

# Bases TCP/IP

---

RALL 2007

Présenté par  
Roger YERBANGA  
Alain Patrick AINA

## Internet Protocoles & Applications

- Introduction
- Architecture TCP/IP
- Niveau interface réseau
  - Ethernet
  - Liaison Point à Point
- Niveau Internet IP
- Adressage IP
- Routage IP

## Internet Protocoles & Applications

- Niveau Transport
  - TCP
  - UDP
- Niveau Application

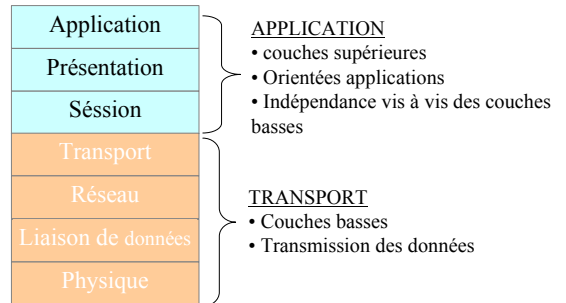
## Introduction

- Objectifs des Réseaux ?
  - Fonctionnels
    - Partage de ressources
    - Échange d'informations
  - Opérationnels
    - Meilleure fiabilité
    - Facilité d'évolution
    - Indépendance de constructeurs
- Types de Réseaux ?
  - LAN: Local Area Network
    - étendue limitée et débit élevé
  - WAN: Wide Area Network
    - Réseaux à grande échelle

## Introduction

- Diversité de technologie, topologie, système d'exploitation → Définition de standards
- ISO: International Standard Organisation
  - Définition des normes OSI (Open System interconnexion) = modèle à 7 couches (1984)
    - Couches basses ou de communication (1-4)
    - Couches hautes ou traitement de l'information (5-7)
  - Protocoles et services
    - Chaque couche N fournit un service à la couche N+1 et utilise celui de la couche N-1
    - L'accès au service : Point d'accès (SAP: Service Access Point)
    - Protocole de couche N : règles d'échange et format de données (Protocole Data Unit : PDU)

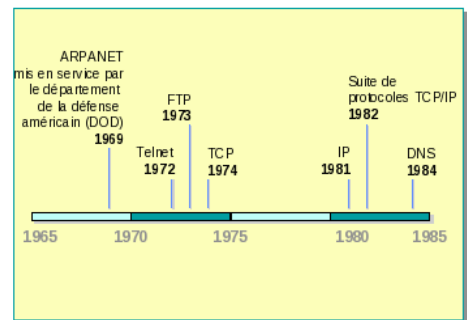
## Modèle OSI



## Présentation Générale TCP/IP

- TCP/IP = suite de protocoles "réseau"
  - Protocoles publics
  - Adressage logique
  - Protocole "routable"
  - Service de "nommage"
  - Contrôle des erreurs et flots de données
  - Support applicatif (ports)

## Évolution TCP/IP

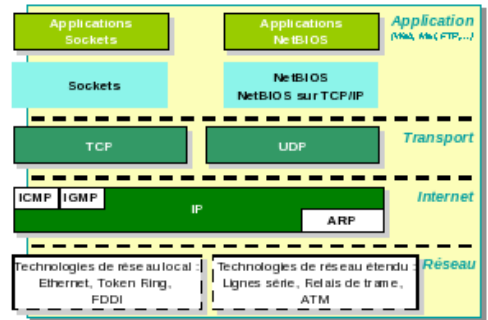


## Succès de l'Internet

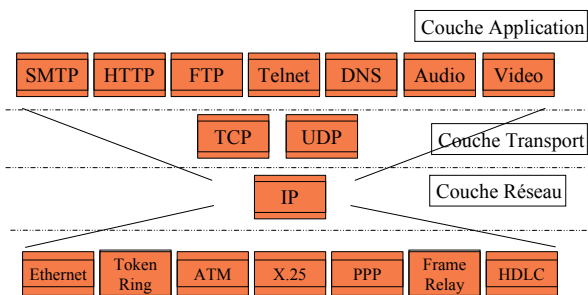
### • Succès de l'internet

- Architecture simplifiée
- Gratuité (protocole du domaine public)
- Diversité des utilitaires applicatifs
  - Transfert de fichiers : ftp, tftp, rcp
  - Exécution à distance : telnet, rsh, rexec
  - Impression à distance : lpr, lpd, lpq
  - Diagnostic du réseau : ping, ifconfig, route, traceroute, netstat, arp, dig, nslookup
  - Courrier électronique : smtp
- World Wide Web : http

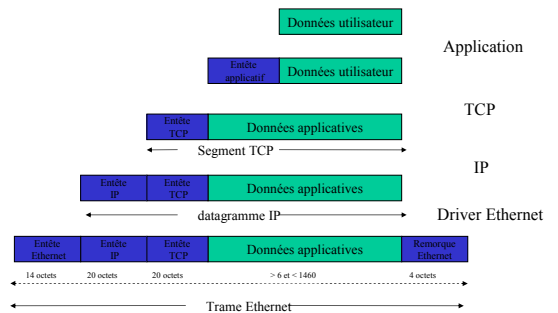
## Architecture TCP/IP



## Couches de protocoles TCP/IP



## Architecture TCP/IP

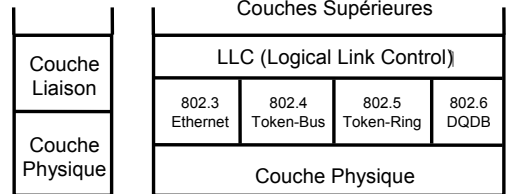


## Couche interface réseau

- Couche interface réseau = couches physique + liaison du modèle OSI
  - Mise des trames sur le support physique
  - Récupération des trames depuis le support physique
  - Contrôle de transmission (optionnel)
- Deux types de technologies
  - LAN et interconnexion de LANs
    - Ethernet, Token Ring, Token bus, FDDI
  - WAN
    - lignes point à point (analogique ou numérique)
    - Protocol PPP utilisé pour encapsuler IP

## Réseaux Locaux

Architecture R.L.  
Norme 802.1



Modèle OSI

## Couche interface réseau

- Sous-couche LLC (norme 802.2)
  - Indépendante de la méthode d'accès
  - Trois modes de fonctionnement
    - LLC 1
      - Pas de reprise sur erreurs, pas contrôle de flux
      - Mode non connecté
    - LLC 2
      - Reprise sur erreurs, contrôle de flux (taille fenêtre = 128)
      - Mode connecté
    - LLC 3
      - LLC 1 +
      - Reprise sur erreurs,
      - contrôle de flux (stop & wait)

## Couche interface réseau

- Sous-couche MAC (Medium Access)
  - Contrôle l'accès au médium
    - Aléatoire (compétition pour l'accès au médium)
      - Réseaux Ethernet
    - Déterministe par l'utilisation de jeton
      - Anneau logique et physique
  - Plusieurs méthodes normalisées par IEEE
    - Accès aléatoire au bus (802.3) : Ethernet
    - Accès en utilisant le jeton sur bus (802.4) : Token Ring
    - Accès en utilisant le jeton sur anneau (802.5) : Token bus
    - WiFi (CSMA/CA) : 802.11a, 802.11b, 802.11g, 802.11g

## Couche interface réseau

### Réseaux Ethernet

- Technologie LAN la plus utilisée
  - 80% des LANs au niveau mondial, statistiques de 1996
  - Selon le Metro Ethernet Forum (MEF), organisme qui promeut l'utilisation du protocole, 97 % des connexions de réseau local se terminent par une prise Ethernet. (2003)
- Facteurs de popularité de Ethernet :
  - Capacité d'évolution, Fiabilité de la technologie
  - Coût d'acquisition faible
- 1ère norme Ethernet 10 Mb/s fut inventé en 1980
- Réinventé en Ethernet 100 Mb/s vers 1990
- Réinventé en Ethernet 1000 Mb/s (Gigabit) vers 1999
- Aujourd'hui, on a du 10 Gb/s

## Couche interface réseau

### Réseau Ethernet

- Chaque station a une adresse MAC de 48 bits
- Les adresses sont assignées par les constructeurs.
- Autorité globale d'assignation d'adresses : IEEE
  - IEEE vend un block d'adresse ( $2^{24}$ ) au prix de 1000 \$
  - 3 premiers octets sont fixés par IEEE pour chaque constructeur

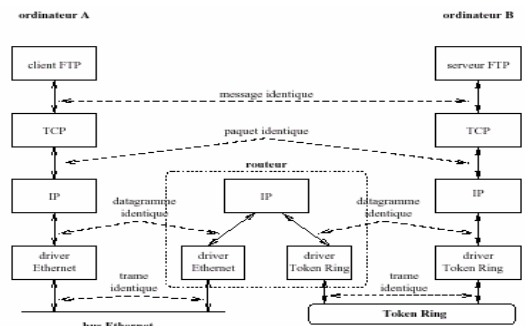
## Couche interface réseau

### Interconnexion de réseaux

- Composants d'interconnexion
  - Répéteurs à deux ou plusieurs ports (hubs)
    - Opère au Niveau Couche Physique
    - Amplification et régénération des signaux sur tous les ports
    - Possibilité de combiner différents médiums ayant la même vitesse
  - Ponts à deux ou plusieurs ports (switches)
    - Opère au Niveau Couche Liaison
    - Filtrage des paquets (en se basant sur adresse source)
    - Possibilité de combiner différents médiums à des vitesses différentes
  - Routeurs : connecter réseaux locaux différents
    - Bloque les broadcasts

## Couche interface réseau

### Interconnexion de réseaux



## Couche interface réseau Liaison série(RFC1055)

- Liaison point à point
- Pas besoin d'adresse au niveau physique
- Protocole qui adapte les paquets IP à la ligne série
  - SLIP : Serial Line Interface Protocole
    - Délimite le début et fin des paquets IP
  - PPP : Point to Point Protocol
    - Extension de SLIP (RFC1661)
    - Authentification
      - PAP : Authentication Protocol
      - CHAP : Challenge Handshake Authentication Protocol (authentification sécurisée)

## Couche internet Protocole IP (RFC791)

- Fonctionnalité principale : **roulage**
  - Acheminement des données de bout en bout
  - Trouver le « meilleur » chemin :
- Autres fonctionnalités
  - Contrôle de flux et de congestion
  - Gestion des erreurs
  - Segmentation et réassemblage
- Unité d'information au niveau réseau (NPDU) :  
Paquet, taille variable (entête, information)

## Les différents types de communication

- Communication unicast : Une machine (source) envoie un message à une machine destination.
- Communication broadcast (Diffusion générale) : Une machine (source) envoie un message à toutes les machines du réseau.
- Communication multicast (Diffusion restreinte) : Une machine envoie un message aux machines d'un groupe (Toutes les machines membres du groupe reçoivent le message, mais pas les non-membres).
- Communication anycast : Une machine (source) envoie un message à un groupe de machines destination, mais le message sera délivré à la machine la plus proche **topologiquement**.

## Couche internet Adresse IP

- Adresse réseau : **identifie** de manière **unique** un nœud sur le réseau (interface réseau).
- Adresse IP : 4 octets = 32 bits ( $2^{32}$  nœuds)
  - Notation pointée : W.X.Y.Z
- Attribution d'adresses IP : AfriNIC, ARIN, RIPE-NCC, APNIC, LACNIC. ← IANA
- Classes d'adresses : ID réseau + ID hôte
  - Classe A : réseaux de grande taille
  - Classe B : réseaux de taille moyenne
  - Classe C : réseaux de petite taille

## Couche internet Adresse IP

L'adressage d'une machine/d'un réseau  
=  
@ IP + masque sous-réseau


- 1 réseau IP = 1 plage IP constituée par :
  - ✓ d'une adresse définissant le réseau (première adresse de la plage).
  - ✓ d'une adresse définissant le broadcast réseau (la dernière adresse de la plage).
  - ✓ d'adresses des hôtes uniques (toutes les autres adresses).
- Il existe des exceptions : des plages IP réservées et d'autres à ne pas router.

## Couche internet Les classes d'adresses

- Appartenance d'une adresse IP à une classe
  - 0bbb : classe A
  - 10bb : classe B
  - 110b : classe C
  - 1110 : classe D → adresses de multicasting
  - 1111 : classe E → plage réservée
- Adresses IP particulières (RFC3330)
  - 0.0.0.0 : quand une machine n'a pas d'adresse IP
  - 255.255.255.255 : diffusion sur tout le réseau local
  - 127.?.?.? : Boucle locale
  - 10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.31.255.255 et 192.168.0.0 à 192.168.255.255 → privé

## Couche internet Masque de réseau

- Mask de sous-réseau = adresse sur 32 bits
- Adresse IP **AND** Mask = ID réseau



■ Distingue l'identificateur de réseau de l'identificateur d'hôte

■ Utilisé pour spécifier si l'hôte de destination est local ou distant

## Couche internet Masque de réseau

- Mask par défaut

Classe d'adresses	Bits utilisés pour le masque de sous-réseau				Notation décimale
Classe A	11111111	00000000	00000000	00000000	255.0.0.0
Classe B	11111111	11111111	00000000	00000000	255.255.0.0
Classe C	11111111	11111111	11111111	00000000	255.255.255.0

Exemple de classe B

Adresse IP	131.107.	16.200
Masque de sous-réseau	255.255.	0.0
Identificateur de réseau	131.107.	y.z
Identificateur d'hôte	w.x.	16.200

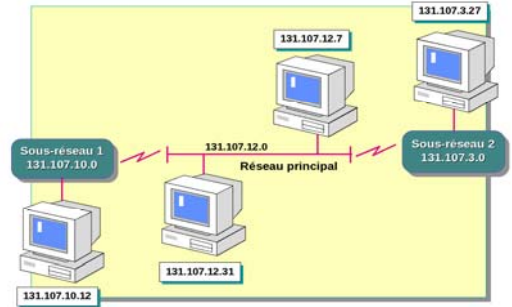
## Couche internet

### Notion de sous-réseaux

- Sous-réseau : segment physique d'un environnement TCP/IP utilisant une partie des adresses IP du réseau
- Pourquoi segmenter un réseau ?
  - définir structures organisationnelles
  - outrepasser les limitations technologiques
  - lier différentes technologies (Ethernet, Token Ring , ...)
  - améliorer les performances du réseau (limiter broadcast)
- Composante d'interconnexion : Routeur

## Couche internet

### Notion de sous-réseaux (RFC950)



## Couche internet

### Notion de sous-réseaux (RFC950)

- Mise en œuvre des sous-réseaux ?
  - Déterminez le nombre de segments physiques du réseau.
  - Déterminez le nombre d'adresses d'hôte requises pour chaque segment physique.
- En fonction des besoins, définissez :
  - Un masque de sous-réseau pour l'ensemble du réseau.
  - Un identificateur de sous-réseau unique pour chaque segment physique.
  - Une plage d'identificateurs d'hôte pour chaque sous-réseau.

## Couche internet

### Principes de sous-réseaux

- Calcul du mask des sous-réseaux ?
  - Convertir le nombre de segments ns en binaire.
  - Compter le nombre de bits représentatif de ns (nb)
  - Placer la valeur 1 nb fois sur les bits de poids fort du 1er octet null du mask par défaut
  - Adresses réservées : nb bits à 1  $\rightarrow 2^{nb}-2$  sous-réseaux
- Calcul du nombre de hôtes par sous-réseau
  - Compter le nombre de bits = 0 du mask du sous-réseau (nbz)
  - Nombre de hôtes / sous-réseau =  $2^{nbz}-2$



## Couche internet

### Principes de sous-réseaux

- Mon adresse IP: 192.168.25.132  
Traduit en binaire:  
11000000.10101000.00011001.10000100
- Le masque de mon réseau: 255.255.255.128  
Traduit en binaire:  
11111111.11111111.11111111.10000000
- @ réseau:  
11000000.10101000.00011001.10000000  
Soit: 192.168.25.128
- **Conclusion: on peut supposer que les machines de mon réseau local ont pour adresse: 128 à 254...**

## Couche internet

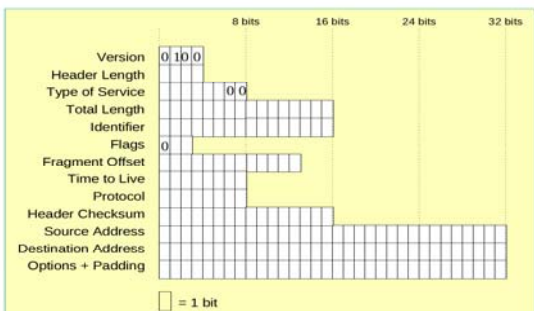
### Notation préfixée (CIDR)

Le masque sous-réseau permet de créer des sous-réseaux ou sur-réseaux qui ne respectent plus le découpage en classes A, B, C.

- C'est le masque sous-réseau qui définit la limite des bits d'adressage du réseau, des bits d'adressage de la machine :  
192.168.10.5/255.255.255.0 ou 192.168.10.5/24 ← 24 bits Rx sur 32  
→ 192.168.10.0 → 192.168.10.255
- 192.168.10.5/255.255.255.128 ou 192.168.10.5/25 ← 25 bits Rx sur 32  
→ 192.168.10.0 → 192.168.10.127
- 192.168.10.5/255.255.252.0 ou 192.168.10.5/22 ← 22 bits Rx sur 32  
→ 192.168.8.0 → 192.168.11.0

## Couche internet

### Paquets IP (RFC791)



## Couche internet

### Paquets IP (RFC791)

- Version : protocole IP sur 4 bits
- Header length : Longueur de l'entête en mots de 32 bits
- Type of service : qualité de service sur 8 bits (6 bits) pour
  - priorité du paquets sur 3 bits (0 défaut)
  - qualité de service sur 3 bits (choix de routes)
    - 1er bit : délai, 2ème bit : débit, 3ème bit : fiabilité
- Total length : longueur totale du paquet (header+data) sur 16 bits
- Flags : champ sur 3 bits:
  - 1er =0, 2ème bit : Don't Fragment(=1), 3ème bit: More Fragments(=1)
- Fragment offset : place du fragment dans le paquet origine (13 bits)
- Time To Live (TTL) : durée de vie du paquet sur 8 bits
- Protocol : identification du protocole supérieur (TCP=6, UDP=17, ICMP=1, ...)
- Header checksum : CRC pour l'entête sur 16 bits
- Options : champ de longueur variable

## Couche internet Protocole IP

- Fragmentation/Ré-assemblage
  - Adapter les paquets IP à la couche interface réseau
  - Chaque technologie → MTU: Maximum Transfert Unit
    - Ethernet, MTU = 1500 octets
    - FDDI, MTU = 4096 octets
    - ...
  - Un fragment peut être fragmenté
  - Fragmentation au niveau des routeurs
  - Ré-assemblage au niveau de la machine destinataire
  - Paquet avec Don't Fragment=1 → rejet du paquet si fragmentation nécessaire.

## Couche internet Protocole IP

- Fragmentation/Ré-assemblage
  - Entraîne une dégradation de performances →
  - Choisir le plus petit MTU des différentes technologies
  - Découverte de MTU (pMTU)
- Congestion du réseau internet
  - Contrôle de flux (ICMP)
  - TTL : Time To Live,
    - initialisé par l'émetteur du paquet (128)
    - décrémenté par routeurs intermédiaires (TTL-1)
    - Si TTL = 0 → paquet rejeté par le routeur

## Couche internet Protocole IP

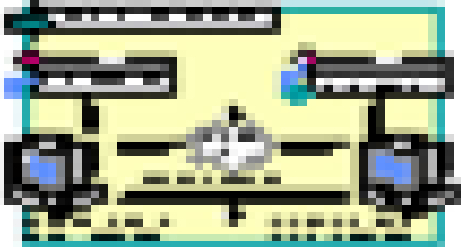
- Options : opérations de mesure et de contrôle
  - option = type (1 octet) , longueur totale , paramètres
- type :
  - 1er bit : option à recopier si fragmentation
  - 2 et 3ème bit : classe de l'option (00: contrôle, 10: mesure)
  - 5 bits restants : identifie une option dans sa classe
- Exemples
  - 0 00 00111 : Record Route
  - 1 00 01001 : Strict Source Route

## Couche Internet Protocole ARP (RFC826)

- Contexte : réseaux à diffusion (Ethernet)
- Résolution d'adresse IP en adresse MAC
- Diffusion sur le LAN pour récupérer l'adresse MAC du destinataire ou de la passerelle.
- Mappage (IP, MAC) stocké dans le cache pour utilisation ultérieure.
- Consultation du cache avant diffusion sur LAN

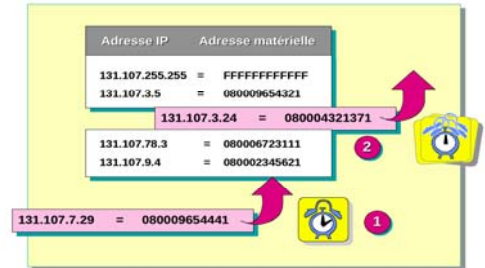
## Couche Internet Protocole ARP (RFC826)

- Résolution d'adresse IP locale



## Couche Internet Protocole ARP (RFC826)

- Le cache ARP

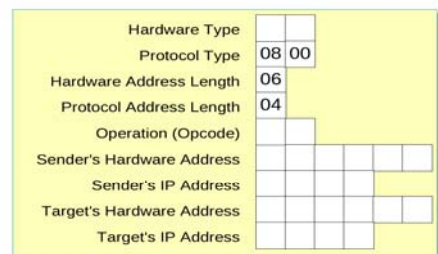


## Couche Internet Protocole ARP (RFC826)

- Commande ARP : gestion du cache ARP
  - a : affiche les entrées actuelles du cache
  - d *ip-addr* : supprime une entrée du cache
  - s *ip-addr mac-addr* : ajoute une entre statique

## Protocole ARP (RFC826)

- Structure d'un paquet ARP

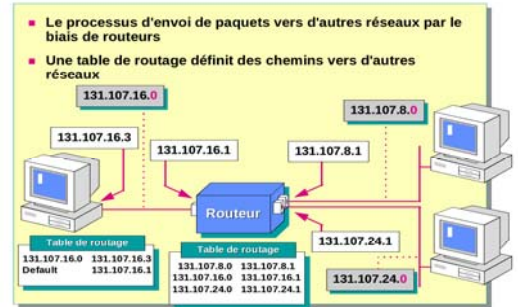


- Hardware type : type de matériel de la couche interface réseau
- Protocol type : IP, IPX, etc.
- Opération : requête / réponse

## Protocole RARP (RFC903)

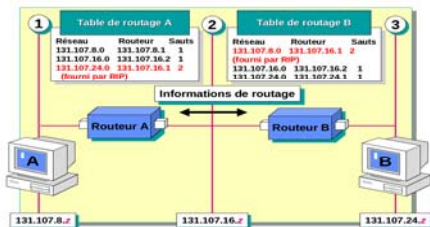
- Utilisé par machines sans disque (diskless)
- Format de trame similaire à ARP
  - opération = 3 pour requête RARP
  - opération = 4 pour réponse RARP
- Serveur RARP nécessaire sur le LAN (serveur rarpd sur station Unix + /etc/ethers)
- Lors de l'initialisation d'une machine diskless
- envoi d'une requête rarp
- réception par les serveurs rarpd
- consultation du /etc/ethers
- envoi de la réponse à la machine

## Couche internet Routage IP



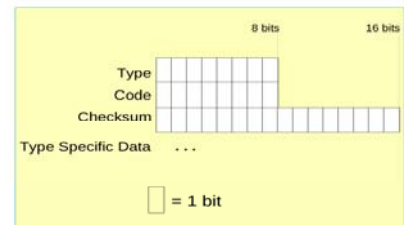
## Couche internet Routage IP

- Routage statique : Routes entrées manuellement l'admin
- Routage dynamique : Les protocoles échangent les informations de routage :
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First)



## Couche Internet Protocole ICMP (RFC792)

- Internet Control Message Protocol :
  - signale les erreurs
  - contrôle de flux pour le compte de IP

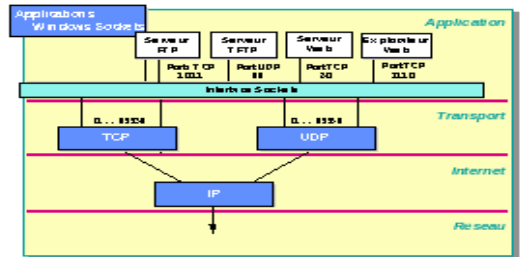


## Couche Internet Protocole ICMP (RFC792)

- Type = 5 : Re-direction
  - code = 0 : pour un sous-réseau
- Type = 11 : TTL a atteint 0
  - code = 0 : pendant le transit
  - code = 1 : pendant ré-assemblage
- Type = 12 : problème de paramétrage
  - code = 0 : pointeur indique l'erreur
  - code = 1 : manque une option
  - code = 2 : longueur incorrecte
  - code = 3 : fragmentation nécessaire et DF=1
  - ...
- Type = 17 : demande de netmask
  - code = 0
- Type = 18 : réponse netmask
  - code = 0

## Couche Transport Ports et sockets

- IP identifie une machine sur le réseau
- Numéro de port identifie une application d'une machine du réseau
- Socket : connexion réseau



## Couche Transport Les ports TCP/IP

- ❖ L'utilité des ports
- ❖ Sont des points d'ancrage pour les services (Telnet, FTP, Web, etc)
- ❖ Associer un paquet à un service :
  - Le serveur Telnet utilise le port 23
  - Le serveur FTP utilise les ports 20 et 21
  - Le serveur de courriels (SMTP) utilise le port 25
  - Le serveur Web utilise le port 80
  - POP3 écoute sur le port 110
- ❖ Il existe des milliers de ports (65536 possibilités) 1

## Couche Transport Port 0 à 1023: Well Known Ports

- ❖ Sont uniquement utilisables par les processus système
- ❖ Certaines assignations par défaut:

#	Service	Transp.	Signification
20	FTP (Default Data)	TCP	File Transfert Protocol
21	FTP (Control)	TCP	
23	Telnet	TCP	
25	SMTP	TCP	Simple Mail Transfert Protocol
53	DNS	TCP/UDP	Domain Name System
67	DHCP (Serveur)	UDP	Dynamic Host Configuration Prot
68	DHCP (Client)	UDP	
69	TFTP	UDP	Trivial File Transfert
80	HTTP	TCP	HyperText Transport Protocol
110	POP3	TCP	Post Office Protocol
119	NNTP	TCP	Network News Transfer Protocol
143	IMAP	TCP	

## Couche Transport Les sockets

- Canaux de communication
- Connexion avec l'adresse IP et le port
- Approche client / serveur
- Serveur: en écoute du client (port serveur) ]

## Couche Transport Ports et sockets

- RFC1700 : liste des n° ports pour applications connues
- N° ports < 1024 réservés (etc/services)
- N° ports >= 1024 applications utilisateurs
- Association entre deux applications
  - adresse IP source
  - adresse IP destination
  - n°port source
  - n°port destination
  - protocole de transport
    - UDP (User Datagram Protocol)  
Données de taille courte
    - TCP (Transmission Control Protocol)  
Données de grande taille

## Couche Transport Protocol UDP (RFC768)

- **Mode non-connecté**
  - Aucune session n'est établie
- **Ne garantit pas la remise**
  - Pas de numéros de séquence
  - Pas d'accusé de réception
- **L'application est responsable de la fiabilité**
- **Utilise les numéros de ports pour une communication**
  - Coté serveur : numéros de port par application (normalisé)
  - Coté client : numéros dynamiquement alloués

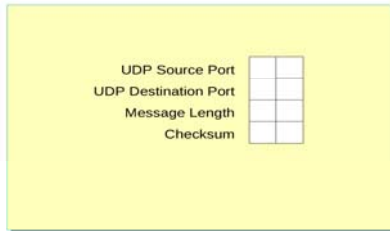
## Couche Transport Protocol UDP (RFC768)

- Certains ports sont réservés (*well-known port assignments*) :

<u>No port</u>	<u>Mot-clé</u>	<u>Description</u>
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
37	TIME	Time
42	NAMESEVER	Host Name Server
53	DOMAIN	Domain Name Server
67	BOOTPS	Boot protocol server
68	BOOTPC	Boot protocol client
69	TFTP	Trivial File transfert protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management

## Couche Transport Protocol UDP (RFC768)

- Structure d'un segment UDP



## Couche Transport Protocole TCP (RFC793)

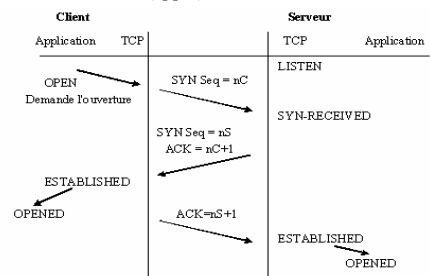
- **Mode connecté**
  - Une session est ouverte avant l'échange des données
- **Remise fiable**
  - Numéros de séquence
  - Accusés de réception (ACK)
- **Communications par flux d'octets**
  - Découpage en segments
  - Bidirectionnelles
  - Niveau de priorité
- **Numéros de port comme extrémités de communication**

## Couche Transport Protocole TCP (RFC793)

- Connexion TCP = circuit virtuel établi avant transfert des données = appel + négociation + transferts
- Connexion = paire d'extrémités de connexion
- Extrémité de connexion = couple (adresse IP, port)
- Exemple de connexion : ((124.32.12.1, 1034), (19.24.67.2, 21))
- Extrémité de connexion peut être partagée par plusieurs connexions: multiplexage (côté serveur)
- Appel en trois phases : (SYN), (SYN, ACK), (ACK)
  - envoi d'un SYN avec un numéro initial de segment (ISN)
  - réception d'un SYN avec ISN du récepteur
- Négociation des paramètres :
  - taille de la fenêtre en octets
  - option MSS (Maximum Size Segment)

## Couche Transport Protocole TCP (RFC793)

- Phase de connexion (appel)



## Couche Transport Protocole TCP (RFC793)

- Transfert de données :
  - émission suite de segments (fenêtre)
  - entrelacés par la réception d'acquiescement
- TCP n'utilise que des Acks positifs
- Retransmission (erreur ou perte) basée sur des temporisateurs
- Premières implémentations de TCP,  $RTO = 2 \cdot T_{ar}$

### algorithme de retransmission adaptative

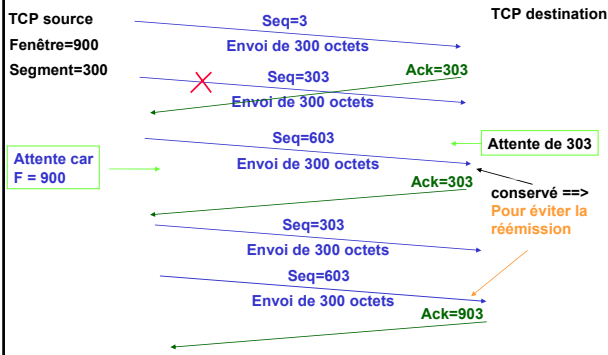
- enregistre la date d'émission d'un segment,
- enregistre la date de réception de l'acquiescement correspondant,
- calcule l'échantillon de temps de boucle A/R écoulé,
- détermine le temps de boucle moyen RTT (Round Trip Time) :  

$$RTT = (a \cdot anc\_RTT) + ((1-a) \cdot NOU\_RTT)$$
 avec  $0 \leq a < 1$

## Couche Transport Protocole TCP (RFC793)

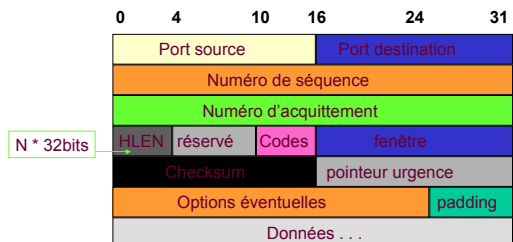
- Cas de retransmission d'un segment, l'émetteur ne peut savoir si l'acquiescement s'adresse au segment initial ou retransmis => calcul erroné du RTT.
- L'algorithme de Karn combine retransmissions avec l'augmentation des temporisations associées (*timer backoff*):
  - une valeur initiale de temporisation est calculée
  - si une retransmission est effectuée, la temporisation est doublée
- Contrôle de flux
  - champ fenêtre = 0, l'émetteur ne peut plus envoyer (état PERSIST)
  - test périodiquement l'état du récepteur (5s, 10s, 20s, ..., 1mn)
  - envoi d'un segment de 1 octet

## Couche Transport Protocole TCP (RFC793)



## Couche Transport Protocole TCP (RFC793)

- Structure d'un segment TCP





## Couche Transport

### Protocole TCP (RFC793)

- Champ **Codes** sur 6 bits : nature du segment TCP
  - URG : segment urgent TCP
  - ACK : Acquiescement
  - PSH : données reçues immédiatement délivrées
  - RST : (reset) fermeture de connexion
  - SYN : ouverture de connexion
  - FIN : Fin connexion
- Champ **option** : taille variable
  - Taille maximale des segments TCP (MSS)
  - Horsdatage : calcul du temps aller-retour