

## Cours : Réseaux Informatiques Locaux

CH API : Notion sur la Transmission de données :

### I - Introduction

Toutes les entreprises possèdent un ou plusieurs systèmes de Telecommunication qui véhiculent les différentes informations nécessaires à son développement. Ces systèmes sont organisés en réseaux comme définie comme des ensembles des équipements et des supports de transmission dont une des fonctions est la transmission et le transfert de l'information.

Les progrès rendent possible le traitement de l'information de nature différente (des sequences vidéos, sonores, les documents)

### II - Nature des informations transmises :

la transmission de l'information sur un support peut être Analogique ou Numérique selon que le signal transporte varie de manière continue ou discrète dans le temps.

- Un signal de parole module d'une manière analogique l'amplitude et la fréquence de une onde porteuse avec une variation de le temps continue

- Une suite de données binaire permet de construire un signal qui prend par exemple deux valeurs 0 et 1 qui varie dans le temps à des intervalles réguliers.

### III - Representation de l'information

la correspondance entre la nature de l'information et la nature de la transmission, ne réduit pas à une bijection.

- la quasi-totalité des transmissions sont numériques. la numérisation d'un signal Analogique consiste en 3 étapes : - l'Echantillonnage : il consiste à prélever un nb déterminé d'élément (échantillon) qui seront suffisant pour reconstituer un signal analogique à l'arrivée.

- la quantification : elle attribue à chaque échantillon une valeur



prise dans une échelle finie de valeur

Codage: chaque échantillon sera codé dans un ensemble de bits par exemple pour codé 256 il faut 8 bit. (le codage ASCII).

## V - La qualité de service

QOS:

\* Disponibilité des moyens

\* le taux d'erreur

\* débit de transfert

\* délai de transmission

la grande priorité de la Télécom

est celle de la transparence:

l'utilisateur final ne connaît

pas la nature du support ou

les équipements intervenants

dans la transmission, il n'est

concerné que par la qualité

du service offert.

Quelques éléments de la QOS

\* Disponibilité des moyens

de transfert qui est liée aux

Taux de panne des équipements

\* le taux d'erreur maximal

$$\text{Taux Err}_{\max} = \frac{\text{Nbre de bits modifiés (Err)}}{\text{Nbre total de bits émis}}$$

\* le débit de transfert:

mesure la quantité d'information transmise / unité de temps (bit./s)

\* le débit nominal: est la quantité théorique d'information pouvant être transmise par unité de temps.

\* le débit utile: est la quantité d'information effectivement transmise par unité de temps

\* le taux d'utilisation: est le rapport du débit utile par le débit nominal

$$\text{Taux d'uti} = \frac{\text{débit utile}}{\text{débit nominal}}$$

\* Délai: [c'est le temps entre l'instant d'émission et l'instant de (transmission) réception] c'est la durée entre la décision d'envoyer l'information et la réception par le destinataire. Il se compose de deux parties.

- le délai de transmission: 
$$\text{délai}_{\text{trans}} = \frac{\text{Quantité d'information}}{\text{débit}}$$

- le délai de propagation: est le temps mis par le signal se propage sur le matériel les équipements traversés

peuvent introduire des retards 
$$\text{délai}_{\text{prop}} = \frac{\text{distance parcourue}}{\text{vitesse}}$$

## VI - Technique de transmission numérique:

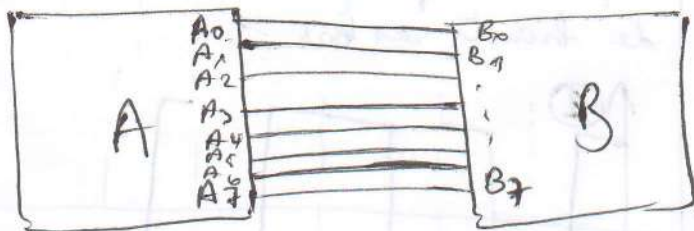
a) Codage: les réseaux informatiques fondent généralement sur



la numérisation des l'information  
la transmission se fait à base  
de code binaire codifier selon  
certain  
une représentation ou formalisme  
précis permettant le traitement  
de la donnée, ce formalisme  
fait correspondre à chaque  
caractère une suite précise  
d'élément binaire, le nbr  
de caractère (d'élément par  
caractère définie la long de  
code choisit

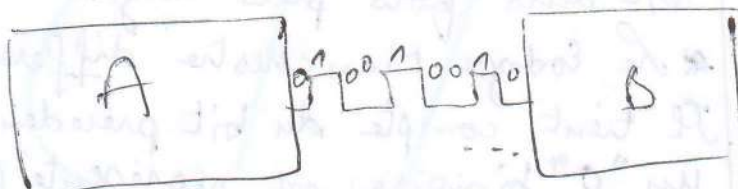
1) transmission // et transmission  
serie:

• transmission parallèle //



Elle est avantageuse ou  
intéressante si la distance  
entre les équipements est  
court courte, Elle a pour effet  
de réduire les délais de  
transmission donc de augmenter  
le débit de transfert (débit)

• transmission série:



(Elle est) c'est le mode  
de transmission le plus  
utilise actuellement

avantageuse → la 2  
distance entre l'émetteur  
et le récepteur est importante  
→ les bits sont envoyés  
les uns après les autres  
sur le même support  
c) transmission synchrone  
et asynchrone:

- transmission asynchrone:  
dans une transmission synch  
les caractères sont émis  
d'un façon irrégulière.  
dans une communication  
entre ordinateur et  
la transmission est  
oxy avec alt débit de  
message on place une  
en-tête de débit on

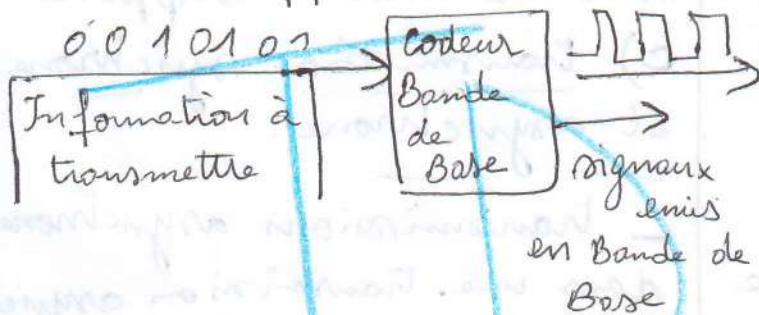
rajoute une message de  
fin. (X)

• les transmission dans les  
réseaux:

Pour transmettre des information  
binaire sur un support de  
transmission, il est nécessaire  
de les transformer au préalable  
en un signal électrique mieux  
adapté aux contraintes physiques  
du système de transmission  
Dans ce contexte, deux techniques  
de transmission sont envisageable  
- La transmission en bande  
de base  
- La transmission par

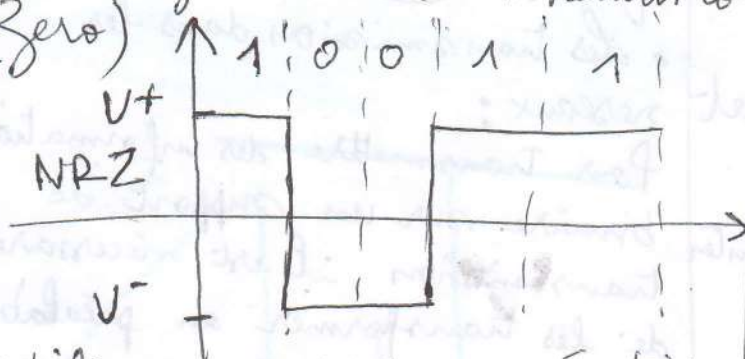


translation du spectre "Modulation"  
 A) transmission en bande de base : la transmission en bande de base consiste à transmettre directement les signaux numériques sur le support de transmission



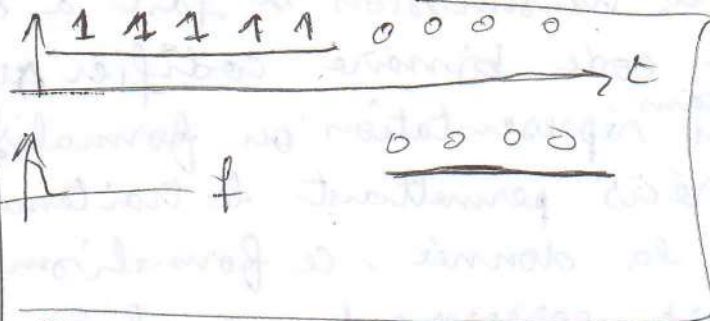
Le codeur a essentiellement pour objet :  
 \* transformer le signal en un autre mieux adapté aux caractéristiques du support (Ex: Bande passante)  
 \* Maintenir la synchronisation.

• Les principaux codage en bande de : ① Le codage NRZ  
 Le codage NRZ (Non Return to Zero)



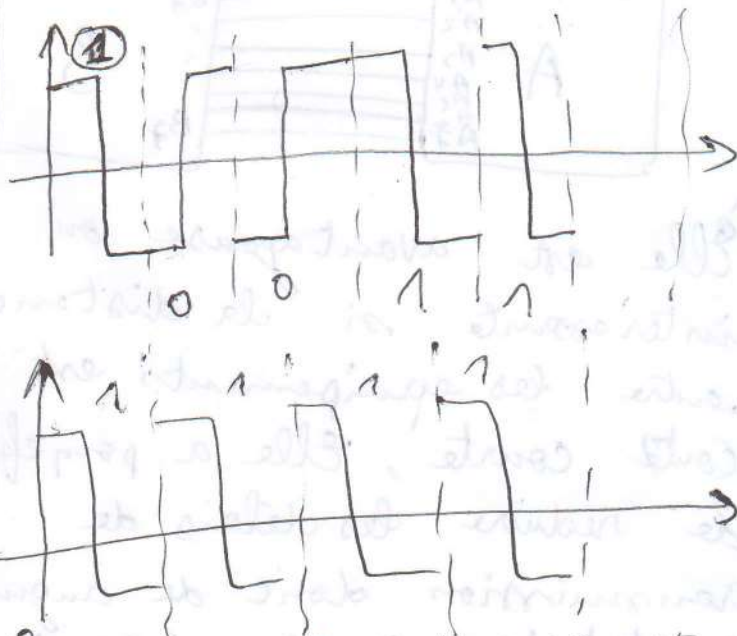
utilise une tension négative pour représenter un "0" binaire et une tension positive pour représenter un "1" binaire. Ce codage est mal adapté (sa puissance maximal est concentré aux basses fréquences). De plus de sérieux problèmes

de synchronisation des horloges sont à redouter.



Le codage Manchester :

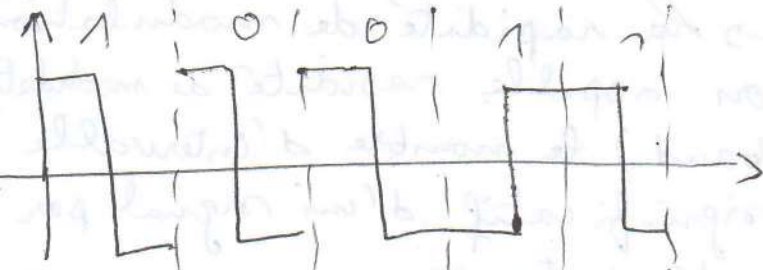
Avec le codage Manchester c'est le point où le signal change qui représente la valeur du bit, transmis. Un "0" binaire est représenté par une tension allant de bas en haut, tandis que le "1" binaire est représenté par une tension allant de haut en bas.



Le codage Manchester nécessite un repérage des fils de spectre est deux fois plus large.  
 \* Le codage Manchester différentiel. Il tient compte du bit précédent. Un "0" binaire est représenté par un changement de tension au début de la transmission, et le "1" par l'absence de changement.



de tension au début de la transmission



Limitation de la transmission en bande de base.

Les signaux en bande de base sont sujet à une atténuation (affaiblissement)

Le signal doit être régénéré pour les grandes distances.

B: Modulation discrète:

Pour mettre en œuvre l'opération de modulation on utilise un organe appelée Modulateur

à la sortie du canal on utilise une organe qui fait l'opération inverse, cette opération s'appelle

Démodulation



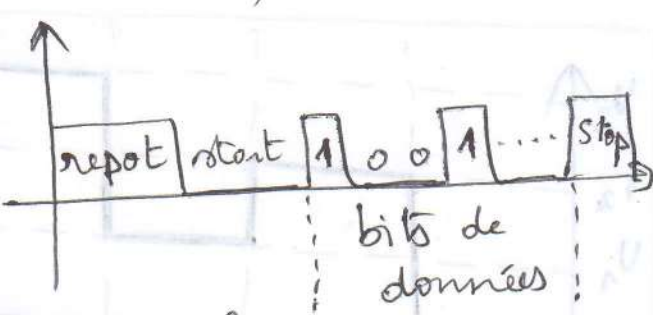
Modulation d'Amplitude

La modulation est employé pour la radio AM (Amplitude modulation) et peut être également utiliser pour les réseaux informatiques.

3  
"0" → Amplitude  $A_1$   
"1" → Amplitude  $A_2$   
 $A_1 \neq A_2$

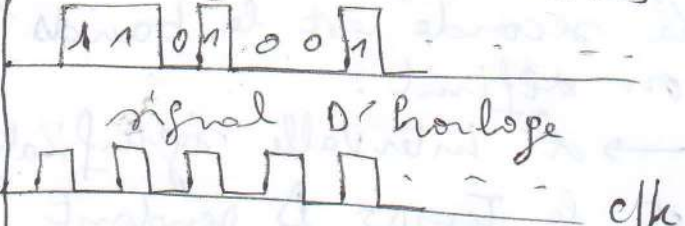
\* asynchrone (suite) de cours \*

les entêtes peuvent être des bits de début (bit start) ou de fin de message (bit stop)



\* Synchronne

Dans une Transmission Synchronne, les bits sont émis d'une façon régulière sans séparation entre les caractères, pour cela une signal d'horloge périodique "T" fonctionne pendant la durée de transmission signal de données



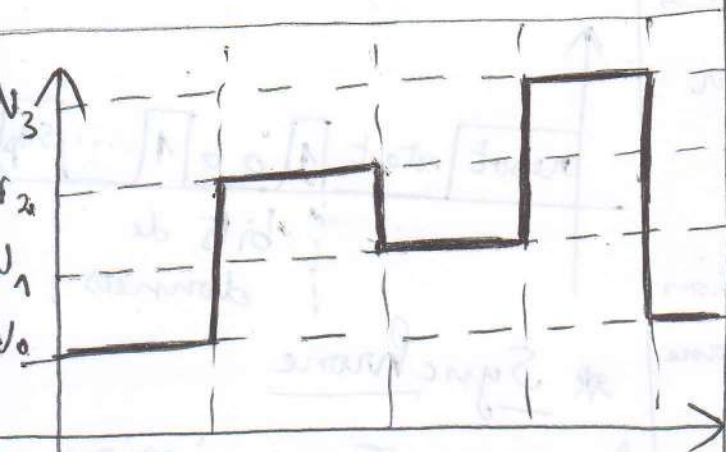
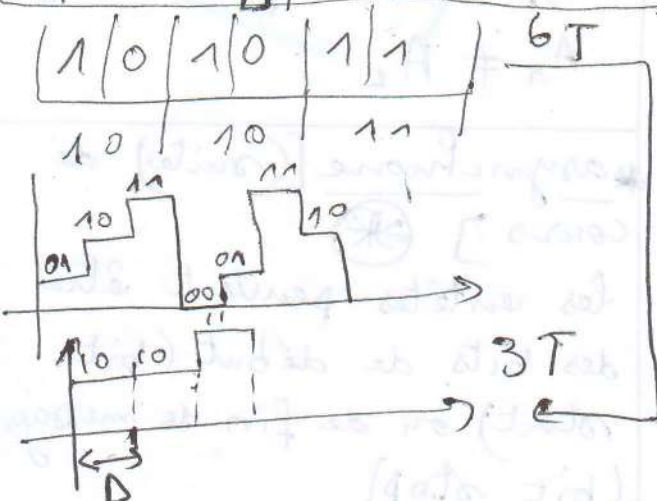
Transmission. Synchron.

d) Notion de débit binaire et de rapidité de modulation:



\* rapidité dépend de temps et l'intervalle significatif

$$R = \frac{1}{\Delta} \text{ (bit/s)}$$



Signal à 4 Niveaux d'Amplitude

Deux unités sont employées pour caractériser la vitesse de Transmission d'un réseau et des lignes de Transmission. La première est le Nbre de bits par seconde (bit binaire) la seconde est le bauds, on définit:

→ l'intervalle significatif et le Temps  $\Delta$  pendant lequel les caractéristiques du signal sont constantes, donc: → significatives d'un

éléments binaire.

→ la rapidité de modulation on appelle rapidité de modulation (baud) le nombre d'intervalle significatif d'un signal par unité de temps.

$$R = \frac{1}{\Delta} \text{ (baud)}$$

→ débit binaire: noté par D est le nombre d'élément binaire (bits) émis par seconde sur un support de transmission. Si "T" est la durée d'un bit

$$D = \frac{1}{T} \text{ bit/s}$$

→ La valence: pour transmettre "n" bits pendant un intervalle significatif  $\Delta$  il faut que le signal de donnée ait  $V = 2^n$ ; V: valence de sig

→ Relation entre R et D

$$R = \frac{1}{\Delta}; D = nR \quad V = 2^n \Rightarrow$$

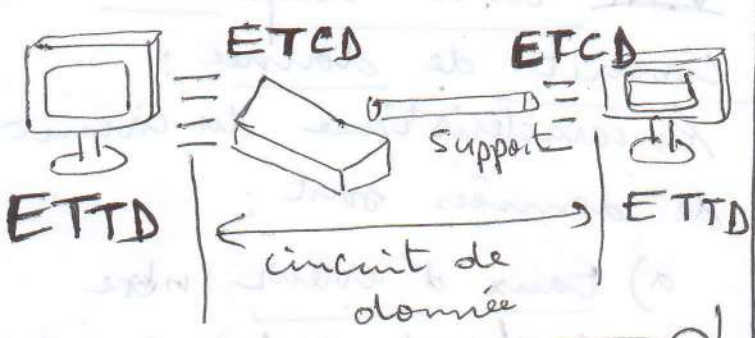
$$D = \log_2(V) \cdot R$$

le débit dépend de la rapidité et le nombre de bits; la) l'intervalle significatif et le temps (recess) (ress) nécessaire pour transmettre n bit; et T le temps pour transmettre 1 bit donc pour transmettre 1 bit n fois plus rapide d'une transmission de n bit



$\begin{array}{c} 0 \quad 1 \quad 0 \quad 3 \text{ bit} \\ \hline \Delta \end{array} \quad \begin{array}{c} 1 \text{ s} \quad 1 \text{ bit} \\ \hline T \end{array}$   
 $R = \frac{1}{\Delta}$   
 $D = \frac{1}{T}$   
 $R = \frac{1}{3T} = \frac{1}{3} D \Rightarrow D = 3R$   
 $D = NR$

# **VI : Elements Constitutifs d'une liaison de données :**



Elément d'une liaison de données, **ETCD**: Elément terminal de circuit de données.

**ETTD**: Elément terminal équipement de traitement de données (DTE); représente l'équipement informatique d'extrémité - cette équipement génère les données à transmettre et traite les données reçues. Il contrôle la communication et le dialogue.

**ETCD**: Equipement terminal du circuit de données (DCE) cette équipement réalise l'adaptation entre le ETDD et le support. Il remplit essentiellement une fonction électrique; En modifiant la nature de signal et non sa signification

- Le support: est possibilité de transmission (débit, taux d'erreur) dépend essentiellement des caractéristiques physiques et l'environnement de celui-ci.

**Remarque**: l'ensemble constitué par le support et les deux ETCD constituent le circuit de données.

## **VII: caractéristique du support de transmission:**

a) type de support physique: ceux sont les éléments permettant de faire circuler l'information entre un équipements Emetteur et un autre receveur. Ils sont généralement classés en 3 catégories:

- \* support filaire / sig elec
- \* support aérien / ondes électromagnétique
- \* support optique / information sous forme lumineuse

Perturbation: La transmission de données sur un canal ne se fait pas sans perte et le temps de transmission n'est pas immédiate d'autre part, des parasites ou des dégradations du signal peuvent apparaître.



## VII - caractéristique du support de transmission :

\* Les parasites ou bruit :  
sont des perturbations modifiant localement la forme du signal. Elles peuvent provenir du canal lui-même ou de l'environnement.

Le bruit peut être de 2 type : 'Bruit Blanc' ou 'Bruit impulsif'.

\* L'affaiblissement du signal représente la perte du signal en énergie dissipée dans la ligne. L'affaiblissement est proportionnel à la longueur du support et à la fréquence du signal.

\* Distorsion : la distorsion du signal caractérise le déphasage entre le signal en entrée et le signal en sortie.

c) La bande passante : la Bp d'un canal de transmission est l'intervalle de fréquence sur lequel le signal ne subit pas un affaiblissement supérieur à un certain seuil généralement 3 dB soit 50%.

d) la capacité d'une ligne est la quantité d'information (bits) pouvant être transmis

sur la ligne par second.

$$C_{\text{Max}} = W \log_2 \left( 1 + \frac{S}{B} \right)$$

(critère de Shannon)

où  $W$  : est bande passante de support.

$\frac{S}{B}$  : est le rapport signal/bruit.

## VIII caractéristique du circuit de donnée :

Les caractéristiques du circuit de données sont :

a) taux d'erreur : nombre de bits / nombre de bits total erronés / émis.

b) la disponibilité : évalue la proportion de temps pendant lequel la transmission est possible.

c) la rapidité de Modulation (vitesse de transmission) indique le Nbre de symboles (symbole : ensemble de bit) (intervalles significatif)

$$R = \frac{1}{\Delta} \text{ (bonds)}$$

Critères de Nyquist

$$R_{\text{max}} = 2W$$

Le débit binaire : il représente le Nbre de bits transmis / s



$$D = R \log_2(V)$$

cela implique

$$D_{\max} = 2W \log_2(V)$$

IX : Classification de transmission en fonction du Contrôle de l'Echange :

a) Selon l'organisation des Echanges : La transmission d'information entre 2 correspondants peut être unidirectionnelle (Echange dans une direction) on parle alors d'une liaison simplex.

- si les correspondants peuvent alternativement repasser les rôles d'émetteurs et de récepteurs

la liaison est dite

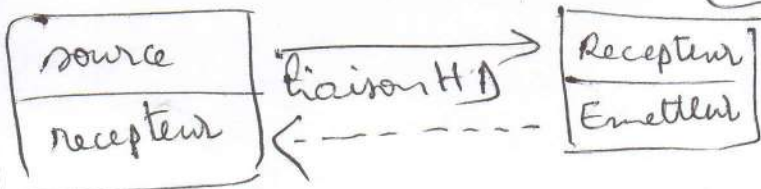
liaison à l'alternat ou liaison half duplex.

- Si l'échange peut s'effectuer simultanément dans les 2 sens la liaison bidirectionnelle intégrale ou full duplex.

Source émetteur

Liaison Simplex

Recepteur

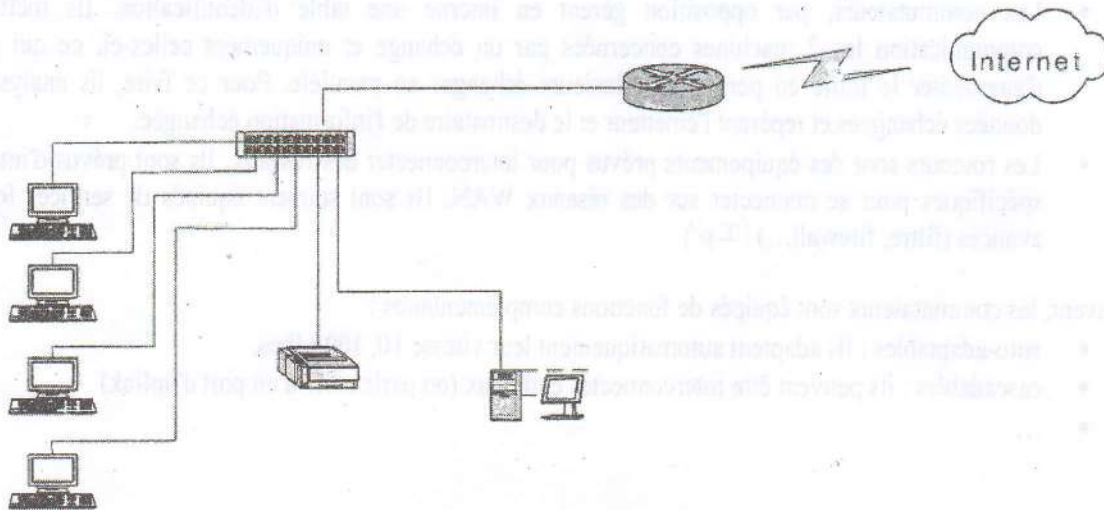




## Chapitre 2. Les réseaux locaux

### PARTIE I : INTRODUCTION AUX RESEAUX LOCAUX

#### 1 Introduction



#### 1.1 *Qu'est-ce qu'un réseau ?*

Un réseau est un ensemble d'ordinateurs ou de matériels reliés les uns aux autres. Il permet aux utilisateurs d'échanger des informations et de partager des ressources matérielles et logicielles.

#### 1.2 *A quoi sert un réseau ?*

Sans réseau, l'échange des informations doit s'effectuer de manière manuelle (disquette, papier, ressaisie ...). Le réseau permet le transfert d'informations directement entre machines, applications et/ou utilisateurs. Le réseau permet un gain de temps et minimise les erreurs (transfert sans temps réel, ressaisie ...)

#### 1.3 *Que permet un réseau ?*

- Le partage d'informations (fichiers, données...)
- Le partage de ressources logicielles (Applications)
- Le partage de ressources matérielles (imprimantes, sauvegardes, disques, fax ...)
- Le travail en groupe grâce aux partages de données (stock, client) et aux logiciels de groupware
- La communication (Internet, messagerie)

Le réseau de par ces différents aspects permet de réaliser des économies par :

Un traitement en temps réel  
Une meilleure synchronisation  
des gains en productivité  
Une communication plus rapide

De quoi est composé un *réseau* ?

Un réseau se devant d'interconnecter des machines, on y trouve :

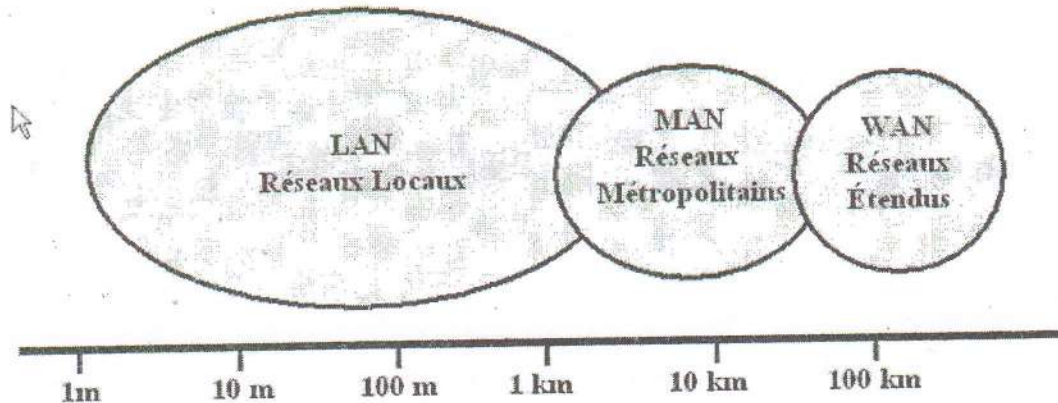
- Des supports de transmission
- Des équipements permettant de se connecter sur ces supports
- Des ressources matérielles et logicielles assurant les fonctions de client (demande de ressources)
- Des ressources matérielles et logicielles assurant les fonctions de serveur (offreur de ressources)
- ...



## 2 Les différents types de réseaux

Les caractéristiques permettant de différencier les familles de réseaux portent sur la taille et le mode de transmission des données.

### 2.1 Répartition des réseaux :



#### 2.1.1 réseau LAN

Local Area Network. Un réseau Lan permet de connecter de 2 à plusieurs centaines de machines à l'intérieur d'une même enceinte. Il s'agit de la plupart des réseaux informatiques présents dans les entreprises.

#### 2.1.2 réseau MAN

Metropolitan Area Network. Il s'agit d'un réseau dont la couverture s'étale à une ville. Le principe est de relier les différents réseaux LAN entre eux. Le principe est identique à celui d'un réseau local, mais les normes de transmission sont différentes.

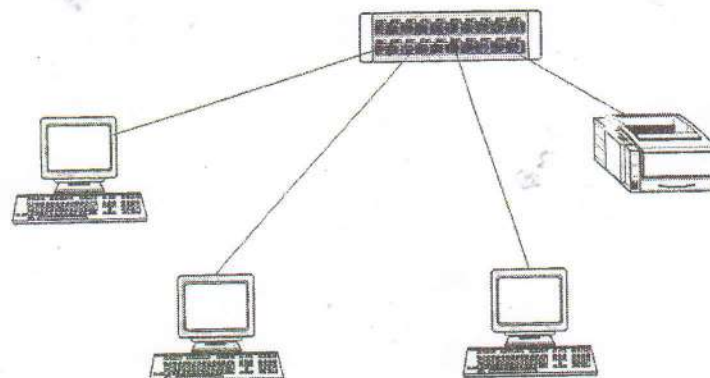
Un MAN ou réseau métropolitain est une série de réseaux locaux interconnectés à l'échelle d'une ville.

#### 2.1.3 réseau WAN

Wide Area Network. Un réseau WAN interconnecte des réseaux LAN et Man pour assurer une couverture et une interconnexion au niveau d'un pays, voire du monde. Ce type de réseau utilise les satellites pour certaines interconnexion.

## 2.2 Poste à poste et client/serveur

### 2.2.1 Les réseaux poste à poste





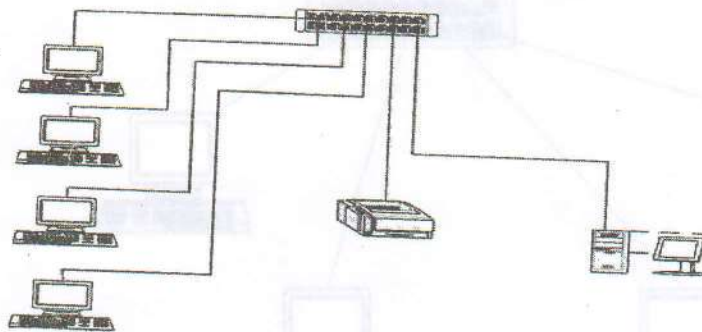
Dans ce type de réseau, tous les postes sont égaux et l'échange des données se fait à l'initiative de l'utilisateur. Le poste est à la fois client (demandeur de ressources) et serveur (fournisseur de ressources). Les principales caractéristiques sont :

- Limitation à quelques postes (< à 10 postes)
- Pas de serveur
- Peu d'administration
- Pas de hiérarchie entre postes
- Peu de sécurité
- Pas de besoin

### 2.2.2 Les réseaux Client/Serveur

Ce type de réseau est basé sur l'utilisation d'un serveur. Chaque machine se connectant raccordant sur le réseau doit être connue et s'identifier. Ce type de réseau est le plus répandu dans les entreprises. Il est possible d'interconnecter plusieurs serveurs. Les principales caractéristiques sont:

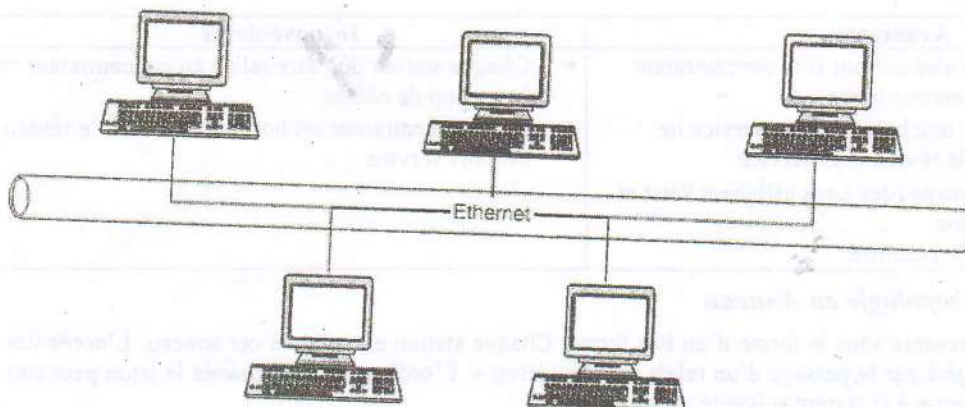
- Utilisation d'un serveur (Machine et SE<sup>1</sup>)
- Partage possible de ressources sur le serveur
- Centralisation des sauvegardes
- Possibilité d'utilisation de base de données client/serveur
- Gestion centralisée des utilisateurs
- Possibilité de mise en place de serveurs d'authentification, de données, d'impression, Web ...
- Sécurité accrue
- ...



## 3 Topologies

Dans un réseau local, les machines ou groupes de machines sont reliées sur le support auquel elles accèdent. On distingue 3 grands types d'organisation:

### 3.1 La topologie en Bus



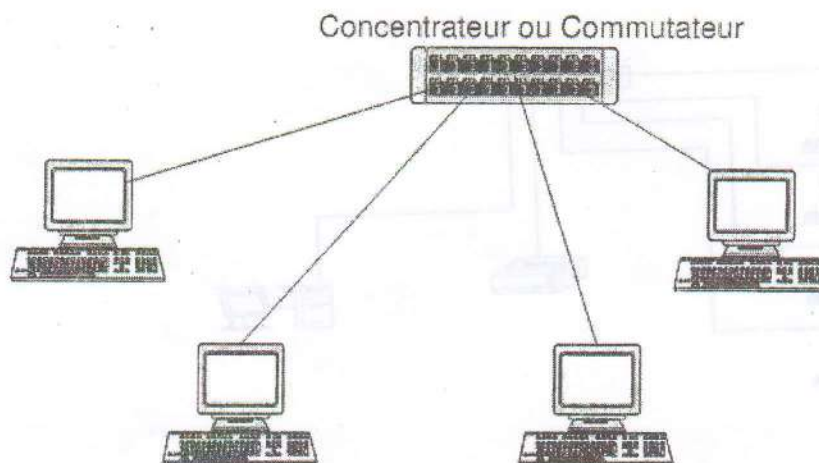


Le bus, un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, celles-ci circulent sur toute la longueur du bus et la station destinataire peut les récupérer. Une seule station peut émettre à la fois. Chaque extrémité du bus se termine par un "bouchon". Pour rallonger ce type de réseau, il est nécessaire de rajouter un élément actif en bout de bus appelé répéteur.

Cette topologie est utilisée dans les réseaux Ethernet 10 Base 2 et 10 Base 5.

Avantages	Inconvénients
<ul style="list-style-type: none"> <li>• Coût du câble</li> <li>• Mise en œuvre simple</li> <li>• Technologie simple et fiable</li> <li>• Facilité d'extension du réseau</li> <li>• Un ordinateur en panne ne met pas le réseau hors service : seule cette station est affectée</li> <li>• Pas de matériel supplémentaire hors mis les cartes réseaux</li> </ul>	<ul style="list-style-type: none"> <li>• Baisse de performances importante en fonction du nombre de stations</li> <li>• Une coupure du câble met le réseau hors service</li> <li>• La localisation des problèmes est difficile</li> <li>• Cette topologie est dite passive : les stations ne réinjecte pas le message régénéré s'il ne leur est pas destiné.</li> <li>• il faut prévoir des équipements spécifiques si la longueur des segments est importante</li> <li>• Une seule station peut émettre à la fois</li> <li>• Le câblage doit respecter la structure de bus</li> </ul>

### 3.2 La topologie en Etoile



C'est la topologie la plus courante aujourd'hui. Toutes les stations sont reliées à un unique élément, le concentrateur ou commutateur.

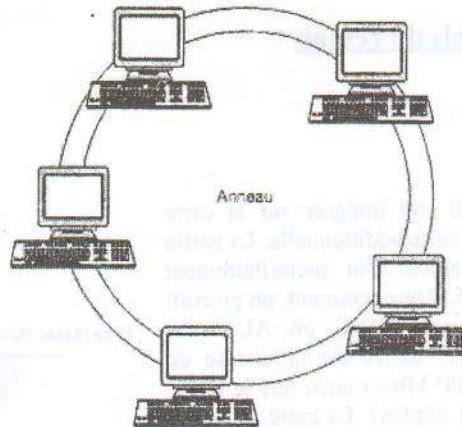
Cette topologie est utilisée par les réseaux Ethernet 10, 100 Base T et suivants.

Avantages	Inconvénients
<ul style="list-style-type: none"> <li>• Ajout de stations aisé surtout si le concentrateur dispose de ports encore libres</li> <li>• Un ordinateur ou une branche hors service ne mettent pas tout le réseau hors service</li> <li>• Facilité de dépannage (des Leds affichent l'état et le trafic sur la ligne)</li> <li>• Le signal peut être amplifié</li> </ul>	<ul style="list-style-type: none"> <li>• Chaque station doit être reliée au concentrateur ⇒ beaucoup de câbles</li> <li>• Si le concentrateur est hors service, tout le réseau est hors service</li> </ul>

### 3.3 La topologie en Anneau

L'anneau ou ring se présente sous la forme d'un bus fermé. Chaque station est reliée à cet anneau. L'accès des stations au réseau est géré par le passage d'un relais appelé « jeton ». L'ordinateur qui possède le jeton peut soit émettre, soit passer le jeton à la station suivante.

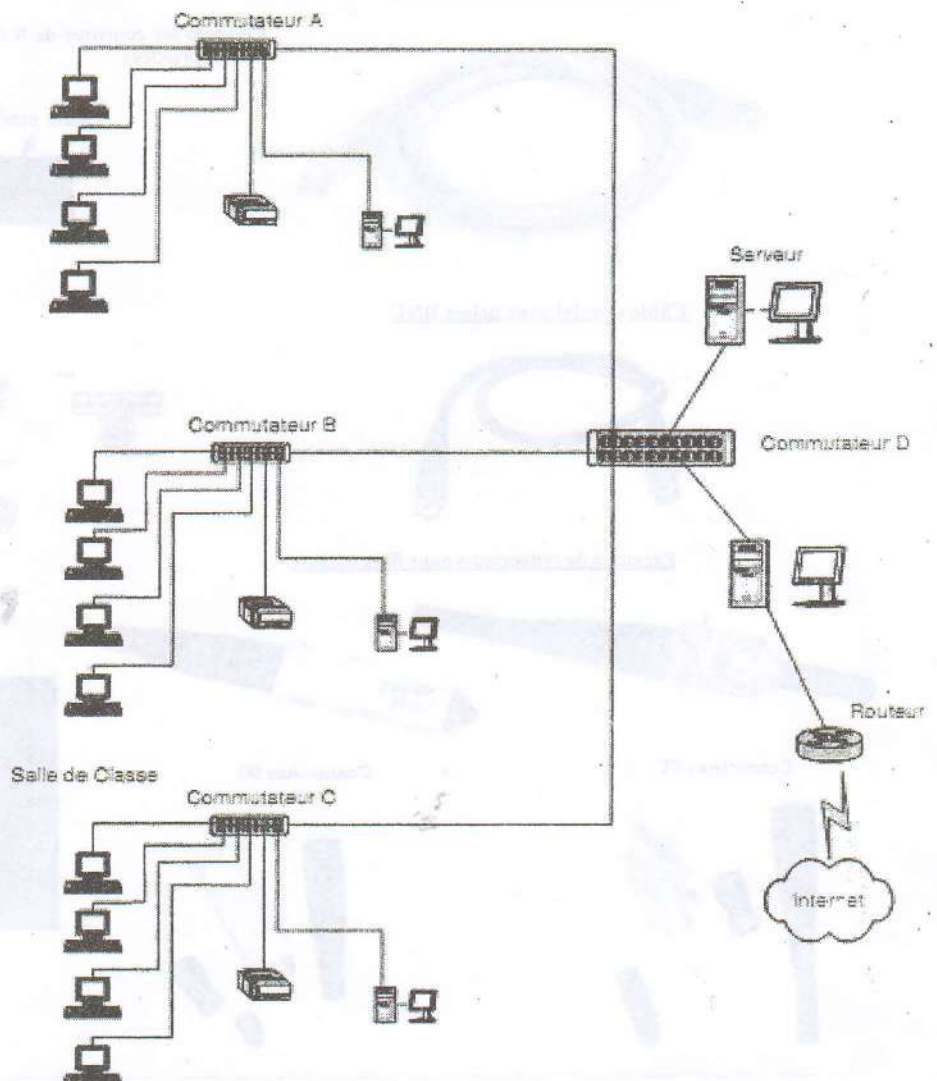




Avantages	Inconvénients
<ul style="list-style-type: none"> <li>• Cette topologie est dite active : chaque station réinjecte le signal sur l'anneau en le régénérant</li> <li>• Performances stables des communications sur le réseau : le principe du jeton fait qu'il n'y a qu'un seul message (pas de collisions), le jeton circule régulièrement sur l'anneau (chaque station est traitée équitablement)</li> </ul>	<ul style="list-style-type: none"> <li>• Une panne de station coupe l'anneau donc affecte tout le réseau</li> <li>• Problèmes difficiles à isoler, l'intervention affecte l'anneau donc le réseau</li> <li>• De même, la modification du réseau (extension par exemple) affecte plus ou moins longtemps le réseau</li> </ul>

### 3.4 Les topologies mixtes

En fonction de l'existant, du câblage, de l'organisation des locaux ... Il est possible de trouver des architectures mixtes. De la même façon, les différentes topologies sont souvent cascades pour étendre le réseau.



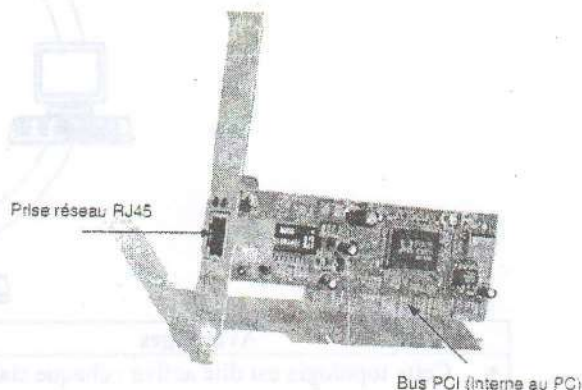


## PARTIE II : MATERIELS

### 1 Les éléments matériels du réseau

#### 1.1 Carte réseau

La fonction réseau est soit intégrée sur la carte mère, soit ajoutée à l'aide d'une carte additionnelle. La partie câblage vers le réseau est aujourd'hui majoritairement constituée d'un connecteur RJ45. Précédemment, on pouvait rencontrer d'autre type de prises (BNC ou AUI). La principale caractéristique de ces cartes est la vitesse de communication (10, 100 ou 1000 Mbps) ainsi que le mode de communication (half ou full duplex). La carte peut être équipée d'une EProm (Boot-Prom) lui permettant de booter sur le réseau. Chaque carte réseau dispose d'une adresse unique (adresse MAC) 1



#### 1.2 Câbles réseaux

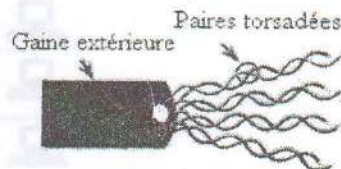
Les câbles réseaux permettent de relier entre eux des équipements afin de les faire communiquer. Ils doivent être adaptés en fonction des équipements en place (prise, vitesse, longueur, norme). Attention, la longueur maximale pour les câbles "RJ45" est de 100 mètres. Les câbles droits permettent de relier un périphérique (PC, imprimante) à un commutateur ou un concentrateur, les câbles croisés sont utilisés pour relier 2 PC entre eux.

Les anciens câbles (autre que "RJ45") faisaient appel à un type de câblage particulier (voir suite).

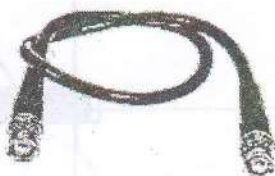
##### Câble équipé de prises RJ45 :



Ce câble est constitué de 8 fils de cuivre sous forme de 4 paires torsadées



##### Câble coaxial avec prises BNC



##### Exemples de connecteurs pour fibre optique

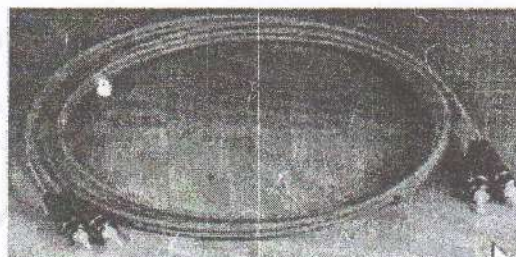


Connecteurs ST

Connecteurs SC



##### Exemple de câbles fibre optique





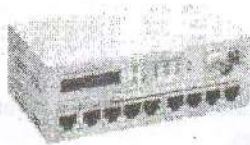
### 1.3 Equipements d'interconnexion :

Cela comprend tous les équipements permettant de relier entre eux les différents éléments d'un réseau. Les principaux équipements sont :

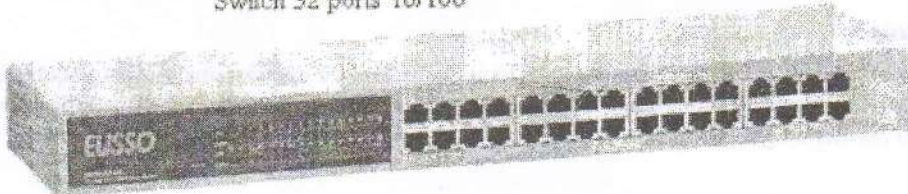
- Les concentrateurs ou hubs permettent d'interconnecter plusieurs machines entre elles sans gestion de trafic ou de priorité. Une donnée envoyée par une machine sera automatiquement acheminée vers tous les ports du concentrateurs et donc toutes les machines connectées.
- Les commutateurs, par opposition gèrent en interne une table d'identification. Ils mettent en communication les 2 machines concernées par un échange et uniquement celles-ci, ce qui permet d'augmenter le trafic en permettant plusieurs échanges en parallèle. Pour ce faire, ils analysent les données échangées et repèrent l'émetteur et le destinataire de l'information échangée.
- Les routeurs sont des équipements prévus pour interconnecter des réseaux. Ils sont prévus d'interfaces spécifiques pour se connecter sur des réseaux WAN. Ils sont souvent équipés de services logiciels avancés (filtre, firewall...) (IP)

Souvent, les commutateurs sont équipés de fonctions complémentaires :

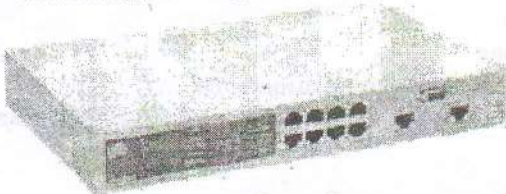
- auto-adaptables : ils adaptent automatiquement leur vitesse 10, 100 Mbps.
- cascadables : ils peuvent être interconnectés entre eux (on parle alors d'un port d'uplink)
- ...



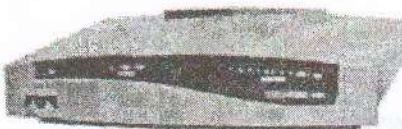
Switch 32 ports 10/100



Switch Gigabits + 8 ports 10/100



Routeur Cisco





LES PRINCIPAUX ORGANISMES NORMALISATEURS			
INDUSTRIELS	NATIONAUX	EUROPÉENS	ISO
IEC	AFNOR (France)	CEN (Europe)	ISO (la CITT)
ECMA	ANSI (USA)	CEC (Europe)	
	DIN (Allemagne)		

## Normalisation et modèle OSI

### 1 Introduction

Pour établir une communication entre deux ordinateurs, il faut tenir compte des différences entre le matériel et le logiciel de chaque machine.

Ces difficultés pour établir une communication se multiplient lorsqu'il s'agit d'interconnecter des réseaux mettant en jeu des matériels et des systèmes informatiques très différents.

Pour créer un réseau, il faut utiliser un grand nombre de composants matériels et logiciels souvent conçus par des fabricants différents. Pour que le réseau fonctionne, il faut que tous ces appareils soient capables de communiquer entre eux.

Pour faciliter cette interconnexion, il est apparu indispensable d'adopter des normes. Ces normes sont établies par différents organismes de normalisation.



LES PRINCIPAUX ORGANISMES NORMALISATEURS			
	EUROPEENS	NATIONAUX	INDUSTRIELS
- ISO - IUT-T (ex CCITT)	- CEN/CENELEC - CEPT	- AFNOR (France) - ANSI (USA) - BSI (UK) - DIN (Allemagne)	- ECMA - IEEE

AFNOR : Association Française de NORmalisation

ANSI : American National Standard Institute

BSI British Standard Institute

UIT-T : Union Internationale des Télécommunications – standardisation du secteur Télécommunication

CCITT : Comité Consultatif International pour le Télégraphe et le Téléphone

CEN : Comité Européen de Normalisation

CENELEC CEN ELECTrotechnique

CEPT Conférence Européenne des Postes et Télécommunications

DIN Deutsche Industry Norm

ECMA European Computer Manufacturers Association

ISO International Standard Organization

IEEE Institute of Electrical and Electronics Engineers

### 3 Le modèle OSI

Le modèle OSI (Open Systems Interconnection) définit de quelle manière les ordinateurs et les périphériques en réseau doivent procéder pour communiquer.

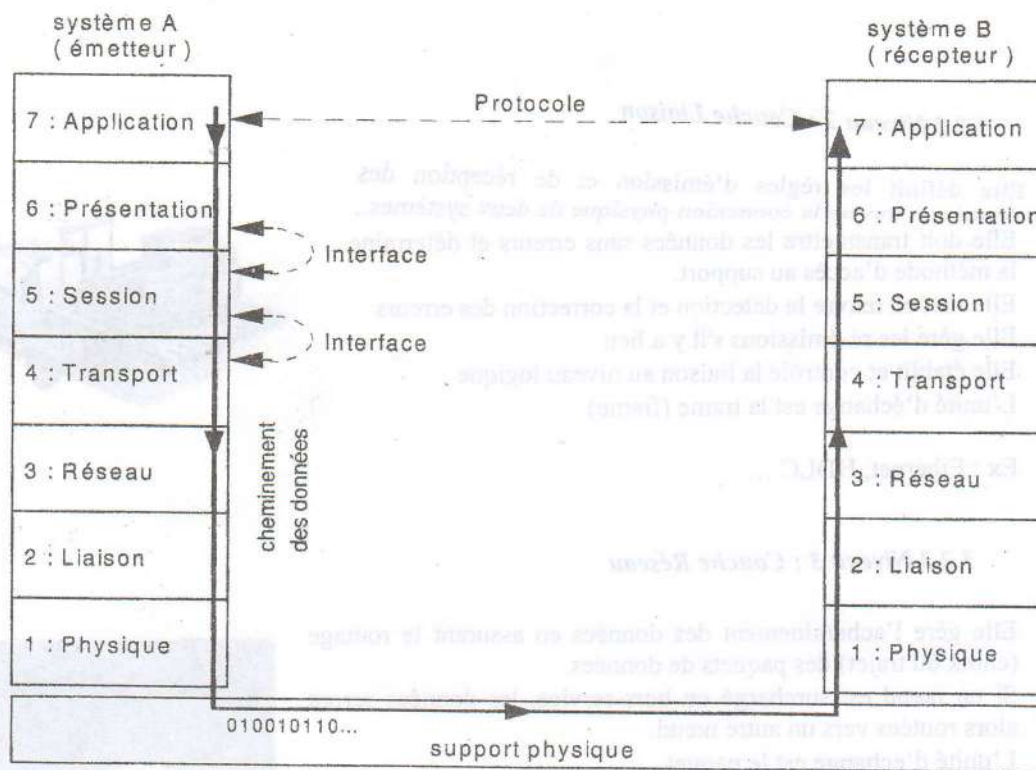
- Il spécifie le comportement d'un système dit ouvert.
- Les règles de communication constituent les protocoles normalisés.
- Le modèle OSI est normalisé par l'ISO.

#### 3.1 Description du modèle

Le modèle OSI se décompose en 7 parties appelées couches.

- Ce modèle date des années 1980
- Chaque couche est responsable de l'un des aspects de la communication.
- Une couche de niveau N communique avec les couches N+1 et N-1 par le biais d'une interface.
- Une couche inférieure transporte les données vers la couche supérieure sans en connaître la signification.
- Les couches N de 2 systèmes communiquent à l'aide de protocoles de communication commun.





- Couches 1 à 3 : couches basses orientées transmission
- Couche 4 : couche intermédiaire
- Couches 5 à 7 : couches hautes orientées traitement

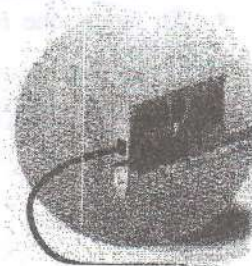
L'organisation en couches permet d'isoler des fonctions réseaux et de les implanter indépendamment de l'ensemble du système.

Cette organisation facilite l'évolution des logiciels réseau (Client / Serveur), en cachant les caractéristiques internes de la couche, au profit de la description des interfaces et des protocoles.

### 3.2 Services rendus par chaque couche

#### 3.2.1 Niveau 1 : Couche Physique

- Elle se charge de l'adaptation du signal au support de transmission, ce qui définit les caractéristiques électriques, logiques et physiques de la connexion de la station sur le réseau. (Câbles, connecteurs, cartes réseau...)
- Elle gère le type de transmission (synchrone ou asynchrone)
- S'il y a lieu, elle met en œuvre les mécanismes de modulation et démodulation du signal
- L'unité d'échange est le bit.





### 3.2.2 Niveau 2 : Couche Liaison

- Elle définit les règles d'émission et de réception des données à travers la connexion physique de deux systèmes..
- Elle doit transmettre les données sans erreurs et détermine la méthode d'accès au support.
- Elle met en œuvre la détection et la correction des erreurs
- Elle gère les ré-émissions s'il y a lieu
- Elle établit et contrôle la liaison au niveau logique
- L'unité d'échange est la trame (frame)

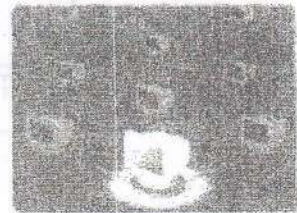
Ex : Ethernet, HDLC ...



### 3.2.3 Niveau 3 : Couche Réseau

- Elle gère l'acheminement des données en assurant le routage (choix du trajet) des paquets de données.
- Si un nœud est surchargé ou hors-service, les données seront alors routées vers un autre nœud.
- L'unité d'échange est le paquet.
- La couche réseau assure également la traduction des adresses logiques en adresses physiques.

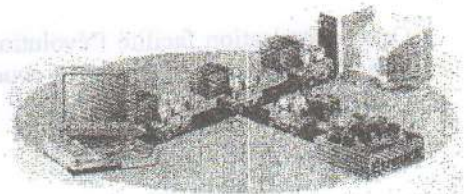
Ex : X25, IP...



### 3.2.4 Niveau 4 : Couche Transport

- Elle fournit un service de transport de bout en bout transparent pour l'utilisateur (même à travers plusieurs réseaux).  
Ex : Etablissement, Maintien, Rupture, ...
- Elle assure également les services qui n'ont pas été pris en compte par les couches inférieures (gestion des erreurs, routage...).
- Elle permet de multiplexer plusieurs flux sur le même support
- En temps qu'émetteur, elle segmente les messages en paquets numérotés
- En temps que récepteur, elle reconstitue les messages en plaçant les paquets dans l'ordre

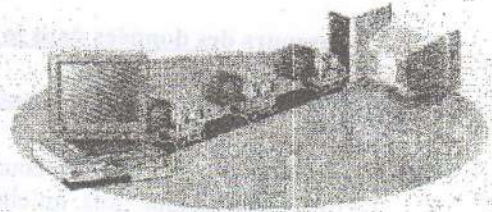
Ex : TCP, UDP, Netbios...





### 3.2.5 Niveau 5 : Couche Session

- C'est la première couche orientée traitement
- Elle permet l'ouverture et la fermeture d'une session de travail entre 2 systèmes distants et assure la synchronisation du dialogue.
- Elle définit le mode de transmission (Half-duplex, Full-duplex)
- Elle définit la liaison entre deux programmes d'application et gère le dialogue.
- Elle gère la chronologie du dialogue afin de mettre en place des procédures de reprise.



### 3.2.6 Niveau 6 : Couche Présentation

- Elle permet de transcrire les données dans un format compréhensible par les 2 systèmes (formatage des données).
- Elle assure la mise en forme de l'information pour qu'elle soit accessible à l'utilisateur
- Elle effectue les fonctions de codage, compression, cryptage et décryptage, ...



### 3.2.7 Niveau 7 : Couche Application

- Elle fournit des services utilisables sur le réseau par les applications installées.
- Les principaux services sont :
  - Transfert de fichiers (FTP)
  - Messagerie ou courrier électronique (pop, smtp)
  - Lecture de pages Internet (http)
  - Accès à distance (Telnet)



## 3.3 Tableau récapitulatif

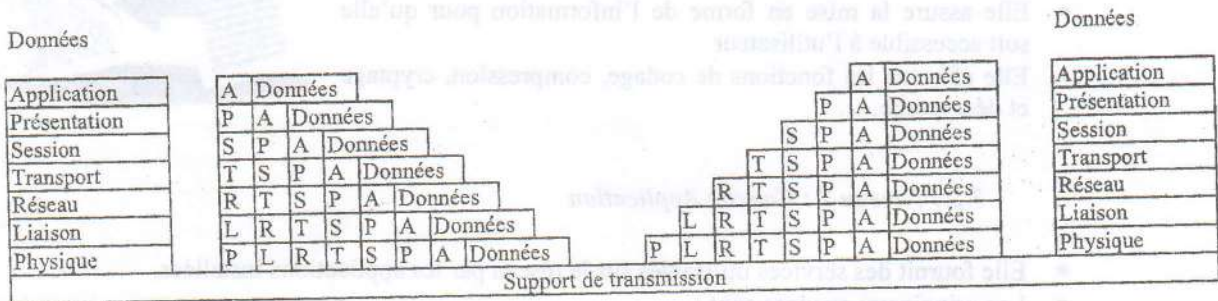
COUCHE	ROLE
1. PHYSIQUE	Envoi et réception des séquences de bits
2. LIAISON	Organisation des données en trames et transmission
3. RÉSEAU	Acheminement des paquets de données (routage, contrôle des flux)
4. TRANSPORT	Découpage du message en paquets (et inversement : ré-assemblage des paquets en message dans le bon ordre) -Gestion de plusieurs connexions sur la même voie de communication (multiplexage) ou éclatement d'une connexion sur plusieurs voies.
5. SESSION	Établissement, contrôle, terminaison d'une connexion entre deux systèmes
6. PRÉSENTATION	Formatage, conversions, (+ compression et cryptage) des données
7. APPLICATION	Fourniture de services réseaux aux applications



## 4

Lorsque les données sont transférées au sein d'un réseau :

- Elles parcourent chacune des couches du modèle OSI de l'émetteur (7-Application → 1-Physique). Chaque fois qu'elles traversent une couche, elles sont enrichies de nouvelles informations : les informations délivrées par le protocole de la couche sont ajoutées (on parle d'encapsulation).
- Elles sont transmises sur le support.
- Elles parcourent chacune des couches du modèle OSI du récepteur (1-Physique → 7-Application). Chaque fois qu'elles traversent une couche, les informations ajoutées par le protocole de même niveau de l'émetteur sont enlevées et exploitées (on parle de désencapsulation).





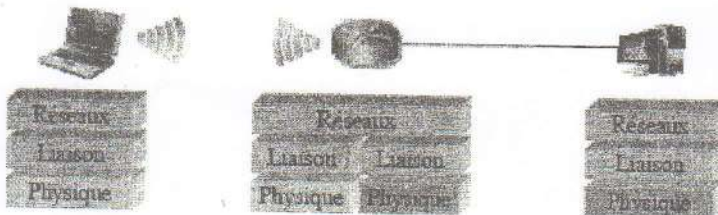
Implémentation	Modèle Internet	Modèle OSI
Application	Application	Application
		Présentation
		Session
Système d'exploitation	TCP - UDP	
	IP	Réseau
Pilote Périphérique	Wi-Fi/Ethernet etc.	Liaison
		Physique

## □ Couches basses: physique, liaison et réseau

- Assure la transmission des données au travers du réseau



Les couches liaison et physiques ne permettent la communication qu'entre des entités directement connectées.



Les couches physiques et liaisons peuvent être différentes d'un réseau à l'autre.

La couche réseau définit des procédures d'acheminement indépendantes des couches inférieures: elle assure l'interconnexion des réseaux.

# L'ADRESSAGE IP

## I. Introduction

Il est nécessaire de différencier les adresses de couche 2 et de couche 3, car l'adressage au niveau de chacune de ces couches n'a pas le même rôle :

- ☐ L'adressage MAC en couche 2 permet d'identifier les machines *sur un même réseau*.
- ☐ L'adressage IP en couche 3 permet d'adresser les machines *sur des réseaux distincts*.

Les adresses de couche 2 sont en rapport avec le matériel réseau utilisé (le protocole de couche 2 est géré au niveau de la carte connectée au réseau et non pas par le système d'exploitation comme les couches supérieures), il est donc difficile de modifier les adresses MAC qui sont censées être codées directement sur la carte réseau. Cela est notamment dû au fait que chaque adresse **MAC doit être unique** sous peine de conflit matériel, et que cette adresse doit être accessible très tôt lors du boot d'une machine.

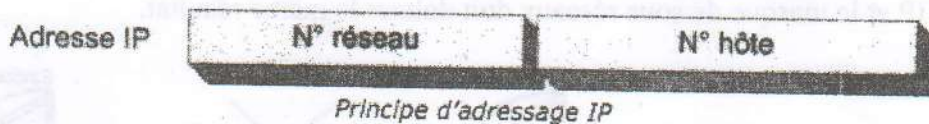
Les adresses de couche 3 quant à elles demandent une certaine souplesse d'utilisation car on ne connaît pas a priori l'adresse du réseau sur lequel une machine va se trouver. Il y a donc une incompatibilité d'utilisation d'une adresse de couche 2 pour une adresse de couche 3, et vice versa.

## II. Constitution d'une adresse IP

Constituée de 4 octets, elle est découpée en 2 parties :

- ☐ Le numéro de réseau (netid)
- ☐ Le numéro de l'hôte sur ce réseau (hostid)

La taille du *netid* dépend de la **classe d'adresse IP** utilisée. Il existe plusieurs classes d'adresses IP dédiées à des usages différents. Plus le numéro de réseau est grand et plus le nombre d'hôtes sur ce réseau sera petit.

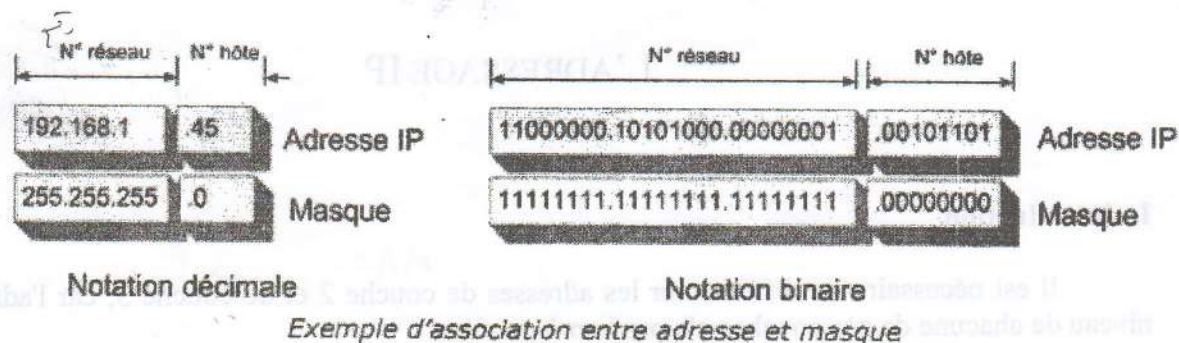


## III. Le masque

Le masque agit comme un séparateur entre le n° de réseau et le n° d'hôte. Le masque est également constitué de 4 octets et est souvent associé à l'adresse IP.

Tous les bits à 1 du masque permettent de définir chaque bit correspondant de l'adresse IP comme un bit faisant partie du n° de réseau. Par opposition, tous les bits à 0 du masque permettent de définir chaque bit correspondant de l'adresse IP comme un bit faisant partie du n° d'hôte.





Le masque servant à faire la séparation en deux parties sur une adresse IP, il est donc indissociable de celle-ci. Une adresse seule ne voudra rien dire puisqu'on ne saura pas quelle est la partie réseau et quelle est la partie machine. De la même façon, un masque seul n'aura pas de valeur puisqu'on n'aura pas d'adresse sur laquelle l'appliquer. L'adresse IP et le masque sont donc liés l'un à l'autre, même si l'on peut choisir l'un indépendamment de l'autre.

Il existe une autre manière de noter le masque. Il s'agit de compter le nombre de bits à 1 du masque et de noter ce chiffre à la fin de l'adresse.

Par exemple, le couple adresse et masque suivant:

- 192.168.1.13
- 255.255.255.0

S'écrit dans cette nouvelle notation :

- 192.168.1.13 / 24

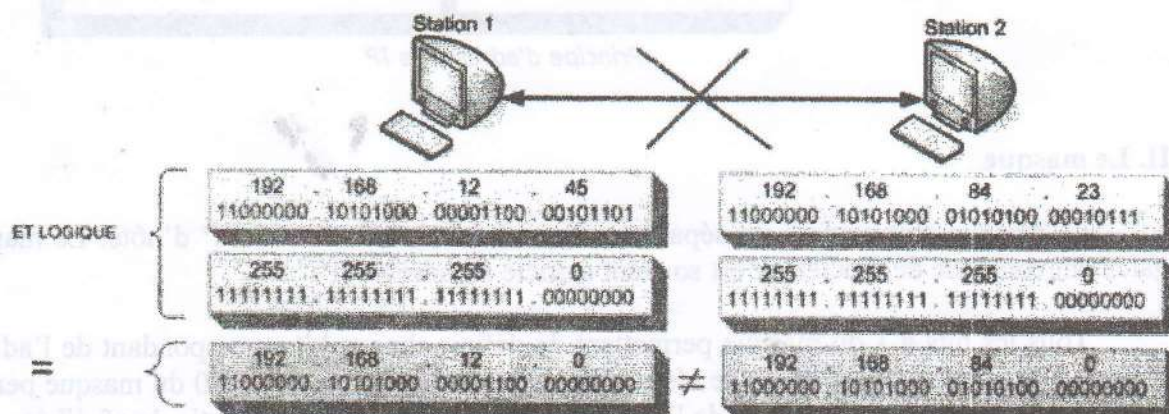
Le chiffre 24 indique que 24 bits du masque sont à 1.

### Remarque

Cette notation est aujourd'hui très utilisée dans tous les équipements réseaux récents afin de simplifier l'écriture et rendre la configuration plus aisée

### Application du masque

Pour que 2 stations puissent communiquer, la règle est la suivante : Un **ET** logique entre l'adresse IP et le masque de sous réseaux doit donner le même résultat.





#### IV. Les classes d'adresses IP

Nous avons vu que l'adresse IP est indissociable de son masque. Néanmoins le choix des adresses et des masques ne doit pas être faite au hasard. C'est là qu'interviennent les classes A, B, C, D et E.

Les classes ont été – car elles ne le sont plus – un moyen efficace de segmenter l'espace d'adressage d'Internet. Nous verrons que si les classes sont encore très utilisées dans les réseaux locaux, d'autres techniques comme le « **subnetting** » ou l'adressage « **CIDR** » sont monnaies courantes sur Internet.

Pour savoir à quelle classe appartient une adresse IP, il faut se pencher sur sa représentation binaire. En effet, la valeur des 4 premiers bits de l'adresse détermine la classe.

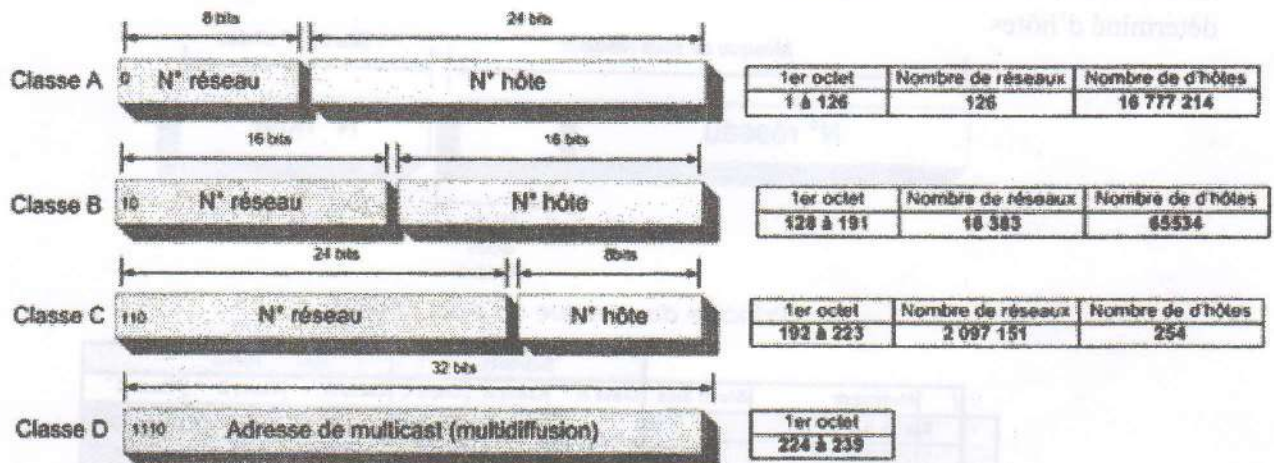
Voici un tableau récapitulatif des différentes classes d'adresses IP en fonction des 1<sup>er</sup> bits du 1<sup>er</sup> octet :

*MSB (Most Significant Bit)*

Bits de poids fort	Classe
0	A
10	B
110	C
1110	D
1111	E

Tableau des classes d'IP en fonction des bits de poids fort

Ceci nous amène à faire quelques constatations sur le potentiel d'adresses et de réseaux détenu par chaque classe d'adresse :



Les classes d'adresses IP

#### Exemples

- 83.206.23.134 : Adresse de classe A , netid = 83 , hostid = 206.23.134
- 190.12.24.56 : Adresse de classe B , netid = 190.12 , hostid = 24.56
- 192.168.1.5 : Adresse de classe C, netid=192.168.1 , hostid=5



## V. Les adresses IP publiques et privées

Les adresses publiques sont celles qui sont utilisées sur Internet. Pour des raisons que nous verrons lorsque nous parlerons du routage, un réseau local **ne doit pas utiliser d'adresses publiques**. Il utilise des adresses privées. La liste des adresses privées autorisées sont :

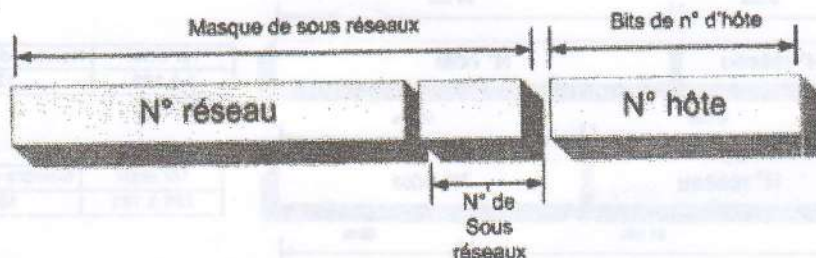
- ☐ Classe A : de 10.10.0.1 à 10.255.255.254
- ☐ Classe B : de 172.16.0.1 à 172.31.255.254
- ☐ Classe C : de 192.168.0.1 à 192.168.255.254

## VI. Technique du « subnetting »

L'objectif du « **subnetting** » est de scinder une classe d'adresses en sous réseaux indépendants. Chaque sous-réseau dispose d'un nombre limité d'adresses.

Cette technique vient combler certaines lacunes des classes d'adresses. En effet, les classes A, B et C sont mal adaptées aux besoins croissants des réseaux. La classe B, par exemple, offre un nombre total de 65534 hôtes alors que la classe C n'en offre que 254. Il apparaît que si les besoins sont légèrement supérieurs aux 254 hôtes qu'offre une classe C, il en résulte un gâchis d'adresses si on choisit une classe B.

L'idée est de réserver quelques bits du numéro d'hôte pour créer des sous réseaux. A chaque n° de réseau, on associe un certain nombre de sous réseaux qui eux-mêmes contiennent un nombre déterminé d'hôtes.



Principe du masque de sous réseau

	Netmask	Block Size	Subnets			Hosts		
			Class A	Class B	Class C	Class A	Class B	Class C
Class A Network	8 255.0.0.0	256	1			16777214		
	9 255.128.0.0	128	2			8388606		
	10 255.192.0.0	64	4			4194302		
	11 255.224.0.0	32	8			2097150		
	12 255.240.0.0	16	16			1048574		
	13 255.248.0.0	8	32			524286		
	14 255.252.0.0	4	64			262142		
	15 255.254.0.0	2	128			131070		
	16 255.255.0.0	256	256	1		65534	65534	
	17 255.255.128.0	128	512	2		32766	32766	
	18 255.255.192.0	64	1024	4		16382	16382	
	19 255.255.224.0	32	2048	8		8190	8190	
	20 255.255.240.0	16	4096	16		4094	4094	
	21 255.255.248.0	8	8192	32		2046	2046	
	22 255.255.252.0	4	16384	64		1022	1022	
Class B Network	23 255.255.254.0	2	32768	128		510	510	
	24 255.255.255.0	256	65536	256	1	254	254	254
	25 255.255.255.128	128	131072	512	2	126	126	126
	26 255.255.255.192	64	262144	1024	4	62	62	62
	27 255.255.255.224	32	524288	2048	8	30	30	30
	28 255.255.255.240	16	1048576	4096	16	14	14	14
	29 255.255.255.248	8	2097152	8192	32	6	6	6
	30 255.255.255.252	4	4194304	16384	64	2	2	2
Class C Network								



## VII. Technique du « supernetting »

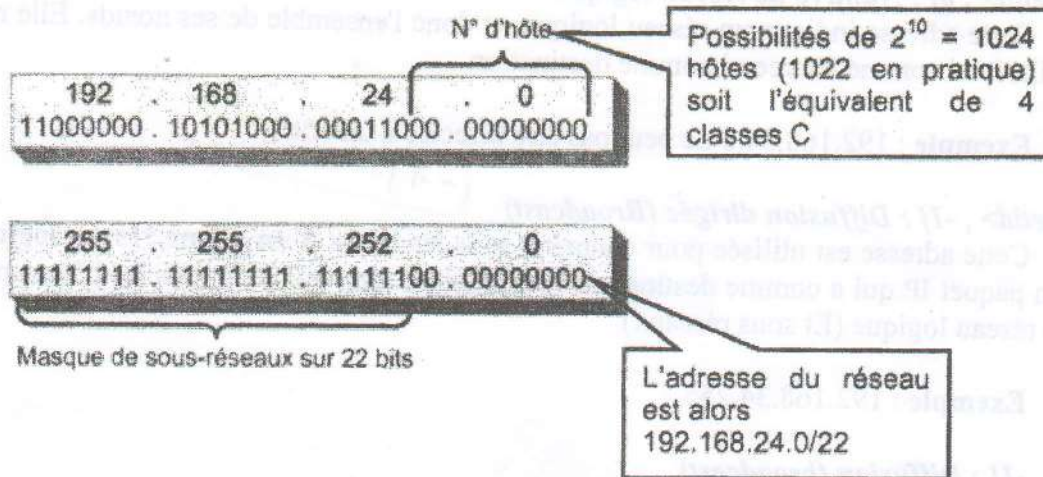
La technique du « supernetting » consiste en une agrégation de plusieurs classes (La classe C) pour former des réseaux de taille permettant d'éviter le gâchis d'adresses.

Nous avons vu que la technique du « subnetting » consistait à utiliser une partie du « hostid » pour créer des sous réseaux. La technique du « supernetting » consiste à utiliser une partie du masque de sous-réseau.

En utilisant quelques bits du masque de sous-réseaux, cela revient à obtenir plusieurs réseaux d'une même classe d'adresse.

Voici un exemple d'un réseau utilisant le « supernetting » en agrégeant 4 classes C :

- ☐ Ici, le numéro d'hôte (hostid) est sur 10 bits, soit 2 de plus qu'un classe C
- ☐ Alors que le numéro de réseau est sur 22 bits.



Exemple d'agrégation de 4 classes C

## VIII. Adressage CIDR (Classless InterDomain Routing)

A partir de 1994, le nombre d'adresses IP n'était plus suffisant pour satisfaire toutes les demandes d'accès à Internet. De plus, les *tables de routage* des routeurs devenaient tellement énormes que les performances chutaient. Si rien n'avait été fait, nous n'entendrions certainement plus parler d'Internet aujourd'hui.

Heureusement, l'adressage basé sur les classes A, B et C a été remplacé par l'adressage CIDR. Il s'agit d'une technique permettant de **répartir plus efficacement les adresses IP** entre les demandeurs.

Au lieu d'avoir une taille fixe pour le numéro de réseau (8,16 ou 24), l'adressage CIDR utilise une taille variable pouvant aller de 13 à 29.

Par exemple pour le numéro de réseau 83.206.23.128 et un masque de 255.255.255.248 on obtient **un réseau de 8 postes connectés directement à Internet** (« pool d'IP fixes »)



Exemple de « pool de 8 IP fixes »

Une adresse prise dans le pool s'écrit : 83.206.23.131/29



## IX. Les adresses IP spéciales

Certaines adresses IP sont spéciales et ne peuvent être utilisées par un hôte sur le réseau. Une adresse IP est composée d'un numéro de réseau complété par un numéro d'hôte :

$$\{< \text{numéro de réseau} >, < \text{numéro d'hôte} >\} = \{< \text{netid} >, < \text{hostid} >\}$$

Certaines valeurs sont donc interdites (0 signifie *tous les bits à 0* et -1 signifie *tous les bits à 1* :  $\{< \text{netid} >, 0\}$ ,  $\{< \text{netid} >, -1\}$ ,  $\{-1, -1\}$ ,  $\{0, 0\}$ ,  $\{0, < \text{hostid} >\}$ ,  $\{127, < \text{quelconque} >\}$  et l'adresses de classe D.

### a. $\{< \text{netid} >, 0\}$ : Numéro de réseau logique

Cette adresse indique un réseau logique, et donc l'ensemble de ses nœuds. Elle ne peut donc être utilisée ni comme source ni comme destination.

**Exemple** : 192.168.34.0 ne peut pas être affectée à un hôte.

### b. $\{< \text{netid} >, -1\}$ : Diffusion dirigée (Broadcast)

Cette adresse est utilisée pour contacter **tous les hôtes d'un même réseau logique**. Dans ce cas, un paquet IP qui a comme destination cette adresse sera envoyé à tous les hôtes appartenant au même réseau logique (Et sous réseaux)

**Exemple** : 192.168.34.255

### c. $\{-1, -1\}$ : Diffusion (broadcast)

Cette adresse est utilisée pour contacter **tous les hôtes quels que soient leur réseau logique**. Dans ce cas, un paquet IP qui a comme destination cette adresse sera envoyée à tous les hôtes du réseau physique.

**Exemple** : 255.255.255.255

### Remarque

Bien évidemment, la plupart des routeurs sont programmés pour ne pas laisser passer ce genre de diffusion (Imaginez un instant que l'on puisse envoyer un message de ce type sur Internet!)

### d. $\{0, 0\}$ : DHCP et BOOTP

Les protocoles DHCP (*Dynamic Host Configuration Protocol*) et BOOTP sont prévus pour permettre à des postes qui n'ont pas d'adresse IP d'en obtenir une automatiquement sans intervention particulière sur la station.

Cette adresse IP est utilisée pour effectuer une demande d'adresse IP auprès d'un serveur DHCP.

**Exemple** : 0.0.0.0

### e. $\{0, < \text{hostid} >\}$ : Hôte dans tous les réseaux logiques

Un paquet IP envoyé avec cette adresse de destination sera envoyé à tous les hôtes ayant le même numéro d'hôte mais situés dans des réseaux logiques différents.

**Exemple** : 0.0.0.12 concernera 192.168.0.12 et 192.168.23.12, etc, etc ...



**f. {127, <quelconque>} : Adresse de boucle locale**

Un paquet IP envoyé avec cette adresse de destination sera reçu par l'expéditeur lui-même. Le paquet ne sort pas sur la carte réseau, il reste local.

**g. Adresses de classe D**

Il s'agit d'adresses spéciales permettant d'envoyer des paquets IP à un groupe de stations. En effet, une station peut se mettre à l'écoute d'une de ces adresses de multidiffusion. Dans ce cas, elle recevra les données.

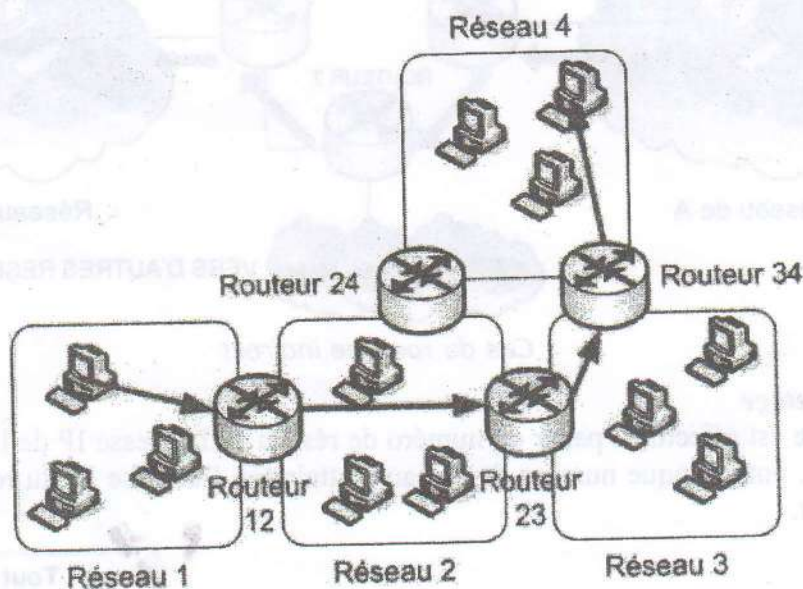
L'appartenance à un groupe est dynamique. C'est-à-dire qu'une station peut très bien décider d'entrer ou de quitter un groupe de multidiffusion.

Parmi les adresses de multidiffusion, il en existe ayant une signification spéciale. La liste suivante n'est pas exhaustive. (La liste complète peut-être obtenue en consultant l'adresse <http://www.iana.org/assignments/multicast-addresses>) :

- ☐ **224.0.0.1** : Tous les hôtes d'un même sous réseau
- ☐ **224.0.0.2** : Tous les routeurs d'un même sous réseau
- ☐ **224.0.0.9** : Routeurs utilisant le protocole RIP2
- ☐ ...

**X. Le routage IP**

Il s'agit sans là de la pierre angulaire des réseaux TCP/IP. Le routage est une orientation des paquets vers un réseau de destination. Chaque routeur est connecté à plusieurs réseaux. Ils maintiennent à jour une table de routage leur permettant de prendre des décisions en fonction des caractéristiques du paquet à orienter.



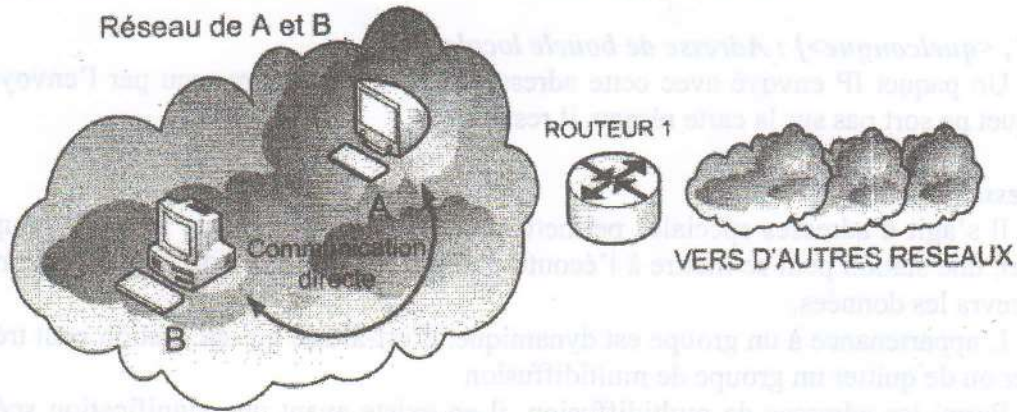
Exemple de routage

**a. Le routage direct**

C'est le cas de deux stations situées dans le même segment de réseau. Il peut s'agir aussi d'une communication entre une station et un routeur. Dans ce cas, la table de routage interne de la station est utilisée pour envoyer le paquet directement au destinataire dont l'adresse physique aura été connue (via le protocole ARP).



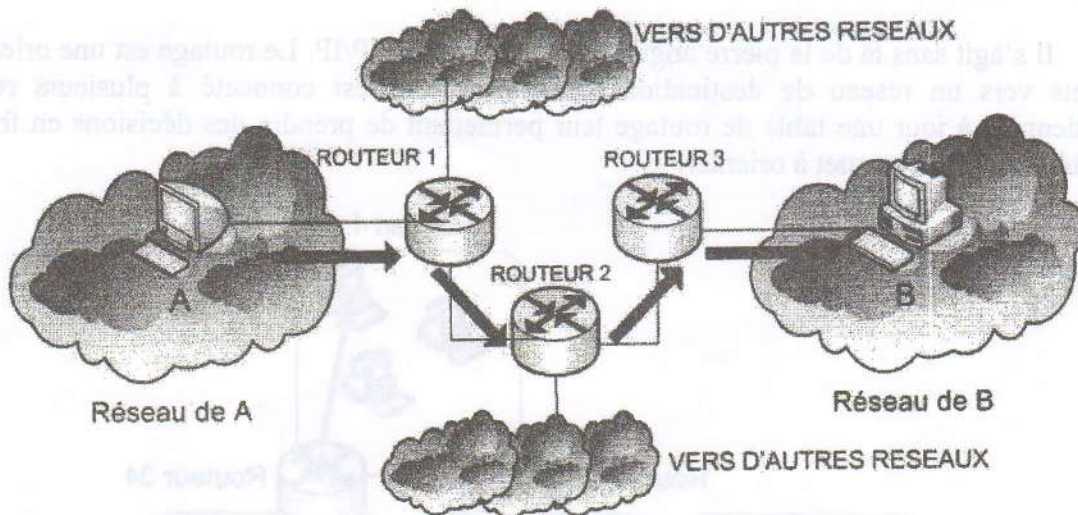
## Réseau de A et B



Cas du routage direct

### b. Le routage indirect

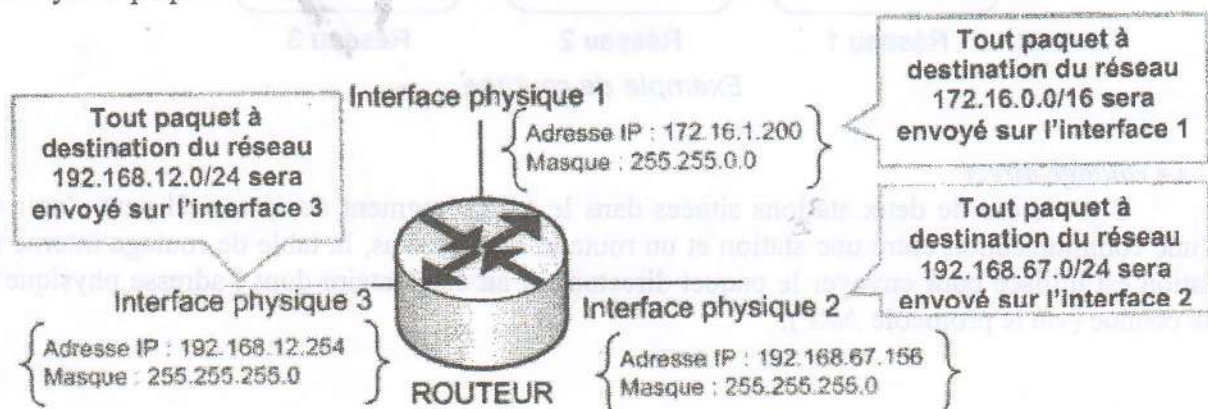
Dans ce cas, le routage est plus complexe car il faut déterminer le routeur qui va se charger d'orienter le paquet vers le bon réseau. C'est généralement le rôle de la passerelle par défaut que tout client peut utiliser lorsque l'adresse IP du destinataire n'est pas une adresse IP faisant partie du sous réseau logique.



Cas du routage indirect

### c. La table de routage

Le routage est effectué à partir du numéro de réseau de l'adresse IP de l'hôte de destination. La table contient, pour chaque numéro de réseau à atteindre, l'adresse IP du routeur auquel il faut envoyer le paquet.



Exemple de constitution d'une table de routage



Ce qui donnerait la table de routage suivante :

Réseau destination	Masque	Interface
192.168.12.0	255.255.255.0	ethernet3
192.168.67.0	255.255.255.0	ethernet2
172.16.0.0	255.255.0.0	ethernet1
0.0.0.0	0.0.0.0	ethernet1

Voici un exemple de table de routage :

```

routeur:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
83.206.23.128    0.0.0.0         255.255.255.248 U        0      0      0 eth3
172.16.101.0     172.16.1.101   255.255.255.0  UG       2      0      0 eth2
172.16.100.0     172.16.1.100   255.255.255.0  UG       2      0      0 eth2
172.16.103.0     172.16.1.103   255.255.255.0  UG       2      0      0 eth2
172.16.102.0     172.16.1.102   255.255.255.0  UG       2      0      0 eth2
172.16.115.0     172.16.1.115   255.255.255.0  UG       2      0      0 eth2
192.168.0.0      0.0.0.0         255.255.255.0  U        0      0      0 eth1
172.16.1.0       0.0.0.0         255.255.255.0  U        0      0      0 eth2
172.16.114.0     172.16.1.114   255.255.255.0  UG       2      0      0 eth2
172.16.109.0     172.16.1.109   255.255.255.0  UG       2      0      0 eth2
172.16.200.0     172.16.1.200   255.255.255.0  UG       2      0      0 eth2
172.16.108.0     172.16.1.108   255.255.255.0  UG       2      0      0 eth2
172.16.111.0     172.16.1.111   255.255.255.0  UG       2      0      0 eth2
172.16.110.0     172.16.1.110   255.255.255.0  UG       2      0      0 eth2
172.16.105.0     172.16.1.105   255.255.255.0  UG       2      0      0 eth2
172.16.104.0     172.16.1.104   255.255.255.0  UG       2      0      0 eth2
172.16.107.0     172.16.1.107   255.255.255.0  UG       2      0      0 eth2
172.16.106.0     172.16.1.106   255.255.255.0  UG       2      0      0 eth2
10.0.0.0         0.0.0.0         255.0.0.0      U        0      0      0 eth0
0.0.0.0          83.206.23.134  0.0.0.0        UG       0      0      0 eth3
routeur:~#

```

Table de routage d'un routeur sous LINUX

Voici la signification des colonnes intéressante de cet exemple :

- ☐ Destination : Il s'agit de l'adresse de l'hôte ou du réseau de destination. Par exemple 192.168.0.0 avec un masque de 255.255.255.0 désigne le numéro de réseau logique 192.168.0
- ☐ Gateway : La passerelle (routeur) à utiliser pour joindre ce réseau (0.0.0.0 signifie qu'il s'agit du routeur sur lequel est stocké cette table).
- ☐ Genmask : Masque de sous réseau associé à l'adresse de destination
- ☐ Flags : Précise l'état courant de la route.
- ☐ Metric : Le nombre de sauts max (routeurs) pour parvenir jusqu'au réseau de destination.
- ☐ Ref : Nombre de références à cette route.
- ☐ Use : Nombre de recherches effectuées sur cette route.
- ☐ IFace : Interface matérielle ou logicielle utilisée pour envoyer les paquets vers cette route.

#### d. Le routage et la couche 2 (MAC)

Le routage intervient au niveau de la couche 3 du modèle OSI. Nous allons voir comment la couche 2 peut utiliser les informations de la couche 3 pour mener à bien une communication entre 2 stations situées dans des réseaux différents.





	Etape	IP source	IP dest	MAC Source	MAC Dest
A contacte son routeur	1	192.168.12.45	172.16.1.45	AA.AA.AA.AA.AA.AA	R0.R0.R0.R0.R0.R0
Routeur contacte B	2	192.168.12.45	172.16.1.45	R1.R1.R1.R1.R1.R1	BB.BB.BB.BB.BB.BB
B répond à routeur	3	172.16.1.45	192.168.12.45	BB.BB.BB.BB.BB.BB	R1.R1.R1.R1.R1.R1
Routeur transmet à A	4	172.16.1.45	192.168.12.45	R0.R0.R0.R0.R0.R0	AA.AA.AA.AA.AA.AA

Exemple de routage indirect avec les informations de couche 2 (MAC)

Nous savons que les adresses matérielles (MAC) des stations d'un réseau physique ne sont pas connues par les stations d'autres réseaux physiques.

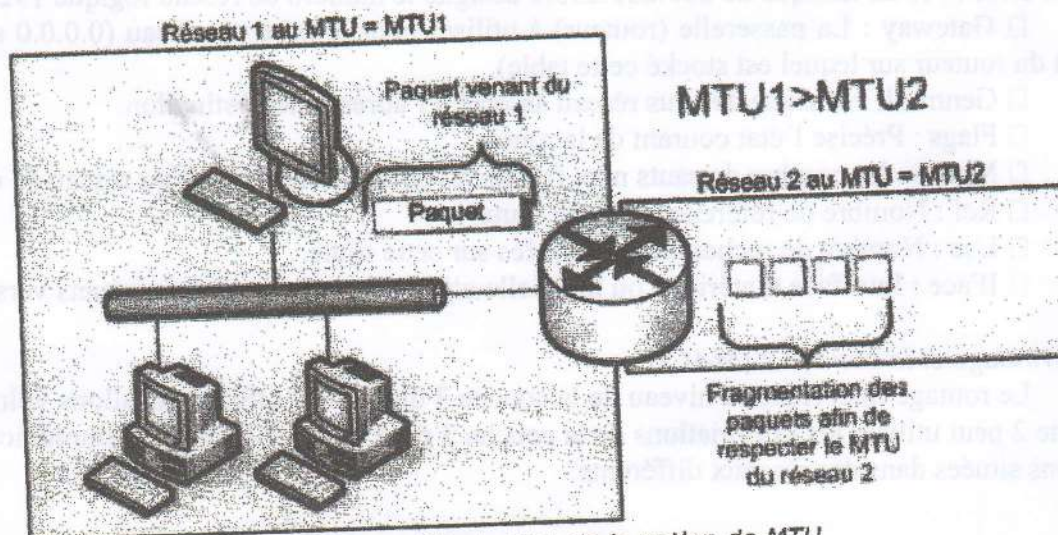
Une station A souhaitant communiquer avec une station B, va donc utiliser l'adresse MAC de sa passerelle par défaut. De l'autre côté, la station B va répondre en utilisant l'adresse MAC de l'interface 1 du routeur. A aucun moment, la station B ne connaît l'adresse MAC de la station A.

#### e. MTU (Maximum Transmission Unit)

Dans le cas de transfert de données dans un réseau routé, la capacité des routeurs à traiter le maximum de paquets en provenance de sources différentes dans un minimum de temps est déterminante.

En effet, un utilisateur donné doit de monopoliser la bande passante des routeurs en transmettant de gros fichiers par exemple. De cette remarque est née l'idée de la fragmentation de données. Cette fragmentation va permettre à chaque routeur de transférer des paquets d'une taille convenable qui permettra à ces équipements de répartir équitablement la bande passante.

Le MTU correspond justement à la taille maximum d'un paquet qui peut être transféré sur un réseau. Au-delà de cette taille, le paquet devra être fragmenté.



Exemple d'illustration de la notion de MTU