

Livres disponibles à la bibliothèque (RDC)

- Réseaux, 3^{ème} édition, A.TANENBAUM, 1997.
- TCP/IP : Architecture, protocoles et applications, 3^{ème} édition, D.COMER, 1998
- TCP/IP : Administration de réseaux, 2^{ème} édition, C.Hung, 1998.
- La communication sous UNIX, 2^{ème} édition, J.M.RIFFLET, 1995.

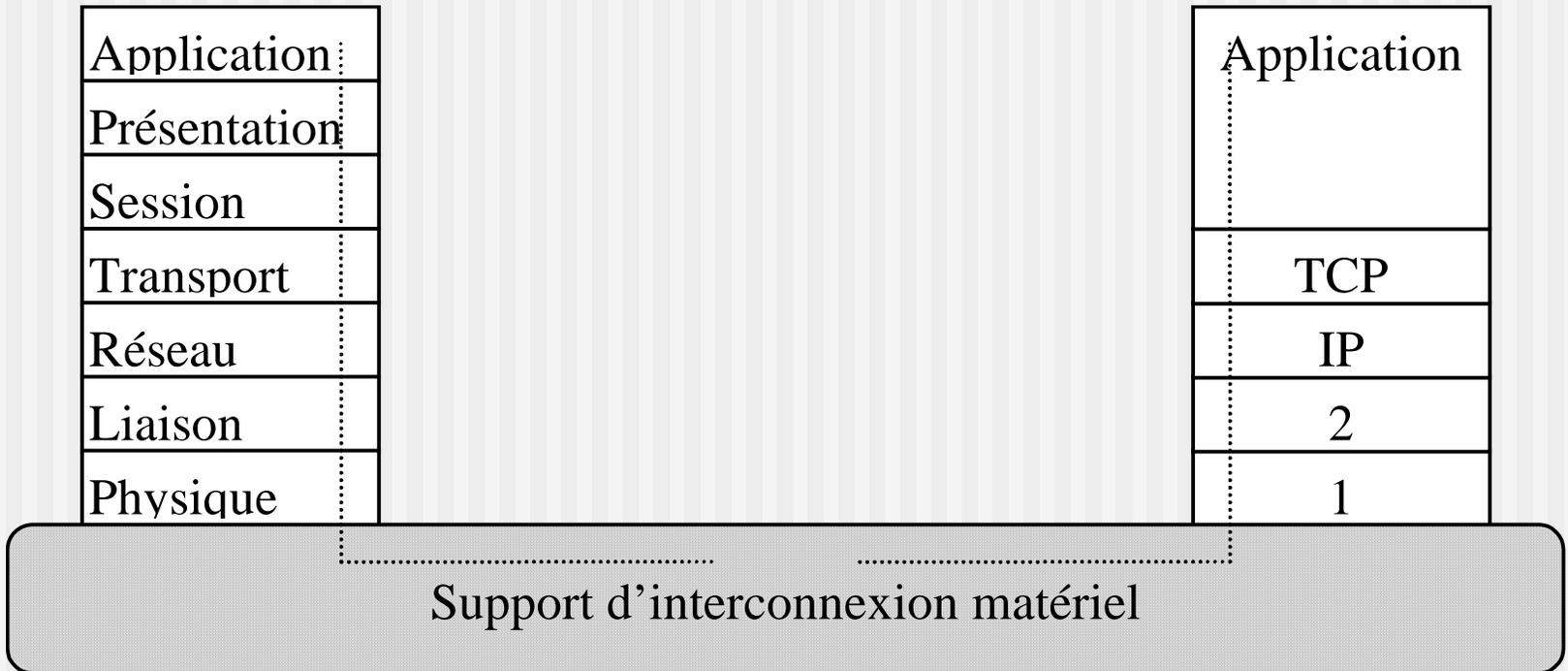
Architecture TCP/IP

Transmission
Control Protocol
/
Interconnection
Protocol

Protocoles TCP/IP

- Historique
 - 1972: spécifications de TCP/IP.
 - 1980: TCP/IP fait partie d'UNIX BSD 4.1.
- Internet/Intranet
- Couches 3 et 4 du modèle OSI
 - TCP : couche Transport
 - IP : couche Réseau

Modèles en couche



Les protocoles TCP et IP

■ Protocole IP

- protocole réseau
- remise non fiable
- mode non connecté

■ protocole TCP

- protocole de transfert fiable en mode connecté
- utile car IP est un protocole de remise non fiable
- du style de la couche transport ISO classe 4

IP : Interconnection Protocol

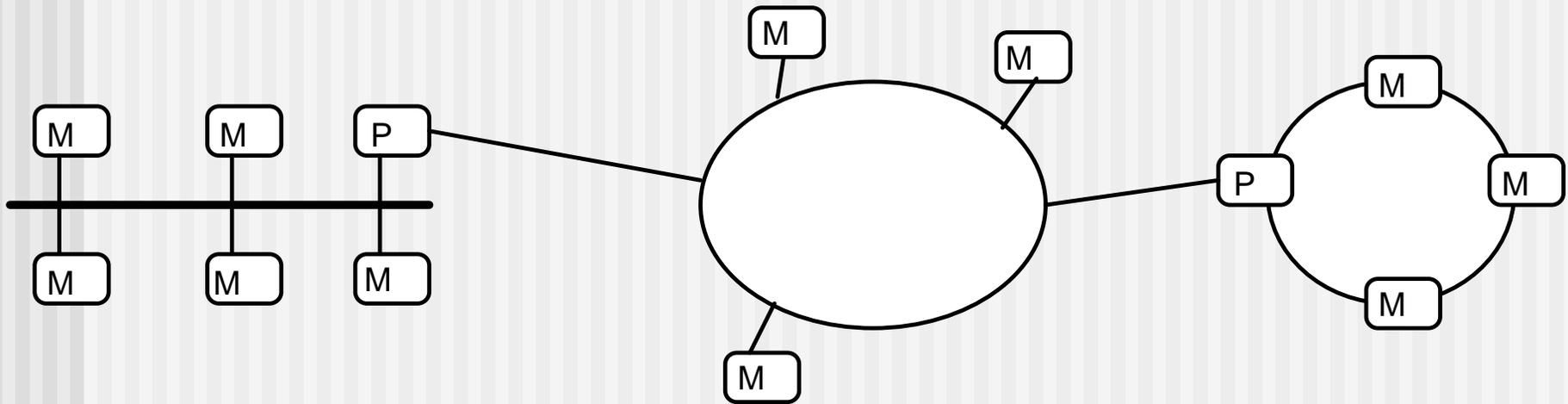
Adressage IP

- Adressage sur 4 octets (147.210.94.1)
- Classes de réseau
 - A: 0.0.0.0 → 127.255.255.255 (grand)
 - [0 Id. Réseau (7bits) Id. Machine (24bits)]
 - B: 128.0.0.0 → 191.255.255.255 (moyen)
 - [1 0 Id. Réseau (14bits) Id. Machine (16bits)]
 - C: 192.0.0.0 → 223.255.255.255 (petit)
 - [1 1 0 Id. Réseau (21bits) Id. Machine (8bits)]
- Adresses particulières
 - 224.0.0.0→239.255.255.255 (diffusion)
 - 240.0.0.0→255.255.255.255 (divers)

Adressage IP (suite)

- Dans chaque classe, une poignée d'adresses sont **privées** :
 - 10.0.0.1 à 10.255.255.254
 - 172.16.0.1 à 172.31.255.254
 - 192.168.0.1 à 192.168.255.254

Schéma d'une interconnexion



Réseau de type ETHERNET

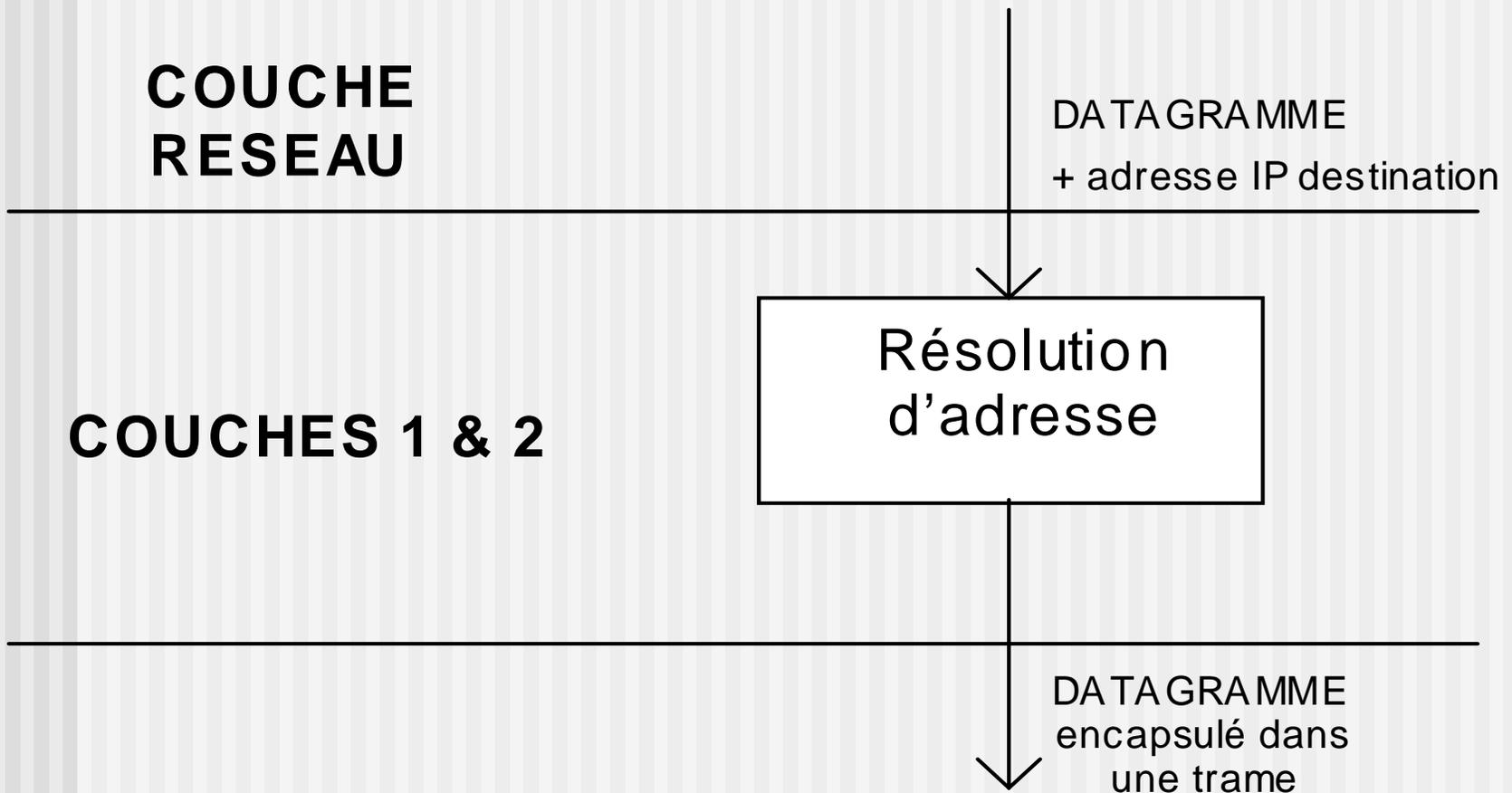
Réseau de type X25

Réseau de type
Anneau à jeton

Résolution d'adresse

- Chaque machine a :
 - adresse physique dans son réseau
 - adresse IP au niveau interconnexion
- correspondance entre les 2 adresses
 - directe
 - protocole ARP (Address Resolution Protocol)
 - table de correspondance

Résolution d'adresse



Protocole IP

Datagramme IP

0	4	8	16	24	31
VERS.	<i>L</i>GENT	TYPE SERVICE	<i>L</i>GR TOTALE		
IDENTIFICATION			DRAP	DEPL-FRAG	
DUREE DE VIE	<i>P</i>ROTOCOLE		TOTAL DE CONTROLE EN-TETE		
<i>A</i>DRESSE IP SOURCE					
<i>A</i>DRESSE IP DESTINATION					
OPTIONS IP EVENTUELLES				BOURRAGE	
DONNEES					
* * *					

Datagramme IP

- VERS
 - numéro de version du protocole utilisé (4)
- LGENT
 - longueur de l'entête du datagramme
- TYPE SERVICE
 - définit comment le datagramme doit être acheminé
 - priorité (0 à 7)
 - priorité au délai
 - priorité au débit
 - priorité à la fiabilité
- LGR
 - longueur total

Datagramme IP

- IDENTIFICATION, DRAP, DEPL-FRAG
 - contrôle la fragmentation
 - IDENTIFICATION permet de connaître le datagramme auquel appartient le fragment.
 - DEPL-FRAG donne la position du fragment courant dans le datagramme initial en multiples de 8 octets.
 - DRAP indique si le fragment est le dernier du datagramme.
- DUREE DE VIE
 - décrémenté à chaque traversée, détruit si égal à 0.
- PROTOCOLE
 - protocole de la couche supérieure qui a créé le datagramme,

Numéros de protocole

■ \$ more /etc/protocols

The form for each entry is:

<official protocol name><protocol number><aliases>

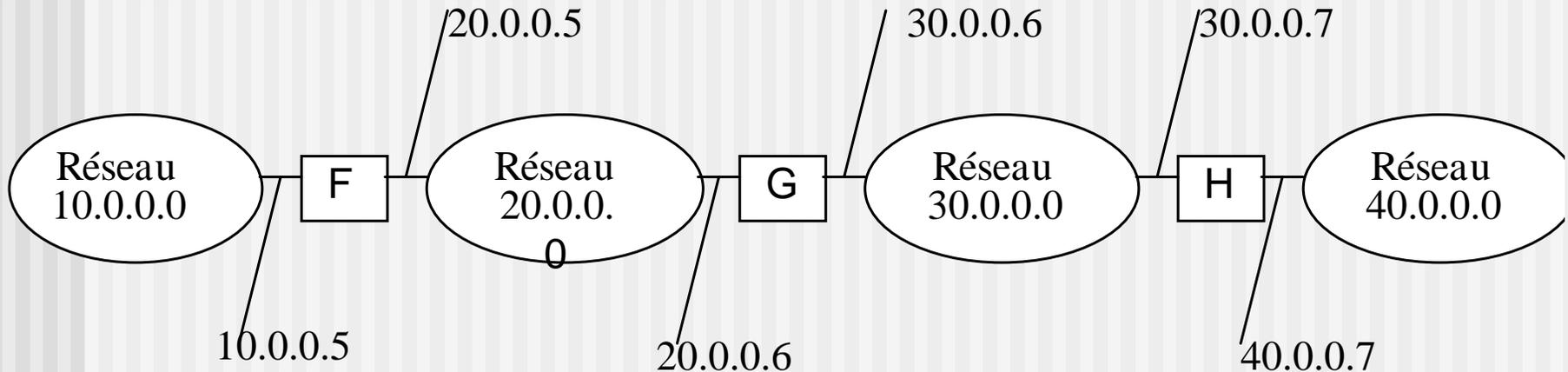
#

#

Internet (IP) protocols

icmp	1	ICMP	# internet control message protocol
tcp	6	TCP	# transmission control protocol
udp	17	UDP	# user datagram protocol

Routage des datagrammes IP



pour atteindre les machines situées sur le réseau	router vers cette adresse
20.0.0.0	Remise directe
30.0.0.0	Remise directe
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

TABLE DE ROUTAGE DE G

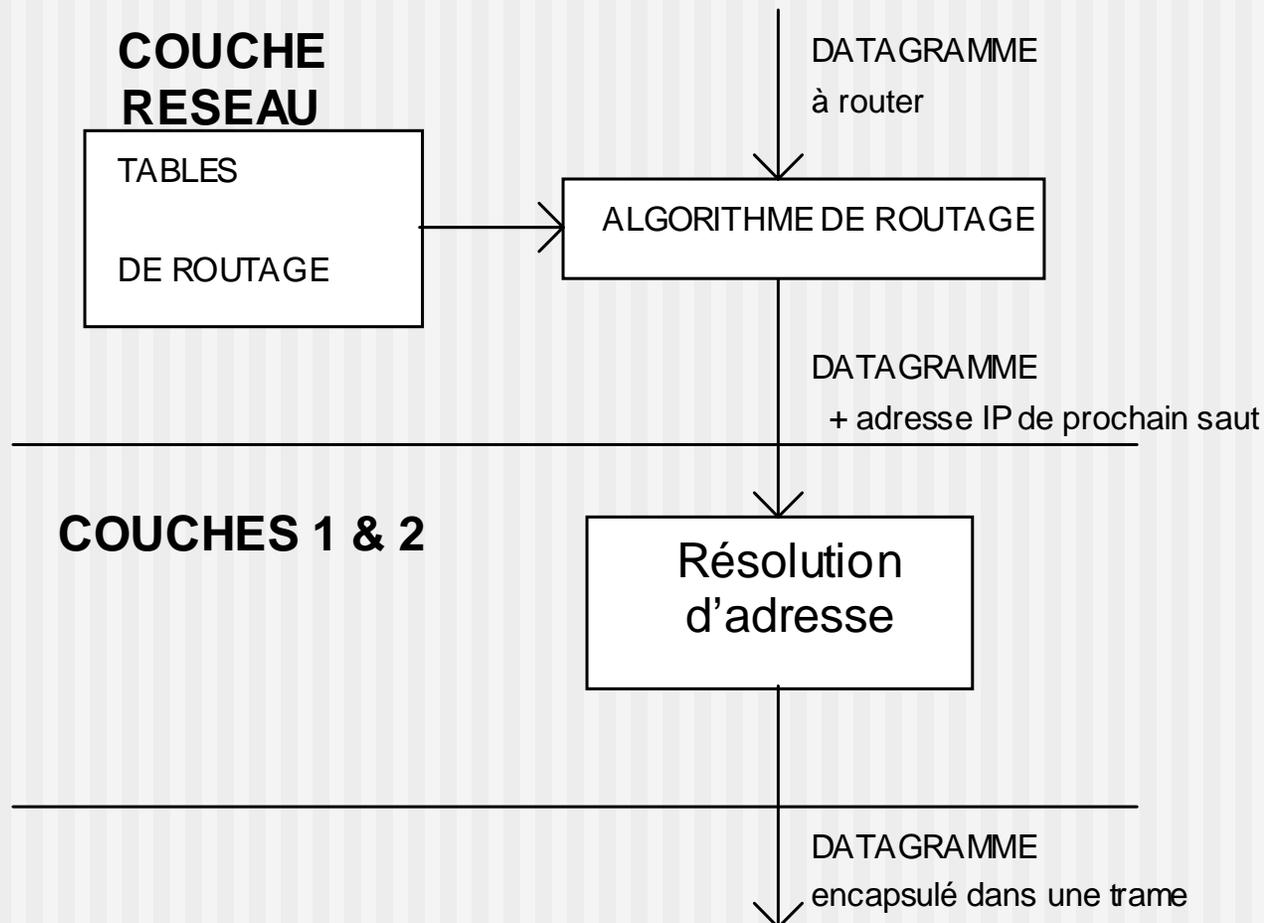
Routage des datagrammes IP

- entre 2 machines du même réseau
 - remise directe
- entre 2 machines de réseaux différents
 - utilisation de passerelles
 - chaque passerelle a deux connexions (donc 2 adresse IP)
 - chaque passerelle constitue une table de routage
 - éventuellement une route par défaut

Routage des datagrammes IP

- l'adresse IP de la prochaine passerelle
 - n'est pas conservée dans le datagramme
 - est traduite en adresse physique

Routage des datagrammes IP



ICMP (Internet Control Message Protocol)

- RFC 792
- Niveau 3
 - Partie intégrante du logiciel IP
 - mais 2 niveaux d'encapsulation
 - Message ICMP encapsulé dans datagramme
 - champ protocol: 1
- Format
 - Type/code/information

Protocole ICMP

- Même niveau que IP
- Pour avertir l'émetteur d'un datagramme d'éventuels problèmes
 - demande d'écho (message d'écho)
 - détection de destination inaccessible
 - demande de limitation de débit (une passerelle est proche de la congestion)
 - demande de modification de route (une passerelle sait qu'il existe une meilleure route)

IP: Echange d'informations de supervision

- Situation d'erreurs niveau 3
 - Congestion
 - Destinataires non accessibles
 - ...
- Echange de messages d'erreur ou de supervision
 - Compte-rendu (et non correction !)
 - Restreint à l'expéditeur (pas possible de faire autrement...)
 - Coopération des administrateurs
- Mécanisme de demande/réponse en écho

Exemples de types/codes des messages ICMP

- 0: réponse à une demande d'écho
- 3: destination inaccessible,
 - Code 0: réseau inaccessible
- 4: demande de limitation de débit (une passerelle est proche de la congestion),
- 5: demande de modification de route (une passerelle sait qu'il existe une meilleure route),
- 8: demande d'écho (utile pour la mise au point et exploité par la commande ping),
- 11: durée de vie expirée.

ICMP: Messages d'écho

0 8 16 24 31

Type (0 ou 8)	Code (0)	TOTAL DE CONTROLE
Identificateur		Numéro de séquence
<i>Données optionnelles</i>		
...		

- Demande d'écho: envoyée par un routeur ou ordinateur
- Réponse: envoyée par toute machine destinataire d'une demande d'écho
- La réponse contient une copie des données envoyées dans la demande
- Permet un test d'accessibilité et d'état

Commande ping

- permet de tester l'accessibilité d'une machine
 - envoi d'un datagramme ICMP ECHO_REQUEST à la machine à tester
 - la machine à tester doit répondre par un ICMP ECHO_RESPONSE

Exemple d'exécution de ping

```
tuba> /bin/ping helicon
PING helicon.info.prive (172.16.94.22): 56 data bytes
64 bytes from 172.16.94.22: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 172.16.94.22: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 172.16.94.22: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 172.16.94.22: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 172.16.94.22: icmp_seq=4 ttl=255 time=0.1 ms
64 bytes from 172.16.94.22: icmp_seq=5 ttl=255 time=0.1 ms

--- helicon.info.prive ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.4 ms
```

TCP: Transmission Control Protocol

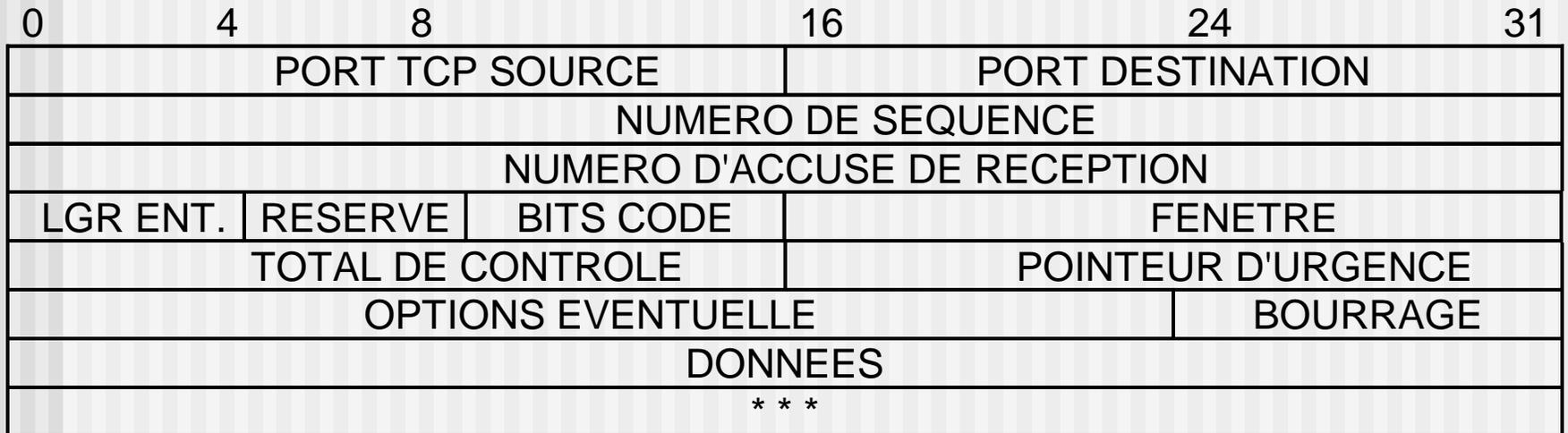
Protocole de
contrôle de
transmission

Protocole TCP

■ Principes

- message est un flot de octets (UNIX !)
 - Connexion non structurée : les applications connaissent la 'structure' du flot.
 - Numéros de séquence
- mode bidirectionnel simultané (technique dite de *superposition* : piggybacking)
- mécanisme d'anticipation (fenêtre glissante): mise en œuvre complexe.
 - taille de la fenêtre d'émission variable (contrôle de flux)
 - on acquitte sur le dernier octet d'une "séquence sans trou"
 - retransmission si temporisateur expire
- port et circuit virtuel
 - Numéros réservés : 20/ftp-data, 21/ftp, 23/telnet...
- ouverture passive/active
- segment et taille maximale de segment
- gestion de la congestion
- Pour en savoir plus : rfc793, rfc1122...

Segment TCP



Segment TCP

- PORT SOURCE, PORT DESTINATION
 - indiquent les numéros de port qui identifient les programmes d'application aux deux extrémités.
- NUMERO D'ACCUSE DE RECEPTION
 - indique le numéro du prochain octet attendu par le récepteur.
- NUMERO DE SEQUENCE
 - est celui du premier octet du segment.
- LGR ENT.
 - contient la longueur de l'en-tête en multiple de 32 bits.
- FENETRE
 - permet d'interagir sur la taille de la fenêtre émission de l'autre extrémité.

Segment TCP

- champ BITS CODE
 - permet de préciser la ou les fonctions du segment:
 - URG: Le pointeur de données urgentes est valide
 - ACK: Le champ accusé de réception est valide
 - RST: Réinitialise la connexion
 - SYN: Synchronise le numéro de séquence
 - FIN: L'émetteur a atteint la fin de son flot de données
 - PSH: oblige TCP-émetteur à envoyer toutes les données même si le tampon n'est pas plein et TCP-récepteur à donner immédiatement les données à l'application
 - exemple:
 - lors de la connexion (bit SYN), les extrémités déterminent les numéros de séquence initiaux

Segment TCP

- **POINTEUR D'URGENCE**
 - permet de repérer dans le flot de données la position de données urgentes (qui doivent "doubler" les autres données) lorsque le bit URG est positionné.
- **OPTION**
 - permet entre autres la négociation de la taille de segment à la connexion.

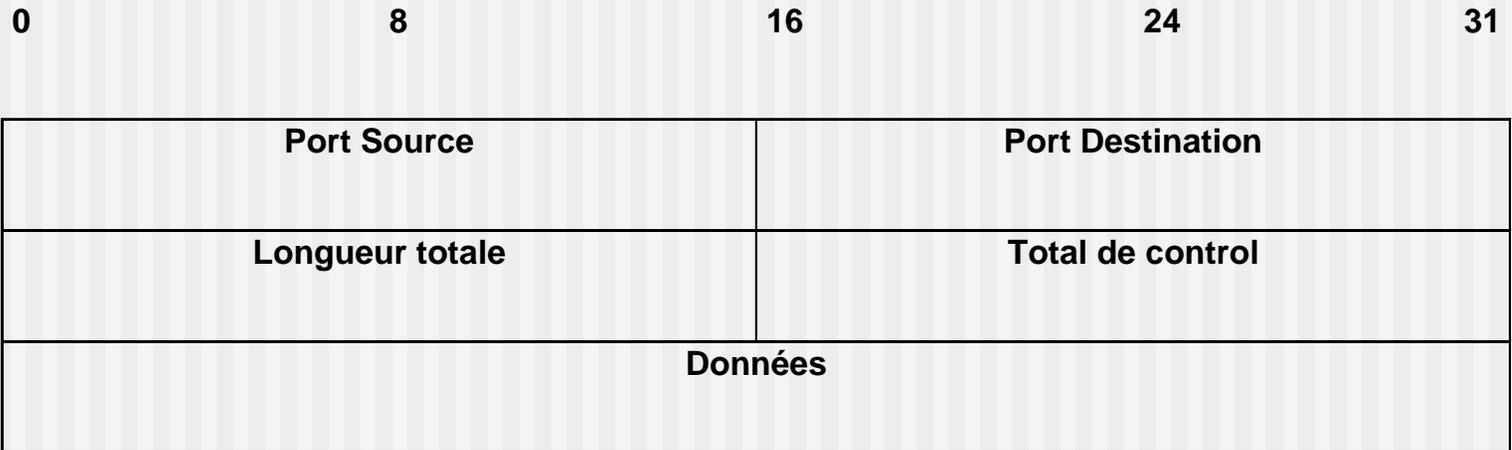
Protocole UDP

User Datagram Protocol

■ Principes

- un service de remise non fiable, mode sans connexion.
 - les messages UDP peuvent être perdus, déséquencés ou retardés.
- mécanisme de "ports" identique à TCP.

Datagramme UDP



Protocole Application NNTP

- **Documentation**

Network News Transfert Protocol, RFC 977 (Request For Comments)

- **But**

Protocole TCP pour l'envoi et la réception des nouvelles, et pour la diffusion des nouvelles entre serveurs NNTP.

- **Principes**

Dialogue client-serveur sur port réservé NNTP (119). Chaque requête du client a pour réponse une ligne commençant par un code numérique à 3 chiffres:

2xx OK

3xx Informations suivent

5xx Pas OK

- **Connexion au serveur**

Réponse du serveur:

200 Service NNTP Microsoft® Internet Services 5.5

Version: 5.5.1775.8 Posting Allowed

Protocole Application NNTP

- **Voir les groupes**

LIST

215 list of newsgroups follow

recreation.cuisine 0 1 y

recreation.soiree 0 1 y

sport 0 1 y

sport.bodybuilding 0 1 y

test 10 1 y

.

NEWGROUPS 001205 000000

231 New newsgroups follow.

recreation.cuisine 0 1 y

sport 0 1 y

sport.bodybuilding 0 1 y

sport.foot 0 1 y

.

Protocole Application NNTP

- **Voir la liste des nouvelles d'un groupe**

```
GROUP sport.foot
```

```
211 0 1 0 sport.foot
```

```
GROUP test
```

```
211 10 1 10 test
```

```
NEWNEWS test 001205 000000
```

```
230 list of new articles by message-id follows.
```

```
<Pd7KWs1XAHA.258@libreville>
```

```
<e91S3l1XAHA.258@libreville>
```

```
<NWuSSk1XAHA.258@libreville>
```

```
<sn2vMd1XAHA.258@libreville>
```

```
<LIRsMd1XAHA.258@libreville>
```

```
<6AHoMd1XAHA.258@libreville>
```

```
<p1VjMd1XAHA.258@libreville>
```

```
<4GYaMd1XAHA.258@libreville>
```

```
<n$NWMd1XAHA.258@libreville>
```

```
<2U3NMD1XAHA.258@libreville>
```

```
.
```

Protocole Application NNTP

- lire une nouvelle

group informat.ethernet

211 2 1 2 informat.ethernet

article 1

220 1 <hgC8#G2XAHA.258@libreville>

From: "admin" <admin@ist>

Subject: Peut-on connecter 2 pc directement en 10BaseT

Date: Wed, 6 Dec 2000 09:51:38 +0100

Lines: 4

X-Newsreader: Microsoft Outlook Express 4.72.3110.5

Message-ID: <hgC8#G2XAHA.258@libreville>

Newsgroups: informat.ethernet

Path: libreville

Xref: libreville informat.ethernet:1

NNTP-Posting-Host: LIBREVILLE 172.16.94.1

j'aimerais savoir s'il est possible de connecter 2 pc directement avec du 10BaseT, ce qui me permettrait d'éviter l'achat d'un hub. Merci pour toute forme de collaboration.

.

Protocole Application NNTP

- lire une nouvelle (suite)

article 3

423 no such article number in group

article <hgC8#G2XAHA.258@libreville>

...

- poster une nouvelle

POST

...

- Fin prématurée

503 connection timed out

- S'en aller

QUIT