Plan des Cours et TPs

- Cours
  - Introduction aux Réseaux
  - Couche Réseaux (IP)
  - Couche Transport (TCP et UDP)
  - Couche Liaison de données
  - Couche Physique

- TPs
  - Administration des Réseaux avec UML (IP, Routage)
  - Programmation Réseaux (Sockets)

Cours 1

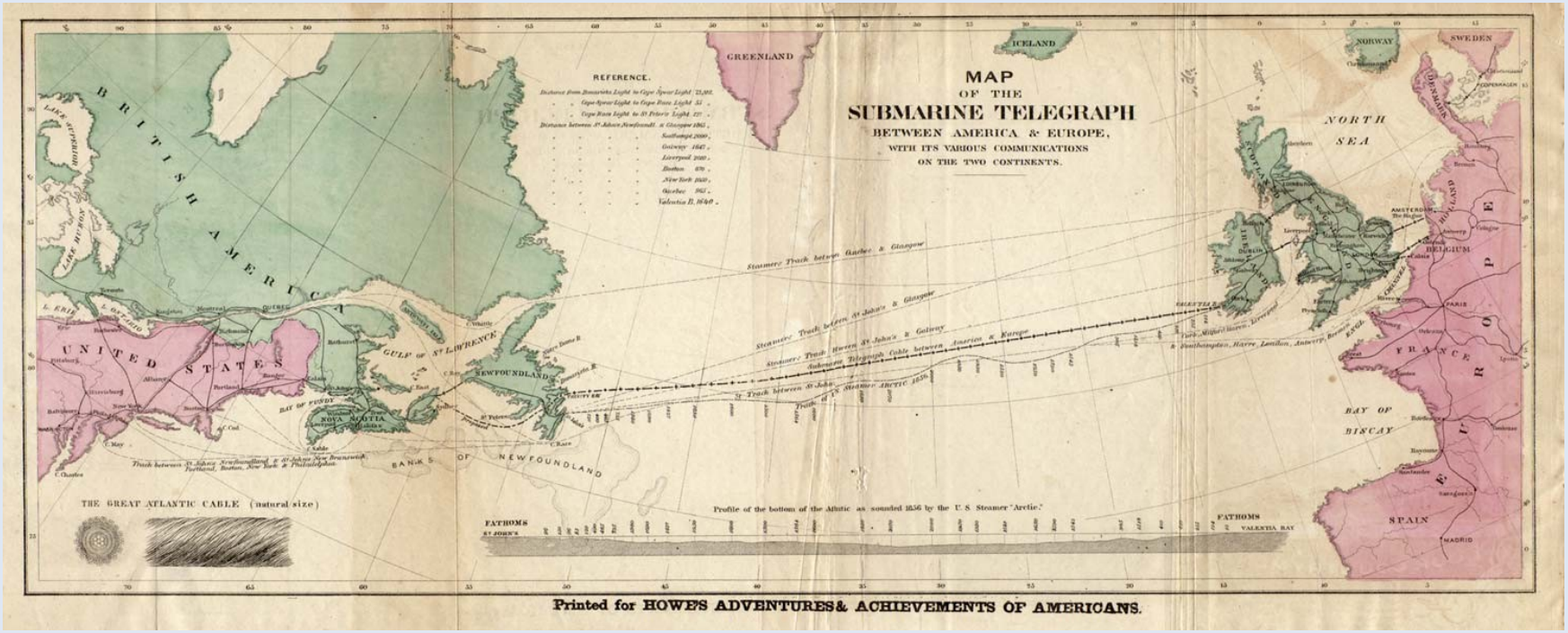
Introduction

Les télécommunications

- Télécommunication : toutes techniques de transfert d'informations
  - technique : filaire, radio, optique, satellites, ...
  - informations : symboles, textes, images, sons, vidéos, ...
- Transfert fiable d'informations entre entités communicantes
  - support de communication (lien)
  - adaptateur entité/support
  - protocole : ensemble des règles à suivre pour communiquer

Historique

- 1832 : télégraphe électrique de Morse
  - première liaison en 1844
  - 1856 en France
  - première liaison transatlantique en 1858



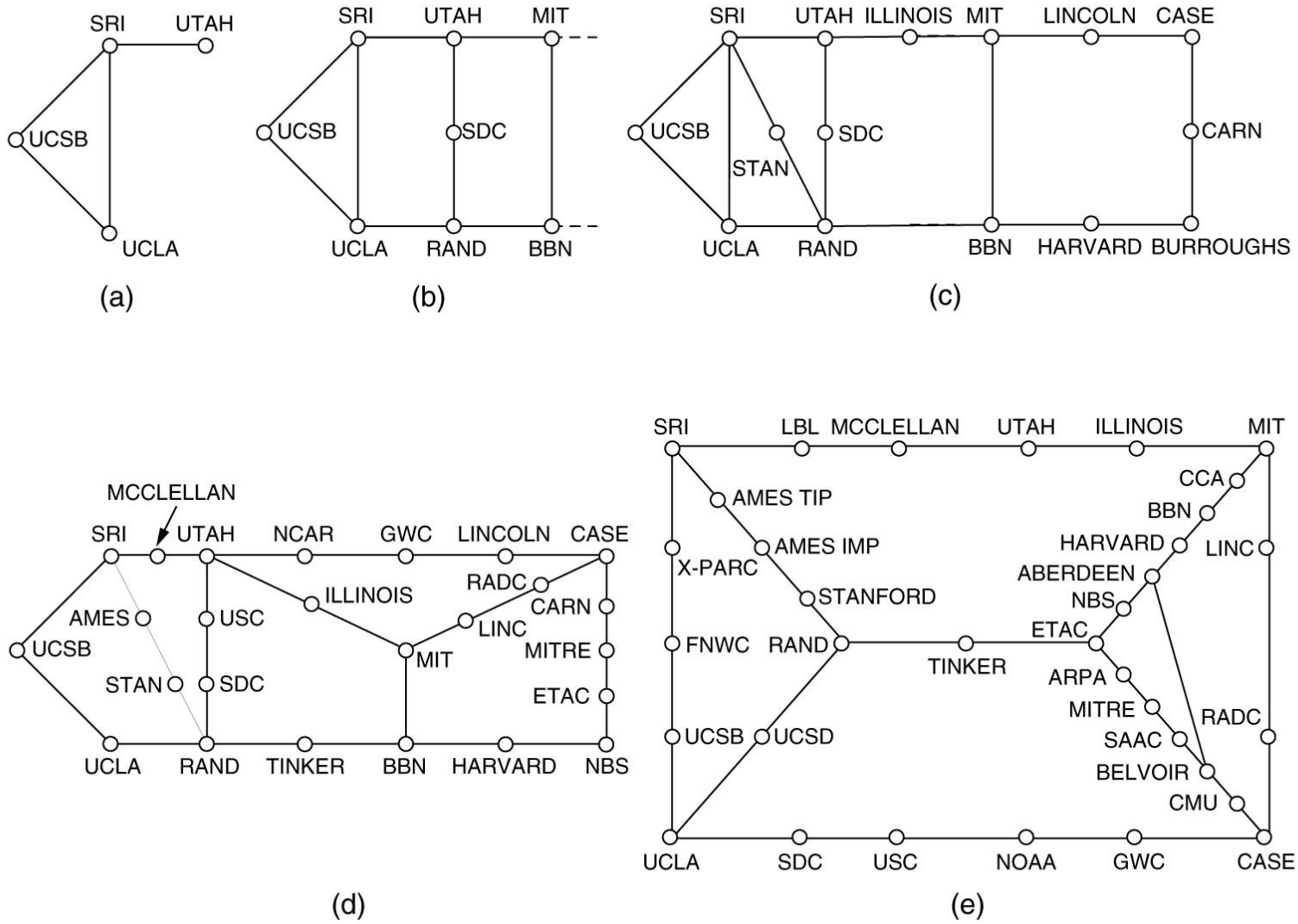
Historique

- 1899 : première liaison par onde hertzienne France/Angleterre
- 1948 : invention du transistor
- 1956 : premier câble téléphonique transocéanique
- 1962 : satellite Telstar1
  - première liaison de télévision transocéanique
- 1969 : permier pas de l'homme sur la lune (en direct)
- 1979 : premier réseau mondial de transmission de données par paquets X.25 ouvert au public
  - Transpac en France
- 1981 : minitel

Historique (Internet)

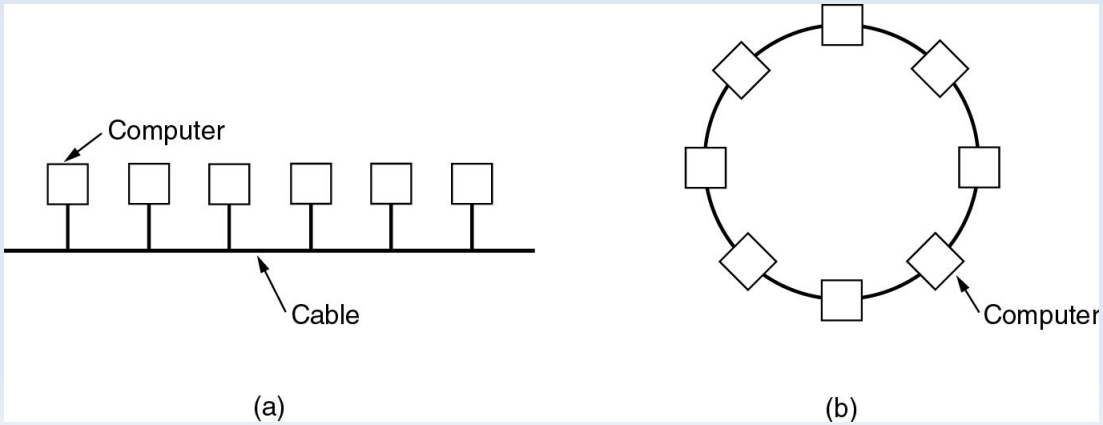
- 1959-1968 : Programme ARPA
  - ministère américain de la défense
- 1969 : ARPANET, l'ancêtre d'Internet
  - connexion des universités américaines au réseau ARPANET
- 1970-1982 : Ouverture sur le monde
  - premières connexions avec la Norvège et Londres
- 1983 : Naissance d'Internet
  - tous les réseaux s'interconnectent via le protocole TCP/IP
  - e-mail, newsgroup, telnet, ftp
- 1990 : Démocratisation d'Internet
  - invention du WWW par un physicien du CERN
  - ouverture au grand public avec les FAI (ou ISP)

ARPANET (1969-1972)



Définitions

- Réseau informatique
  - ensemble d'ordinateurs interconnectés par un support de transmission capables d'échanger de l'information
- Commutation
  - mise en relation d'un ordinateur avec n'importe quel autre
- Topologie
  - disposition des différents postes informatiques du réseau
  - bus, anneau, graphe complet, ...



Définitions

- Adressage
  - localiser un ordinateur dans un réseau décentralisé
- Contrôle d'erreur
  - détection : repérage des messages dont au moins un bit a changé de valeur lors du transfert
  - correction : compensation des erreurs soit par correction des données à l'aide de code correcteurs d'erreurs ou par destruction du message erroné et demande de retransmission
- Contrôle de flux
  - synchronisation des communications destinée à empêcher qu'un interlocuteur reçoive plus de messages qu'il ne peut en traiter

Définitions

- Multiplexage
  - technique qui consiste à faire passer deux ou plusieurs informations à travers un seul support de transmission
    - temporel (commutation)
    - spatial (féquentiel)
- Segmentation ou Fragmentation
  - découpage d'un message en plusieurs fragments de plus petites tailles puis concatenation des fragments à la réception
- Routage
  - Mécanisme par lequel le message d'un expéditeur est acheminé jusqu'à son destinataire, même si aucun des deux ne connaît le chemin complet que le message doit suivre...

Classification des réseaux

- Selon la taille
  - PAN, LAN, MAN, WAN, Internet
- Selon les types de transmission
  - supports (filaires, optique, sans fil)
  - modes de diffusion
- Selon les performances
  - latence et débit
- Selon les types de terminaux
  - réseaux informatiques, téléphoniques, domestiques

Taille des réseaux

- PAN (Personal Area Network)
  - réseau personnel : ordinateur et ses périphériques (1 m)
- LAN (Local Area Network)
  - réseau local : salle, immeuble, campus (10 m / 1 km)
- MAN (Metropolitan Area Network)
  - réseau métropolitain : à l'échelle de la ville (10 km)
- WAN (Wide Area Network)
  - réseau longue distance : à l'échelle d'un pays/continent (100 km / 1 000 km)
- Internet
  - interconnexion de réseaux à l'échelle de la planète

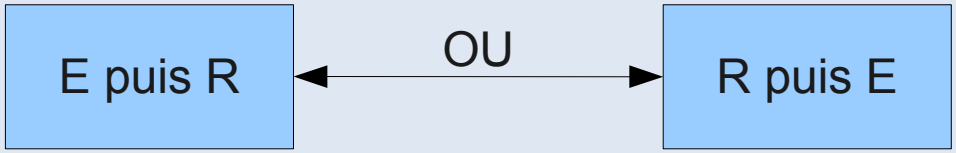
Performance des réseaux

- Débit
  - nombre de bits que le réseau peut transporter par seconde
- Latence
  - nombre de secondes que met le premier bit pou aller de la source à la destination
- Quelques exemples de débits (en bit/s)
  - modem RTC 56K, ADSL (1M à 8M)
  - Ethernet (10M, 100M, 1G, 10G), ATM (155M), FDDI (100M), ...
  - sans-fil : IEEE 802.11 (11M à 54M), GSM (14,4K), ...

Mode de transmission

- Simplex

- Half-Duplex

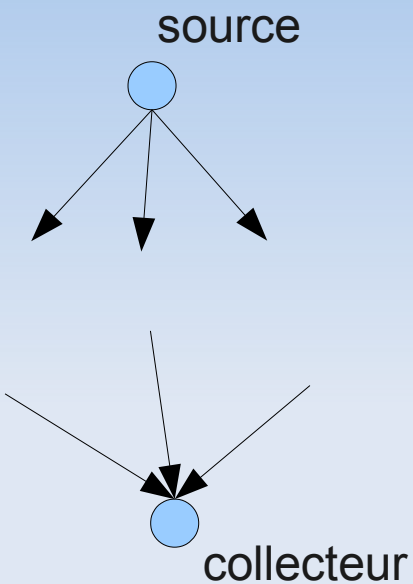


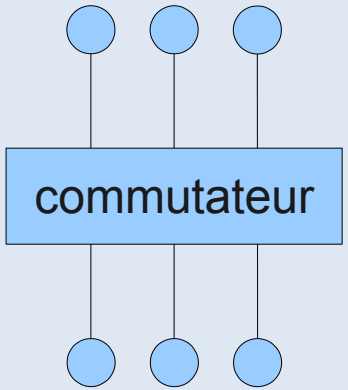
- Full-Duplex

E : Emetteur ; R : Récepteur.

Mode de diffusion

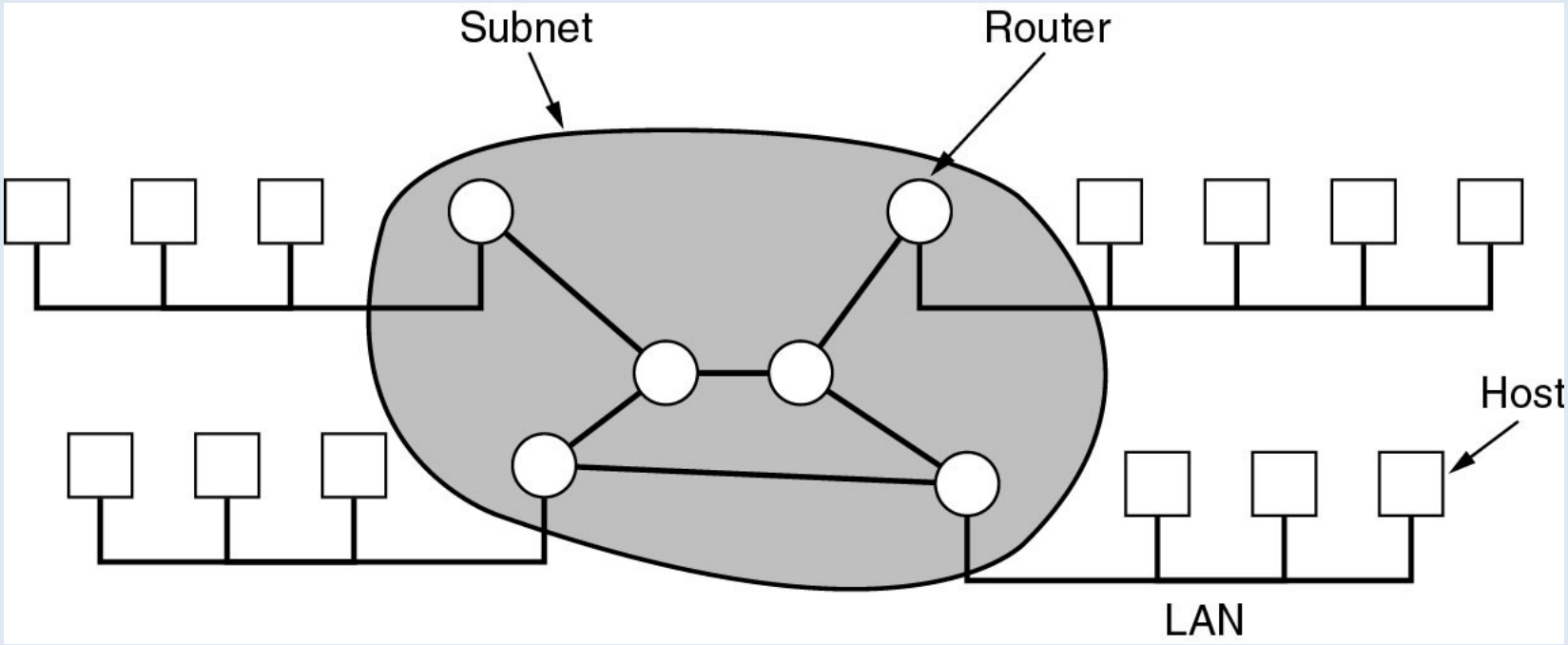
- Diffusion de 1 vers N
  - réseaux de radiodiffusion
- Collection de N vers 1
  - réseaux de télémesure
- Commutation 1 à 1 parmi N
  - réseaux téléphoniques commutés





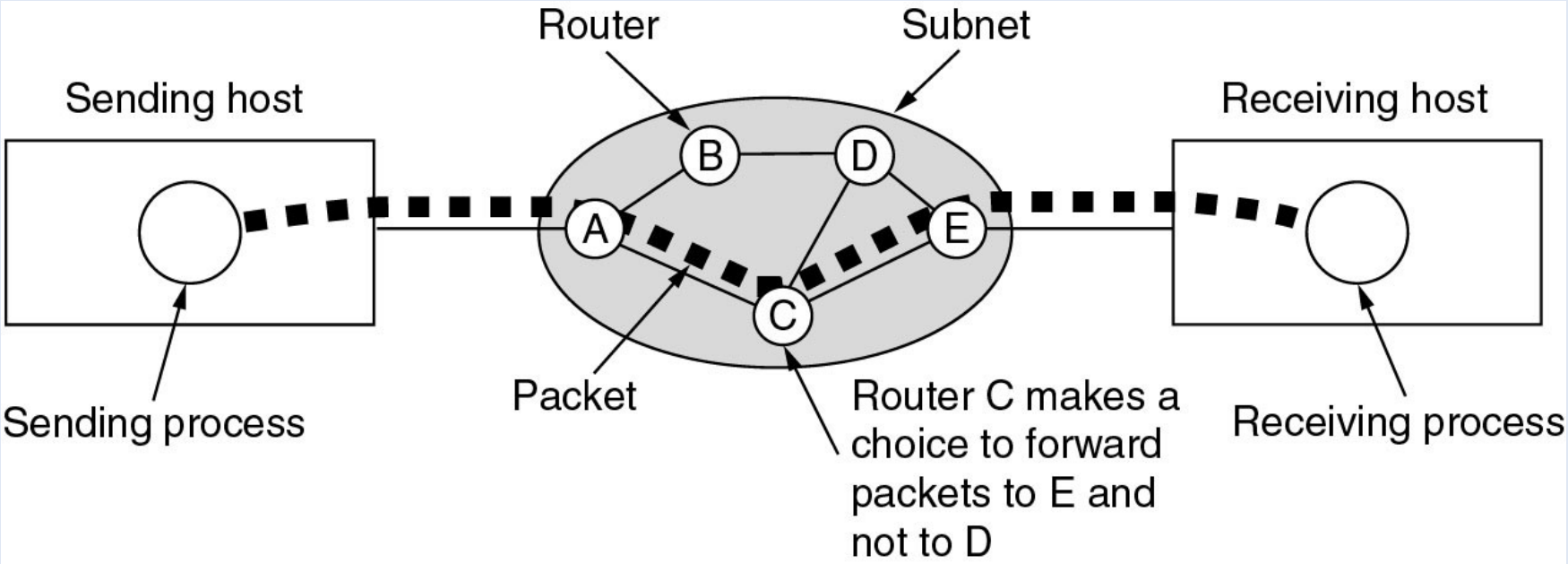
WAN (Wide Area Network)

- Réseau décentralisé comme Internet
  - collabaration nécessaire entre les sous-réseaux pour acheminer des messages entre des machines qui ne sont pas connectés directement !

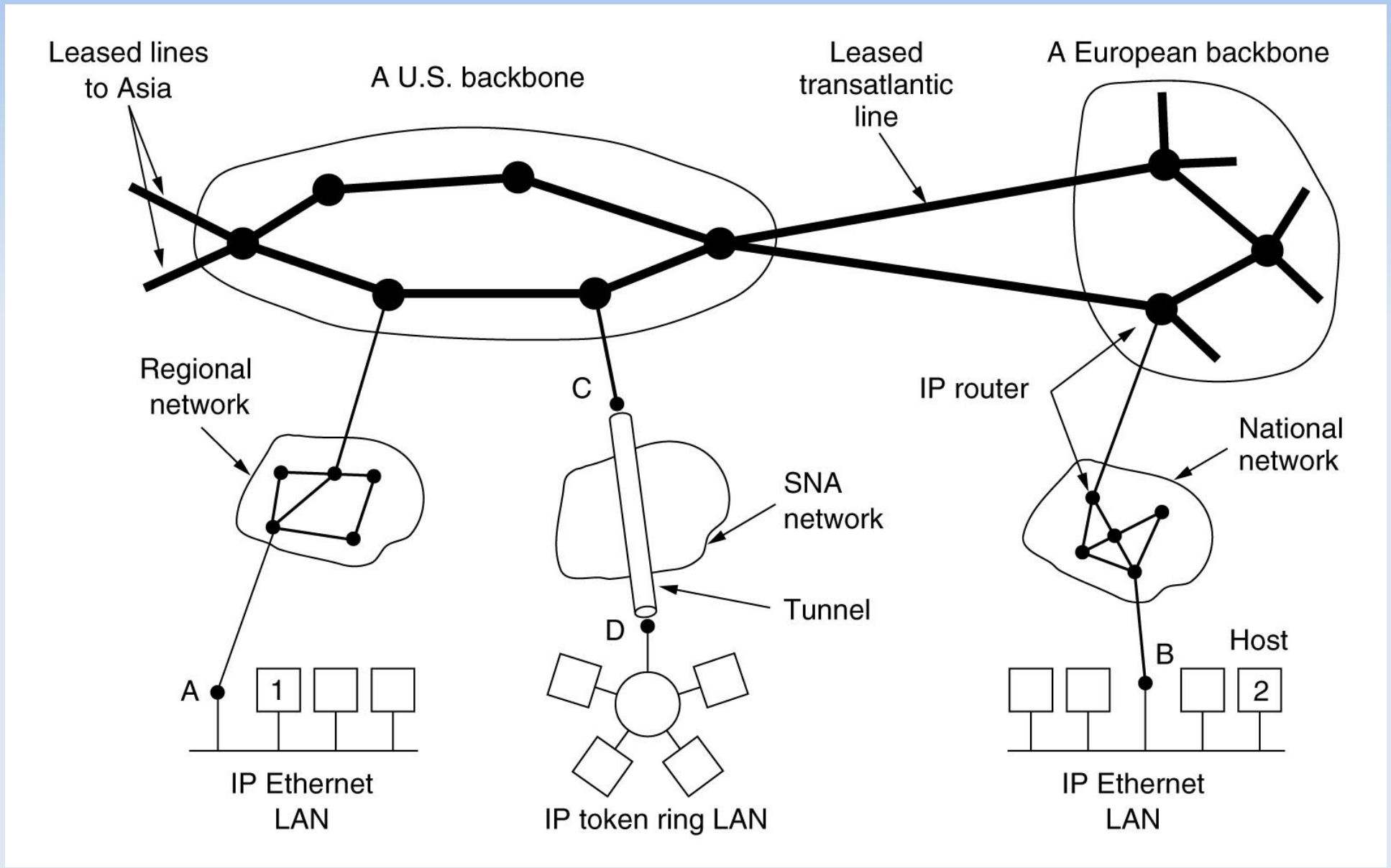


Routage

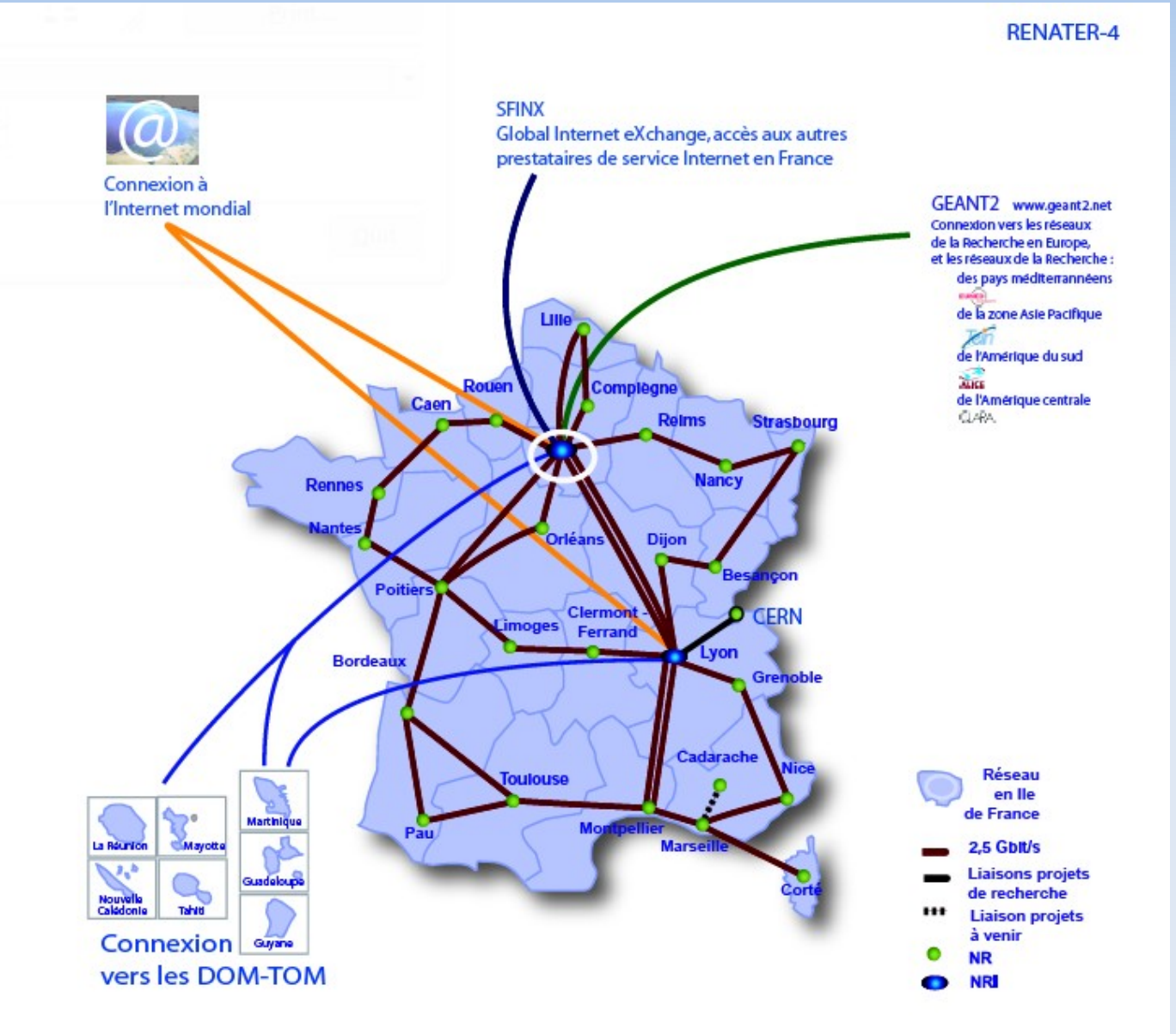
- Principe
  - Mécanisme par lequel le message d'un expéditeur est acheminé jusqu'à son destinataire, même si aucun des deux ne connaît le chemin complet que le message doit suivre...



Réseau informatique : Internet

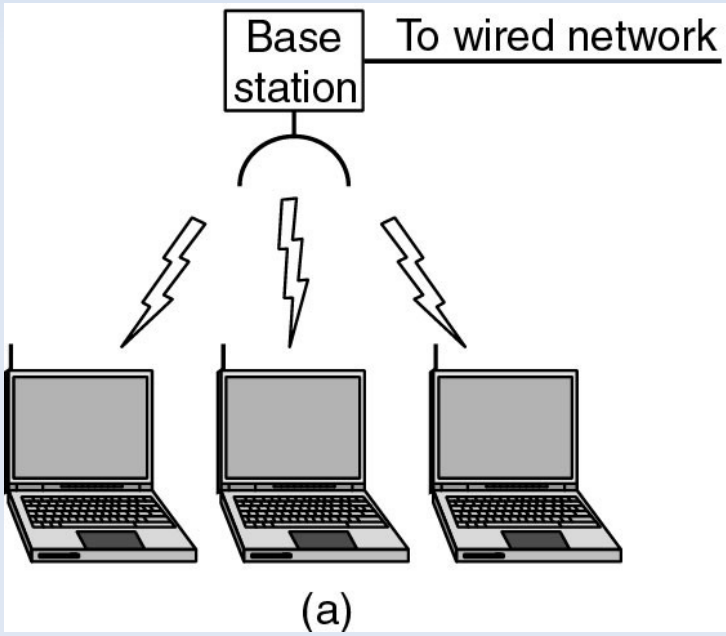


Exemple de Renater

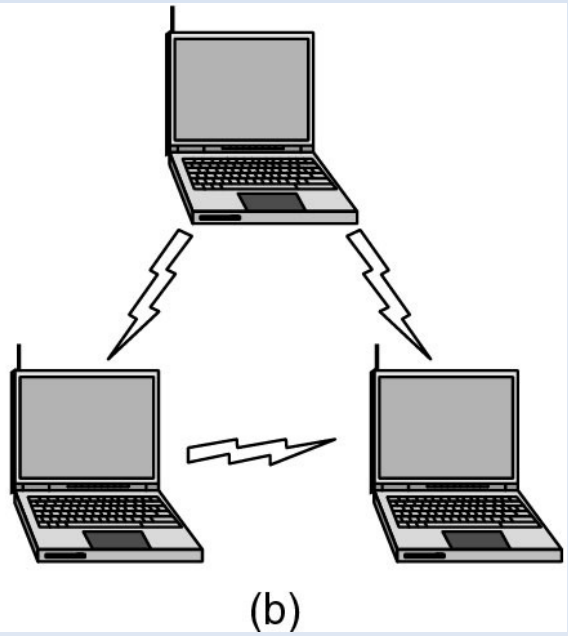


WLAN (Wireless LAN)

- Wi-Fi (IEEE 802.11b)
  - 6 à 11 Mbit/s, 300m maxi, 2,4 Ghz (13 canaux radio)



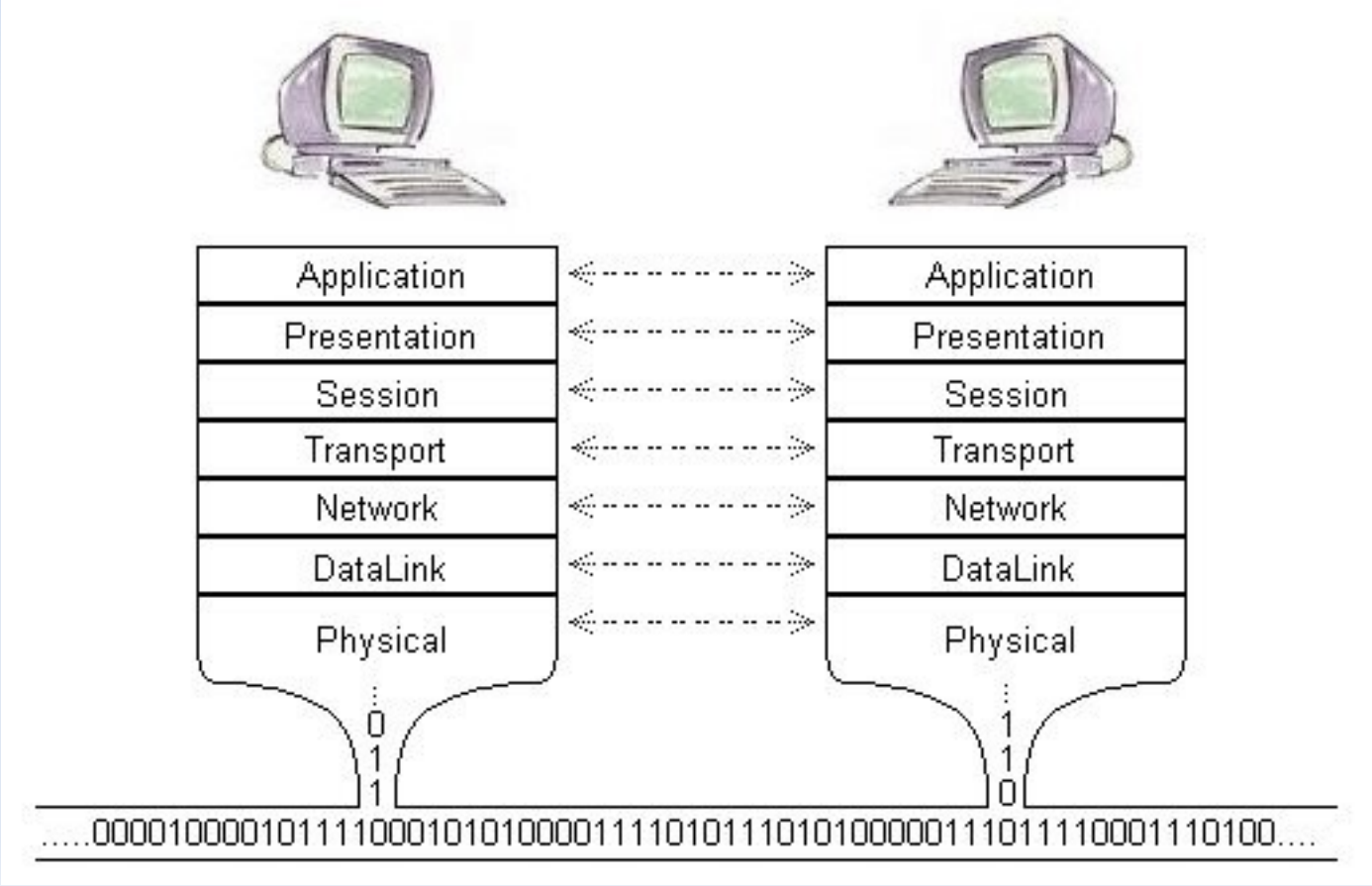
réseau sans-fil avec station de base



réseau sans-fil ad hoc

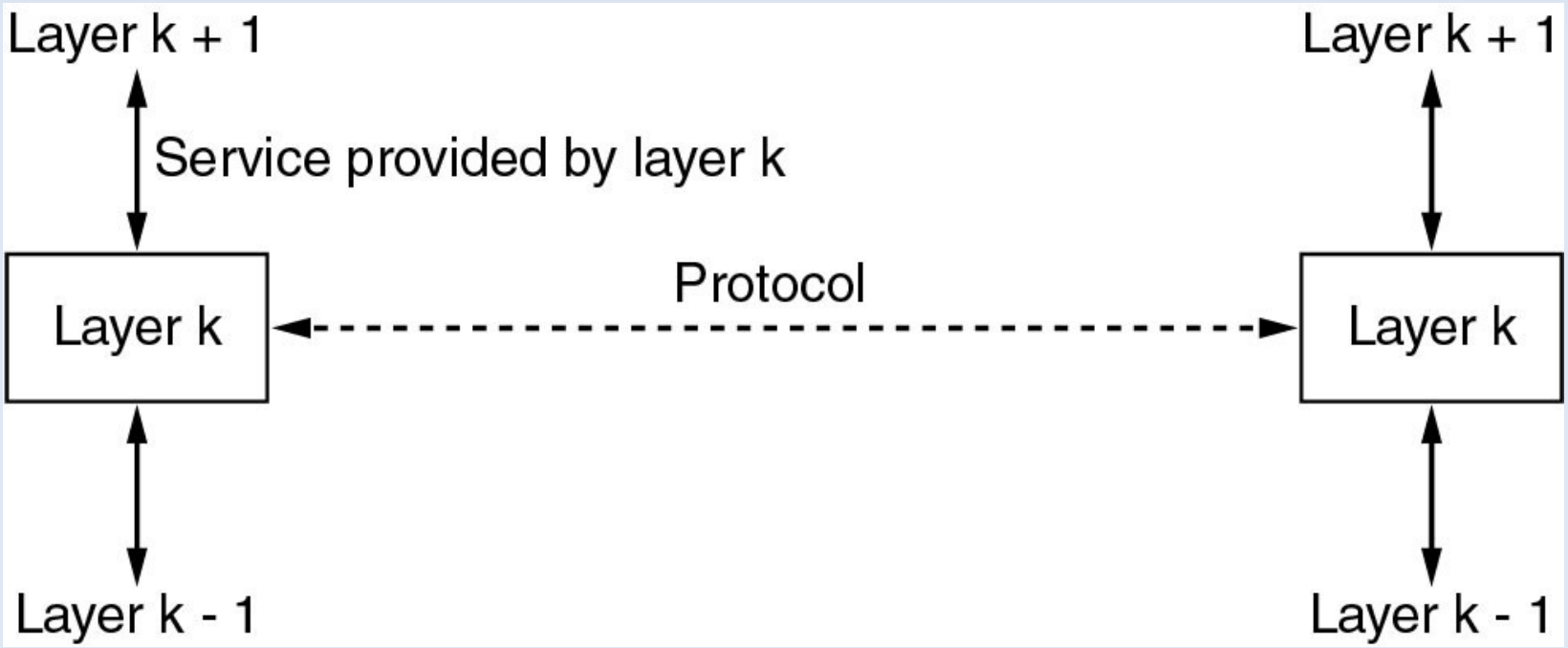
Modèle de référence OSI

- Protocole
  - spécification de plusieurs règles pour communiquer sur une même couche d'abstraction entre deux machines différentes

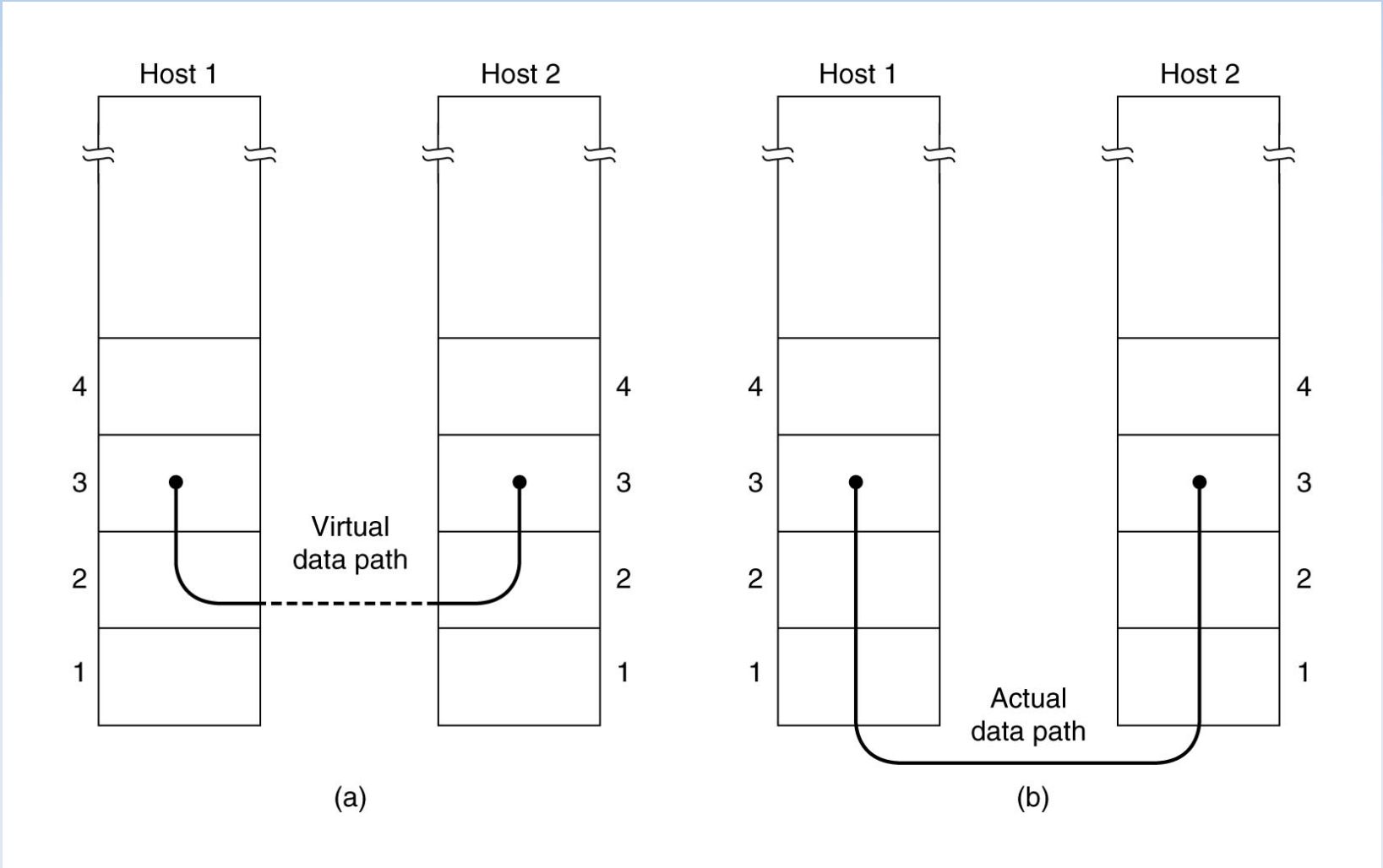


Abstraction en couche

- Pile de protocoles
  - le protocole de la couche k fournit un service à la couche k+1 en s'appuyant sur le service fournit par la couche k-1



Abstraction en couche



Les couches basses (OSI)

(1) Couche physique (physical layer)

- transmission effective des signaux entre les interlocuteurs
- service typiquement limité à l'émission et la réception d'un bit ou d'un train de bit continu

(2) Couche liaison de données (datalink layer)

- communications entre 2 machines adjacentes, i.e. directement reliés entre elle par un support physique

(3) Couche réseaux (network layer)

- communications de bout en bout, généralement entre machines : adressage logique et routage des paquets

(4) Couche transport (transport layer)

- communications de bout en bout entre processus

Les couches hautes (OSI)

(5) Couche session (session layer)

- synchronisation des échanges et transaction, permet l'ouverture et la fermeture de session

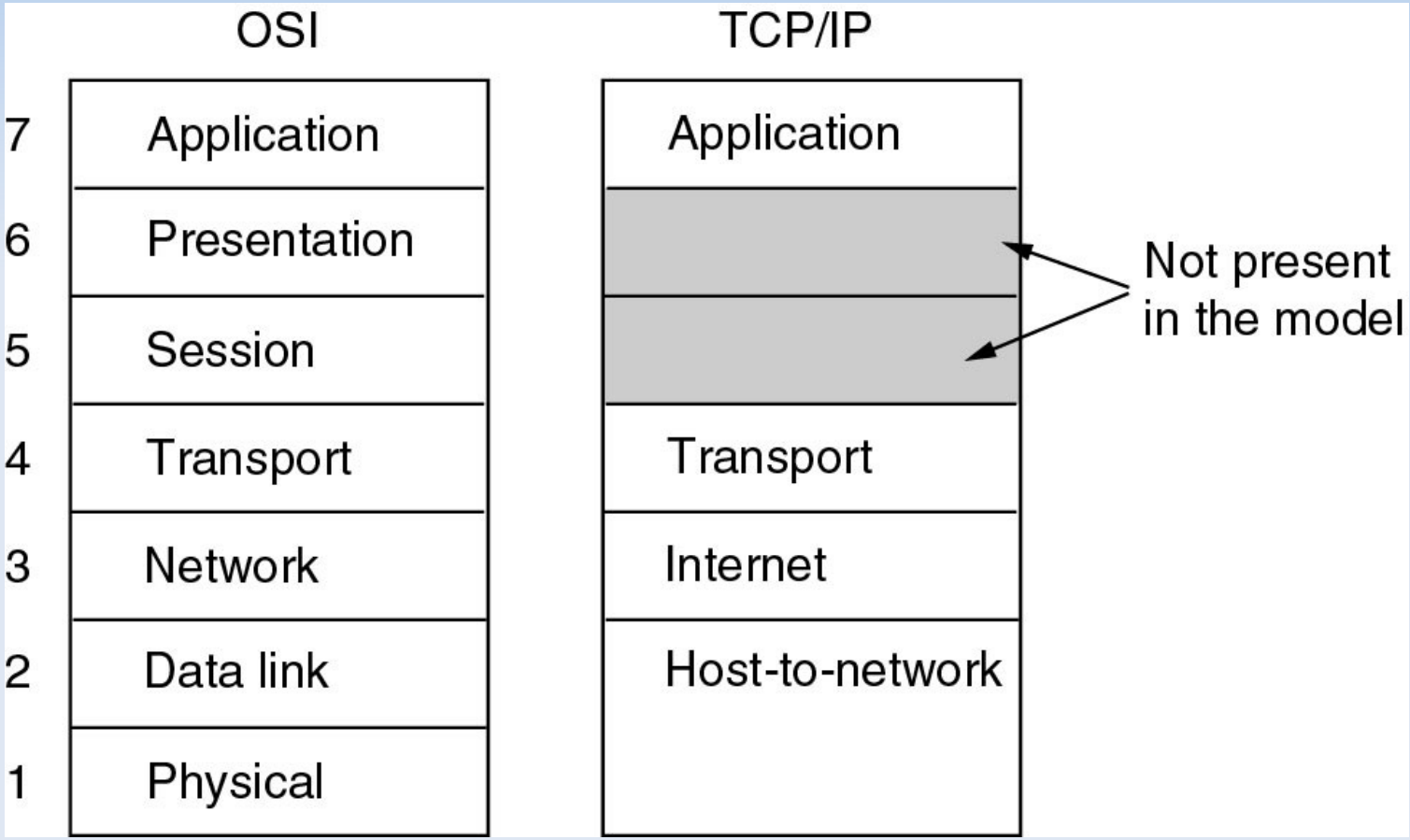
(6) Couche présentation

- codage des données applicatives, et plus précisément conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises

(7) Couche application

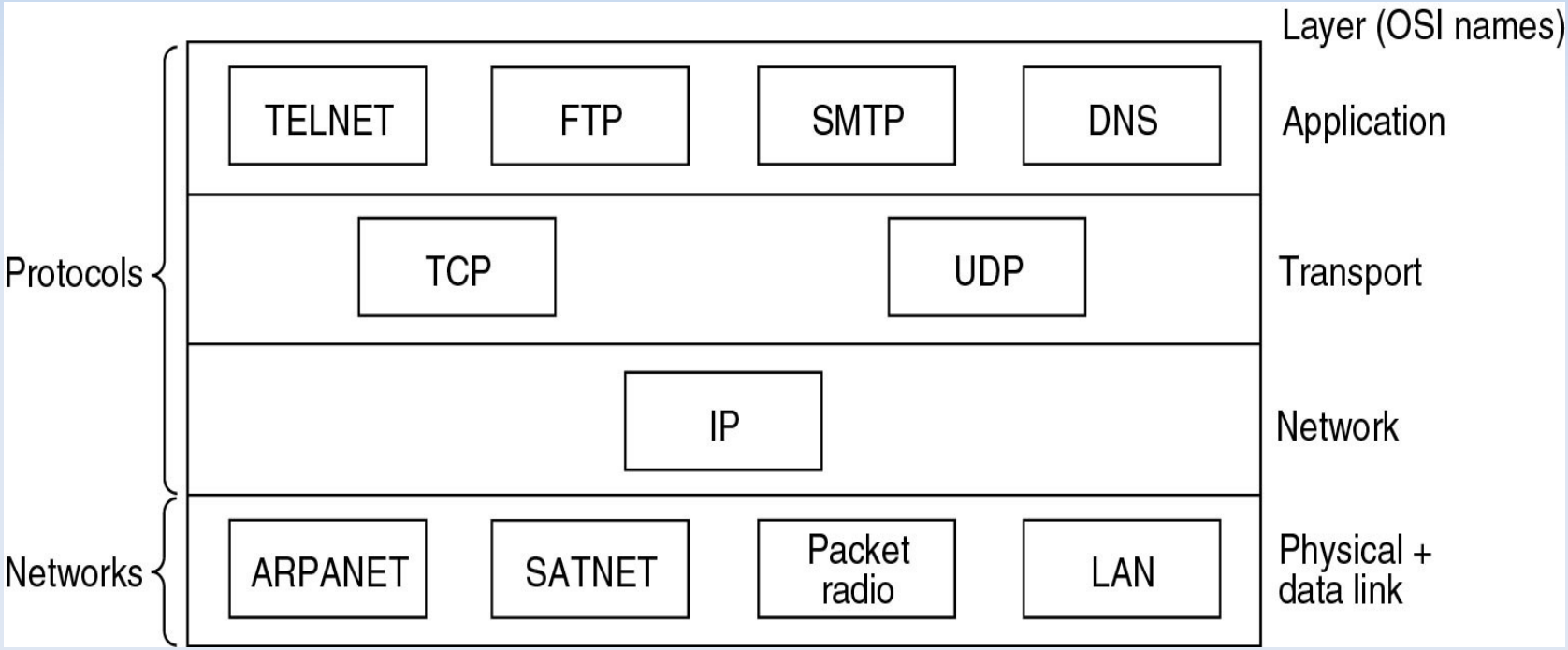
- point d'accès aux services réseaux
- elle n'a pas de service propre spécifiable et entrant dans la portée de la norme

Modèles OSI et TCP/IP

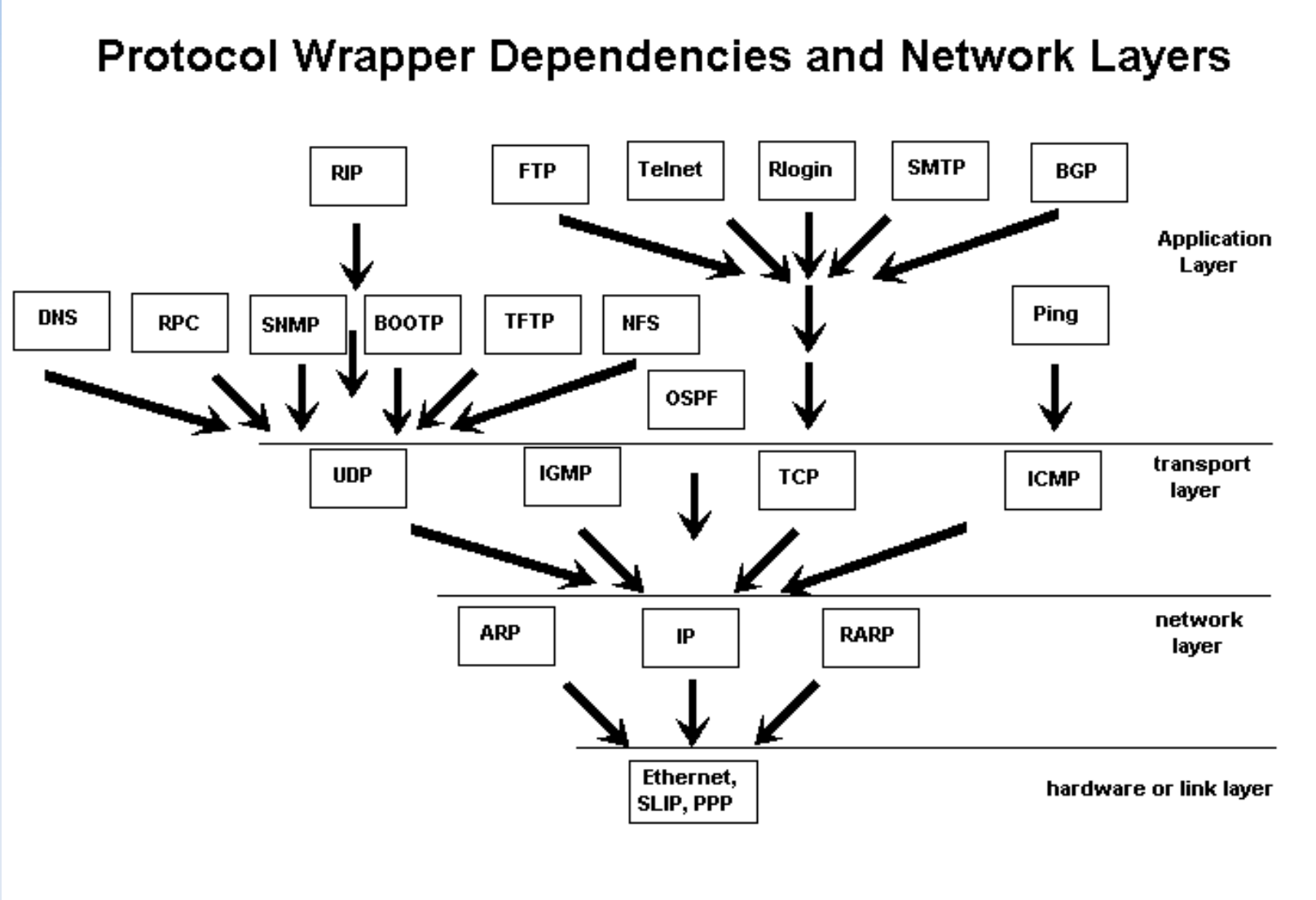


Famille de protocoles TCP/IP

- IP, TCP, UDP, ...

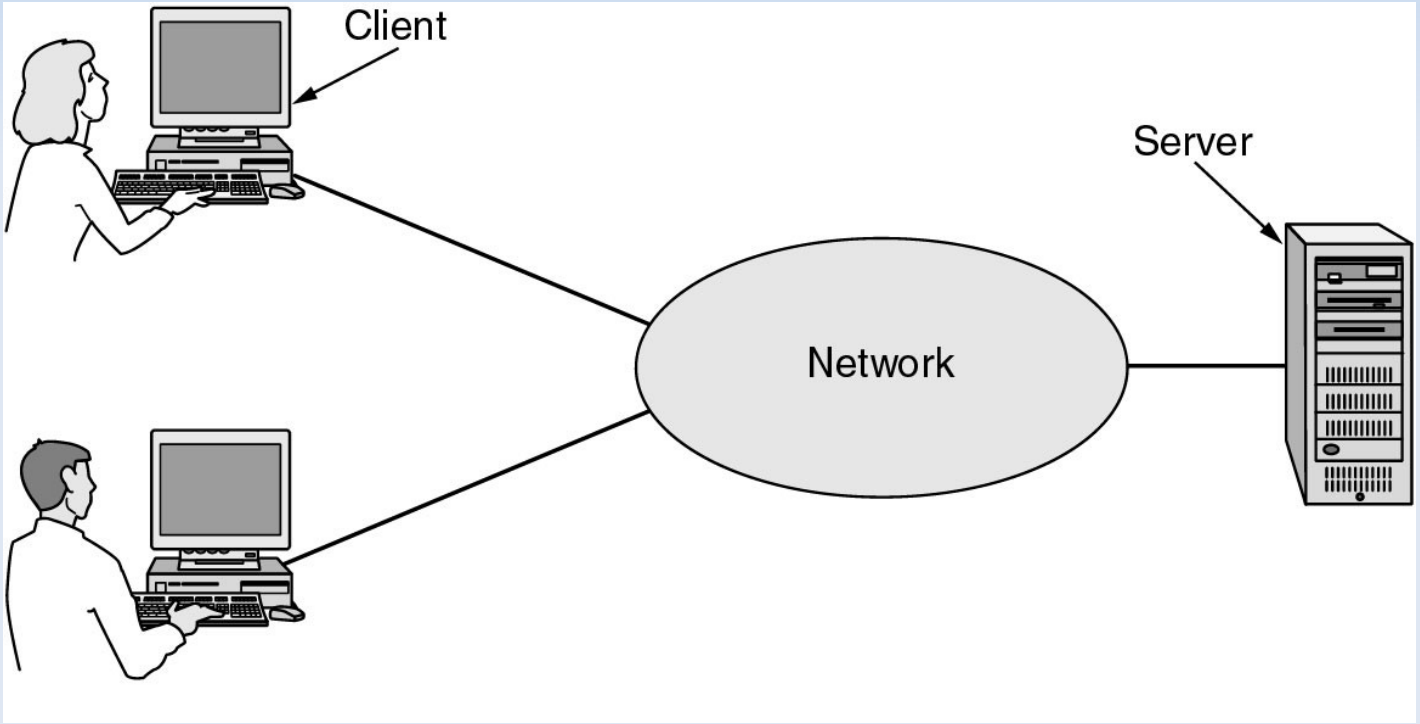


Piles de protocoles



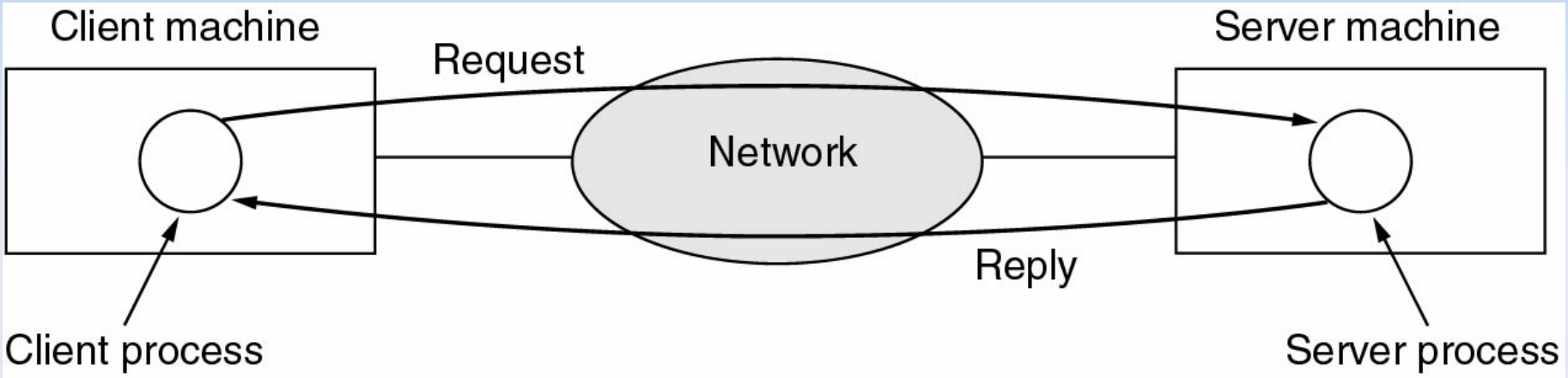
Modèle client-serveur

- Plusieurs clients et un serveur



Modèle client-serveur

- Schéma de communication requête-réponse...



- Notion de connexion
  - adresse IP source, numéro de port source
  - adresse IP destination, numéro de port destination

Cours 2

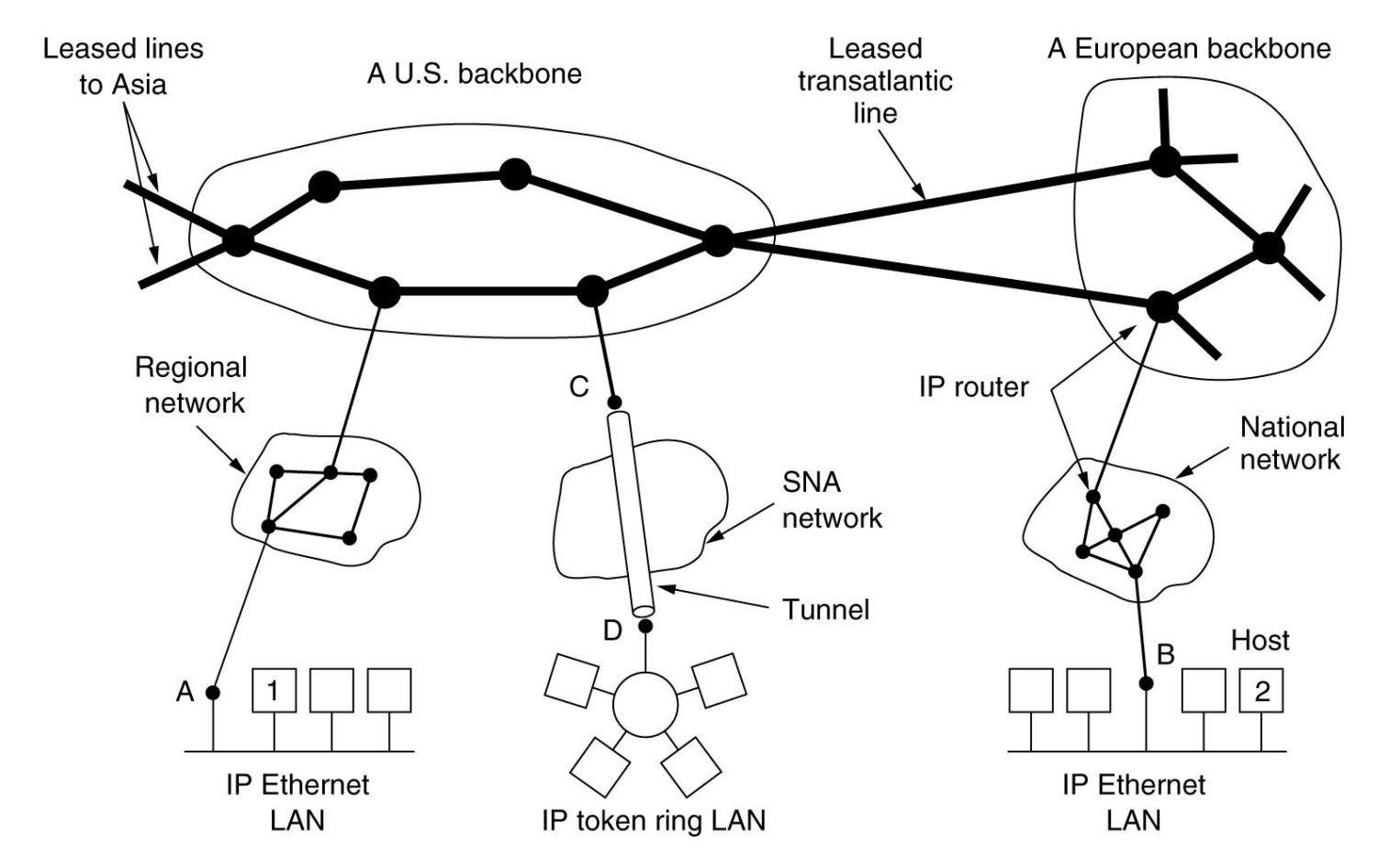
Couche Réseaux
(IP)

Introduction

- Internet Protocol (IP)
  - communication de bout en bout entre des machines qui ne sont pas connectés directements, c'est-à-dire situées dans des réseaux locaux différents (géographie, technologie)
  - adressage logique : identifier les machines indépendament de l'adressage physique (Ethernet, ...)
  - routage : acheminement des données entre les réseaux via des routeurs/passerelles intermédiaires
- Versions
  - IPv4, RFC 791, sept. 1981 (2^{32} adresses)
  - IPv6, le successeur de IPv4, RFC 2460, déc. 1998 (2^{128} adresses)

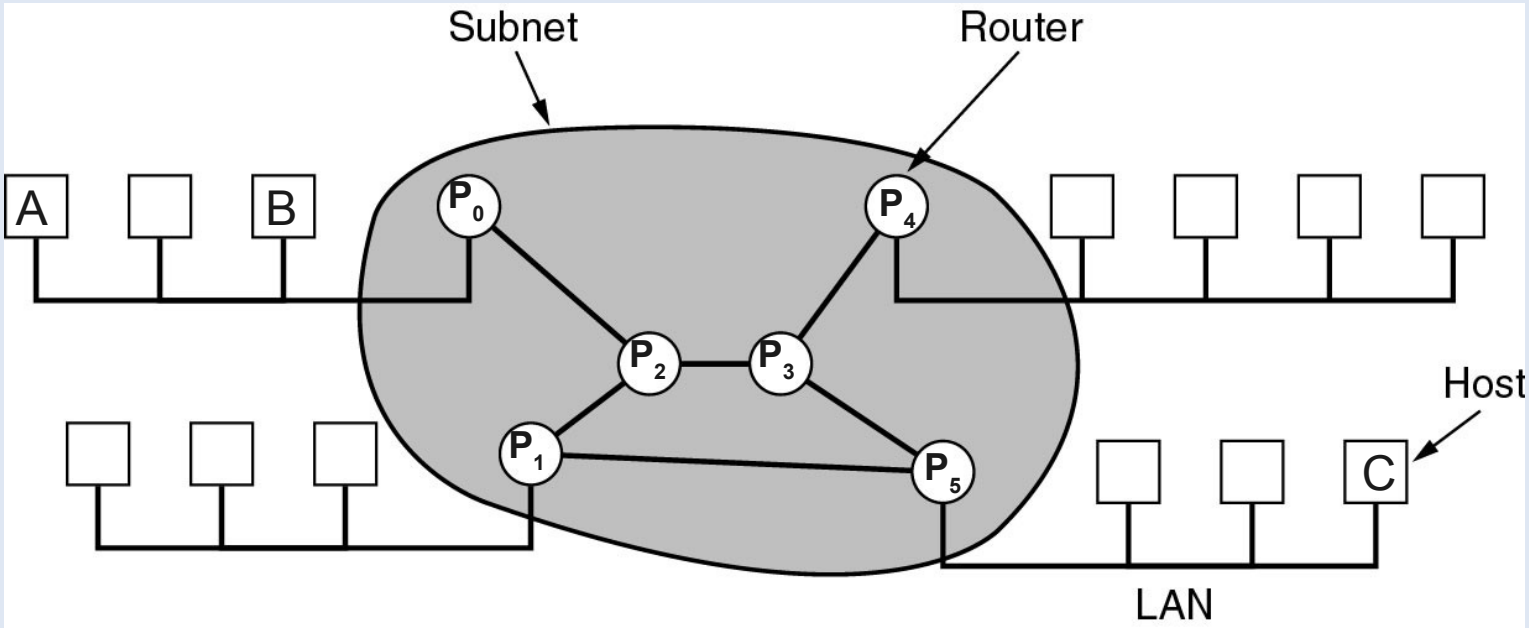
Le réseau Internet

- Interconnexion de multiples réseaux hétérogènes et distants...

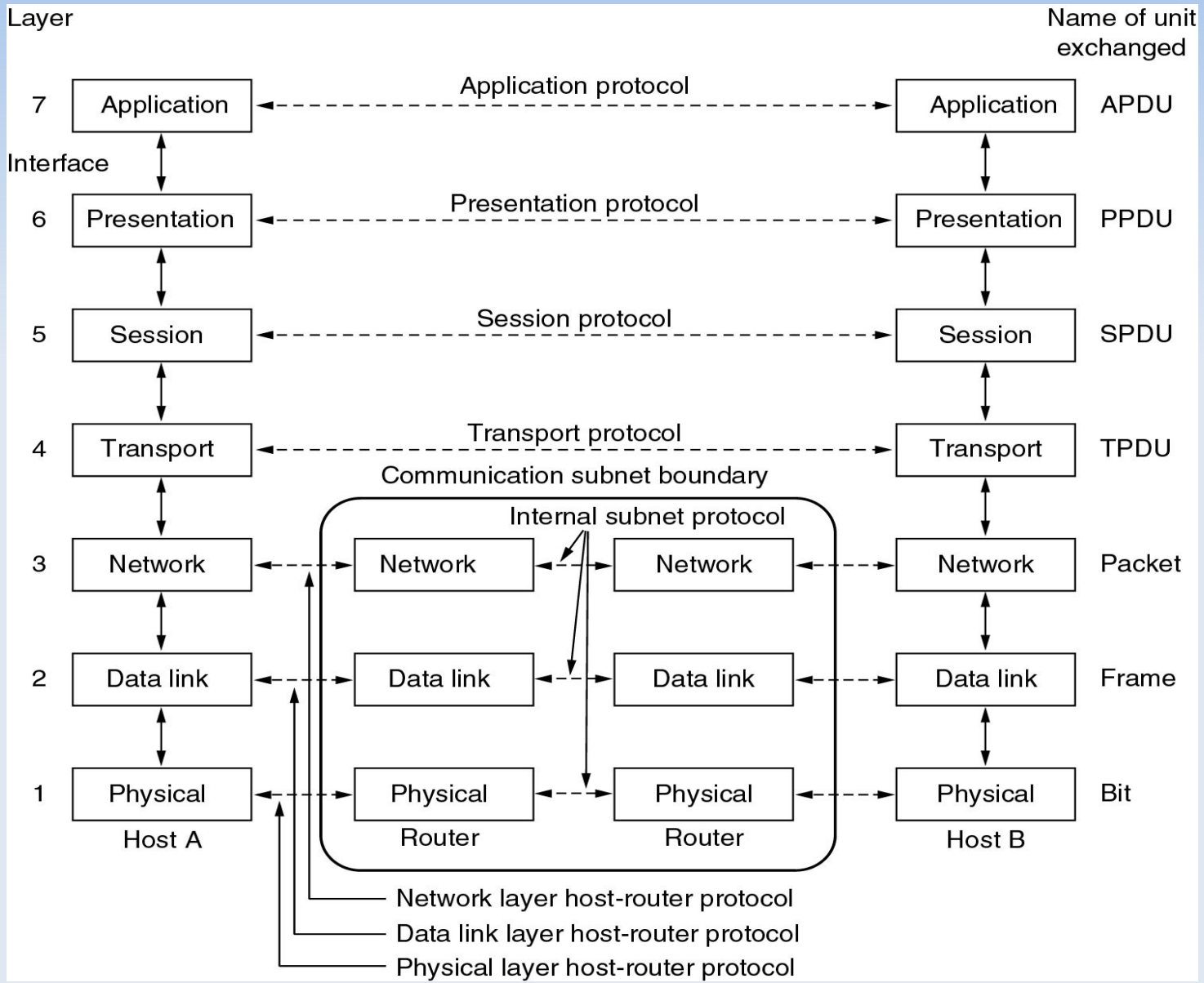


Introduction

- Communication directe de A vers B
- Communication de A vers C via P_0, puis P_2, ...
  - la passerelle permet de passer d'un réseau à un autre ; elle possède donc deux interfaces réseau

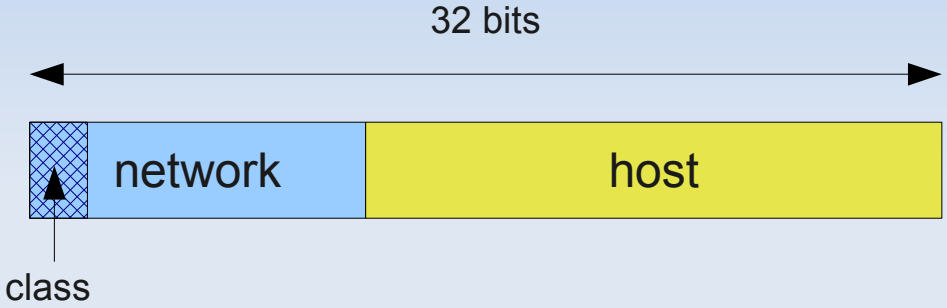


Modèle OSI : routeur



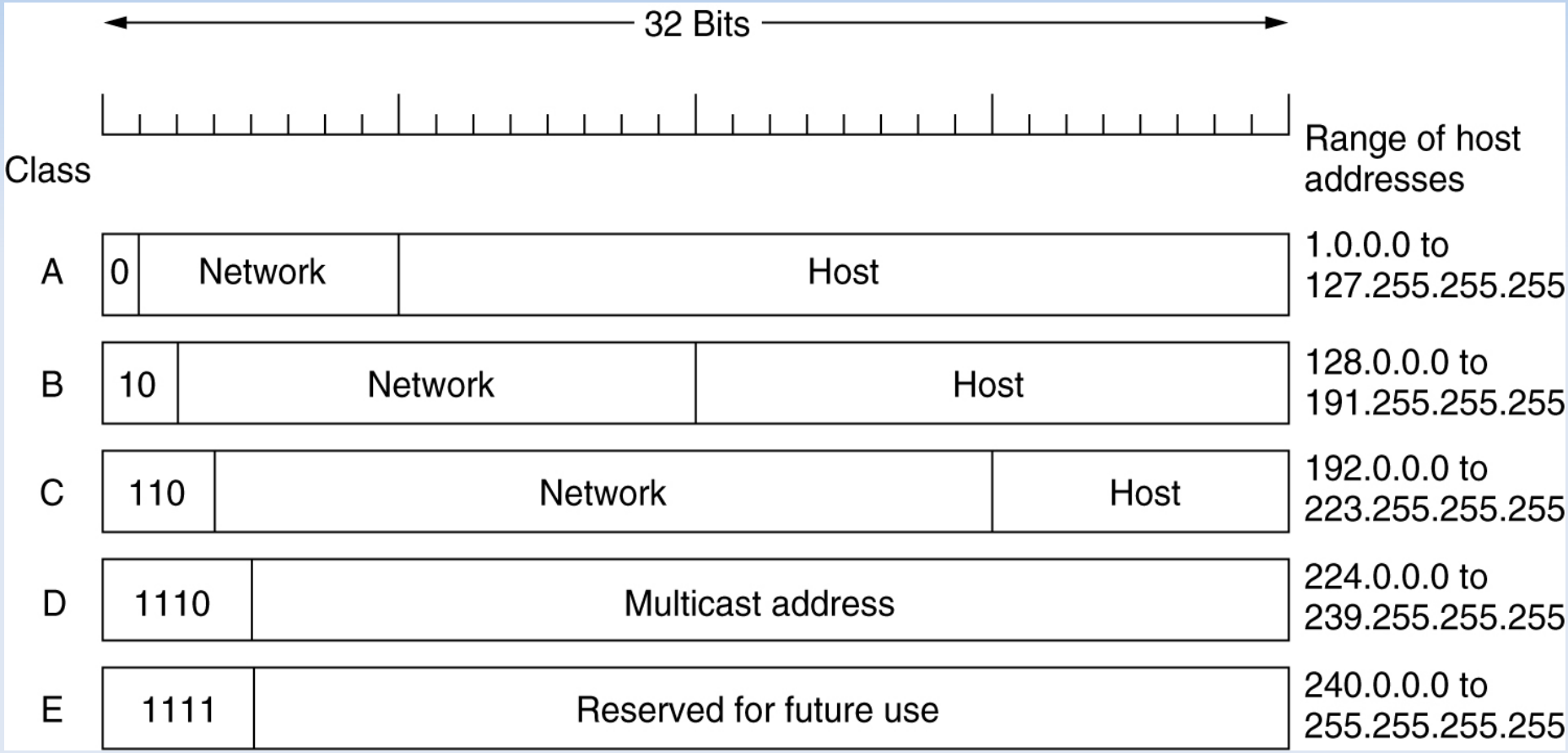
Adressage IP

- Format des adresses IP (32 bits)
  - 2^{32} adresses, environ 4 milliards d'adresses



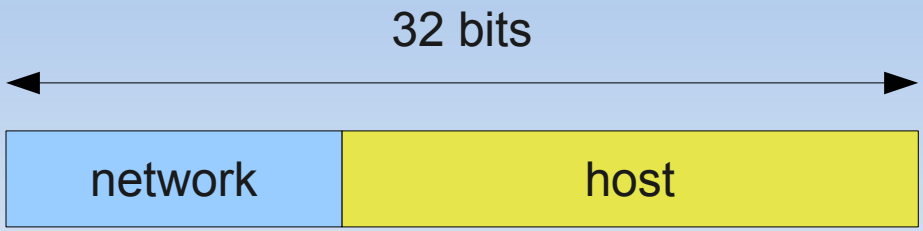
- Les 5 classes d'adresse IP
  - classes générales A, B, C (unicast)
    - classe A : 8 bits network, 24 bits host (grands réseaux)
    - classe B : 16 bits network, 16 bits host (moyens réseaux)
    - classe C : 24 bits network, 8 bits host (petits réseaux)
  - classe D (multicast)
  - classe E (réservé pour un usage futur)

Adressage IP



Adressage IP

- Format des adresses IP



- Les adresses spéciales
  - Adresse de la machine locale : 0.0.0.0
  - Adresse de diffusion dans le réseau local : 255.255.255.255
  - Adresse de la boucle locale (loopback) : 127.*.*.*
  - Adresse d'un réseau distant : tous les bits de l'adresse hôte sont à 0
  - Adresse de diffusion dans un réseau distant : tous les bits de l'adresse hôte sont à 1
  - Adresse du routeur (par convention) : adresse de diffusion – 1

Adressage IP

- Exercice 2.1
  - Compléter le tableau suivant...

Adresse IP Hôte	Classe d'adresses	Adresse Réseau	Adresse Hôte	Adresse de broadcast réseau	Masque de sous-réseau
216.14.55.137					
123.1.1.15					
175.12.239.244					

Adressage IP

- Exercice 2.1 (correction)

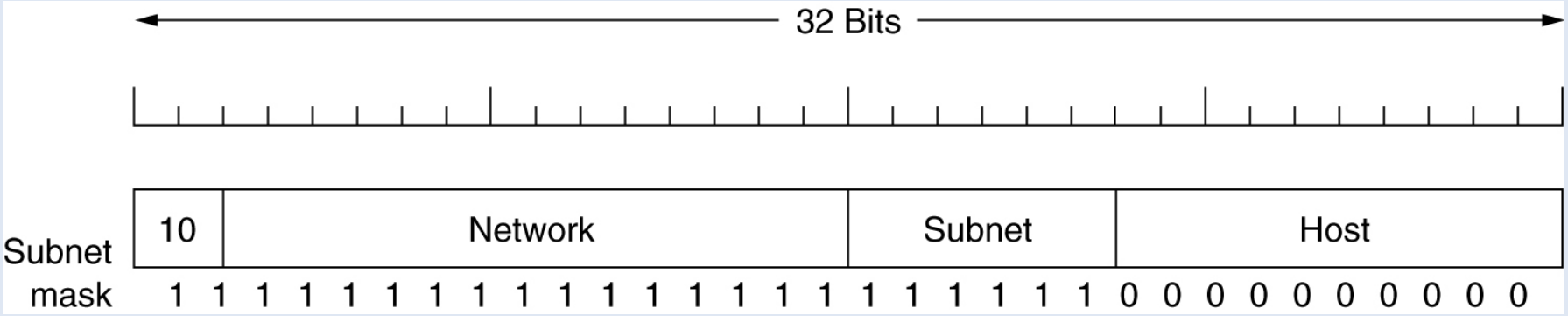
Adresse IP Hôte	Classe d'adresses	Adresse Réseau	Adresse Hôte	Adresse de broadcast réseau	Masque de sous-réseau
216.14.55.137	C	216.14.55.0	.137	216.14.55.255	255.255.255.0
123.1.1.15	A	123.0.0.0	1.1.15	123.255.255.255	255.0.0.0
175.12.239.244	B	175.12.0.0	239.244	175.12.255.255	255.255.0.0

Réseau privé

- Besoin de réseaux privés
  - sécurité : réseau inaccessible depuis l'extérieur (Internet)
  - palier le manque d'adresse dans IPv4
    - seulement 256 adresses publiques disponibles pour un réseau acheté de classe C
- Adresses privées (utilisables uniquement en interne)
  - classe A : 10.0.0.0 – 10.255.255.255 (1 réseau)
  - classe B : 172.16.0.0 – 172.31.255.255 (16 réseaux)
  - classe C : 192.168.0.0 – 192.168.255.255 (256 réseaux)
- Seule la passerelle d'un réseau privé nécessite de posséder une adresse Internet publique !

Sous-réseaux

- Délimitation de plusieurs sous-réseaux dans un réseau
  - Adresse IP découpée en trois parties (network, subnet, host)
  - On utilise une partie des bits de l'hôte pour identifier le sous-réseau (subnet).



- Masque de sous-réseau
  - Le masque du sous-réseau s'obtient en mettant à 1 tous les bits du réseau et du sous-réseau, puis le reste à 0.
  - (adresse IP) AND (masque) = (adresse sous-réseau)

Sous-réseaux

- Exercice 2.2
  - Dans un réseau de classe C d'adresse IP 193.51.199.0, on souhaite constituer 5 sous-réseaux.
  - Combien de bits sont nécessaires pour coder ces sous-réseaux ?
  - Quel est le masque de réseau et de sous-réseau ?
  - A quel sous-réseau appartient la machine d'adresse 193.51.199.67 ?

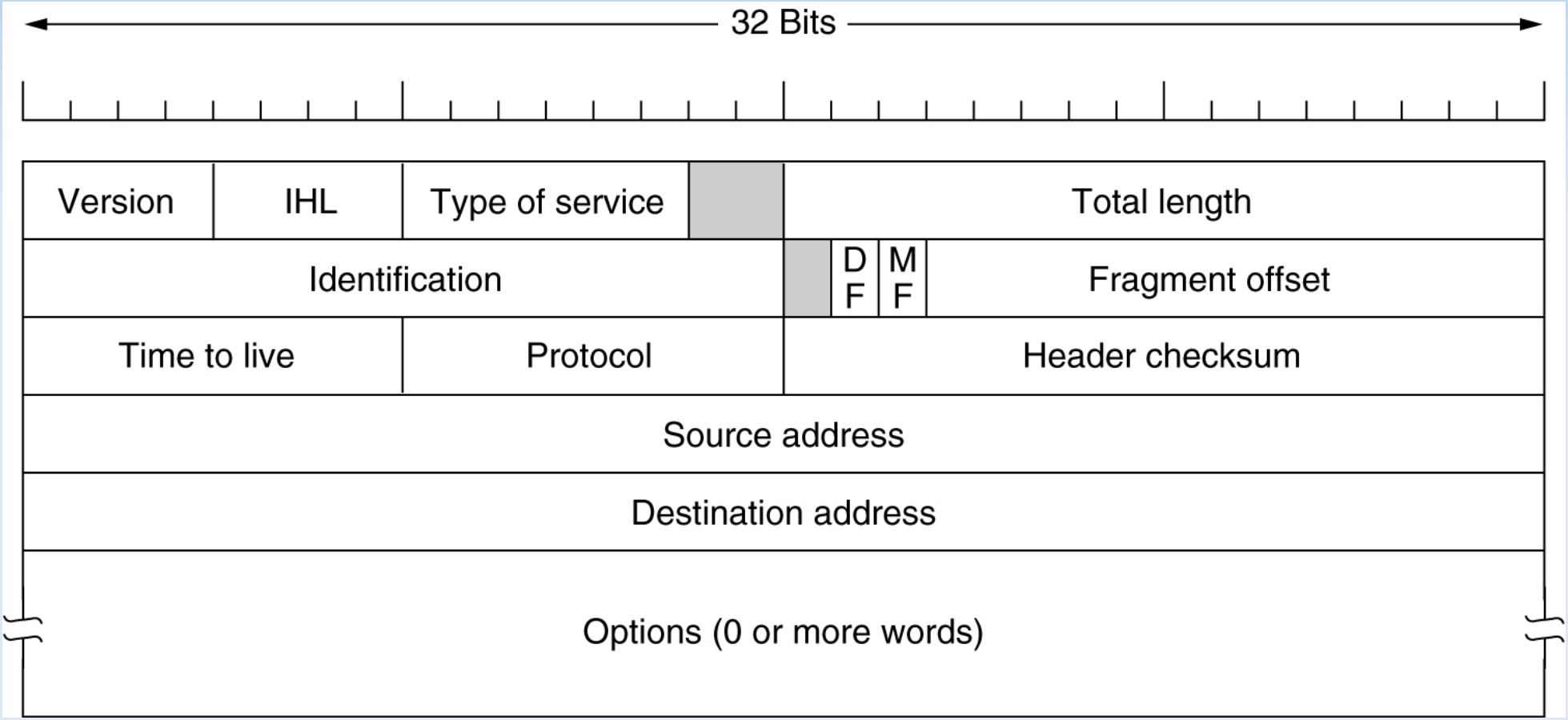
Sous-réseaux

- Exercice 2.2 (correction)
  - Il faut 3 bits pour coder la partie sous-réseau à choisir parmi 000, 001, 010, 011, 100, 101, 110 et 111 (nb max de sous-réseaux avec n bits = 2^n)
  - Le masque du réseau de classe C est 255.255.255.0.
  - Le masque du sous-réseau est 255.255.255.224 car 224 = $(1110\ 0000)_{binaire}$
  - adresse du réseau
    - 193.51.199.67 AND 255.255.255.0 = 193.51.199.0
  - adresse sous-réseau
    - 193.51.199.67 AND 255.255.255.224 = 193.51.199.X
    - X = 67 AND 224 = $(010\ 00011)_{binaire}$ AND $(111\ 00000)_{binaire}$
    - X = 010 0000 = 64 ; adresse sous-réseau = 193.51.199.64

Sous-Réseaux : VLSM

- Sous-réseaux de tailles variables
  - VLSM = Variable-Length Subnet Masking...
  - http://www.iprezo.org/index.php?page=vlsm
  - A compléter...

En-tête du paquet IP (v4)



En-tête du paquet IP (v4)

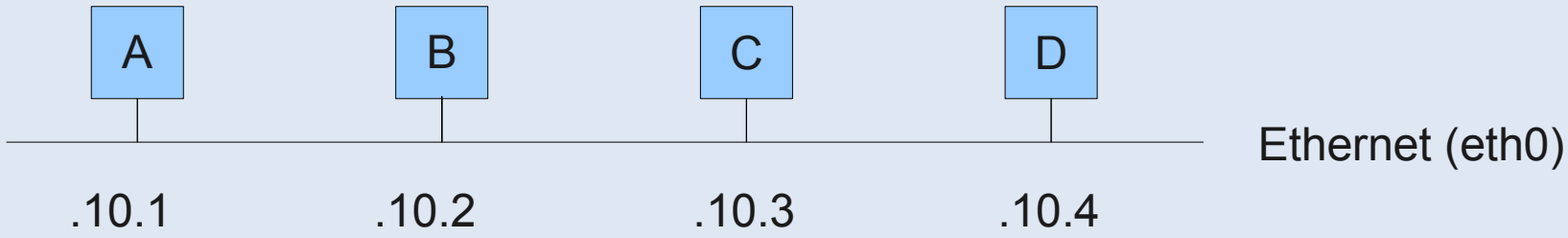
- Version : v4
- IHL (Internet Header Length) : longueur de l'en-tête en mot de 32 bits
- Type of Service : qualité de service (minimal cost: 0x02, reliability: 0x04, throughput: 0x08, low delay: 0x10)
- Identification : identifiant d'un ensemble de fragments pour leur rassemblage
- Flags : DF (Don't Fragment) / MF (More Fragment)
- Fragment Offset : position du fragment dans le message
- Time To Live (TTL) : temps de vie maximal en sec.
- Protocol : protocole de la couche supérieur encapsulé dans le paquet (ICMP, UDP, TCP, etc.)
- Header Checksum : contrôle d'erreurs de l'en-tête
- Adresses IP source et destination

Administration : réseau IP

- Configuration du réseau 192.168.10.0/24
  - Configuration de la machine A (masque de 24 bits)

    $ ifconfig eth0 192.168.10.1 netmask 255.255.255.0
  - De même pour toutes les machines B, C et D
  - On peut ensuite effectuer des tests avec 'ping'

    $ ping 192.168.10.2



Administration : réseau IP

- Configuration du réseau 192.168.10.0/24
  - Configuration des interfaces réseaux de la machine A ?

$ Ifconfig -a

eth0 Link encap:**Ethernet** HWaddr **00:15:c5:3d:52:b6**
inet addr:**192.168.10.1** Bcast:**192.168.10.255** Mask:**255.255.255.0**
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:66 errors:0 dropped:0 overruns:0 frame:0
TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7571 (7.3 KB) TX bytes:9560 (9.3 KB)
Interrupt:18

eth1 Link encap:**Ethernet** HWaddr **00:13:02:dc:2a:fd**
...

lo Link encap:**Local Loopback**
inet addr:**127.0.0.1** Mask:**255.0.0.0**
...

Adresse Ethernet

Adresse IP de la machine

Masque du Réseau IP

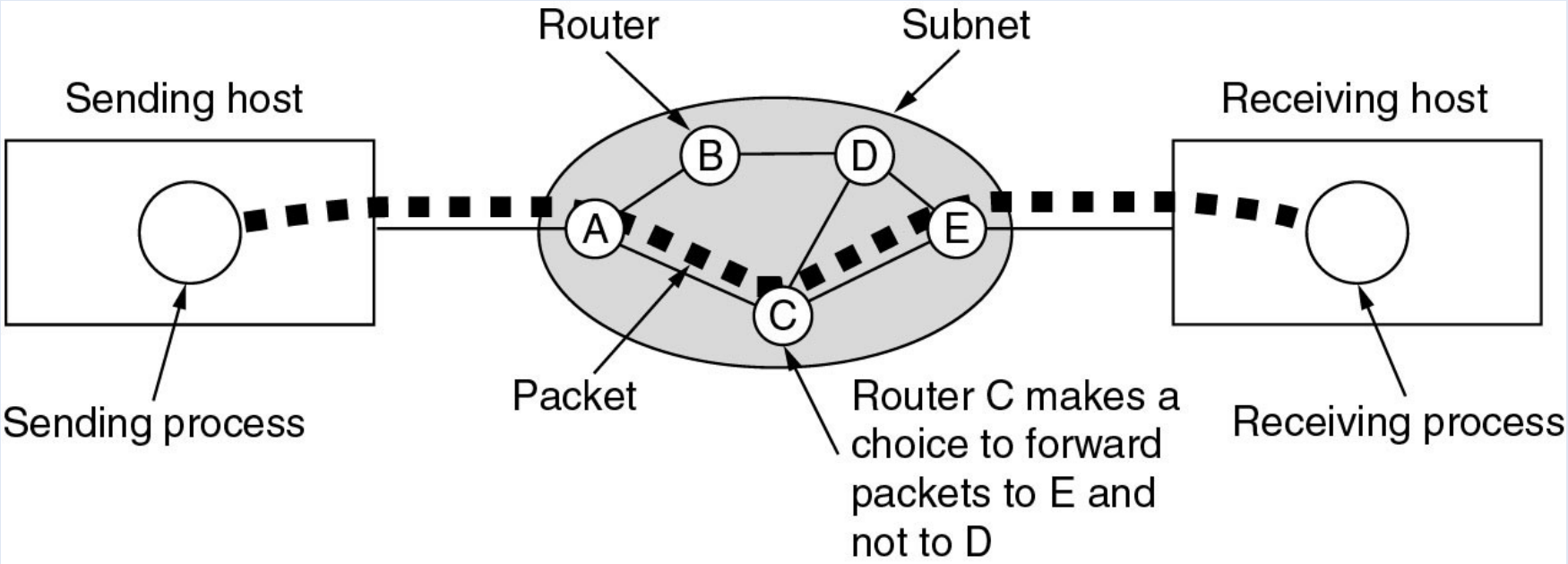
Routage

- Principe
  - Mécanisme par lequel le message d'un expéditeur est acheminé jusqu'à son destinataire, même si aucun des deux ne connaît le chemin complet que le message doit suivre...

- Deux types logiques d'ordinateur dans le WAN
  - les hôtes (hosts) ou stations, qui sont reliés à un seul réseau et qui ont par conséquent une table de routage simple
  - les routeurs/passerelles (gateway), qui relient au moins deux réseaux et possèdent une table de routage plus complexe

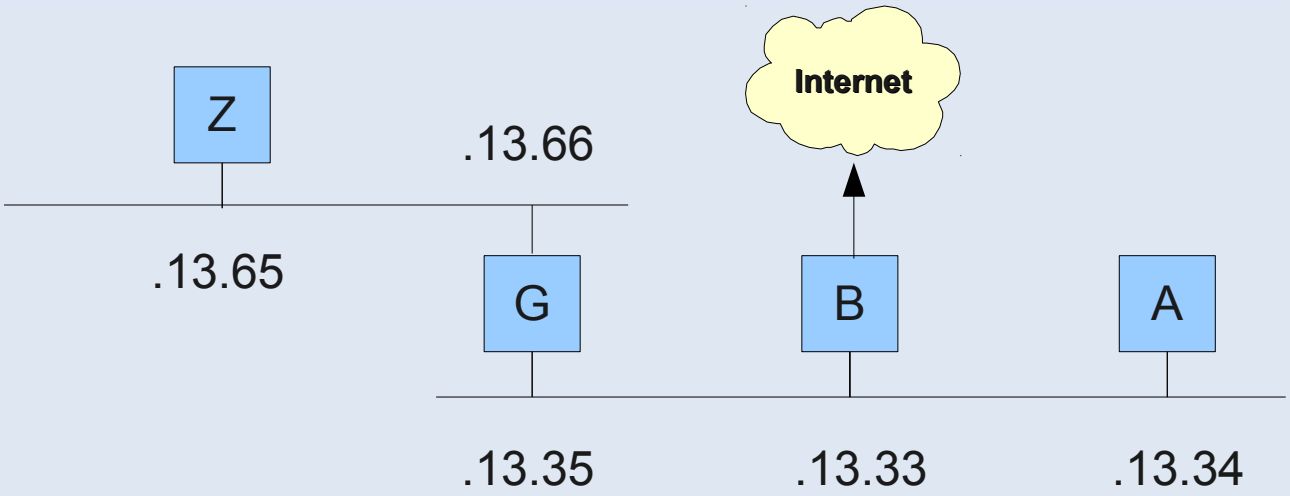
Routage

- Routage statique et dynamique
  - statique (pour les stations)
  - dynamique (pour les routeurs) : adaptation de la table de routage pour optimiser les chemins et réagir aux pannes



Exemple de routage statique

- Routage statique
  - On considère le réseau de classe B d'adresse IP 140.252.0.0. Ce réseau local est composé de deux sous-réseaux d'adresses 140.252.13.32 et 140.252.13.64.



- Exercice 2.3
  - Quel est le masque de chaque sous-réseau et son adresse de broadcast ?

Exemple de routage statique

- Exercice 2.3 (correction)
  - Calcul du masque
    - sous-réseaux 140.252.13.32 et 140.252.13.64
    - on a 32_{10} = 001**0** 0000$_2$ et 64_{10} = 010**0** 0000$_2$
    - donc masque commun de 27 bits (255.255.255.224), car 111**0** 0000$_2$ = 128 + 64 + 32 = 224_{10}
  - Calcul de l'adresse de broadcast (adresse maxi du sous-réseau)
    - @Broadcast(Rx/27) = @Rx AND 0000 ... 000**1** 1111$_2$
    - Il suffit d'ajouter 000**1** 1111$_2$ = 31_{10} à @Rx
    - @Broadcast(140.252.13.32/27) = 140.252.13.63
    - @Broadcast(140.252.13.64/27) = 140.252.13.95

Table de routage

- Principe
  - U : la route est active (Up)
  - G : route indirecte qui passe par un routeur (Gateway)
    - sinon route directe (pas G)
  - H : l'adresse destination est une adresse de machine (Host)
    - sinon l'adresse destination est celle d'un réseau (pas H)

$ route -n

Destination	*Gateway*	*Genmask*	*Flags*	*Interface*
140.252.13.64	140.252.13.35	255.255.255.224	UG	eth0
127.0.0.1	*	0.0.0.0	UH	lo
140.252.13.32	*	255.255.255.224	U	eth0
default	140.252.13.33	0.0.0.0	UG	eth0

- Exercice 2.4
  - Donner la signification de chaque ligne de la table de routage...

Exemple...

- Exercice 2.4 (correction)
  - Ligne 1 : Indique que pour atteindre les machines du réseau 140.252.13.64 (machines G et Z), il faut passer par le routeur G d'adresse 140.252.13.35.
  - Ligne 2 : Indique que pour envoyer un message à soi-même, il suffit d'envoyer ce message à l'adresse 127.0.0.1 (loopback)
  - Ligne 3 : Indique que toutes les machines du réseau 140.252.13.32 (pas de flag H) peuvent être atteintes directement.
  - Ligne 4 : Indique que lorsque l'on ne sait pas comment atteindre une destination (une machine Internet par exemple), il faut envoyer le message au routeur 140.252.13.33 (default).

Algorithme de routage statique

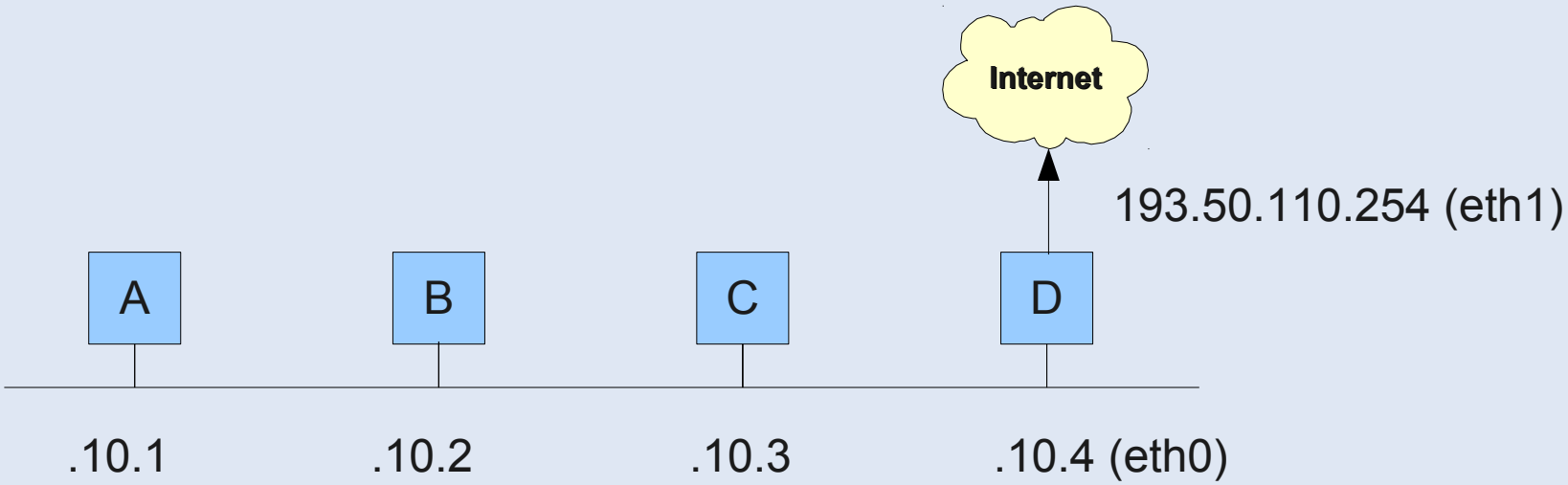
- Principe
  - On regarde les routes “Up” telles que :
    - l'adresse dans la table de routage soit la même que l'adresse destination, si l'adresse dans la table est l'adresse d'une machine (flag H).
    - l'adresse dans la table de routage soit la même que “adresse destination” AND “masque réseau”, si l'adresse dans la table est l'adresse d'un réseau (pas de flag H)
  - Si la route est directe (pas de flag G), le paquet est envoyé directement au destinataire. Sinon, le paquet est envoyé au routeur pour atteindre l'adresse du destinataire.

Administration : routage

- Configuration d'une passerelle D pour le réseau 192.168.10.0/24 permettant d'accéder à Internet
  - Activer la machine comme passerelle (IP Forward)

    $ echo 1 > /proc/sys/net/ipv4/ip_forward
  - Configuration d'une route par défaut vers l'extérieur...

    $ route add default gw 192.168.10.4



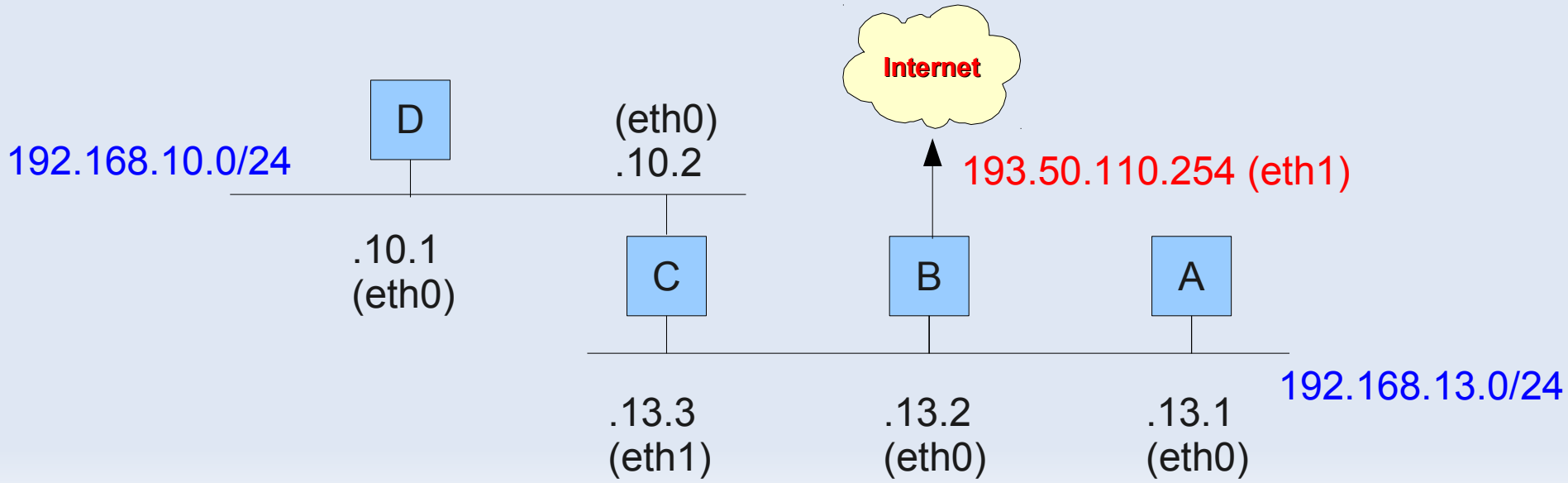
Administration : routage

- Pour les machines de 192.168.10.0/24, C joue le rôle de passerelle par défaut

```
root@D$ route add default gw 192.168.10.2
```

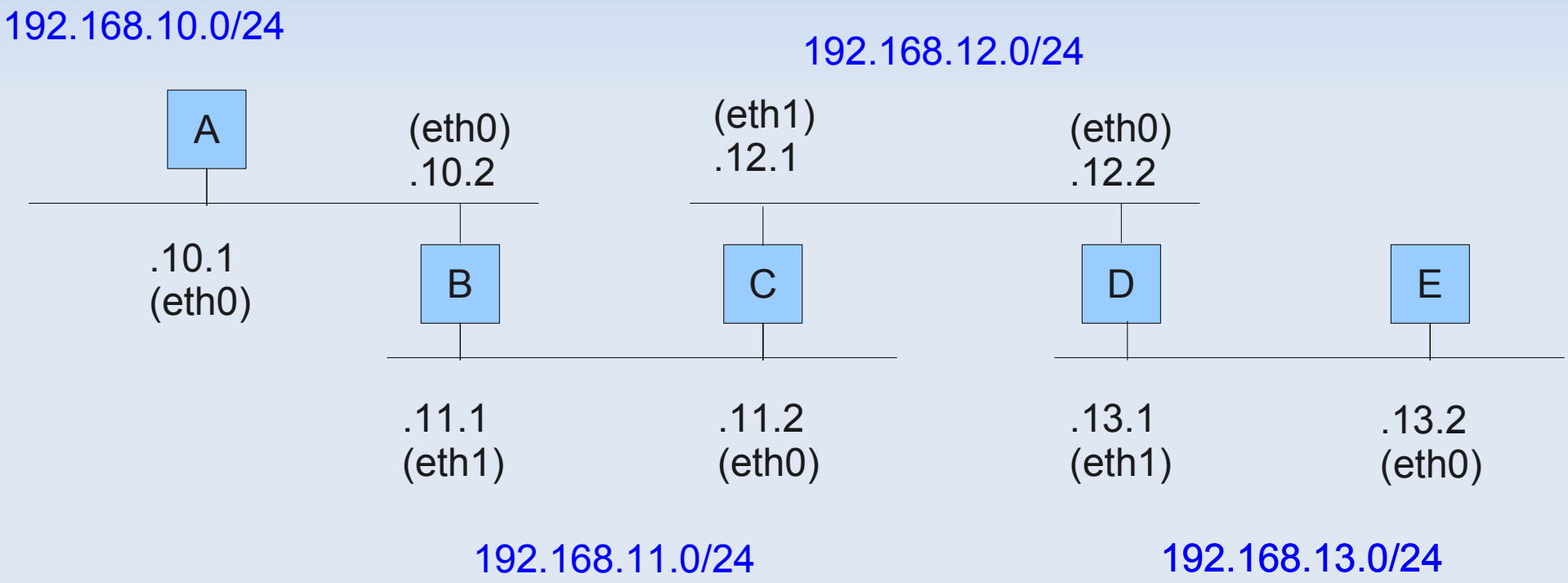
- Pour 192.168.13.0/24, C joue le rôle de passerelle vers 192.168.10.0/24 et B joue le rôle de passerelle par défaut

```
root@A$ route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.13.3
root@A$ route add default gw 192.168.13.2
...
```



Exercice

- Ecrire les règles de routages pour toutes les machines



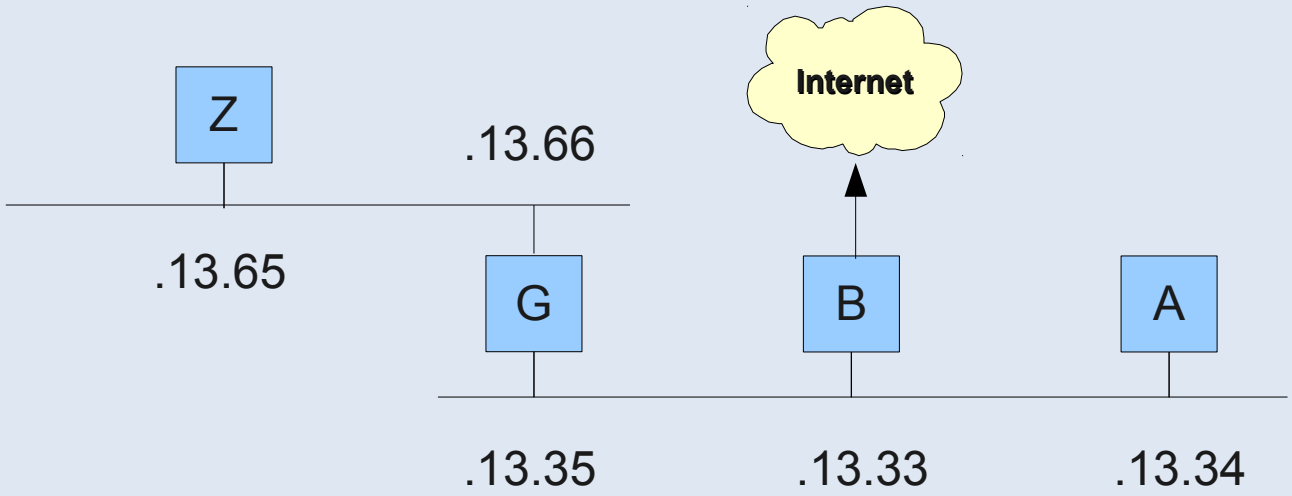
ARP

- Address Resolution Protocol (ARP), RFC 826
  - Récupérer l'adresse Ethernet correspondant à une adresse IP lorsque celle-ci n'est pas connue par une station (broadcast de la requête “arp who has $@IP_{dest}$; answer $@E_{source}$”)
  - Mise à jour du cache ARP dans le kernel de la station
    - association @IP / @E

- Attaque ARP-spoofing
  - L'attaquant X répond à la requête “arp who has $@IP_Y$” par l'adresse $@E_X$ le plus rapidement possible (avant Y) afin de falsifier les caches ARPs des stations sur le réseau...
  - Ainsi l'attaquant X recevra les messages destinés à $@IP_Y$

Routage statique et ARP

- Notation
  - On note @E(@IP) l'adresse Ethernet correspondant à l'adresse Internet @IP.
  - On note ($@E_{source}$,$@E_{dest}$,$@IP_{source}$,$@IP_{dest}$) un paquet IP est émis de *source* vers *dest*.



- Exercice 2.5
  - Représentez avec cette notation la trame envoyée de A vers G.
  - Même chose de A vers Z.

Routage statique et ARP

- Exercice 2.5 (correction)
  - Cas de A vers G
    - récupérer l'adresse Ethernet de G : arp “who has $@IP_G$”, réponse “$@E(@IP_G)$”
    - envoi de la trame : “$@E(@IP_A),@E(@IP_G),@IP_A,@IP_G$”
  - Cas de A vers Z (route indirecte par G)
    - pas besoin de récupérer l'adresse Ethernet de G, déjà dans la cache ARP
    - envoi de la trame : “$@E(@IP_A),@E(@IP_G),@IP_A,@IP_Z$”
    - mise à jour de la trame par le routeur (sans toucher au paquet IP) : “$@E(@IP_G),@E(@IP_Z),@IP_A,@IP_Z$”

ICMP

- Internet Control Message Protocol (ICMP), RFC 792
  - accompagne IP pour gérer les erreurs et propager des informations de routage

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

  - Exemple du ping : envoi d'une requête ICMP '*echo request*' et attente de la réponse '*echo reply*'

Cours 3

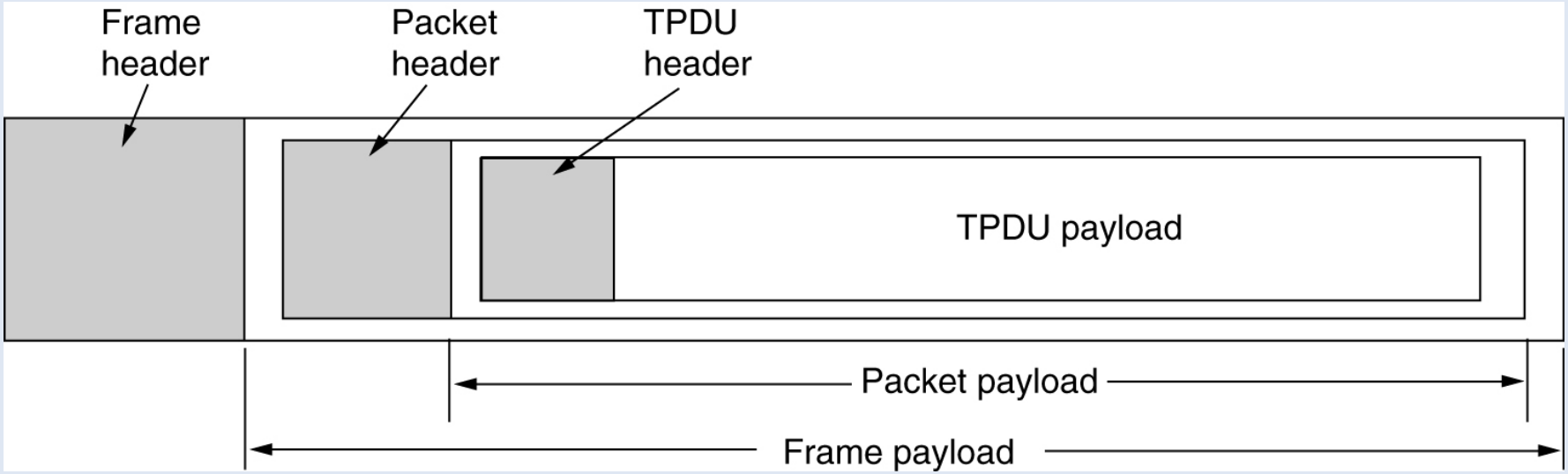
Couche Transport
(TCP, UDP)

Introduction

- La couche réseau (IP)
  - Communication de bout-en-bout ntre machines
  - Transfert de paquet en “best-effort” (non fiable)
- La couche transport
  - TCP : communication de bout-en-bout entre processus, orienté connexion et fiable
  - UDP

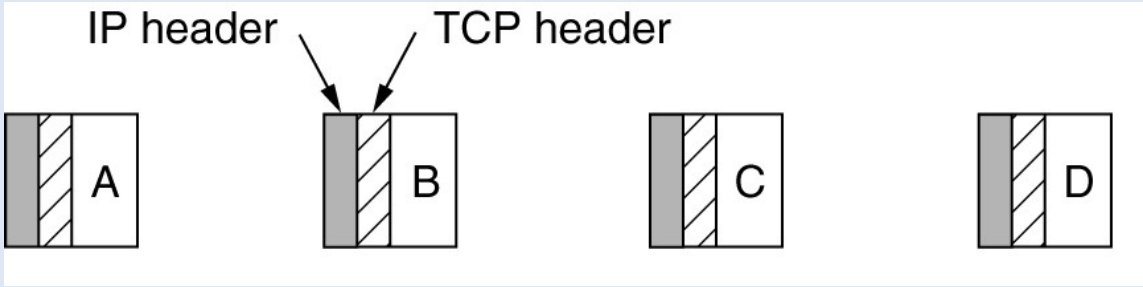
TCP

- Transmission Control Protocol (TCP)
  - service en mode connecté
  - connexion bidirectionnelle et point-à-point
    - (IP_{source} ; $Port_{source}$; $IP_{destination}$; $Port_{destination}$)
  - le numéro de port désigne un processus et un seul

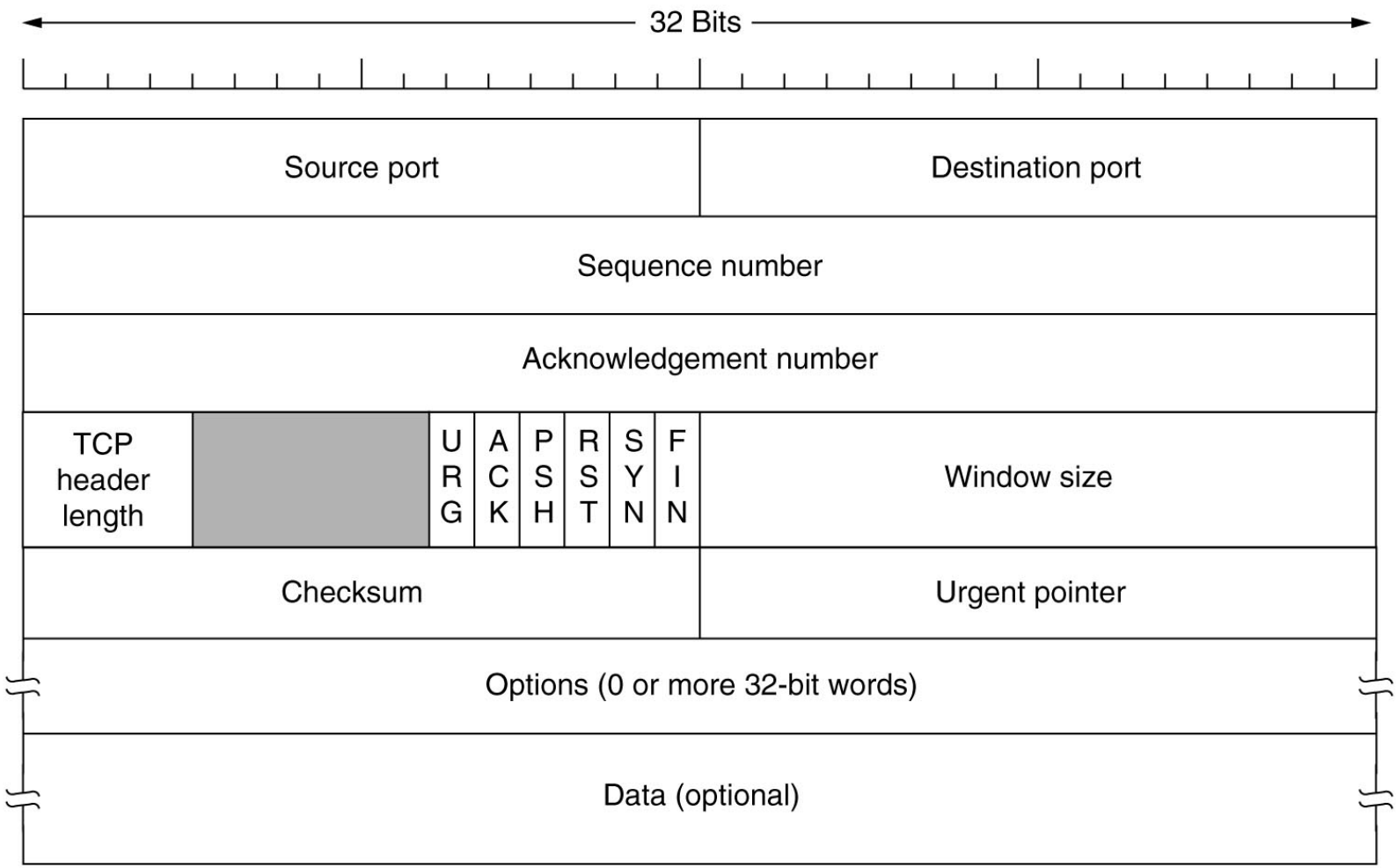


TCP

- MTU (Maximum Transfert Unit)
  - Taille maximale des paquets IP (1500 octets sur Ethernet)
- Fragmentation des messages en plusieurs segments
  - Numérotation des segments composant le message
- Exemple de fragmentation en 4 segments du message ABCD



En-tête TCP

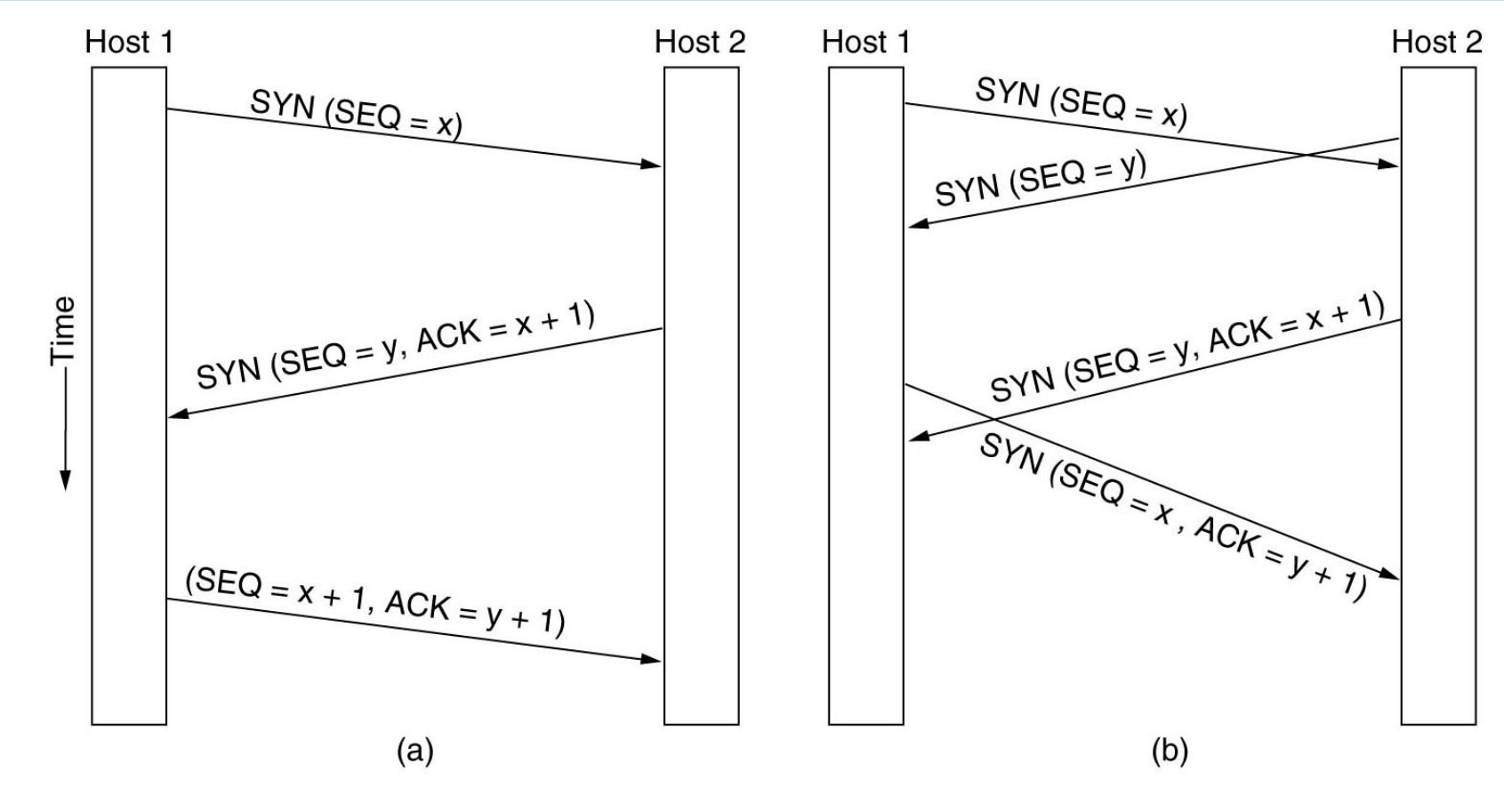

32 Bits
Source port
Destination port
Sequence number
Acknowledgement number
TCP header length
URG
ACK
PSH
RST
SYN
FIN
Window size
Checksum
Urgent pointer
Options (0 or more 32-bit words)
Data (optional)

En-tête TCP

- Source Port et Destination Port
- Numéro de séquence : le numéro du segment TCP
- Numéro d'accusé de réception : numéro du prochain octet attendu
- 6 flags binaires :
  - ACK : indique si le numéro d'accusé de réception est valide
  - SYN : demande d'établissement d'une connexion
  - FIN : libération de la connexion
  - RST : réinitialisation d'une connexion (reset) ; rejet d'une connexion
  - Autres : PSH, URG
- Window size : nombre d'octets souhaités pour la réception ; si 0, stoppe temporairement la transmission

Connexion TCP

- La “poignée de main” en 3 étapes
  - Synchronisation des numéros de séquence



Connexion standard

Connexion simultanée

TCP

- Les états d'une connexion TCP

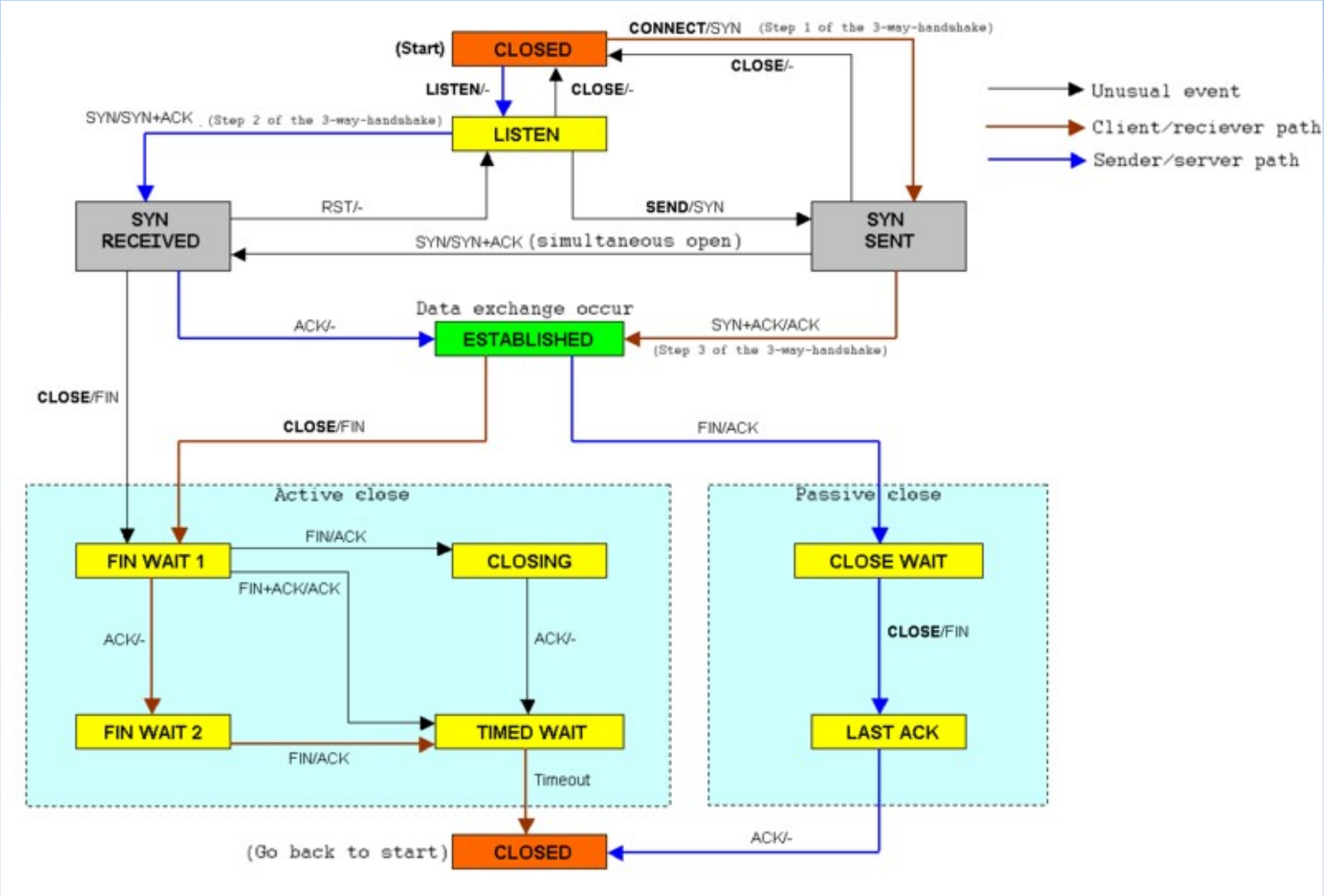
State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

Netstat

- netsat -tnap (liste des connexions TCP/IP)

Proto	R-Q	S-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:2208	*:*	LISTEN	3266/hpiod
tcp	0	0	127.0.0.1:34818	*:*	LISTEN	3275/python
tcp	0	0	127.0.0.1:3306	*:*	LISTEN	3642/mysqld
tcp	0	0	0.0.0.0:25	*:*	LISTEN	3525/exim4
tcp	0	0	82.225.96.37:35551	147.210.8.143:993	ESTABLISHED	10503/mozilla
tcp	0	0	82.225.96.37:39243	147.210.13.65:22	ESTABLISHED	13758/ssh
tcp	0	0	82.225.96.37:35750	147.210.9.15:22	ESTABLISHED	13763/ssh
tcp6	0	0	*:80	*:*	LISTEN	3979/apache2
tcp6	0	0	*:22	*:*	LISTEN	3746/sshd
tcp6	0	0	*:25	*:*	LISTEN	3525/exim4

TCP



E/M →

Lorsque l'evènement E se produit, envoyé le message M ou ne rien faire si M='-'.

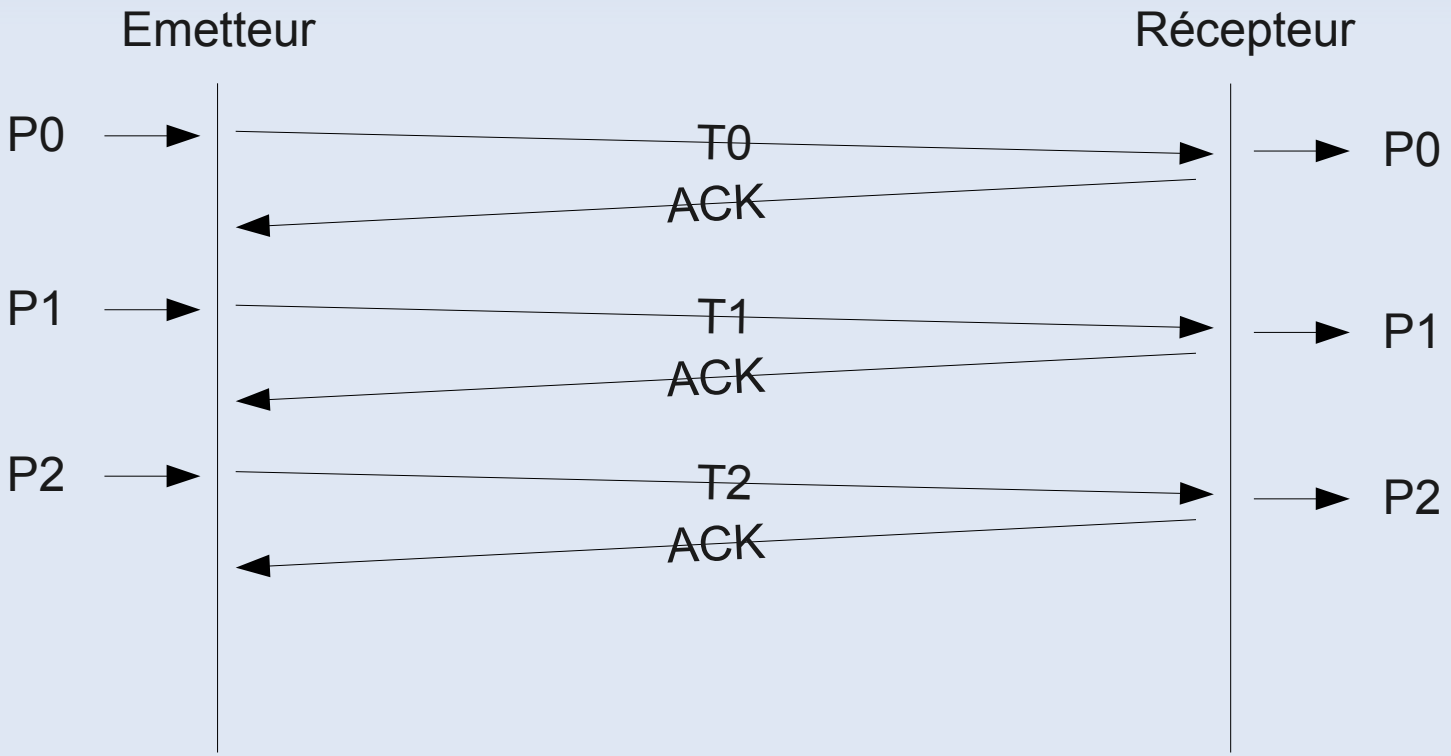
TCP

- Exemples de service TCP standards (ports < 1024)

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

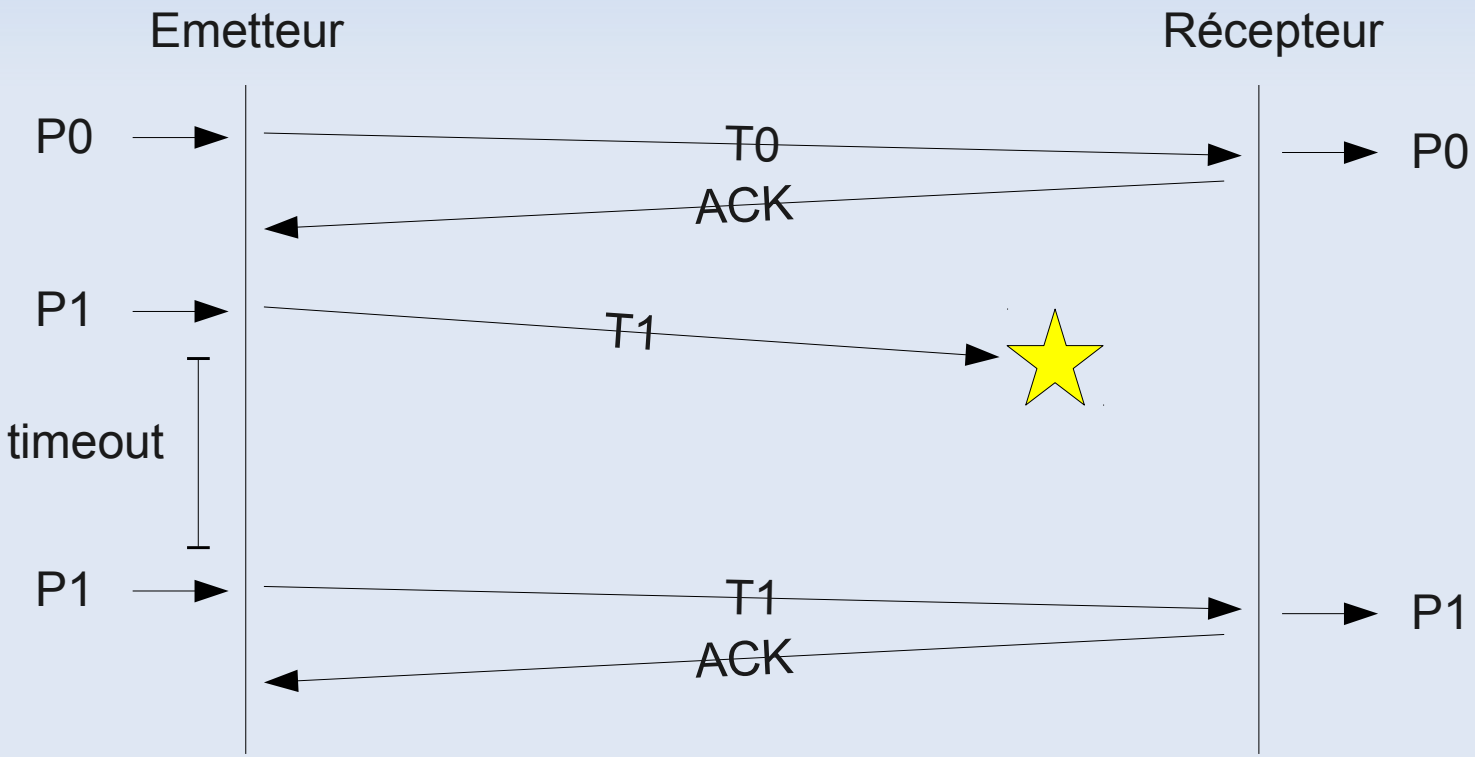
Contrôle de flux

- Protocole n° 1 (“envoyer et attendre”)
  - L'emetteur envoie une trame et attend que le récepteur ait eu le temps de la traiter avant d'envoyer la suivante...



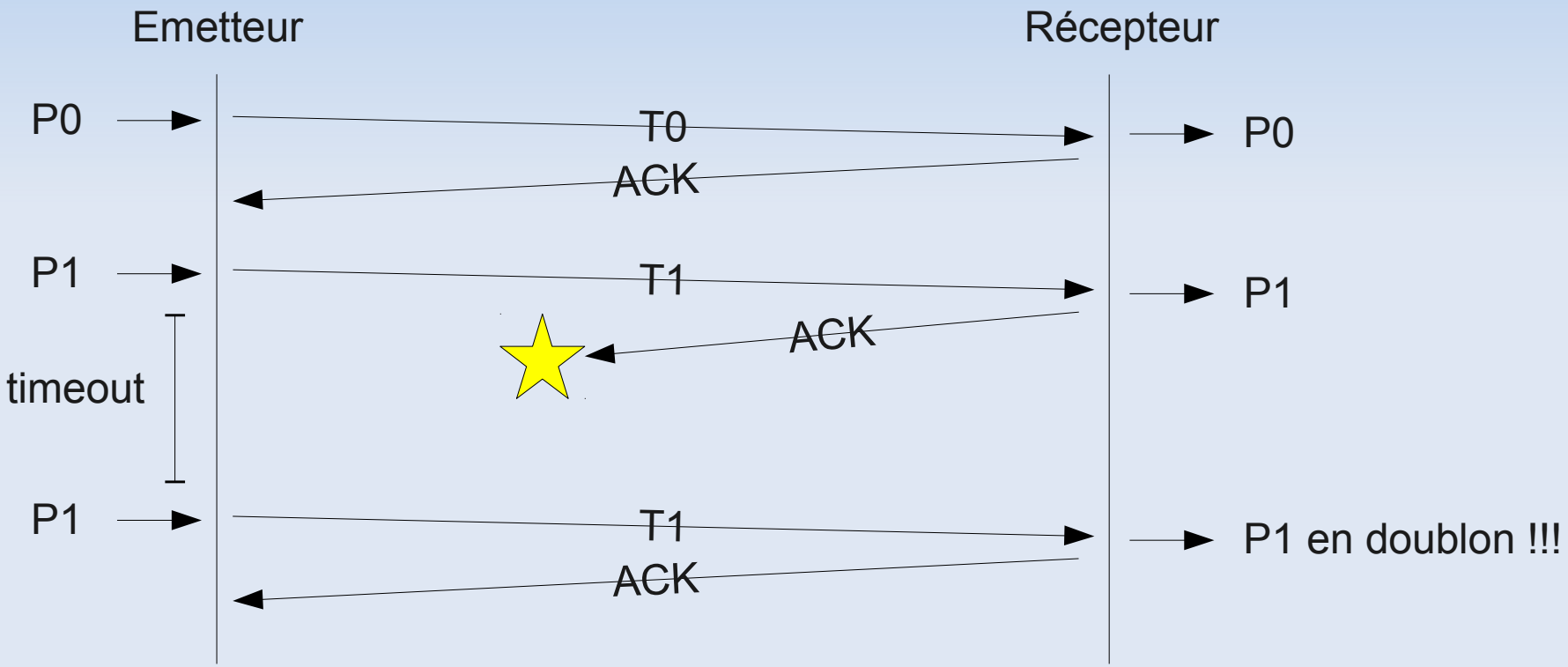
Contrôle de flux

- Si l'emetteur ne reçoit pas un acquitement passé un certain délai (timeout), il considère la trame perdue et décide de la renvoyer.



Contrôle de flux

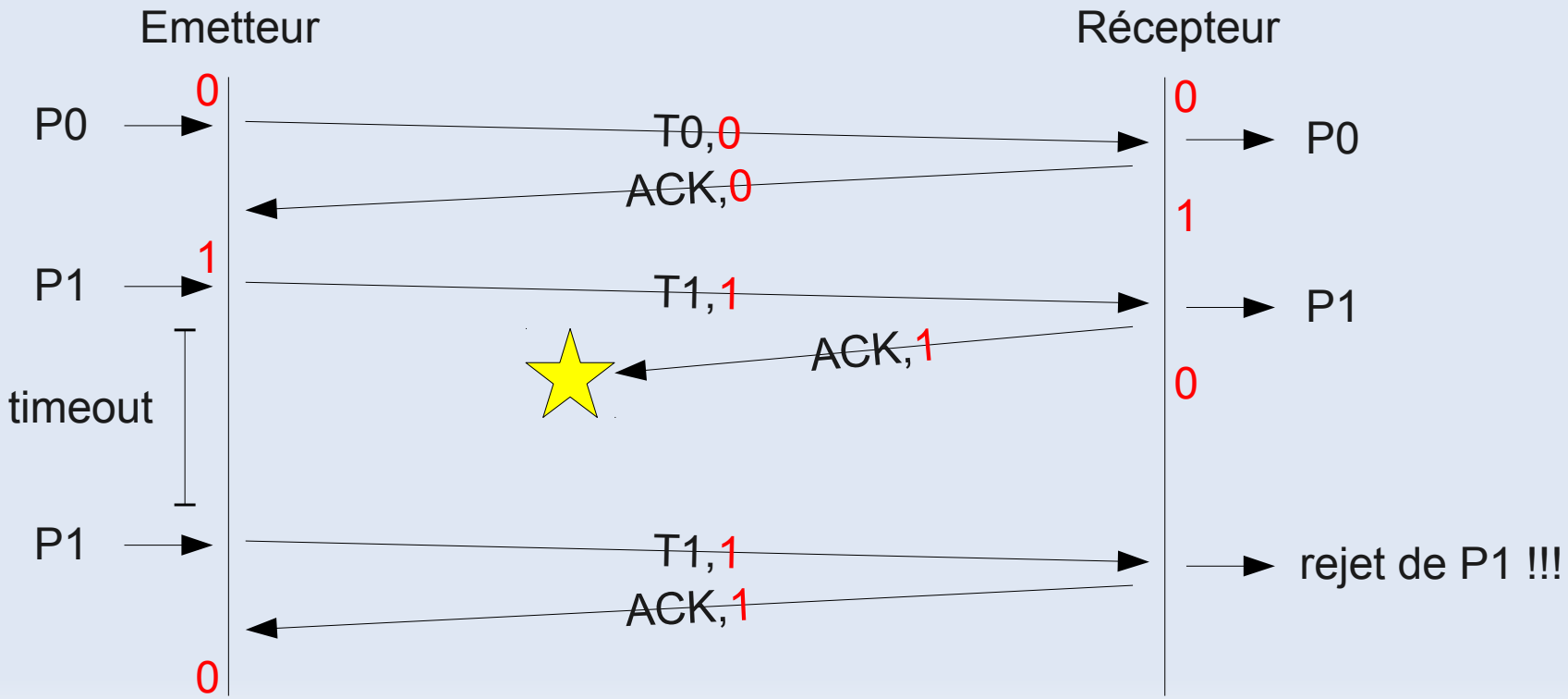
- Le problème des doublons !!!



- Autres problèmes lié au réglage de la durée du timeout...
  - si timeout trop court, pas le temps de recevoir les acks
  - si timeout trop grand, inefficacité en cas d'erreurs

Contrôle de flux

- Protocole n° 2 du “bit alterné”
  - Numérotation des trames et des acquittements sur 1 bit (0,1)
  - Le récepteur rejette les trames qui ne correspondent pas au numéro attendu !



Contrôle de flux

- Taux d'utilisation
  - capacité du canal : D bit/s ; taille des trames : S bits ; délai de propagation : τ
  - on envoie pendant S/D et on attend ensuite pendant 2τ
  - taux d'utilisation = $T_{emission}$ / T_{total} = S/(S+2τD)

- Exercice 3.1 sur le protocole “envoyer et attendre”
  - Considérons un canal satellite à 50 kbit/s avec un délai de propagation $\tau = 250$ ms avec des trames de 1000 bits.
  - A t = 0, on effectue l'envoi d'une trame. A quelle date t' pourra-t-on envoyer une nouvelle trame ? Quel est le taux d'utilisation du canal de transmission ?

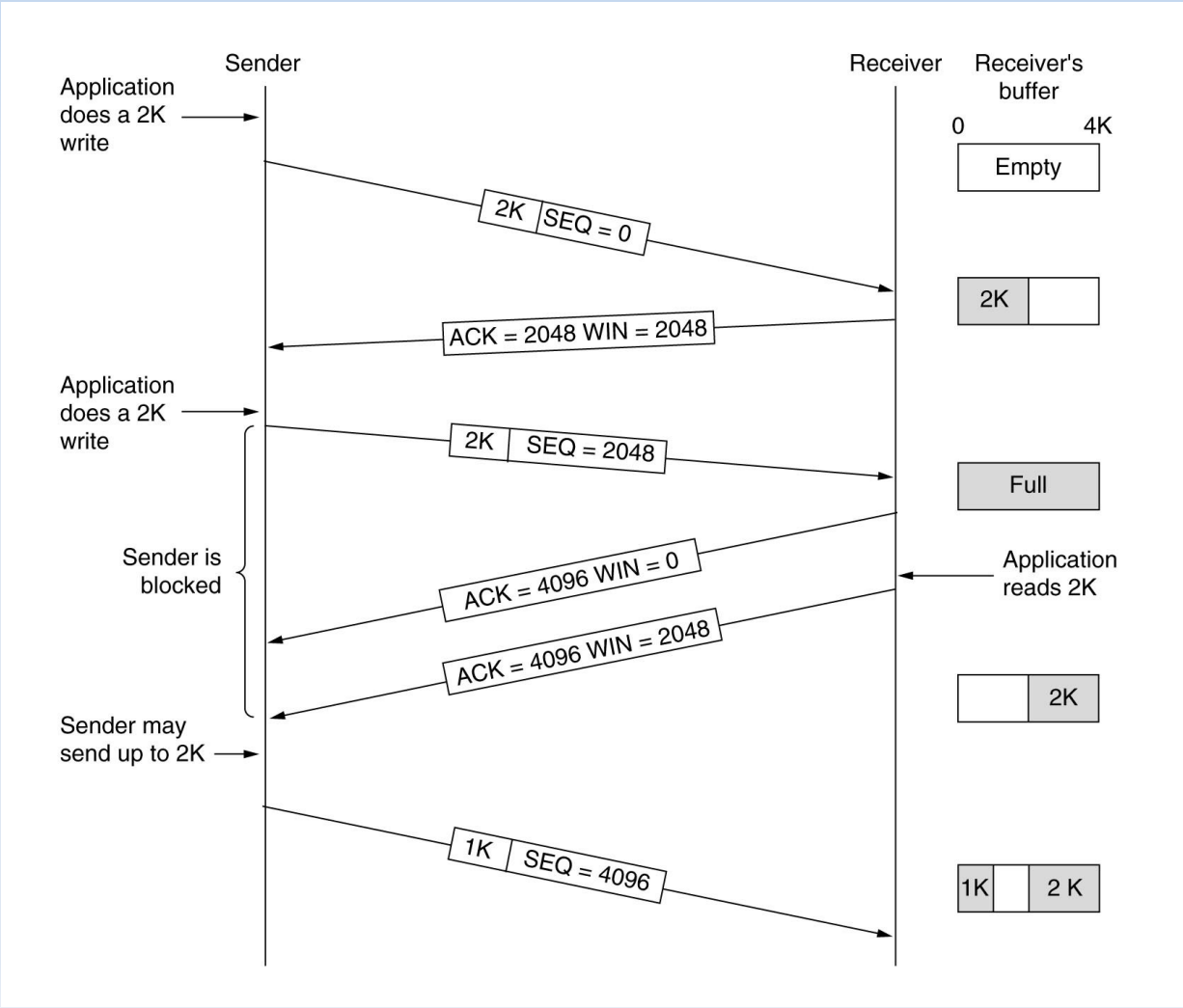
Contrôle de flux

- Exercice 3.1 (correction)
  - L'envoi d'une trame à $t = 0$ met 20 ms (1000 bits / 50 kbit/s).
  - L'envoi d'une nouvelle trame commence immédiatement après la réception de l'acquitement précédent (supposé de petite taille), soit à la date $t' = 520$ ms.
  - Le taux d'utilisation est de 20/520, soit 4%. En effet, l'émetteur reste bloqué durant 500/520, soit 96% du temps.

- Conclusion
  - Le protocole précédent est fiable mais ne permet pas d'atteindre des débits élevés !

TCP

- Gestion de fenêtre sous TCP



Administration : firewall

- Configurer le firewall avec iptables...
  - Lister les règles

    $ iptables -t filter -L - v

  - Ajouter une nouvelle règle

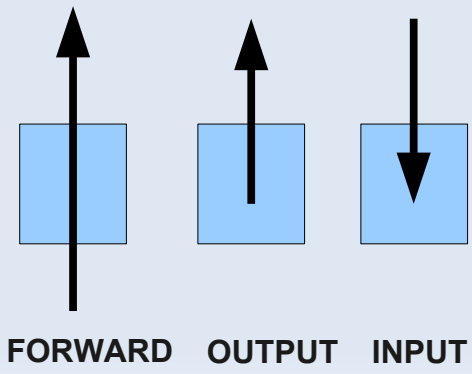
    $ iptables -t filter -A <CHAIN> <SRC> <DST> <...> -j <ACTION>

  - Politique par défaut (si aucune règle ne s'applique avant)

    $ iptables -t filter -P <CHAIN> <ACTION> # <ACTION> = ACCEPT | DROP

  - Memento

    <CHAIN> = FORWARD | INPUT | OUTPUT
    <ACTION> = ACCEPT | REJECT | DROP
    <SRC> = -i eth0 | -s 192.168.0.1 | -s 192.168.0.0/24
    <DST> = -o eth0 | -d 192.168.0.1 | -d 192.168.0.0/24
    <...> = -p icmp | -p tcp –dport 80 | -m state –state <STATE>
    <STATE> = NEW | ESTABLISHED
    * NEW : établissement d'une nouvelle connexion
    * ESTABLISED : une connexion déjà établie



Administration : firewall

- Protéger une machine connectée directement sur Internet...
  - On configure le firewall de A pour les chains INPUT / OUPUT
- Exemple
  - On interdit tout par défaut...

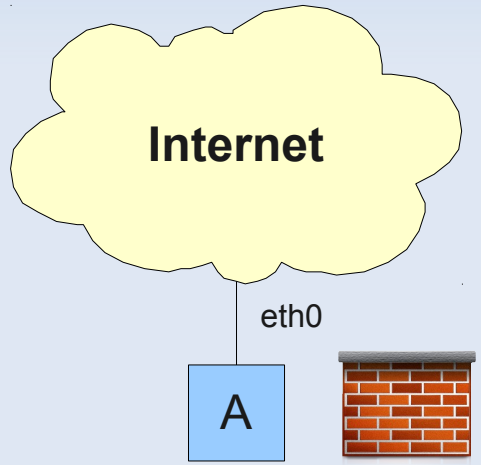
```
$ iptables -t filter -P INPUT DROP
$ iptables -t filter -P OUTPUT DROP
```

  - On autorise le ping !

```
$ iptables -t filter -A INPUT -p icmp -j ACCEPT
$ iptables -t filter -A OUTPUT -p icmp -j ACCEPT
```

  - On autorise uniquement l'accès de A au web...

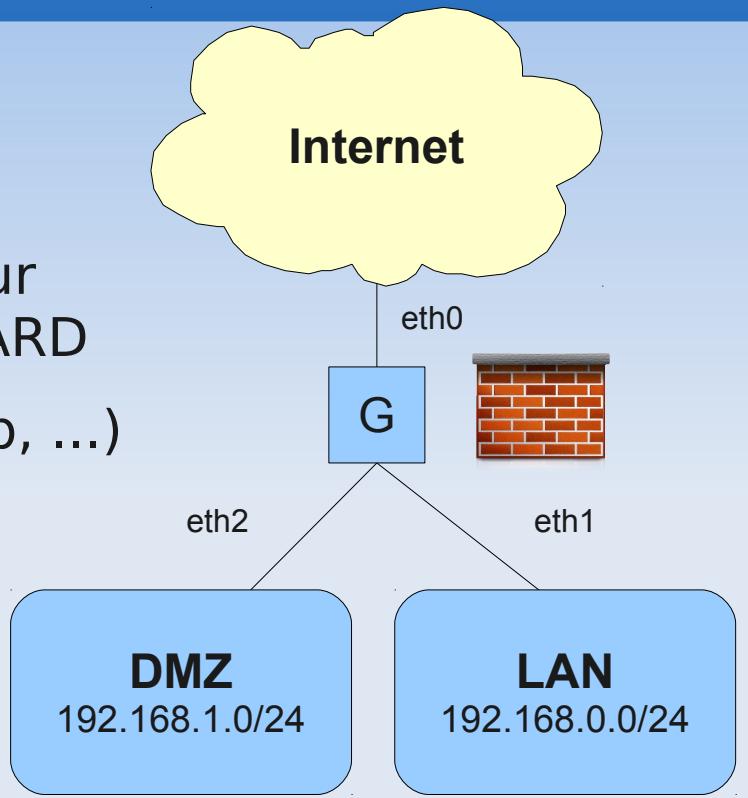
```
$ iptables -t filter -A OUTPUT -p tcp –dport 80 -j ACCEPT
$ iptables -t filter -A INPUT -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT
```



Administration : firewall

- Protéger un réseau...
  - On configure le firewall uniquement sur la passerelle G pour la chain FORWARD
  - On déporte les services sensibles (web, ...) dans un sous-réseaux, appelé DMZ
- Exemple
  - On interdit tout par défaut

    $ iptables -t filter -P FORWARD DROP



  - On autorise l'accès aux serveurs web dans la DMZ

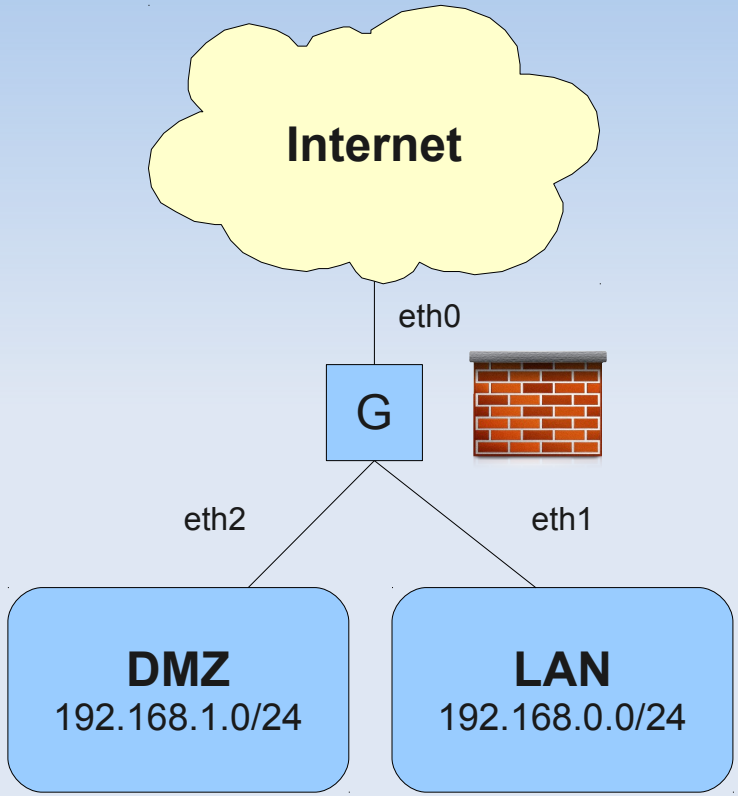
    $ iptables -t filter -A FORWARD -d 192.168.1.0/24 -p tcp –dport 80 -j ACCEPT
    $ iptables -t filter -A FORWARD -s 192.168.1.0/24 -p tcp –sport 80
    -m state –state ESTABLISHED -j ACCEPT

  - On autorise tout le traffic sortant du LAN (et le retour...)

    $ iptables -t filter -A FORWARD -s 192.168.0.0/24 -j ACCEPT
    $ iptables -t filter -A FORWARD -d 192.168.0.0/24 -m state –state ESTABLISHED -j ACCEPT

Administration : firewall

- Exercice

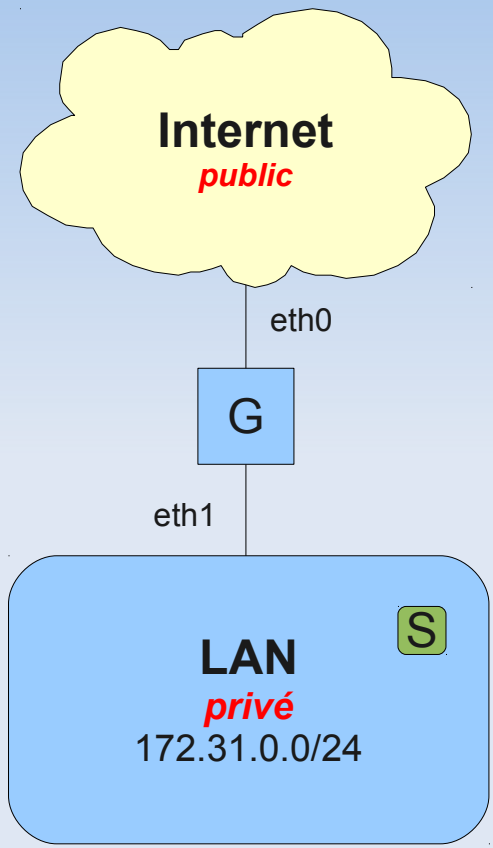


Administration : NAT

- NAT (Network Address Translation)
  - Un réseau privé ne peut pas accéder et n'est pas accessible depuis Internet (adresses IP non routables)
  - Mais possibilité d'utiliser une passerelle NAT !
- Exemples
  - Exemple de masquage des IPs du LAN : les machines du LAN peuvent communiquer avec Internet en empruntant l'adresse publique de G

    root@G$ iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
  - Exemple de Port-Forwarding de G:80 vers S:80 : le serveur web S (port 80) est ainsi accessible depuis l'extérieur

    root@G$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to <S>:80



Cours 4

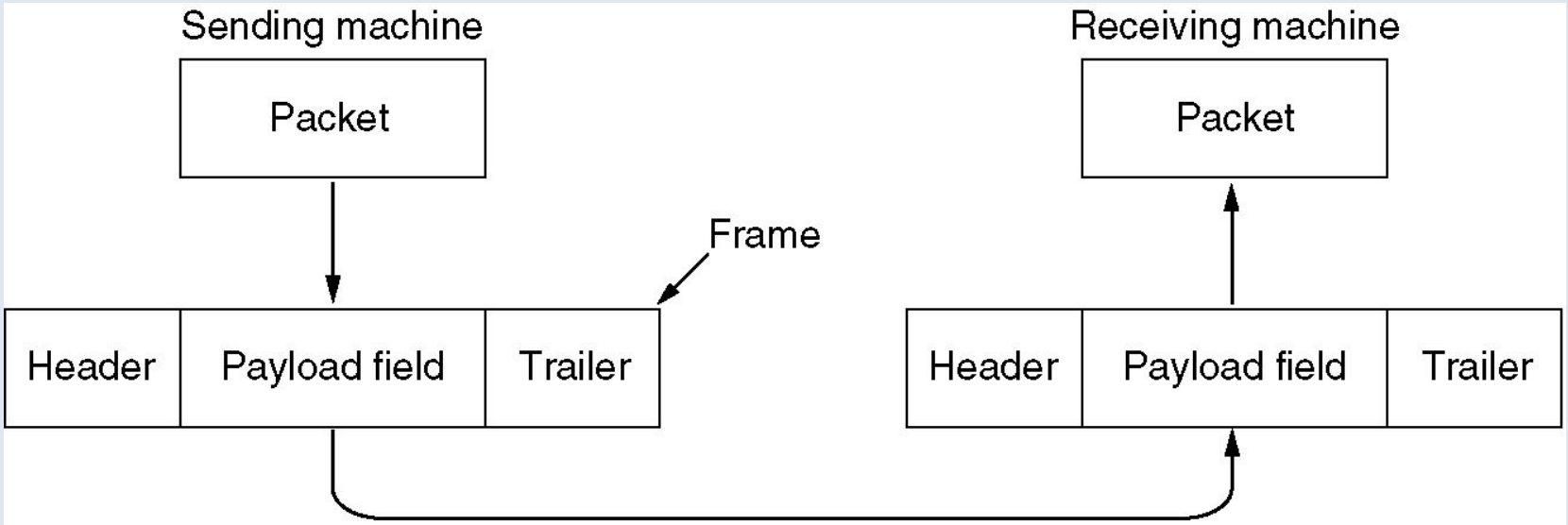
Couche Liaison de Données (Ethernet)

Introduction

- La couche liaison de données
  - Le rôle de la couche liaison est de fournir à la couche réseau une transmission fiable en s'appuyant sur des supports de transmission qui ne sont pas parfaits !
- Plan
  - Notion de Trame
  - Contrôle d'erreurs (parité, Hamming, CRC)
  - Ethernet et CSMA/CD
  - Switch, Hub
  - Autres exemples de protocoles (PPP, ATM, ...)

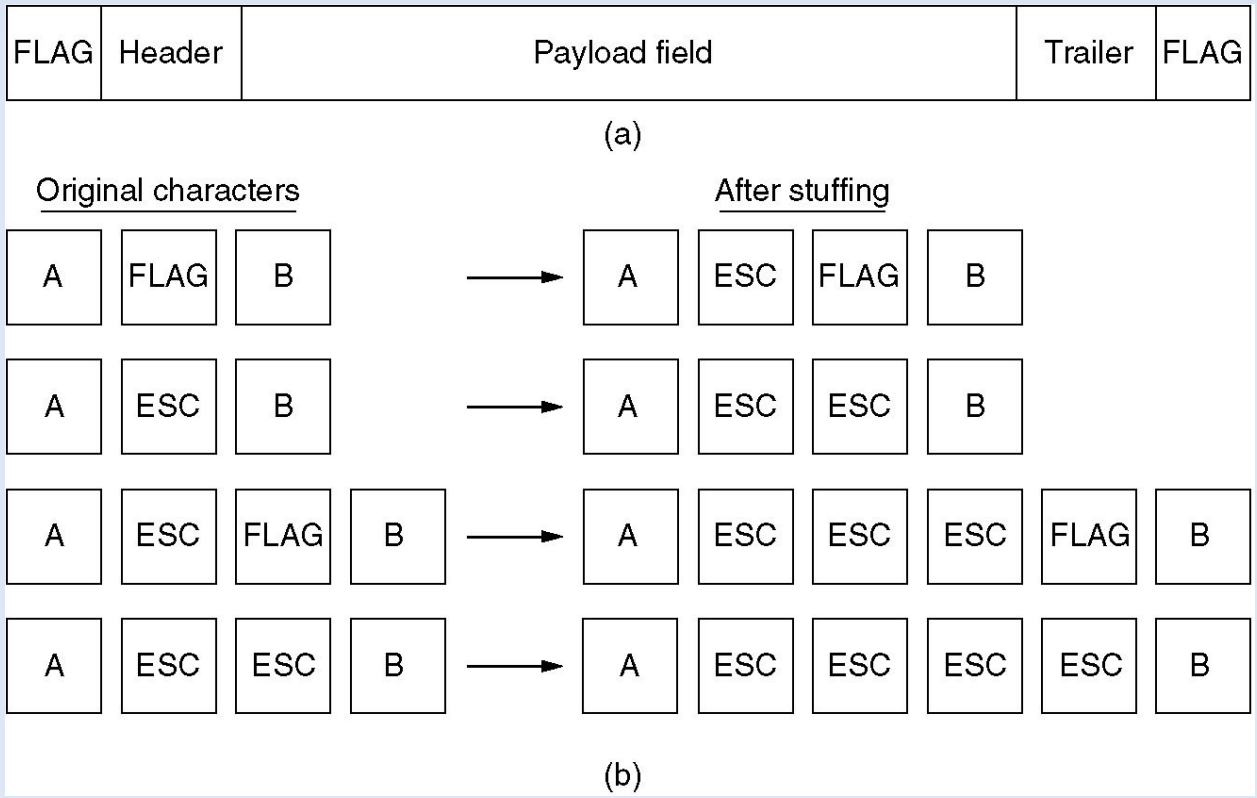
Notion de trame

- Composition d'une trame (*frame*)
  - en-tête (*header*)
  - paquet fourni par la couche supérieure (la couche réseau)
  - en-queue (*trailer*)



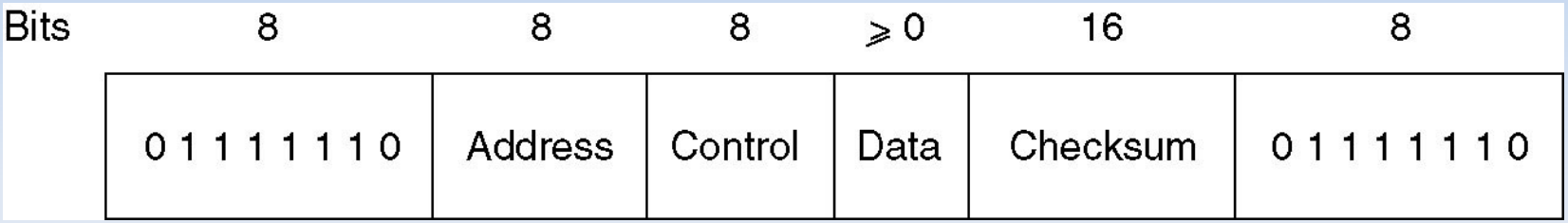
Trames

- Délimitation des trames (flag)
  - utilisation d'un caractère d'échappement (esc) si les caractères flag ou esc apparaissent dans le message initial

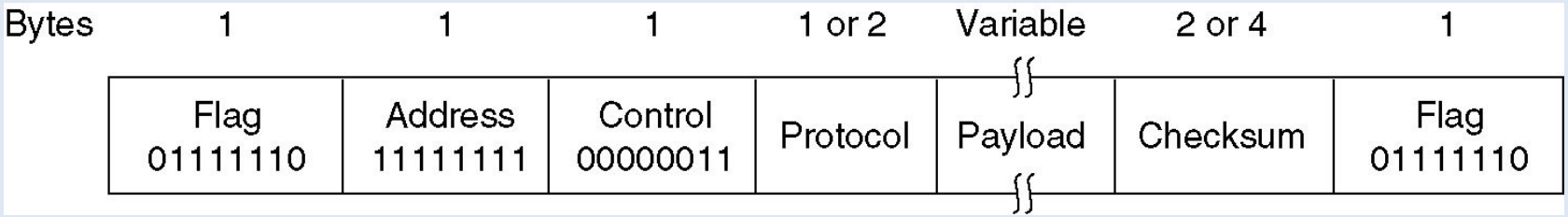


Format des trames

- Exemple HDLC

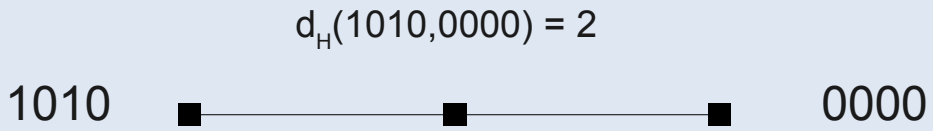


- Exemple du protocole PPP



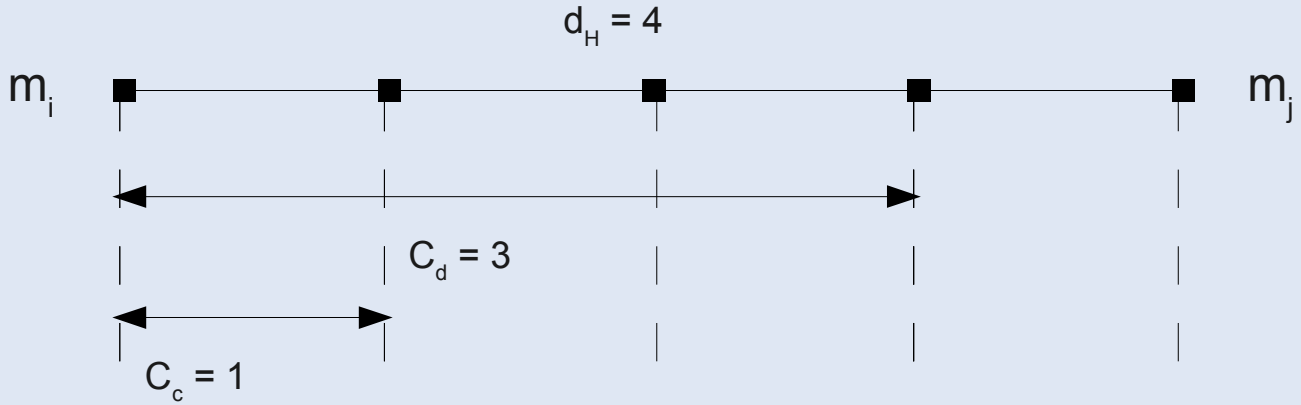
Contrôle d'erreurs

- Etant donné un code C = {m_0,m_1,m_2, ...} avec m_i un mot binaire du code de longueur noté $|m_i|$
- Distance de Hamming entre deux mots m_i et m_j
  - $d_H(m_i,m_j)$ = nombre de bits qui différent entre m_i et m_j
- Distance de Hamming du code C
  - $d_H(C)$ = min des distances de Hamming entre les mots du code
  - Tous les mots du code sont au moins à une distance $d_H(C)$
- Exemple



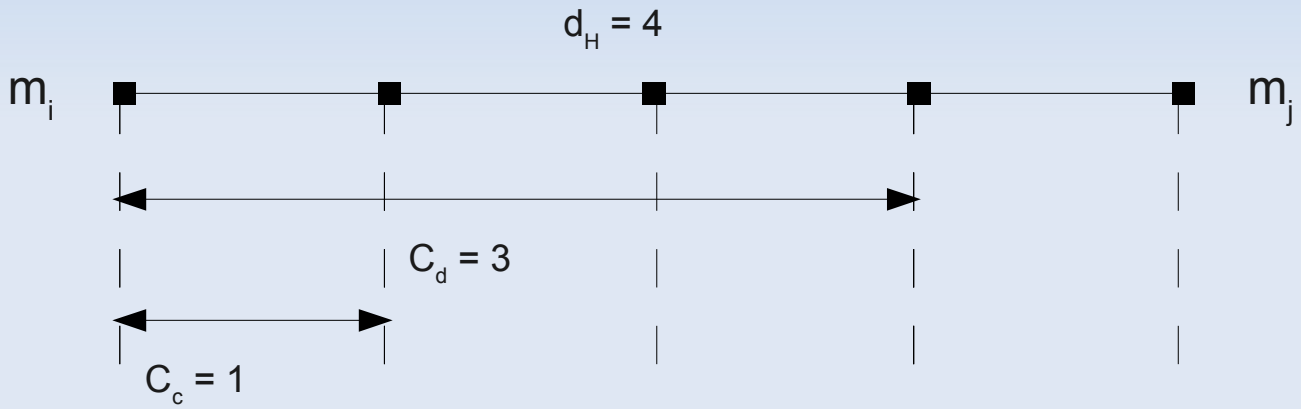
Contrôle d'erreurs

- Capacité de détection d'un code C
  - nombre maximum d'erreurs pouvant être détectés
  - $C_d(C) = d_H(C) - 1$
- Capacité de correction d'un code C
  - nombre maximum d'erreurs pouvant être corrigés
  - $C_c(C) = d_H(C) / 2 - 1$ si pair ; $(d_H(C) - 1) / 2$ sinon
- Exemple d'un code C avec $d_H = 4$



Contrôle d'erreurs

- Exemple d'un code C avec $d_H = 4$
- Transmission de m_i



- En cas d'erreurs de transmission, plusieurs bits ont pu changer...
  - si 1 bit d'erreur, détection et correction
  - si 2 ou 3 bits d'erreur, détection sans correction
  - si 4 bits d'erreur, reconnaissance d'un autre mot !!!

Contrôle d'erreurs

- Exercice 4.1 (code barre postal)
  - Quel est le code postal suivant ?

    I.I.II - ..IIII- I..III - .III.I - .III.I
  - Réponse 33405
  - Quel est la distance de Hamming de ce code ?
  - Combien d'erreurs peut-on détecter et corriger ?

(0) . . I I I I

(1) . I . I I I

(2) . I I . I I

(3) . I I I . I

(4) I . . I I I

(5) I . I . I I

(6) I . I I . I

(7) I I . . I I

(8) I I . I . I

(9) I I I . . I

Lecture de droite à gauche.

Bit de parité

- Principe
  - Considérons un mot binaire $m=(m_1,m_2,m_3,...,m_n)$ de taille *n*
  - Ajout à la fin de m du bit m_{n+1} tel que la somme de tous les bits du mot soit paire
- Exemple
  - m = 0101001 et m' = 01010011

Code de Hamming (m,n)

- Considérons un mot binaire de données de taille n

$$d=(d_1,d_2,d_3,...,d_n)$$

- Insertion dans d de k bits de contrôle p_i aux positions

2^0, 2^1, 2^2, 2^3, ... c'est-à-dire 1, 2, 4, 8, ...

- Soit s le mot à transmettre de taille m=n+k

$$s = (s_1,s_2,s_3,...,s_j,..., s_{n+k}) = (p_1,p_2,d_1,p_3,d_2,d_3,...,p_i,...,d_n)$$

- Le nombre de bits de contrôle est le premier entier k supérieur à $\log_2(m)$. Ex. : $\log_2(11) < 4$ donc k=4 et n=7

Code de Hamming

- Calcul des bits de contrôle
  - Le bit de donnée s_j est contrôlé par les bits dont les positions sont les coefficients de la décomposition binaire de j.
  - Le bit de contrôle p_i (en position i) est choisi de telle sorte que la somme des bits qu'il contrôle (ainsi que lui-même) fasse 0 modulo 2 (contrôle de parité).
- Détection et correction d'erreur
  - à la réception d'un message, on effectue le contrôle de parité sur le bits de contrôle
  - si p_a et p_b sont faux, alors il y a une erreur sur le bit s_{a+b} qui peut être corrigée !
  - Capacité de détection et de correction d'une seule erreur !

Exemple

- Exemple de calcul des bits de parités dans le code de Hamming (11,7)

	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	d_7
Data word (without parity):			**0**		**1**	**1**	**0**		**1**	**0**	**1**
p_1	**1**		0		1		0		1		1
p_2		**0**	0			1	0			0	1
p_3				**0**	1	1	0				
p_4								**0**	1	0	1
Data word (with parity):	**1**	**0**	0	**0**	1	1	0	**0**	1	0	1

Calculation of Hamming code parity bits

Exercice

- Exercice 4.2 : Code de Hamming (11,7)
  - Quels sont les bits qui contrôlent s_{11} ?
  - Quels sont les bits contrôlés par p_1, par p_4 ?
  - Calculer le code de Hamming du mot 1101011 ?
  - Quel est le message correspondant au code 11111011100 ?
    - Y-a-til une erreur ? Si oui, corriger cette erreur !

Code de Hamming

- Correction
  - le bit $s_{11} = d_7$ est contrôlé par p_1, p_2 et p_8 (11 = 1 + 2 + 8)
  - p_1 contrôle $s_3+s_5+s_7+s_9+s_{11}$; p_4 contrôle $s_8+s_9+s_{10}+s_{11}$
  - d = 1101011 ; s = p_1.p_2.1.$p_3$1.0.1.p_4.0.1.1 = 00101010011
  - s' = 11111011100 (après réception)
    - p_1 faux, p_2 faux, p_3 faux et p_4 ok
    - erreur sur le bit d'indice 1+2+4=7
    - s = 11111001100 (après correction)
    - d = 1100100 (mot reçu)

CRC

- CRC (Cyclic Redundancy Check)
  - Calcul d'un checksum basé sur l'arithmétique polynomiale modulo 2
  - On considère le mot binaire suivant de taille *n*

$$b=(b_{n-1},b_{n-2},...,b_1,b_0)$$

  - Ce mot s'exprime sous la forme d'un polynôme de degrés n-1, à coefficient binaire :

$$B(X)=b_{n-1}.X^{n-1} + b_{n-2}.X^{n-2} + ... + b_1.X + b_0$$

  - La clé C(X) associée à un tel mot est définie comme étant le reste de la division de $B(X).X^k$ par un polynôme générateur G(X) de degré k.
  - Le mot à transmettre est alors $M(X) = B(X).X^k + C(X)$.

CRC

- Exemple d'utilisation des CRCs
  - CRC-1 (bit de parité) : $G(X) = X + 1$
  - CRC-8 (ATM) : $G(X) = X^8 + X^2 + X + 1$
  - CRC-16 (USB, PPP, Bluetooth, ...)
  - CRC-32 (Ethernet) : $G(X) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$
  - CRC-160 (MD5 checksum)

Exemple

- Quel est la clé associée au mot 110111 avec G(X) = x^2+x+1 ?
  - Mot = 110111
  - B(X) = $X^5 + X^4 + X^2 + X + 1$
  - B(X).X^2 = $X^7 + X^6 + X^4 + X^3 + X^2$
  - Calcul : B(X).X^2 / G(X) = ...
  - Le reste est C(X) = X+1
  - Donc la clé est 11 (coefficients de C(X))
  - Le mot à envoyer sera 11011111
  - Vérifier que M(X) est divisible par G(X) (reste nul)
    - M(X) est le polynôme correspondant au mot transmis...

CRC

- Correction...

$B(X).X^2 = X^7 + X^6 + X^4 + X^3 + X^2$ | $G(X) = X^2 + X + 1$

$-(X^7 + X^6 + X^5)$ | $P(X) = X^5 + X^3 + 1$

$X^5 + X^4 + X^3 + X^2$

$-(X^5 + X^4 + X^3)$

X^2

$-(X^2 + X + 1)$

$C(X) = X + 1$

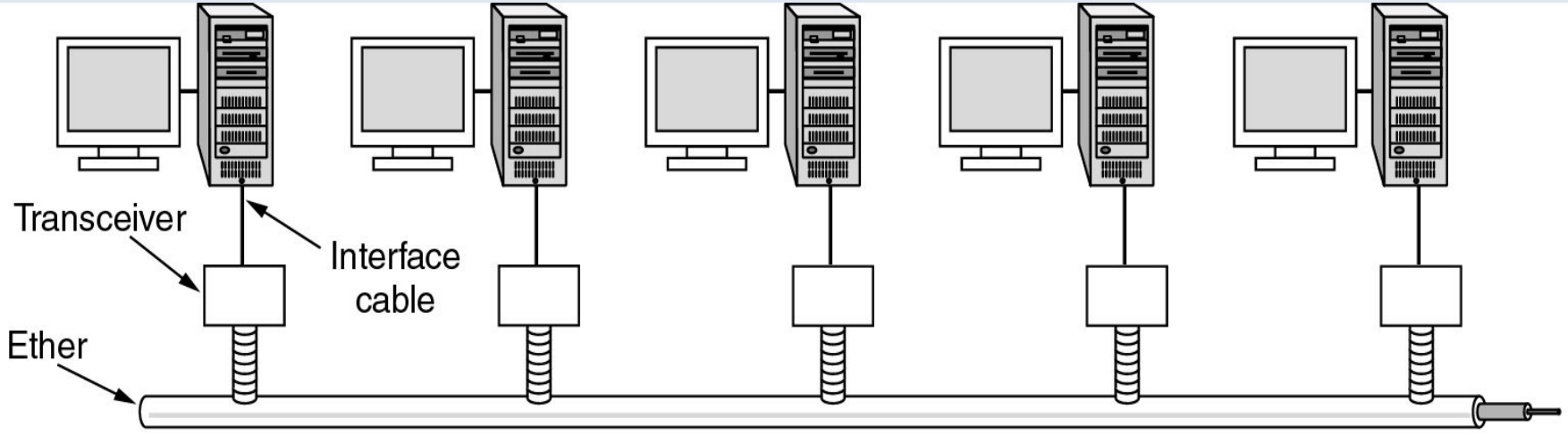
CRC

- Détection d'erreur
  - M(X) doit être divisible par G(X).
  - On peut le vérifier en effectuant la division de M(X) par G(X) ; le reste R(X) doit être nul.
  - Si ce n'est pas le cas, une erreur est détectée !

- Quelle condition doit vérifier B(X), C(X) et G(X) ?
  - $B(X).X^k = P(X).G(X) + C(X)$ avec C(X) de d° < k
  - $M(X) = B(X).X^k + C(X) = P(X).G(X) + C(X) + C(X) = P(X).G(X)$
  - En effet, en algèbre binaire (modulo 2), on a 1+1 = 0 ou encore 1 = -1, par conséquent ajouter est identique à soustraire !

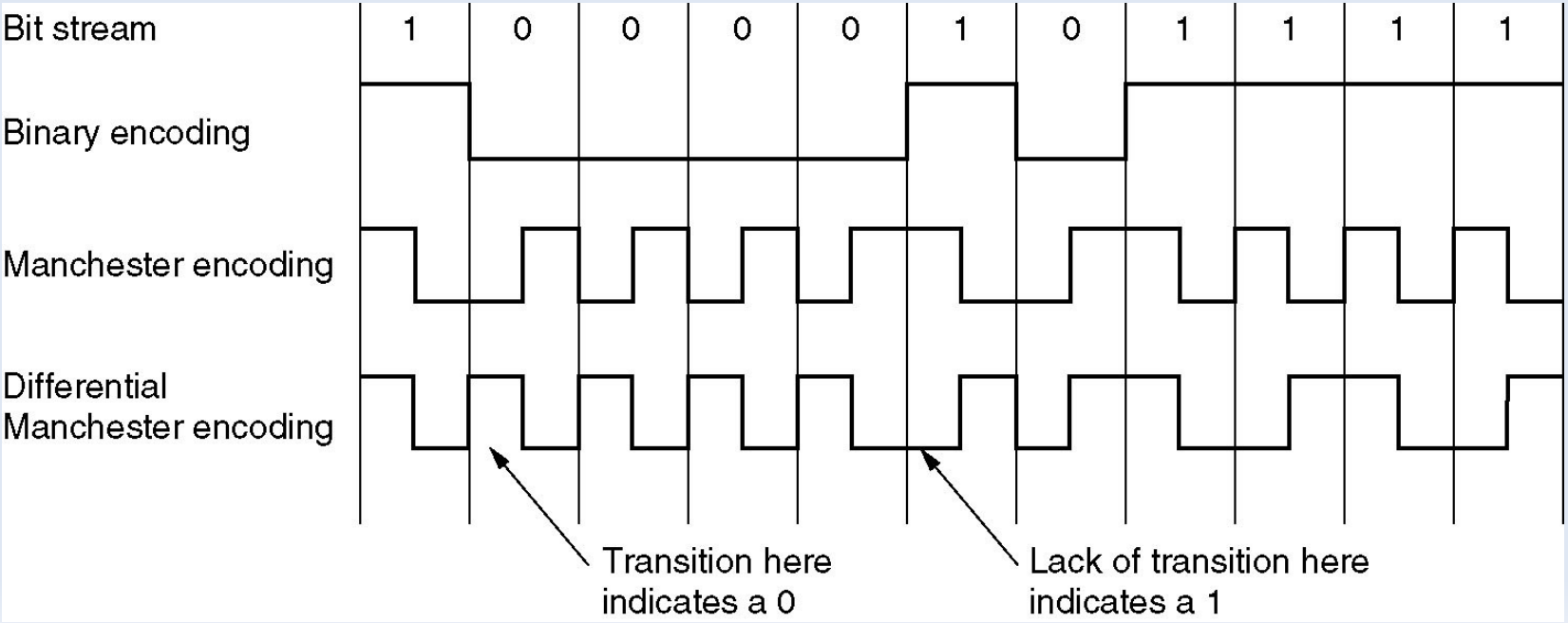
Ethernet (IEEE 802.3)

- Première technologie LAN haut-débit grand-public
  - un standard qui existe depuis plus de 20 ans...
  - permet d'échanger des trames sur divers supports physiques
  - adresse MAC des cartes Ethernet (ex. 00:15:C5:3D:52:B6)



Ethernet

- Codage du flux binaire
  - Ethernet est basé sur le codage Manchester (simple)
  - tensions -0.85 et +0.85 volts
  - approche robuste utilisant une transition pour chaque bit, ce qui facilite la synchonisation ainsi que la détection du début de l'émission

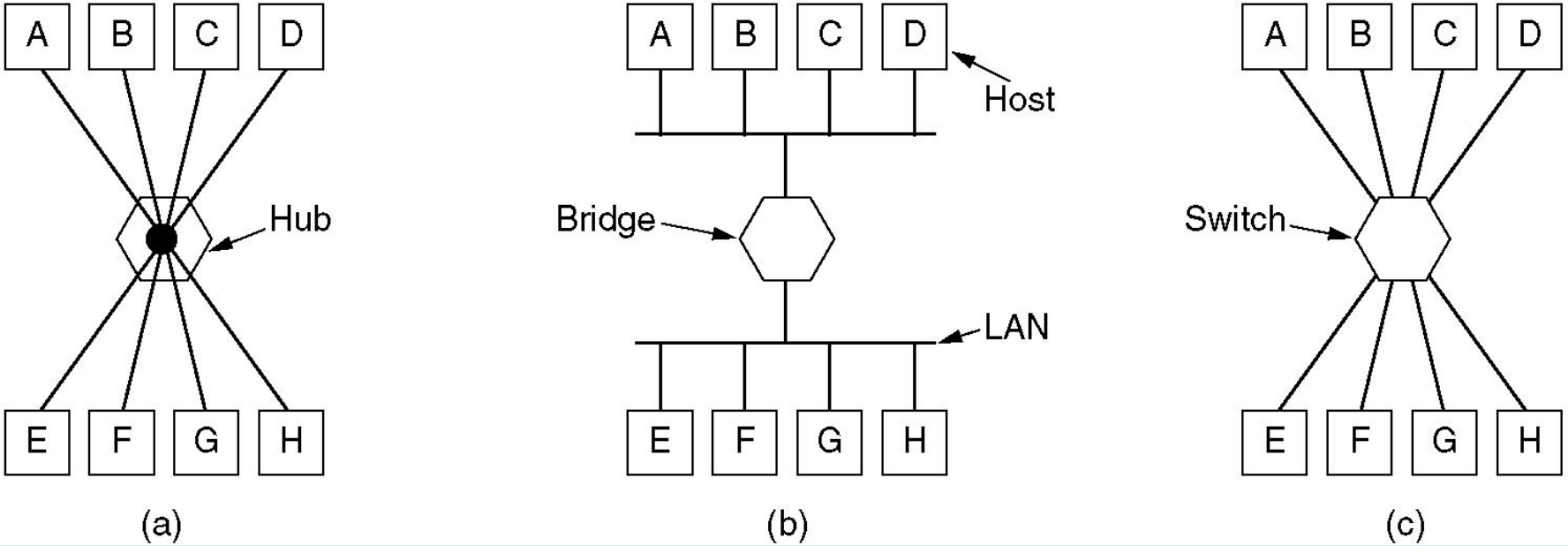


Ethernet

- Répétiteur
  - amplification du signal pour limiter l'atténuation
- Hub (concentrateur)
  - diffusion à tout le monde (équivalent bus)
  - mode semi-duplex, CSMA/CD
- Switch (commutateur)
  - diffusion des trames uniquement au destinataire choisi
  - ligne dédiée entre la station et le commutateur (mode full-duplex) donc pas de collision possible, donc pas besoin de CSMA/CD
- Bridge (pont)
  - généralisation du commutateur lorsqu'on interconnecte plusieurs technologies différentes...

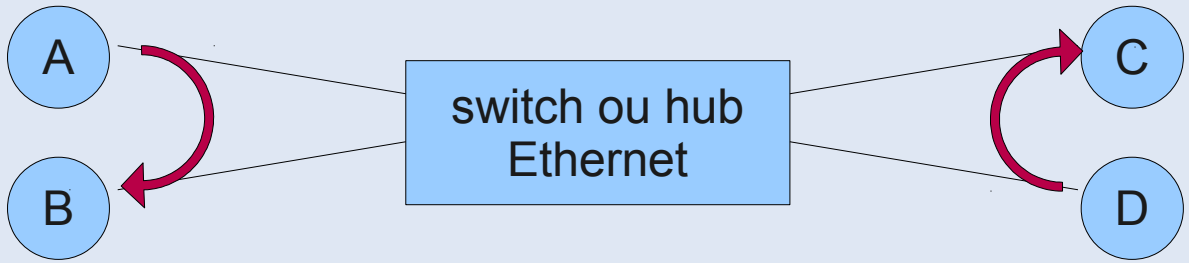
Ethernet

- Hub, Bridge, Switch



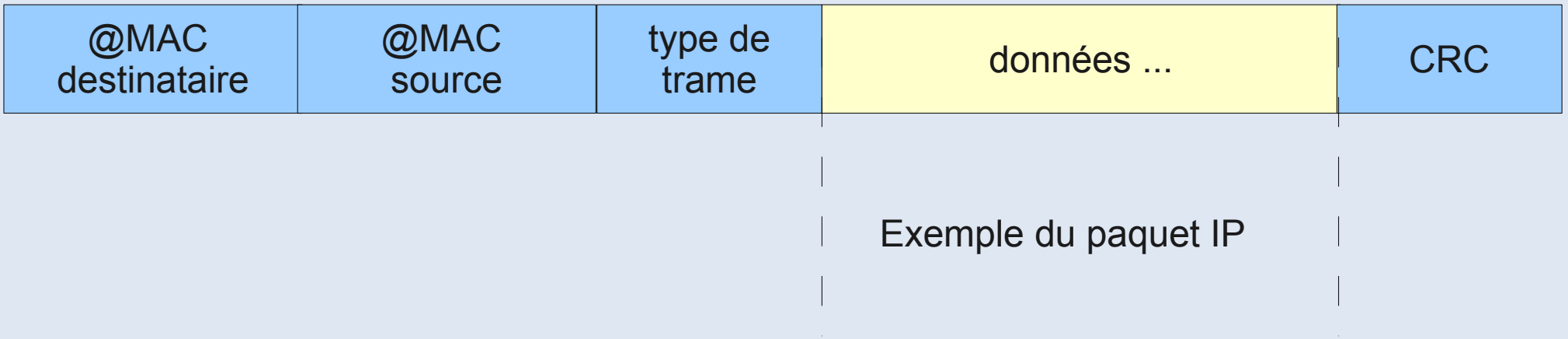
Exercice

- Au même moment, A communique avec B et D avec C en saturant un réseau Ethernet 100 Mbit/s
  - quel est le débit maximal atteint entre A et B dans le cas d'un hub ?
  - même question dans le cas d'un switch



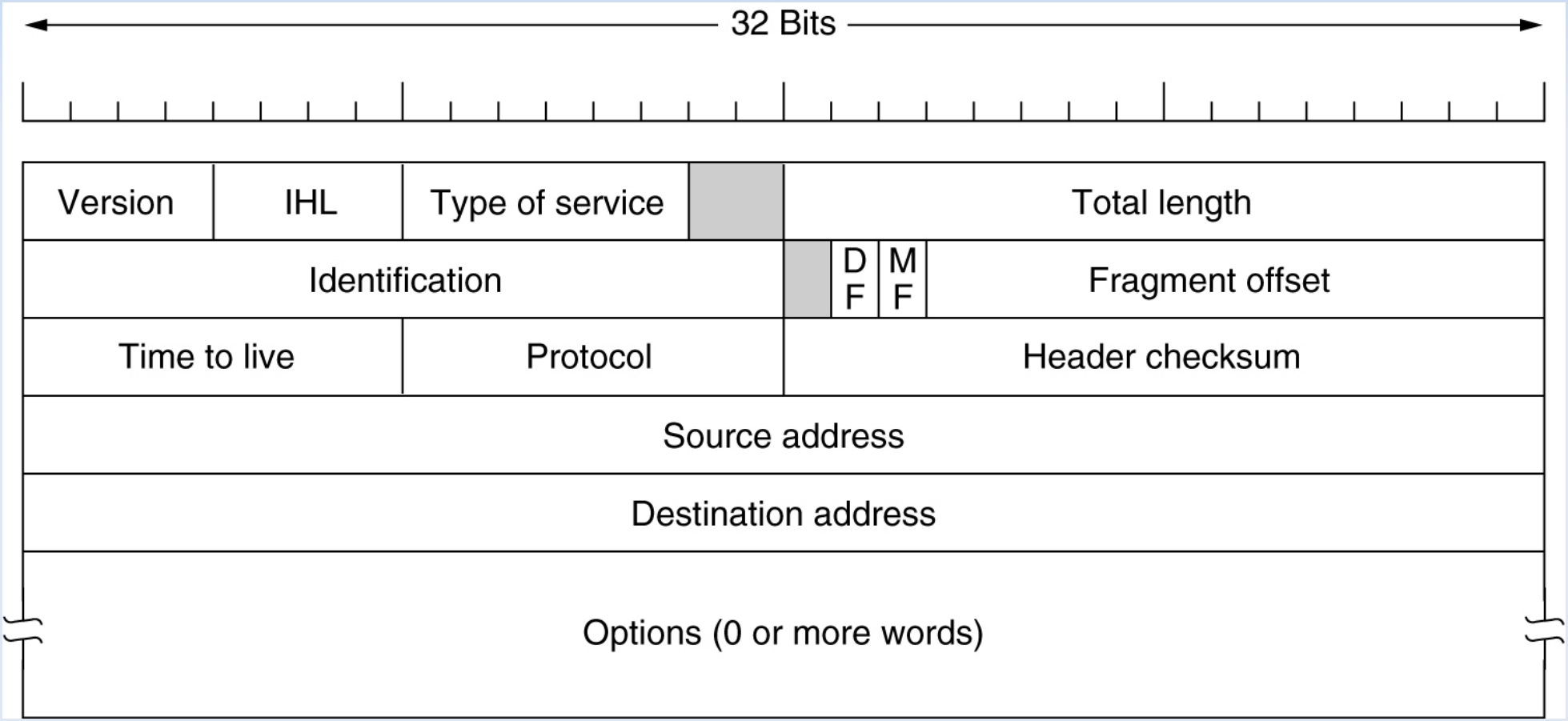
La trame Ethernet

- Format des trames (frames)
  - Adresse MAC du destinataire (6o) et du source (6o)
  - Type de protocole : 0800 = IP ; 0806 = ARP ; ... (2o)
  - Code CRC-32 (4o)
  - Données : au minimum 46o, jusqu'à 1500o
    - caractères de bourrage si données < 46o



Exemple du paquet IP (v4)

- Le paquet IP de la couche réseau est encapsulé dans la trame



Exercice

- Exemple de trame Ethernet

  00 40 07 03 04 2b 02 60 8c e8 02 91 08 00 45 00

  00 2c 14 ee 00 00 3c 06 85 7a 93 d2 5e 63 93 d2

  5e 5c 10 a4 09 e7 42 0c 56 01 00 00 00 00 60 02

  40 00 c1 29 00 00 02 04 05 b4 02 80 xx xx xx xx

- Questions
  - adresses MAC du destinataire et de l'émetteur ?
  - que repésente les 4o de la fin ?
  - protocole encapsulé dans la trame ?
  - bits de bourrage ?

Correction

- Exemple de trame Ethernet

  00 40 07 03 04 2b 02 60 8c e8 02 91 08 00 [45 00

  00 2c 14 ee 00 00 3c 06 85 7a 93 d2 5e 63 93 d2

  5e 5c 10 a4 09 e7 42 0c 56 01 00 00 00 00 60 02

  40 00 c1 29 00 00 02 04 05 b4 ~~02 80~~] xx xx xx xx

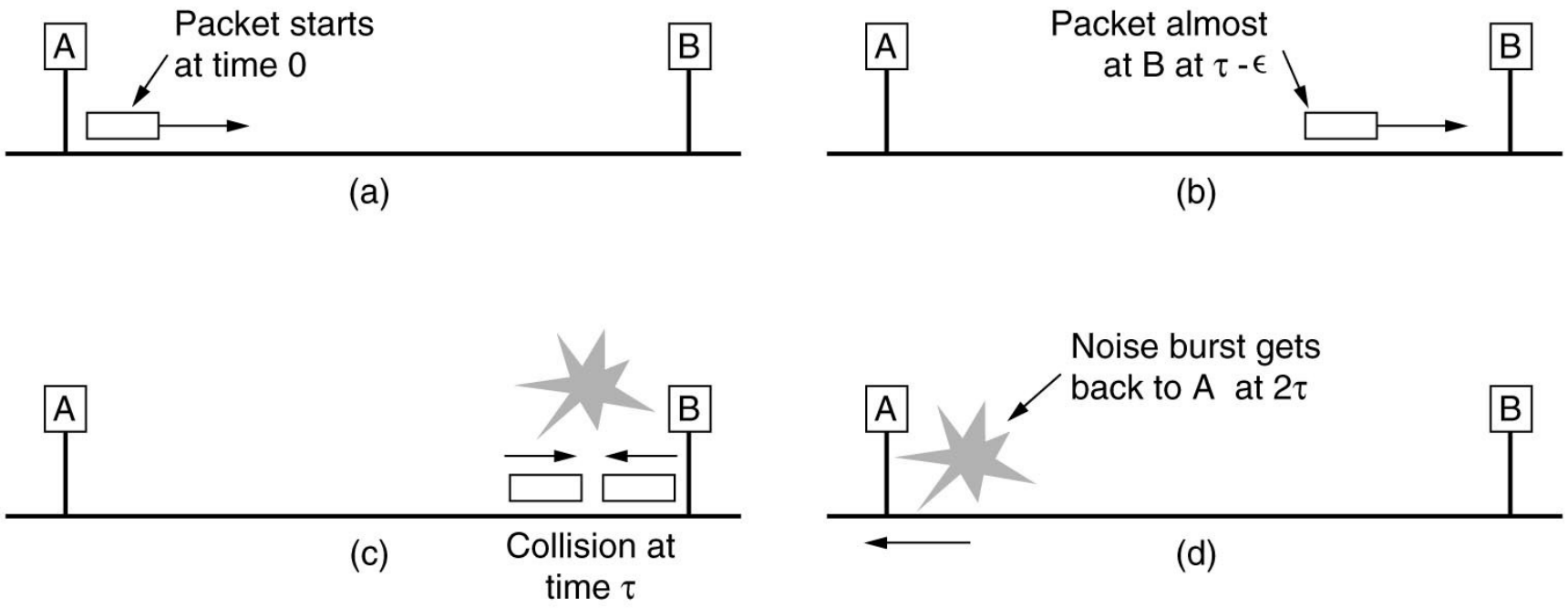
- Analyse
  - @MAC destinataire : 00 40 07 03 04 2b
  - @MAC source : 02 60 8c e8 02 91
  - Type de protocole : IP (0800)
  - Taille du paquet IP : 00 2c, soit 44 o dont 2o de bourrage
  - xx xx xx xx : CRC-32

Ethernet (CSMA/CD)

- CSMA/CD : Carrier Sense Multiple Access / Collision Detection
  - un seul émetteur à la fois qui monopolise le canal
  - pas de multiplexage, donc débit max pour chaque émetteur
  - écoute de porteuse : permet de sonder si le canal est libre

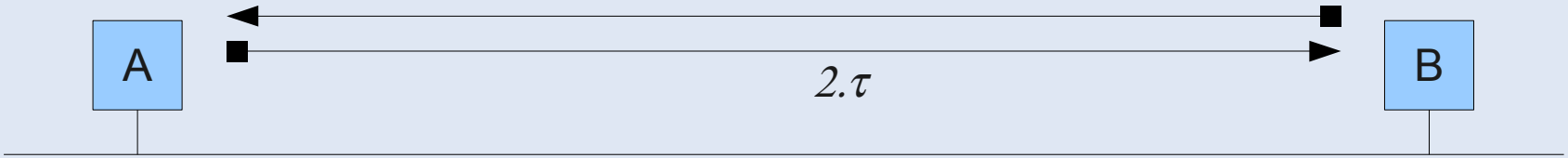
- Principe détection de collision sur le bus Ethernet
  - la détection doit se produire lors de l'emission qui doit donc durer au moins $2.\tau$
  - en cas de collision, réémission avec un délai aléatoire supplémentaire

Ethernet (CSMA/CD)



Ethernet (CSMA/CD)

- Exercice 3.5
  - Calcul de la taille minimale S_{min} d'une trame Ethernet en fonction du débit D de la carte Ethernet, de la distance maximale d_{max} séparant deux stations (A et B) et de la vitesse v de propagation du signal ?



- La détection de collision doit avoir lieu pendant l'émission...
  - donc : $T_{emission\ min} = T_{détection\ collision} = 2.\tau$

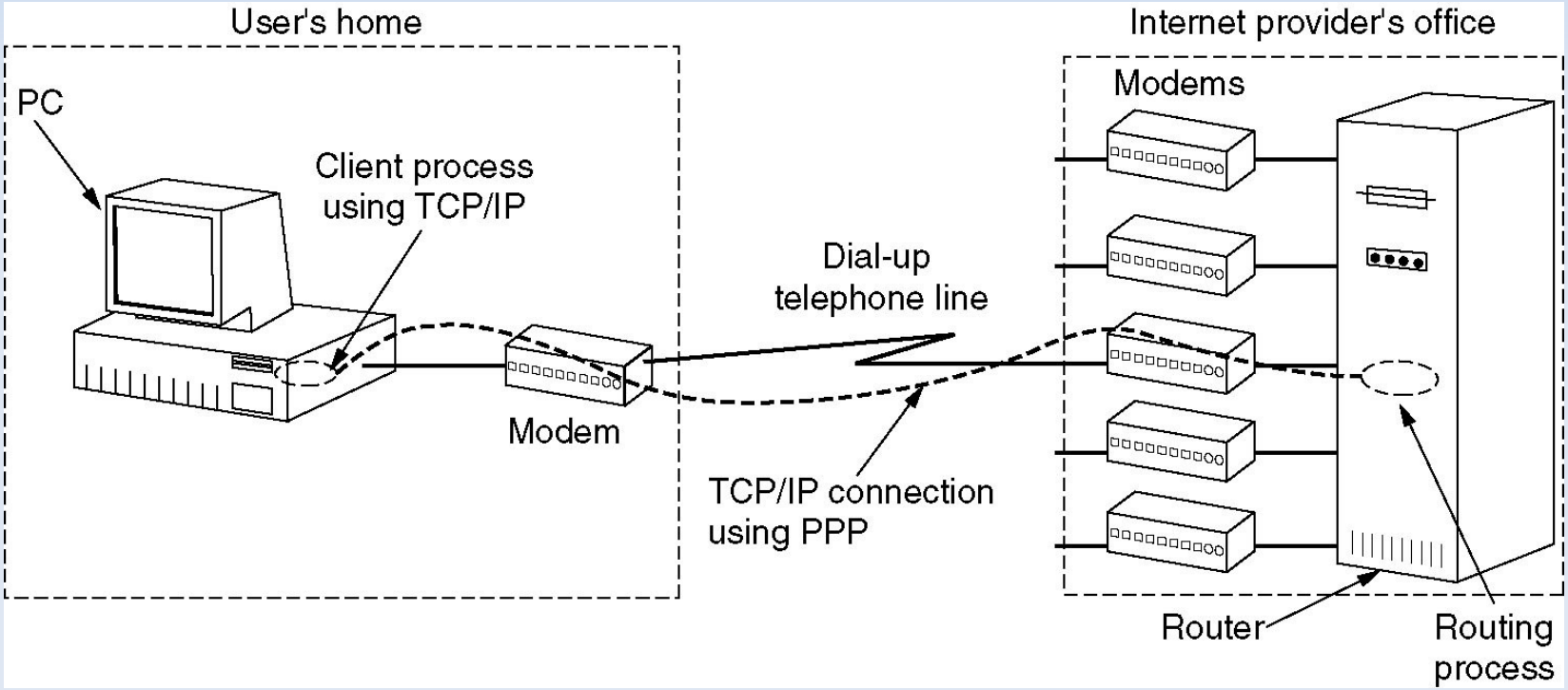
Ethernet (CSMA/CD)

- Exercice 3.5 (correction)
  - $T_{min} = 2.\tau$ avec $\tau = d_{max} / v$
  - $D = S_{min} / T_{min}$ donc $S_{min} = D.T_{min} = 2D.d_{max} / v$

- Cas Ethernet (10 Mbit/s)
  - D = 10 Mbit/s et d_{max} = 5000 m
  - v = 0,70 c = 200 000 km/s (vitesse signal électrique)
  - $T_{min} = 2\tau$ = 2.5000 / 200 000 000 = 50 µs
  - En fait, T_{min}= 51,2 µs
  - Donc $S_{min} = T_{min}$. D = $51,2.10^{-6}$ x 10.10^{6} = 512 bits = 64 o

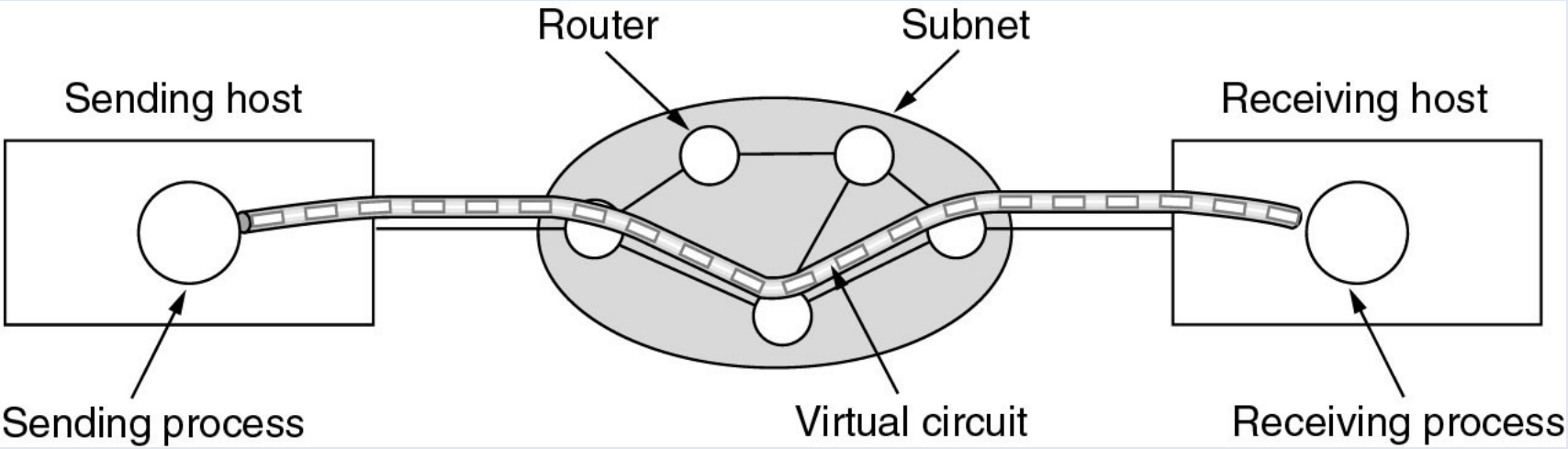
PPP

- PPP (Point-to-Point Protocol)
  - protocole de connexion directe entre une station et un FAI



ATM

- ATM (Asynchronous Transfer Mode)
  - très répandu au coeur des réseaux de télécommunication
    - en particulier, les FAIs ADSL
  - transmission des données par « cellules » de 53 octets plutôt que par trames de longueur variable comme Ethernet



ATM

- Exercice 3.7
  - On considère le lien ATM à fibre optique s'étendant sur 400 km. La vitesse de propagation dans la fibre optique est de 2.5×10^5 km/s. Le débit d'ATM est de 155 Mb/s. Contrairement à Ethernet qui utilise des trames de taille variable, ATM utilise des trames, appelées cellules, de taille fixe égale à 53 octets.
  - Questions
    - Calculer le temps de transmission d'une cellule.
    - Calculer la durée d'un trajet aller-retour.
    - Calculer la taille minimum de la fenêtre (en nombre de cellules) pour que l'émetteur puisse envoyer des cellules de façon continue avant de recevoir le premier acquittement.

ATM

- Exercice 3.7 (correction)
  - Avec un débit de 155 Mb/s, le temps de transmission d'une cellule de 53 octets est de :

$$t = (53 \times 8) / (155 \times 10^6) = 2.73\ \mu s$$

  - La durée du trajet aller-retour s'écrit :

$$t_{AR} = (2 \times 400) / (2.5 \times 10^5) = 3.2\ ms$$

  - L'accusé de réception parviendra à la source après une durée t_{AR}. Pendant ce temps, il faut que la source envoie des cellules de manière continue. En d'autres termes, la taille minimum de la fenêtre doit être :

$$3.2\ X\ 10^{-3} / 2.73 \times 10^{-6} = 1172\ \text{cellules}$$

Cours 5

Couche Physique

Introduction

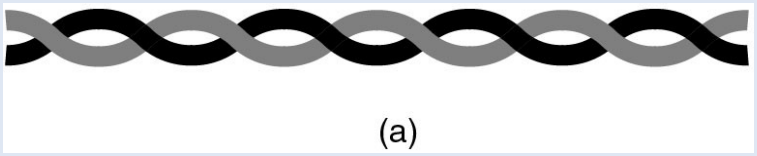
- La couche physique
  - transmission effective des signaux entre les interlocuteurs
  - service typiquement limité à l'émission et la réception d'un bit ou d'un train de bit continu
- Plan
  - Les supports de transmission
  - Bases théoriques de la transmission
  - Modulation et Multiplexage
  - Modem 56k, GSM, ADSL
  - Commutation

Supports de transmission

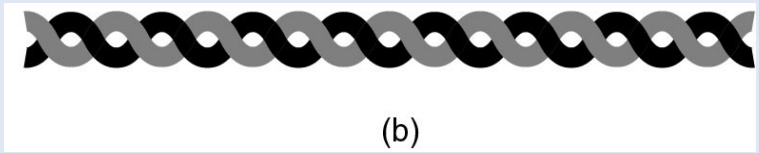
- Supports guidés
  - Paires torsadées
  - Câbles coaxiaux
  - Fibres optiques
- Supports non guidés à base d'ondes (sans fil)
  - Ondes radios terrestres (hertziens)
  - Satellites
  - *etc.*

Supports de transmission

- Paire torsadée (non blindée) ou UTP
  - paires de fils de cuivre (épasseur de qq mn)
  - torsadée pour diminuer les radiations parasites
  - plusieurs Mbit/s sur quelques kilomètres
- Catégorie des fils
  - UTP 3 (bande-passante 16 MHz, téléphone)
  - UTP 5 (bande-passante 100 Mhz)
- Avantages : simple et faible coût



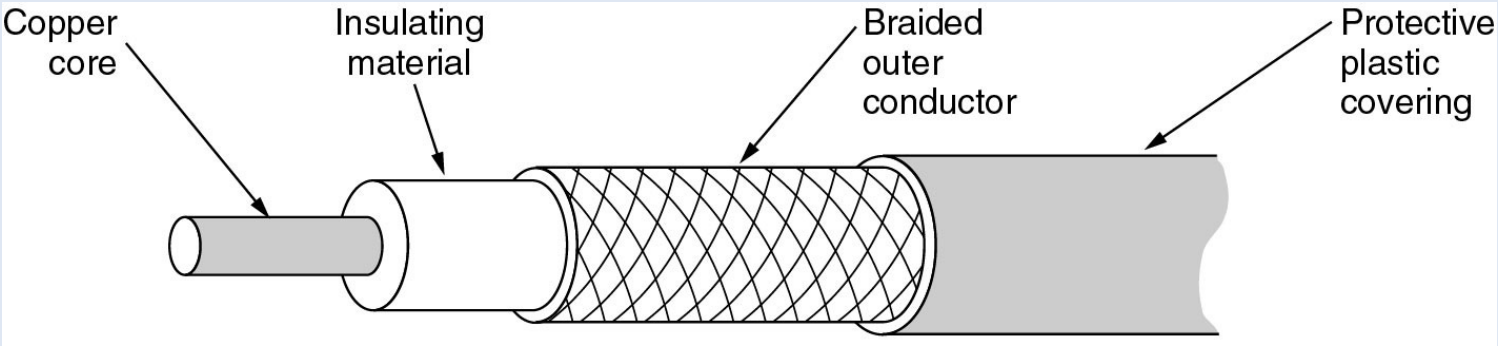
catégorie 3



catégorie 5

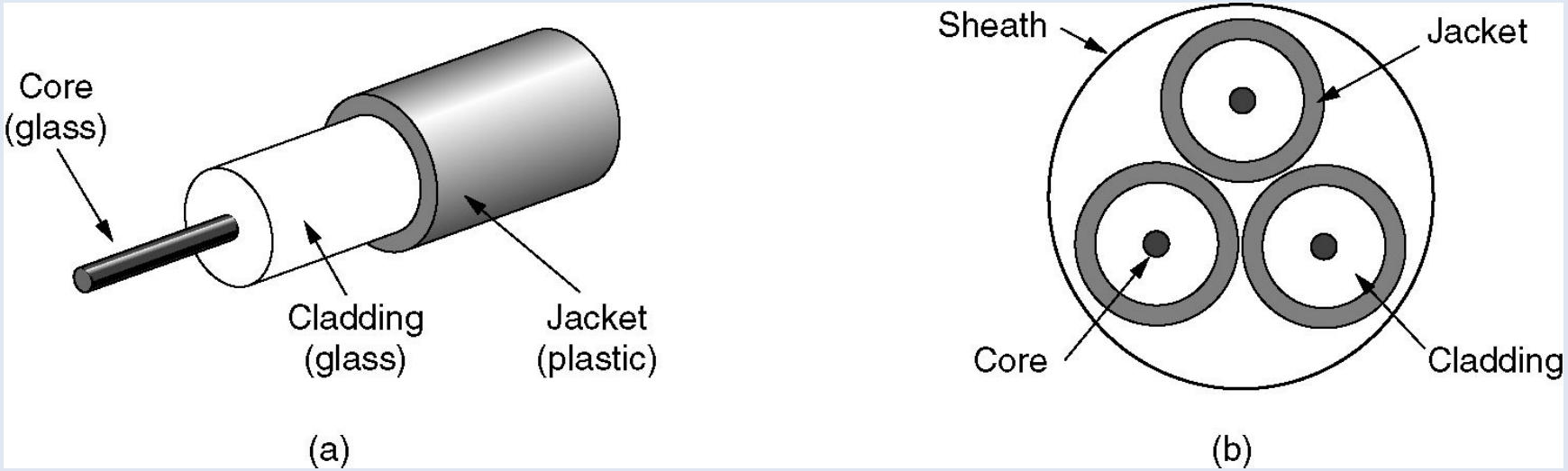
Supports de transmission

- Câble coaxial
  - 2 conducteurs cylindriques coaxiaux et isolés (3.6 mm)
  - meilleure protection au bruit donc débit plus élevé
  - bande-passante 1 Ghz, débit 100 Mbit/s
  - réseau téléphonique, câble TV
- Avantages : faible coût, robuste, débit élevé



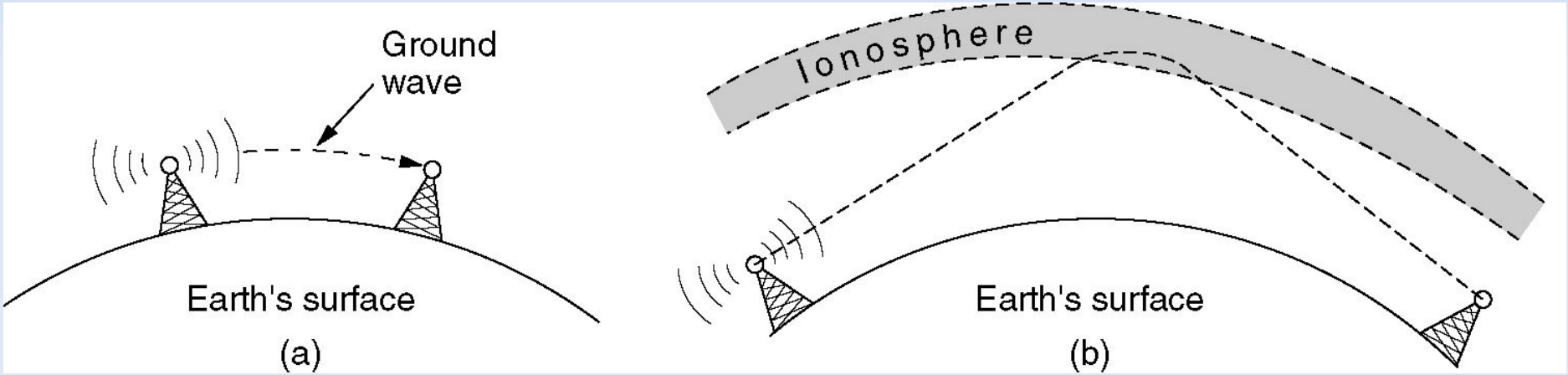
Supports de transmission

- Fibre optique
  - guide d'onde qui exploite les propriétés réfractrices de la lumière
  - débits : 10 à 1000 Gbit/s
  - bande-passante de plusieurs GHz, diamètre < 0.1 mm
  - faible atténuation du signal (régénérateur tous les 50 kms)



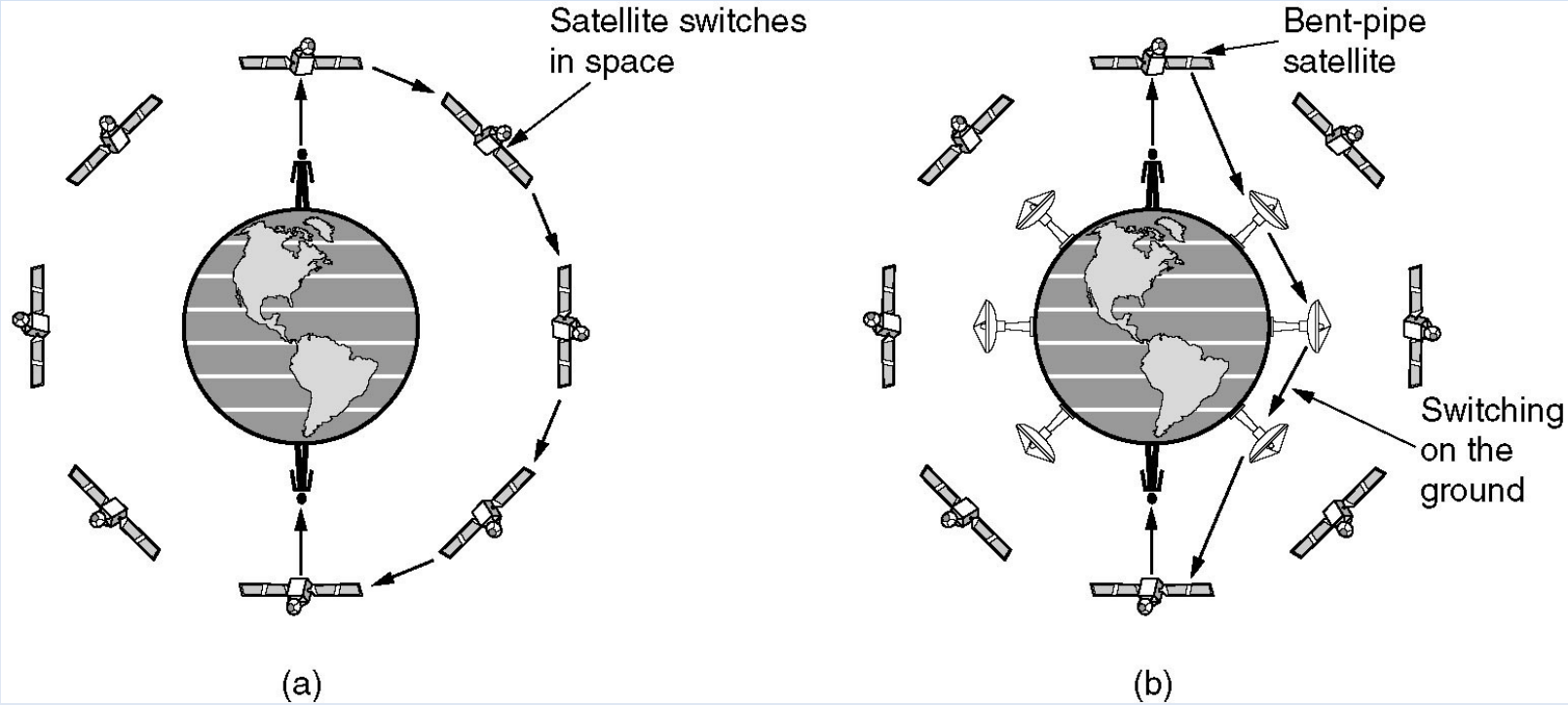
Supports de transmission

- Ondes radio terrestres (hertziens)



Supports de transmission

- Canaux satellitaires

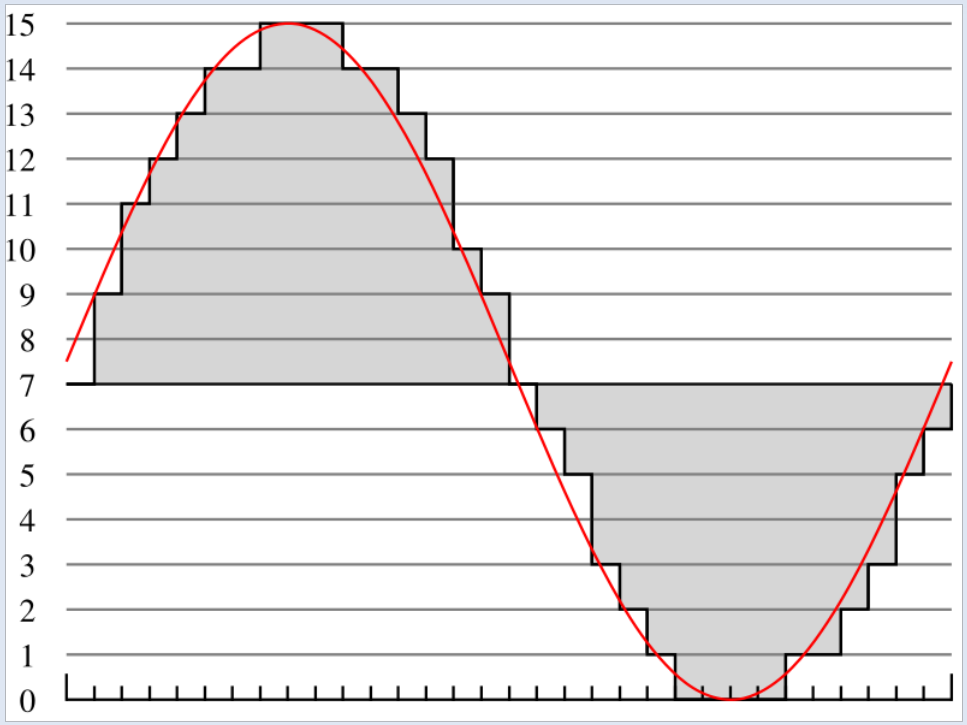


Base théorique de la transmission

- Numérisation d'un signal
  - transformation d'un signal analogique (continu) en signal numérique (discret)
- Echantillonnage
  - capture des valeurs du signal analogique à intervalle de temps régulier T (en s)
  - fréquence d'échantillonnage $f_e = 1 / T$ (en Hz)
- Quantification
  - échelle de V valeurs par échantillon
  - codage sur un mot binaire de longueur $log_2 V$ (*en* bits)
  - Ex. : 4 valeurs (0,1,2,3) codées sur 2 bits (00,01,10,11)

Base théorique de la transmission

- PCM (Pulse Code Modulation)
  - technique d'échantillonage non comprimée
  - Ex. téléphonie numérique, format son numérique, CD, ...



Base théorique de la transmission

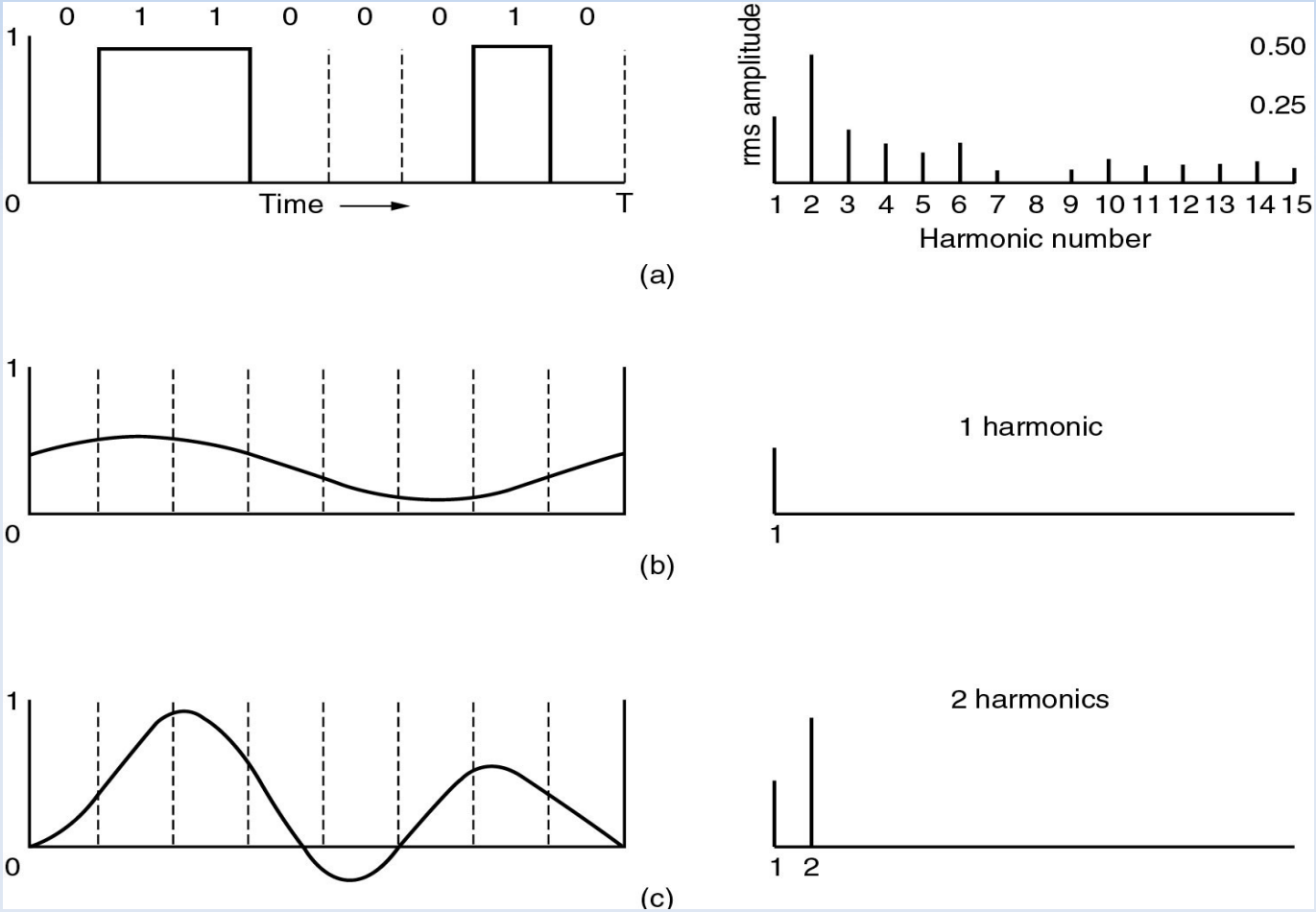
- Analyse de Fourier
  - décomposition d'un signal *f(x)* de période T en une somme (théoriquement infinie) de fonctions sinusoïdales

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cdot \cos\left(nx\frac{2\pi}{T}\right) + b_n \cdot \sin\left(nx\frac{2\pi}{T}\right)\right)$$

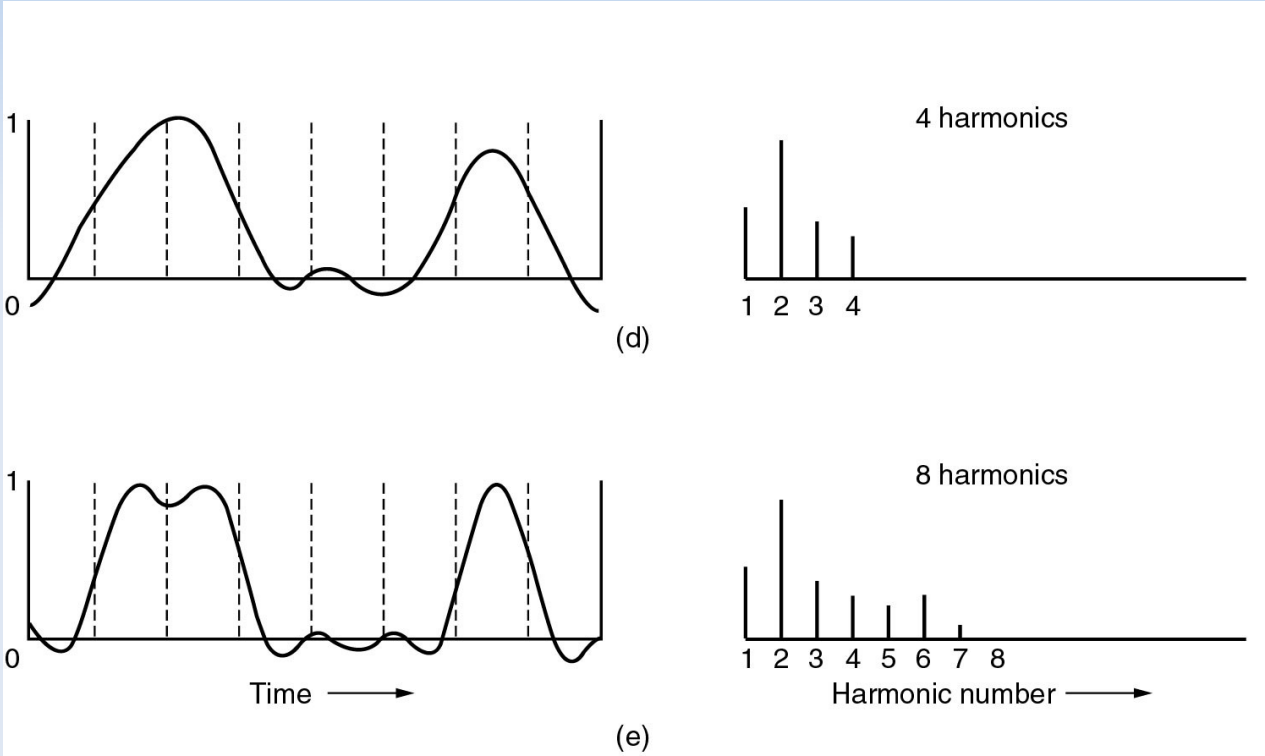
  - fréquence fondamentale *f=1/T*
  - *n*^{ème} harmonique de fréquence *n.f*
  - énergie transmise proportionnelle à ($a_n^2 + b_n^2$)

Base théorique de la transmission

- Codage du caractère ASCII b codé sur 8 bits (01100010)



Base théorique de la transmission

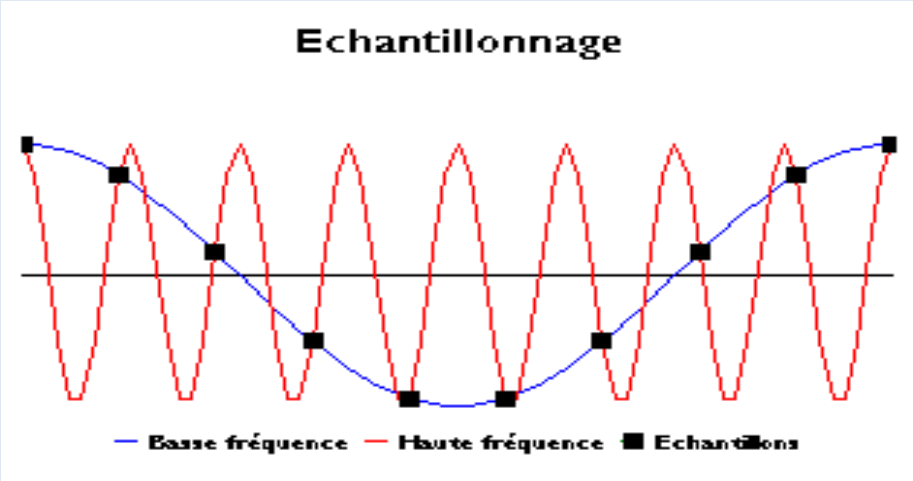


Base théorique de la transmission

- Thèorème fondamental de l'échantillonnage
  - La fréquence d'échantillonnage f_e d'un signal doit être égale ou supérieure au double de la fréquence maximale f_{max} contenue dans ce signal, afin de pouvoir le numériser sans perte d'information.

$$f_e > 2.f_{max}$$

- Exemple d'échantillonnage de deux signaux



Bande-passante

- Quelque soit le support de transmission
  - perte de puissance lors de la transmission
  - perte non uniforme selon les fréquences (distorsion)
- Bande-passante (bandwidth)
  - plage de fréquences [f_{min},f_{max}] n'entraînant pas une trop forte atténuation du signal émis
  - bande-passante $H = f_{max} - f_{min}$
  - en général, la bande-passante est définie telle que la moitié de la puissance du signal émis soit conservée (-3dB)
- Débit binaire
  - nombre de bits transmis par seconde (bit/s)

Théorème de Nyquist

- Cas d'un signal parfait (non bruité)
  - application d'un filtre passe-bas de bande-passante H
- Théorème de Nyquist
  - signal composé de V niveaux significatifs
  - débit binaire maximal : $D = 2H \log_2 V$ (en bit/s)

Théorème de Shanon

- Cas du signal bruité
  - S : puissance du signal ; N : puissance du bruit
  - rapport signal sur bruit (en dB) : $10 \log_{10} S/N$
- Théorème de Shanon
  - capacité du canal : $C = H \log_2 (1 + S/N)$ (en bit/s)
  - C est le débit binaire maximal théorique, indépendemment de la technique de transmission utilisée (multiplexage, ...)
  - C contraint le nombre maximal V de niveau que l'on peut distinguer de manière significative ($D < C$)

Exercices

- Ex 2.1
  - Pourquoi selon vous les CD audio sont-ils échantillonés à 44.1 kHz ?
- Ex 2.2
  - Un canal téléphonique a une bande-passante de 3100 Hz (entre 300 Hz et 3400 Hz). Quel est le débit pour un signal binaire ?
  - Le canal téléphonique n'est en fait pas parfait, avec rapport signal sur bruit de 30 dB. Quel est le débit maximal théorique ?
  - Comment la plupart des modems RTC (56k, ADSL) peuvent-ils avoir un débit supérieur ?

Corrections

- Ex 2.1
  - L'oreille humaine peut capter les sons jusqu'à 16 kHz, quelquefois jusqu'à 20 kHz. Il convient donc, lors de la numérisation, d'échantillonner le signal audio à au moins 40 kHz.
  - 44,1 kHz est la valeur normalisée par l'industrie.
- Ex 2.2
  - Nyquist : $D = 2H \log_2 V = 2 \times 3100 \times \log_2 2 = 6200$ bit/s = 6 kbit/s
  - Shanon : S/N=30 dB = 1000, $C = 3100 \times \log_2 (1+1000) =$ 30.17 kbit/s
  - Grâce au multiplexage (voir suite).

Modulation

- Modulation
  - processus par lequel l'émetteur transforme le message de sa forme originale en une forme plus adaptée à la transmission
  - translation du spectre du signal-message autour de la fréquence de la porteuse (carrier)
- Démodulation
  - processus inverse côté récepteur
- Modem (modulateur-démodulateur)
  - baud : nombre de modulation par seconde
  - utilisation de plusieurs techniques de modulation pour transmettre plusieurs bits (k) par modulation
  - débit binaire = k x baud (en bit/s)

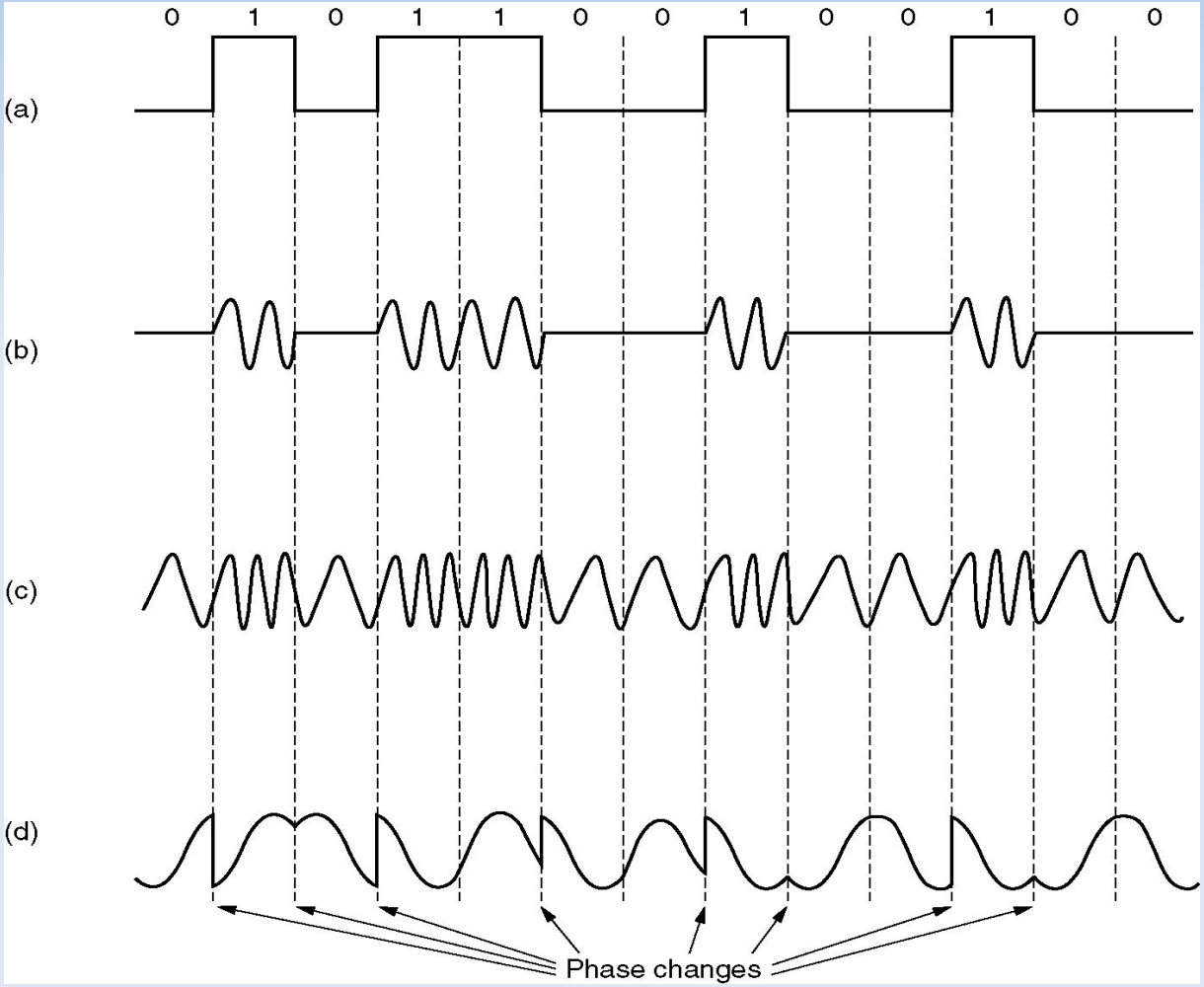
Les différentes modulations

signal

modulation d'amplitude

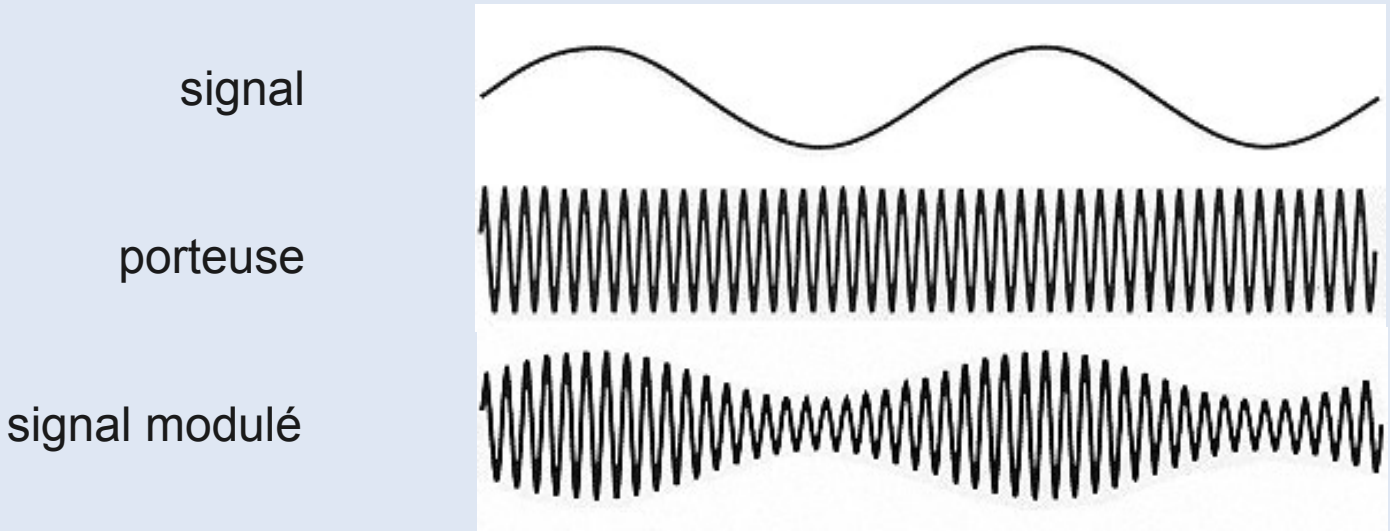
modulation de fréquence

modulation de phase



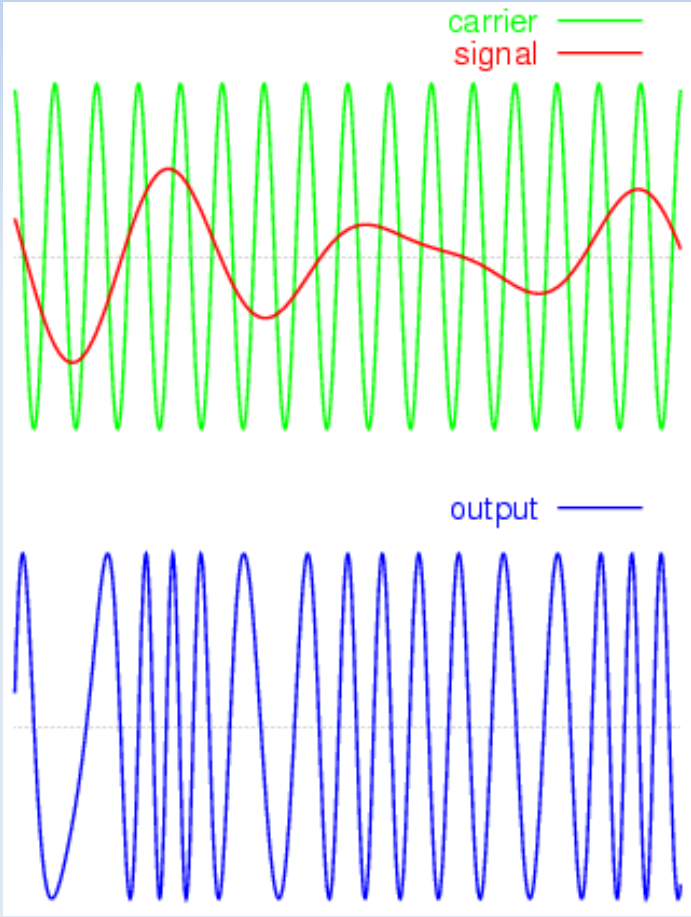
Modulation d'amplitude

- Principe
  - modulation de la valeur de l'amplitude de la porteuse (opération de multiplication)
- Exemples
  - Radio AM (GO, PO, ...)
  - Télévision Hertzienne



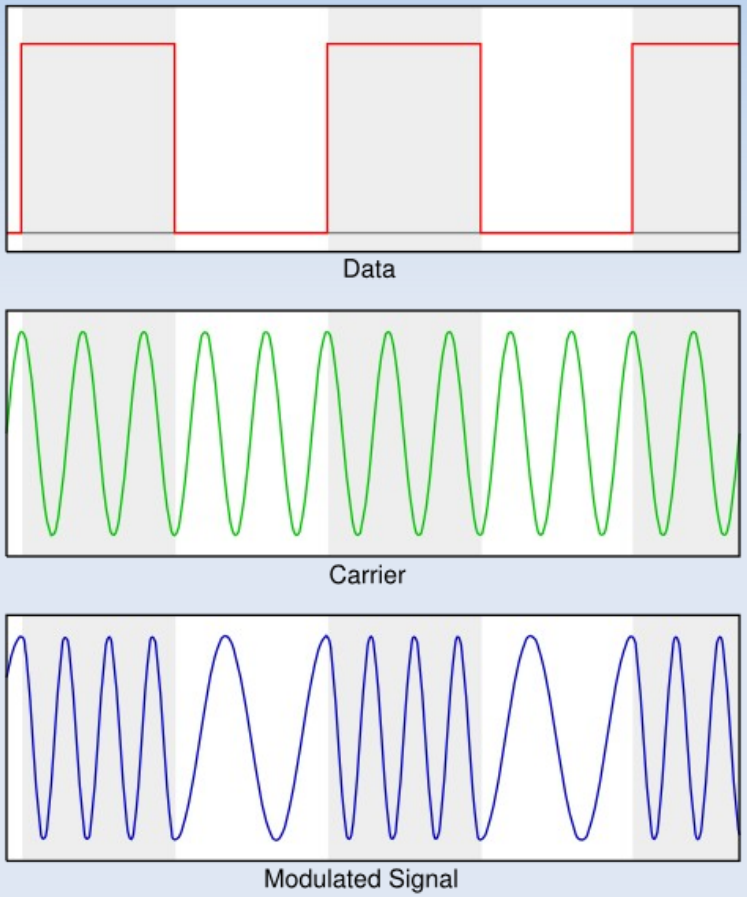
Modulation de fréquence

- Cas du signal continu
  - signal (en rouge) superposé avec la fréquence porteuse (en vert)
  - signal modulé (en bleu)
- Exemple Radio FM
  - porteuse (bande 87.5 - 107.9 MHz)
  - signal G+D de 0 à 15 kHz (mono)
  - signal G-D, complément stéréo autour de 38 kHz
  - signal pilote stéréo 19 kHz
  - signal RDS (autour de 57 kHz)



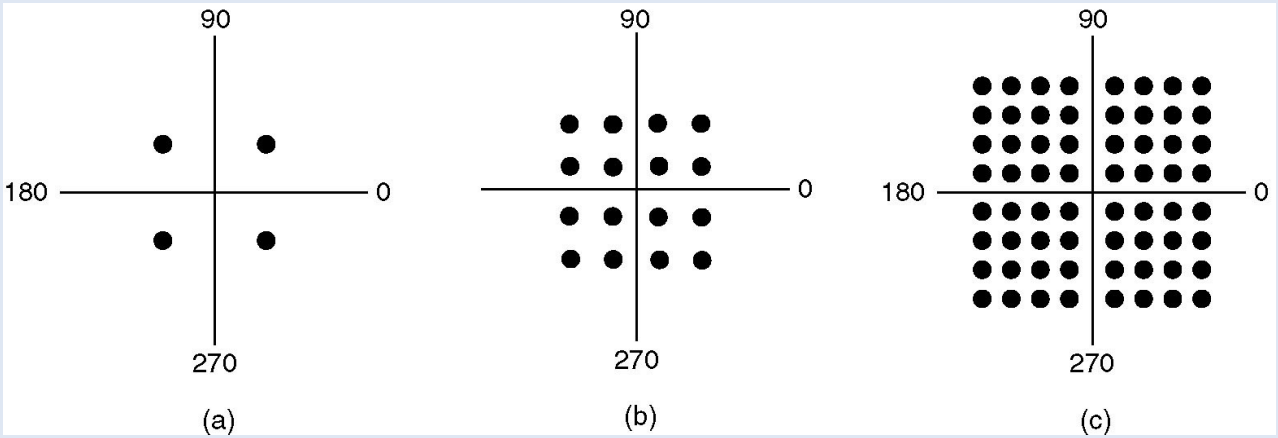
Modulation de fréquence

- Cas du signal numérique
  - FSK (Frequency-Shift Keying)
  - signal modulé varie entre des fréquences prédéterminées
    - 0 = fréquence basse
    - 1 = fréquence haute
- Exemples
  - Norme GSM (Global System for Mobile) basée sur une variante de FSK



Modulation de phase

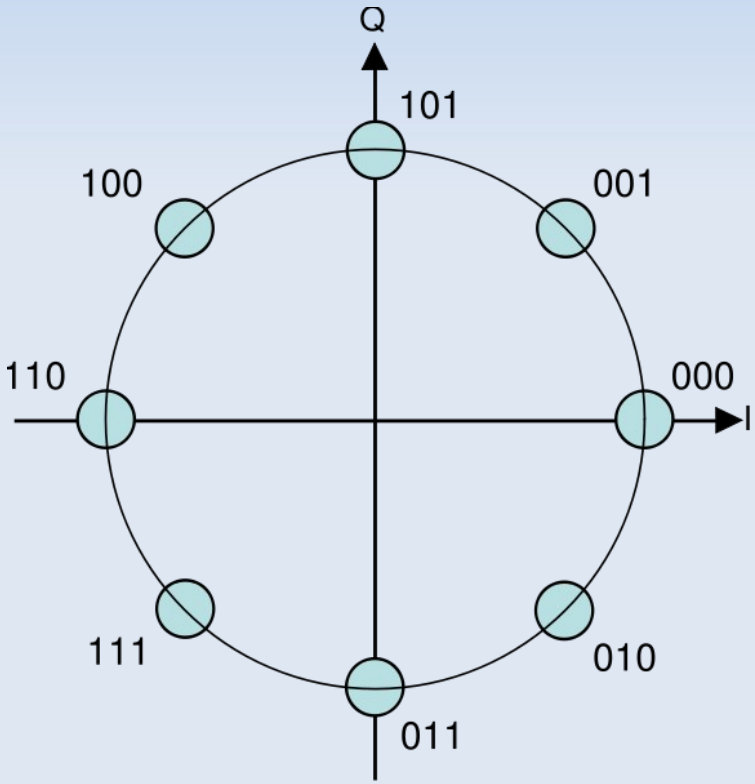
- QPSK (Quadrature Phase Shift Keying)
  - 4 décalages de phase sur la porteuse : 0°, 90°, 180° et 270°
  - ce qui permet de coder 2 bits par baud
- QAM-16 (Quadrature Amplitude Modulation)
  - 4 amplitudes et 4 phases, soit 16 combinaisons (4 bits)
  - débit de 9600 bit/s sur une ligne à 2400 bauds



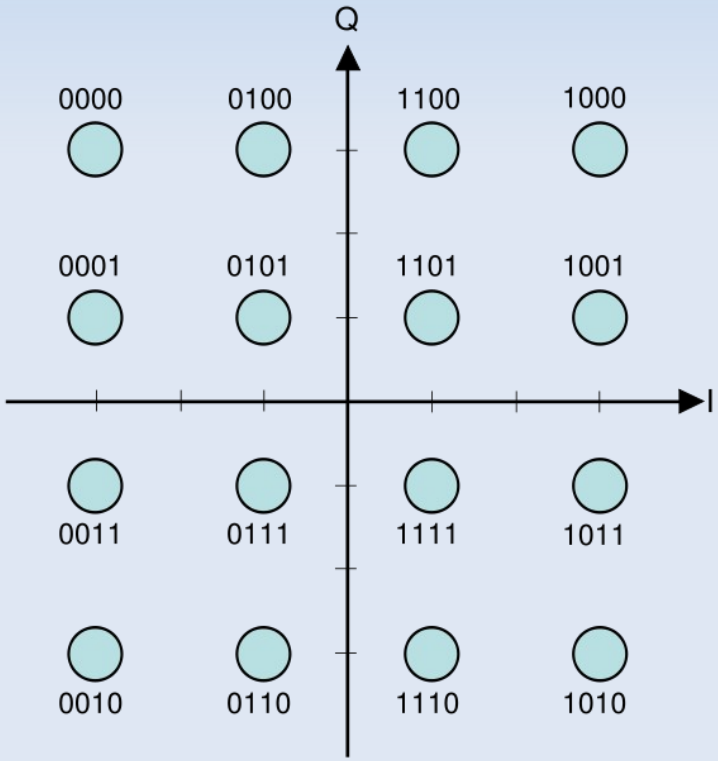
QPSK QAM-16 QAM-64

Modulation de phase

- PSK-8 (3 bits)

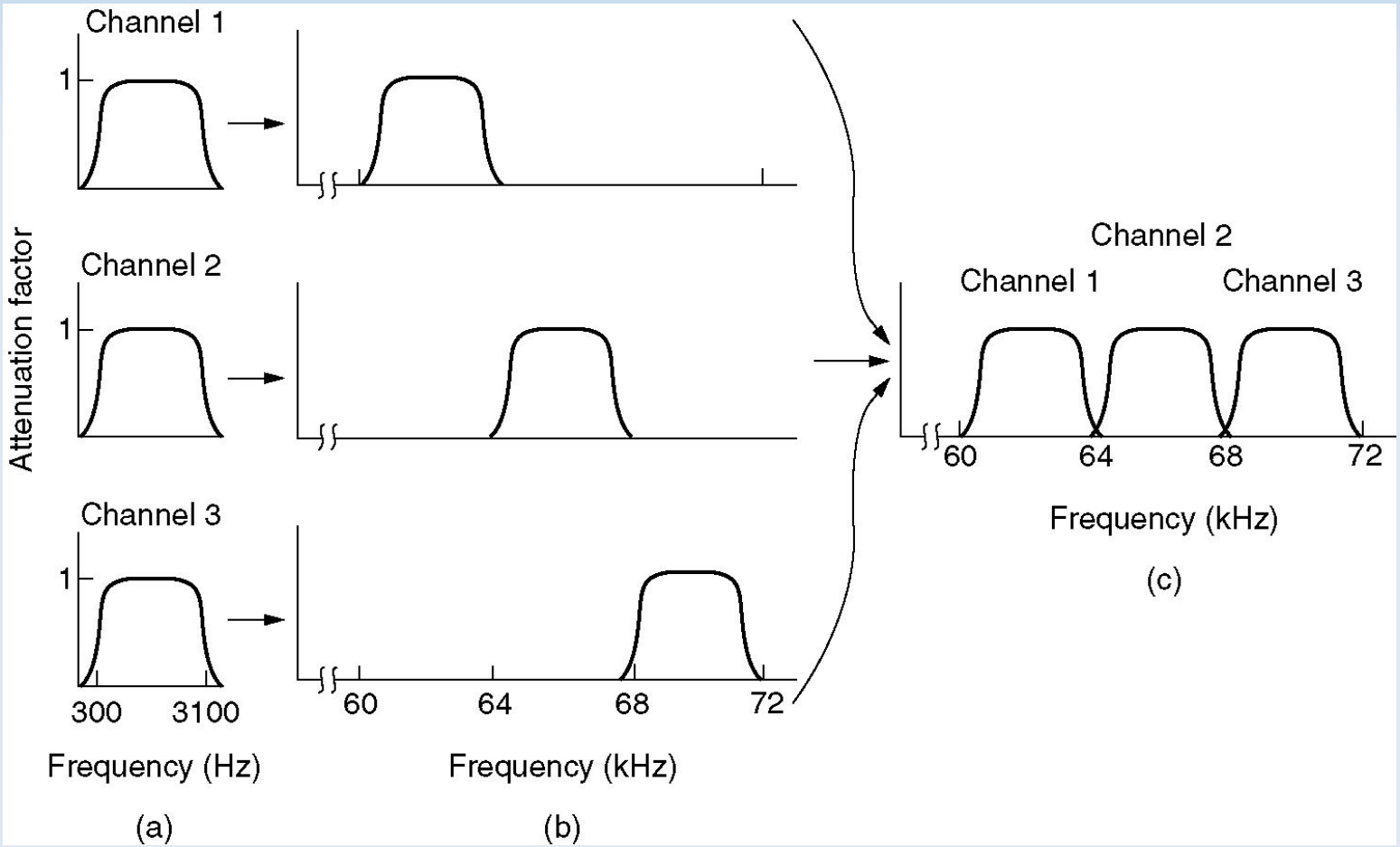


- QAM-16 (4 bits)



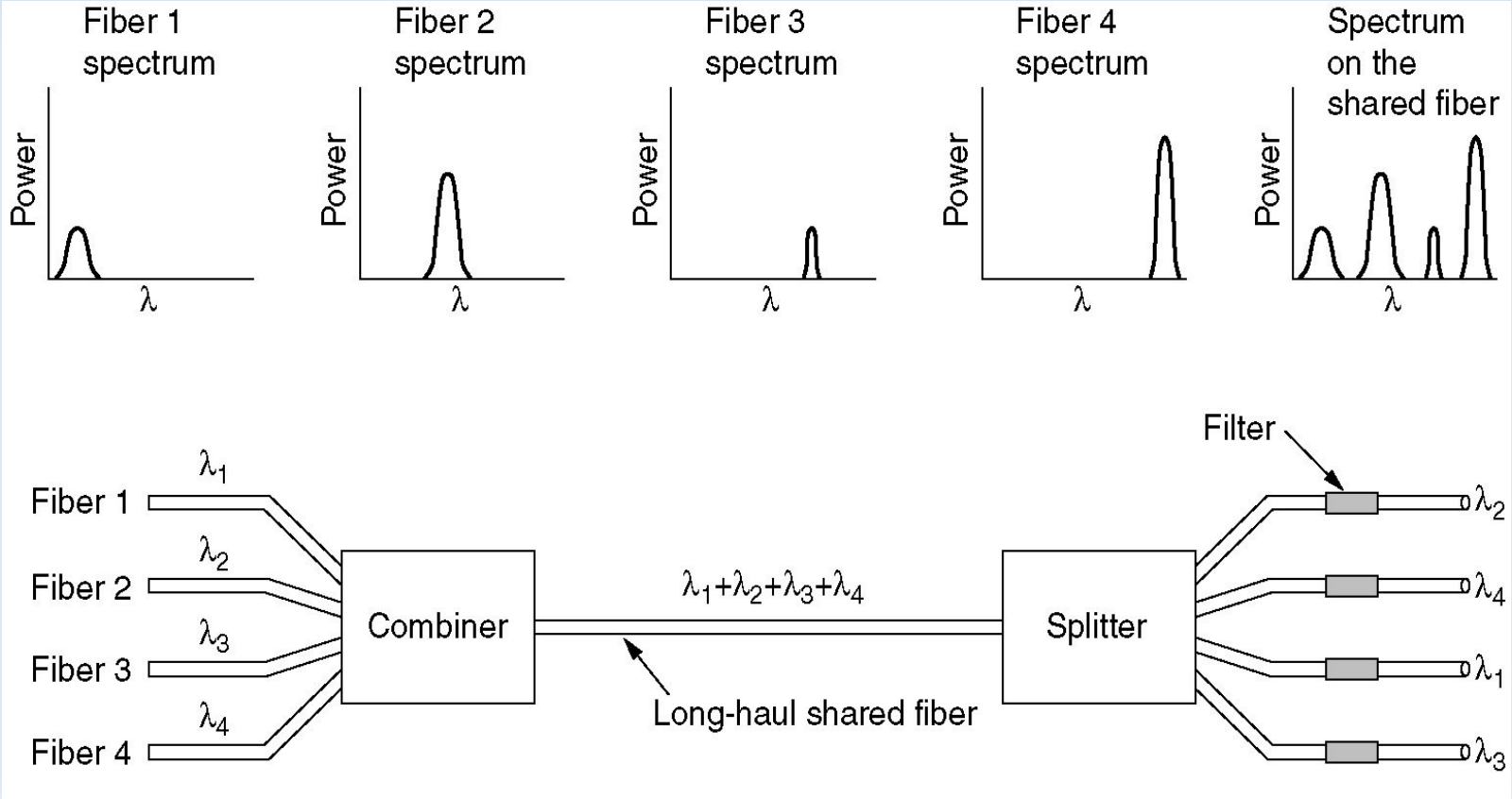
Multiplexage fréquentiel

- transmission simultanée de messages différents ayant des spectres disjoints



Multiplexage en longueur d'onde

- WDM (Wavelength Division Multiplexing)
  - variante du multiplexage fréquentiel adapté à la fibre optique
  - le débit de chaque fibre en entrée est limité par l'électronique !



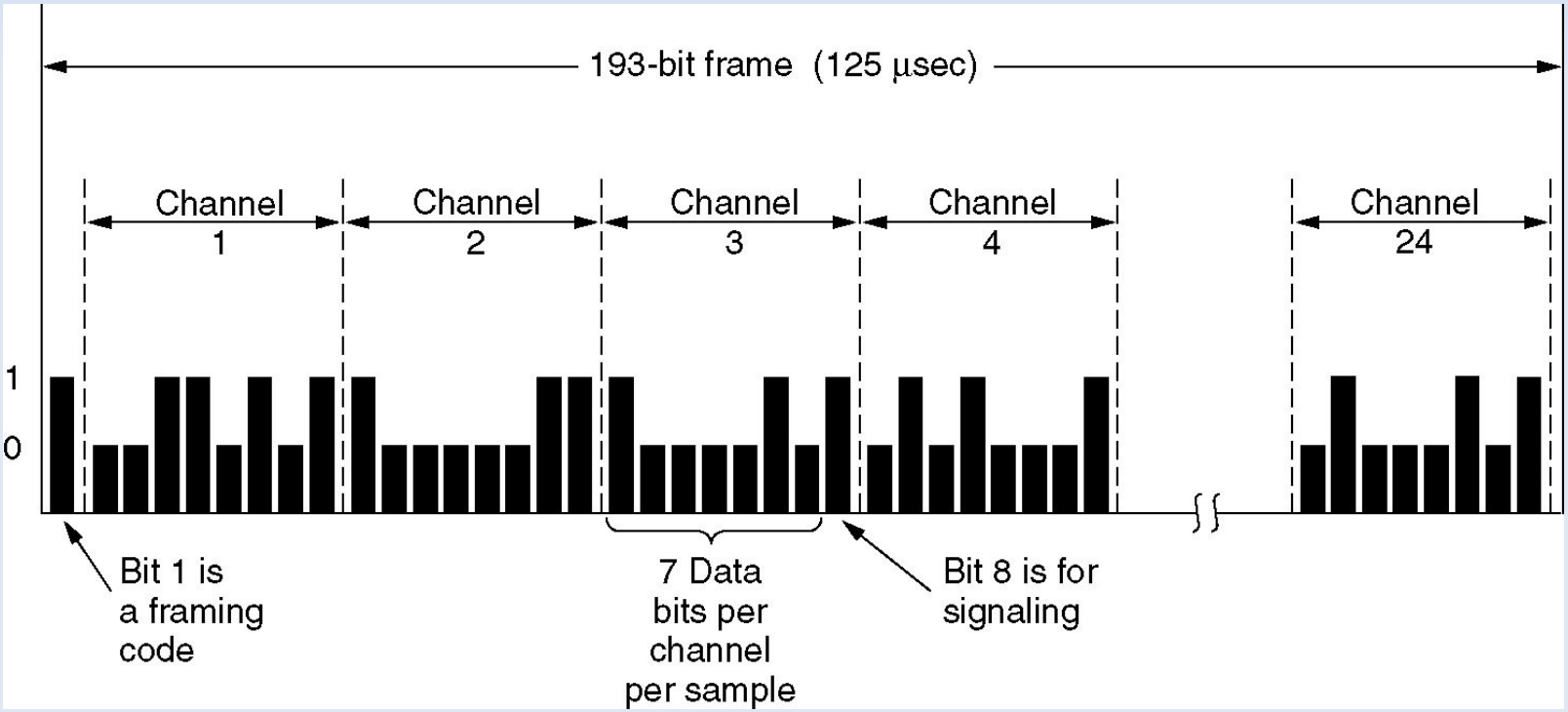
Multiplexage temporel

- TDM (Time Division Multiplexing)
  - uniquement appliquable à des signaux numériques
  - utilisation d'un codec (codeur-décodeur) pour convertir les signaux analogiques en blocs de 8 bits

- Exemple du réseau téléphonique
  - combinaison de plusieurs signaux vocaux analogique échantillonée en PCM sur une seule artère numérique (le coeur du réseau téléphonique)
  - échantillonnage à 8000 Hz (0,125 ms/échantillon) pour une bande-passante du réseau téléphonique à 4 kHz (Nyquist)

Multiplexage temporel

- Exemple du réseau téléphonique T1 aux USA
  - débit 1,544 Mbit/s, échantillonage à 0.125 ms

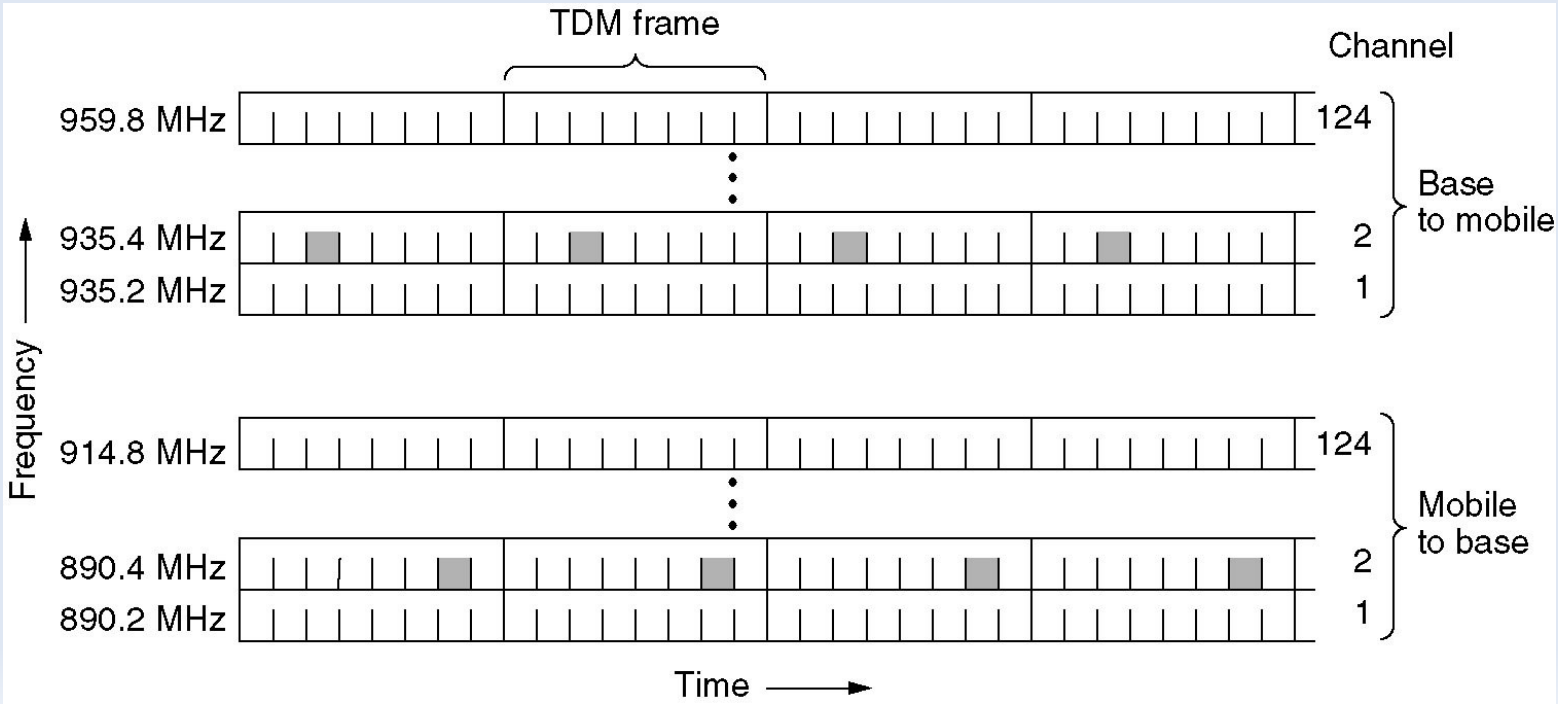


Modem 56k (norme V.90)

- Caractéristiques
  - 8000 bauds maxi sur le RTC d'après Nyquist
  - 8 bits par modulation (dont 1 bit de contrôle)
  - débit = 7 x 8000 = 56 000 bit/s
- Débit asymétrique
  - débit de 56 kbit/s pour la liaison descendante (downstream)
  - débit de 33,6 kbit/s pour la liaison montante (upstream)
- Modulation TCM (Trellis Coded Modulation)
  - 8 bits / modulation avec une variante du QAM (modulation de phase et d'amplitude)

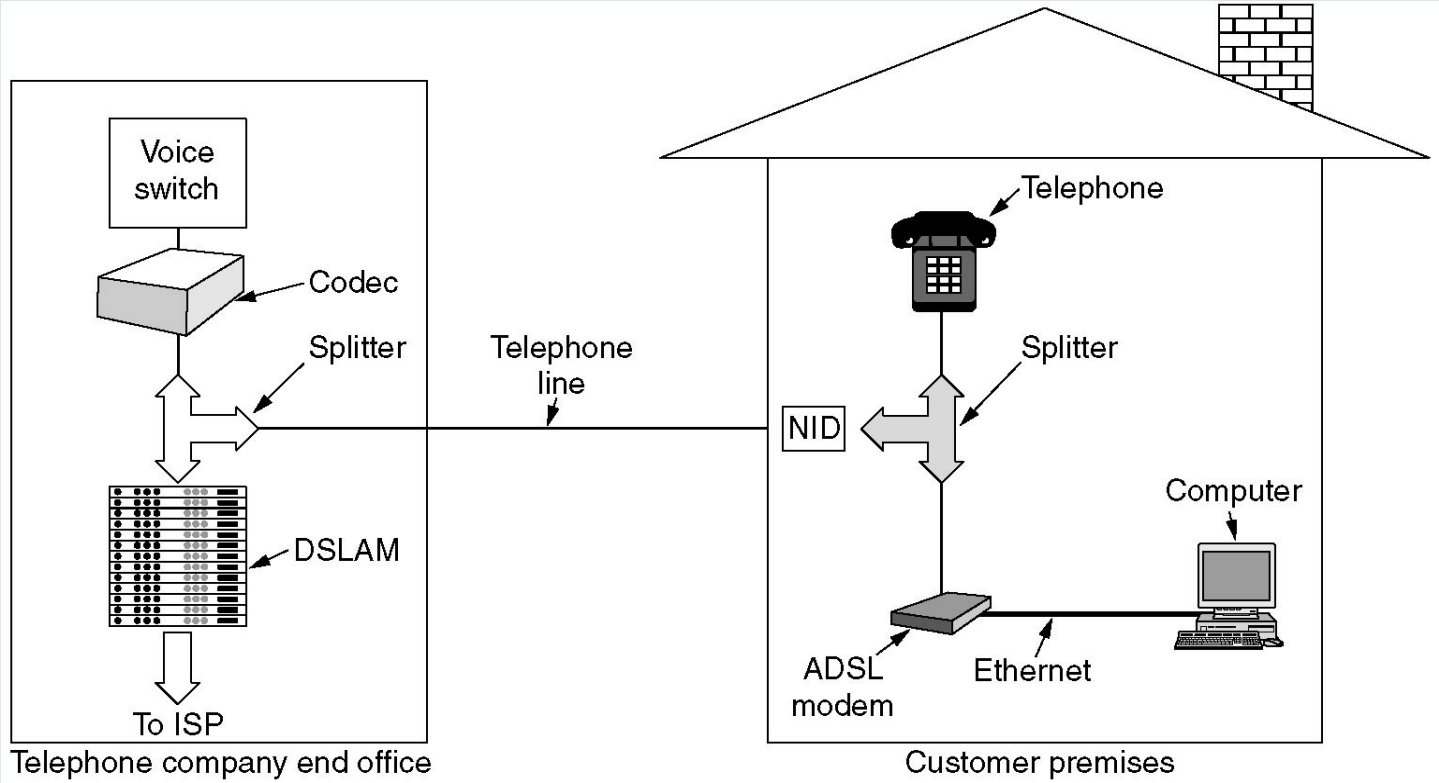
GSM

- GSM (Global System for Mobile Communication)
  - voix numérique (G2)
  - 124 paires de canaux simplex (montants et descendants)
  - 1 canal simplex : bande-passante 200 kHz, 8 connexions
  - multiplexage fréquentiel et temporel



ADSL

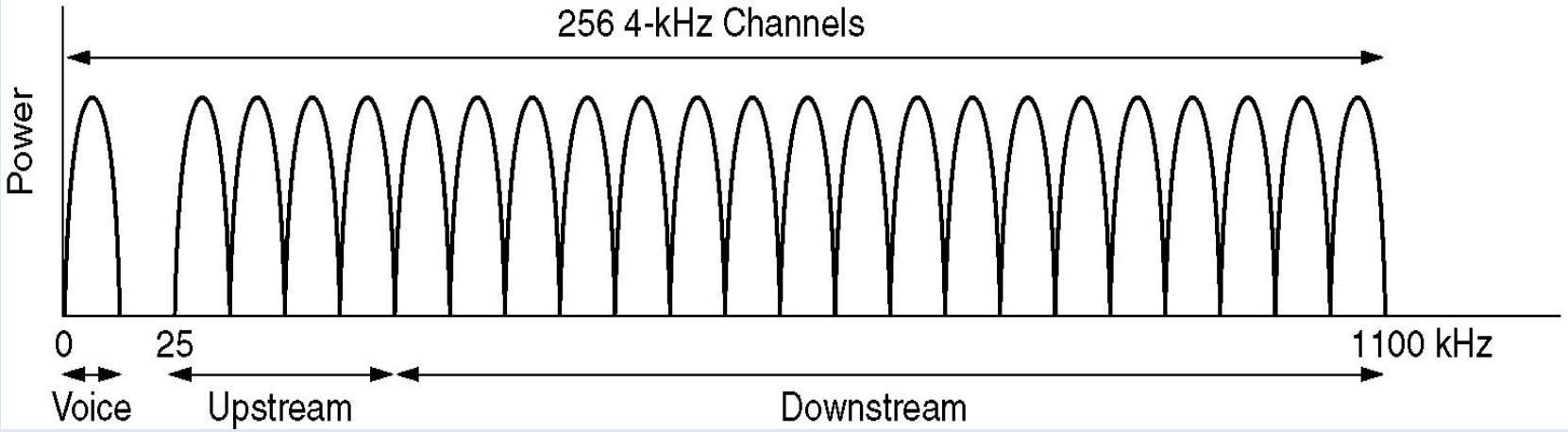
- ADSL (Asymmetric Digital Subscriber Line)
  - utilisation des fréquences hautes du réseau de téléphonie (RTC)
  - ADSL 1 (< 1.1 MHz) et ADSL 2+ (< 2.2 MHz)



(ISP : Internet Service Provider ; DSLAM : DSL Access Multiplexer)

ADSL

- Principe
  - Modulation fréquentiel : division en plusieurs canaux de 4.3 kHz
  - Répartition asymétrique des canaux pour l'envoi et la réception
    - débit montant (upload)
    - débit descendant (download), 80 à 90% des canaux
  - Modulation QAM-250 en parallèle pour chaque canal (ATM)



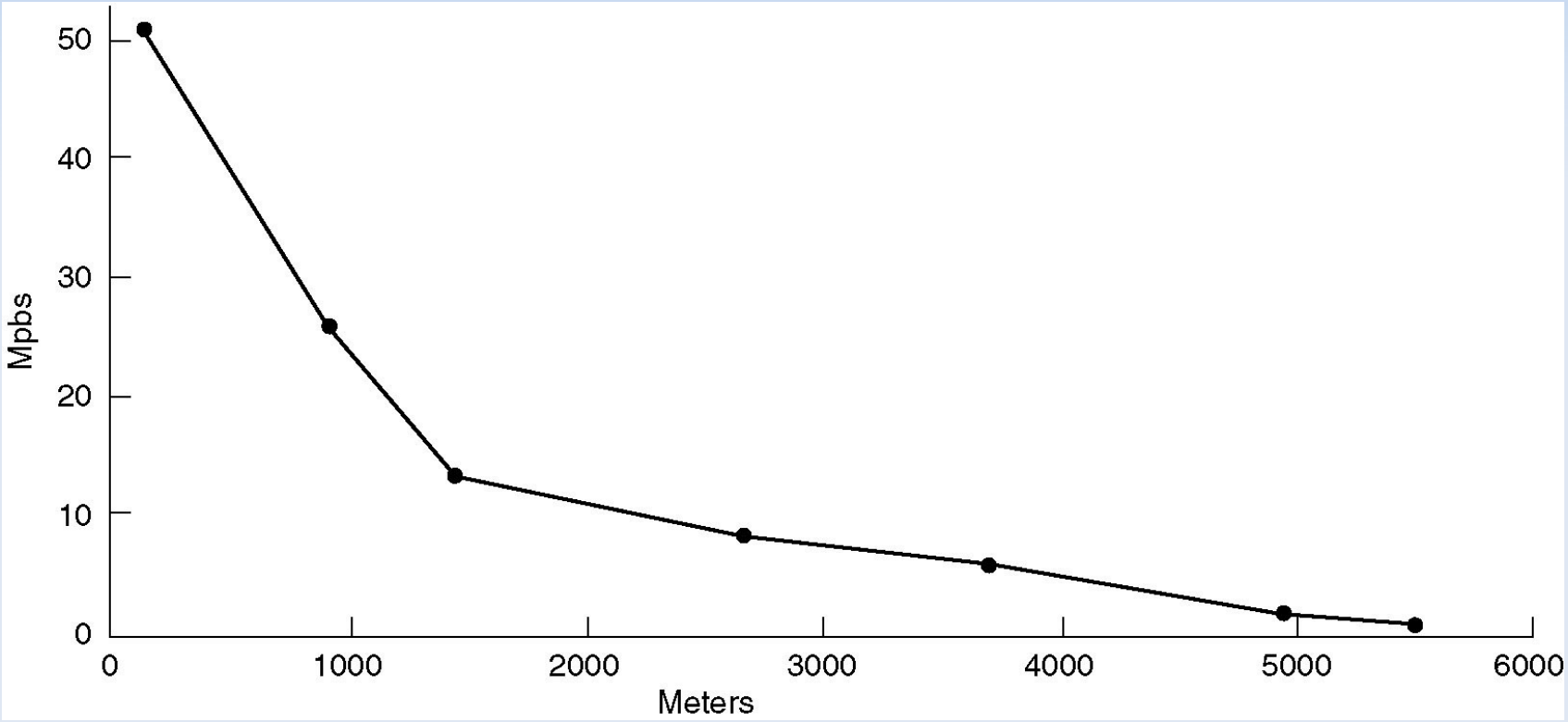
Exemple de l'ADSL 1

ADSL

- Quel débit descendant pour l'ADSL 1 ?
  - ex. : QAM-250, 224 canaux descendants, 4000 bauds
- Solution
  - 15 bits par modulation en QAM-250
  - débit théorique = 15 * 4000 * 224 = 12 Mbit/s
- Débits descendants réels
  - ADSL 1 : jusqu'à 8 ou 12 Mbit/s
  - ADSL 2+ : jusqu'à 24 Mbit/s

ADSL

- Atténuation du débit en fonction de la distance...

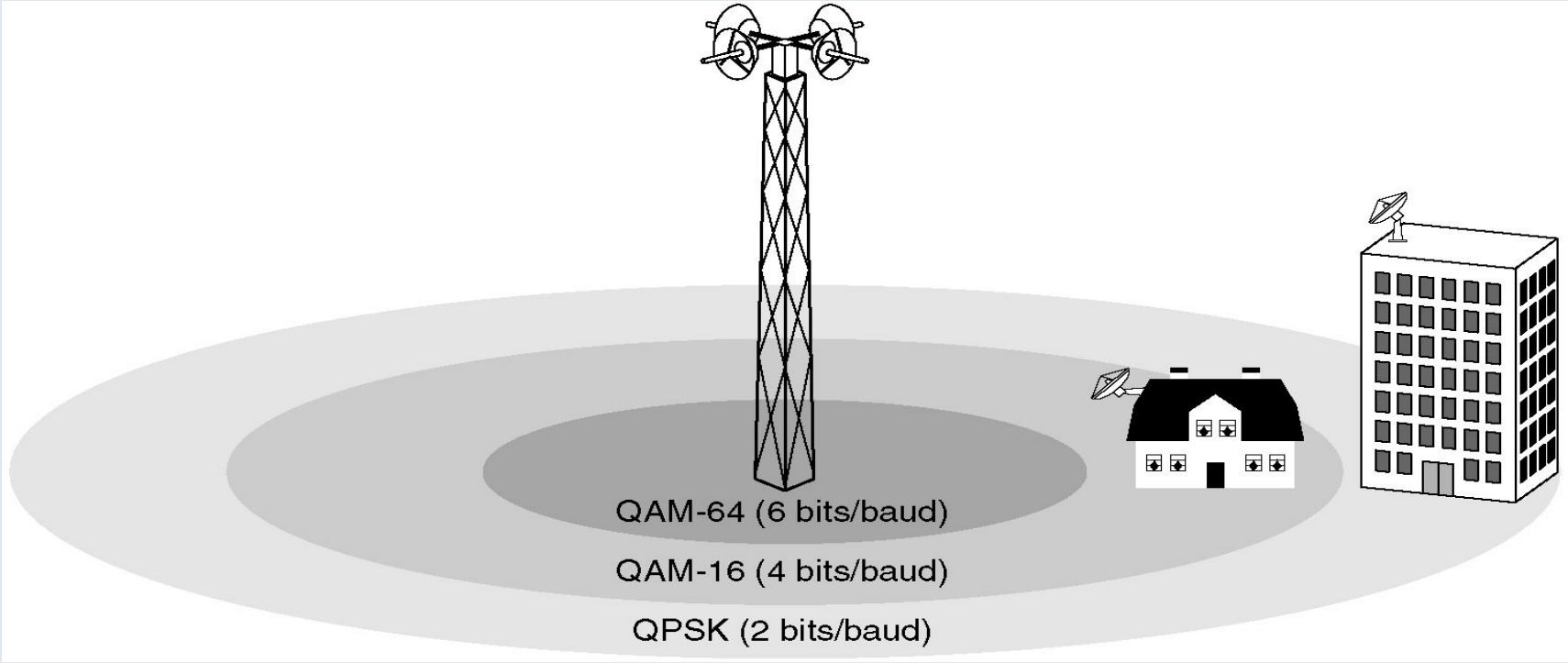


Wi-Fi (IEEE 802.11)

- Norme IEEE 802.11b : la plus répandue (oct. 1999)
  - différents débits : 1 Mbit/s – 11 Mbit/s
  - débit théorique max. 11 Mbit/s
    - en réel 6 Mbit/s (TCP/IP) pour une portée de 30 m
  - bande-passante [2.4 GHz - 2.5 GHz]
    - découpage en 13 canaux radio pour la France
- Multiplexage
  - cas du 1 Mbit/s
  - cas du 11 Mbit/s
    - modulation de phase QPSK (Quadrature Phase-Shift Keying)
    - CCK (Complementary Code Keying)

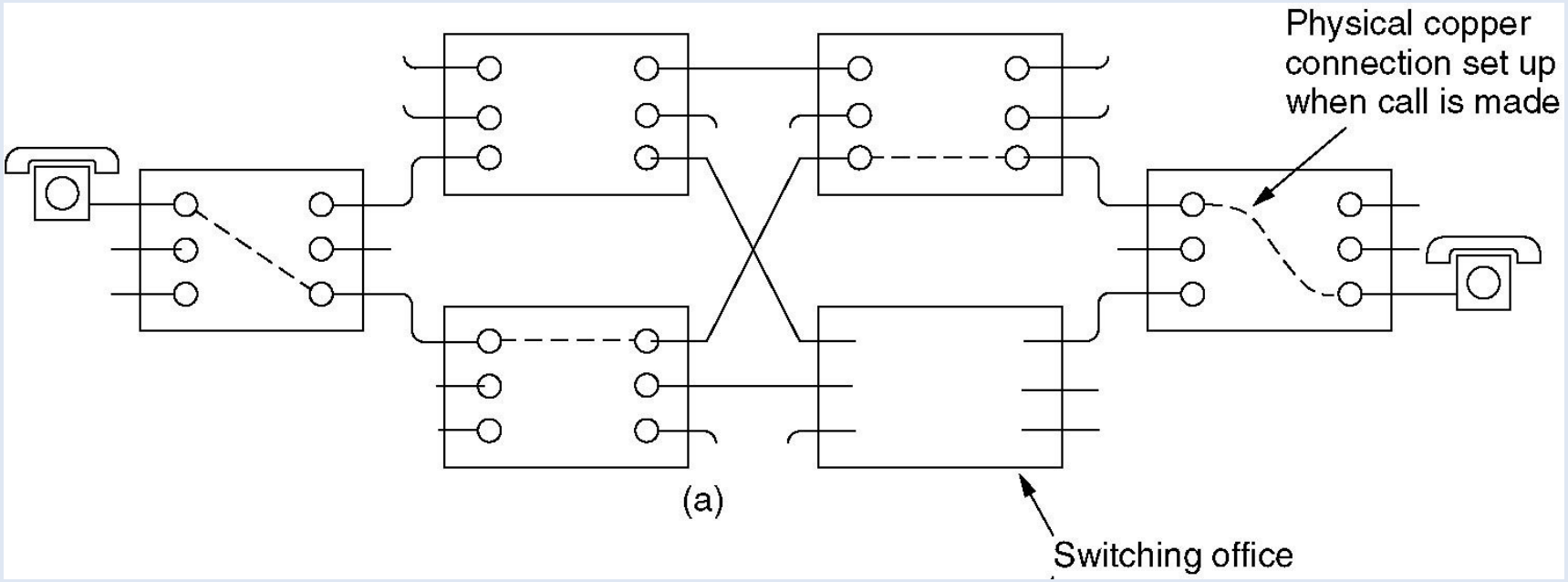
WiMax (IEEE 802.16)

- WiMax : Worldwide Interoperability for Microwave Access (déc. 2001)
  - théorique 70 Mbit/s, 112 km
  - réel 10 Mbit/s, 10 km



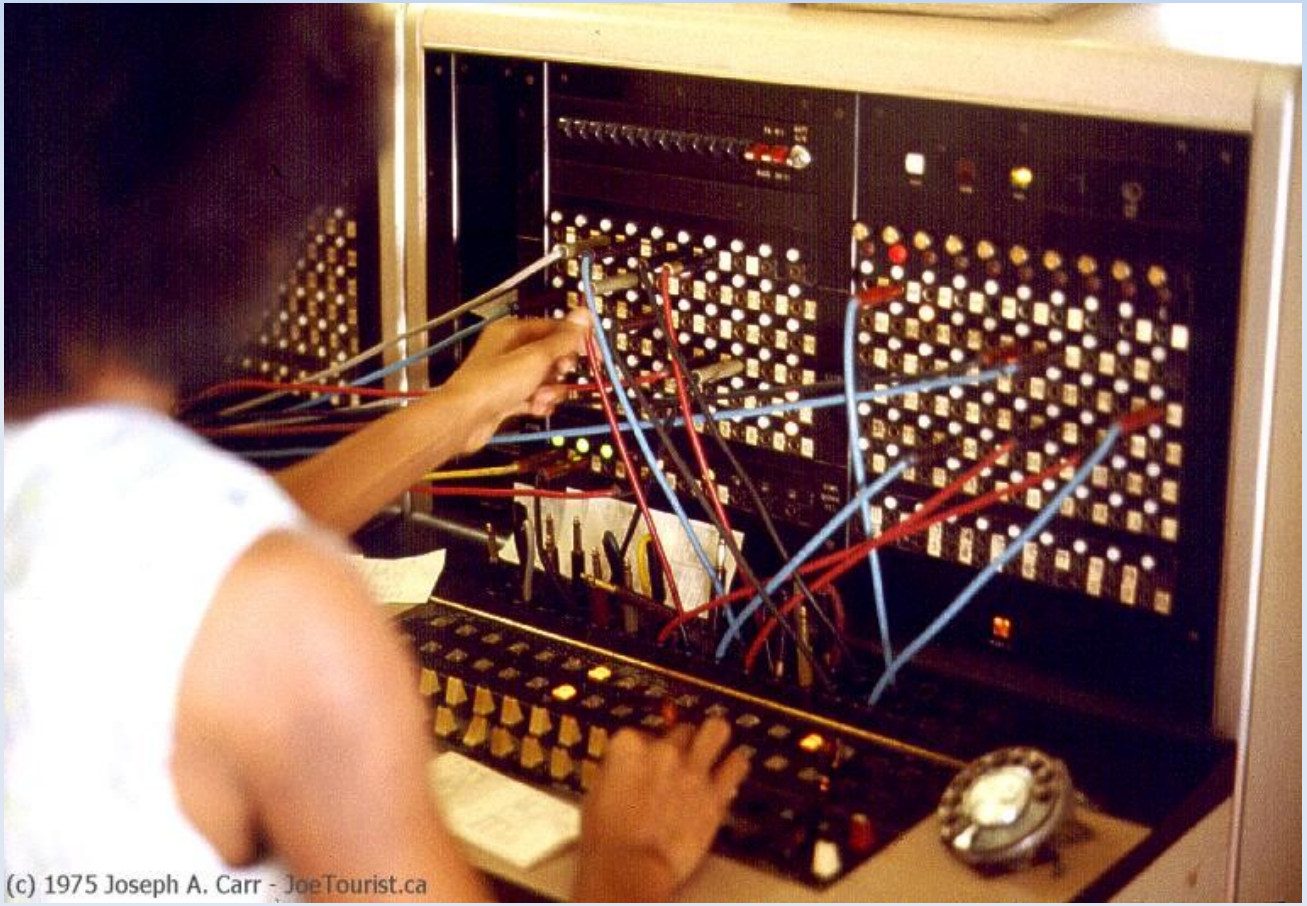
Commutation

- Commutation de circuit dans le réseau téléphonique
  - boucle locale, artère principale
  - centres d'informations (les commutateurs)
  - lors d'un appel, établissement d'une connexion physique



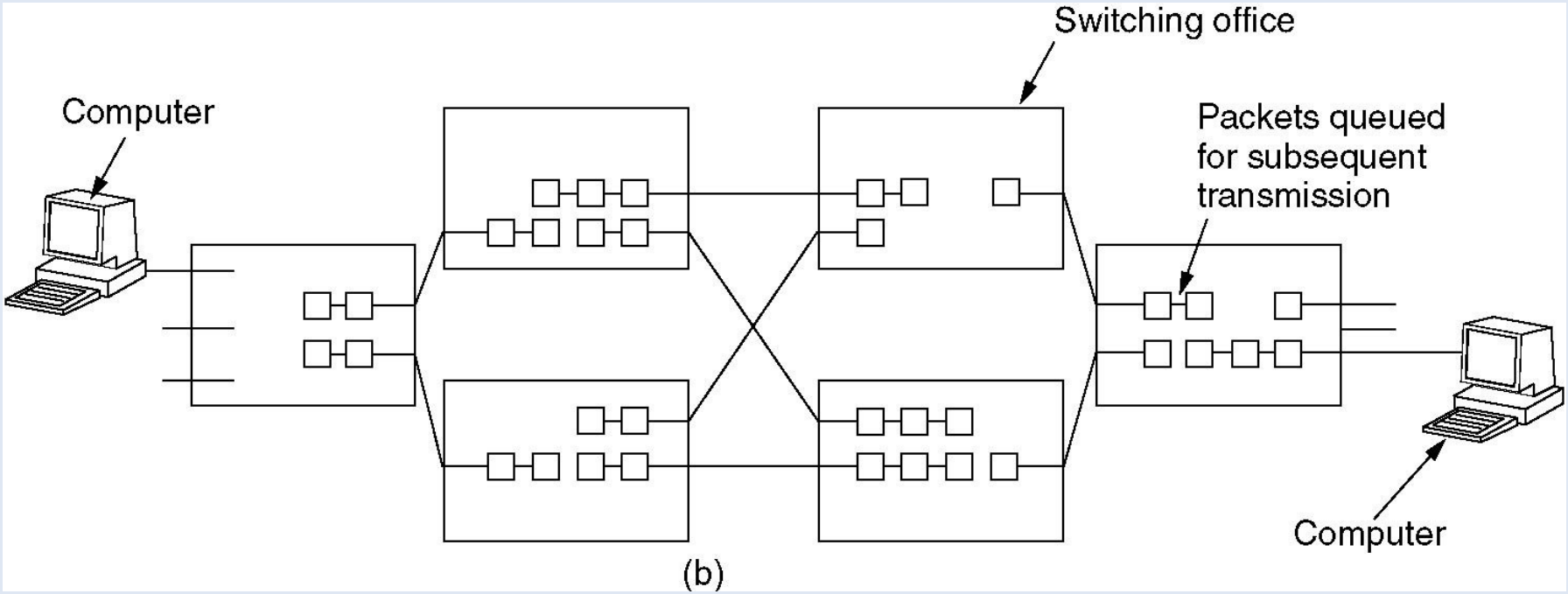
Commutation

- “à la main...”



Commutation

- Commutation de paquets
  - routage de paquets dans un réseau informatique
  - commutateurs = routeurs qui font transiter les paquets de proche en proche vers le destinataire



Annexes

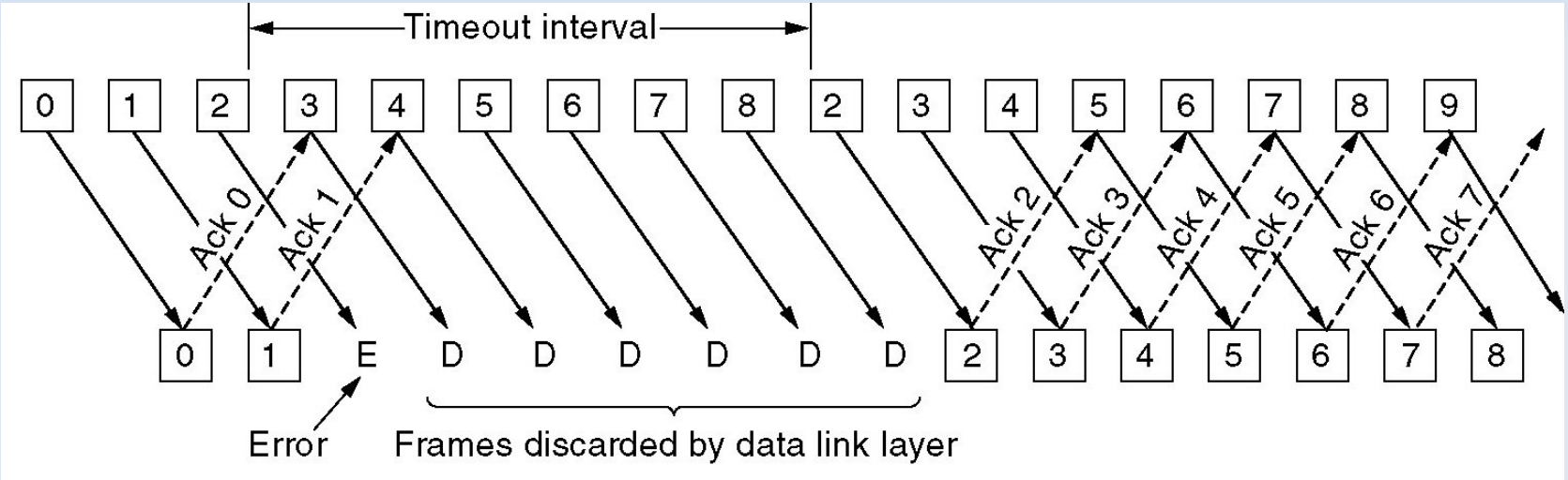
Divers

Contrôle de flux

- Protocole n° 3 à fenêtre de largeur *n*
  - Afin d'améliorer l'efficacité du canal, on décide d'envoyer *n* trames avant de s'arrêter pour attendre le premier acquittement.
  - Utilisation d'une fenêtre d'émission et d'une fenêtre de réception jouant le rôle de tampon
  - Difficultés
    - Après une erreur détectée à la réception, que faire des trames suivante reçues même correctes ?
    - On rappelle que la couche liaison doit remettre les paquets à la couche réseau en respectant l'ordre d'émission...

Contrôle de flux

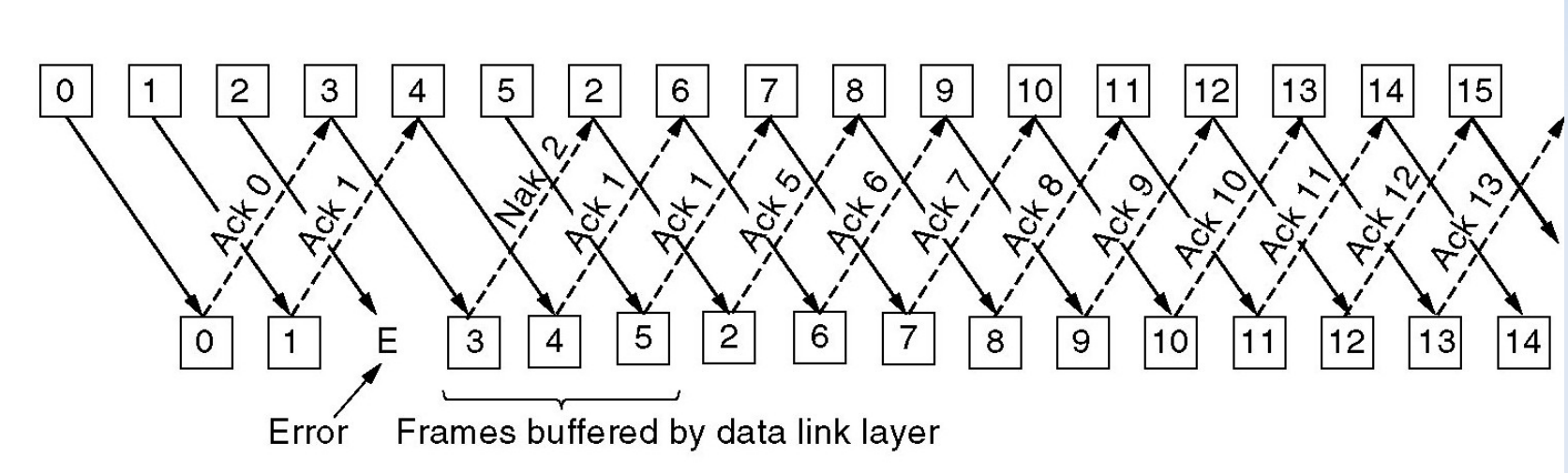
- Fenêtre de réception et rejet global
  - à la réception, on rejette toutes les trames suivant une trame éronnée



  - cela revient à n'accepter que la trame qu'il faut remettre à la couche réseau (i.e. fenêtre de réception de taille 1)

Contrôle de flux

- Fenêtre de réception et rejet sélectif
  - la fenêtre de réception permet de placer les trames reçues dans un tampon avant de les transmettre à la couche réseau



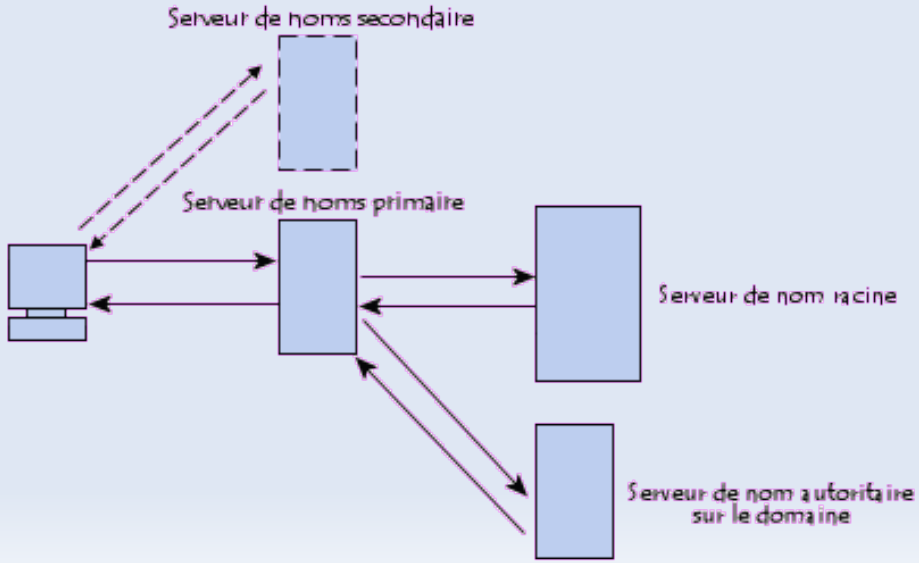
  - Le récepteur bloque sur Ack 1, tant qu'il n'a pas reçue la trame 2 et peut acquiter d'un coup plusieurs trames reçues (Ack 5)
  - le Nak accèlére la retransmission d'une trame spécifique en évitant d'attendre un timeout côté émetteur

DNS

- Domain Name System (DNS)
  - Système permettant d'établir une correspondance entre une adresse IP (numérique) et un nom de domaine
  - Ensemble de serveurs DNS répartis, qui ne possède chacun qu'une connaissance restreinte...
  - Serveur DNS primaire ayant authorité sur le domaine
  - Serveur DNS secondaire : DNS cache du FAI qui permet d'accélérer les résolutions mais n'est pas forcément à jour !
- Les domaines
  - génériques : .com, .edu, .net, .org, .int, .gov, .mil, .arpa (transition ARPAnet)
  - géographiques : .us, .fr, ...

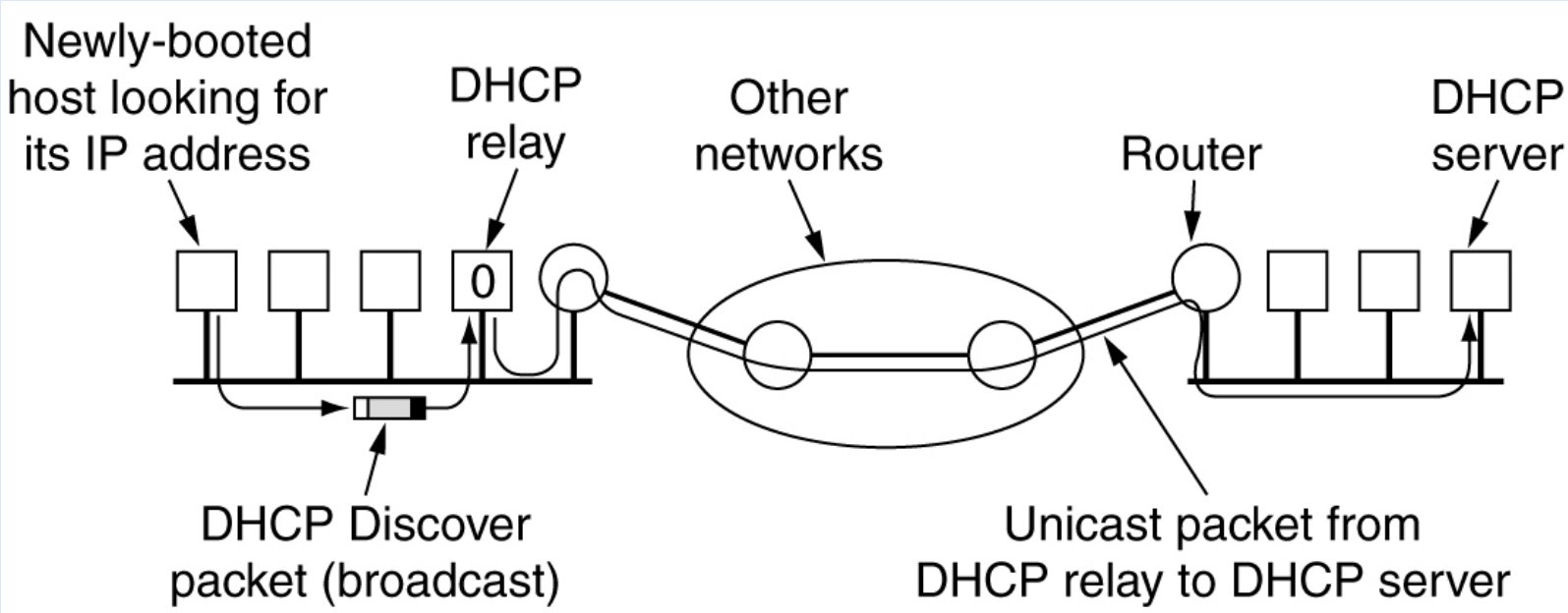
DNS

- Principe de résolution d'un nom de domaine (resolve)
  - Interrogation du serveur DNS de votre FAI pour trouver l'adresse IP de *fr.wikipedia.org*
  - Demande à un serveur DNS racine les serveurs DNS connaissant la zone *org*
  - Puis, on interroge un de ces serveurs pour obtenir l'adresse d'un nouveau serveur DNS connaissant la zone *wikipedia.org*, et ainsi de suite jusqu'à trouver *fr.wikipedia.org*



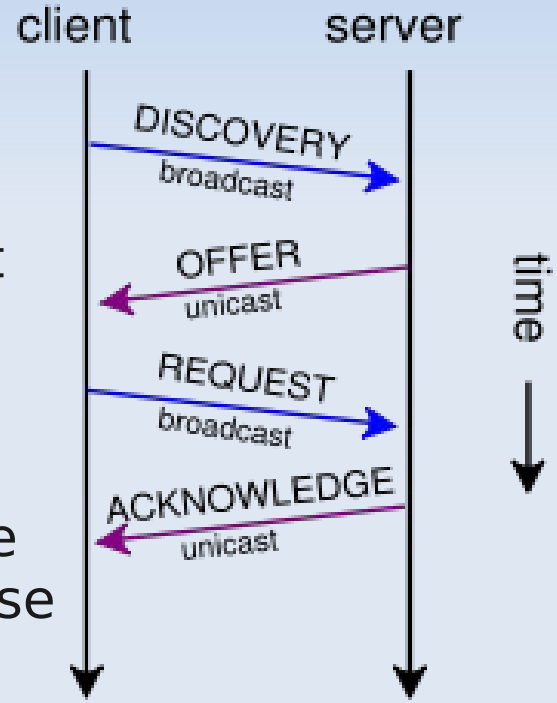
DHCP

- Dynamic Host Configuration Protocol (DHCP), RFC 2132
  - pour surmonter les difficultés de l'adressage statique
  - assignation dynamique d'une adresse IP et d'un masque de sous-réseau, configuration de la passerelle et du DNS
  - configuration centralisée par le serveur DHCP



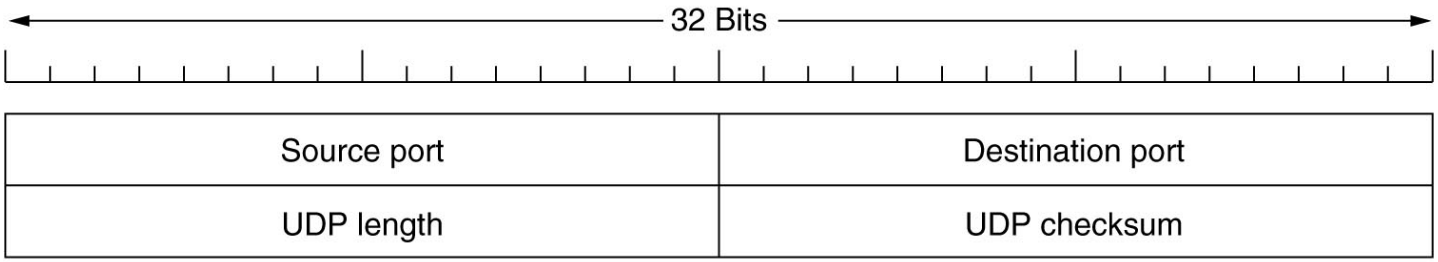
DHCP

- Principe
  - broadcast du client sur le port 67 d'un datagramme DISCOVERY (contenant son adresse MAC)
  - réponse d'un serveur DHCP au client (sur le port 68) d'un datagramme OFFER qui contient l'adresse IP du serveur, une proposition d'adresse IP pour le client, ...
  - le client retient la première offre reçue en répondant à tout le monde (broadcast) avec le datagramme REQUEST qui contient son adresse IP et celle du serveur DHCP choisi
  - le serveur envoi un accusé de réception (ACK)



UDP

- User Datagram Protocol (UDP)
  - sans connexion, numéro de port comme TCP
  - pas de contrôle de flux, de contrôle d'erreurs, de retransmission
  - transfert simple et rapide, mais non fiable



- Applications d'UDP
  - RTP (Real-time Transport Protocol), DNS, ...

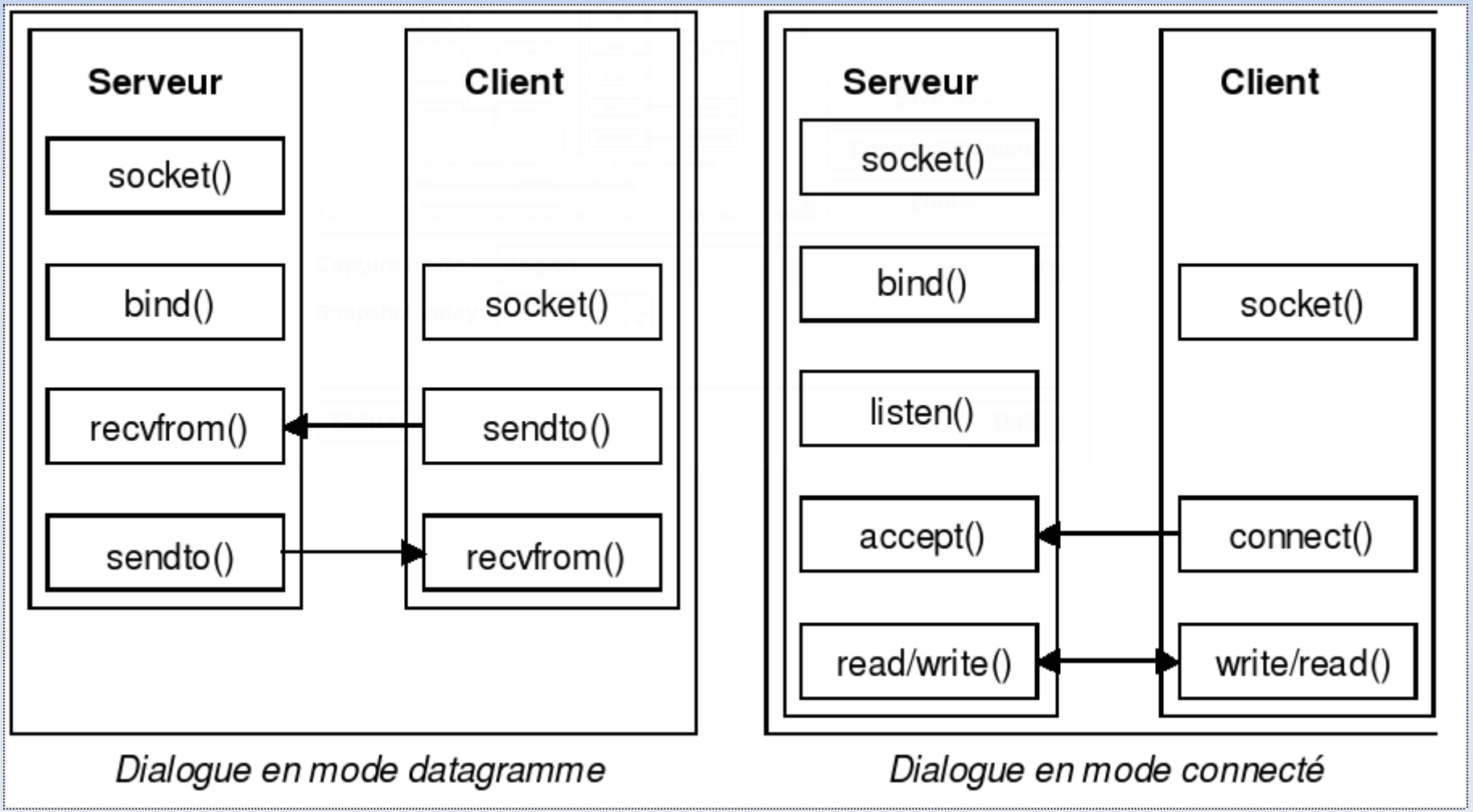
Les Sockets

- Les primitives Unix (Berkeley)
  - permettent l'établissement, l'utilisation et la libération de connexions

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Les Sockets

- TCP ou UDP



Programmation avec Socket

- Voir en TP...

Configuration IP

- ifconfig : configuration des interfaces réseaux

```
eth0      Link encap:Ethernet  HWaddr 00:15:C5:3D:52:B6
          inet addr:82.225.96.37  Bcast:82.225.96.255  Mask:255.255.255.0
          inet6 addr: fe80::215:c5ff:fe3d:52b6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6898 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7893 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1395845 (1.3 MiB)  TX bytes:944079 (921.9 KiB)
          Interrupt:185

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100 (100.0 b)  TX bytes:100 (100.0 b)
```

Table de routage

- route ou nestat -rn (liste la table de routage)

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
82.225.96.0	*	255.255.255.0	U	0	0	0	eth0
default	82.225.96.254	0.0.0.0	UG	0	0	0	eth0

Traceroute

- traceroute www.google.fr

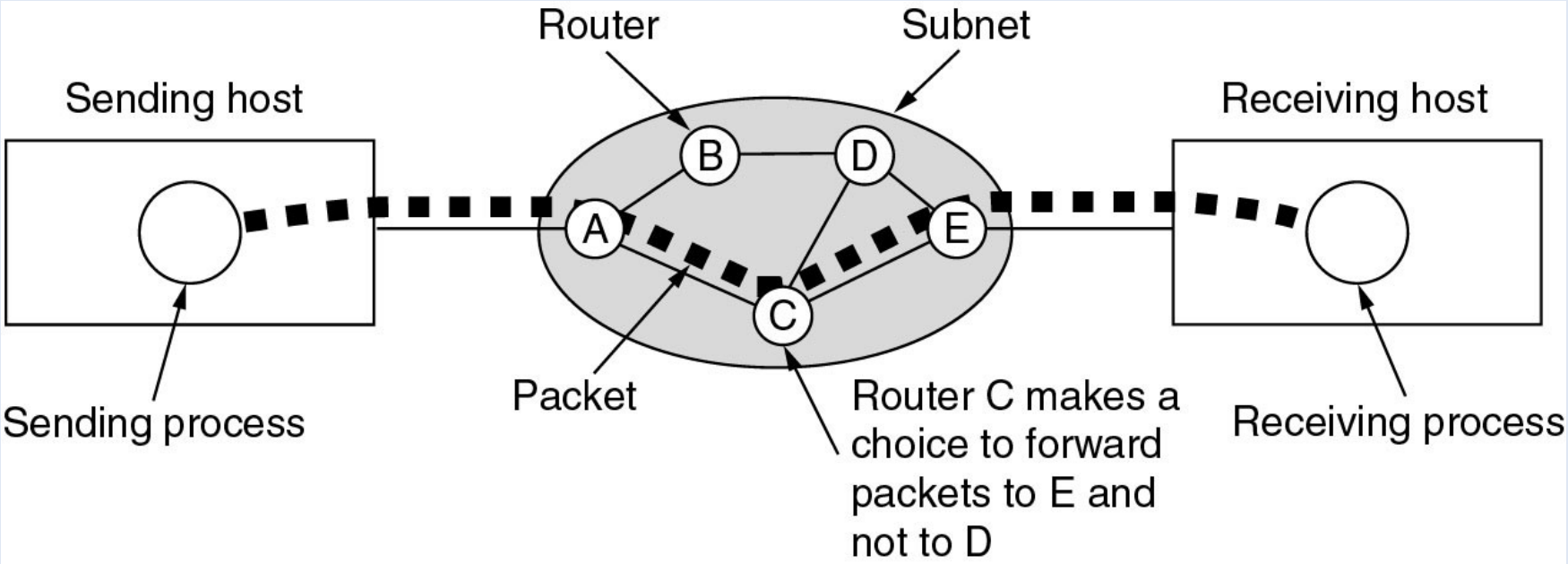
```
traceroute to www.l.google.com (209.85.129.104), 30 hops max, 40 byte packets
 1  82.225.96.254 (82.225.96.254)  26.164 ms  26.134 ms  25.874 ms
 2  * 213.228.9.190 (213.228.9.190)  26.394 ms  26.590 ms
 3  * * *
 4  * ldc-6k-1-po20.intf.routers.proxad.net (212.27.51.10)  35.513 ms *
 5  google.freeix.net (213.228.3.136)  35.258 ms  49.203 ms  36.452 ms
 6  72.14.233.105 (72.14.233.105)  49.734 ms  50.936 ms  50.293 ms
 7  72.14.232.203 (72.14.232.203)  50.213 ms  50.587 ms  50.265 ms
 8  72.14.233.210 (72.14.233.210)  50.706 ms  50.911 ms  55.020 ms
 9  fk-in-f104.google.com (209.85.129.104)  52.185 ms  50.159 ms  51.891 ms
```

Routage

- Principe
  - Mécanisme par lequel le message d'un expéditeur est acheminé jusqu'à son destinataire, même si aucun des deux ne connaît le chemin complet que le message doit suivre...
- Deux types logiques d'ordinateur dans le WAN
  - les terminaux, ou hôtes, qui sont reliés à un seul réseau et qui ont par conséquent une table de routage simple
  - les routeurs, qui relient au moins deux réseaux et possède une table de routage plus complexe

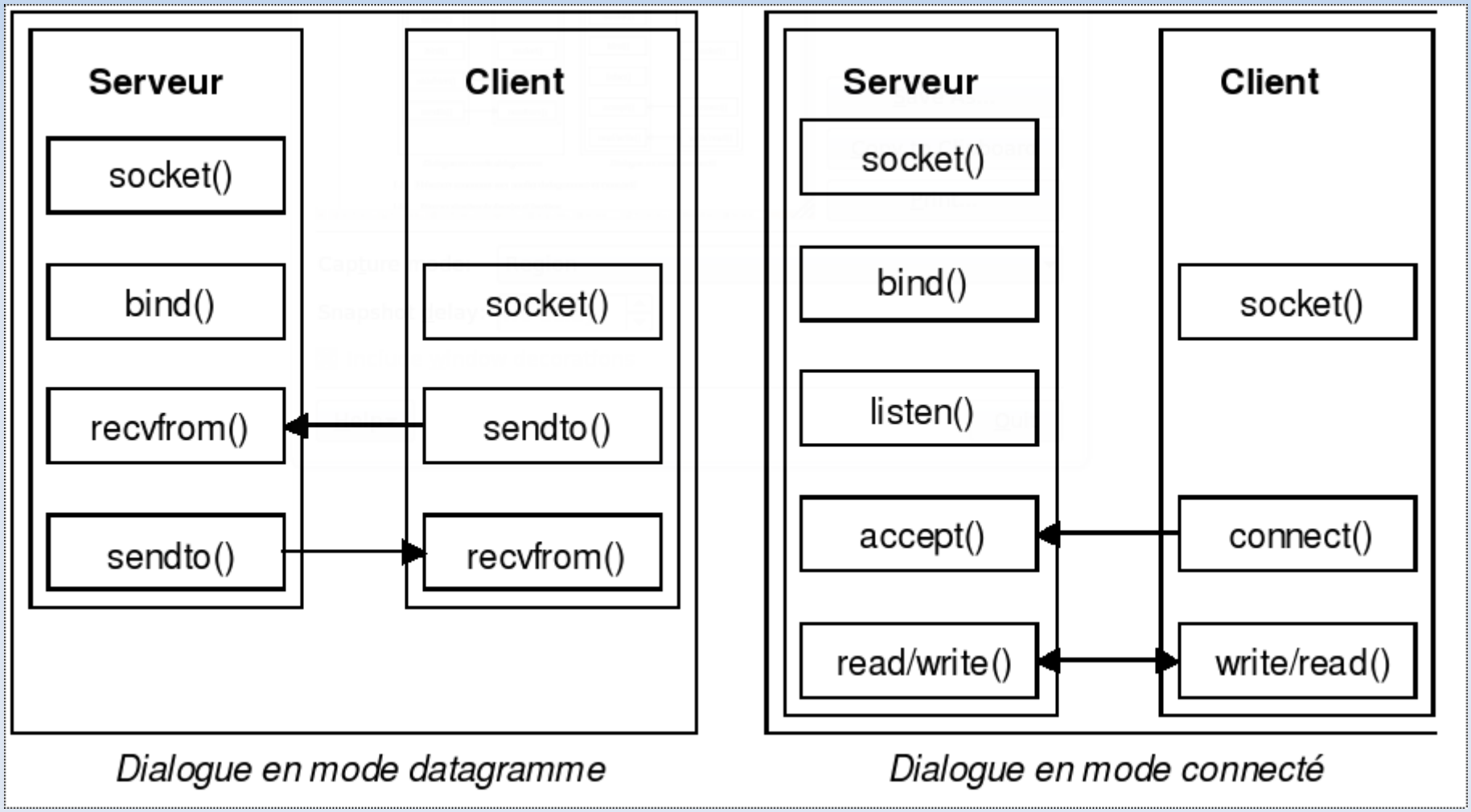
Routage

- Routage statique vs dynamique
  - statique
  - dynamique



Les sockets...

- Mode non connecté (UDP) et connecté (TCP)



Modèle peer-to-peer

- Dans le modèle P2P, il n'y a pas de serveur et de clients fixés...