USTHB-Info |2023

COURS
RÉSEAUX
L3 ACAD

Par
Dr. Khadidja CHAOUI

PLAN

I. Introduction aux réseaux informatiques

II. Transmission de données

III. Protocoles de transmission

IV. Les réseaux locaux

V. Architecture des réseaux informatiques

CHAPITRE V

Architecture des réseaux informatiques

V.1 Introduction

- Le rôle principal de la couche réseau est de :

-Transporter des paquets de la source vers la destination via les différentes nœuds de commutation du réseaux traversés

-Trouver un chemin tout en assurant une régulation et répartition de la charge des réseaux

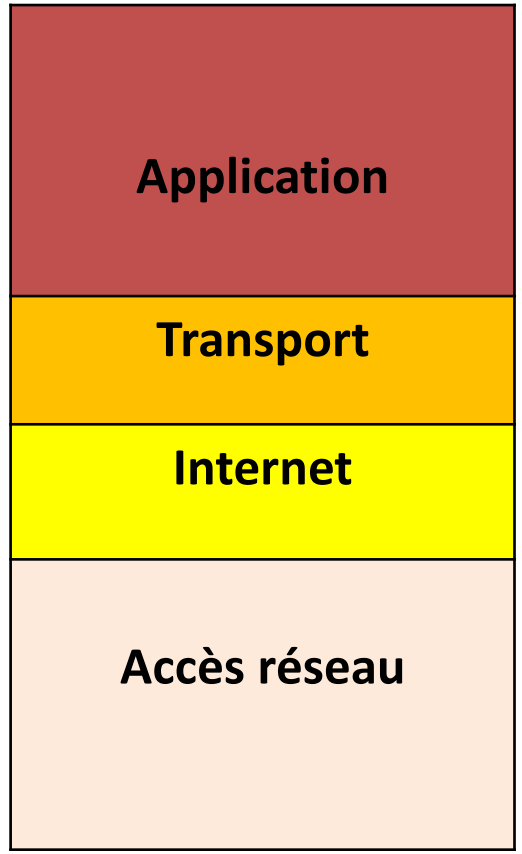
Ce rôle est assuré par un ensemble de fonctions :

- Fragmentation et réassemblage
- Adressage et routage

V.2 Architecture de la pile TCP/IP

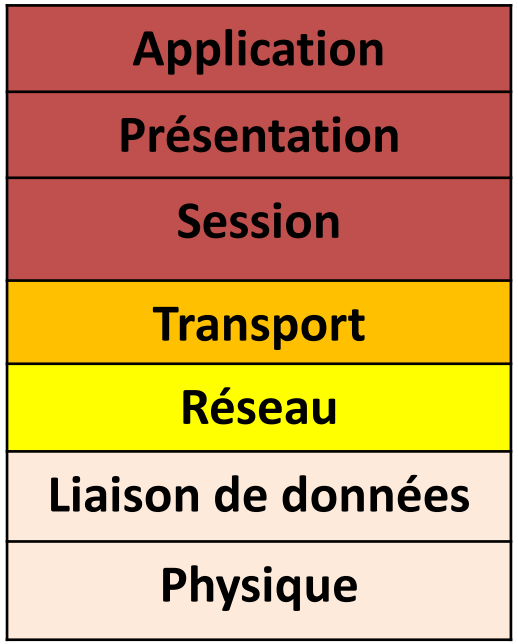
TCP/IP est structuré en quatre couches de protocoles :

- *La couche Accès réseau* est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.
- *La couche Internet* gère la circulation des paquets à travers le réseau en assurant leur routage.
- *La couche Transport* assure tout d'abord une communication de bout en bout.
- *La couche Application* est celle des programmes utilisateurs, tels que telnet (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc.

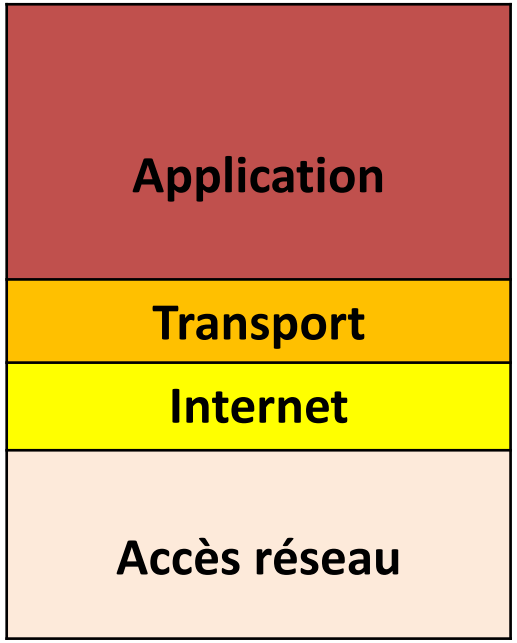


Comparaison avec le modèle TCP/IP

- Les protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle OSI



Modèle OSI



Modèle TCP/IP

V.3. L'adressage IP

V.3.1. Définition d'une adresse IP

- Chaque ordinateur, d'un même réseau, doit dispose d'une adresse IP unique (codée sur 32bits pour IPv4).
- Une adresse IP est représentée dans une notation décimale pointée, constituée de 4 nombres compris chacun entre 0 et 255 et séparés par un point.:

197 . 75 . 200 . 22

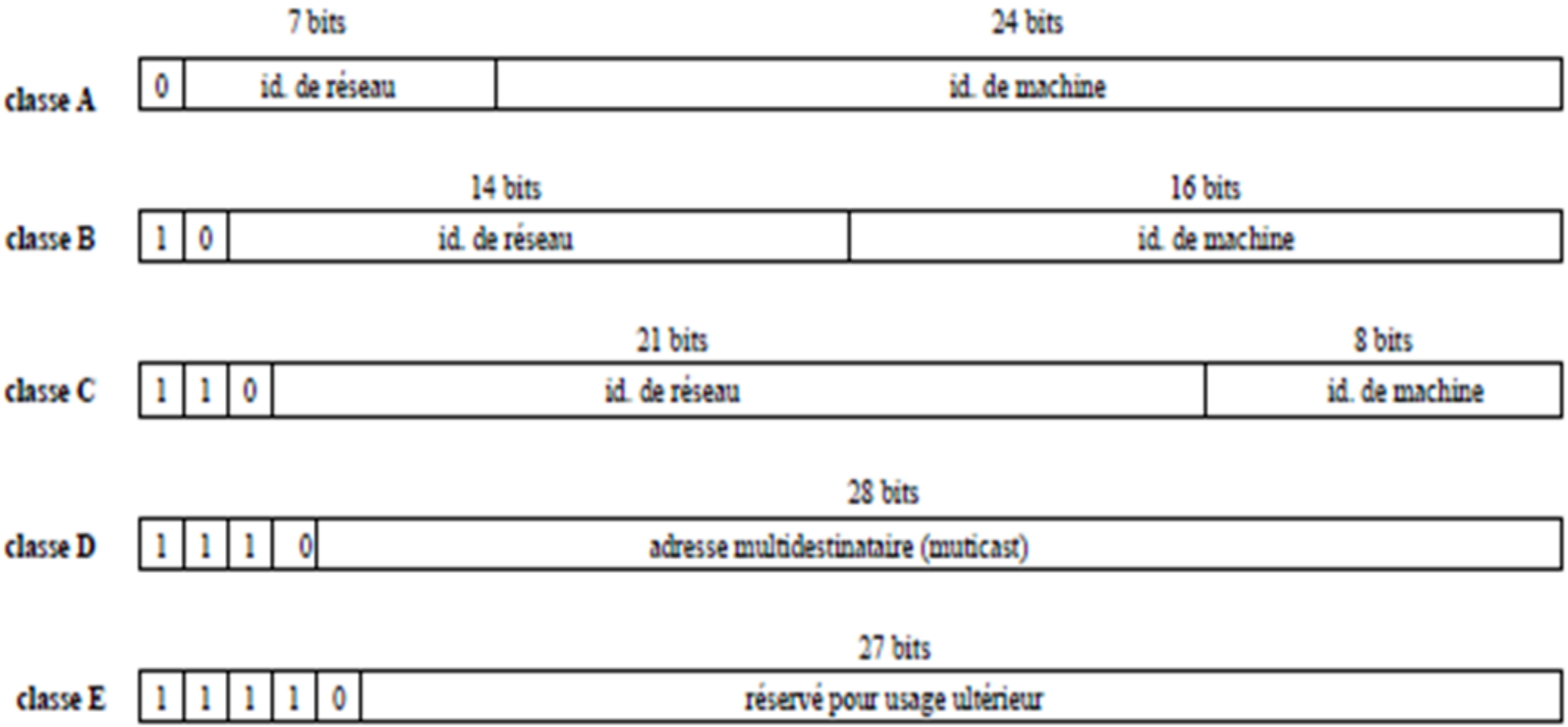
11000101. 01001011. 11001000. 00010110

- Une adresse IP se décompose en :
  - **Partie réseau:** située à l'extrême gauche de l'adresse qui indique le réseau dont l'adresse IP est membre. Tous les périphériques du même réseau ont, dans leur adresse IP, la même partie réseau
  - **Partie machine:** représente la partie restante de l'adresse qui identifie un appareil spécifique sur le réseau. Cette partie est unique pour chaque appareil ou interface sur le réseau.

- Initialement, 5 classes d'adresse (*A*, *B*, *C, D* et *E*) ont été définies qui instaurent une certaine hiérarchie. Une adresse IP appartient à une classe donnée selon la valeur de son premier octet.

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques
E	non défini	240.0.0.0 - 255.255.255.255	adresses uniques	adresses uniques

- *Si le premier bit est 0,* l'adresse est de *classe A*. On dispose de 7 bits pour identifier le réseau et de 24 bits pour identifier l'hôte. On a donc les réseaux de 1 à 127 et 224 hôtes possibles, c'est à dire 16 777 216 machines différentes (de 0 à 16 777 215).
- *Si les deux premiers bits sont 10,* l'adresse est de *classe B*. Il reste 14 bits pour identifier le réseau et 16 bits pour identifier la machine. Ce qui fait 2^{14} = 16 384 réseaux (128.0 à 191.255) et 65 534 (65 536 − 2) machines.
- *Si les trois premiers bits sont 110,* l'adresse est de *classe C*. Il reste 21 bits pour identifier le réseau et 8 bits pour identifier la machine. Ce qui fait 2^{21} = 2 097 152 réseaux (de 192.0.0 à 223.255.255) et 254 (256−2) machines.
- *Si les quatre premiers bits de l'adresse sont 1110*, il s'agit d'une classe d'adressage spéciale, la *classe D*. Cette classe est prévue pour faire du "multicast ", ou multipoint. (RFC 1112 [S. Deering, 1989]), contrairement aux trois premières classes qui sont dédiées à l'unicast ou point à point.
- *Si les quatre premiers bits de l'adresse sont 1111*, il s'agit d'une classe expérimentale, la *classe E*. La RFC 1700 précise "*Class E addresses are reserved for future use*".


7 bits
24 bits
classe A
0
id. de réseau
id. de machine
14 bits
16 bits
classe B
1
0
id. de réseau
id. de machine
21 bits
8 bits
classe C
1
1
0
id. de réseau
id. de machine
28 bits
classe D
1
1
1
0
adresse multidestinataire (muticast)
27 bits
classe E
1
1
1
1
0
réservé pour usage ultérieur

V.3.2 Adresses particulières

- *<id. de réseau nul>.<id. de machine>* est utilisée pour désigner une machine sur son réseau lors d'un boot (processus d'amorçage). 0.0.0.0 est aussi utilisée par une machine pour connaître sa propre adresse IP lors d'un processus d'amorçage par exemple.
- *<id. de réseau>.<id. de machine nul>* permet de désigner le réseau lui-même.
- *<id. de réseau>.<id. de machine avec tous ses bits à 1>* est une adresse de *diffusion* ou de *broadcasting*, c'est-à-dire qu'elle désigne toutes les machines du réseau identifié. Un datagramme adressé à cette adresse sera ainsi envoyé à toutes les machines du réseau *<id. de réseau>*.
- *255.255.255.255* est une adresse de diffusion locale, car elle désigne toutes les machines du réseau auquel appartient l'ordinateur qui utilise cette adresse. L'avantage par rapport à l'adresse précédente est que l'émetteur n'est pas obligé de connaître l'adresse du réseau auquel il appartient.
- *127.0.0.0* est un réseau d'adresses de bouclage qui est utilisée pour permettre les communications interprocessus sur un même ordinateur ou réaliser des tests de logiciels, car tout logiciel de communication recevant des données pour ces adresses les retourne simplement à l'émetteur.

- Les adresses de classe *A* de 10.0.0.0 à 10.255.255.255, de classe *B* de 172.16.0.0 à 172.31.255.255 et de classe *C* de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux locaux privés (*Intranet).*
- On les appelle les *adresses privées*, à l'inverse des *adresses publiques* qui sont celles utilisées pour identifier les machines sur Internet.
- Un *Intranet* est un réseau d'étendue géographique très limitée, par exemple pour une entreprise, basé sur la technologie TCP/IP mais non relié à Internet. Un *Extranet* est également un réseau privé bâti sur TCP/IP, non connecté à Internet, mais réparti sur des sites géographiques distants.
- Les adresses de réseaux publique d'Internet sont affectées par un organisme international: *ICANN (Internet Corporation for Assigned Names and Numbers)*.

V.3.3 Adressage des sous réseaux.

- Le système des adresses IP permet également la définition d'adresses de sous-réseaux en découpant *la partie <ID machine>* en deux parties :
  - Un *identificateur* de sous-réseau : Nombre de bits nécessaire pour identifier tous les sous réseaux
  - Un identificateur machine : Le reste de bits pour identifier toutes les machines de chaque sous réseau
  - **Exemple :** Un réseau de classe *B*, sur lequel on pourrait nommer 65 534 machines pourra être décomposé en 254 sous-réseaux de 254 machines comme suit :
- ***<id. de réseau sur 16 bits>. <id. de sous-réseau sur 8 bits>. <id. de machine sur 8 bits>***
- L'administrateur d'un réseau peut décider de découper où il veut la zone des identificateurs de machines, ce découpage facilite le travail des routeurs. Cette technique a pour effet de provoquer un routage hiérarchique.

V.3.3. Le masque de sous réseau

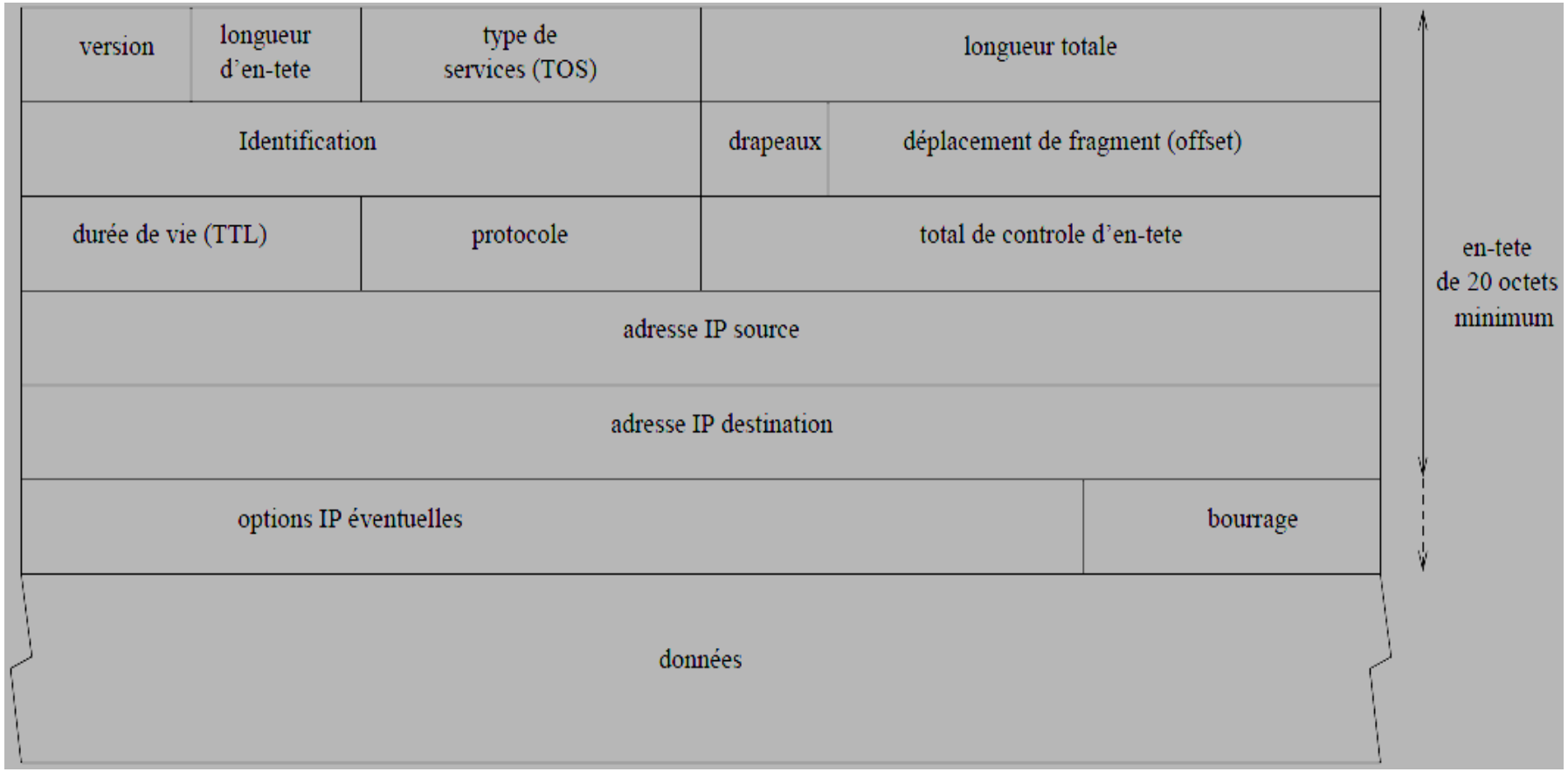
- Pour permettre au routeur de faire la séparation entre la partie réseau et la partie machine de l'adresse IP, on introduit la *masque de sous réseaux.*
- **Adresse machine AND Masque de réseau = Adresse du réseau de destination**

V. 4 La couche réseau : le protocole IP

- Le protocole IP (Internet Protocol, RFC 791) est au cœur du fonctionnement d'un internet. Son rôle est centré autour de trois fonctionnalités :
  - Définir le format du datagramme IP qui est l'unité de base des données circulant sur Internet.
  - Définir le routage dans Internet.
  - Définir la gestion de la remise non fiable des datagrammes.
- Le protocole IP assure un service *non fiable* de délivrance de datagrammes IP. En effet, il n'existe aucune garantie pour que les datagrammes IP arrivent à destination, puisqu'il est *sans connexion*. Certains datagrammes peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre.

V.4.1 Le datagramme IP

Un datagramme IP est constitué d'un en-tête suivi d'un champ de données. Sa structure précise est détaillée :



- *Le champ version* du protocole IP utilisé (IPv4 ou 6), codé sur 4 bits.
- *Le champ longueur d'en-tête* du datagramme IP codé sur 4 bits
- *Le champ TOS(Type Of Service)* codé sur 8 bits: indique la façon dont le datagramme doit être traité et se décompose en six sous champs comme suit :

  - *Le champ priorité* varie de 0 (000) priorité normale (valeur par défaut) à 7 (111) priorité maximale et permet d'indiquer l'importance de chaque datagramme : Suivant les valeurs de ce champ, le routeur peut privilégier un datagramme par rapport à un autre.
  - Les 4 bits *D, T, R, C* indiquent au routeur l'attitude à avoir vis à vis de ce datagramme :

- *D* est mis à 1 pour essayer de minimiser le délai d'acheminement (ex : choisir un câble sous-marin plutôt qu'une liaison satellite),
- *T* est mis à 1 pour maximiser le débit de transmission,
- *R* est mis à 1 pour assurer une plus grande fiabilité et
- *C* est mis à 1 pour minimiser les coûts de transmission (une fct coût).

Ces 4 bits servent à améliorer la qualité du routage et ne sont pas exigées. Simplement, si un routeur connaît plusieurs voies de sortie pour une même destination, il pourra choisir celle qui correspond le mieux à la demande.

application	minimiser le délai	maximiser le débit	maximiser la fiabilité	minimiser le coût
telnet / rlogin	1	0	0	0
FTP				
contrôle	1	0	0	0
transfert	0	1	0	0
SMTP				
commandes	1	0	0	0
données	0	1	0	0
NNTP	0	0	0	1
SNMP	0	0	1	0

- *Le champ longueur totale* en octets du datagramme. Ce champ est sur 2 octets on en déduit que la taille complète d'un datagramme ne peut dépasser *65535 octets*. Utilisée avec la longueur de l'en-tête elle permet de déterminer où commencent exactement les données transportées.
- *Les champs identification (16 bits), drapeaux (3bits) et déplacement de fragment (13 bits) :* interviennent dans le processus de fragmentation des datagrammes IP.
- *Le champ durée de vie (TTL)* codé sur 8 bits indique le nombre maximal de routeurs que peut traverser le datagramme IP. Il est initialisé à *N (souvent 32 ou 64)* par la station émettrice et décrémenté de 1 (il perd une vie) par chaque routeur qui le reçoit et le réexpédie. Lorsqu'un routeur reçoit un datagramme dont la durée de vie est nulle (TTL = 0), il le détruit et de ce fait, il est impossible qu'un datagramme tourne indéfiniment dans le réseau.

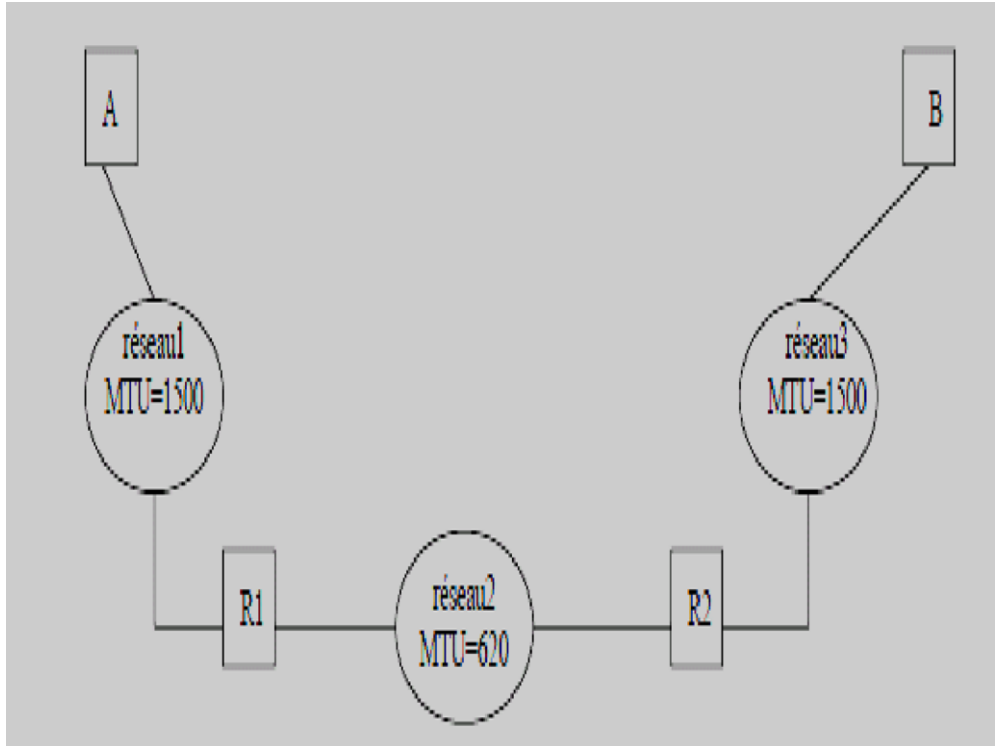
- Le champ *déplacement de fragment (offset)* précise la localisation du début du fragment dans le datagramme initial.
- Les fragments sont des datagrammes dont l'en-tête est quasiment identique à celle du datagramme original.
  - Le champ identification est un entier qui identifie de manière unique chaque datagramme émis, ce champ est recopié dans le champ identification de chacun des fragments si ce datagramme est fragmenté.
  - Le champ longueur totale est recalculé pour chaque fragment. Chaque fragment est un datagramme indépendant, susceptible d'être à son tour fragmenté.
  - Le champ *drapeaux* comprend trois bits dont deux qui contrôlent la fragmentation. S'il est positionné à 1, *le premier bit indique que l'on ne doit pas fragmenter le datagramme* et si un routeur doit fragmenter un tel datagramme, alors il le rejette et envoie un message d'erreur à l'expéditeur.
  - Un autre bit appelé *fragments à suivre* est mis systématiquement à 1 pour tous les fragments qui composent un datagramme sauf le dernier. Ainsi, quand le destinataire reçoit le fragment dont le bit *fragment à suivre* est à 0, il est apte à déterminer s'il a reçu tous les fragments du datagramme initial, grâce notamment aux champs *offset* et *longueur totale* de ce dernier fragment.

- *Le champ protocole* codé sur 8 bits identifie le protocole de plus haut niveau qui a servi a créé ce datagramme. Les valeurs sont **1** pour ICMP, **2** pour IGMP, **6** pour TCP et **17** pour UDP. Ainsi, la couche IP de la station destinatrice qui reçoit le datagramme IP pourra diriger les données qu'il contient vers le protocole supérieur adéquat.
- *Le champ Total de contrôle d'en tête* (HEADER CHECKSUM), codé sur 16 bits pour s'assurer de l'intégrité de l'en-tête. A la réception de chaque paquet, la couche calcule cette valeur, si elle ne correspond pas à celle trouvée dans l'en-tête, le datagramme est oublié ("*discarded*") sans message d'erreur.
- *Les adresses IP source et destination* sur 32 bits.
- *Le champ options* est une liste de longueur variable, mais toujours complétée par des bits de bourrage pour atteindre une taille multiple de 32 bits. Ces options sont très peu utilisées car peu de machines sont aptes à les gérer. Parmi elles, on trouve des options de sécurité et de gestion (domaine militaire), d'enregistrement de la route, d'estampille horaire, routage strict, etc...

V.4.2 Fragmentation des datagrammes IP

- La taille maximale d'un datagramme IP est de 65535 octets. Pour optimiser le débit, il est préférable qu'un datagramme IP soit encapsulé dans une seule trame de niveau 2 (Ethernet par exemple).
- Un datagramme IP peut transiter à travers Internet sur un ensemble de réseaux aux technologies différentes, il est impossible de définir, a priori, une taille maximale des datagrammes IP qui permette de les encapsuler dans un seul type de trame (1500 octets pour Ethernet et 4470 pour FDDI). En effet, chaque réseau est caractérisé par une taille maximale d'une trame, appelée *la MTU (Maximum Transfert Unit).*
- Ceci cause un problème lorsqu'un routeur reçoit des datagrammes issus d'un réseau à grande *MTU* et doit les réexpédier vers un réseau à plus petite *MTU*.
- Pour remédier à ce problème, on a recourt à la *fragmentation des datagrammes*. Celle-ci se fait au niveau d'un routeur. La *MTU* est utilisée pour fragmenter les datagrammes trop grands pour le réseau qu'ils traversent. Si le *MTU* d'un réseau traversé est suffisamment grand pour accepter un datagramme, évidemment il sera encapsulé tel quel dans la trame du réseau traversé.

Exemple : Si la station *A*, reliée à un réseau Ethernet, envoie un datagramme de 1300 octets à destination de la station *B*, reliée également à un réseau Ethernet, le routeur R_1 relié à un réseau de *MTU=620* octets ne pourra faire le routage des datagrammes. Le routeur R_1 va fragmenter le datagramme de 1300 octets envoyé par la station *A* à destination de la station *B*, de la manière suivante :



datagramme initial	en-tête du datagramme	données1 600 octets	données2 600 octets	données3 80 octets
fragment1	en-tête du fragment1	données1 600 octets	déplacement 0	
fragment2	en-tête du fragment2	données2 600 octets	déplacement 600	
fragment3	en-tête du fragment3	données3 80 octets	déplacement 1200	

V.4.3 Protocole ARP

- ARP fournit une correspondance dynamique entre une adresse IP connue et l'adresse matérielle lui correspondant.

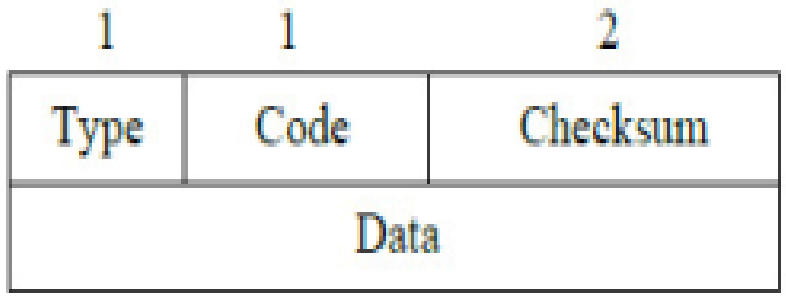
Fonctionnement

- Le module ARP envoie une requête ARP dans une trame Ethernet avec une adresse de destination broadcast (ff:ff:ff:ff:ff:ff). Ainsi, toutes les machines du réseau local reçoivent cette requête contenant l'adresse IP à résoudre.
- La couche ARP de la machine du serveur reconnaît que cette requête lui est destinée et répond par une réponse ARP contenant son adresse matérielle (par exemple 00:20:AF:AB:42:43). Les autres machines du réseau ignorent la requête.
- La réponse ARP est reçue par l'émetteur de la requête. Pour ce retour, il n'y a pas de problème de résolution puisque l'adresse physique du client étant envoyée dans la requête *elle est connue de la machine qui répond*.
- La réponse ARP est reçue par la couche ARP du client, et le driver Ethernet peut alors émettre le paquet IP avec la bonne adresse Ethernet de destination.

V.4.4 ICMP : Internet Control Message Protocol

- ICMP est souvent considéré comme faisant partie de la couche IP
- Il communique les messages d'erreurs
- Les message ICMP sont transmis à l'intérieur des datagrammes IP

Format variable selon la requête/réponse



- type=00 et code=00 : Réponse à une demande d'écho
- type=03 et code=00 : Réseau inaccessible
- type=03 et code=01 : Hôte inaccessible
- type=03 et code=02 : Protocole inaccessible
- type=03 et code=03 : Port inaccessible
- type=03 et code=04 : Fragmentation nécessaire mais interdite
- type=03 et code=05 : Echec de routage par la source
- type=03 et code=06 : Réseau de destination inconnu
- type=03 et code=07 : Hôte de destination inconnue
- type=03 et code=08 : Machine source isolée
- type=03 et code=09 : Réseau de destination interdit administrativement
- type=03 et code=10 : Hôte de destination interdite administrativement
- type=03 et code=11 : Réseau inaccessible pour ce type de service
- type=03 et code=12 : Hôte inaccessible pour ce type de service
- type=03 et code=13 : Communication interdite par un filtre
- type=03 et code=14 : Host Precedence Violation
- type=03 et code=15 : Precedence cutoff in efect
- type=04 et code=00 : Volume de donnée trop importante
- type=05 et code=00 : Redirection pour un hôte
- type=05 et code=01 : Redirection pour un hôte et pour un service donné
- type=05 et code=02 : Redirection pour un réseau
- type=05 et code=03 : Redirection pour un réseau et pour un service donné
- type=08 et code=00 : Demande d'écho
- type=09 et code=00 : Avertissement routeur
- type=10 et code=00 : Sollicitation routeur
- type=11 et code=00 : Durée de vie écoulée avant d'arrivée à destination
- type=11 et code=01 : Temps limite de réassemblage du fragment dépassé

Type	Code	Message	Signification du message
8	0	Demande d'ECHO	La commande PING utilise ce type de massage, pour tester le réseau.
0	0	Réponse d'ECHO	Réponse au message de type 8

V.4.5 Les protocoles de transport

4.5.1 TCP : Transmission Control Protocol

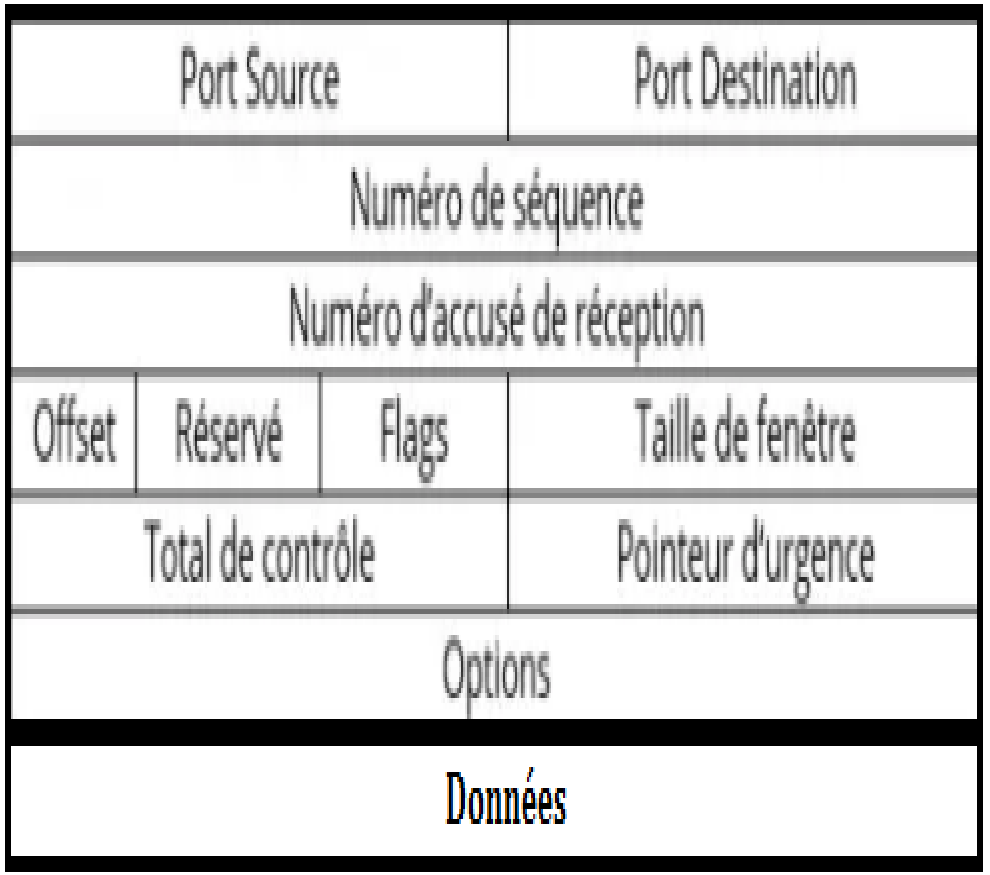
- Protocole de transport orienté octet
- Communications fiables et orientées connexion
    - Pour des applications nécessitant fréquemment des transferts de grandes quantités de données à la fois, ou nécessitant un accusé de réception
    - Offre un service avec connexion de type circuit virtuel

Caractéristiques

- Mode connecté
- Full Duplex
- Contrôle de flux
- Fiable

Transmission Control Protocol (TCP)

- Envoi des confirmations (ACK)
- Notion de port pour faire communiquer deux applications Contrôle des erreurs pour assurer une transmission fiable
- Prend l'information à envoyer et la segmente sur plusieurs paquets
- Numérote chaque paquet reçu ainsi l'entité distante peut reconstituer les données dans l'ordre et vérifier s'il y a eu des perte


Port Source
Port Destination
Numéro de séquence
Numéro d'accusé de réception
Offset
Réservé
Flags
Taille de fenêtre
Total de contrôle
Pointeur d'urgence
Options
Données

20 octets

- **Port source**
- **Port destination**
- **Numéro de séquence ou ordre:** Lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier mot du segment en cours. Lorsque SYN est à 1, le numéro d'ordre est égal au numéro d'ordre initial utilisé pour synchroniser les numéros de séquence (ISN).
- **Numéro d'accusé de réception**: Le numéro d'accusé de réception également appelé numéro d'acquittement correspond au numéro du prochain segment attendu, et non le numéro du dernier segment reçu.

- **Numéro de Déplacement** : il est rendu nécessaire par le champ de longueur variable option. Il est exprimé en nombre de mots de 32 bits.

- **Réservé (6 bits):** Champ inutilisé actuellement mais prévu pour l'avenir.

- **Fonctions**: est un vecteur de bits dont les composantes indiques quand leur valeur est 1 que le paquet à la fonction correspondante :
  - URG : indique un message urgent le champ pointeur urgent est valide.
  - ACK : indique que le champ ACK est valide
  - PSH les données contenues dans le paquet doivent être remise
  - RST : la connexion est détruite
  - SYN : ouverture

  FIN : fermeture

- **Crédits (taille de la fenêtre)** : donne le nombre maximum d'octets qu'on est prêt à émettre (taille de la fenêtre).

- **Somme de contrôle** : pour assurer une meilleur fiabilité; permet la détection des erreurs

- **Pointeur Urgent** : emplacement dans le flot du dernier octet des données urgentes

- **Options**: utiliser pour divers tâches (taille des tampons).

- **Bourrage**: On remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits.

Port	Nom	Signification
21	FTP	Transfert de fichiers
22	SSH	Connection à distance sécurisée
23	Telnet	Connection à distance
25	SMTP	Courrier électronique
80	HTTP	Protocole de transfert hypertexte

4.5.2 UDP : User Datagram Protocol

- Protocole de transport de type datagramme sans contrôle ni acquittement
- La responsabilité du bon acheminement est à la charge de l'application
- Permet des communications hors connexion sans garantir le bon acheminement des paquets
    - Pour des applications ne transférant que des petites quantités de données à la fois

- UDP fournit un service, sans connexion, de transmission de message entre des processus s'exécutant sur des machines interconnectées sous IP. La qualité de service fournie est celle d'IP :
  - Pas d'ordre
  - Pas de reprises en cas d'erreur
  - Si le message ne parvient pas on n'est pas averti

Port source	Port destination
Longueur	Somme de contrôle
Données	

8 octets