# Couche réseau

# 1 Introduction

C'est la couche n° 3 du modèle OSI. Elle fournit :

- Le **choix du meilleur chemin** entre plusieurs solutions. => ROUTAGE ;
- La **remise en ordre** des trames ;
- La possibilité de **segmenter** des trames ;
- le **contrôle d'erreurs.**

Protocoles les plus connus :

- Internet Protocol,
- X25

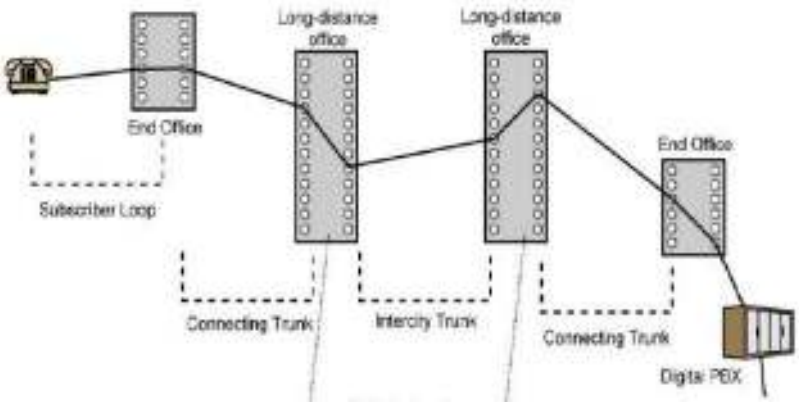
## 1.1 La commutation de circuits

### 1.1.1 Commutation de circuits réels

l'Ancêtre analogique.

Aujourd'hui la technique a évolué pour donner naissance à la commutation de circuits numériques.

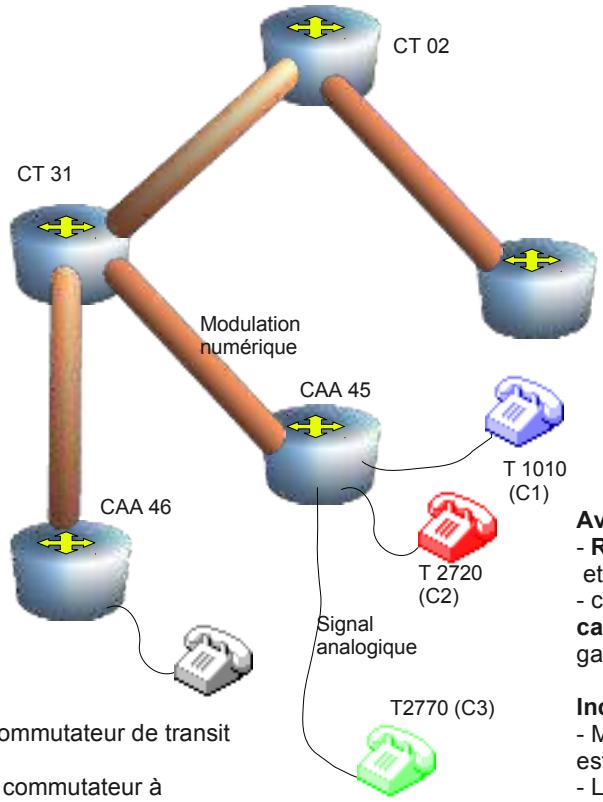
Cette technique a elle aussi évolué et donné naissance à la commutation de circuits virtuels.




### 1.1.2 Commutation de circuits virtuels

Utilisé dans ATM (Asynchronous Transfer Mode), X25 ou Frame Relay.

Par analogie à la commutation de circuits électriques que nous connaissons pour le téléphone, **l'adresse n'est communiquée qu'au début de la connexion**, et le paquet reçoit un identifiant sur chaque tronçon entre 2 commutateurs. L'identifiant est plus court et les commutateurs ont moins de travail à fournir car l'identifiant peut avoir un lien direct avec le numéro de port de sortie du commutateur. Dans le cas de circuits réels, la liaison est réservée de bout en bout et ne peut être utilisée par d'autres. Dans le cas de circuits virtuels, il y a **surréservation** du réseau et le réseau s'adapte en fonction de la demande de chacun. Ainsi, si 2 correspondants ne dialoguent plus ensemble, mais n'ont pas encore rompus la communication, la bande passante qui leur était allouée est redistribuée sur le réseau.



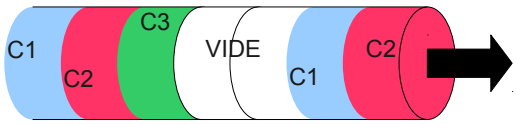

CT : commutateur de transit

CAA : commutateur à autonomie d'acheminement.

**Transmission Synchrone** : multiplexage temporel dans le medium (fibre optique en SDH par exemple) entre un CAA et un CT.

Le signal émis par le téléphone ou le modem est échantilloné (8bits/8kHz) par le CAA puis transmis à un débit supérieur vers le CT.

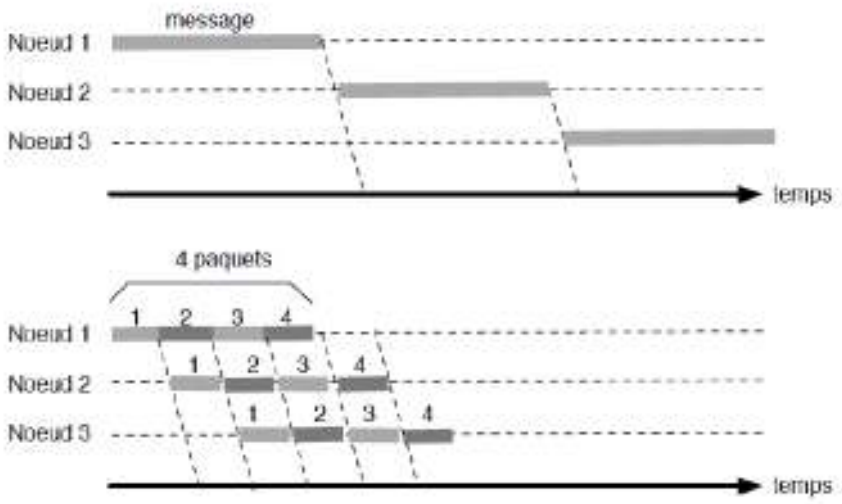
Pour l'ADSL, une bande de fréquence au dessus des 20 kHz est utilisée par le modem afin de ne pas perturber la voix. Dans ce cas le CAA est épaulé par un DSLAM.




**Avantages :**
- **Routage simplifié.** Le CAA ne connaît que ses abonnés et son CT.
- chaque téléphone, une fois la connexion établie, a son **canal réservé** : délai d'acheminement et débit constants garantis.

**Inconvénients :**
- Même s'il n'y a pas d'information échangée, le canal est réservé : **pas de surbooking** faisable.
- Le chemin entre 2 abonnés est toujours le même : pas de délestage possible.
- Connexion obligatoire pour échanger de l'information : perte de temps.

## Avantage des petits messages

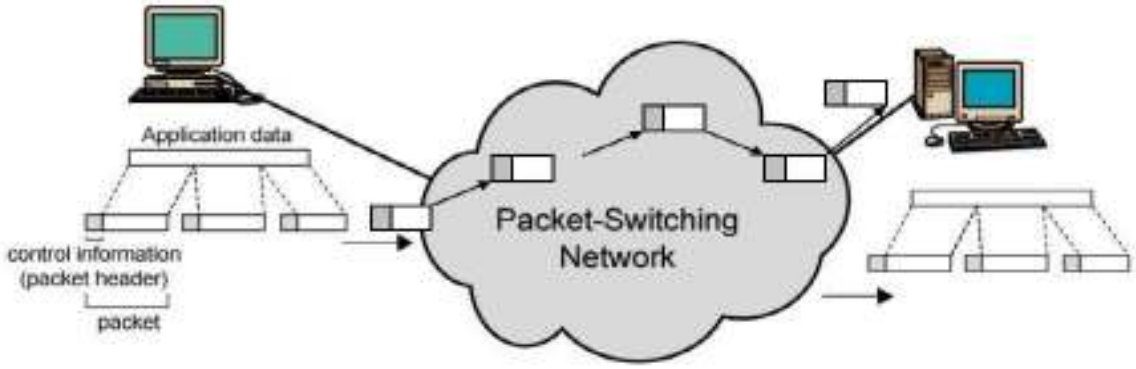



*Les petits paquets arrivent avant les gros paquets.*

Mais dans ce cas, il faut que l'overhead soit peu important. Dans ATM, une cellule fait 53 octets dont 5 octets pour l'entête et 48 pour les données. Chaque cellule ATM ne transporte que les informations liées à l'identification du circuit.

## 1.2 La commutation de paquets

Pour acheminer un paquet à travers un réseau de routeurs (ou commutateurs) un autre solution a vu le jour : L'**acheminement par adresse** de datagrammes comme dans IP.

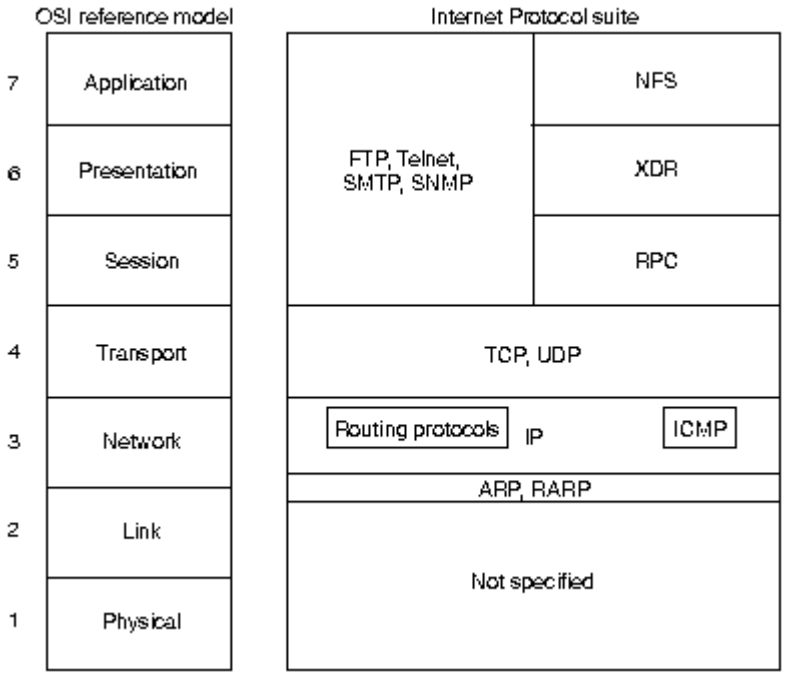



Le paquet est trié dans chaque routeur en fonction de son adresse de destination ; cela demande plus de puissance de calcul que dans le cas de la commutation de circuit, mais c'est simple à mettre en oeuvre.

Les différentes trames :

- les trames de données ;
- les trames de contrôle des données (contrôle de flux, acquittement, reprise en cas d'erreurs...) ;
- les trames de supervision du réseau (gestion du routage, maintenance afin de prévenir la congestion...).

# 2 - Le protocole Internet




Dans le milieu des années 70, le **DARPA** (Defence Advanced Research Projects Agency) fut intéressé par la réalisation d'un réseau à commutation de paquets pour fournir un moyen de communication aux centres de recherches américains. Ce fut le début de l'engouement pour la commutation de paquets, mais aussi le début des problèmes que tout le monde connaît actuellement concernant l'interconnexion de systèmes hétérogènes.

Le résultat du DARPA et de l'université de Stanford fut le développement de la suite de protocoles Internet, les plus connus étant TCP (Transmission Control Protocol) et IP (Internet Protocol).

Les protocoles Internet peuvent être utilisés pour communiquer sur un ensemble de réseaux interconnectés. Ils sont conçus « aussi bien » pour les LAN que les WAN. Ils offrent en outre non seulement des moyens de contrôle

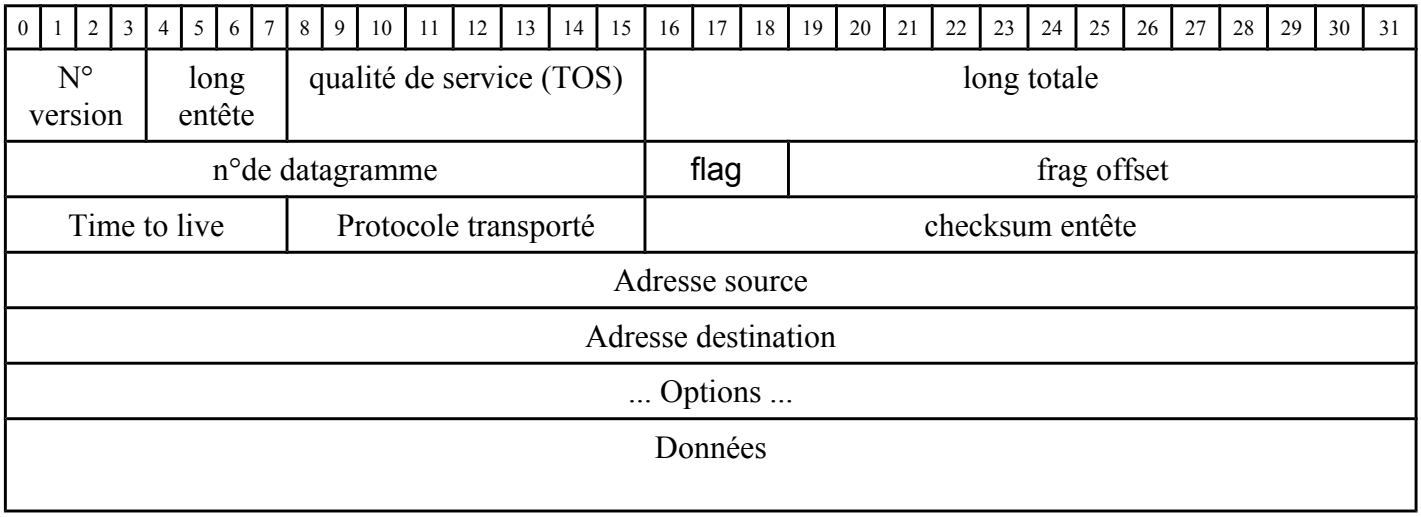
de la transmission des paquets, mais aussi des applications tels que le courrier électronique, l'émulation de terminal à distance, et le transfert de fichiers. La figure ci-dessous donne quelques exemples et la relation avec le modèle OSI.

Les spécifications du protocole Internet se font par des RFC (Request for Comments). Ces RFC sont publiés, puis revues par la communauté Internet, et republiées. Ces travaux sont toujours en cours afin d'améliorer la suite de protocoles IP. Par exemple la RFC 1340 référence tous les codes hexadécimaux utilisés par IP, mais aussi Ethernet.

# 2.1 - La trame de données

## 2.1.1 - Description de la trame

IP est la couche 3 des protocoles Internet. En plus de l'adressage et du routage, IP fournit les services de fragmentation et réassemblage des datagrammes et la notification d'erreurs sur l'entête seulement. IP et TCP sont les fondations de cette suite de protocoles. Le format des paquets est représenté ci-dessous. C'est la norme Big Endian qui est utilisée pour le format des nombres.




- **N° version** : Numéro de version d' IP utilisé (actuellement 4).
- **long entête** : longueur de l'entête en mots de 32 bits.
- **qualité de service** : niveau d'importance du datagramme transporté (souvent non utilisé)
- **long totale** : longueur en octet du paquet.
- **n°de datagramme** : Identifiant de datagramme. Un ensemble de paquets fragmentés issus du même datagramme ont le même identifiant.
- **flag** : 3 bits dont le MSB signifie que le paquet ne doit pas être fragmenté et le LSB qu'il reste des paquets fragmentés à venir.
- **frag offset** : position du paquet dans le paquet fragmenté, en multiple de 8 octets. Un paquet est fragmenté quand il passe sur un réseau de MTU (Maximum Transmit Unit) plus petit.
- **Time to live :** décrémenté à chaque passage par un routeur afin d'éviter un bouclage sans fin des paquets perdus. Décrémenté de 1 ou du temps en seconde de traversé d'un routeur.
- **Protocole transporté** : par exemple TCP = 6 et UDP =17
- **checksum entête** : Pour le contrôle d'erreur. Somme sur 16 bits en complément à 1.
- **Adresse source** : adresse sur 4 octets de l'émetteur de départ.
- **Adresse destination** : adresse sur 4 octets du récepteur final.

## 2.1.2 Adressage

Une adresse IP est représentée sur 32 bits. Elle est divisée en 2 parties de longueur variable : l'adresse réseau et l'adresse de la machine. Il appartient à l'administrateur du réseau de diviser ou non son réseau en sous réseau.
Les adresses réseaux sont réparties en 5 catégories, suivant l'étendue du codage de la partie réseau de l'adresse :
**Classe A** : de 0.0.0.0 à 126.255.255.255, soit 7 bits utiles pour l'adresse réseau (8 bits mais premier bit = 0), pour les grands réseau.
**Classe B** : de 128.0.0.0 à 191.255.255.255, soit 14 bits utiles pour l'adresse réseau (16 bits mais les deux premiers bits = 10) ; pratiquement plus d'adresses de ce type disponibles.
**Classe C** : de 192.0.0.0 à 223.255.255.255, soit 21 bits utiles pour l'adresse réseau (24 bits mais les 3 premiers bits = 110)
**Classe D :** de 224.0.0.0 à 239.255.255.255. réservée pour le multi-adressage, afin qu'une trame devant aller sur plusieurs machines ne soit dupliquée que le plus tard possible. Ceci nécessite un protocole particulier où les machines s'abonnent à un groupe de diffusion.
**Classe E** : usage future.

Exemple d'adresse de classe C en notation décimale pointée : 194.199.103.7

Les classes d'adresses sont distribuées par l' IANA (Internet Assigned Numbers Authority) qui délègue à chaque pays cette distribution.

Afin de faire face à la pénurie d'adresse de classe B, on met en oeuvre une technique d'agrégation des adresses de classe C, appelée CIDR (classless interdomain routing). Les adresses de classes C doivent être contiguës et doivent pouvoir être masquables.

La technique du masque permet de reconnaître la partie réseau de la partie machine. Le masque ou « netmask » est un nombre de 32 bits dont les bits correspondant à la partie adresse machine sont à 0 et les autres à 1. Lorsque l'on fait le ET logique netmask & adresse IP, on doit trouver l'adresse réseau, c'est à dire la première adresse disponible sur un réseau.

exemple :

Soit le réseau 194.64.3.0 contenant 4 sous-réseaux.

en binaire cette adresse s'écrit :

```
11000010 01000000 00000011 00000000
```

Si l'on considère les 4 sous-réseaux ensembles, le masque de ce réseau global est celui des réseaux de classe C :

```
11111111 11111111 11111111 00000000 soit 255.255.255.0
```

Par contre pour distinguer les 4 sous réseaux, on a besoin du masque suivant :

```
11111111 11111111 11111111 11000000 soit 255.255.255.192
```

Remarque : lorsque l'on attribue des adresses à des machines la première adresse et la dernière d'un sous-réseau sont réservées à la diffusion sur tout le réseau. On n'attribuera donc pas ces adresses.

Dans l'exemple précédent, pour le premier sous-réseau, les adresses 194.64.3.0 et 194.64.3.63 sont réservées. Un manière plus concise de donner le netmask associé à l'adresse réseau et de coller à la suite de l'adresse réseau le nombre de 1 du netmask. Exemple 194.64.3.0/26.

Enfin, il existe un certain nombre d'adresses réservées :

- Toute machine se voit localement comme faisant aussi partie d'un réseau local d'adresse 127.0.0.0 et s'attribue l'adresse 127.0.0.1. Cette adresse permet de simuler ou tester des applications IP localement en faisant communiquer des processus localement.

- Il existe 3 ensembles d'adresses qui ne seront jamais distribuées par l'IANA. Ce sont les adresses 10.0.0.0 à 10.255.255.255 (10.0.0.0/8), 172.16.0.0 à 172.31.255.255 (172.16.0.0/12) et 192.168.0.0 à 192.168.255.255 (192.168.0.0/16 ). Elles peuvent donc servir pour adresser des machines cachées (car invisible de l'extérieur du réseau de l'entreprise) qui n'ont pas besoin d'accéder au reste de la communauté Internet. Ces adresses ne sont pas routées par les routeurs à moins que cela ne soit explicitement marqué dans la table de routage.

## 2.1.3 - Attribution d'adresses à une machine :

Pour un réseau local, ceci se fait soit de manière **statique** (l'adresse IP est entrée à la main à la configuration de la carte réseau) ou par le biais d'un serveur **DHCP** (Dynamic Host Configuration Protocol). La machine envoie une trame de **diffusion** à tout le réseau local pour trouver le serveur DHCP et celui-ci lui renvoie une adresse **IP libre** (parmi une ensemble d'adresses qu'il gère). L'adresse est louée pour une durée au delà de laquelle le serveur DHCP reprend l'adresse en avertissant la station. Pendant la **durée de validité**, le serveur DHCP «ping» la station de temps à autre pour savoir si cette machine est toujours connectée.
En plus de l'adresse IP, le serveur DHCP peut aussi fournir l'adresse de la passerelle et du serveur DNS.

Évidemment le serveur DHCP doit être sur le même réseau local que la station demandeuse.

Pour un accès à distance (RTC, ADSL...) le serveur d'accès est aussi serveur DHCP.

## 2.1.4 - Résolution de Nom : DNS

Lorsqu'une application veut envoyer un message à une autre elle utilise en général le nom de domaine. Par exemple la machine cybele de l'école possède le nom suivant : *cybele.ecole.ensicaen.fr*. Cependant, le protocole IP n'utilise pas les noms de machines pour qu'un paquet arrive à la bonne destination, mais les adresses IP, par exemple 193.49.200.148.
La machine doit donc pouvoir faire la correspondance entre les noms et les adresses IP.
Plusieurs techniques existent :

- La machine possède un fichier ***/etc/hosts*** (Unix) ou *lmhosts* (Windows) dans lequel on a une correspondance entre des noms et des adresses IP ;
- La machine est connecté à un serveur **NIS** (Network Information Service de Unix) ou WINS (de Windows) et ce serveur met à disposition son propre fichier */etc/hosts ;*
- Netbios Name Server, un service propore à Windows ;
- Domain Name serveur ;
- Multicast DNS, un service de la série Zeroconf.

### interrogation d'un DNS (Domain name System)

Un serveur DNS est une machine qui répond à des requêtes de noms de domaines. Ainsi chaque domaine ou sous-domaine est géré par une machine qui fait autorité. C'est elle qui connaît toutes les adresses IP de toutes les machines du domaine. Cette machine est capable aussi d'aller interroger le bon serveur DNS quand elle ne connaît pas la réponse. Souvent, elle stocke en cache la réponse et devient capable de donner la réponse la prochaine fois. Cette réponse sera dite « non authoritative ».
Les serveurs DNS permettent aussi de fournir l'adresse IP du serveur de mail (serveur SMTP ) d'un domaine.

**Ceci est un exemple, cliquez sur le lien de téléchargement pour obtenir le cours complet.**