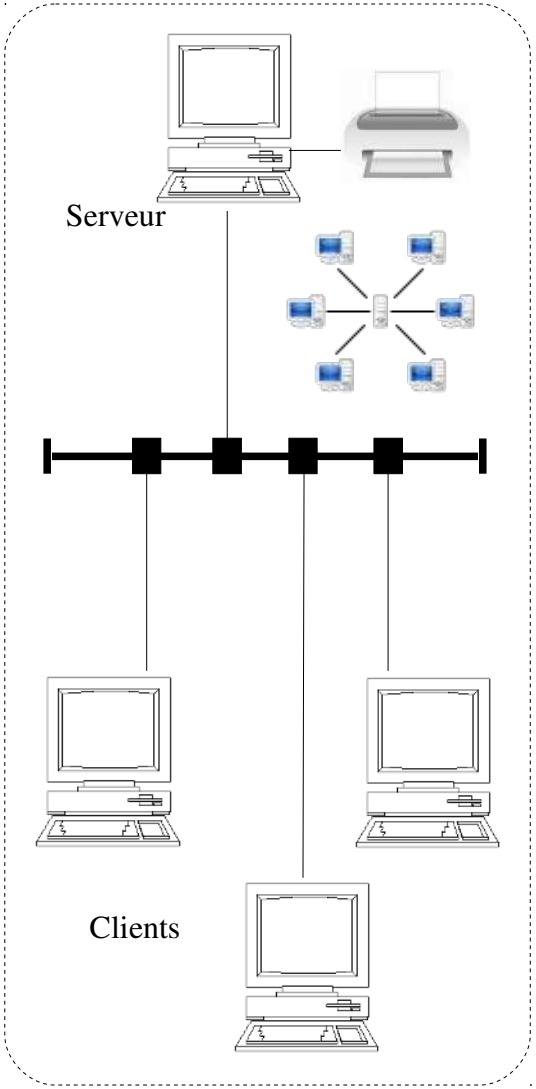
Réseaux

« En 1962, pour chacun des trois terminaux, j'avais trois jeux différents de commandes. Si bien que si j'étais en train de parler en direct avec quelqu'un à Santa Monica et que je voulais discuter de ça avec quelqu'un que je connaissait à Berkeley ou au MIT, il fallait que je me lève de devant le terminal, que j'aille m'enregistrer sur l'autre terminal afin d'entrer en contact avec eux.
Je me suis dit, hé, mec, ce qu'il me reste à faire est évident : au lieu d'avoir ces trois terminaux, il nous faut un terminal qui va partout où tu veux et où il existe un ordinateur interactif.
Cette idée était l'ARPAnet. »
Robert Taylor, co-auteur avec J.C.R. Licklider de The Computer as a Communications Device

Besoins

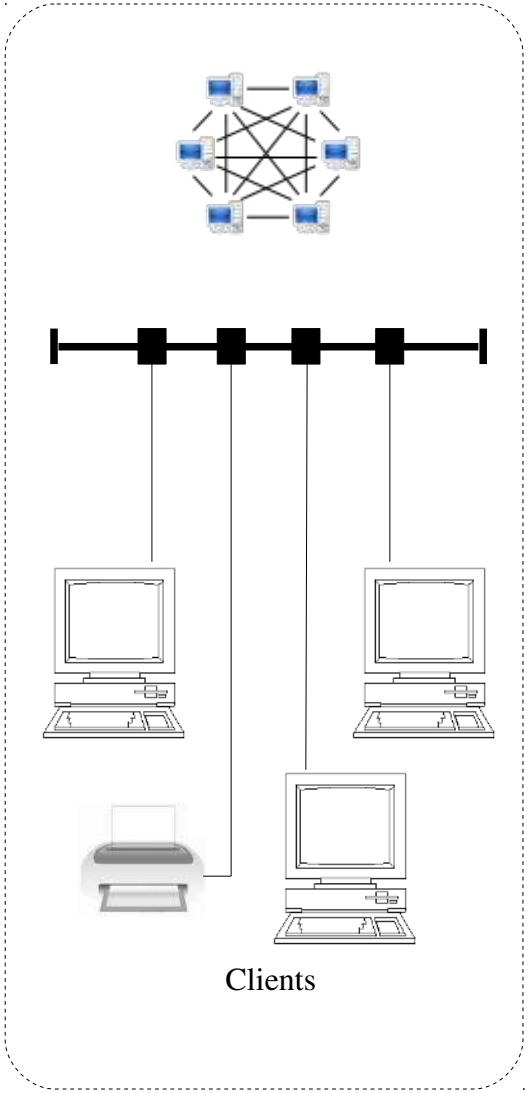
- La solution réseau permettra ***l'optimisation des ressources matérielles et logicielles*** par :
  - Le ***partage***
    - de ressources : imprimante, espace disque, *modem*, ...
    - d'informations : transfert des fichiers, ...
  - La ***centralisation***
    - des données : espace centralisé et sécurisé (base de données),
    - des services : messagerie, ...
- Et en :
  - assurant les tâches de gestion et de production
  - assurant une rapide et fiable circulation des informations
  - respectant les contraintes des implantations géographiques

Architecture réseau



L'architecture client/serveur centralise des ressources sur un serveur et offre des services pour les clients.

Les systèmes poste à poste ou pair-à-pair (*peer-to-peer*) permettent de partager simplement des objets (des fichiers le plus souvent, mais aussi des flux multimédia continus (streaming), le calcul réparti, ...).
Les systèmes *peer-to-peer* permettent une décentralisation des systèmes, en permettant à tous les ordinateurs de jouer le rôle de client et de serveur.



Définitions

- Un ***réseau*** est un ensemble d'équipements informatiques interconnectés

- Un ***réseau*** s'appuie sur deux notions :
  - L'***interconnexion*** : transmettre les données d'un nœud à un autre
  - La ***communication*** : échanger des des données entre processus (un programme en cours d'exécution)

- Un ***réseau*** désigne un ensemble d'équipements matériels et logiciels mis en oeuvre pour permettre la communication entre applications, quelles que soient les distances qui les séparent.

Types de réseaux

- Les réseaux locaux ou **LAN** (*Local Area Network*) qui correspondent aux réseaux intra-entreprise (quelques centaines de mètres et n'exèdent pas quelques kilomètres), généralement réseaux dits "privés".
- Les réseaux **MAN** (*Metropolitan Area Network*) sont des réseaux s'étendant sur une ville et permettant l'usage de très hauts débits
- Les réseaux grandes distances ou **WAN** (*Wide Area Network*), réseau étendu, généralement réseaux dits "publics" (opérateurs publics ou privés), et qui assurent la transmission des données sur des longues distances à l'échelle d'un pays ou de la planète.
- Autres dénominations connues : PAN (*Personal Area Network*), WPAN et WLAN (*Wireless* ...), SAN (*Storage Area Network*), ...

Éléments d'un réseau

- Les ordinateurs équipées d'une carte de communication
- Les logiciels
  - navigateur, client de messagerie, serveur web, …
- Les supports
  - de LAN : câbles paires cuivre torsadées, prises RJ45, WIFI, CPL, ...
  - de WAN : ligne téléphonique, ADSL, fibre optique, …

- Les équipements d'interconnexion
  - de LAN : répéteur (*transceiver*), concentrateur (*hub*), commutateur (*switch*)
  - de WAN : routeur

Caractéristiques

- La **topologie** définit l'architecture d'un réseau : on distinguera la topologie physique (qui définit la manière dont les équipements sont reliés entre eux, de la topologie logique (qui précise la manière dont les équipements communiquent entre eux) :
  - par exemple, une topologie logique en bus (Ethernet 10BASET) pourra se câbler avec une topologie physique en étoile (*hub*).

- Le **débit** mesure une quantité de données numériques (bits) transmises par seconde (bit/s ou bps).

- La **distance maximale** (ou portée), qui différencie essentiellement les LAN et WAN, dépend de la technologie mise en oeuvre :
  - WIFI 802.11g (54 Mbps – environ 50 m), Ethernet paires torsadées 100BASET (100 Mbps – 100 m) et fibre optique 100BASEFX (100 Mbps – 2 km)

La communication en réseau

- Les échanges de données sont basés sur une communication ***logique***.

- Les communications dans un réseau obéissent à des règles :

  - l'***adressage*** qui permet d'identifier de manière unique les deux unités en communication

  - l'***architecture*** qui définit les rôles endossés par les deux unités

  - les ***protocoles*** qui assurent l'échange des données

Topologie

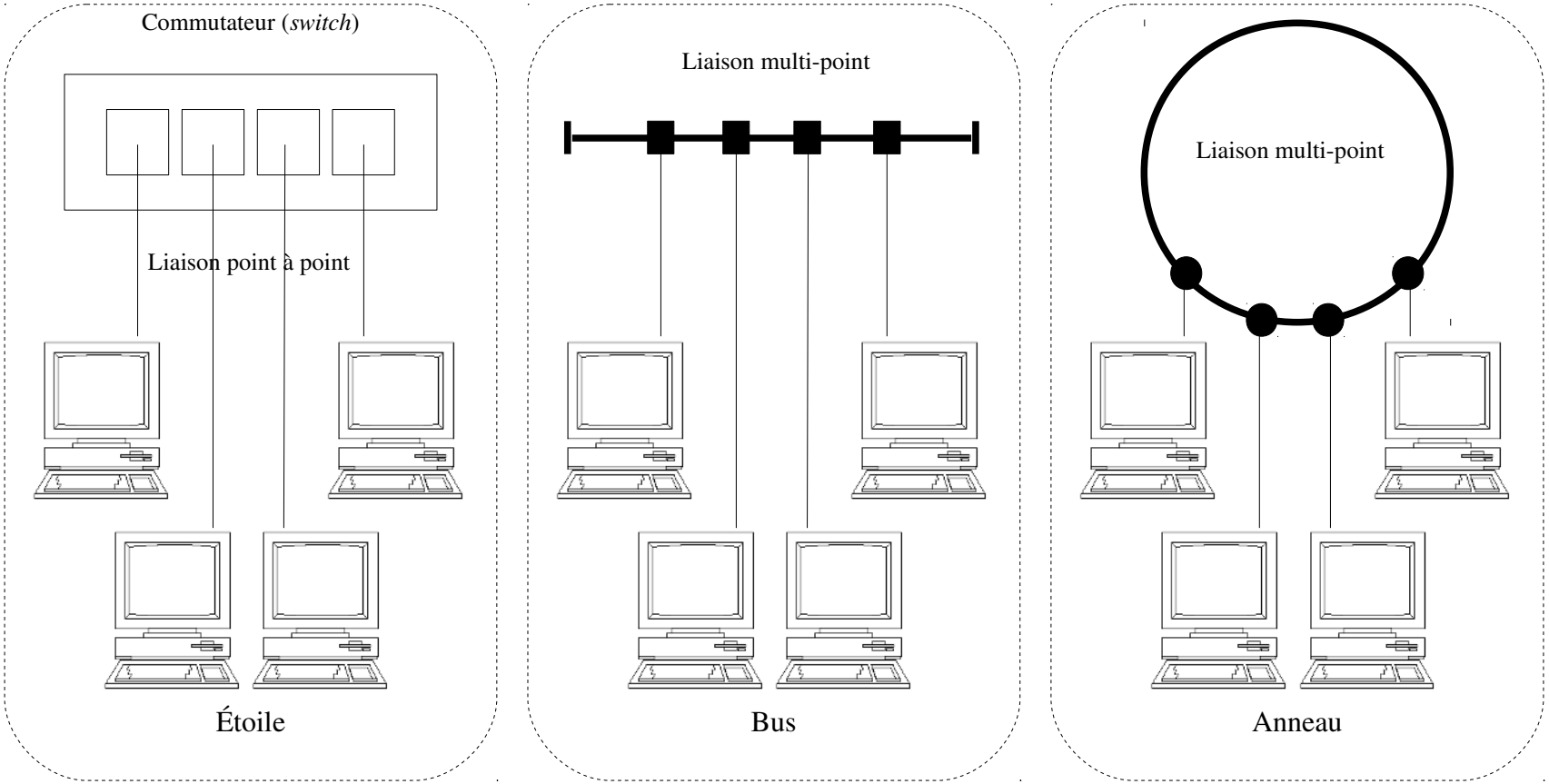
- Il existe 2 modes de diffusion classant les différentes topologies :
  - **MODE MULTI-POINT**
    - (exemple : topologie en bus ou en anneau)

      Ce mode de fonctionnement consiste à n'utiliser qu'un seul support de transmission. Le principe est que le message est envoyé sur le réseau, toute unité réseau est capable de voir le message et d'analyser selon l'adresse du destinataire si le message lui est destiné ou non.
  - **MODE POINT A POINT**
    - (exemple : topologie en étoile, arbre ou maillée)

      Dans ce mode, le support physique ne relie qu'une paire d'unités seulement. Pour que deux unités réseaux communiquent, elles passent obligatoirement par un équipement d'interconnexion (un routeur ou un commutateur).

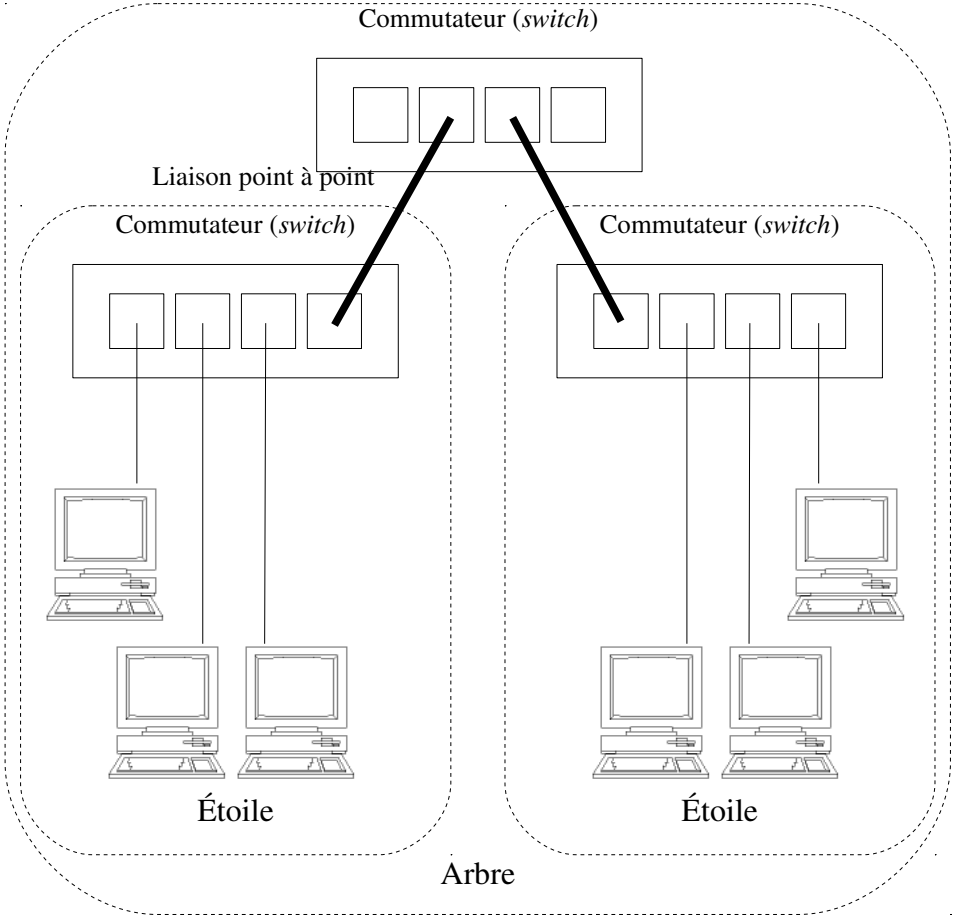
Topologies (I)

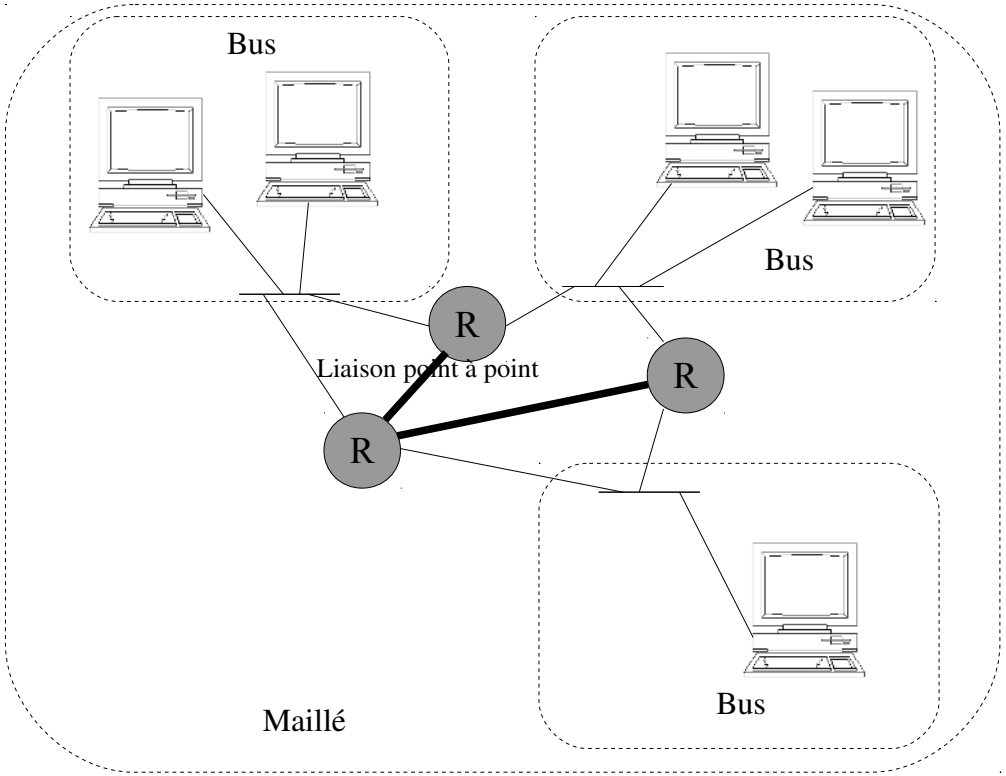
- Certaines topologies sont plus adaptées aux LAN (bus, anneau, étoile), d'autres aux WAN (maillé).



Topologies (II)

- Certaines topologies (arbre, maillé) sont plus adaptées pour interconnecter des LAN entre eux.

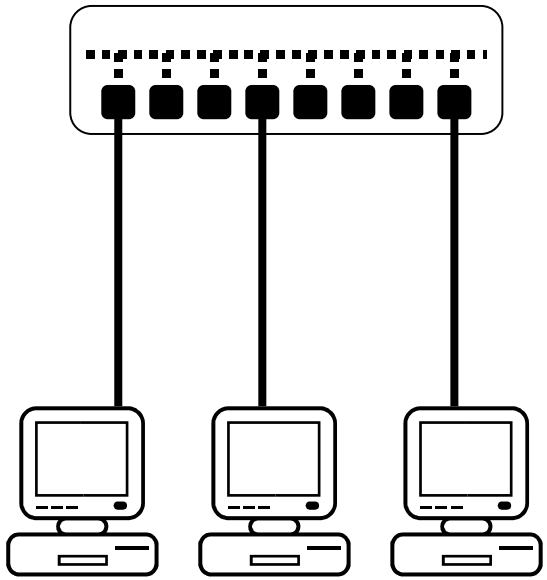




Câblage étoile

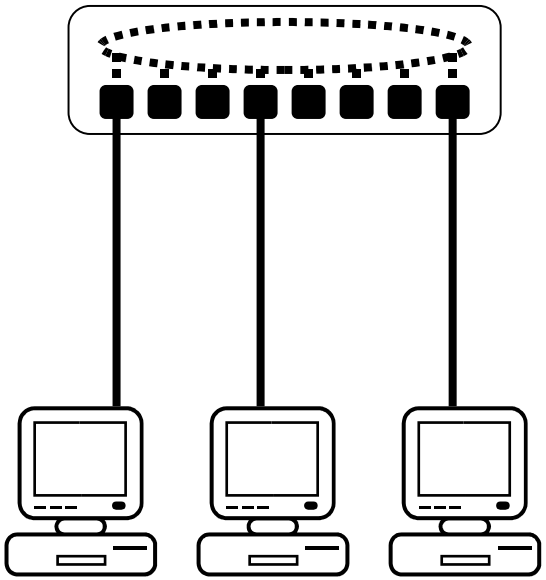
- Un concentrateur (*hub*) est un dispositif électronique permettant de créer un réseau informatique local de type Ethernet. Cet appareil permet la connexion de plusieurs équipements sur une même ligne de communication, en régénérant le signal, et en répercutant les données émises par l'un vers tous les autres.

Concentrateur
HUB



Topologie en **BUS**
ETHERNET 10/100BASET

Concentrateur
MAU



Topologie en **ANNEAU**
TOKEN RING

Les protocoles

- Rendent possible le dialogue entre des machines différentes

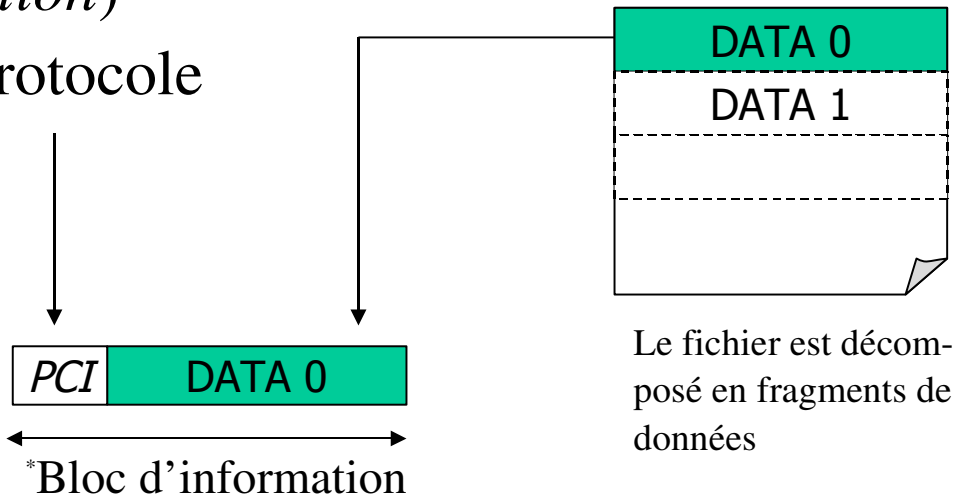
- Un protocole de communication définit l'ensemble des procédures (ou règles) pour réaliser une communication :

  - Le dictionnaire : les primitives (demande connexion, acquittement, ...)
  - Le scénario du dialogue : enchaînement des primitives (diagramme de l'échange)
  - Les modalités : taille et représentation des informations, temps d'attente, etc …
  - Les messages échangés : les différents champs (taille et contenu)

Protocole de communication

PCI (*Protocol Control Information*)
En-tête (*header*) ajouté par le protocole réseau

Il sera décodé
par le récepteur, qui doit
donc posséder le même
protocole réseau.

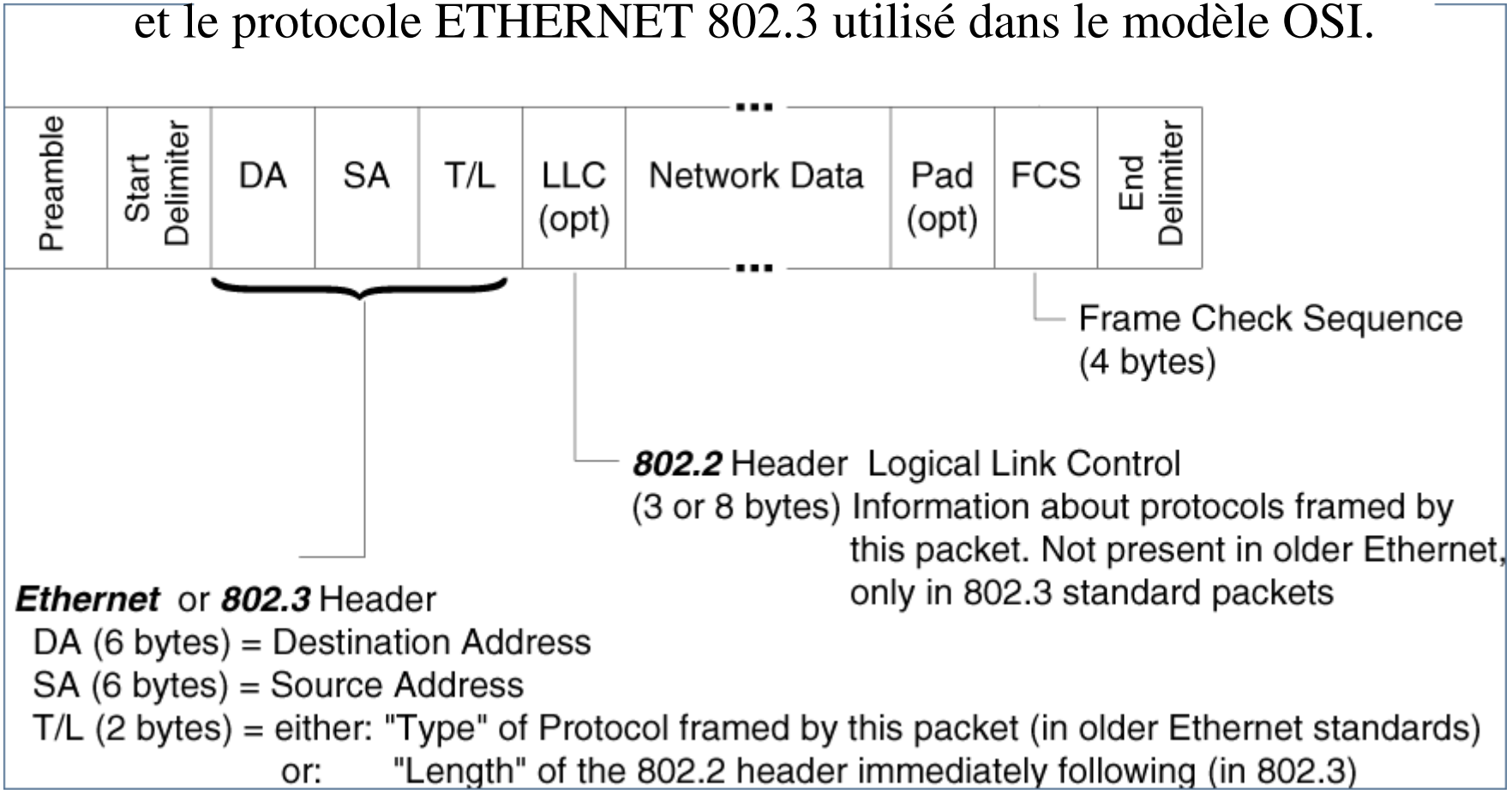


Un protocole réseau définit :
- le contenu détaillé du PCI
- la taille du bloc d'information
- la manière de les échanger

*Termes couramment utilisés pour désigner un bloc d'information :
trame, **paquet**, **datagramme**, **segment**, **message**, **fragment**, …

Trames Ethernet

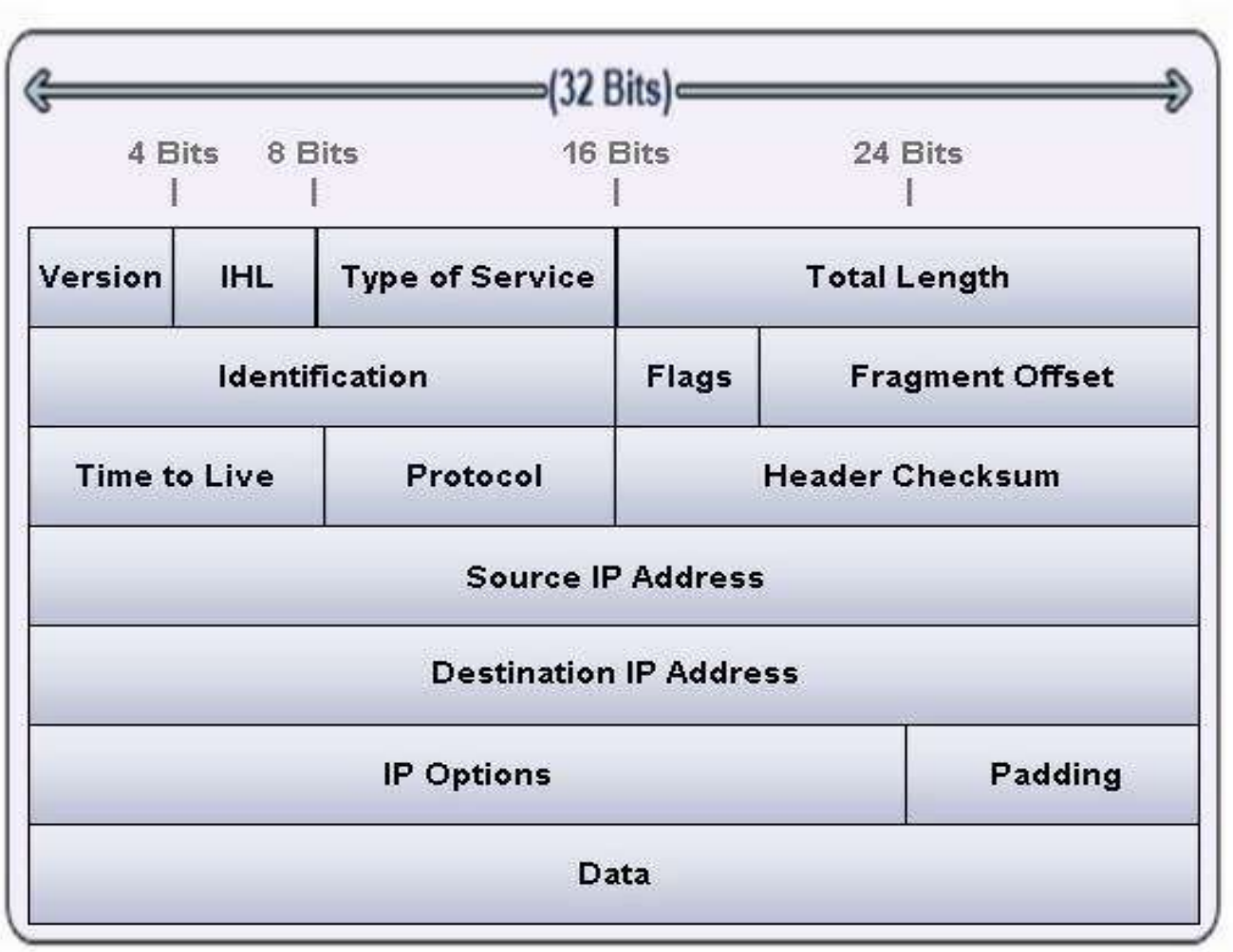
- On distinguera deux protocoles pour les trames Ethernet :
  le protocole ETHERNET_II, plus ancien et utilisé dans le modèle TCP/IP
  et le protocole ETHERNET 802.3 utilisé dans le modèle OSI.



Protocole IPv4

IP (*Internet Protocol*) représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée.

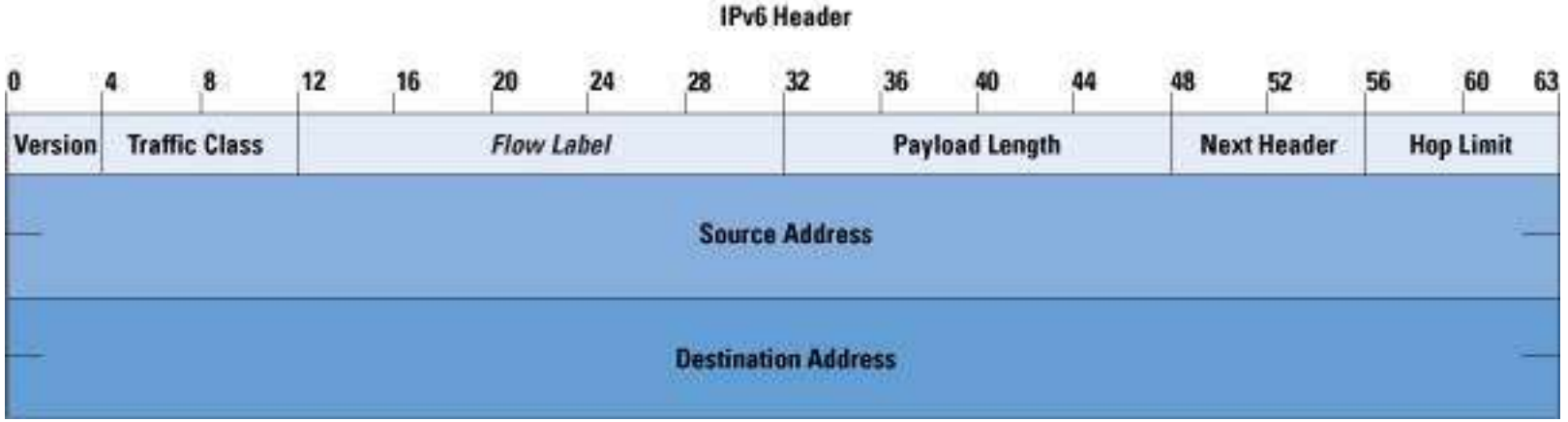
Ce protocole utilise ainsi la technique dite de commutation de paquets. Les détails du protocole IP sont spécifiés dans la RFC791.



Protocole IPv6

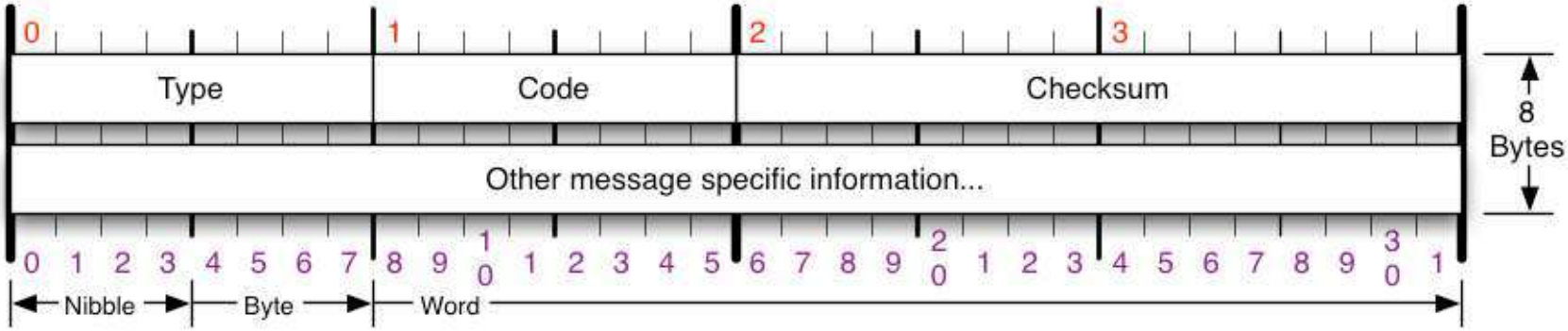
- Les différences avec IPv4 :
  - Les champs *Traffic Class* et *Flow Label* ont un rôle équivalent à TOS
  - Le champ *Hop Limit* remplace le champ TTL (64 par défaut)
  - Le champ *Next Header* permet un chaînage des options
  - Les adresses IP sources et destination sont codées sur 128 bits (soit 16 octets)

Le champ *Next Header* (NH) :
0 : option "Hop-by-Hop"
4 : IPv4
6 : TCP
17 : UDP
43 : option "Routing Header"
44 : option "Fragment Header"
45 : Interdomain Routing Protocol
46 : RSVP
50 : option "Encapsulation Security Payload" (IPsec)
51 : option "Authentification Header" (IPsec)
58 : ICMP
59 : No next header
60 : option "Destination Options Header"



Protocole ICMP

- ICMP (*Internet Control Message Protocol*) est un protocole de la couche Réseau qui transmet des message de contrôle et d'erreurs (RFC 792). Um message ICMP est encapsulé dans un paquet IP.



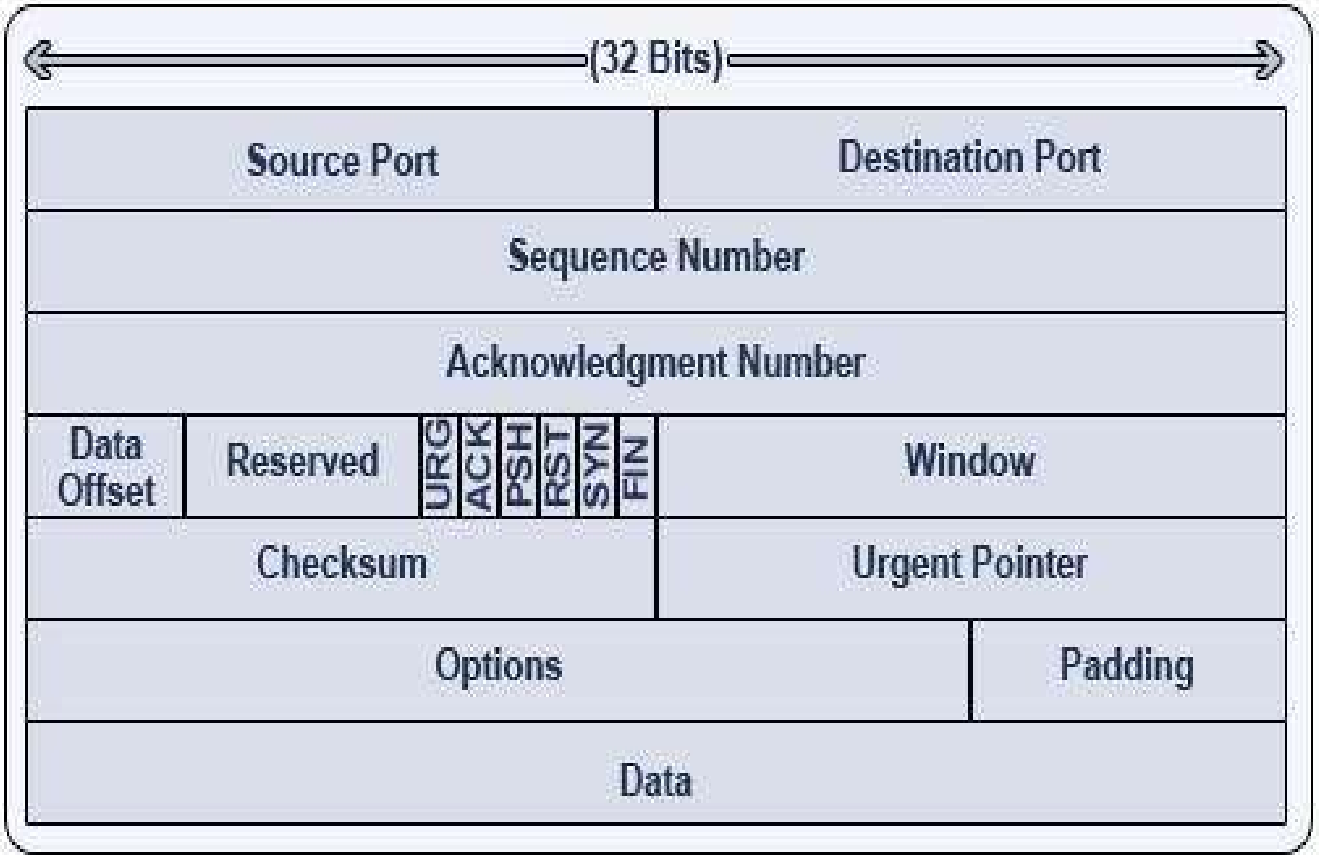
L'utilisation la plus connue du protocole ICMP est celle de la commande **ping** qui permet d'obtenir des informations (en particulier le temps de réponse de la machine à travers le réseau) et aussi quel est l'état de la communication avec cette machine.

ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Protocole TCP

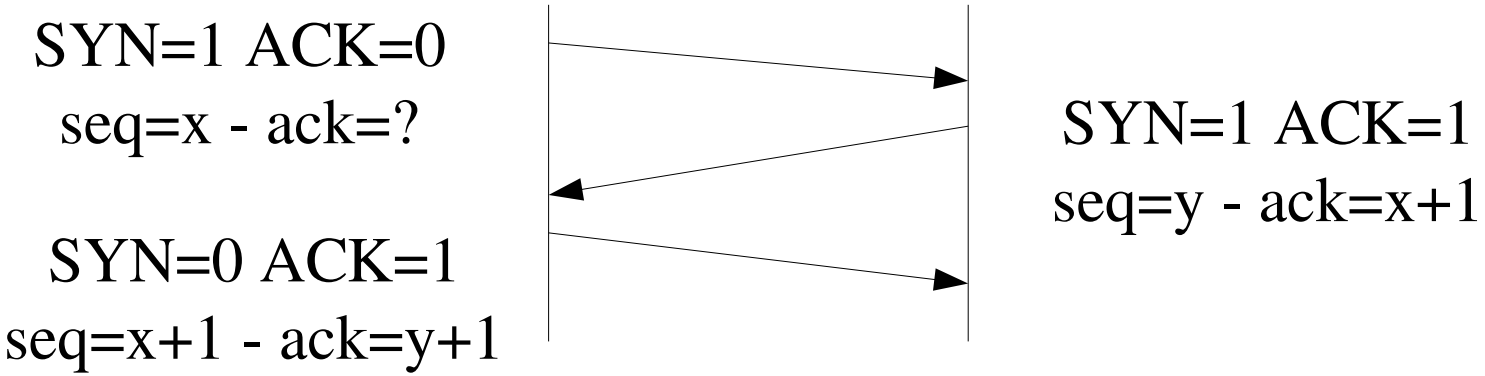
TCP (*Transmission Control Protocol*) est un protocole de transport fiable, en mode connecté (RFC 793) qui assure la transmission des données de bout en bout (d'un processus à un autre processus).



Modes de communication

- De manière générale, on distingue deux techniques possibles pour assurer une communication ou pour caractériser un protocole :
  - Le mode connecté : ce mode se déroule en trois phases (établissement de la liaison, transmission et libération). Exemples : le protocole TCP, le téléphone, …

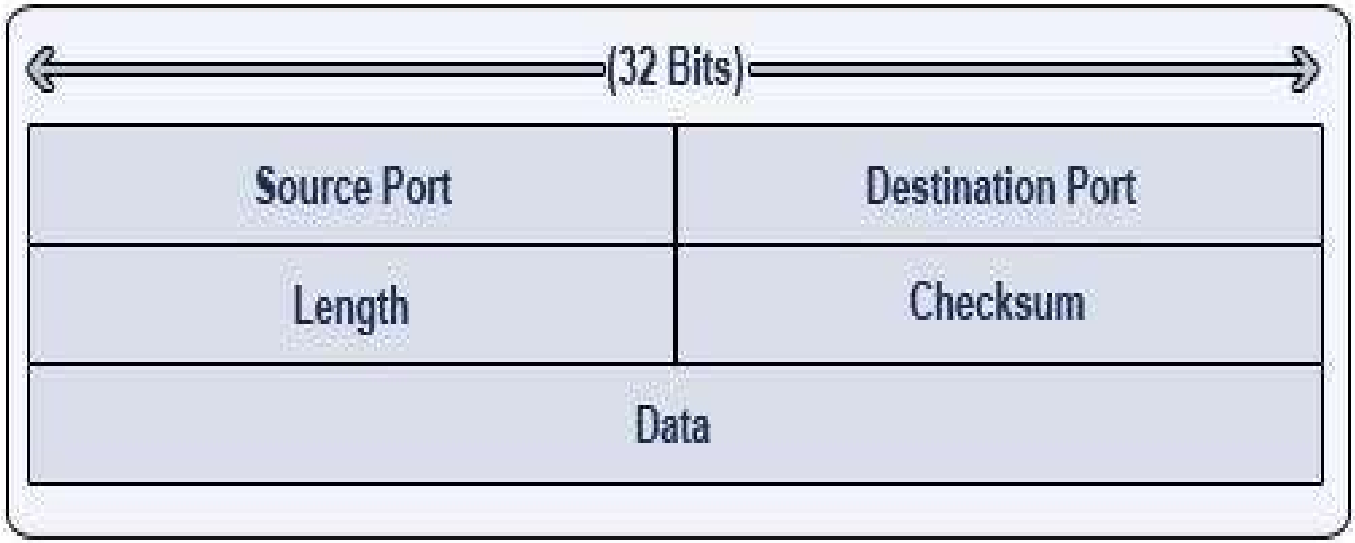
Exemple d'une connexion TCP en trois temps (*Three Way Handshake*)



  - Le mode non connecté : ce mode ne nécessite pas de phase de connexion (et donc de libération). On transmet directement. Le mode non connecté est décrit de manière générale comme moins fiable mais plus rapide que le mode connecté. Exemple : les protocoles IP et UDP, la diffusion télévision hertzienne ou satellite, ...

Protocole UDP

UDP (*User Datagram Protocol*) est un protocole souvent décrit comme étant non-fiable, en mode non-connecté (RFC 768), mais plus rapide que TCP.



Protocole HTTP

- Le Protocole HTTP (*HyperText Transfert Protocol*) sert notamment au dialogue entre un client web (navigateur par exemple) et un serveur (apache par exemple).
- Comme la plupart des protocoles de la couche Application, c'est un **protocole orienté texte (ASCII),** basé sur TCP. Il existe deux spécifications la 1.0 et la 1.1 (RFC 1945).

Requête HTTP

```
GET /index.html HTTP/1.1\r\n
Host: www.btsiris.net\r\n
\r\n
```

→ Ligne vide = fin de l'en-tête HTTP

En-tête

Le corps est vide

Corps

Réponse HTTP

```
HTTP/1.1 200 OK
Date: Wed, 10 Mar 2010 09:58:08 GMT
Server: Apache/2.2.11 (Mandriva
Linux/PREFORK-10.7mdv2009.1)
Content-Length: 215
Connection: close
Content-Type: text/html
```

→ Ligne de statut

→ Ligne vide = fin de l'en-tête HTTP

En-tête

```
<html>
<body>
<h1>It works!</h1>
</body>
</html>
```

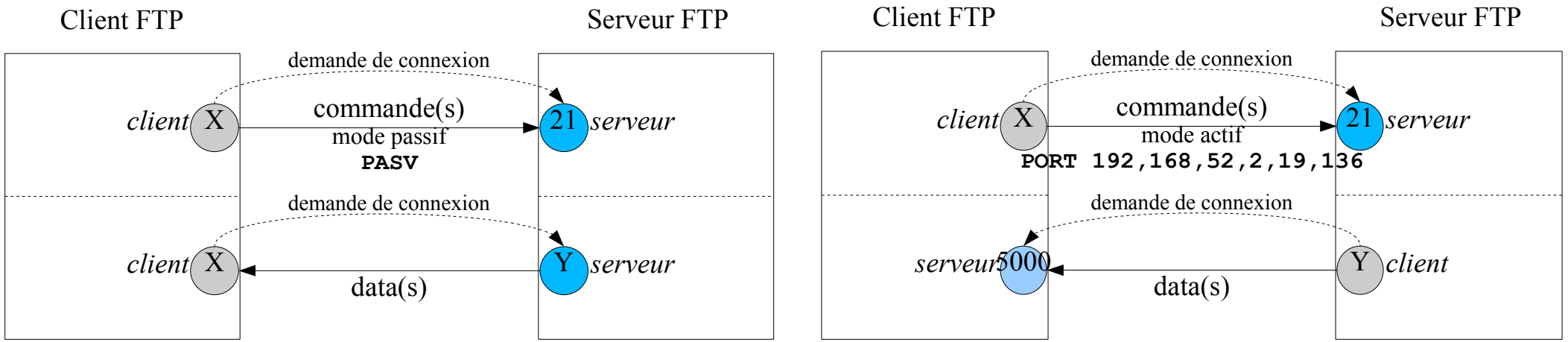
Le corps de la réponse contient le contenu du fichier index.html demandé dans la requête

Corps

Protocole FTP

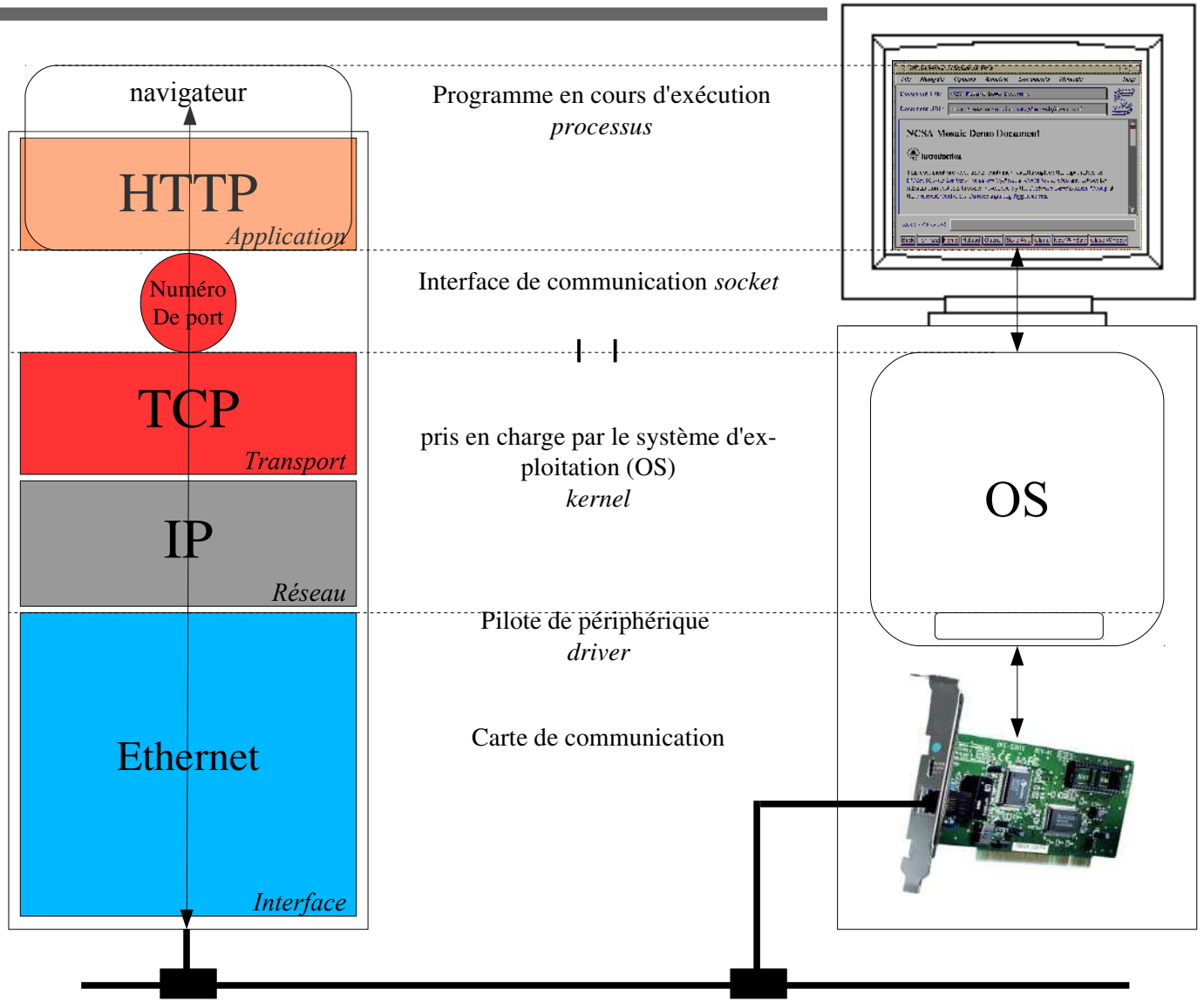
- Le protocole FTP (*File Transfer Protocol*) est un protocole de transfert de fichier (R-FC959). Le protocole FTP s'utilise de façon standard sur le **port 21 du serveur en mode TCP**. Par contre le **FTP ne fonctionne que sur du TCP**. Il existe un protocole TFTP (*Trivial FTP*) qui est basé sur UDP.

- Lors d'une connexion FTP, deux canaux de transmission sont ouverts :
  - Un canal pour les commandes (canal de contrôle) : USER, PASS, LIST, RETR, STOR, ...
  - Un canal pour les données



Modèle de référence (I)

- Un modèle de référence est utilisé pour décrire la structure et le fonctionnement des communications réseaux
- Le modèle DoD (*Departement of Defense*) ou « TCP/IP » est composé de 4 couches
- En raison de son apparence, la structure est très souvent appelé **pile** ou **pile de protocoles**.

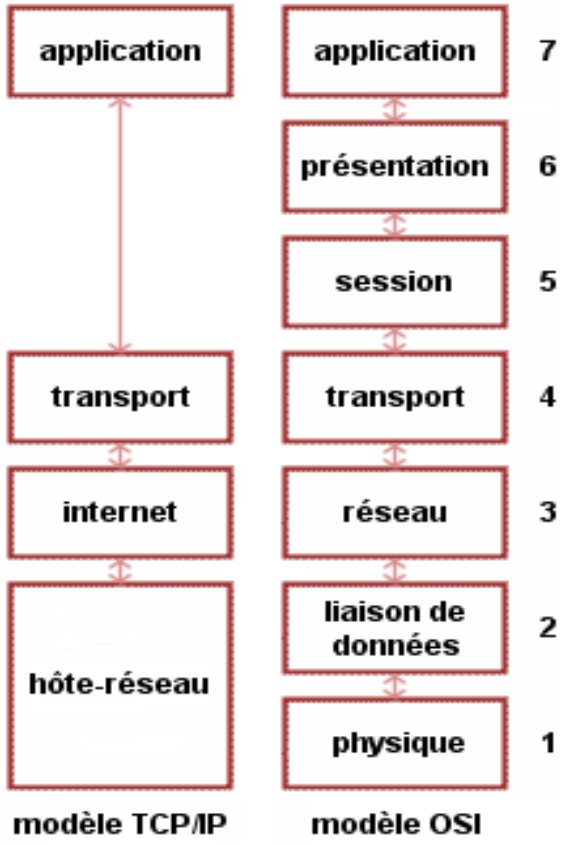


Modèle de référence (II)

- Un modèle de représentation développé par **l'ISO** (*International Standards Organization*) est souvent utilisé pour décrire la structure et le fonctionnement des communications réseaux : le modèle **OSI** (*Open Systems Interconnect Reference Model*).

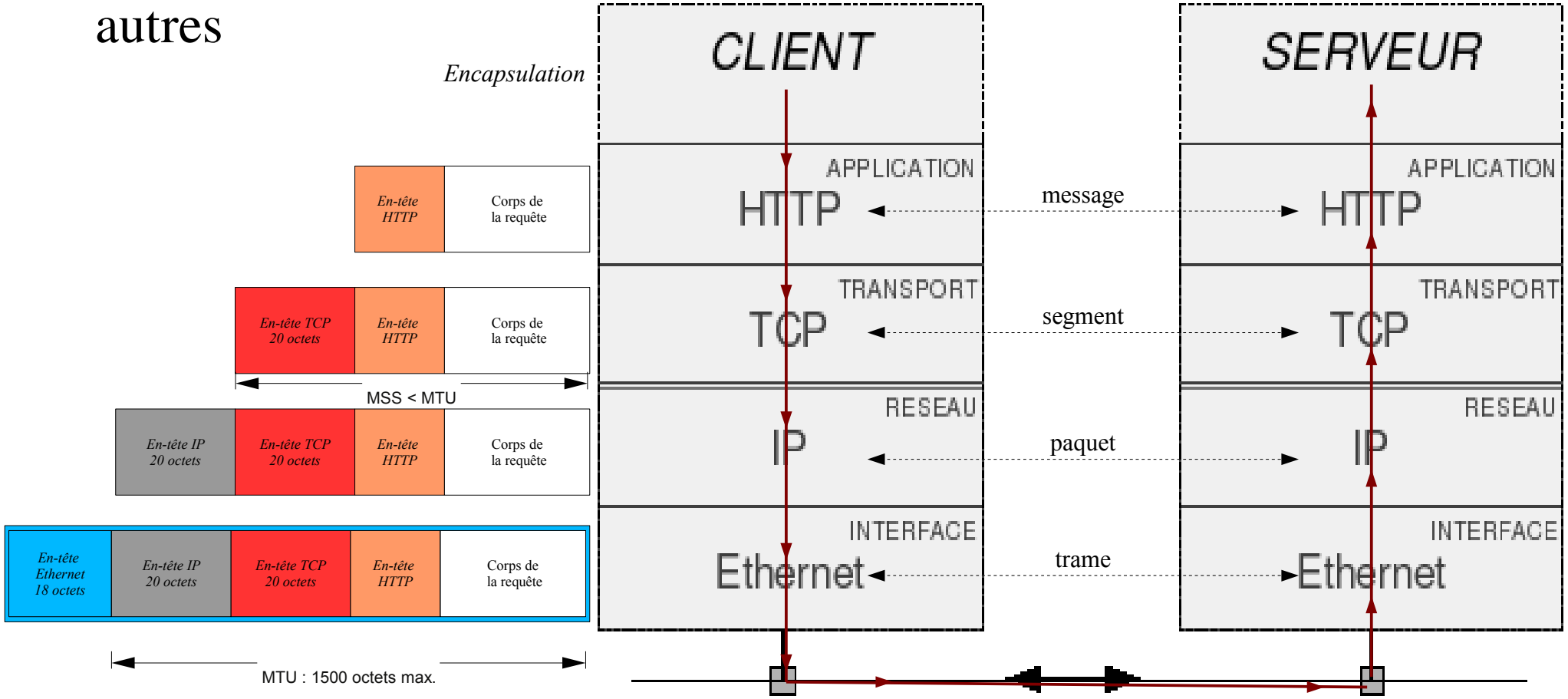
- Le modèle OSI contient **7 couches ou niveaux** qui définissent les **fonctions** des protocoles de communication qui vont de l'interface physique à l'interface avec les applicatifs utilisant le réseau.

- <u>Critiques du modèle OSI :</u>
  - Ce n'était pas le bon moment : trop tôt ou trop tard ?
  - Ce n'était pas la bonne technologie : trop complet et trop complexe
  - Ce n'était pas la bonne implémentation : trop lourd et trop lent
  - Ce n'était pas la bonne politique : trop normalisé et trop bureaucatrique



L'encapsulation

- Dans une communication entre deux équipements, de nombreux protocoles sont mis en oeuvre : ils sont encapsulés les uns dans les autres



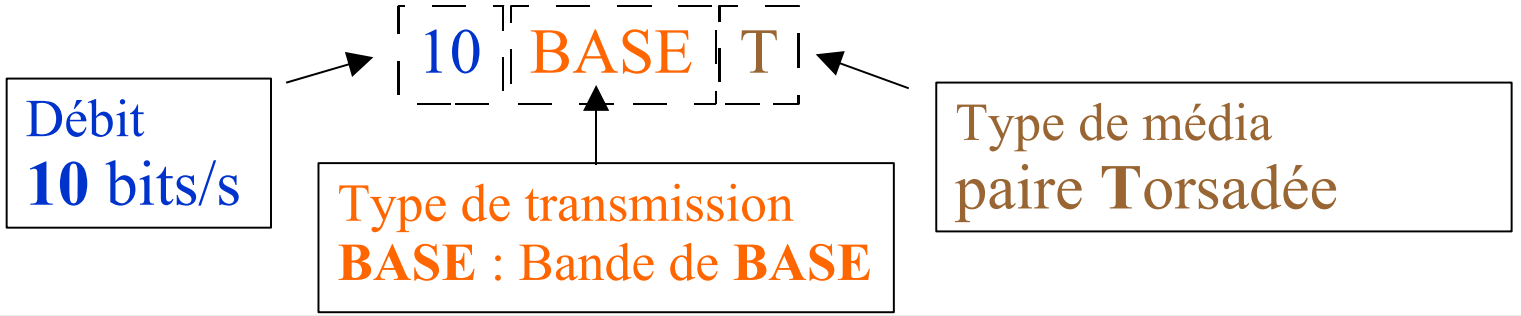
La couche Physique

- Son rôle est la transmission des **bits** sur le support physique.
- Ces fonctions principales sont :
  - fournir les caractéristiques électriques, mécaniques et fonctionnelles ;
  - définir le mode d'exploitation (semi-duplex, duplex intégral, //, série, ...) de la liaison (point à point ou multipoint) ;
  - assurer la compatibilité des interfaces qui réalisent les fonctions de codage, modulation et amplificateur du signal.

- Exemples : V24, X21, RS232, *Transceiver*, MAU, HUB, Répéteur, Prise DB25 et DB9, RJ45 et RJ11, etc ...

Ethernet (couche physique)

- Mise au point dans les années 80 par XEROX, Intel et DEC, l'architecture Ethernet permet l'interconnexion de matériels divers avec de grandes facilités d'extension.
- Les différentes normes :
  - Ethernet à 10 Mbits/s : 10BASET, 10BASE5, 10BASE2 et 10BASEF (802.3)
  - FastEthernet à 100 Mbits/s : 100BASET (802.3u)
  - Gigabit Ethernet (Gig-E) à 1 Gbits/s : 1000BASE-LX, 1000BASE-SX, 1000BASE-CX, 1000BASE-LH (802.3z) et 1000BASE-T (802.3ab)
  - Décagigabit Ethernet à 10 Gbits/s (10 Gigabit Ethernet) ...

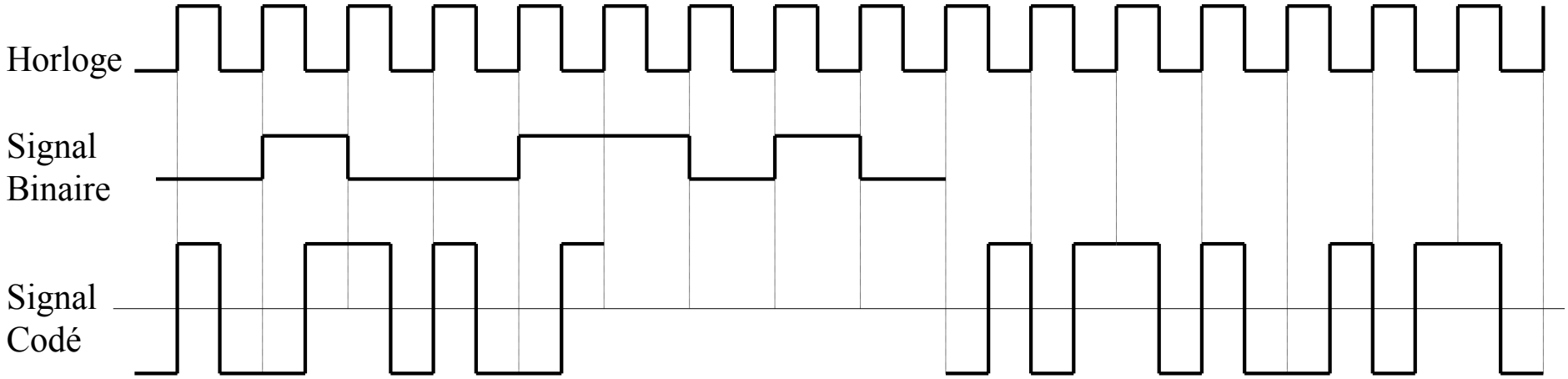


Transmission bande de base (BdB)

- La transmission en bande de base est une **transmission numérique** (sans transposition de fréquence par modulation).
- Les codages numériques sont utilisés pour plusieurs raisons :
  - la récupération du signal d'horloge facilitée par les transitions pour chaque bit transmis
  - le spectre d'un signal binaire est concentré sur les fréquences basses (les plus affaiblies)
  - les perturbations subies par un signal sont proportionnelles à la largeur de sa bande de fréquence.
- Les codages en bande de base vont donc essentiellement avoir pour rôle de diminuer la largeur de bande du signal binaire, de transposer celle-ci vers des fréquences plus élevées et d'utiliser les transitions du signal afin d'assurer une **transmission synchrone** (qui permettront au récepteur de synchroniser son horloge).
- Quelques codages utilisés sur Ethernet :
  - 10BASET : codage manchester (ou exclusif entre les DATA et l'Horloge)
  - 100BASET : codage 4B/5B MLT3 (**paires torsadées**)
  - 100BASEFX : codage 4B/5B NRZI (fibre optique), le GigaBit utilise le codage 8B/10B

Codage Manchester

- Le codage Manchester est utilisé sur le 10BASET :

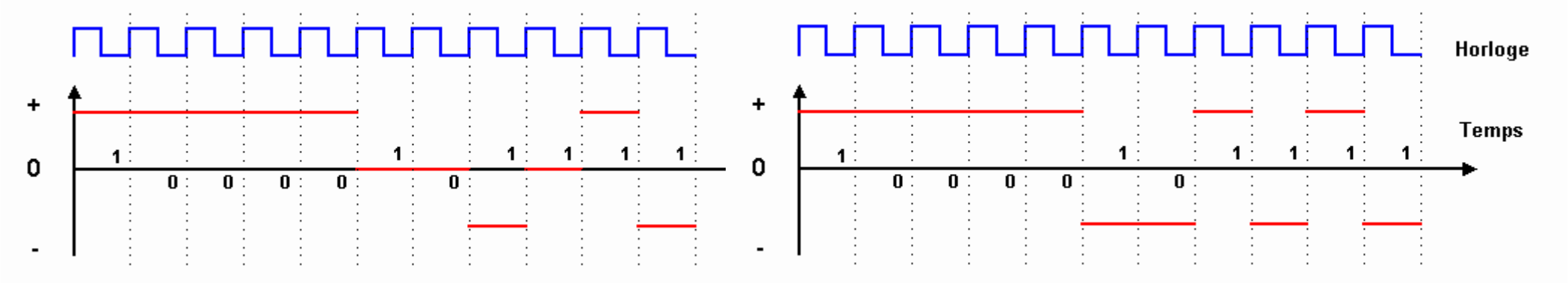


Principe : Une opération XOR (ou exclusif) est réalisée entre l'horloge et les données, d'où une transition systématique au milieu de chaque bit du signal binaire.

Codage numérique pour le 100 Mbps

Dans ce codage MLT3, seuls les 1 font changer le signal d'état en prenant successivement sur trois états : +V, 0 et -V (le codage Non Retour à Zéro Inversé n'utilise que 2 états). Les 0 sont codés en conservant la valeur précédemment transmise.

Le principal avantage du codage MLT3 est de diminuer fortement la fréquence nécessaire pour un débit donné grâce à l'utilisation de 3 états. Par contre, les longues séquences de 0 peuvent entraîner une perte ou un déphasage de l'horloge du récepteur. Pour éviter cela, on met en place un codage 4B/5B. Il consiste à coder, à l'aide d'une table de correspondance, une série de 4 bits en 5 bits (par exemple, la séquence 0000 sera codé 01010) : il faudra toujours au minimum 2 transitions pour 5 bits et on n'aura jamais plus de 2 zéros consécutifs)



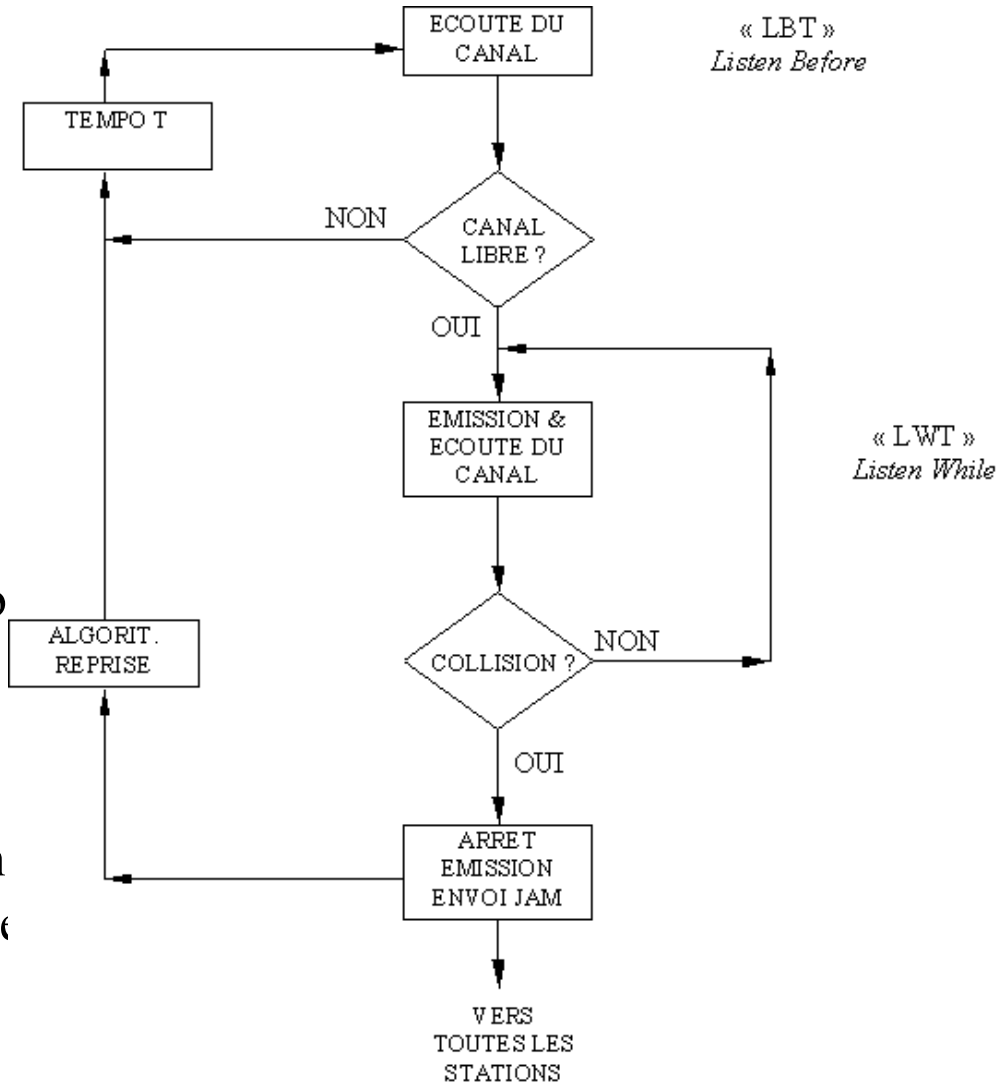
La couche Liaison

- Elle est responsable de l'acheminement sans erreurs des **trames** sur la ligne physique.
- Ces fonctions principales peuvent être :
  - établir et libérer les connexions ligne ;
  - assurer la mise en trames et la synchronisation ;
  - détecter et corriger les erreurs de transfert ;
  - gérer le contrôle de flux .
- La couche Liaison est découpée en deux sous couches appelées **MAC** (*Medium Access Control*) et **LLC** (*Logical Link Control*).
- Exemples : Ethernet 802.3 (ISO), Ethernet_II (DoD), Token Ring 802.5, PPP, LLC 802.2, *switch*, WIFI 802.11g, ...

Ethernet : sous-couche MAC

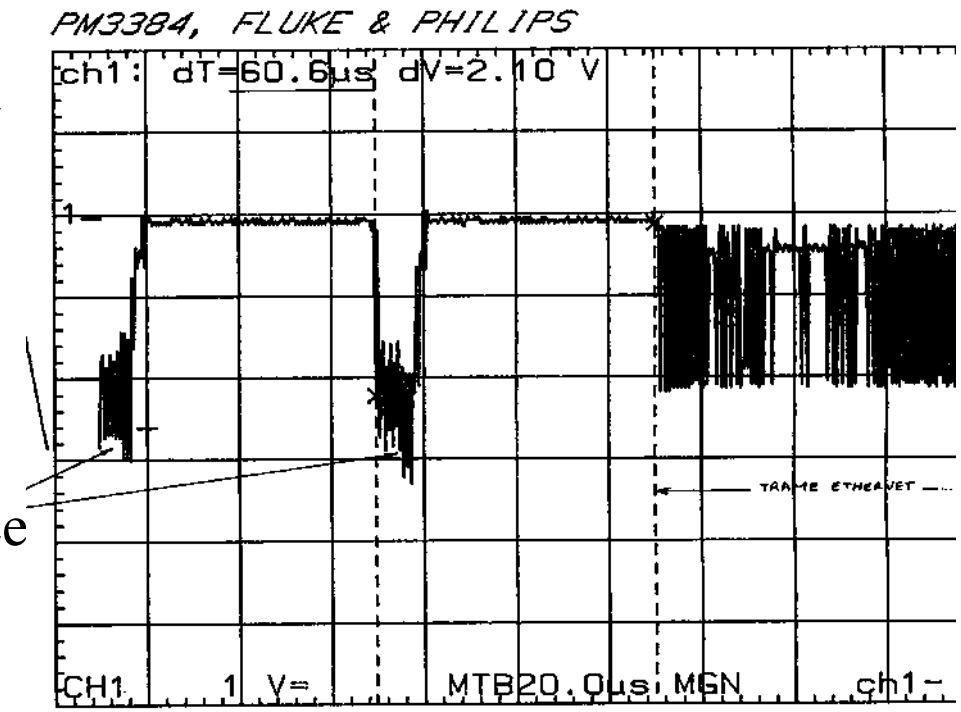
- La sous-couche **MAC** (*Medium Access Control*) d'Ethernet gère l'accès au support selon les principes de **CSMA/CD** (*Carrier Sense Multiple Access / Collision Detection*) :

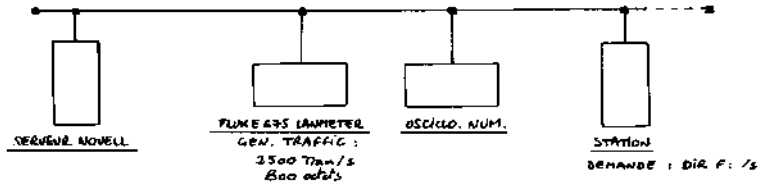
Sur ce type de réseau, il est possible que 2 ou plusieurs stations détectent le support libre, décident de transmettre en même temps et ce qui provoque une collision : cette situation pose problème. Le réseau Ethernet a décidé de s'en accommoder en mettant en place un mécanisme de détection et reprise de collision (arrêt de la transmission des stations impliquées, attente d'un temps aléatoire et reprise de la procédure normale).



Ethernet : CSMA/CD

- La détection de collision se fait par écoute du support. Lorsque la tension sur le câble est plus élevée que la tension maximale pouvant être générée par un seul *transceiver*, une collision est détectée.
- On ne peut prévoir la présence et le nombre de collisions qui vont exister sur ce type de réseau.
- Donc on qualifie ce type de réseau de **probabiliste** (ou à accès aléatoire).
- Un réseau **déterministe** serait un réseau de type Token Ring ou bus CAN par exemple.



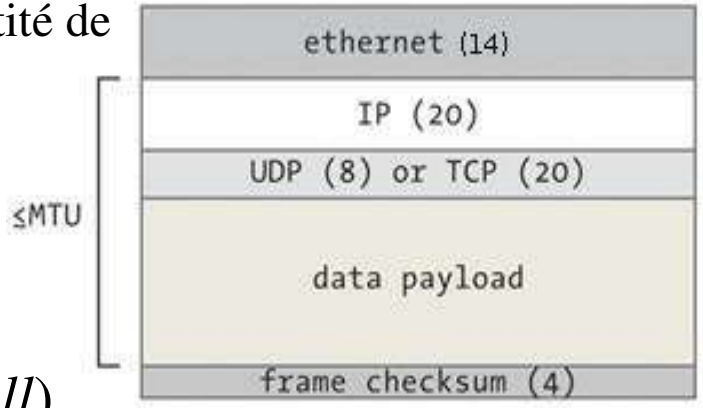


La couche Réseau

- Son rôle est de permettre l'acheminement de **paquets** (indépendamment les uns des autres) dans n'importe quel réseau jusqu'à destination.
- La fonction principale de cette couche est de réaliser le routage.
- Cette couche assure aussi la fragmentation qui est le découpage d'un paquet de données en paquets plus petits (fragments), pour passer à travers un lien de plus faible MTU (*Maximum Transmission Unit*). Le MTU définit la taille maximale (en octets) d'un paquet pouvant être encapsulé dans une trame de la couche inférieure.
- Dans le modèle « TCP/IP », comme aucune connexion n'est établie, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.
- Exemples : IP (*Internet Protocol*), IPX (*Internet Packet eXchange*), routeur, ...

La couche Transport

- Elle est responsable du transport des **messages** complets de bout en bout au travers du réseau.
- Fonctions :
  - gérer les adresses de transport (les numéros de port dans le modèle DoD) ;
  - gérer le transport en établissant et libérant une connexion (TCP) ou non (UDP) ;
  - gérer les messages (segments) : segmentation des données, réassemblage des données, contrôle du séquencement (TCP) ;
  - gérer la qualité de service : acquittement et retransmission sur absence, d'acquittement, contrôle de flux (fenêtre coulissante), détection des erreurs (TCP) ;
  - gérer le MSS (*Maximum Segment Size*) qui désigne la quantité de données (en octets) qui pourra être encapsulé dans un paquet non fragmenté.



- Exemples : TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), SPX (*Sequenced Packet eXchange*), pare-feu (*firewall*), …

Les couches Session – Présentation et Application

- **La couche Session** établit une communication entre émetteur et récepteur en assurant l'ouverture et la fermeture des sessions (des communications) entre usagers, définit les règles d'organisation et de synchronisation du dialogue entre les abonnés. Exemple : RPC (*Remote Procedure Call*), *firewall stateful*, ...

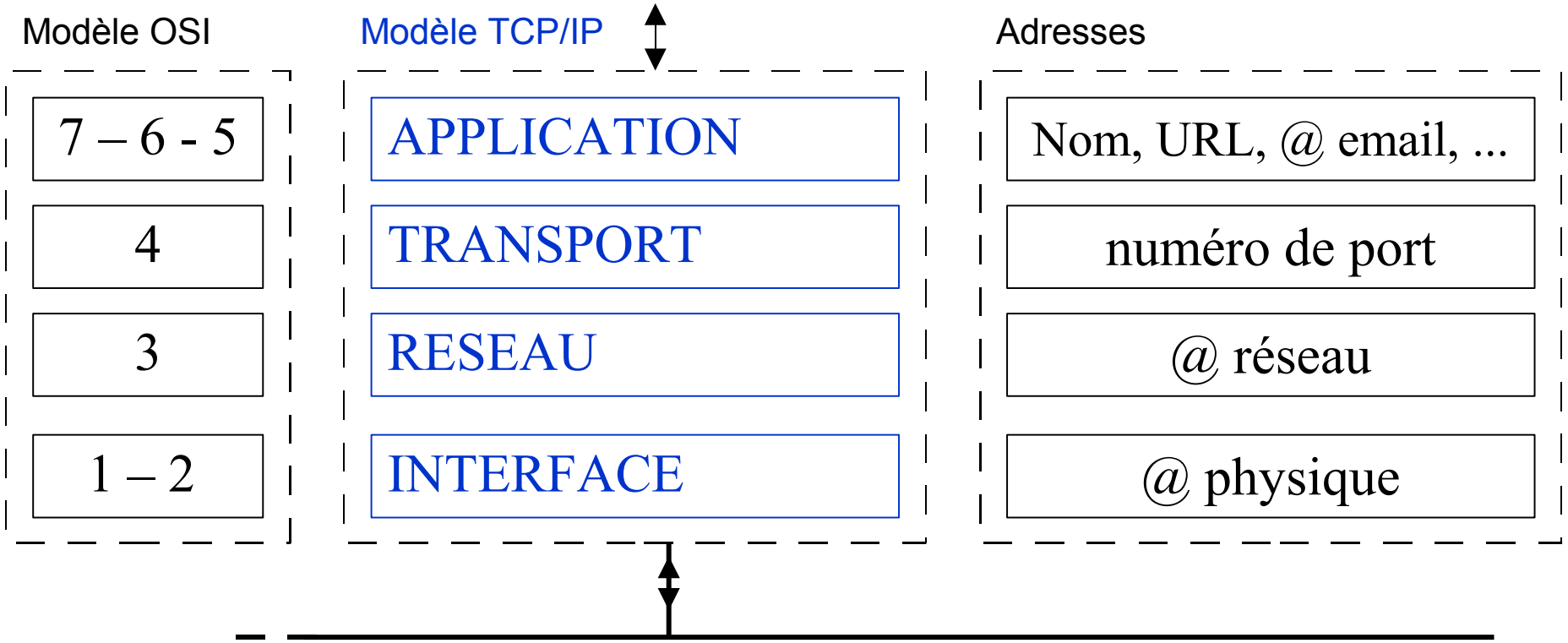
- **La couche Présentation** met en forme les informations échangées pour les rendre compatibles avec l'application destinatrice, dans le cas de dialogue entre systèmes hétérogènes.Elle peut comporter des fonctions de traduction, de compression, d'encryptage, ... etc. Exemple : XDR (*eXternal Data Representation*).

  - *Remarque :* ces deux couches ne sont présentes dans le modèle TCP/IP, tout simplement parce qu'elles sont apparues inutiles ou que très rarement utiles. Le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

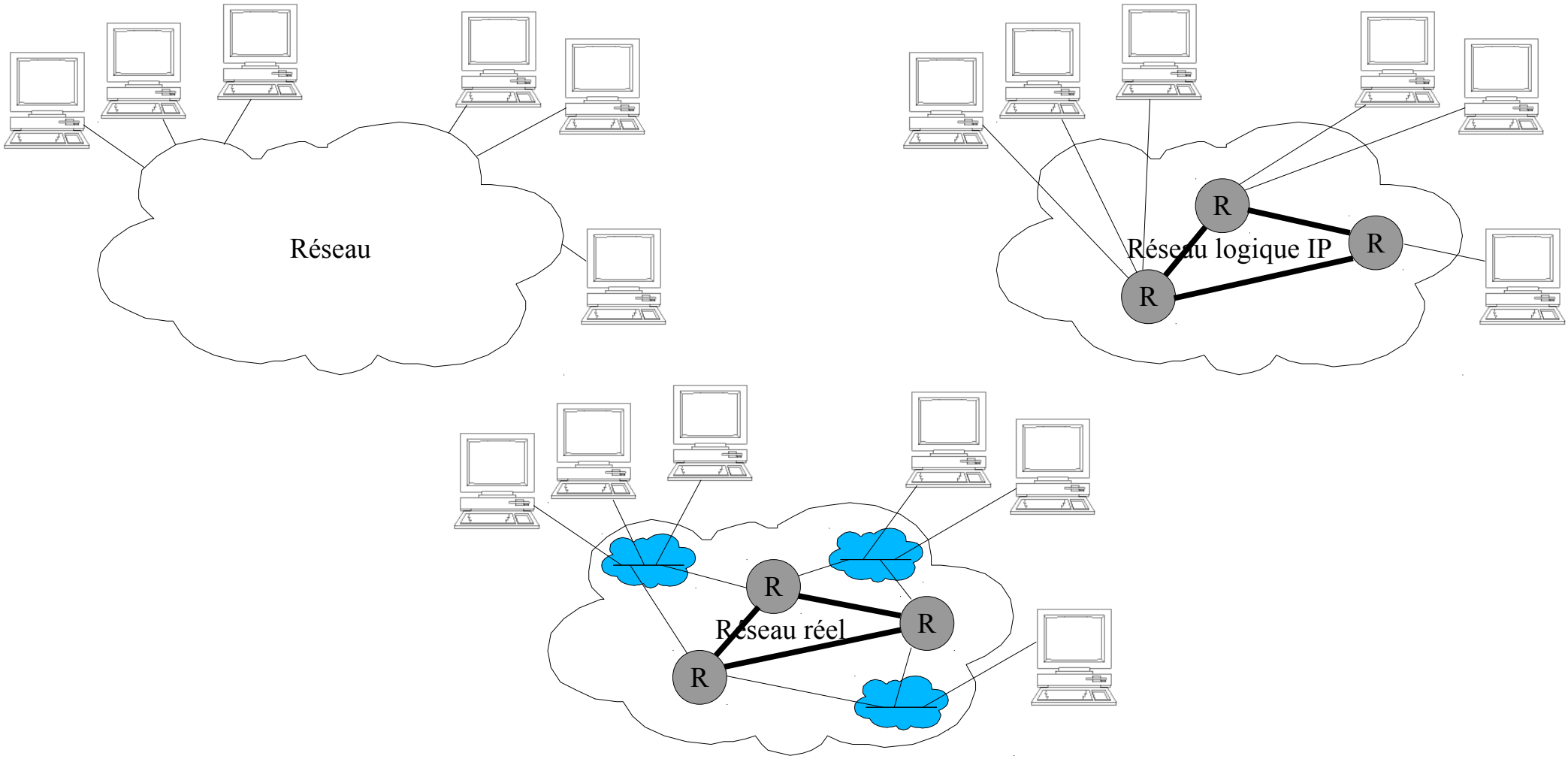
- **La couche Application** va apporter les services de base offerts par le réseau. Elle ne contient pas l'"application" de l'utilisateur, mais réalise l'interface pour les fonctions de communication avec les applicatifs. Exemples : FTP (*File Transfert Protocol*), HTTP (*HyperText Transfert Protocol*), etc …

L'adressage (I)

- Identifier de manière unique une interface, un poste, une application (un processus), une ressource, un fichier, un document, un utilisateur, ... sur un réseau
- On distinguera donc plusieurs types d'adresse :

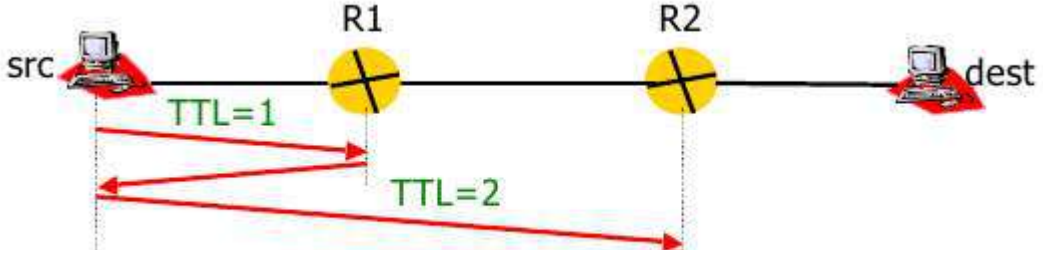


L'adressage (II)



Tracer la route

- traceroute est un programme utilitaire qui permet de suivre le chemin qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau. En exploitant le champ TTL de l'en-tête IP, il découvre ainsi les routeurs de proche en proche.




```
# traceroute -nI www.google.fr
traceroute to www.google.fr (209.85.227.104), 30 hops max, 60 byte packets
 1  192.168.52.1  0.935 ms  1.185 ms  1.449 ms
 2  90.36.253.1  118.547 ms  119.879 ms  122.841 ms
 3  10.125.49.14  124.873 ms  124.961 ms  125.348 ms
 4  193.253.86.234  126.607 ms  127.735 ms  130.226 ms
 5  193.252.101.86  138.891 ms  140.009 ms  141.475 ms
 6  193.252.161.182  149.277 ms  149.219 ms  150.707 ms
 7  193.251.128.226  152.001 ms 193.251.128.230  176.682 ms 193.251.129.57  176.654 ms
 8  193.251.249.46  175.432 ms  177.436 ms  177.426 ms
 9  209.85.250.142  203.125 ms  202.047 ms  201.006 ms
10  216.239.43.233  188.632 ms  181.575 ms  186.189 ms
11  209.85.252.83  181.654 ms  177.028 ms 216.239.49.45  176.469 ms
12  209.85.243.93  186.766 ms 209.85.243.97  175.459 ms 209.85.243.93  208.022 ms
13  209.85.227.104  196.754 ms  195.144 ms  191.072 ms
```

Tester l'état de la connexion (*ping*)

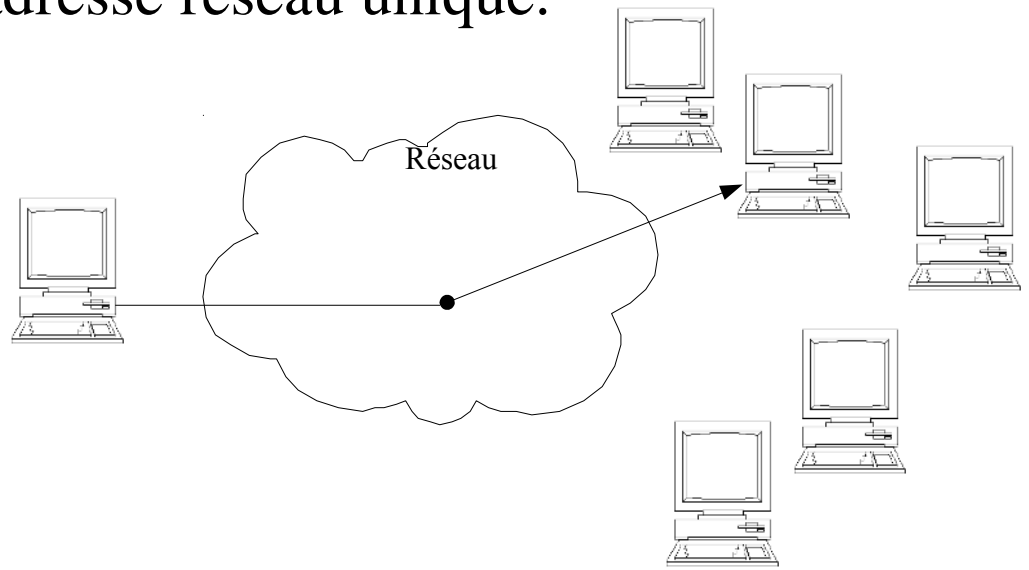
- En utilisant le protocole ICMP, la commande **ping** permet d'obtenir des informations (en particulier le temps de réponse de la machine à travers le réseau) et aussi quel est l'état de la communication avec cette machine.

```
# ping -c 1 -t 12 209.85.227.104
PING 209.85.227.104 (209.85.227.104) 56(84) bytes of data.
From 209.85.243.101 icmp_seq=1 Time to live exceeded

# ping -c 1 -t 13 209.85.227.104
PING 209.85.227.104 (209.85.227.104) 56(84) bytes of data.
64 bytes from 209.85.227.104: icmp_seq=1 ttl=52 time=149 ms

rtt min/avg/max/mdev = 149.220/149.220/149.220/0.000 ms
```

Techniques d'adressage : l'*unicast*

Le terme *unicast* définit une connexion réseau point à point, soit le transfert d'un hôte vers un autre hôte.

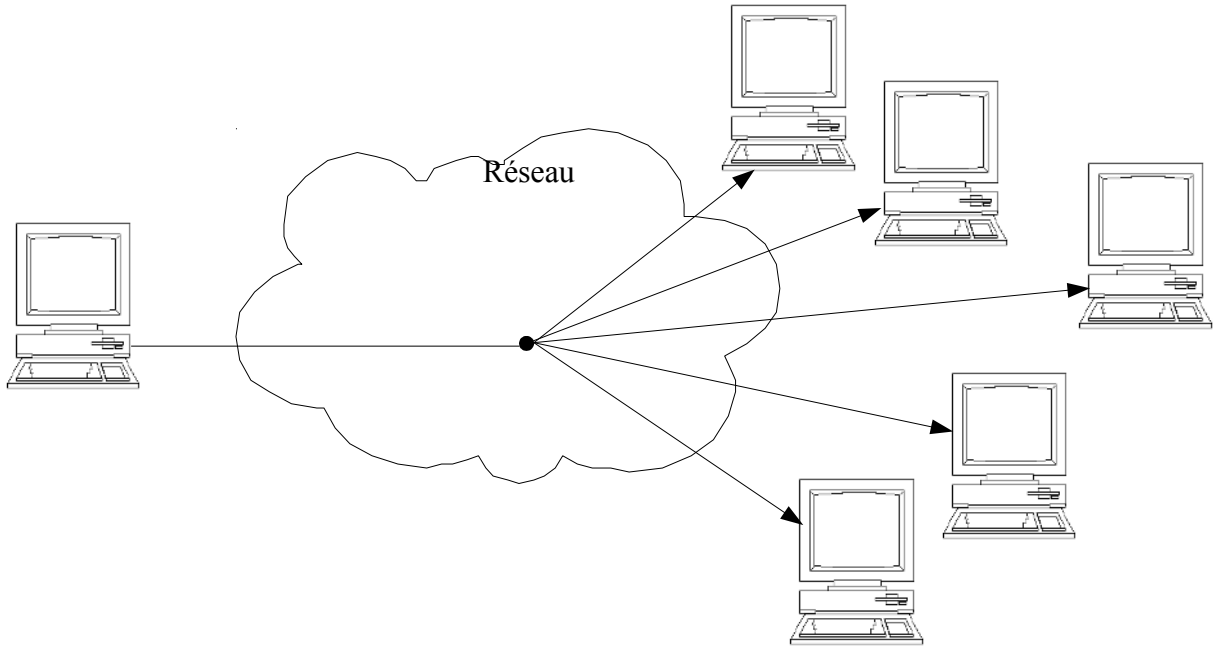
On entend par *unicast* le fait de communiquer entre deux ordinateurs identifiés chacun par une adresse réseau unique.



Le terme *anycast* désigne une technique où on l'on dispose de plusieurs adresses pour une destination mais une seule sera utilisée.

Techniques d'adressage : le *broadcast*

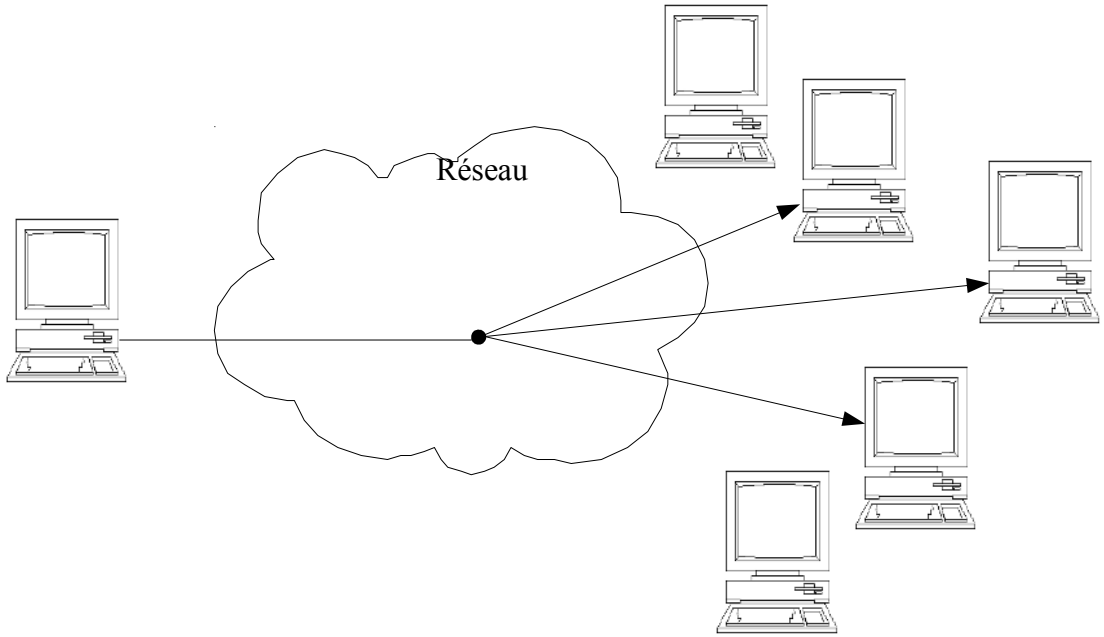
Le terme *broadcast* définit une connexion réseau multi-point, soit le transfert d'un hôte vers tous les autres hôtes, en utilisant une adresse spécifique nommée adresse de *broadcast* (ou adresse de diffusion générale).



Techniques d'adressage : *multicast*

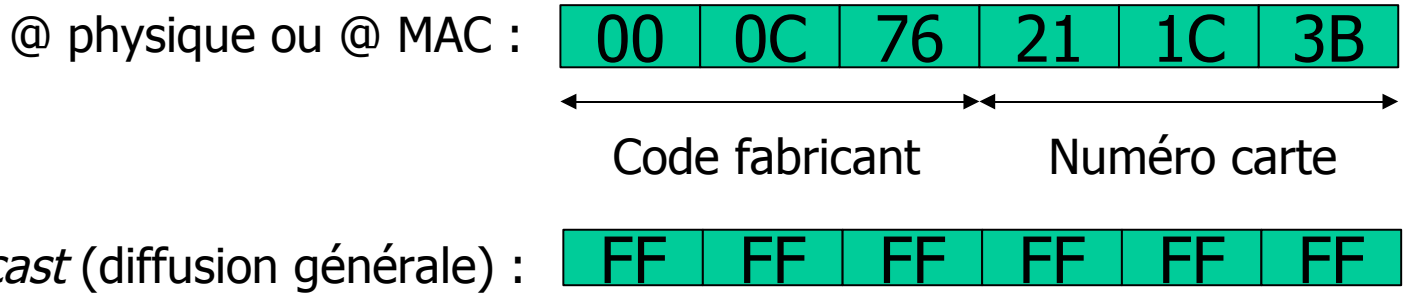
On entend par *multicast* le fait de communiquer simultanément avec un groupe d'ordinateurs identifiés par une adresse spécifique (adresse de groupe).

Les récepteurs intéressés par les messages adressés à ce groupe doivent s'abonner au préalable à ce groupe.



L'adresse MAC

- Identifier de manière unique une carte de communication sur un réseau physique
  - Stockée dans l'interface et mondialement unique
  - Composée de 6 codes hexadécimaux (6x8 = 48 bits)
  - Utilisée comme adressage dans les trames
- L'adresse physique MAC (ou adresse matérielle ou *hardware*) est une adresse de la couche Liaison qui ne donne aucune indication sur la situation géographique du poste et donc ne permet pas une organisation optimale du réseau. Cette faiblesse sera compensée par un adressage au niveau de la couche Réseau.



VLAN

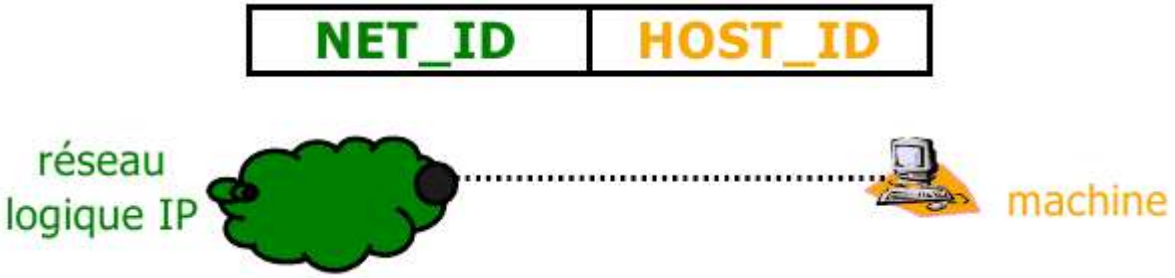
- Un réseau virtuel, communément appelé VLAN (*Virtual LAN*), est un réseau logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur (*switch*).
- Intérêt des VLAN :
  - Segmentation : réduire la taille d'un domaine de diffusion (*broadcast*)
  - Flexibilité : filtrer les adresses MAC du niveau 2 (couche liaison) voire jusqu'au niveau 3 (IP)
  - Sécurité : permettre de créer un ensemble logique isolé. Le seul moyen pour communiquer entre des VLAN différents sera alors de passer par un routeur.
- Les trames d'un VLAN doivent être identifiées avec un protocole commun. Le protocole 802.1Q ajoute une étiquette à l'en-tête du paquet Ethernet, la marquant comme appartenant à un certain VLAN, ceci est la méthode préférée actuellement et la seule option valable dans un environnement avec des équipements de fournisseurs multiples.
  - VLAN par port (*Port-based VLAN*) : l'administrateur affecte chaque port à un VLAN
  - VLAN par adresse MAC (*MAC address-based VLAN*) : chaque carte MAC est gérée individuellement en maintenant une table @ MAC ↔ VLAN (par défaut)
  - VLAN par adresse de niveau 3 : on affecte une adresse de niveau 3 à un VLAN (+ lent)
  - Autres : par protocoles, par SSID, ...

L'adressage IP (I)

- Une adresse IP (*Internet Protocol*) est le numéro qui identifie de manière unique chaque équipement connecté à un réseau IP. Il existe des adresses IP de version 4 (codées sur 32 bits) et de version 6 (codée sur 128 bits). L'adresse de version 4 est actuellement la plus utilisée : elle est généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points (exemple : 212.85.150.134). L'adresse IP est utilisée dans l'en-tête IP des paquets transmis.
- Certaines adresses ne sont pas (ou tout du moins ne devraient pas être) routées sur Internet : elles sont réservées à un usage local (au sein d'une organisation, où là elles peuvent être routées). En IPv4, les classes d'adresses ont été réservées pour un usage privé comme suit (RFC 1918) :
  - Dans la classe A : 10.0.0.1 à 10.255.255.254 (notation CIDR : 10.0.0.0/8)
  - Dans la classe B : 172.16.0.1 à 172.31.255.254 (notation CIDR : 172.16.0.0/12)
  - Dans la classe C : 192.168.0.1 à 192.168.255.254 (notation CIDR : 192.168.0.0/16).

L'adressage IPv4 (II)

- Une adresse IP est décomposée en deux parties : une partie identifie le réseau (*net-id*) auquel appartient l'hôte et une partie identifie le numéro de l'hôte (*host-id*) dans ce réseau.

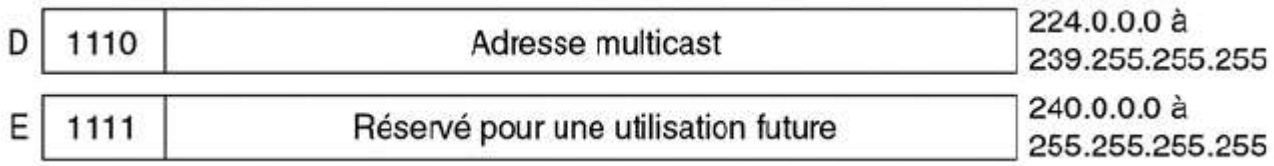


- Le masque de sous-réseau permet de savoir quelle partie d'une adresse IP correspond à la partie numéro de réseau et laquelle correspond à la partie numéro de l'hôte. On utilise une opération de ET bit à bit entre l'adresse IP et le masque de sous-réseau pour extraire la partie réseau de l'adresse.
- L'adressage CIDR (*Classless Inter-Domain Routing*) a été mis au point afin (principalement) d'insuffler une plus grande durée de vie aux adresses IPv4 dans l'attente d'un passage à IPv6. La notation CIDR abandonne l'adressage par classe et indique une adresse réseau suivi d'un '/' et d'un nombre indiquant les bits à 1 constituant le masque de sous-réseau (en partant de la gauche). Exemple : 10.0.0.0/8 correspond un masque 255.0.0.0.

Les classes d'adresse IP

Les adresses IP sont organisées en différentes classes :

Classe	*1° octet en binaire*	*Masque par défaut*	*Plages d'@ réseaux possibles*	*Plages d'@ hôtes possibles*	*Nb de réseaux possibles*	*Nb d'hôtes possibles*	*@ de broadcast dans le réseau*
A	**0**000 0001 - **0**111 1110	255.0.0.0	1.0.0.0 - 126.0.0.0	0.0.0.1 - 0.255.255.254	2^7 - 2 = 126	2^{24} - 2 = 16 777 214	xxx.255.255.255
B	**10**00 0000 - **10**11 1111	255.255.0.0	128.0.0.0 - 191.255.0.0	0.0.0.1 - 0.0.255.254	2^{14} = 16 384	2^{16} - 2 = 65 534	xxx.xxx.255.255
C	**110**0 0000 - **110**1 1111	255.255.255.0	192.0.0.0 - 223.255.255.0	0.0.0.1 - 0.0.0.254	2^{21} = 2 097 151	2^8 - 2 = 254	xxx.xxx.xxx.255



Adresses IP interdites et réservées

- D'autre part, il y a des **adresses interdites** que l'on ne peut pas utiliser comme adresse IP pour un équipement :

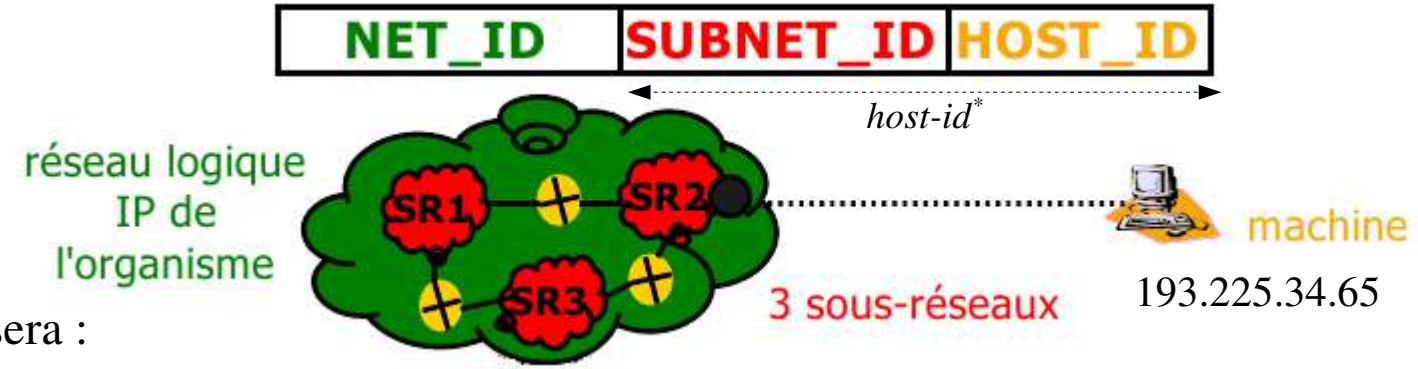
- les **adresses réseaux** : tous les bits de la partie *host-id* à zéro (X.0.0.0, X.Y.0.0, X.Y.Z.0)
- les **adresses de diffusion générale** (***broadcast***) : tous les bits de la partie *host-id* à un (X.255.255.255 , X.Y. 255.255, X.Y.Z.255)
- l'**adresse de boucle locale** (***loopback***) 127.0.0.1 associé au nom *localhost*. De manière générale, toutes les adresses de ce réseau 127.0.0.0
- l'**adresse 0.0.0.0** qui est utilisée par certains services (DHCP, tables de routage, ...) pour différentes significations : adresse courante de la machine, route par défaut, ...
- l'**adresse 255.255.255.255** qui est le *broadcast* ultime :)

Classe	*1° octet en binaire*	*Masque par défaut*	*Plages d'@ réseaux possibles*	*Plages d'@ hôtes possibles*	*Nb de réseaux possibles*	*Nb d'hôtes possibles*
A	0000 1010	255.0.0.0	10.0.0.0	**0.0.0.1 - 0.255.255.254**	**1**	**2^{24} - 2 = 16 777 214**
B	1010 1100	255.255.0.0	172.16.0.0 - 172.31.0.0	**0.16.0.1 - 0.31.255.254**	**16**	**2^{16} - 2 = 65 534**
C	1100 0000	255.255.255.0	192.168.0.0 - 192.168.255.0	**0.0.0.1 - 0.0.255.254**	**256**	**2^{8} - 2 = 254**

Les plages d'adresses réservées à usage privé pour les classes A, B et C

L'adressage IP des sous-réseaux

- Pour segmenter un réseau en sous-réseau, il faut alors décomposer la partie *host-id** de l'adresse IP en deux parties : une adresse de sous réseau (*subnet-id*) et une adresse machine (*host-id*).
- Par exemple, pour créer 3 sous-réseaux, il faudra prendre 2 bits dans la partie *host-id* (2^2 = 4 sous-réseaux créés). Soit un réseau 193.225.34.0/24 découpé en 3 sous-réseaux, on obtiendra :
  - net-id = 24 bits
  - subnet-id = 2 bits
  - host-id = 8 – 2 = 6 bits

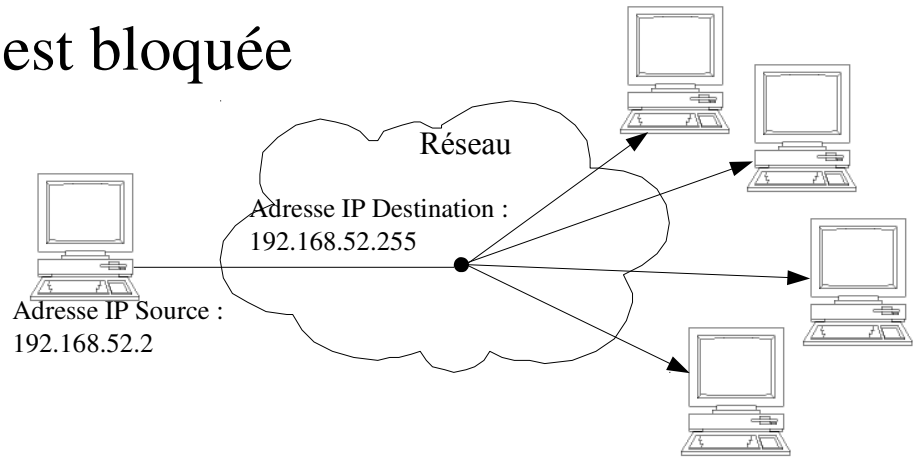


- Le masque de sous-réseau sera :
  24 + 2 = 26 bits soit 255.255.255.192
- Le nombre de machines adressables dans chaque sous-réseau sera de 2^6 – 2 adresses interdites = 62 adresses
  - Sous-réseau n°1 193.225.34.0/26 : 193.225.34.1 à 193.225.34.62 (broadcast = 193.225.34.63)
  - Sous-réseau n°2 193.225.34.64/26 : 193.225.34.65 à 193.225.34.126 (broadcast = 193.225.34.127)
  - Sous-réseau n°3 193.225.34.128/26 : 193.225.34.129 à 193.225.34.190 (broadcast = 193.225.34.191)

Broadcast IP

Par exemple, en IP version 4 (IPv4), une adresse IP de diffusion telle que 192.168.52.255 sera interceptée par toutes les machines ayant une adresse IP entre 192.168.52.1 et 192.168.52.254, pour autant que le masque de sous-réseau de l'interface soit défini comme 255.255.255.0.

L'étendue de diffusion sera restreinte au domaine de diffusion (le réseau logique IP) : un routeur ne transmet normalement pas les paquets de « *broadcast* ». L'adresse 255.255.255.255 (soit tous les postes de tous les réseaux) est bloquée par les routeurs Internet.

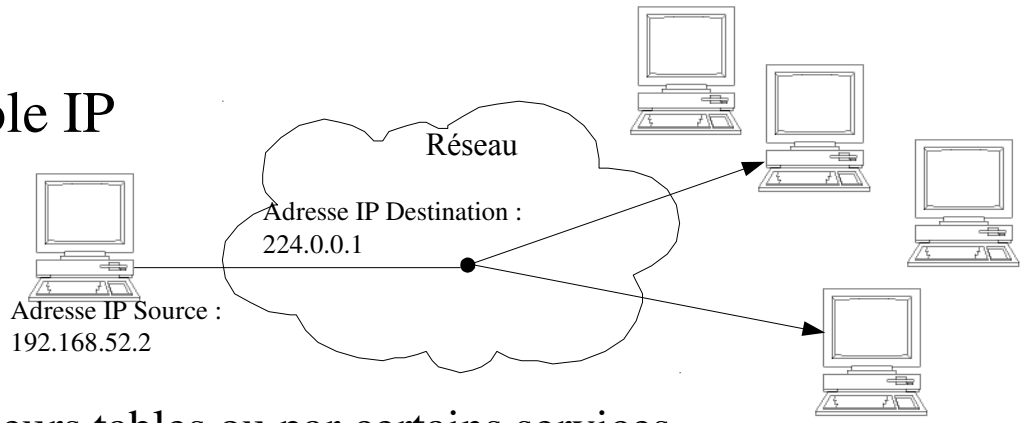


Multicast IP

En *multicast*, le protocole IP (en version 4) utilise les adresses de la classe d'adresses D 224.0.0.1 à 239.255.255.254. Les adresses IP *multicast* 224.0.0.1 à 224.0.0.255 sont locales à un lien.

Un groupe *multicast* se compose d'un ensemble de machines. Il est entièrement dynamique (une station peut rejoindre ou quitter le groupe à tout moment), et ouvert (une station peut émettre un paquet dans un groupe sans en faire partie). Un groupe *multicast* est désigné par une adresse IP. Lorsqu'un poste veut envoyer un paquet à un groupe *multicast*, il envoie ce paquet à l'adresse IP identifiant ce groupe (par exemple : 239.254.254.254).

Le protocole IGMP est utilisé par le protocole IP pour l'adhésion aux groupes *multicast*.



Le *multicast* est utilisé par les routeurs pour diffuser leurs tables ou par certains services comme le *streaming* ...

Usage de l'adressage IP

- On distingue deux situations :
  - Les équipements communiquement directement entre eux à condition qu'ils soient sur le **même réseau IP**. Ils peuvent être interconnectés par des **concentrateurs** (***hub***) et/ou des **commutateurs** (***switch***).
  - Les équipements qui n'appartiennent pas au même réseau IP ne peuvent pas communiquer entre eux directement. Ils pourront le faire par l'intermédiaire d'un **routeur** (*gateway*).
- Pour fixer l'adresse IP, on distingue deux types de réseaux :
  - le **réseau Internet** où chaque équipement connecté doit posséder une adresse unique au niveau mondial.
  - les **réseaux privés**, dans ce cas le choix des adresses est libre.
- *Remarques :*
  - Si un réseau privé doit être interconnecté avec le réseau Internet, il faudra alors utiliser des adresses privées qui ne puissent correspondre à des adresses publiques utilisées sur Internet. Des plages d'**adresses réservées à usage privé** existent et elles ne sont donc pas acheminées par les routeurs Internet, ce qui supprime tout rique de conflit.
  - Dans ce cas, pour interconnecter un réseau privé avec Internet, on utilisera un **routeur NAT** (*Network Address Translation*) qui permet de remplacer l'adresse IP source privée par l'adresse publique du routeur.

L'adressage IPv6

- Les adresses IPv6 sur 128 bits sont décomposées en :
  - un préfixe de localisation public - 48 bits
  - un champ de topologie locale du site (*subnet*) - 16 bits
  - un identifiant de désignation de l'interface (basé sur l'@MAC) sur 64 bits (équivalent à HOST_ID) qui garantie l'unicité de l'adresse

- Notation : groupes de 4 chiffres hexadécimaux séparés par ':'

FE80:0000:0000:0000:020C:76FF:FE21:1C3B

(:: représente un ou plusieurs groupes de 0000)

FE80::20C:76FF:FE21:1C3B

ARP (*Address Resolution Protocol*)

- Le protocole ARP sert à traduire une adresse réseau IP en une adresse physique.

- Un poste désire envoyer un paquet IP à un poste appartenant au même réseau physique que lui. Il doit connaître l'adresse physique du destinataire. Or souvent, il ne connait que son adresse IP. Le protocole ARP va lui permettre de trouver l'adresse physique du poste destinataire. Ce mécanisme est transparent pour l'utilisateur.
- Une table de conversion est générée dynamiquement sur chaque hôte dans ce qu'on appelle l'"***ARP cache***". Quand ARP reçoit une demande de conversion, il consulte sa table et retourne l'adresse physique si elle s'y trouve sinon il envoie un paquet spécial *ARP Request Packet* à tous les hôtes du même réseau physique incluant l'adresse IP à rechercher et en utilisant l'adresse *broadcast* MAC FF FF FF FF FF FF.
- La machine possédant l'adresse réseau IP demandée répond en lui renvoyant donc son adresse physique qui est alors placée dans la table ARP. Le cache ARP est généralement vide à chaque démarrage de la machine.
- Le protocole RARP (*Reverse ARP*) permet d'associer une adresse réseau à une adresse physique.

DHCP

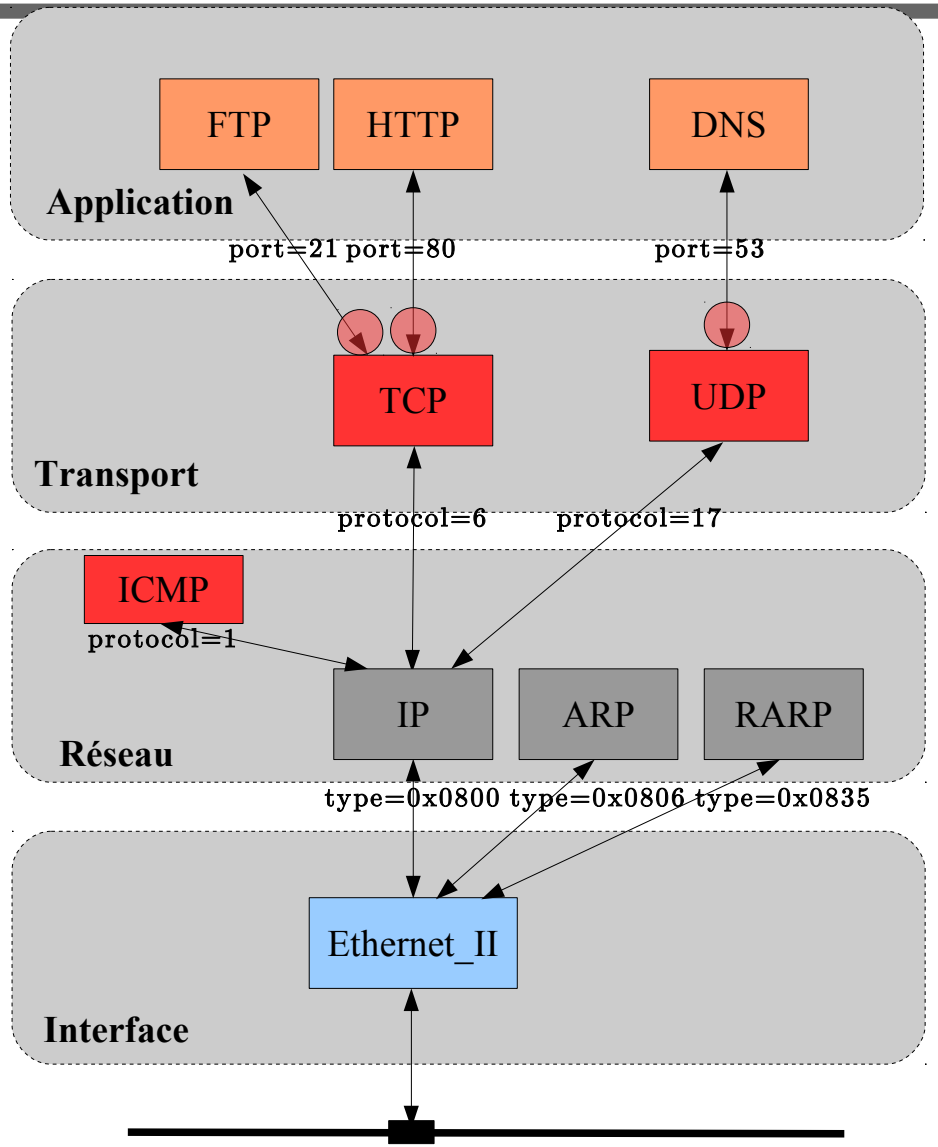
- DHCP (*Dynamic Host Configuration Protocol*) désigne un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous-réseau.
- Par opposition, l'assignation manuelle d'une adresse IP sera nommée adresse IP statique ou adresse IP fixe.
- L'ordinateur, dépourvu d'adresse IP, envoie par diffusion un datagramme (DHCP DISCOVER) vers le port 67 de n'importe quel serveur à l'écoute sur ce port.
- Tout serveur DHCP ayant reçu ce datagramme, diffuse une offre (DHCP OFFER) vers le client sur le port 68, identifié par son adresse physique. Il se peut que plusieurs offres soient adressées au client.
- Le client retient une des offres reçues (la première qui lui parvient), et diffuse sur le réseau un datagramme de requête DHCP (DHCP REQUEST).
- Le serveur DHCP choisi élabore un datagramme d'accusé de réception (DHCP ack pour acknowledgement) qui assigne au client l'adresse IP et son masque de sous-réseau, la durée du bail de cette adresse, deux valeurs T1 et T2 qui déterminent le comportement du client en fin de bail, et éventuellement d'autres paramètres : adresse IP de la passerelle par défaut, adresses IP des serveurs DNS, ...

Les numéros de port

- Un numéro de port sert à identifier l'application (un processus) en cours de communication par l'intermédiaire de son protocole de couche application (associé au service utilisé, exemple : 80 pour HTTP).
- Pour chaque port, un numéro lui est attribué (codé sur 16 bits), ce qui implique qu'il existe un maximum de 65 536 ports (2^16) par ordinateur (et par protocoles TCP et UDP).
- L'attribution des ports est faite par le système d'exploitation, sur demande d'une application. Cette dernière peut demander à ce que le système d'exploitation lui attribue n'importe quel port, à condition qu'il ne soit pas déjà attribué.
- Lorsqu'un processus client veut dialoguer avec un processus serveur, il a besoin de connaître le port écouté par ce dernier. Les ports utilisés par les services devant être connus par les clients, les principaux types de services utilisent des ports qui sont dits réservés. Une liste des ports attribués est disponible dans le fichier /etc/services sous Unix/Linux.

Adressage des protocoles - SAP (*Service Access Point*)

- Identifier le protocole ou service de niveau supérieur
- Dans le modèle « TCP/IP », un protocole utilise des numéros (les *assigned numbers*) identifiant les protocoles de niveau supérieur qu'il transporte.



L'adressage web : URI/URL

- Un URI (*Uniform Resource Identifier*) soit littéralement « identifiant uniforme de ressource », est une courte chaîne de caractères identifiant une ressource sur un réseau (par exemple une ressource Web) physique ou abstraite, et dont la syntaxe respecte une norme d'Internet mise en place pour le World Wide Web (voir RFC 3986).
- Un URL (*Uniform Resource Locator*) littéralement « localisateur uniforme de ressource », est une chaîne de caractères utilisée pour adresser les ressources du World Wide Web : document HTML, image, son, forum Usenet, boîte aux lettres électronique, etc. Elle est aussi appelée adresse web.
- Le format d'une adresse web ou URL :

```
protocole://[<login>:<mot_de_passe>]<serveur>[:<numero_port>]/[<chemin>/]<ressource>
```

Exemples : **http://www.example.com/tim/page.html**
http://192.168.52.83/index.php
ftp://ftp.is.co.za:21/rfc/rfc1808.txt

DNS (1/2)

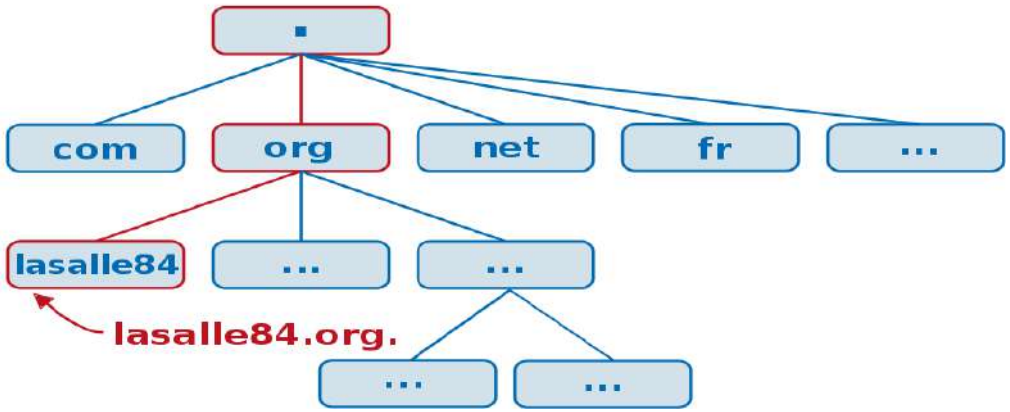
- DNS (*Domain Name System* ou système de noms de domaine) est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

- Avant le DNS, la résolution devait se faire grâce à un fichier texte appelé HOSTS, local à chaque ordinateur. Sous UNIX/Linux, il se trouve dans le répertoire /etc. Sous Windows, il se trouve par défaut dans %SystemRoot %\system32\drivers\etc.

- Avec DNS, la résolution se fait par l'intermédiaire d'un serveur (port 53 sur UDP). Quand un utilisateur souhaite accéder à un serveur web, par exemple celui de fr.wikipedia.org, son ordinateur émet une requête vers un serveur DNS, demandant 'Quelle est l'adresse de fr.wikipedia.org ?'. Le serveur répond en retournant l'adresse IP du serveur, qui est dans ce cas-ci, 91.198.174.2.

DNS (2/2)

- Le système des noms de domaines consiste en une hiérarchie dont le sommet est appelé la racine. On représente cette dernière par un point.
- Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau TLD (*Top Level Domain*). Les noms de domaines ne correspondant pas à une extension de pays sont appelés des domaines génériques (gTLD), par exemple .org ou .com. S'ils correspondent à des codes de pays (fr, be, ch...), on les appelle ccTLD
(*country code TLD*).



FQDN (Fully qualified domain name)

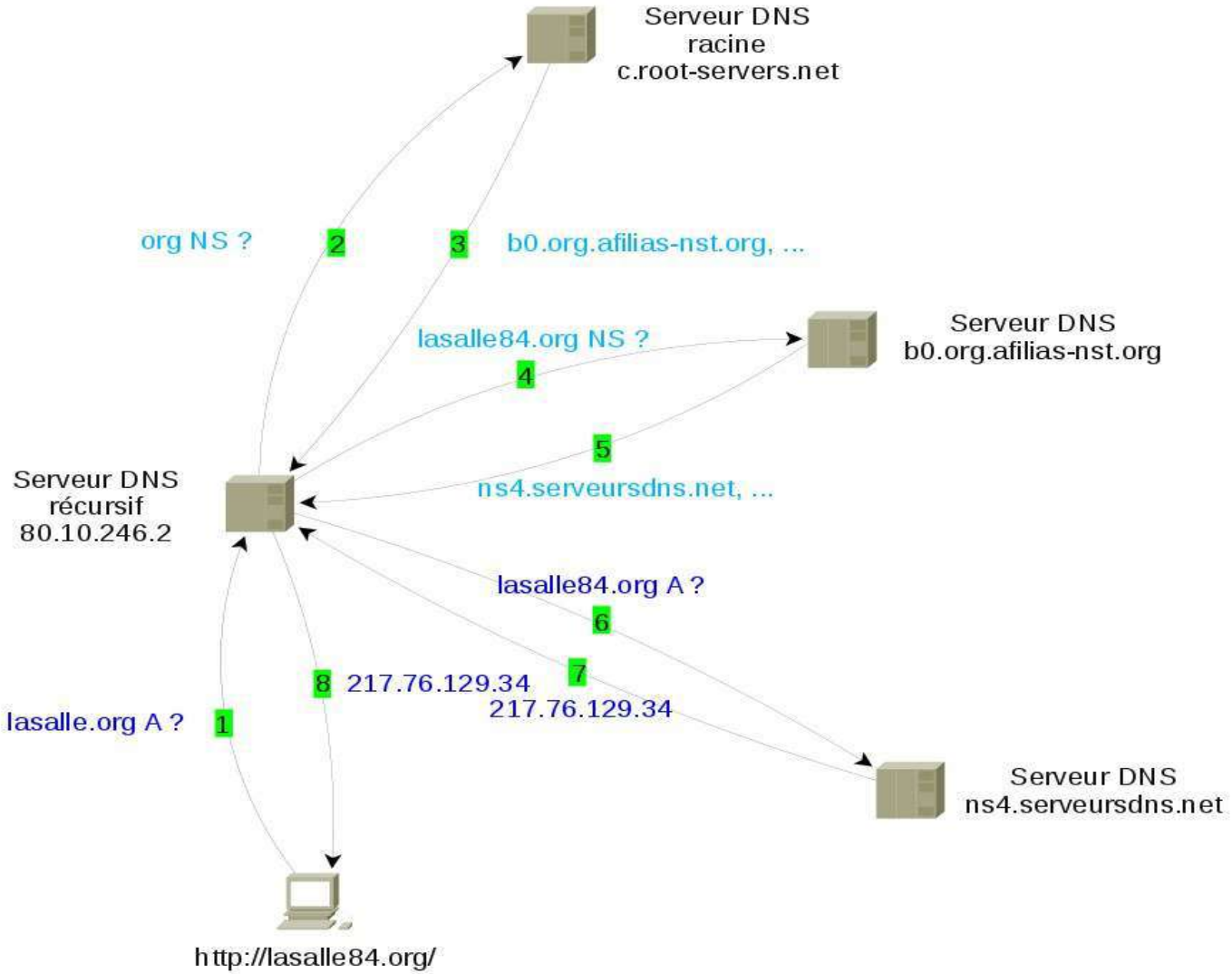
- On entend par FQDN ou Nom de domaine pleinement qualifié un nom de domaine écrit de façon absolue, y compris tous les domaines jusqu'au domaine de premier niveau (TLD), il est ponctué par un point final.

- Dans une réseau TCP/IP, une adresse FQDN sera l'association entre le nom de la machine et le domaine auquel elle appartient.

- *Remarque : la norme prévoit qu'un élément d'un nom de domaine (appelé label) ne peut dépasser 63 caractères, un FQDN ne pouvant dépasser 255 caractères.*

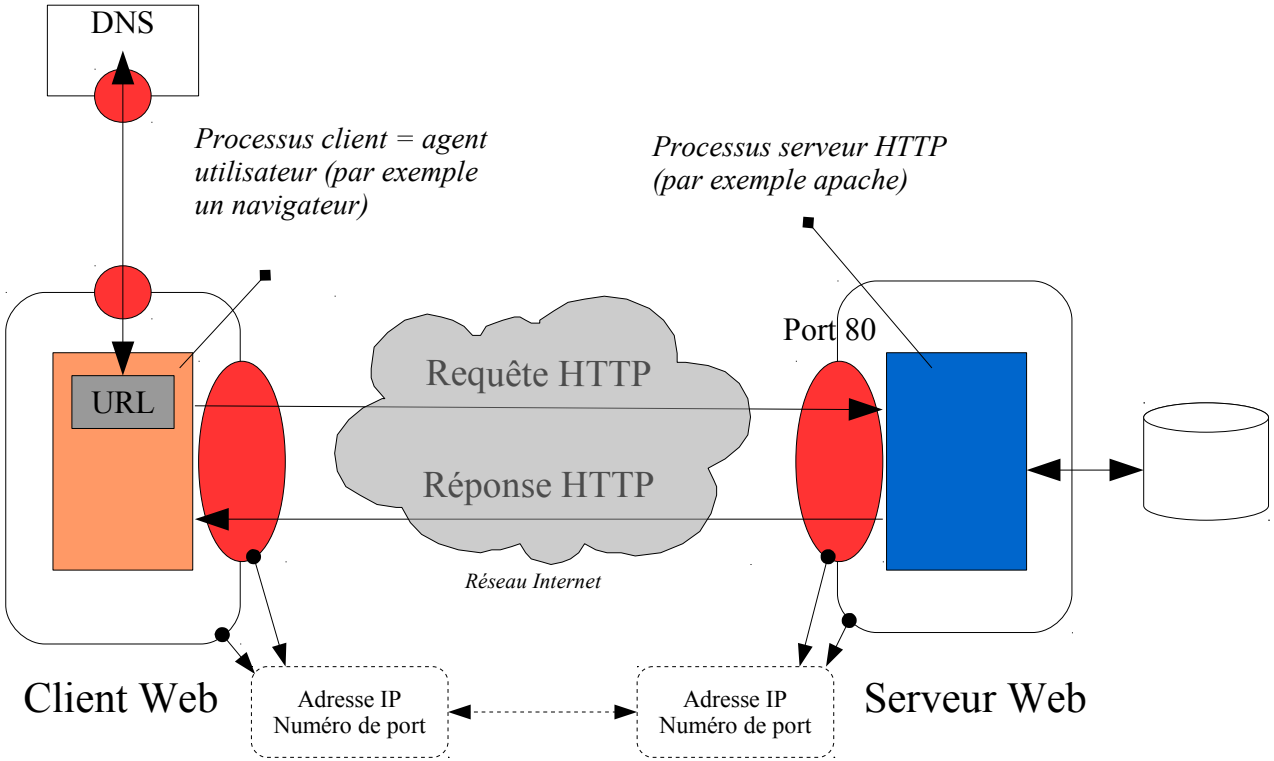
Résolution de nom

Quand un serveur DNS récursif doit trouver l'adresse IP de www.lasalle84.org, un processus itératif démarre pour consulter la hiérarchie DNS.
Ce serveur demande aux serveur DNS appelés serveurs racine que serveurs peuvent lui répondre pour la zone org. Parmi ceux-ci, notre serveur va en choisir un pour savoir quels serveurs sont capables de lui répondre pour la zone lasalle84.org. C'est un de ce derniers qui pourra lui donner l'adresse IP de www.lasalle84.org.
S'il se trouve qu'un serveur ne répond pas, un autre serveur de la liste sera consulté.



Architecture Client/Serveur (1/2)

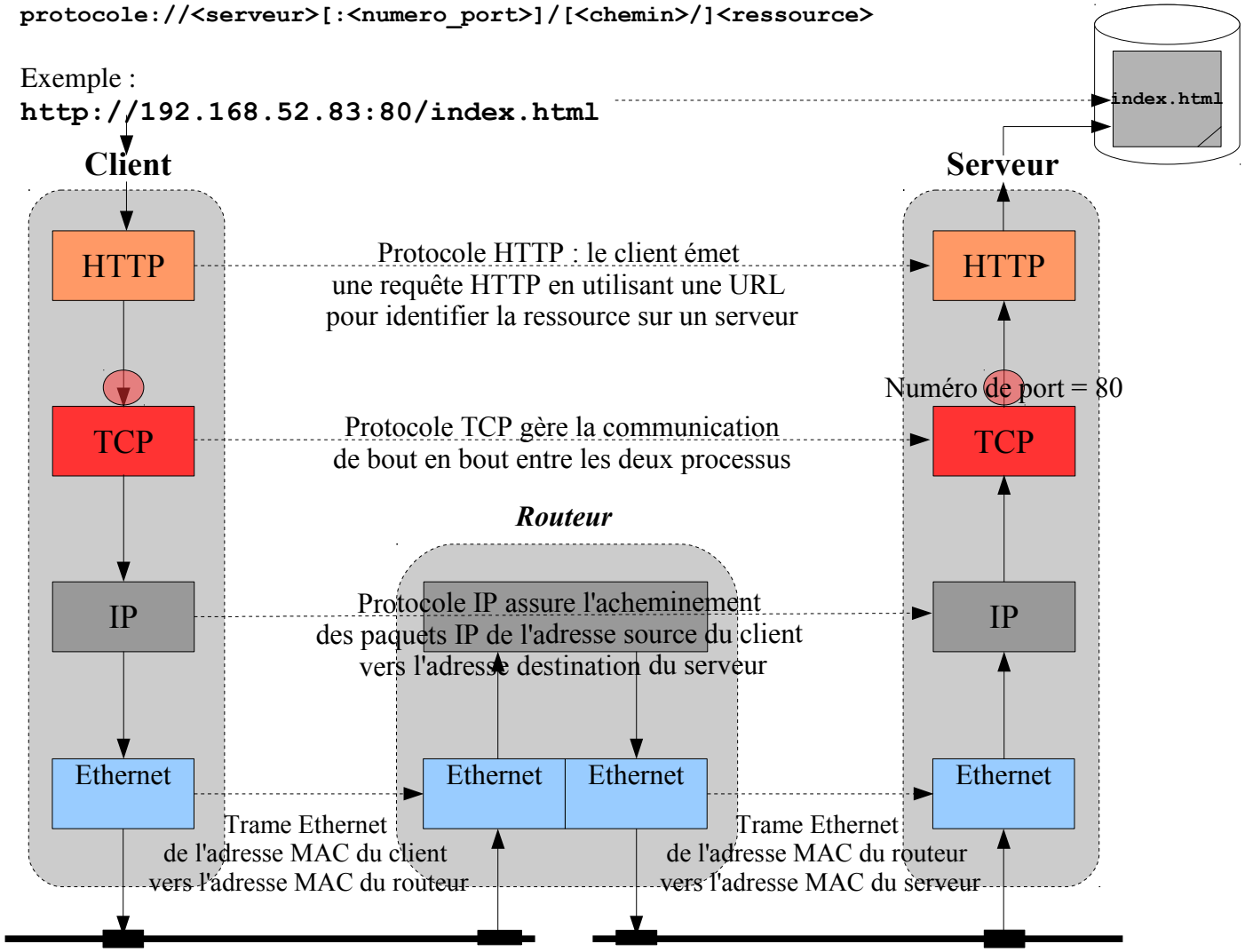
- Serveur : offre un service (en attente)
- Client : demandeur d'un service
- La communication s'initie TOUJOURS à la demande du client.



Architecture Client/Serveur (2/2)

Format d'une URL :
`protocole://<serveur>[:<numero_port>]/[<chemin>/]<ressource>`

Exemple :
`http://192.168.52.83:80/index.html`

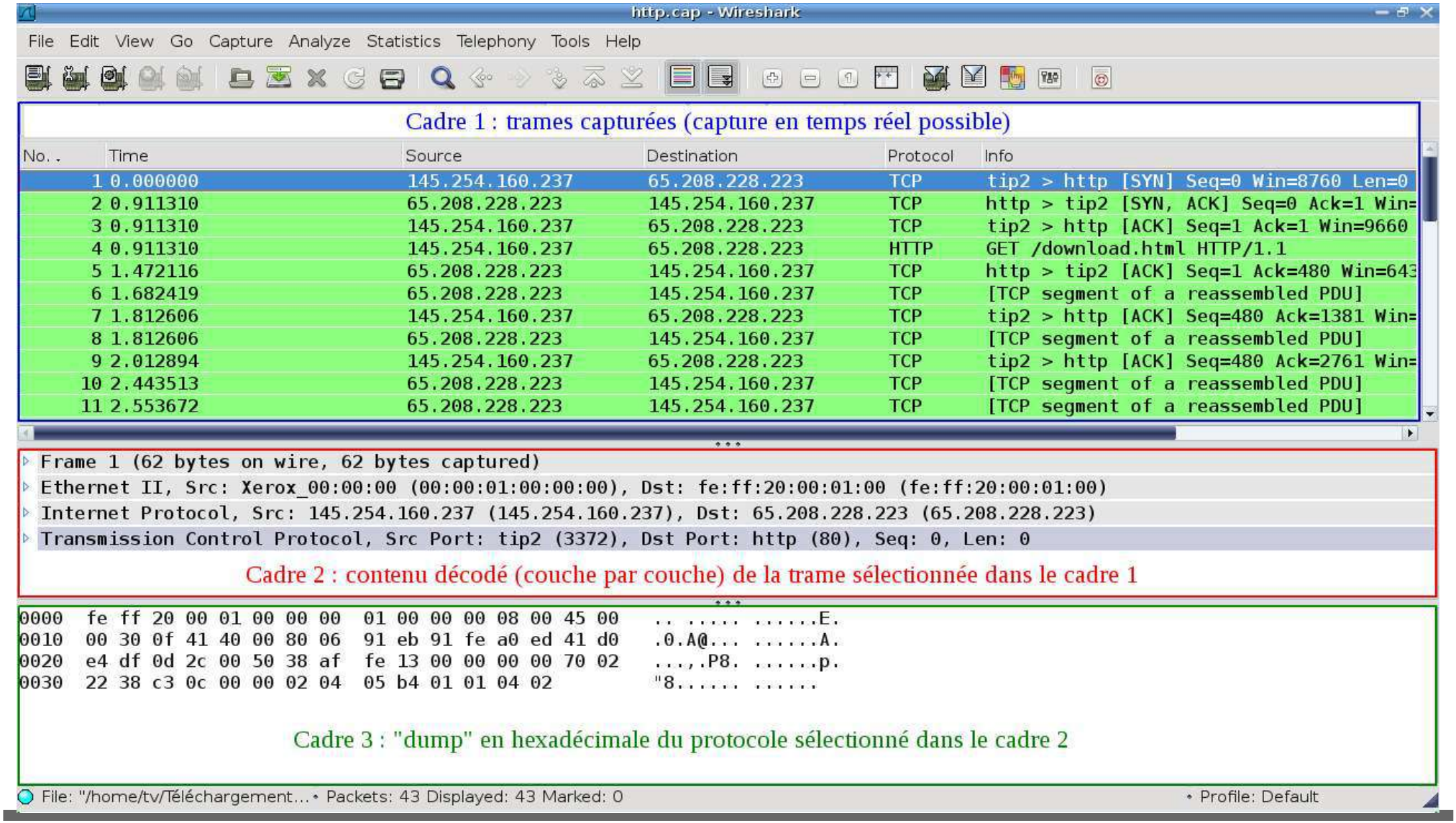


Analyseur de protocole

- tcpdump est un « packet sniffer » en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. C'est un outil de mise au point apprécié pour sa puissance. Site officiel : http://www.tcpdump.org/

- Wireshark (anciennement Ethereal) est un logiciel libre d'analyse de protocole, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark est multi-plates-formes, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles. Site officiel : http://www.wireshark.org/

wireshark


http.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Cadre 1 : trames capturées (capture en temps réel possible)
No. . Time Source Destination Protocol Info
1 0.000000 145.254.160.237 65.208.228.223 TCP tip2 > http [SYN] Seq=0 Win=8760 Len=0
2 0.911310 65.208.228.223 145.254.160.237 TCP http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=
3 0.911310 145.254.160.237 65.208.228.223 TCP tip2 > http [ACK] Seq=1 Ack=1 Win=9660
4 0.911310 145.254.160.237 65.208.228.223 HTTP GET /download.html HTTP/1.1
5 1.472116 65.208.228.223 145.254.160.237 TCP http > tip2 [ACK] Seq=1 Ack=480 Win=643
6 1.682419 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
7 1.812606 145.254.160.237 65.208.228.223 TCP tip2 > http [ACK] Seq=480 Ack=1381 Win=
8 1.812606 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
9 2.012894 145.254.160.237 65.208.228.223 TCP tip2 > http [ACK] Seq=480 Ack=2761 Win=
10 2.443513 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
11 2.553672 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
Frame 1 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
Cadre 2 : contenu décodé (couche par couche) de la trame sélectionnée dans le cadre 1
0000 fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00 .. ..E.
0010 00 30 0f 41 40 00 80 06 91 eb 91 fe a0 ed 41 d0 .0.A@... ......A.
0020 e4 df 0d 2c 00 50 38 af fe 13 00 00 00 00 70 02 ...,.P8. ......p.
0030 22 38 c3 0c 00 00 02 04 05 b4 01 01 04 02 "8..... ......
Cadre 3 : "dump" en hexadécimale du protocole sélectionné dans le cadre 2
File: "/home/tv/Téléchargement... Packets: 43 Displayed: 43 Marked: 0
Profile: Default

Notions d'API

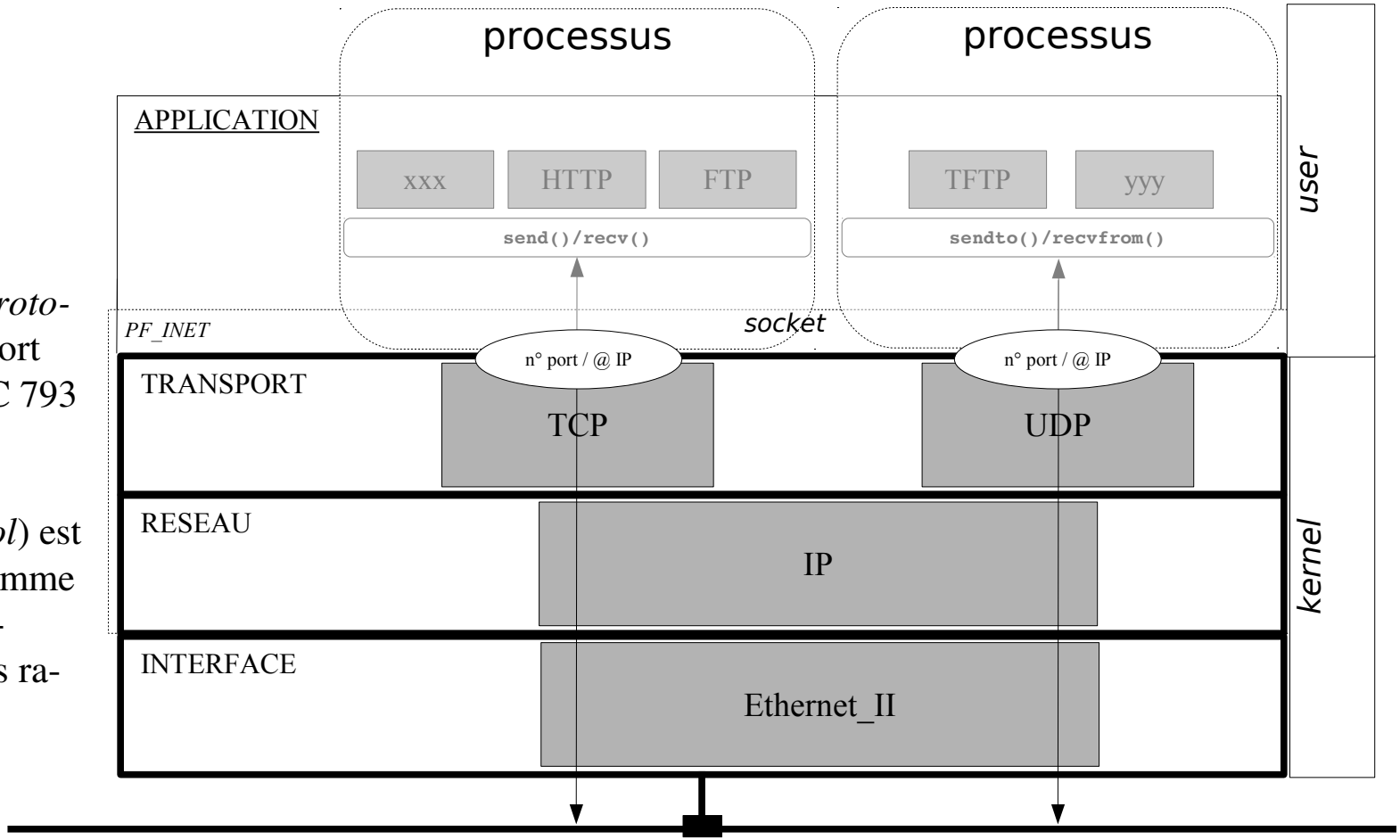
- Les services offerts par une couche constituent l'interface à la couche supérieure.
- Cette interface est implémentée sous forme de bibliothèque de fonctions soit une **API** (*Application Program Interface*).
- Le développeur utilisera donc concrètement une interface pour programmer une application TCP/IP grâce par exemple :
  - à l'API Socket BSD sous Unix/Linux ou
  - à l'API WinSocket sous Windows
- Une ***socket*** est un point de communication par lequel un processus peut émettre et recevoir des informations. Ce point de communication devra être relié à une adresse IP et un numéro de port.
- Une ***socket*** est communément représentée comme un point d'entrée initial au niveau TRANSPORT du modèle à couches dans la pile de protocole.

L'interface *socket*

- En programmation, on utilisera l'interface *socket* pour réaliser des applications réseaux :

TCP (*Transmission Control Protocol*) est un protocole de transport fiable, en mode connecté (RFC 793).

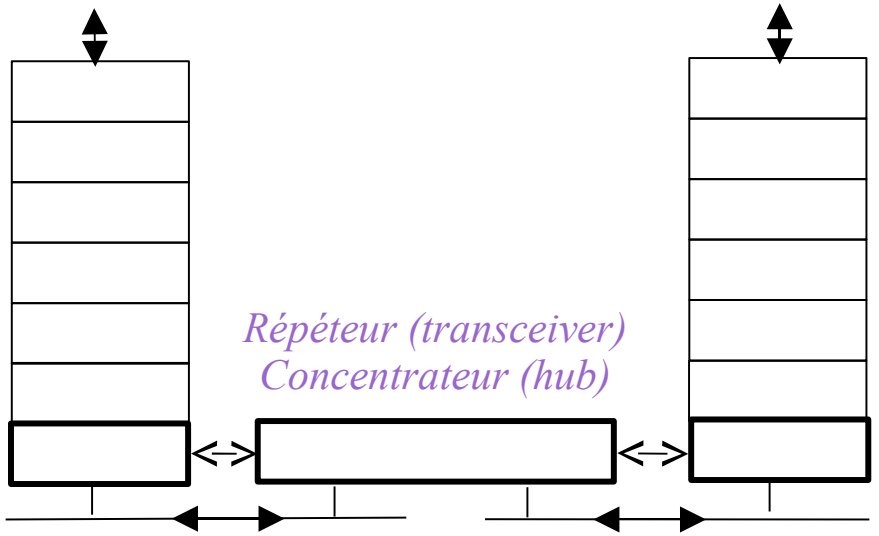
UDP (*User Datagram Protocol*) est un protocole souvent décrit comme étant non-fiable, en mode non-connecté (RFC 768), mais plus rapide que TCP.



Interconnexion de niveau 1

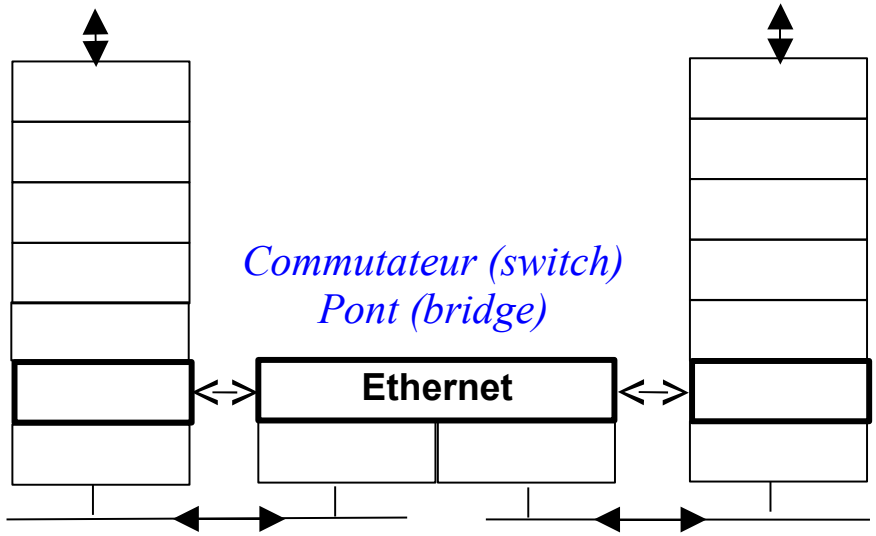
- ***Fonctions** d'un répéteur :*
  - la répétition des bits d'un segment sur l'autre (augmenter la distance)
  - la régération (amplification) du signal pour compenser l'affaiblissement
  - le changement du support physique
- Remarque : la trame n'est jamais modifiée lors de la traversée d'un répéteur.
- Le HUB se comporte comme un répéteur multi-ports. Avec HUB 100Mbps, on obtient un débit partagé de 100Mbps pour l'ensemble des équipements raccordés.

Remarque : dans un réseau Ethernet, une seule des machines connectées peut transmettre à la fois. Dans le cas contraire, une collision se produit, les machines concernées doivent retransmettre leurs trames après avoir attendu un temps calculé aléatoirement par chaque émetteur (méthode d'accès CSMA/CD).



Interconnexion de niveau 2

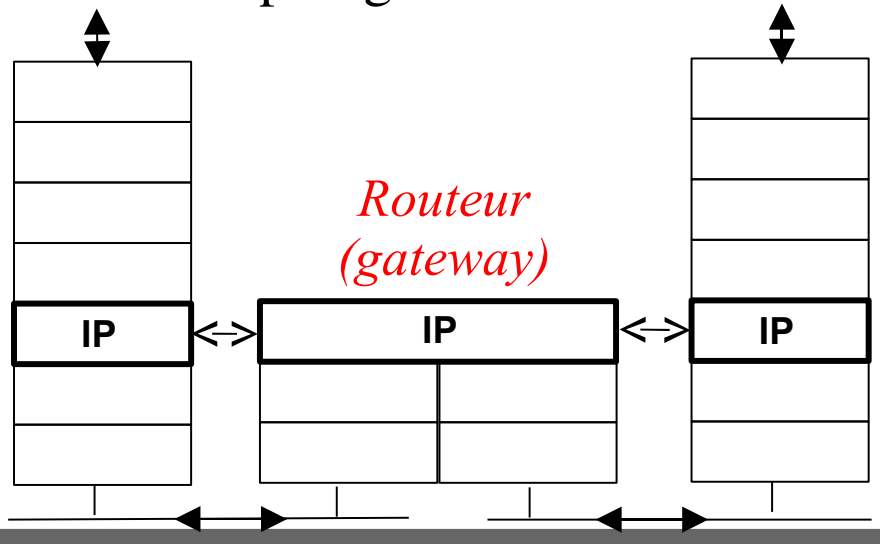
- ***Fonctions** d'un pont ou d'un commutateur :*
  - analyser les trames qui circulent sur chaque segment ;
  - stocker et mettre à jour périodiquement la table de correspondance @ MAC/n°de port (possibilité de gérer des VLAN) ;
  - filtrer les trames en fonction de l'@ MAC du destinataire (segmentation de réseaux physiques)
  - assurer les fonctions d'un répéteur
- Dans le cadre d'un switch 100Mbps, on obtient un débit dédié de 100Mbps par port. Les caractéristiques principales à vérifier pour choisir un switch sont :
  - le nombre d'adresse MAC maximum qui peuvent mise en mémoire
  - le nombre de paquet par seconde (PPS) que la matrice de fond de panier peux commuter
  - manageable ou standard, supervision (SNMP)
- Le pont permet d'interconnecter deux réseaux de couche liaison différente. Par exemple, on trouvera des ponts permettant de relier des réseaux Ethernet et Token Ring.



Interconnexion de niveau 3

- *Les **fonctions** assurés par le routeur sont :*
  - traiter et **router** les paquets des protocoles de niveau 3 (IP) ;
  - mettre à jour ses tables de routage (routage dynamique) en dialoguant avec d'autres routeurs et en utilisant des protocoles spécifiques (RIP, OSPF, EGP, BGP, …)
  - dialoguer avec d'autres routeurs (protocole ICMP) pour signaler des congestions, synchroniser des horloges, estimer les temps de transit, ...
  - interconnecter toutes les topologies.

Remarque : une adresse IP par interface



Synthèse des équipements d'interconnexion

- Une synthèse comparative des différents équipements Ethernet :

	Répéteur	HUB	Switch	Pont	Routeur
Agit sur la couche du modèle OSI	1	1	2	2	3
Permet de relier plusieurs équipements	Non	Oui	Oui	Oui	Oui
Fournit un débit dédié par interface	Non	Non	Oui	Oui	Oui
Sépare les domaine de braodcast niveau 2	Non	Non	Non	Oui	Oui
Sépare les domaine de braodcast niveau 3	Non	Non	Non	Non	Oui

www.frameip.com

Routage

- Le routage consiste à **déterminer la route qu'un paquet doit prendre pour atteindre une destination**.
- Cette tâche est réalisée au niveau de la **couche RESEAU** du modèle à couches : dans cette couche, on utilise un adressage qui permet de spécifier à quel réseau appartient un équipement (hôte ou routeur). Les équipement (hôtes ou routeurs) qui se situent sur des réseaux différents devront utiliser les services d'un **routeur** (*gateway* dans la terminologie IP) pour communiquer.
- Les **fonctions** au niveau de la **couche RESEAU** sont :
  - **Acheminer** (hôte ou routeur) : envoyer un paquet vers une destination (hôte ou routeur)
  - **Relayer** (routeur) : acheminer un paquet d'un réseau vers un autre réseau
- Chaque équipement (hôte ou routeur) achemine un paquet en fonction de l'**adresse IP destination** uniquement.
- Pour **déterminer la route** à prendre, le pilote IP utilise sa **table de routage** qui indique pour chaque destination (hôte, réseau ou sous-réseau), la route (interface ou passerelle) à prendre : c'est le routage de proche en proche.

Différents types de routage

- On distingue :
  - **Le routage statique** si les routes sont fixées manuellement par l'administrateur réseau
  - **Le routage dynamique** si les tables de routages sont automatiquement mises à jour pour tenir compte d'une modification du réseau global (panne de routeur, nouvelle route, …)
- Il y a deux types de routage :
  - Le routage direct : Délivrance d'un paquet à un hôte qui appartient au même réseau physique
  - Le routage indirect : Délivrance d'un paquet à un hôte qui appartient à un réseau physique différent
- Le routage s'effectue en consultant une table de routage (contenant des routes) et en appliquant un algorithme pour déterminer la route à prendre en fonction de l'adresse destination.
- Les tables de routage doivent être configurées sur l'ensemble des équipements (hôtes et routeurs) :
  - Cas des hôtes : les tables de routages des postes se limitent souvent à une route par défaut vers le routeur (*gateway*, donc souvent passerelle en français) qui permettra de sortir du réseau physique.
  - Cas des routeurs : les tables de routages sont donc configurées principalement au niveau des routeurs manuellement (routage statique) ou automatiquement acquises par dialogue entre routeurs (routage dynamique).

Algorithme de routage

- L'algorithme a évolué pour tenir compte l'abandon de la notion de classe. Ceci conduit à utiliser seulement le *netmask* pour déterminer la taille du réseau. On utilise aussi le terme **CIDR** (*Classless InterDomain Routing*).

```
POUR une adresse IP destination
 trouvé ← rechercher dans la table de routage le préfixe
 le plus long (netmask) qui correspond à l'adresse desti
 nation
 SI trouvé
  ALORS  envoyer le paquet
  SINON  renvoyer le message : "Destination unreacheable"
 FSI
FPOUR
```

Remarques : la route par défaut est notée 0.0.0.0, soit un masque de longueur nulle et toutes les adresses destinations correspondront. Les routes vers des hôtes utiliseront un masque de 255.255.255.255 pour obtenir une correspondance exacte.

Table de routage

- Une table de routage indique pour chaque destination (hôte, réseau ou sous-réseau) la route (interface ou passerelle) qu'il faut prendre. Les informations pour chaque route sont donc les suivantes :

Aller vers	*Passer par*
la destination (hôte ou réseau)	**la route**
Champs: Destination et Genmask	*Champs:* Passerelle et Iface

- Pour afficher une table de routage, on utilise les commandes **`nestat`** ou **`route`**. Il existe de nombreux champs supplémentaires dont :
  - Le champ Indic (*Flags*) qui indique si :
    - U (*Up*) : la route est active
    - H (*Host*) : la route conduit à un hôte
    - G (*Gateway*) : la route passe par une passerelle (voisine)
  - Le champ Métrique (*Metric*) indique la distance, en nombre de passerelles, pour atteindre la destination

Routage statique et dynamique

- Le routage statique, utilisé dans les réseaux de petite taille, est réalisé manuellement par l'administrateur réseau. On l'utilise notamment pour : les postes de travail (route par défaut) ou pour un routeur avec une route par défaut vers le Fournisseur d'Accès Internet (ou ISP: *Internet Service Provider*)

Avantages	***Inconvénients***
Utilisation de fichiers de configuration donc stabilité de la configuration	Si le réseau comporte de nombreux routeurs : - tâche fastidieuse - risque d'erreur important
	Impossibilité pour gérer les routes redondantes

- Le routage dynamique est assuré par les routeurs eux-même en s'échangeant des informations sur leurs tables de routage et nécessite un protocole de routage

Avantages	***Inconvénients***
Simplicité de la configuration	Dépend du protocole de routage utilisé et de la taille du réseau : - consommation de la bande passante - temps de convergence - sécurité
Adaptabilité à l'évolution du réseau	
Optimisation (sélection des meilleurs routes)	
Elimination des boucles de routage	

Protocoles de routage

- Il faut distinguer deux types de domaine de routage :
  - **IGP** (*Interior Gateway Protocol*) : protocole de routage interne utilisé au sein d'une même unité administrative (AS) ;
  - **EGP** (*Exterior Gateway Protocol*) : protocole de routage externe utilisé entre passerelles appartenant à des unités administratives différentes (AS)

	Internet	***ISO***
Routage intra-domaines IGP Taille < 100 routeurs	On distingue deux types de protocoles : **- distance vecteur** (*distant vector*) : RIP (*Routing Information Protocol*), IGRP (*Internet Gateway Routing Protocol*) de la société CISCO (le protocole a été amélioré sous le nom EIGRP) **- état de liens** (*link state*) : OSPF (*Open Shortest Path First*)	IS-IS (*Intermediate System to Intermediate System*)
Routage inter-domaines EGP Taille = Internet	EGP (*Exterior Gateway Protocol*) : obsolète, remplacé par BGP (*Border Gateway Protocol*)	IDRP (*Inter Domain Routing Protocol*)
Entre équipement et routeur	ICMP *Redirect*	IS-ES

Pare-feu (*firewall*)

- Un système pare-feu (*firewall*) est un dispositif conçu pour examiner et éventuellement bloquer les échanges de données entre réseaux. C'est donc un élément de sécurité.
- Le pare-feu joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle DoD ou OSI (analyse des en-têtes des protocoles).
- Il existe trois types principaux de pare-feu :
  - filtrage de paquets : adresse source et destination, protocole et numéro de ports
  - filtrage de paquets avec état (*firewall stateful*) : assure un suivi de session et de connexion
  - proxy : jusqu'à la couche application

- Les fabricants de pare-feu ont tendance à intégrer un maximum de fonctionnalités :
  - filtrage de contenu (URL, *spam* mails, code ActiveX, applets Java, …), réseau virtuel privé (VPN), détection d'intrusions (IDS), tolérance de pannes (haute disponibilité, équilibrage de charge, NAT, ...

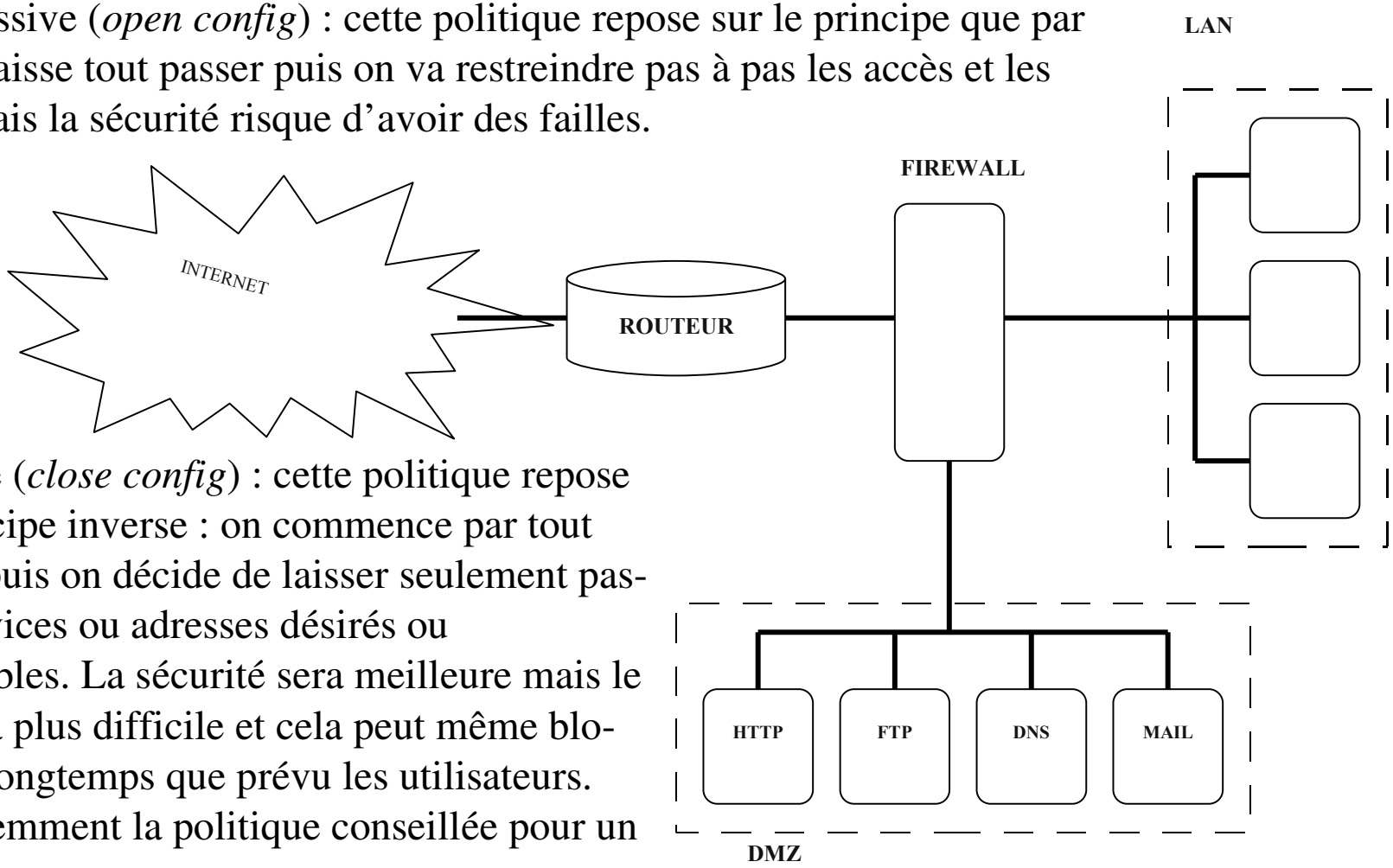
DMZ (*De-Militarized Zone*)

- Il existe plusieurs **zones de sécurité** commune aux réseaux. Ces zones déterminent un niveau de sécurité en fonction des accès réseaux et donnent les bases de l'architecture.

- On considère en général trois zones ou réseaux :
  - Réseaux externes : c'est le réseau généralement le plus ouvert. L'entreprise n'a pas ou très peu de contrôle sur les informations, les systèmes et les équipements qui se trouvent dans ce domaine.
  - Réseaux internes : les éléments de ce réseau doivent être sérieusement protégés. C'est souvent dans cette zone que l'on trouve les mesures de sécurité les plus restrictives et c'est donc le réseau le moins ouvert.
  - Réseaux intermédiaires : cette zone est un compromis entre les deux précédentes. Ce réseau est composé de services fournis aux réseaux internes et externes. Les services publiquement accessibles (serveurs de messagerie, Web, FTP et DNS le plus souvent) sont destinés aux utilisateurs internes et aux utilisateurs par Internet. Cette zone, appelée **réseau de service** ou de **zone démilitarisée** (**DMZ** *De-Militarized Zone*), est considérée comme la zone moins protégée de tout le réseau de l'entreprise.

Politique de sécurité

- Politique de sécurité
  - Politique permissive (*open config*) : cette politique repose sur le principe que par défaut on laisse tout passer puis on va restreindre pas à pas les accès et les services mais la sécurité risque d'avoir des failles.



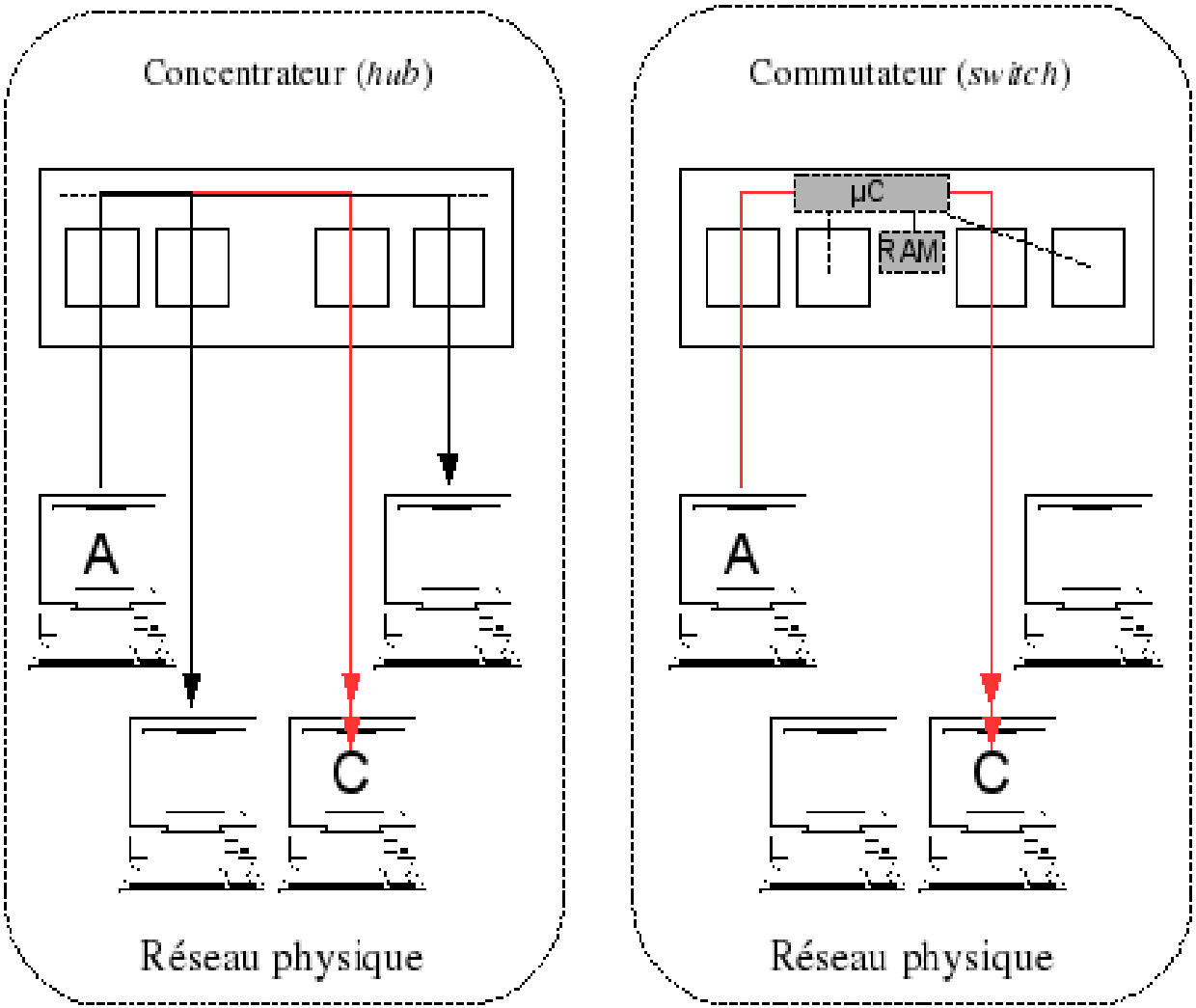
  - Politique stricte (*close config*) : cette politique repose sur le principe inverse : on commence par tout interdire, puis on décide de laisser seulement passer les services ou adresses désirés ou indispensables. La sécurité sera meilleure mais le travail sera plus difficile et cela peut même bloquer plus longtemps que prévu les utilisateurs. C'est évidemment la politique conseillée pour un pare-feu.

Serveur mandataire (*proxy*)

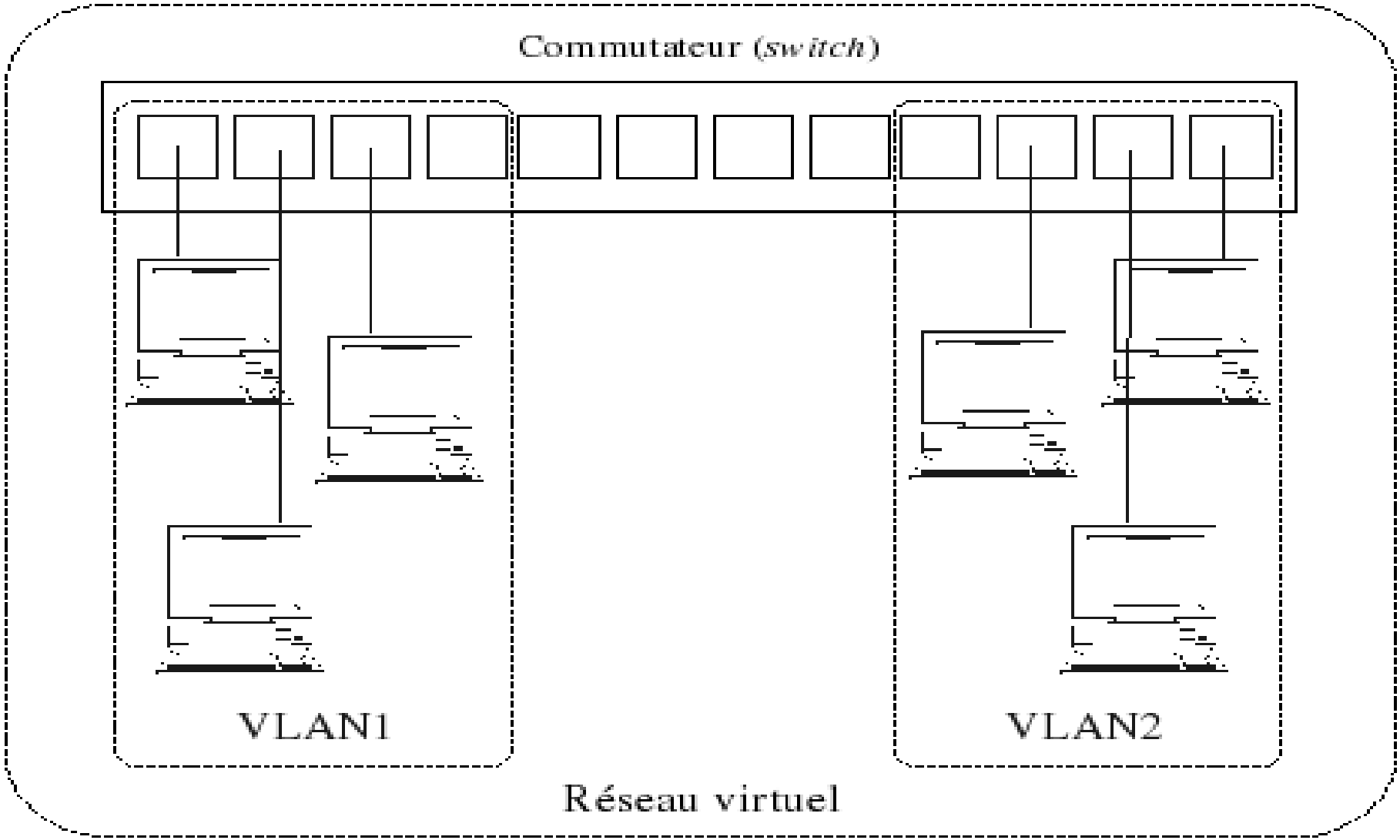
- Un serveur mandataire ou *proxy* est un serveur qui a pour fonction de relayer des requêtes entre un poste client et un serveur d'application.

- Les serveurs proxy sont notamment utilisés pour assurer les fonctions suivantes :
  - mémoire cache (amélioration des performances)
  - la journalisation des requêtes (« logging »)
  - la sécurité du réseau local
  - le filtrage et l'anonymat
  - l'authentification pour autoriser ou non l'accès au service

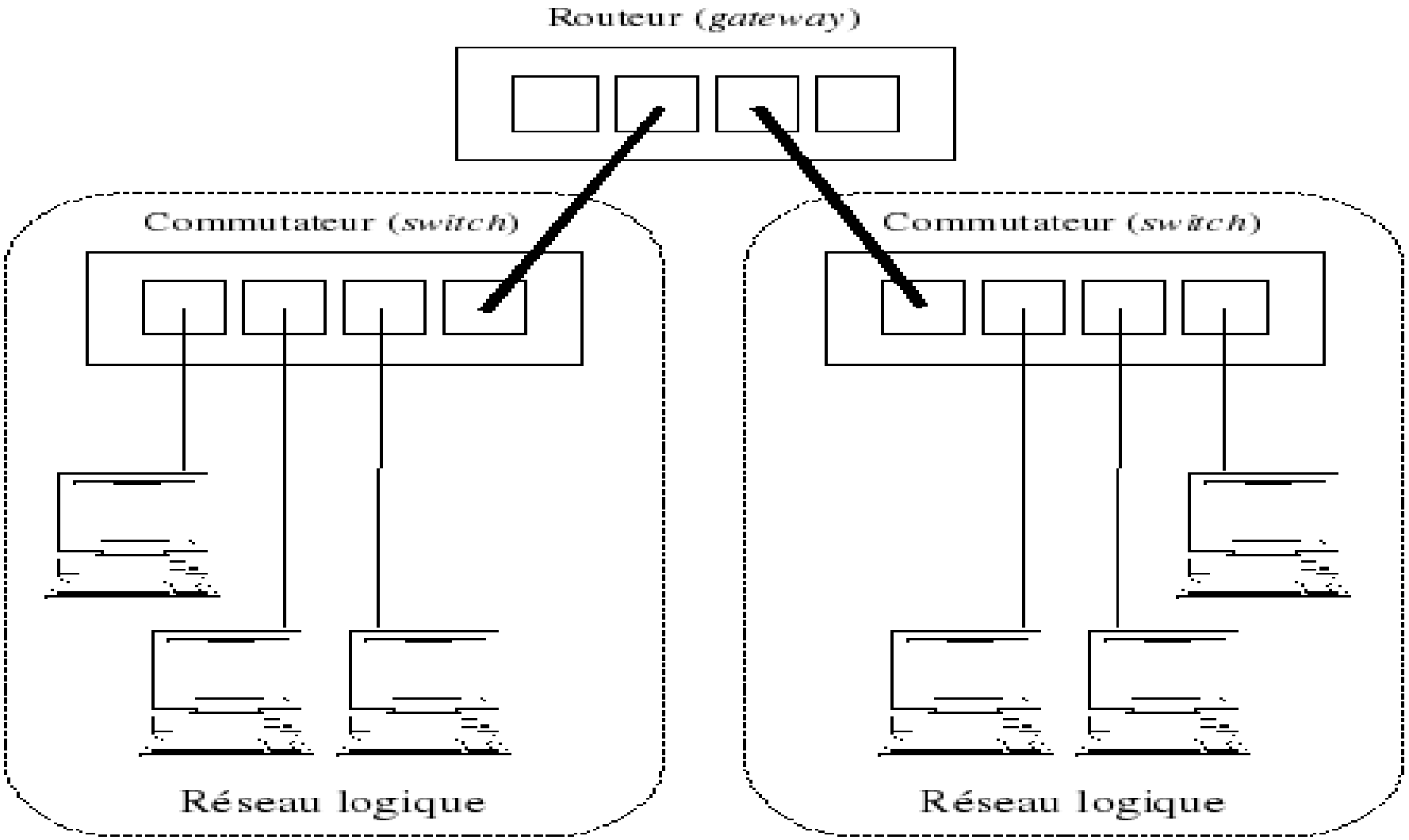
Réseau physique



Réseau virtuel

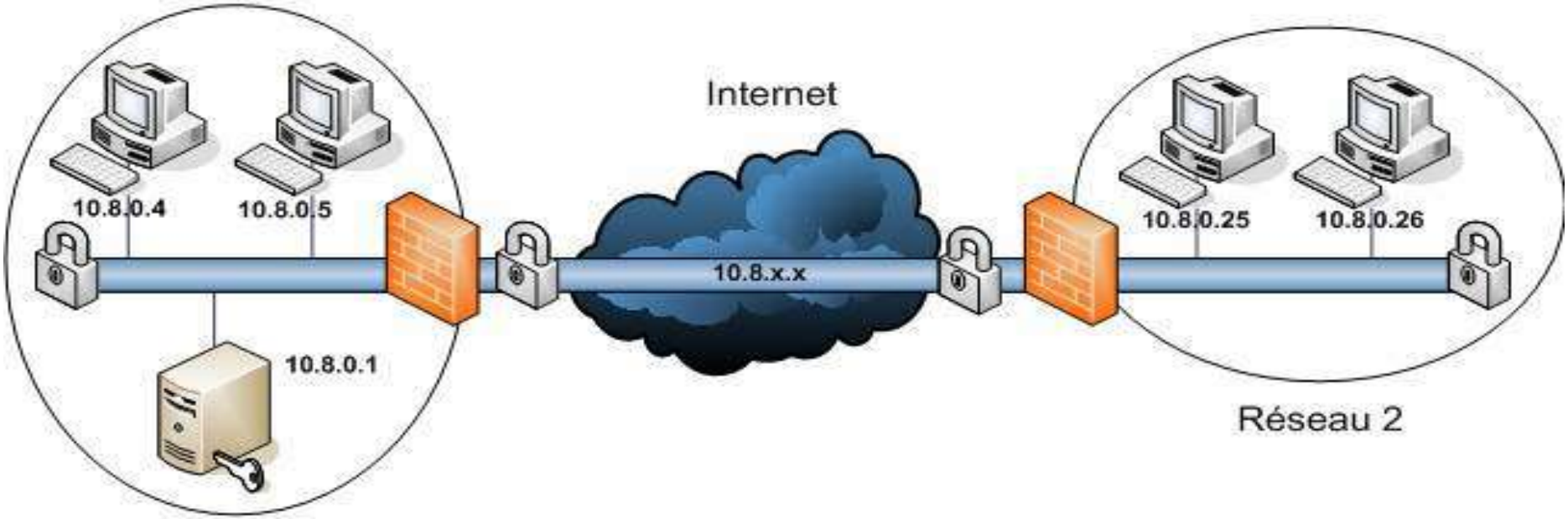


Réseau logique



Réseau privé virtuel

- Le réseau privé virtuel VPN (*Virtual Private Network*) est vu comme une extension des réseaux locaux et préserve la sécurité que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel » (*tunneling*), c'est-à-dire en encapsulant les données à transmettre de façon chiffrée. Les principaux protocoles de tunnelisation sont : L2TP, IPsec et aussi SSH.



Les commandes de base

Description	*Linux*	*Windows*
Configurer une interface réseau	ifconfig	ipconfig, netsh, net
Afficher les connexions réseau, les tables de routage, les statistiques des interfaces, ...	netstat	netstat
Envoyer des datagrammes ICMP ECHO_REQUEST à des hôtes sur un réseau	ping	ping
Afficher le chemin qu'un paquet IP va prendre pour aller d'une machine A à une machine B	traceroute	tracert
Suivre le chemin qu'un paquet IP va prendre pour aller d'une machine A à une machine B pour découvrir le MTU à utiliser sur ce chemin	tracepath	
Afficher et manipuler la table de routage IP	route	route
Manipuler la table ARP du système	arp	arp
Outil d'analyse et de capture réseau	ethereal/wireshark tcpdump	ethereal/wireshark windump
Outil d'exploration réseau et analyseur de sécurité	nmap	nmap
Fournir un moyen de communication TCP bi-directionnel et orienté octet (caractère)	telnet	telnet, putty
Lire et écrire en utilisant TCP ou UDP	netcat	netcat
Remarque :		
Accès aux options des commandes	nom_commande -h nom_commande --help	nom_commande /?
Accès à la documentation	man nom_commande	

Les fichiers de configuration

Description	*Linux*	*Windows*
Configuration réseau	**Fichiers texte dans /etc/ /proc/net**	**Panneau de configuration Base de registre (regedit)**

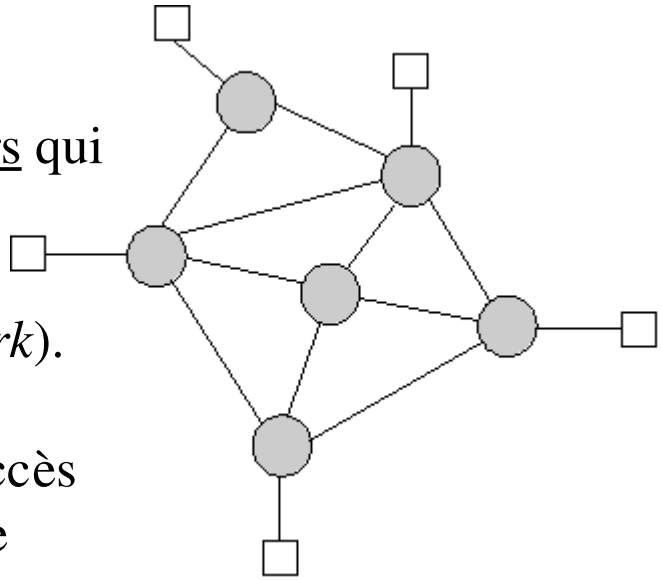
Fichier	*Description*
Mandriva : `/etc/sysconfig/network-scripts/ifcfg-eth0` **Ubuntu : `/etc/network/interfaces`**	Configuration des interfaces
`/etc/host.conf`	Configuration de la résolution de noms
`/etc/hosts`	Correspondances statiques de noms d'hôtes
`/etc/ethers`	Base de données adresses Ethernet - adresses IP
`/etc/resolv.conf`	Fichier de configuration de la résolution de noms
`/etc/protocols`	Fichier de définition des protocoles internet
`/etc/services`	Liste des services internet

Internet (I) : historique

- 1958 : La BELL crée le premier Modem permettant de transmettre des données binaires sur une simple ligne téléphonique
- 1961 : Leonard Kleinrock du MIT publie une première théorie sur l'utilisation de la commutation de paquets pour transférer des données
- 1962 : Début de la recherche par ARPA, une agence du ministère de la Défense américain
- 1964 : Leonard Kleinrock du MIT publie un livre sur la communication par commutation de paquets pour réaliser un réseau
- 1969 : Connexion des premiers ordinateurs sur l'ARPANET
- 1979 : Création des NewsGroups (forums de discussion) par des étudiants américains
- 1982 : Définition du protocole TCP/IP et du mot « Internet »
- 1983 : Premier serveur de noms de sites (DNS)
- 1988 : Première connexion Internet en France
- 1991 : Annonce publique du *World Wide Web* qui est basé sur trois inventions, le protocole de communication client/serveur HTTP (*Hypertext Transfer Protocol*), les adresses web (URI/URL) et le langage HTML (*HyperText Markup Language*).
- 1994 : Premier moteur de recherche

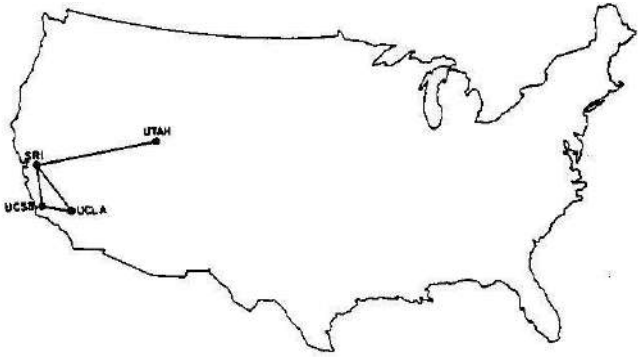
Internet (II) : un réseau de réseaux

- Un réseau de réseaux
  - Internet est un réseau public mondial qui relie des milliers de réseaux plus petits ou des ordinateurs isolés.
  - L'interconnexion des réseaux est réalisé par des routeurs qui donnent une topologie de type maillé.
  - Internet est un réseau de type WAN (*Wide Area Network*).
  - Le plus souvent, on passe par un FAI (Fournisseur d'Accès Internet) ou ISP (*Internet Service Provider*) pour se connecter (raccorder) au réseau Internet.

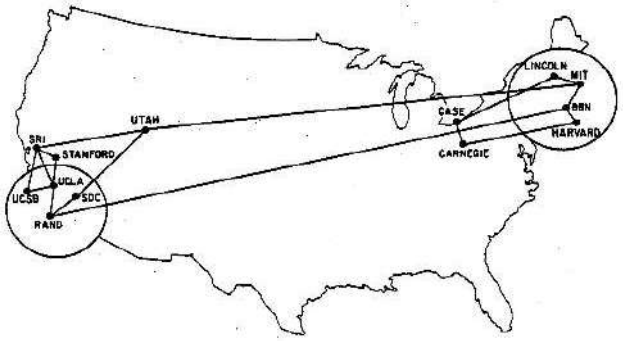


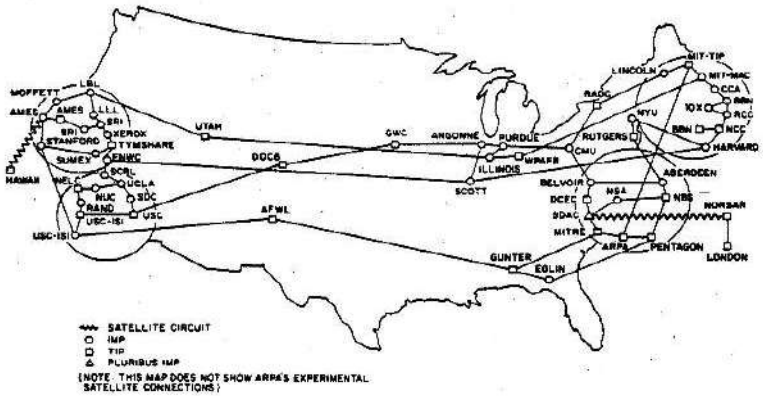
Internet (III) : évolution

- Depuis 2006, il y a plus d'un milliard d'ordinateurs connectés à Internet ...



Il y a seulement 4 noeuds à la création du réseau ARPAnet fin 1969.





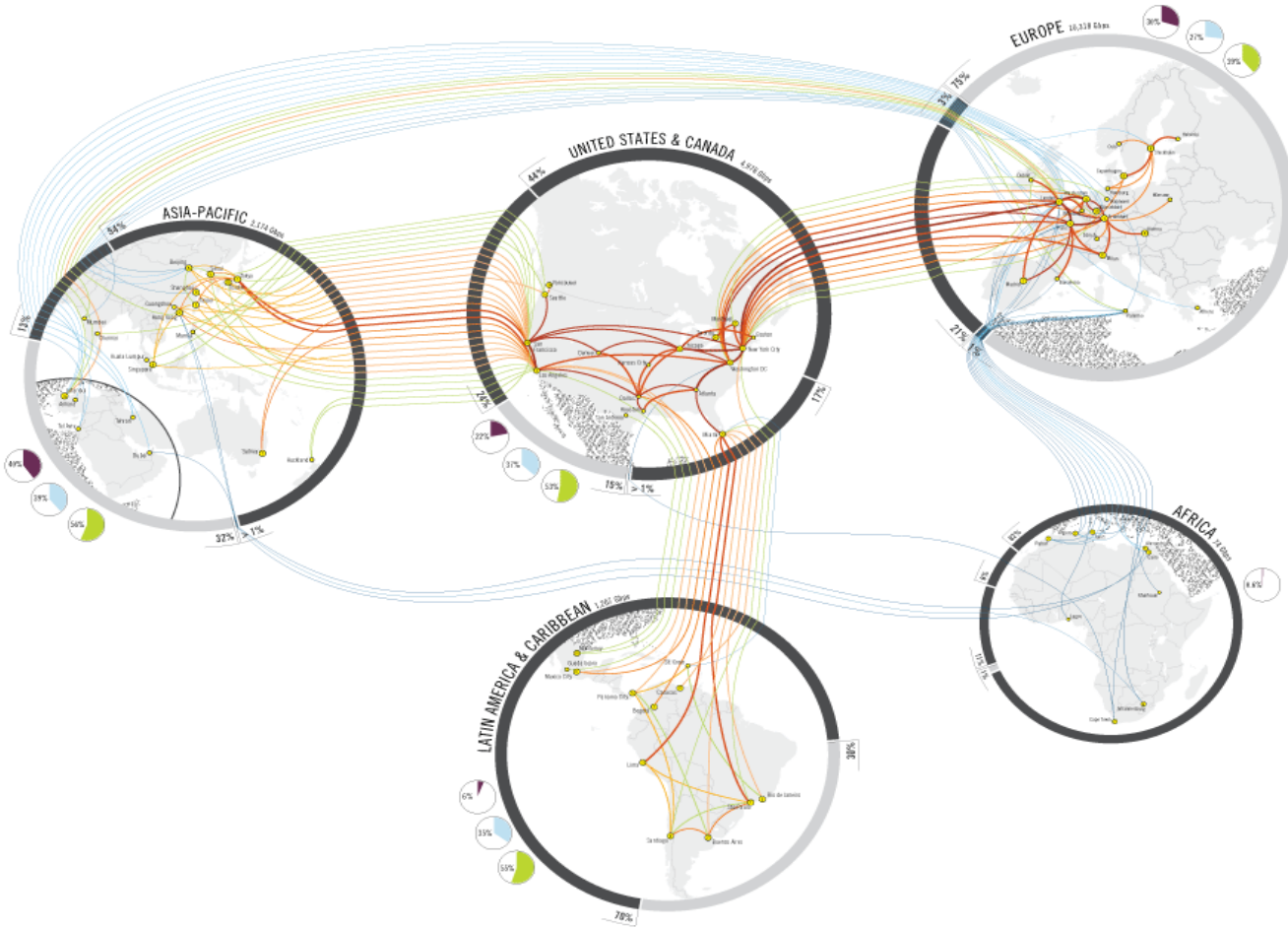
Un an plus tard, fin 1970, il y a 13 noeuds d'interconnectés, le réseau maillé se construit ...

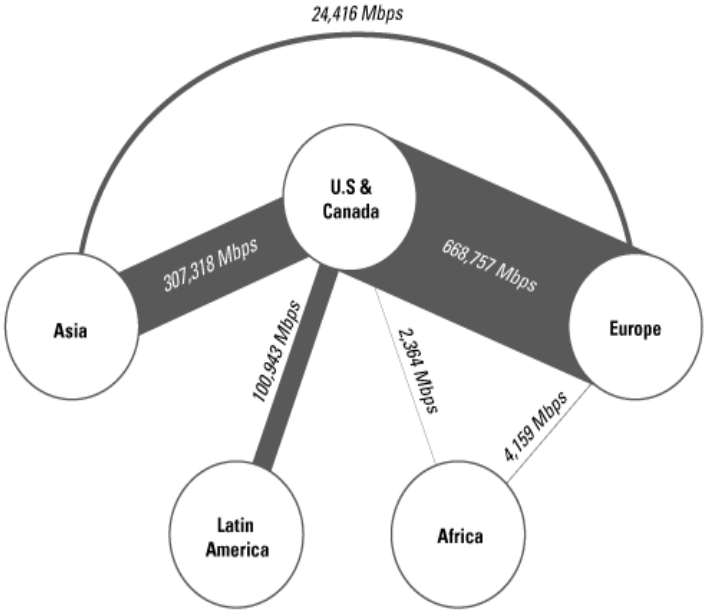
Il y aura plus de 100 000 noeuds à la fin des années 80

L'équipe de Christian HUITEMA à l'INRIA Sophia Antipolis réalise la première connexion Internet en France en juillet 1988.

Internet (IV) : réseau mondial

- Source : http://www.telegeography.com/ee/free_resources/





Internet (V) : un réseau de services

- Un réseau de services
  - On utilise le réseau Internet pour les services qu'il propose : web, messagerie, ...
  - Les services Internet sont fournis par des serveurs. Les demandeurs du service sont nommé les clients. L'architecture qui en découle se nomme client/serveur.
  - Chaque service, pris en charge par un processus, est identifié par un numéro de port.
  - Chaque service est associé à un protocole (couche Application) :
    - Web (www) : HTTP - Transfert de fichiers : FTP, BitTorrent, eDonkey, ...
    - Courrier électronqiue (mail) : SMTP, POP, IMAP, ...
    - Messagerie instantanée : AIM, ICQ, Jabber, XMPP, MSN Messenger, ...
    - Discussion (chat) : IRC - Système de fichiers : NFS, SMB, ...
    - Session distante (émulation de terminal) : Telnet, Rlogin, SSH, ...
    - Forum de discussion (news) : NNTP (Usenet), ... - Supervision : SNMP, ...
    - Résolution d'adresse DNS - Synchronisation horaire NTP - Affichage distant XDMCP
    - etc ...

Internet (VI) : RFC

- Les *Requests For Comment* (RFC), littéralement demande de commentaires, sont une série numérotée de documents électroniques documentant les aspects techniques d'Internet.
- Peu de RFC sont des standards, mais tous les standards d'Internet sont des RFC.
- Les RFC sont rédigées pas des experts techniques. En mai 2008, le nombre de RFC a atteint les 5 000.
- La première RFC (RFC 1), titrée "Logiciel hôte", a été publiée le 7 avril 1969 par Steve Crocker.

Terminologie Internet

- Une passerelle (*gateway*) est un dispositif permettant de relier deux réseaux informatiques, comme par exemple un réseau local et Internet. Cependant, le terme passerelle (sans autre précision) est couramment employé comme exact synonyme du terme routeur. Par exemple, on parle de passerelle par défaut (*default gateway*) ou ***gateway IP*** pour désigner un routeur qui interconnecte deux réseaux IP. Le routeur est un équipement réseau qui permet de relayer les paquets d'un réseau vers un autre.
- **Internet** est le réseau informatique mondial qui rend accessibles au public des services (comme le courrier électronique et le World Wide Web). Ses utilisateurs sont désignés par le néologisme « **internaute** ». Techniquement, Internet se définit comme le réseau public mondial utilisant le protocole de communication « TCP/IP » (au sens les protocoles de la famille TCP/IP).
- Lorsque les technologies Internet (TCP/IP, services, etc.) sont mises en oeuvre au sein de réseaux privés (entreprises, administrations, etc ...), on parle alors d'**intranet**.

Bibliographie

- "TCP/IP sous Linux" de JF Bouchaudy - Formation Tsoft © Ed. Eyrolles
- "TCP/IP Administration de réseau" de Craig Hunt © Ed. O'Reilly
- "Les protocoles TCP/IP et Internet" d'Eric Lapaille © NetLine 1999
- "Webmaster in a nutshell" © Ed. O'Reilly
- "Technique des réseaux locaux sous Unix" de L. Toutain © Ed. Hermes
- "Pratique des réseaux locaux d'entreprise" de JL Montagnier © Ed. Eyrolles
- "Transmission et Réseaux" de S. Lohier et D. Present © ED. DUNOD
- Les sites www.frameip.com, fr.wikipedia.org, www.w3.org, etc ...