source	Adresses IPv4 sources et destination
Adresse IP destination	

IPv6 fera l'objet d'une découverte plus tard.

2.2. Les protocoles ARP et RARP.

Le protocole ARP permet une résolution d'adresse MAC d'après une adresse IP, nécessaire pour le remplissage de l'entête Ethernet.

La résolution se fait via deux requêtes : une requête **ARP request**, émise en broadcast, et une requête **ARP reply**, unicast.



Les valeurs précédentes ne sont données qu'à titre d'exemples et ne se veulent pas exhaustives.

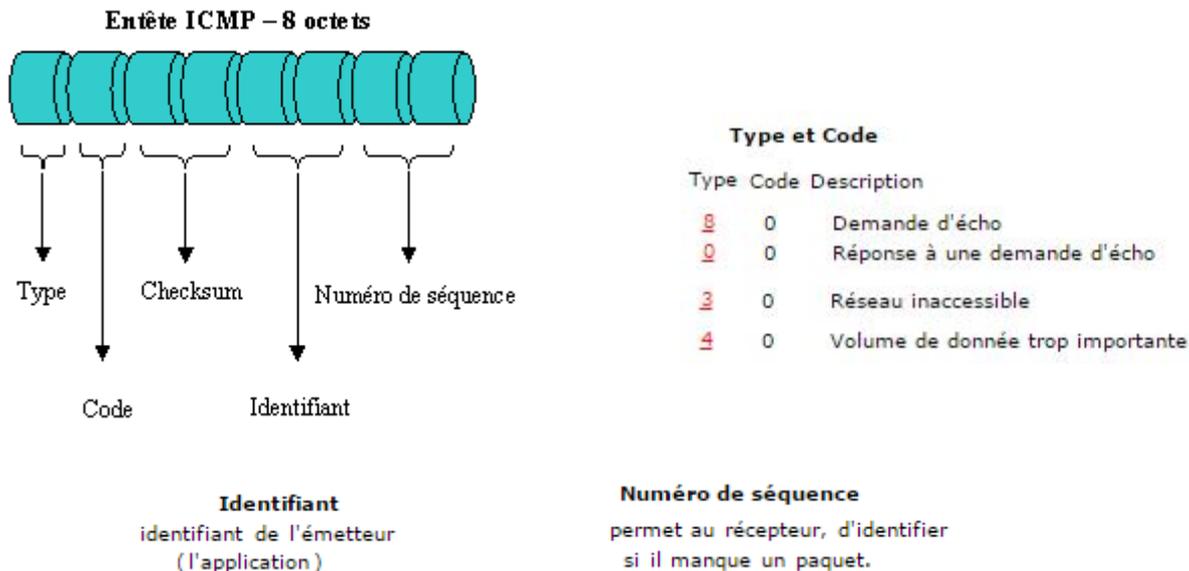
Le protocole RARP permet de retrouver une adresse IP à partir d'une adresse MAC, de façon similaire à ARP.

A noter que les protocoles ARP et RARP font partie de la couche Internet, mais que les trames ARP et RARP sont dénuées d'entête IP. C'est pourquoi on place ces protocoles en partie basse de la couche Internet (en dessous de IP).

2.3. Le protocole ICMP.

ICMP est un protocole permet de gérer les informations relatives aux erreurs du protocole IP. Il est implémenté dans tous les matériels d'infrastructure administrables (commutateurs, routeurs, ponts, ...).

L'outil PING est le principal outil. Toutefois, les matériels d'infrastructure émettent des trames ICMP pour délivrer des informations au réseau.



Quelques détails :

Type,Code : 8,0 = PING Request

0,0 = PING reply

3,0 = Le routeur ne peut acheminer le paquet (IP destinataire inconnue)*

4,0 = Le routeur manque de mémoire pour traiter ce paquet*.

** ce type de trame est émis directement par les routeurs à destination de l'émetteur de la trame faisant l'objet d'un impossible traitement.*

A noter que le protocole ICMP fait partie de la couche Internet, et que les trames ICMP incluent un entête IP. C'est pourquoi on place ces protocoles en partie haute de la couche Internet (au dessus de IP).

3. La couche Hôte à hôte.

3.1. TCP.

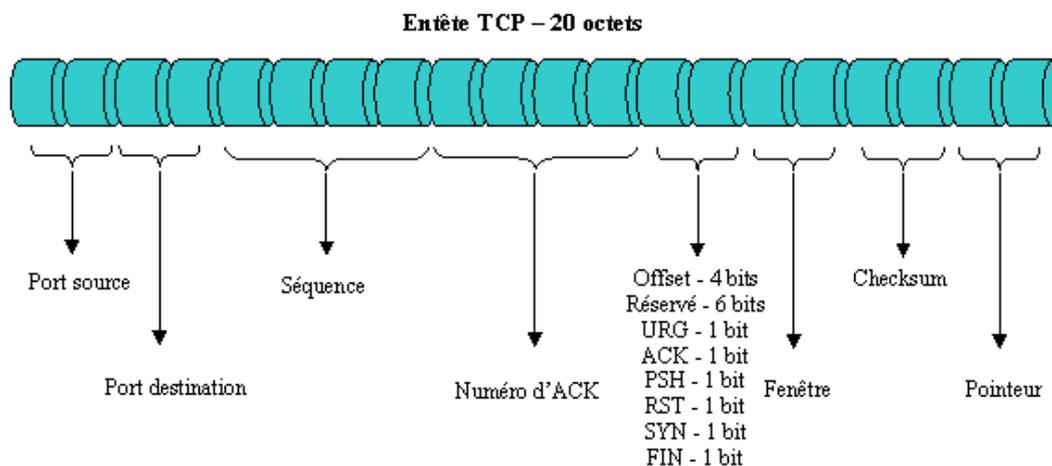
TCP (Transmission Control Protocol, Protocole de contrôle de la transmission) est probablement le protocole transport le plus répandu. **TCP fournit un service sécurisé de remise des paquets.** TCP est un protocole fiable, orienté **connexion**.

TCP garantit l'ordre et la remise des paquets, il vérifie l'intégrité de l'entête des paquets et des données qu'ils contiennent. TCP est responsable de la retransmission des paquets altérés ou perdus par le réseau lors de leur transmission.

Cette fiabilité fait de TCP un protocole bien adapté pour la transmission de données basée sur la session, les applications client-serveur et les services critiques tels que le courrier électronique.

La fiabilité de TCP a un prix. Les entêtes TCP requièrent l'utilisation de bits supplémentaires pour effectuer correctement la mise en séquence des informations, ainsi qu'un total de contrôle obligatoire pour assurer la fiabilité non seulement de l'en-tête TCP, mais aussi des données contenues dans le paquet. Pour garantir la réussite de la livraison des données, ce protocole exige également que **le destinataire accuse réception des données**.

Ces accusés de réception (ACK) génèrent une activité réseau supplémentaire qui diminue le débit de la transmission des données au profit de la fiabilité. Pour limiter l'impact de cette contrainte sur la performance, la plupart des hôtes n'envoient un accusé de réception que pour un segment sur deux ou lorsque le délai imparti pour un ACK expire.



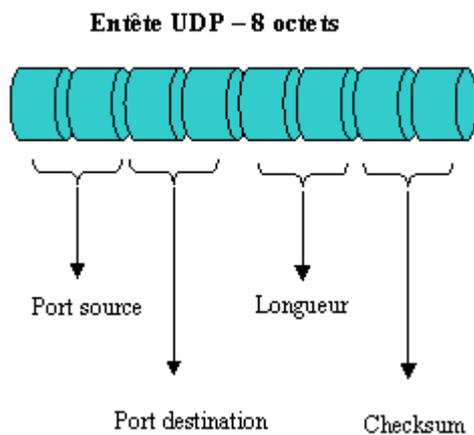
Port Source	Port de réponse définit par l'application initiatrice de la communication
Port Destination	Port d'écoute du service sur le serveur, avec qui la communication a été établie.
Séquence	Numéro du paquet
Numéro d'ACK	Numéro d'accusé de réception, permettant de vérifier le bon acheminement des données
Offset	Taille de l'entête TCP, exprimée par blocs de 4 octets.
Réservé	Positionné à 0 en attendant une utilité non encore définie.
Flags	URG : Si le paquet est marqué urgent ACK : Il s'agit d'un accusé de réception PSH : Indicateur de requête terminée. RST : Demande de réinitialisation de la connexion SYN : Demande de connexion synchronisée FIN : Indique la fin de la connexion
Fenêtre	Nombre d'octets que le récepteur a encore la possibilité de recevoir. En cas de dépassement, une trame ICMP 4,0 est émise.
Checksum	...
Pointeur	Permet de définir le numéro de séquence de la donnée urgente.

3.2. UDP.

UDP (User Datagram Protocol) est un complément du protocole TCP qui offre un **service de remise de datagrammes sans connexion** qui ne garantit ni la remise ni l'ordre des paquets délivrés. Les sommes de contrôle des données sont facultatives dans le protocole UDP.

Ceci permet d'échanger des données sur des réseaux à fiabilité élevée sans utiliser inutilement des ressources réseau ou du temps de traitement. Les messages (ou paquets UDP) sont transmis de manière autonome (sans garantie de livraison.).

Ex: TFTP (trivial FTP) s'appuie sur UDP, DHCP également, Windows utilise UDP pour les Broadcast en TCP-IP.



Port Source	Port de réponse définit par l'application initiatrice de la communication
Port Destination	Port d'écoute du service sur le serveur, avec qui la communication a été établie.
Longueur	Taille de l'entête UDP et de ses données (tout ce qui est placé derrière l'entête).
Checksum	...

3.3. Les ports de la couche Transport.

Afin que plusieurs applications d'un même client puissent communiquer en même temps sur le réseau, et que plusieurs services réseaux puissent répondre en même temps sur un même serveur, il faut que les données partent et reviennent sur des **canaux de communication**.

Les ports d'écoute des services réseaux sont généralement définis dans la liste dite des **ports bien connus** (Well Known Ports), dont le numéro est inférieur à 1024. Rien n'empêche un service réseau d'écouter un **port supérieur ou égal à 1024**.

Ainsi, tout service réseau sur un serveur écoute un port unique sur ce serveur. Par exemple, on définit par défaut le service web sur le port 80 et le service SSH sur le port 22.

Les **ports établis**, ou ports de réponse, sont définis pour l'application émettrice, afin de s'assurer du bon retour des réponses du serveur contacté.

Chaque port est distribué de façon aléatoire aux applications qui en font la demande, et toujours de façon unique. Les ports établis sont définis comme étant supérieurs ou égaux à 1024, mais en raison du débordement des ports d'écoute en dehors des ports bien connus, les ports établis sont souvent supérieurs à 30000.

Les ports bien connus à connaître :

Service réseau	N° de Port	Description
ICMP	7	Commandes Ping
FTP	20	Échange des données
	21	Connexion et manipulation du répertoire FTP distant
SSH	22	Connexion distante sécurisée par clé asymétrique
DNS	53	Serveurs de noms de domaine
BOOTPS	67	Port d'écoute du Serveur DHCP
BOOTPC	68	Port établi du Client DHCP
HTTP	80	Serveur Web
HTTPS	443	Serveur Web avec transmission sécurisée
SMTP	25	Envoi de courriels
SMTPS	465	Emission sécurisée de courriels
POP3	110	Réception de courriels
POP3S	995	Réception sécurisée de courriels

3.4. Le fonctionnement des routeurs NAT.

Comme nous l'avons déjà vu, les routeurs NAT substituent l'adresse IP d'une trame sortante par l'adresse IP déterminée pour que la trame puisse être transmise sur le réseau (généralement Internet).

En fait, ils changent également le port d'écoute précisé dans l'entête Hôte à hôte.

Ainsi, ils peuvent aisément identifier les trames à leur retour, et remettre en place l'adresse IP et le port d'écoute, afin de garantir d'envoyer la trame vers le bon destinataire.