



# Réseaux informatiques

Responsable: Pr. Hamid AKSASSE

*haksasse@gmail.com*

ENSA Agadir

AU: 2020-2021

# Plan du cours

Chapitre 1 : Introduction aux réseaux Informatiques

- Définitions et concepts de base

Chapitre 2 : modèles et architectures de référence

- Normalisation des réseaux
- Modèle OSI
- Architecture TCP / IP

Chapitre 3 : Systèmes et Supports de transmission de données

- Les systèmes de transmission
- Les supports des transmission

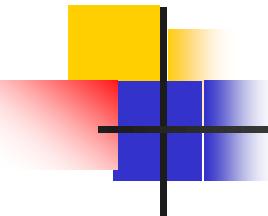
# Plan du cours (suite)

## Chapitre 4 : Les réseaux locaux

- Etude de la couche liaison de données
- Les réseaux locaux
  - Les réseaux Ethernet
- Interconnexion des réseaux locaux

## Chapitre 5 : Le modèle TCP/IP

- Historique
- Architecture
- L'encapsulation des données
- Protocoles Normalisés de la couche Réseau
- Protocoles Normalisés de la couche Transport
- Protocoles Normalisés de la couche Application



## Chapitre -1-

# Introduction aux Réseaux Informatiques

# 1. Définitions et concepts de base

## Définition

Un réseau en général est un ensemble de matériels interconnectés les uns avec les autres.

Exemple de réseau :

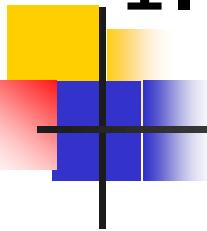
- Réseau de transport : Transport de personnes (trains, bus, taxi)
- Réseau téléphonique : Transport de la voix de téléphone à téléphone
- Réseau de neurones : Cellules reliées entre elles

Un réseau informatique est un ensemble d'équipements reliés entre eux afin de partager des données, des ressources et d'échanger des informations.

- Réseau informatique : Ensemble d'ordinateurs reliés entre eux pour échanger des données numériques (des 0 ou des 1)

Besoin de partage de ressources: données, messages, graphiques, imprimantes, télécopieurs, modems, autres

# 1. Définitions et concepts de base



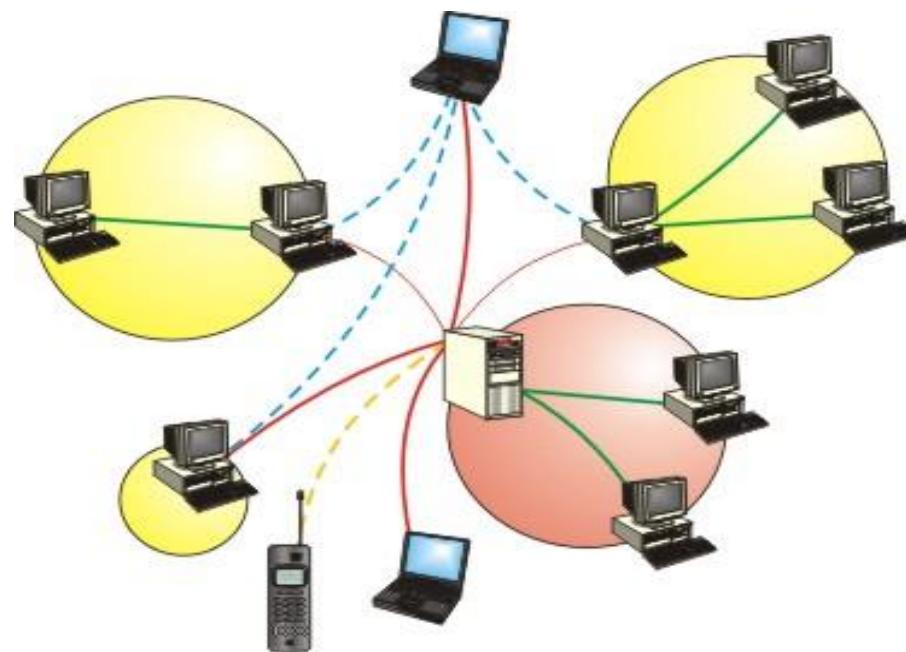
**Un réseau:** définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres.

Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

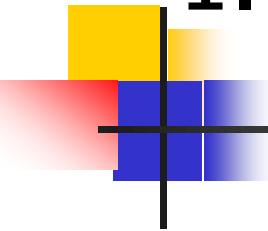


# 1. Définitions et concepts de base

**Réseau informatique:** ***computer network*** ensemble d'ordinateurs et de périphériques qui sont reliés entre eux par des supports de transmission et échangent les informations sous forme de données numériques.



# 1. Définitions et concepts de base



Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.).
- La communication entre personnes (courrier électronique, discussion en direct, etc.).
- La garantie de l'unicité de l'accès à l'information (bases de données en réseau).
- L'accès au World Wide Web.
- Les services utilisant le Web (documentation, commerce électronique, etc.).
- ...

# 1. Définitions et concepts de base

## Intérêt d'un réseau

### ■ Le partage

Un réseau sert essentiellement à partager quelque chose avec d'autres personnes tel que: Des données, du matériel, de logiciel,...

- Économies financières
- Gains de productivité

### ■ La centralisation

- La base de données
- Les sauvegardes

## Les inconvénients du réseau

### La complexité

- Personnels spécialisé
- Nombreuses pannes

### La dépersonnalisation des échanges

# 1. Définitions et concepts de base

## Questions pour décrire un réseau

Pour décrire un réseau, il faut répondre aux questions suivantes :

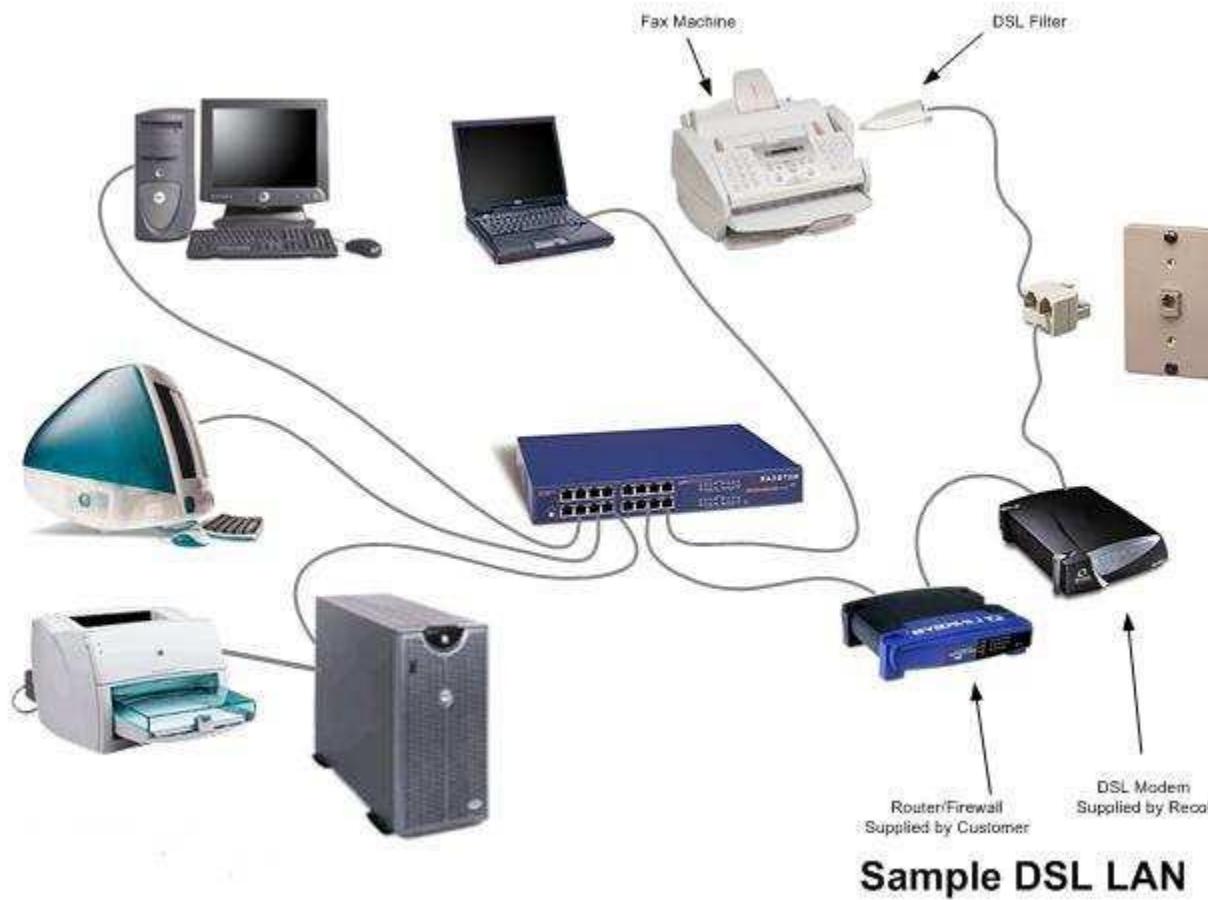
- Que transporte le réseau ?
- Qui assure le transport ?
- Comment le transporte-il ?

Exemple pour le « réseau informatique » :

- Que transporte le réseau ?
  - Des informations (octets sous forme de fichiers)
- Qui assure le transport ?
  - Support physique (cuivre, fibre optique, onde radio)
- Comment le transporte-il ?
  - En utilisant des protocoles de communication.

# 1. Définitions et concepts de base

## Exemple de réseau



# 1. Définitions et concepts de base

Téléinformatique : informatique à distance

C'est une science qui associe le traitement de l'information (les données) qui est le domaine propre de l'ordinateur, avec le transport de l'information, qui est le domaine des télécommunications...

Pourquoi des réseaux?

Sans réseau l'échange des informations s'effectue en général par de nombreux documents imprimés et le transport de fichiers sur support du masse (clé USB, CD, ...). A la perte de temps, il faut même parfois ajouter la perte d'informations.

# 1. Définitions et concepts de base

## Les similitudes de différents réseaux

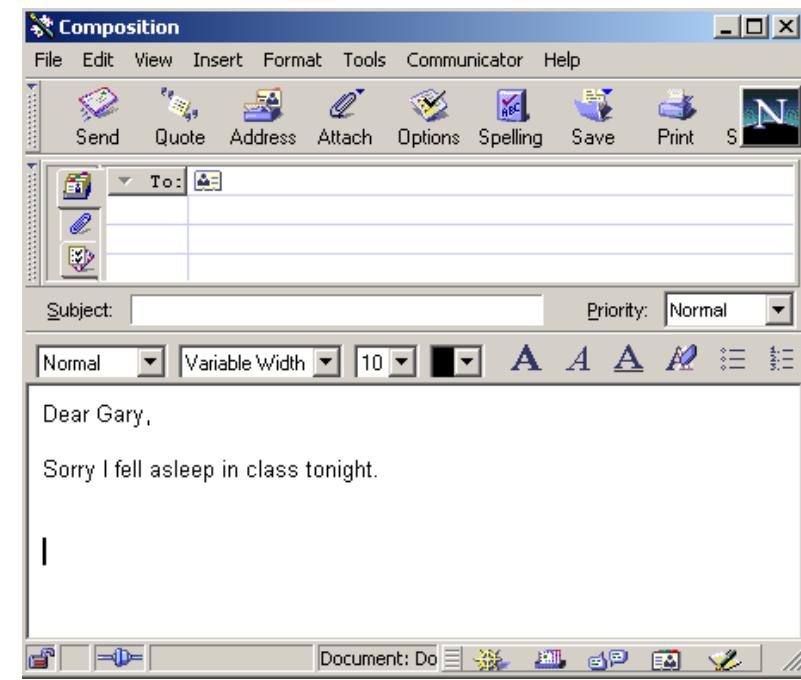
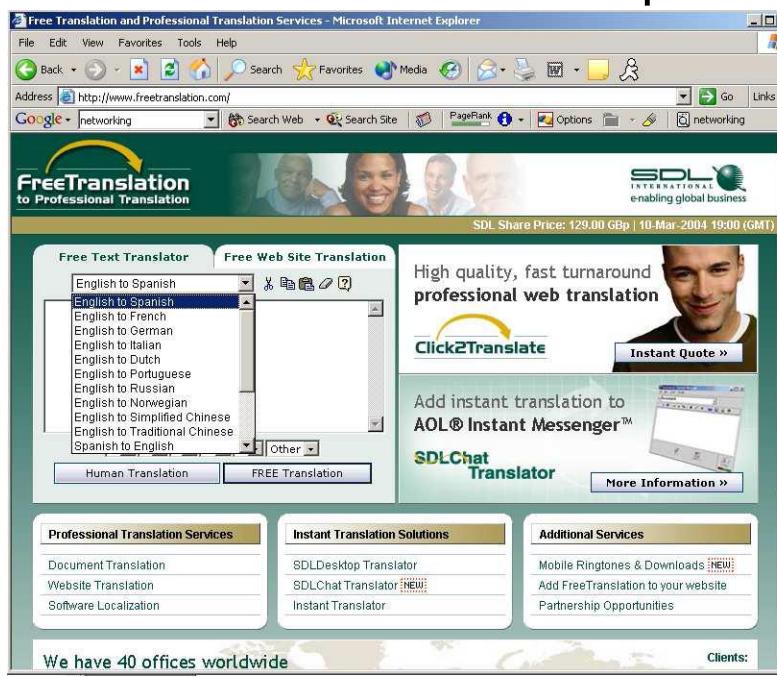
Partage des ressources :

- **Serveurs:** ordinateurs qui fournissent les ressources partagées aux utilisateurs par un serveur de réseau
- **Clients:** ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau
- **Support de connexion:** façon dont les ordinateurs sont connectés entre eux
- **Données partagées:** fichiers fournis par des serveurs de réseau
- **Imprimantes et autres périphériques partagés:** fichiers, imprimantes ou autres élément utilisés par les usagers de réseau
- **Ressources diverses:** autres ressources fournies par le serveur

# 1. Définitions et concepts de base

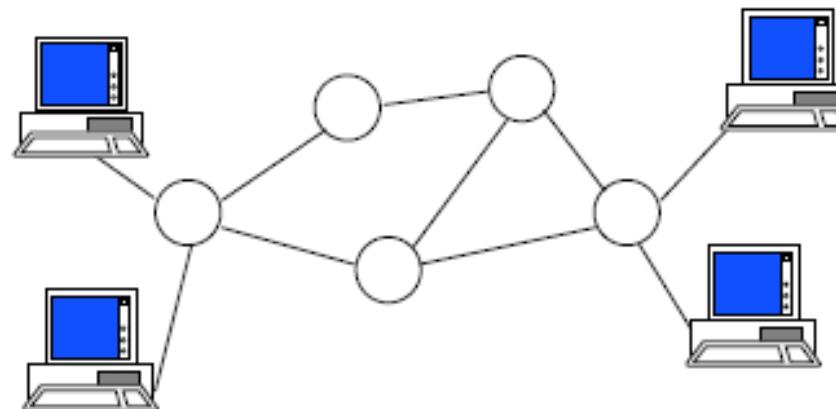
## Applications du réseaux

- Accès au World Wide Web
- Courrier électronique (mail)
- Transfert de fichiers (ftp)
- Accès à distance (telnet)
- Transfert du texte de la parole et de la vidéo



## 2. Types de réseaux

- Réseau à commutation
  - Données transférés à travers une série de nœuds intermédiaires
  - Commutation de circuit (Téléphone )
  - Commutation de paquets (Internet)

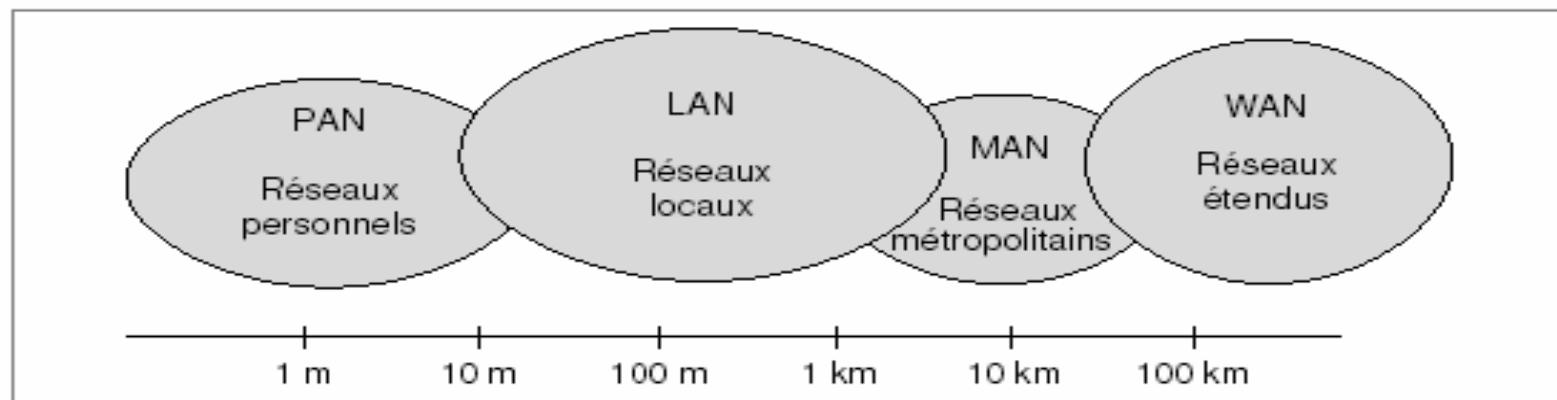


### 3. Classification des réseaux

- Nature de la liaison entre les organes connectés.
- Couverture géographique.
- Caractéristiques physiques: support, débit.
- ...

# 3. Classification des réseaux

## Couverture géographique :



PAN : Personal Area Network

LAN : Local Area Network

MAN : Metropolitan Area Network

WAN : Wide Area Network

# 3. Classification des réseaux

## Couverture géographique :

**PAN : Personal Area Network** désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Réseau individuel ou domestique.

**LAN (Local Area Network):** un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau.

Les débits sont importants (de 10 Mb/s à 1 Gb/s)

# 3. Classification des réseaux

## Couverture géographique :

**MAN (Metropolitan Area Network):** interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Le débit varie jusqu'à 100Mb/s.

**WAN (Wide Area Network):** interconnecte plusieurs MANs à travers de grandes distances géographiques.

Le débit est plus faible de 50b/s à quelques Mb/s.

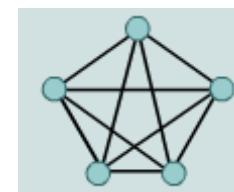
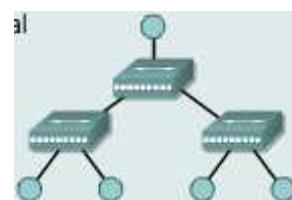
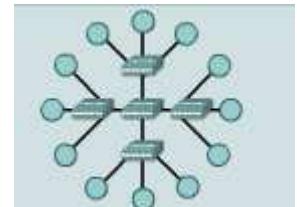
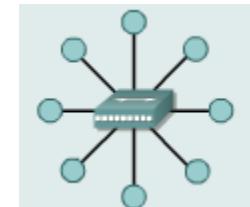
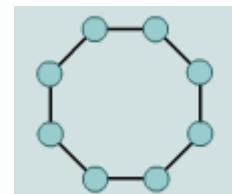
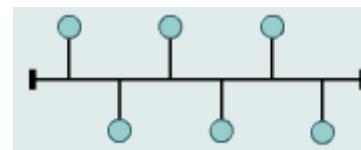
# 4. Topologie des réseaux

- Une **topologie de réseau** est une définition de l'architecture d'un réseau.
- Elle donne une certaine disposition des différents postes informatiques du réseau et une hiérarchie de ces postes.
- Il existe différents types de topologies,



# 4. Topologie des réseaux

- Topologie réseau physique
  - En bus
  - En anneau
  - En étoile
  - En étoile étendue
  - En hiérarchie
  - Maillé



# 4. Topologie des réseaux

## Notion de terminal et de nœud

- Réseau = terminaux + nœuds + liens
  - Terminaux : DTE (Data Terminal Equipment)
  - Nœuds : systèmes intermédiaires DCE (Data Communication Equipment)
  - Liens : liaisons entre DTE, DCE et DCE, DCE (cuivre, fibre, hertzien)

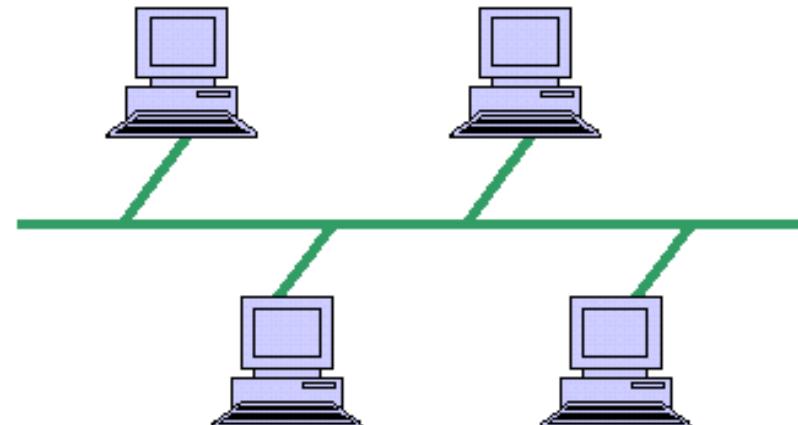
## Topologie :

- comment les nœuds sont interconnectés (physique)
- comment l'information est transmise (logique)

# 4. Topologie des réseaux

## ***Topologie en bus***

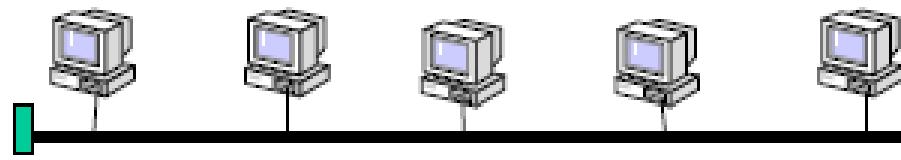
- ✓ Les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire d'un câble.
  - ✓ Une station en panne ne perturbe pas le reste du réseau.
  - ✓ Cette topologie est très facile à mettre en place.
- 
- ⌚ Elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.
  - ⌚ Faible sécurité des données.



# 4. Topologie des réseaux

## Réseaux en bus (LAN)

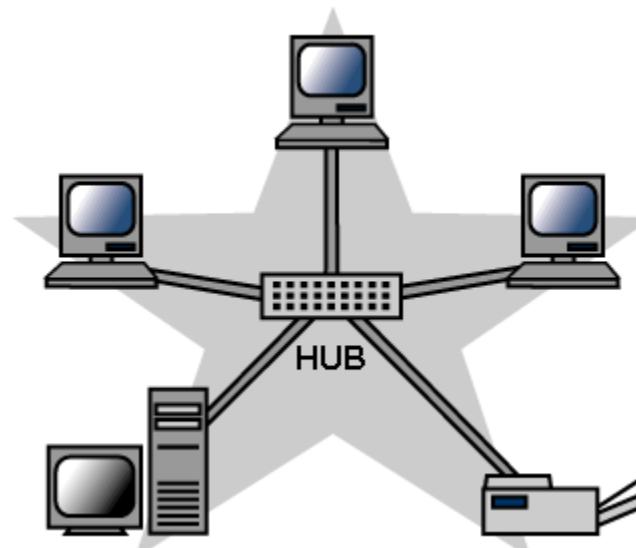
- La topologie en bus utilise un seul segment pour relier les stations.
- Diffusion (les messages sont reçus par l'ensemble des stations connectées )
- Accès direct au réseau (protocole d'accès complexe)
- Ajout et suppression de stations sans perturbation du réseau



# 4. Topologie des réseaux

## ***Topologie en étoile***

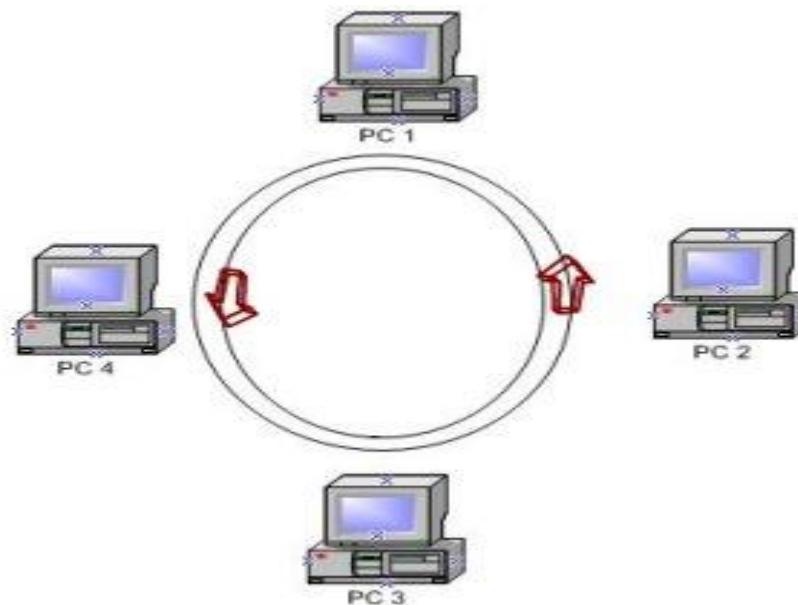
- Les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur**.
- Les topologies en étoile sont beaucoup moins vulnérables.
- ⌚ Si le concentrateur est défectueux, tout le réseau est en panne.



# 4. Topologie des réseaux

## ***Topologie en anneau***

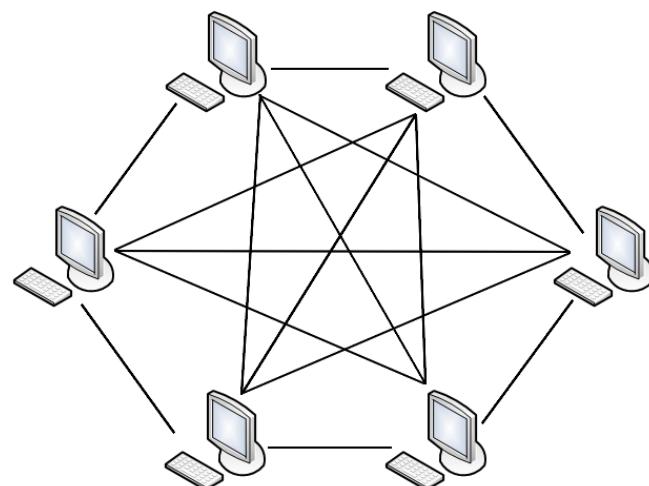
- ✓ Les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.
- ⌚ Une station en panne bloque toute la communication du réseau



# 4. Topologie des réseaux

## ***Topologie maillée***

- Une topologie maillée, est une évolution de la topologie en étoile
  - Les noeuds sont interconnectés les uns aux autres.
  - Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents noeuds.
- 
- ⌚ Le nombre de liaisons nécessaires est très élevé (en fonction du nombre de terminaux).



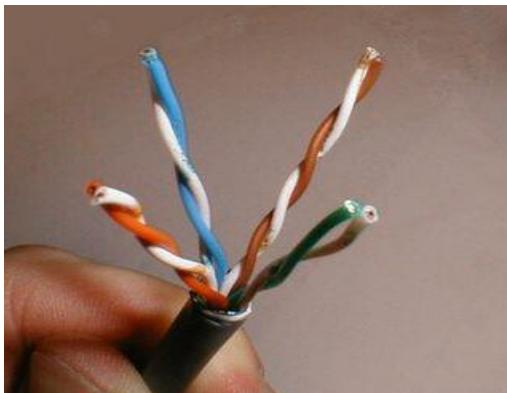
# 5. Les composantes d'un réseau

La mise en réseau nécessite donc:

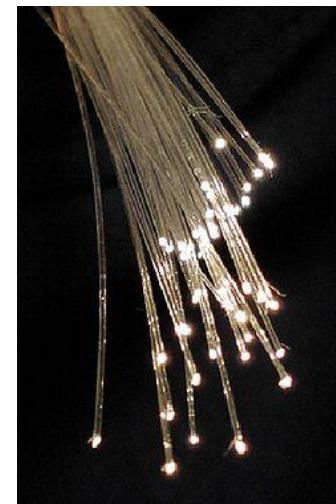
- **Les équipements terminaux** (ordinateurs, stations, serveurs, périphériques, machines hôtes, etc.)
- **Les supports de communication** (câbles, fibres, faisceaux, liaisons physiques, lignes de transmission, médium, etc.).
- **Les équipements d'interconnexion** (nœuds, routeurs, ponts, switch, passerelles, etc).

# 5. Les composantes d'un réseau

## A-Support de transmission



Paire torsadée



Fibre optique



Câble coaxial

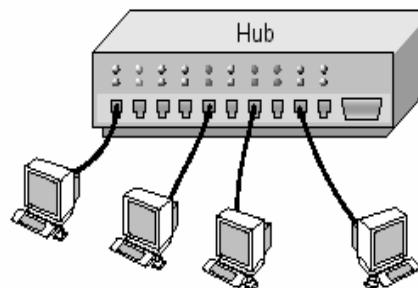
# 5. Les composantes d'un réseau

## B-Equipements d'interconnexion

### Le concentrateur:

Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux.

Son rôle c'est de prendre les données binaires parvenant d'un port et les diffuser sur l'ensembles des ports.



# 5. Les composantes d'un réseau

## B-Equipements d'interconnexion

### Le concentrateur:

Les deux types de concentrateurs existants sont décrits ci-dessous

- *Concentrateurs passifs.* Ils retransmettent directement le signal reçu au moyen de leurs ports, sans aucun traitement.
- *Concentrateurs actifs.* Parfois appelés *répéteurs multiports*, ils reçoivent des signaux entrants et les traitent avant de les retransmettre avec leur niveau et leur définition d'origine aux ordinateurs ou aux composants auxquels ils sont connectés.

# 5. Les composantes d'un réseau

## B-Equipements d'interconnexion

### Le commutateur:

Le commutateur (en anglais switch) est un élément matériel qui permet de relier plusieurs ordinateurs (machines) entre eux.

Sa seule différence avec le Hub, il est capable de connaître l'adresse physique des machines qui lui sont connectées et d'analyser les trames reçues pour les diriger vers la machine de destination.

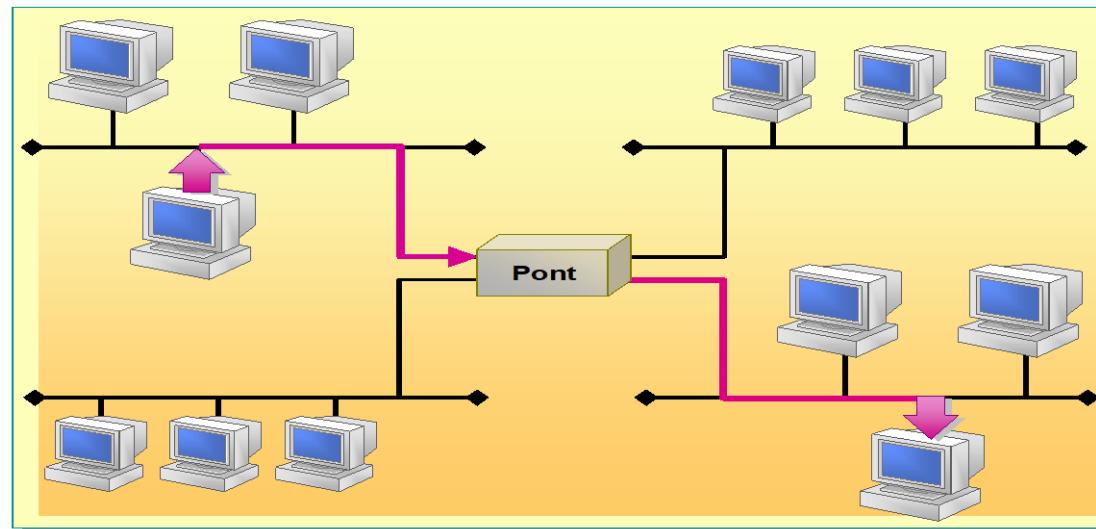


# 5. Les composantes d'un réseau

## B-Equipements d'interconnexion

### Le pont:

Un pont transmet un signal à la fois. Si un paquet est destiné à un ordinateur situé sur le segment de réseau de l'expéditeur, le pont conserve le paquet au sein de ce segment. Si le paquet est destiné à un autre segment, le pont transmet le paquet à ce segment



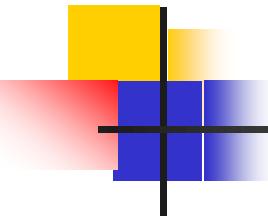
# 5. Les composantes d'un réseau

## B-Equipements d'interconnexion

### Le routeur:

Un routeur est un périphérique qui joue le rôle de pont ou de commutateur, mais qui propose un plus grand nombre de fonctionnalités. Lorsqu'il transmet des données entre différents segments du réseau, le routeur examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet

Un **routeur** est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

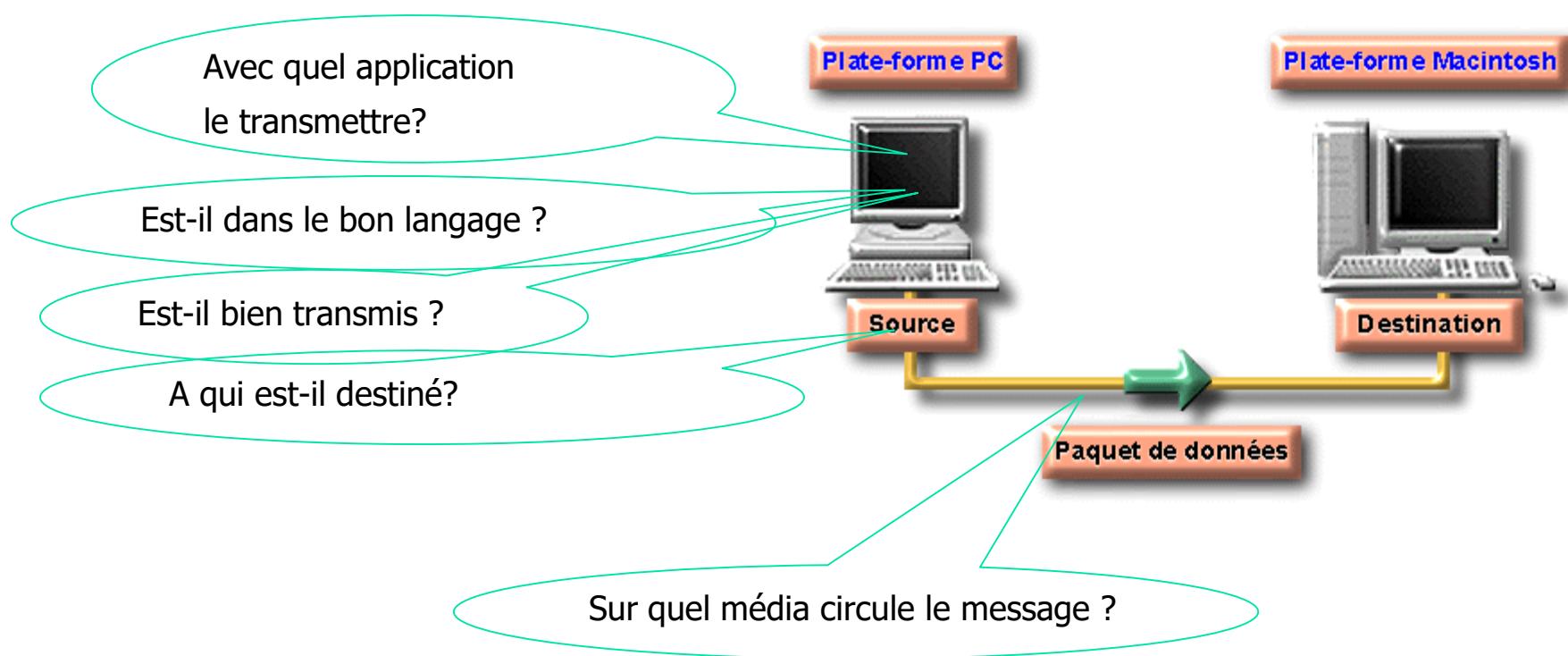


## Chapitre -2-

# Modèle de référence OSI & Architecture TCP/IP

# 1. Objectif

Structurer et décomposer les fonctions du réseau  
Séparer les traitements applicatifs et l'acheminement des données



## 2. Architecture protocolaire réseau

Architecture protocolaire réseau : un modèle complet de communication

**Objectifs :** Une cohérence parfaite entre les différentes parties du réseau. Une grande modularité, chaque partie peut être modifiée ou remplacée sans affecter les autres (conception modulaire)

**Historiquement**, chaque constructeur a créé sa propre architecture

- SNA (System Network Architecture) d'IBM
- DSA (Distributed System Architecture) de BULL

**Besoin d'un modèle normalisé**

- Pour une entreprise qui met en œuvre des réseaux, la diversité des solutions adoptées et l'hétérogénéité des équipements est une nécessité fondamentale
- Pour prendre en compte une informatique existante non encore connectée et hétérogène pour des raisons économiques ou historiques.
- Pour ne pas se limiter à un seul fournisseur.
- Pour pouvoir tirer partie de complémentarité des produits de différents constructeurs
- Pour pouvoir s'adapter au mieux à l'évolution des flux d'information à traiter dans l'entreprise.

# 3. La normalisation

« Normalisation » : ensemble de règles destinées à satisfaire un besoin de manière similaire

## Avantages :

- réduction des coûts d'études rationalisation de la fabrication
- garantie d'un marché plus vaste
- garantie d'interfonctionnement, d'indépendance vis à vis d'un fournisseur, de pérennité des investissements

modèle de référence ou modèle OSI (Open System Interconnexion) définit par l'ISO (International Standardization Organization) au début des années 80 (1983)

## Quelques Organisme de normalisation :

- I.S.O. International Standardization Organization organisation non gouvernementale, centaine de pays membres, édite des normes dans tous les domaines.
- I.E.E.E. Institute of Electrical & Electronics Engineers (USA) La plus grande organisation professionnelle et universitaire du monde, groupe de normalisation pour l'informatique (IEEE 802)
- U.I.T . Union Internationale des Télécommunications (ex CCITT) (Genève)

# 4. Interconnexion des Systèmes Ouverts

## Le Modèle en couche OSI

Le Modèle OSI (Open System Interconnexion) est inspiré des architectures réseaux comme DEC Net (Digital Equipment Corporation net ), SNA et TCP/IP.

Il a été mis au point par l'ISO en 1983 (International Standard Organisation)

Le modèle a été créé pour faciliter l'interopérabilité de systèmes informatiques différents

### Pourquoi un modèle en couche?

- Réduire la complexité de l'ensemble
- Uniformiser les interfaces entre les fonctions
- Faciliter la conception modulaire
- Assurer l'interopérabilité des technologies
- Faciliter l'évolution
- Simplifier l'enseignement et l'apprentissage

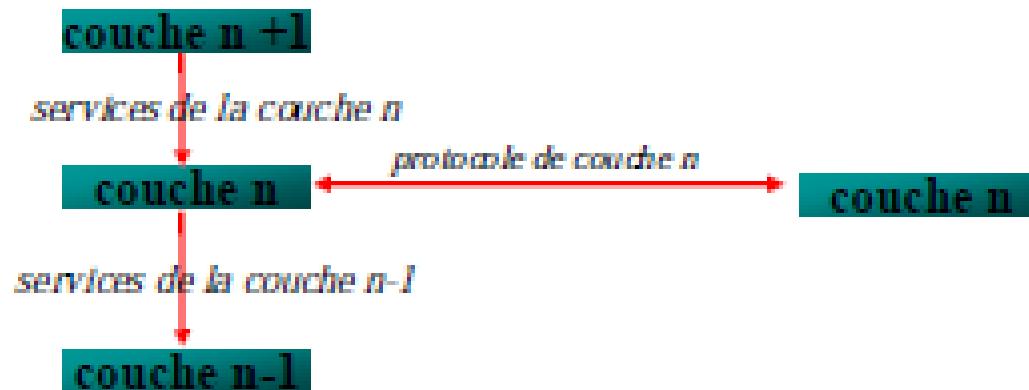


# 4. Interconnexion des Systèmes Ouverts

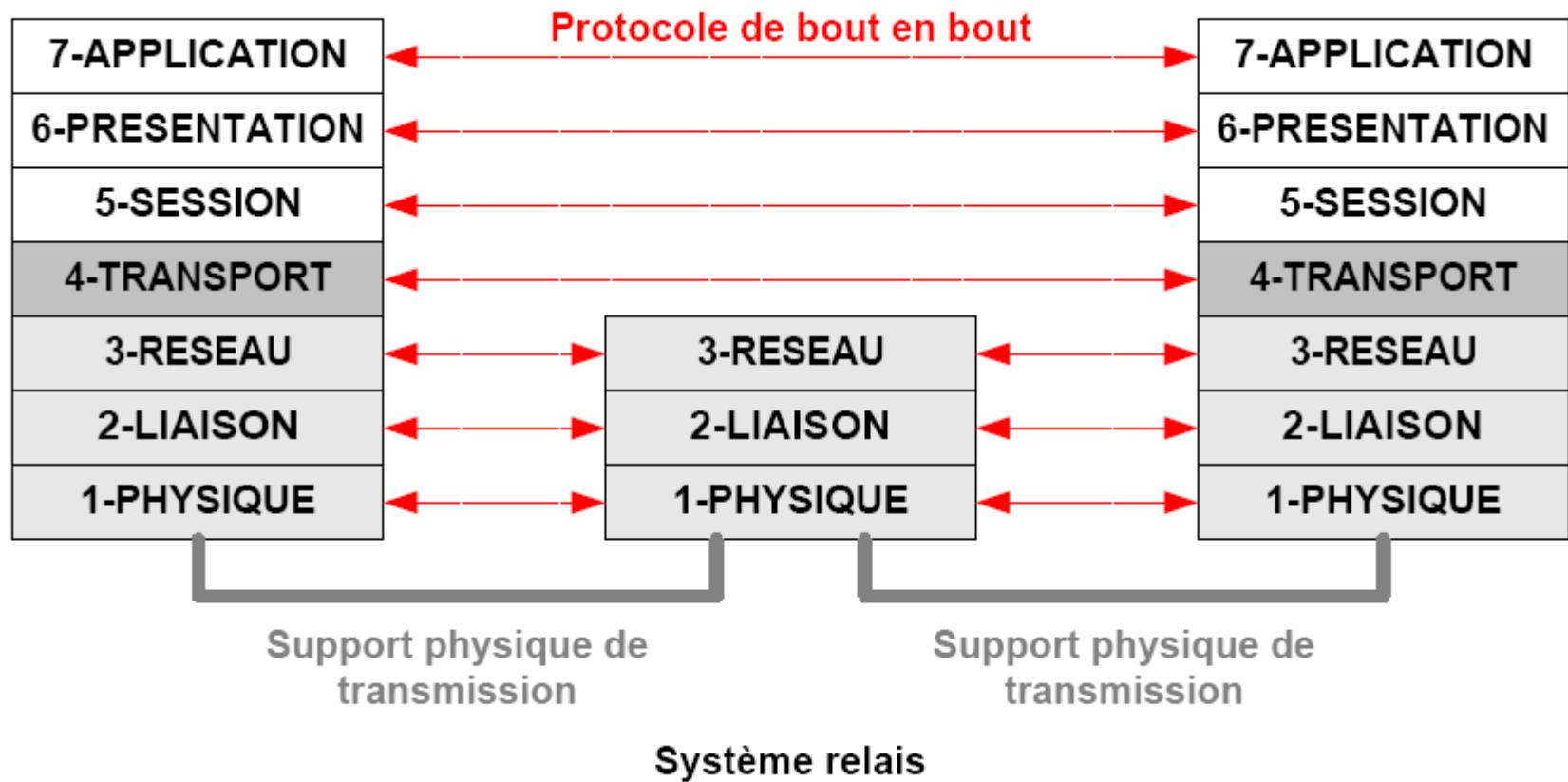
**une couche** : un ensemble homogène destiné à accomplir une tâche ou à rendre un service

Il y a 2 types de dialogue :

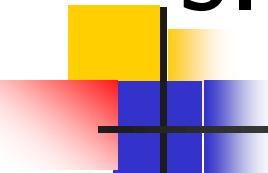
- dialogue horizontal entre couches homologues à l'aide du protocole de niveau N
- dialogue vertical à l'aide de service



# 5. Le modèle de référence - OSI



# 5. Le modèle de référence - OSI



Le modèle OSI constitue une référence, il présente 7 couches, plus de raffinement des fonctions et une conception modulaire très importante. Il présente les avantages suivants:

- Il permet de diviser les communications sur le réseau en éléments plus petits et plus gérables.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multi constructeur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Les modifications apportées à une couche n'affectent pas les autres couches.
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement

# 5. Le modèle de référence - OSI

## OSI: Couches « hôtes »

Tâche requérant des services de communication.  
Ex : FTP, le courrier électronique...

Format et structure de l'information, lisibilité  
des données pour la destination  
Ex : ASCII, EBCDIC, html, encryptions...

Paramètres de la communication : organisation,  
synchronisation et gestion du dialogue.  
Ex : Ouverture et fermeture de la session,  
autorisation, éviter de refaire les retransmissions  
à zéro en cas de panne,...

Fiabilité de l'échange de l'information,  
Segmentation, détection des pannes et  
reprise de contrôle de flux, ...  
Ex : Accusés de réception (ACK)...



# 5. Le modèle de référence - OSI

## OSI: Couches « média »

Acheminement au mieux de l'information

Ex : Adresse IP (Internet)

Ex : No. de téléphone (PSTN: Public Switched Telephone Network)

- Accès au médium de communication Ex : Ethernet

-Adresse physique du prochain nœud

-Contrôle de flux (Synchronise les débits)

Transmission binaire: Standardise les support

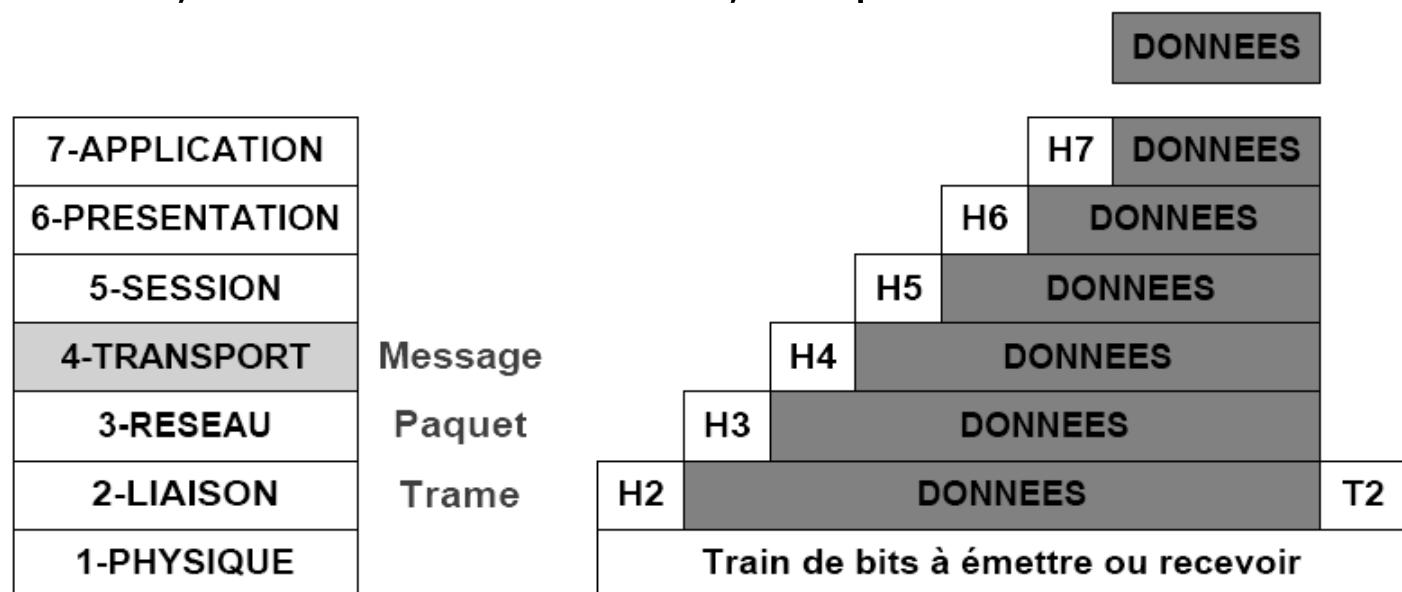
Tension (V), taux (bps), codage ...

Ex : 10BaseT, modem...



# 5. Le modèle de référence - OSI

Les données de la couche  $n+1$  sont encapsulées dans une unité de données de niveau  $n$  (en-tête couche  $n$  et données  $n+1$ ). L'en-tête contient les informations nécessaires au traitement distant sur la couche homologue (identifiant du service, adresse du destinataire, compteurs de contrôle de l'échange, ...)



La couche  $n$  ajoute l'en-tête  $H_n$  (encapsulation)

La couche liaison ajoute un champ supplémentaire  $T_2$  pour le contrôle de la transmission (FCS, Frame Check Sequence)

# 5. Le modèle de référence - OSI

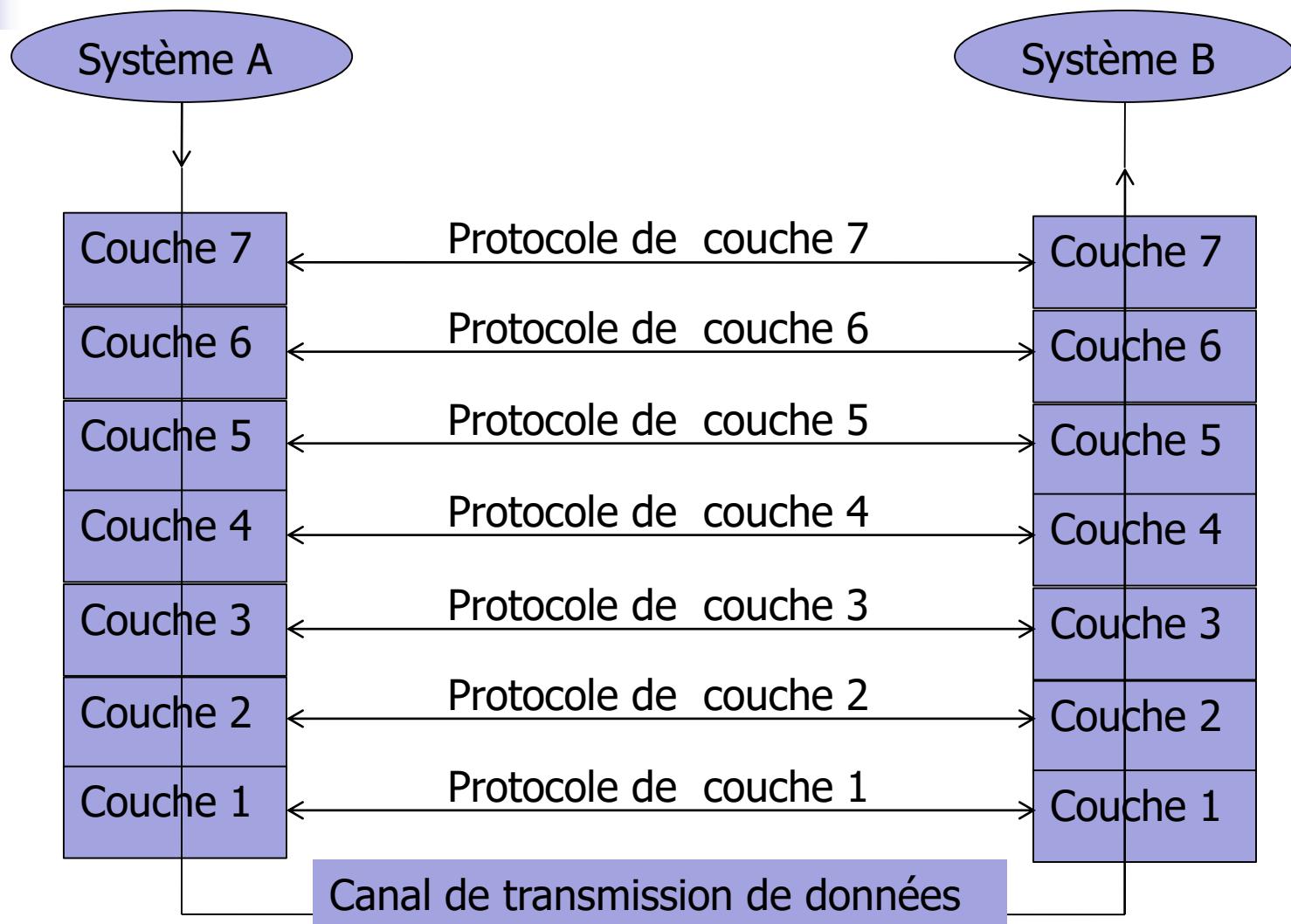
## L'encapsulation :

L'encapsulation est un processus qui consiste à ajouter des en-têtes et des en-queux de protocole déterminé avant que ces données soient transmises sur le réseau.

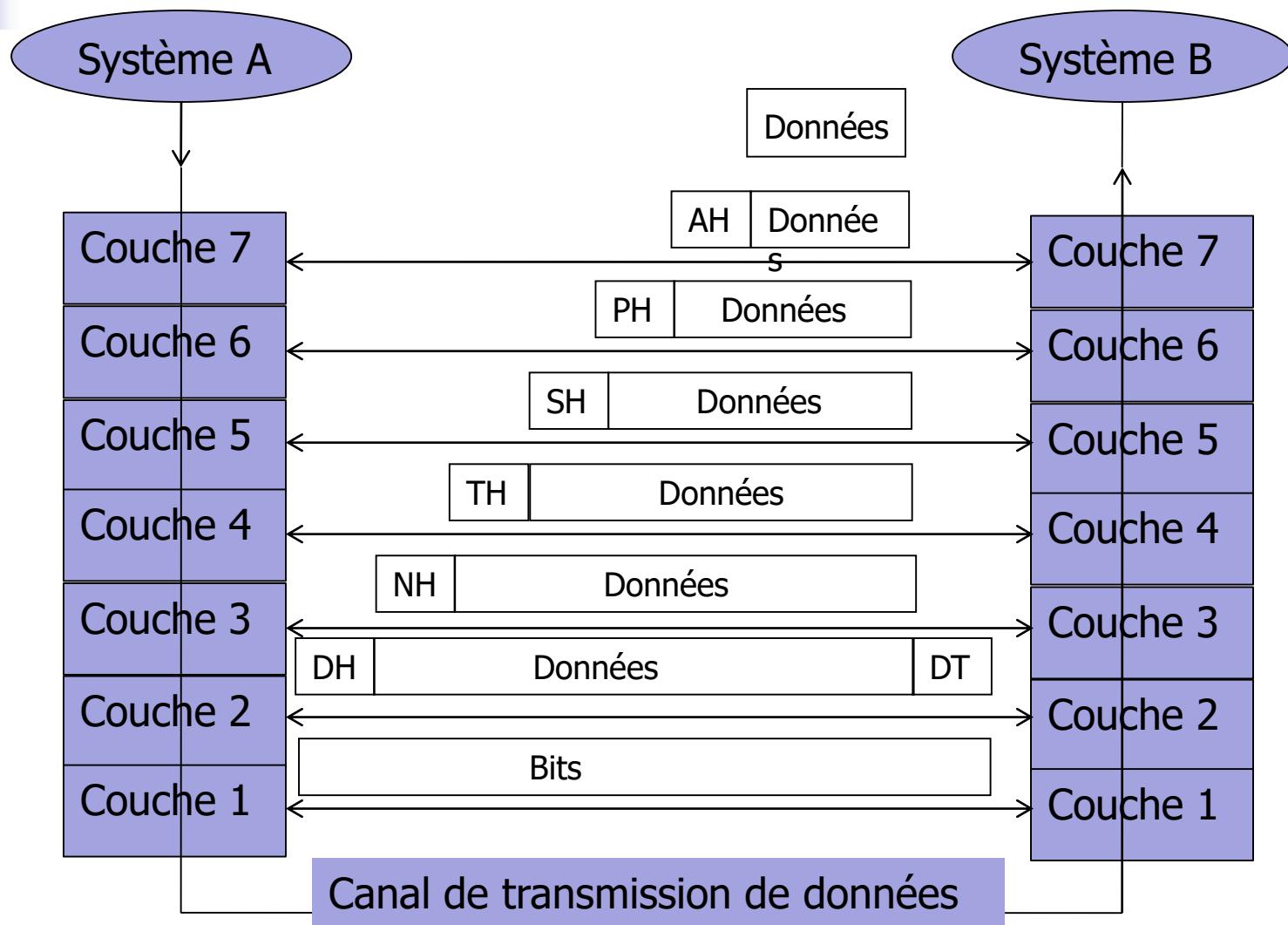
Les cinq étapes de conversion afin d'encapsuler les données:

- 1. Construction des données pouvant circuler dans l'interréseau.
- 2. Préparation des données pour le transport de bout en bout en utilisant des segments.
- 3. Ajout de l'adresse IP du réseau à l'en-tête (paquets, ou datagrammes), contenant un en-tête de paquet constitué des adresses logiques d'origine et de destination.
- 4. Ajout de l'en-tête et de l'en-queue de la couche de liaison de données : placer le paquet dans une trame.
- 5. Conversion en bits pour la transmission pour la transmission sur le média.

# 5. Le modèle de référence - OSI



# 5. Le modèle de référence - OSI



# 5. Le modèle de référence - OSI

- La couche Application:

- C'est le programme qui gère l'application proprement dite,
- Exp: ftp : prendre le fichier sur le disque local et le passer au «réseau»

- La couche Présentation:

- Mise en forme et représentation des informations,
- Exp: cryptage, représentation des données entiers, compression des images,

- La couche Session:

- Gestion du dialogue,
- Exp: synchronisation d'un dialogue (à qui le tour de parler)

Elles sont réunies la plupart du temps en une seule couche : application

# 5. Le modèle de référence - OSI

- La couche Transport:

- Etablissement et rupture des connexions multiples,
- Dialogue de bout en bout( en ne s'occupe pas des nœuds intermédiaires)
- Découpage des message :segmentation / réassemblage
- Contrôle de flux
- Contrôle de congestion

- La couche Réseau:

- Routage et adressage des paquets à travers le réseau
- Segmentation / réassemblage
- Contrôle de congestion

# 5. Le modèle de référence - OSI

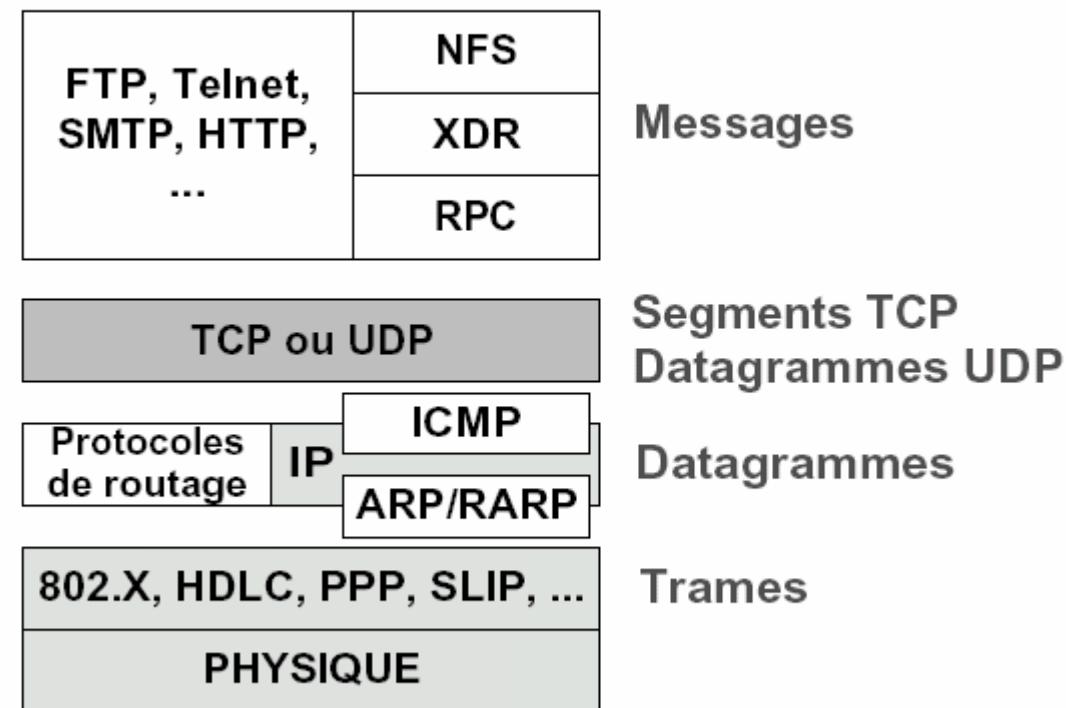
- La couche Liaison des données :
  - La mise en trame de l'information,
  - La détection et la correction des erreurs
  - Le contrôle de flux visant à asservir la vitesse de l'émetteur à celle du récepteur
- Sous couche liaison de données: le partage des voies physiques à diffusion
  - le partage des voies physiques à diffusion (très utilisé dans les réseaux locaux) MAC: Medium Access Control
  - Illustration détaillé: le protocole Ethernet
- La couche Physique:
  - Principales caractéristiques des voies physiques,
  - Passage de l'information binaire aux ondes électriques, ondes lumineuses, ondes radio, ...
  - Traitement du signal ( Modulation, démodulation, ...)

# 6. Modèle OSI et Architecture TCP/IP

## Architecture OSI

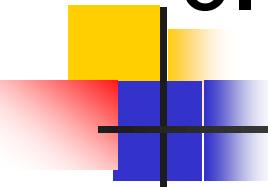


## Architecture TCP/IP



En comparant le modèle OSI au modèle TCP/IP, vous remarquerez des similitudes et des différences.

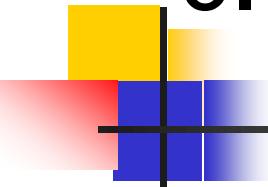
# 6. Modèle OSI et Architecture TCP/IP



Les similitudes sont les suivantes:

- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services très différents.
- Tous deux comportent des couches réseau et transport comparables.
- Les professionnels des réseaux doivent connaître ces deux modèles.
- Tous deux supposent que les paquets sont commutés. Cela signifie que chaque paquet peut prendre des chemins différents pour atteindre une même destination. Cela est différent des réseaux à commutation de circuits, où tous les paquets prennent le même chemin.

# 6. Modèle OSI et Architecture TCP/IP



Les différences sont les suivantes:

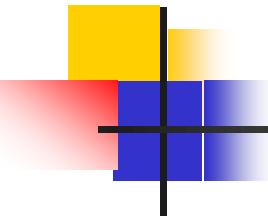
- TCP/IP intègre la couche présentation et la couche session dans sa couche application.
- TCP/IP regroupe la couche physique et la couche liaison de données du modèle OSI dans la couche d'accès réseau.
- TCP/IP paraît plus simple, car il comporte moins de couches.
- Les protocoles TCP/IP constituent la norme sur laquelle s'est développé Internet. Aussi, le modèle TCP/IP a-t-il bâti sa réputation sur ses protocoles. En revanche, les réseaux ne sont généralement pas architecturés autour du protocole OSI, même si le modèle OSI puisse être utilisé comme guide.

# 6. Modèle OSI et Architecture TCP/IP

## Choix du modèle OSI

Bien que les protocoles TCP/IP constituent les normes sur lesquelles repose Internet, le modèle OSI a été choisi pour les raisons suivantes dans le cadre de ce cursus:

- Il s'agit d'une norme générique et indépendante du protocole.
- Ce modèle comporte davantage de détails, ce qui le rend plus utile pour l'enseignement et l'étude.
- Cette richesse de détails peut également s'avérer fort utile au moment du dépannage.



## **Chapitre -3-**

# **Systèmes et Supports de transmission de données**

Modèle général d'un Système de transmission

Le codage et la transmission de l'information

La transmission en bande de base

La Modulation (la transmission large bande)

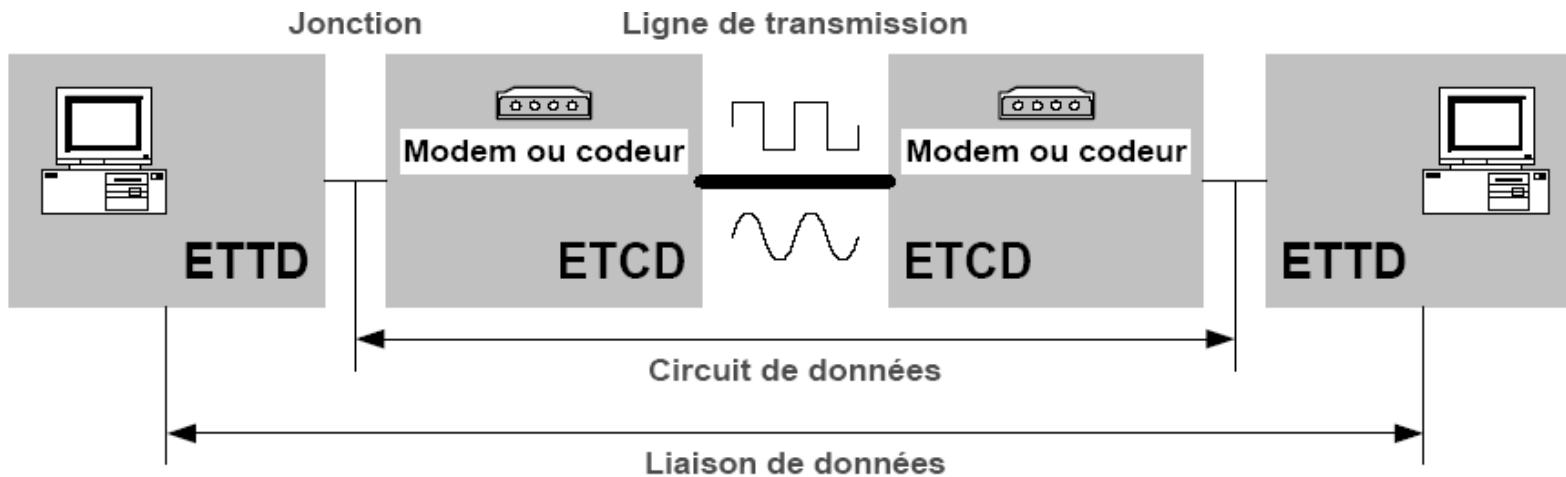
Le multiplexage

La modulation ADSL

Les supports de transmission

Les modes de transmission

# 1. Modèle général d'un Système de transmission



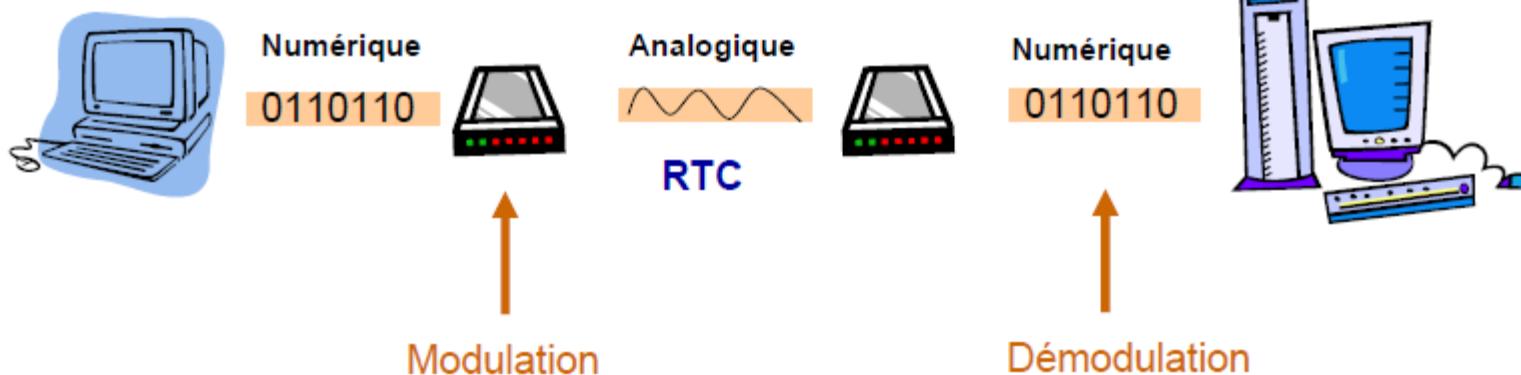
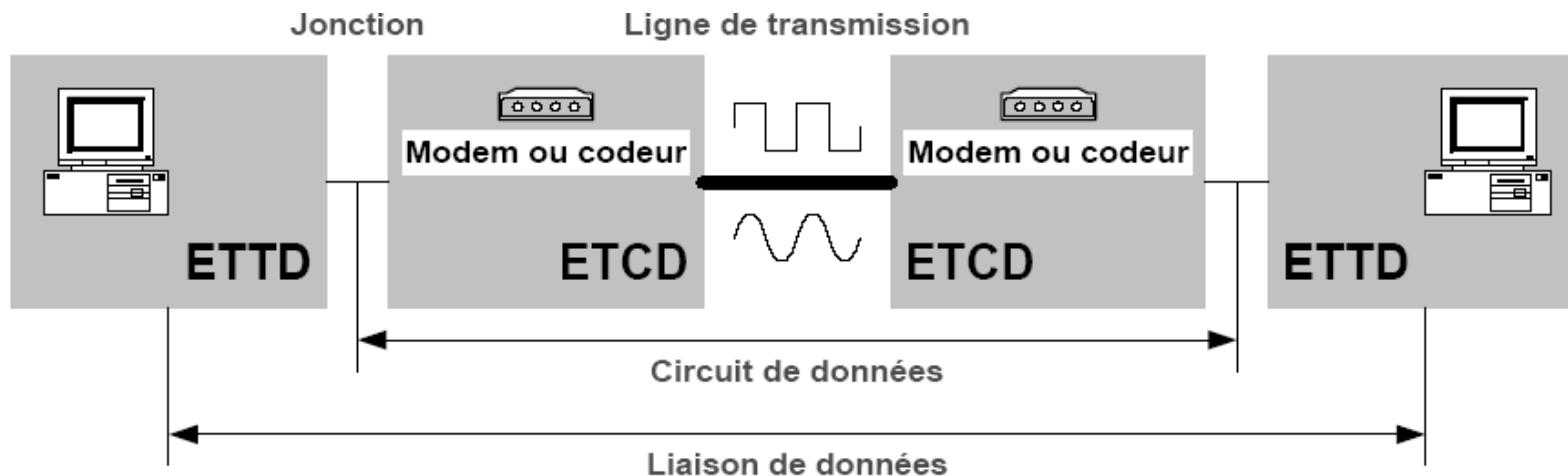
**ETTD** : Equipement Terminal de Traitement de Données

- contrôle de la communication source/collecteur des données

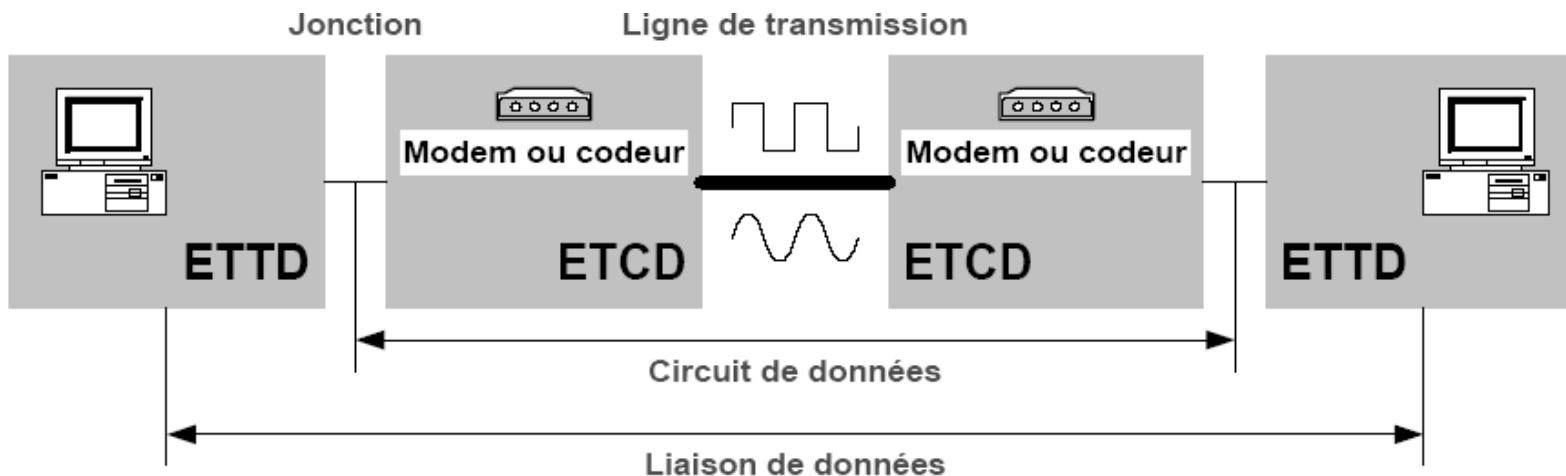
**ETCD** : Equipement Terminal de Circuit de Données

- adaptation entre le terminal et le support
- fournit au support un signal adapté à ses caractéristiques (une onde électrique, lumineuse, acoustique, électromagnétique, ...)

# 1. Modèle général d'un Système de transmission



# 1. Modèle général d'un Système de transmission



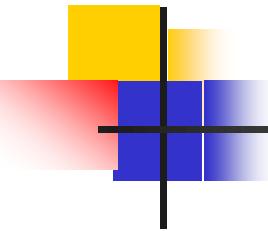
## Jonction ou interface :

- permet à l'ETTD de piloter l'ETCD pour établissement et libération du circuit, échange de données, ...
- signal numérique

## Support ou ligne de transmission :

- transmission d'une onde lumineuse, acoustique, électromagnétique ou électrique sur **un supports optiques, aériens, filaires**
- caractéristiques physiques de la ligne (débit, taux d'erreurs, ...)

# 2. Le codage de l'information



Deux étapes:

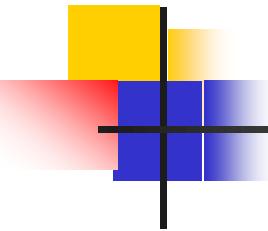
- Codage des informations

- Information discrète: Code ASCII (7 bits), EBCDIC (8 bits), Unicode (16bits)
- Informations continue: échantillonnage, quantification, codage

- Transmission des informations

- Bande de base
- Modulation (large bande)

## 2. Le codage de l'information



On traite souvent deux types d'information

### Données continues analogique

- Données continues résultant de la variation continue d'un phénomène physique ( voix, température, image, tension, courant, lumière ....)
- Une infinité de valeurs dans un intervalle borné
- un capteur fournit une tension électrique proportionnelle à l'amplitude du phénomène.

### Données discrètes numérique

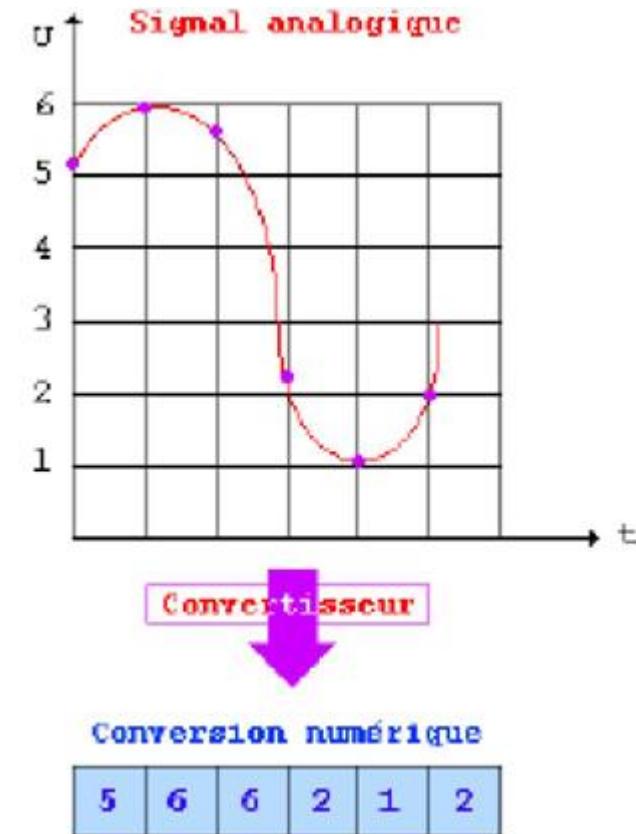
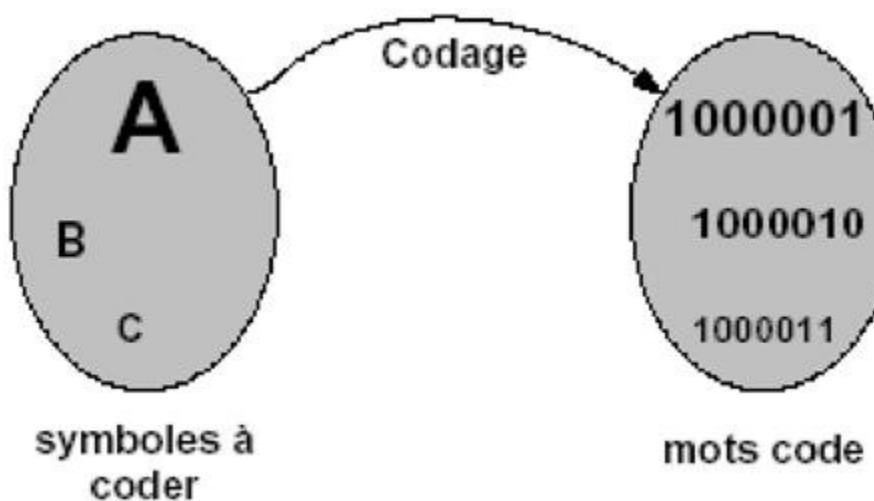
- Suite discontinue de valeurs dénombrable
- Un texte est une association de mots eux-mêmes composés de lettre (symbole élémentaires)
- Une image numérique est un ensemble de pixel qui prennent des valeurs discrètes

## 2. Le codage de l'information

### Traitement informatique

- Il faut associer une valeur binaire à chaque élément d'information:

- Numérisation de l'information analogique (échantillonnage et quantification)
- Codage de l'information pour des données discrètes (code ASCII, ..)



# 3. La transmission de l'information

**Problème:**

Comment l'émetteur peut-il envoyer un signal que le récepteur reconnaîtra comme étant '0' ou '1'

**Solutions:**

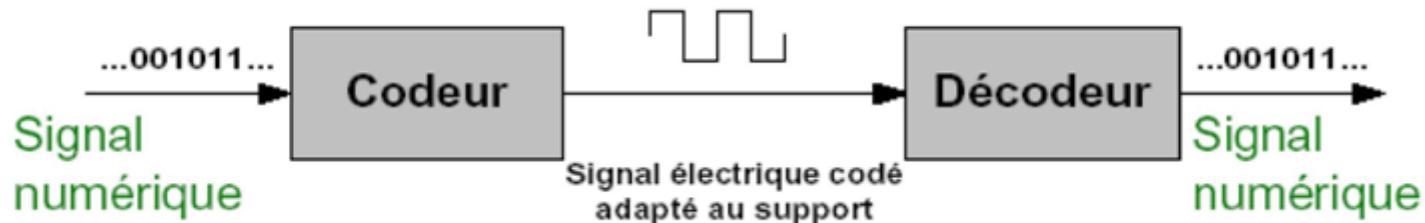
Transmission en bande de base

Transmission par modulation

# 3.1 Transmission en bande de base

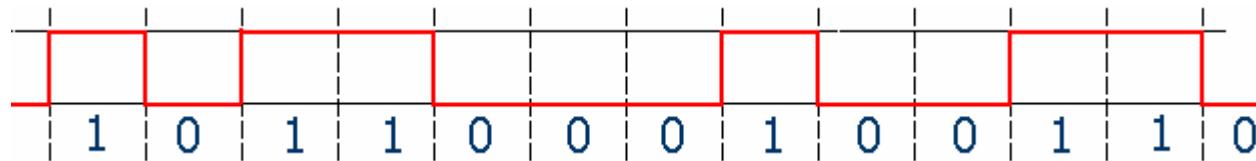
On transmet directement l'information binaire à l'aide de signaux pouvant prendre n valeurs (n est appelé la valence)

- Exemple: valence de 2 → 0 et 1 volt sur un support métallique
- Simplicité du codage mais distances limitées à quelques kilomètres
- Occupe toute la bande passante (pas de multiplexage)
- Exemple de codage en bande de base : code Tout ou Rien, code NRZ, code Manchester, ...



# 3.1 Transmission en bande de base

Soit la suite de bits (à transmettre) suivante : 1011000100110 la représentation sous la forme d'un signal électrique est donnée par la figure suivante :



Codage avec Retour à Zéro (Tout ou Rien)

Le codeur transforme la suite de bits  $\{a_i\}$  en une suite de signaux électriques  $\{d_i\}$  (2 niveaux 0V ou 5V). Les  $d_i$  ont tous la même durée  $T$  (période d'échantillonnage calculée à partir d'une horloge).

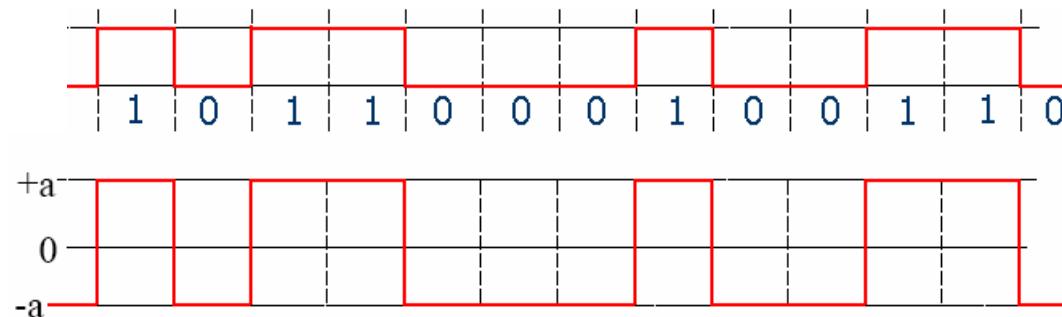
Si le signal comporte de longues suites de bits identiques, il peut se poser des problèmes d'horloge du côté du récepteur. En effet, le récepteur a un organe de décodage utilisant un échantillonneur. Pour bien fonctionner, l'échantillonneur doit connaître la période d'échantillonnage avec précision.

# 3.1 Transmission en bande de base

On utilise alors des codes qui permettent de calculer la période de l'horloge T a partir des transitions du signal. (exemples : codage NRZ, Manchester, ...)

## Codage NRZ (Non Return to Zero)

- Les niveaux '0' sont codés par une tension  $-a$
- Les niveaux '1' sont codés par une tension  $+a$ :

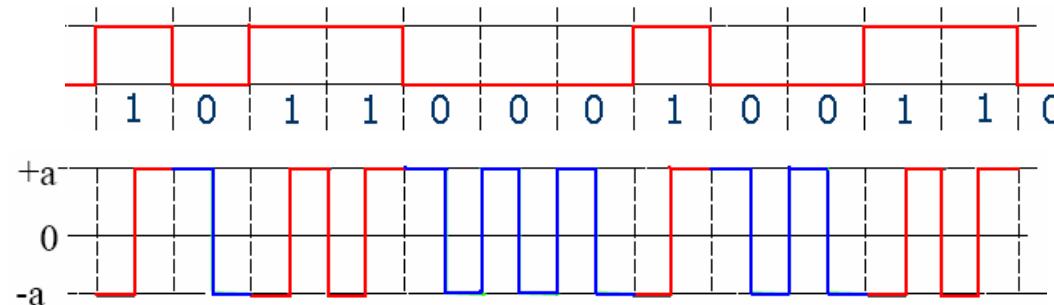


# 3.1 Transmission en bande de base

## Codage Manchester biphasé

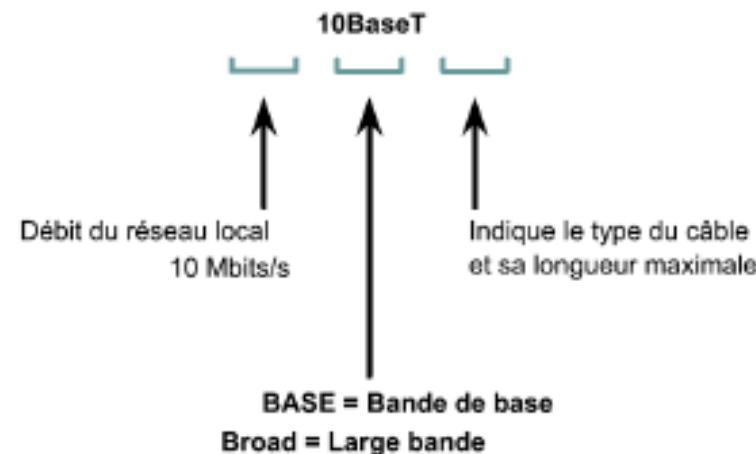
Le niveau logique '0' provoque le passage de  $+a$  à  $-a$  au milieu du moment élémentaire

Le niveau logique '1' provoque le passage de  $-a$  à  $+a$  au milieu du moment élémentaire



# 3.1 Transmission en bande de base

## Spécifications des câbles



# 3.1 Transmission en bande de base

## Problèmes des Signaux en bande de base:

- Dégradation rapide au fur et à mesure de la distance parcourue.
- Si le signal n'est pas régénéré très souvent, il prend une forme quelconque que le récepteur est incapable de comprendre.

## Solution (Modulation)

Si distance ( $>5\text{km}$ ) on utilise plutôt un signal sous forme sinusoïdal. Ce type de signal même affaibli, peut très bien être décodé par le récepteur

- Modulation de fréquences
- Modulation d'amplitudes
- Modulation de phases

## Les Modems

Transformer les signaux binaires de base en signaux analogiques sous forme sinusoïdale.

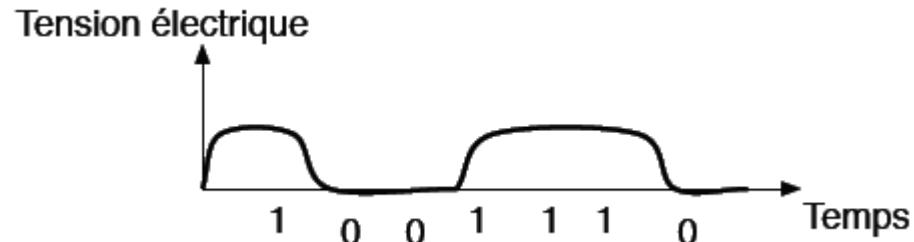
## 3.2 Passage de l'information binaire à une onde

70

La transmission de données sur un support physique se fait par propagation d'un phénomène vibratoire. Il en résulte un signal ondulatoire dépendant de la grandeur physique que l'on fait varier:

- dans le cas de la lumière il s'agit d'une onde lumineuse
- dans le cas du son il s'agit d'une onde acoustique
- dans le cas de la tension ou de l'intensité d'un courant électrique il s'agit d'une onde électrique

Exemple :

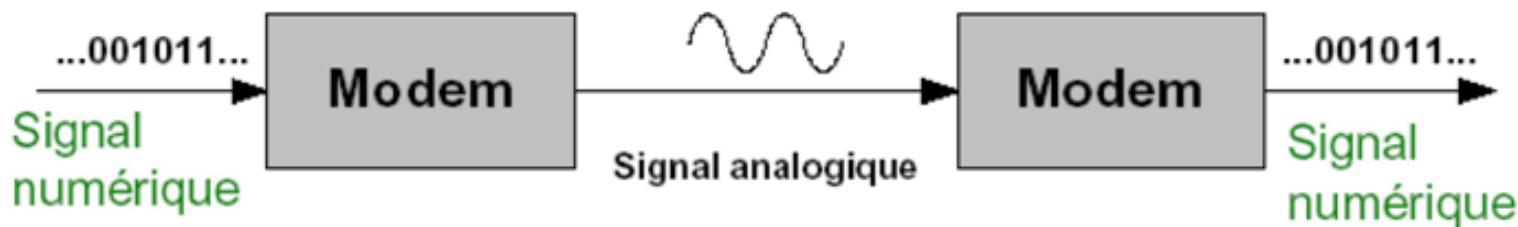


- Une onde possède une vitesse qui dépend du support
- Le temps de propagation dépend de la vitesse V de l'onde et la longueur L du support :  $T=L/V$
- Le débit d'une ligne est défini par le nombre de bits émis par seconde sur le support
- **Débit** et **vitesse** sont complètement indépendants

## 3.2 Transmission large bande (modulation)

La modulation utilise la théorie de Fourier sur la décomposition d'un signal périodique adaptée aux longues distances (transposition dans un domaine de fréquences adapté au support, protection du bruit)

- L'information codée sert à modifier un ou plusieurs des paramètres (amplitude, fréquence, phase) d'un signal sinusoïdal appelé onde porteuse utilisée sur les lignes téléphoniques à travers les Modems (Modulateur/démodulateur)
- Résout le problème du multiplexage
- Plus adapté pour des supports à forte atténuation (moyenne distance)



## 3.2 Transmission large bande (modulation)

Transmission avec modulation d'une onde porteuse

- pour s'adapter à une bande passante
- pour multiplexer des voies de transmission
- pour s'affranchir des zones et des effets de bruit
- pour augmenter le débit en bits/s
- Pour permettre la transmission longue distance, on module une onde porteuse sinusoïdale.

Mathématiquement, elle est de la forme :

$$s(t) = A \cdot \sin(\omega t + \phi) \text{ ou } s(t) = A \cdot \sin(2\pi f t + \phi)$$

A : Amplitude, f : Fréquence,  $\omega$  : Pulsation,  $\phi$  : Phase initiale

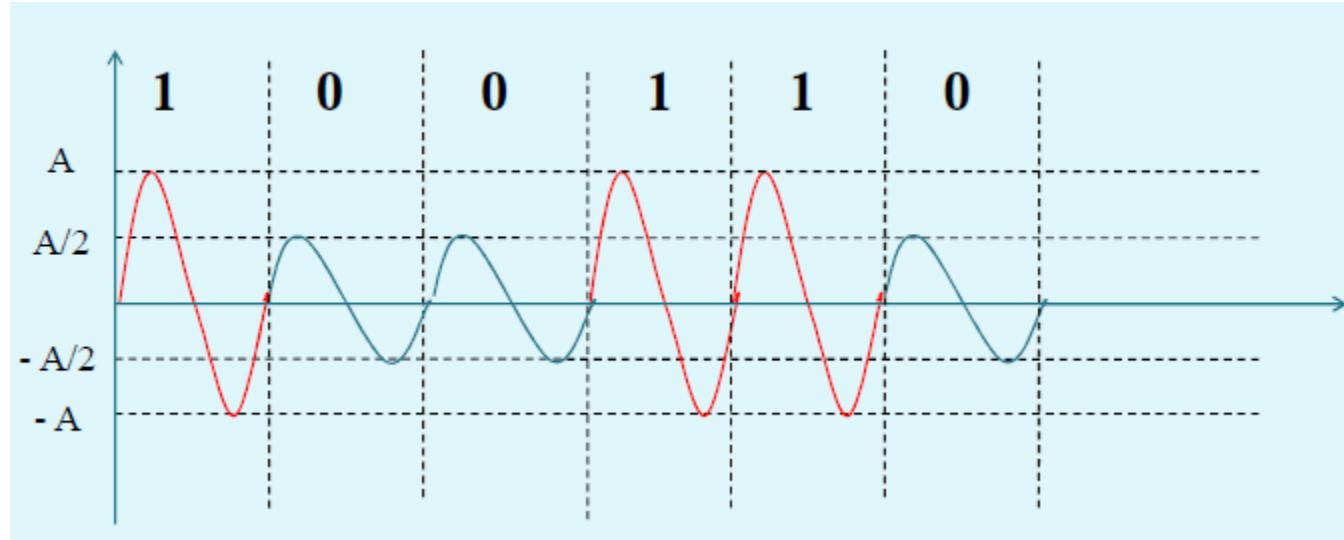
Trois techniques de modulation sont envisageables, selon la caractéristique de la porteuse qui sera modulée: modulation d'amplitude, de fréquence ou de phase.

## 3.2 Transmission large bande (modulation)

Modulation d'amplitude :  $s(t) = A(t) \cdot \sin(2\pi f t + \phi)$

Le signal est modulé en faisant varier l'amplitude

- Une valeur  $V_l$  pour un niveau logique '0' .
- Une valeur  $V_h$  pour un niveau logique '1'.



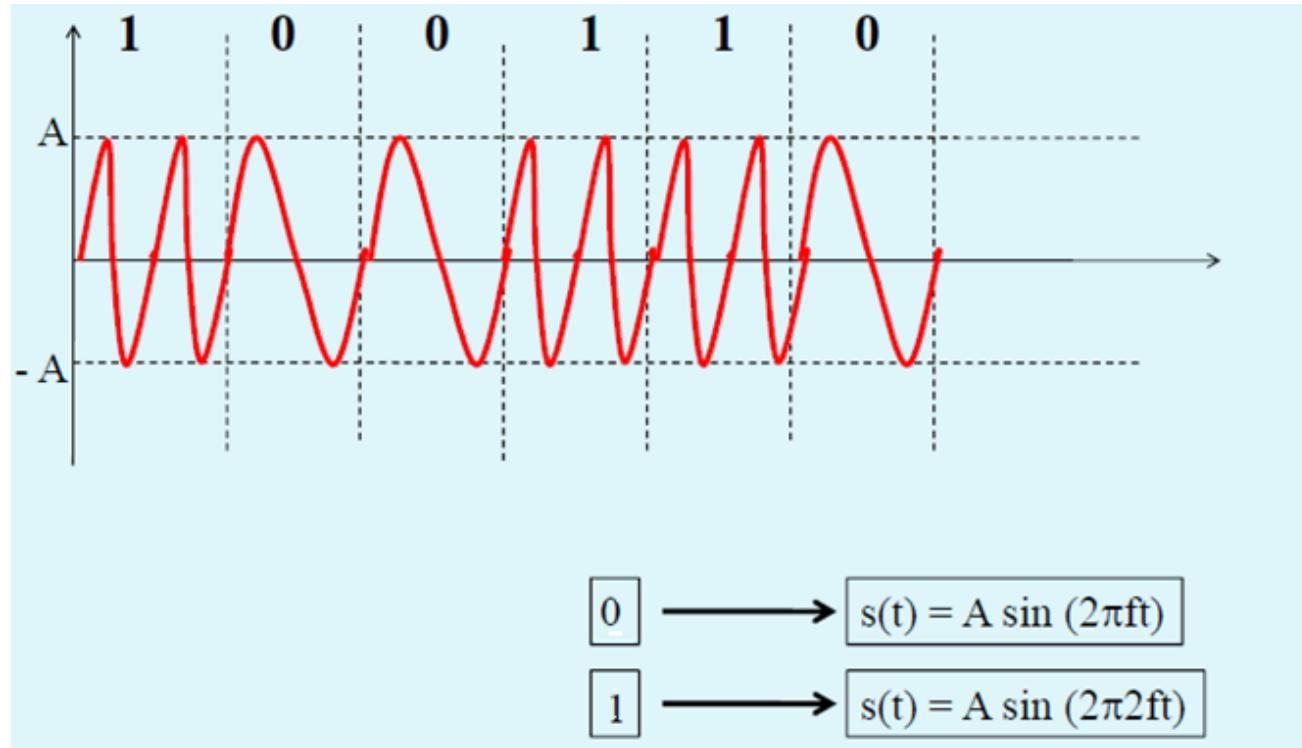
Exemple de Modulation en amplitude à deux niveaux 0 et 1

## 3.2 Transmission large bande (modulation)

Modulation de fréquence :  $s(t) = A \cdot \sin(2\pi f(t).t + \phi)$

Le signal est modulé en faisant varier la fréquence

- une valeur  $f_0$  pour un niveau logique '0'.
- une valeur  $f_1$  pour un niveau logique '1'.

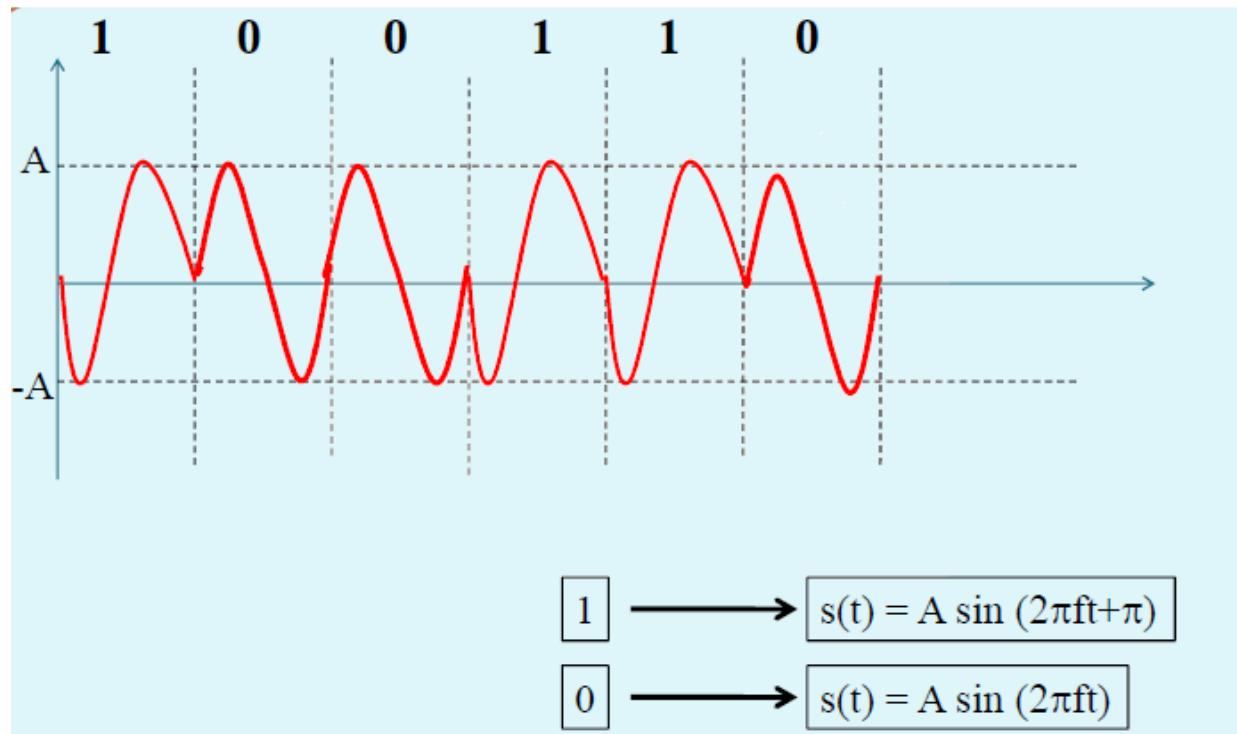


## 3.2 Transmission large bande (modulation)

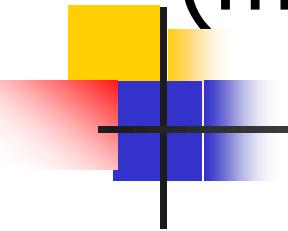
Modulation de phase :  $s(t) = A \cdot \sin(2 \pi f.t + \Phi(t))$

Cette modulation est obtenue en jouant sur la valeur de  $\Phi$

- une valeur  $\Phi_0$  pour un niveau logique '0'.
- une valeur  $\Phi_1$  pour un niveau logique '1'.



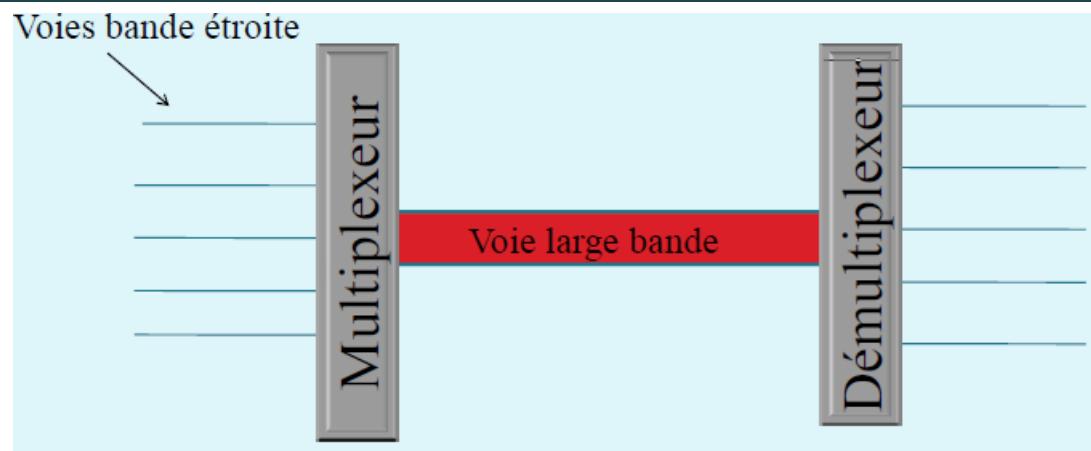
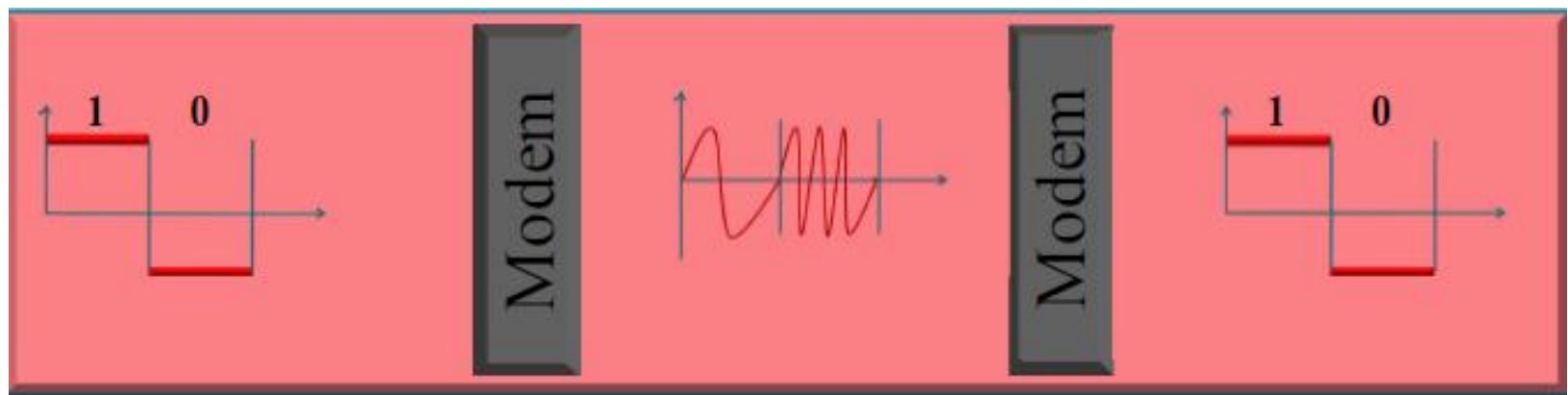
## 3.2 Transmission large bande (modulation)



Ces types de modulation servent essentiellement à la transmission des données sur des lignes téléphoniques ou par voies hertziennes. Les organes de conversion de signaux numériques-analogiques (Les «modems») utilisent l'une ou l'autre des ces modulations ou encore la combinaison de trois modulations, selon le type de support et le débit binaire choisi. Les modulations retenues sont précisées par des recommandations du CCITT.

## 3.2 Modulation - Multiplexage

La modulation concerne l' adaptation du signal au canal  
Le multiplexage concerne le partage de la bande passante du canal



# 4. Le multiplexage

Fonction de multiplexage d'une liaison:

-Partage d'une même liaison entre plusieurs communications simultanées.

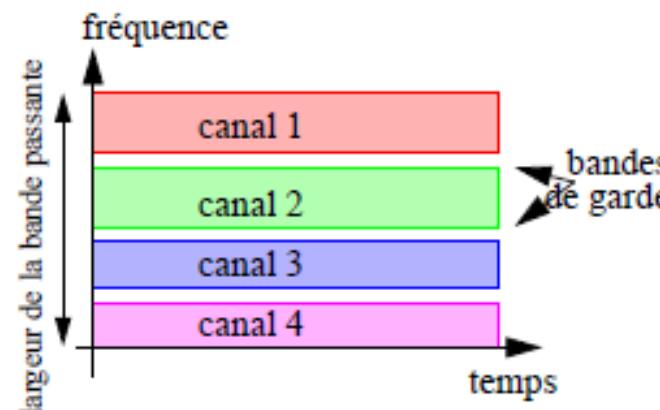
Deux types de multiplexage :

**Multiplexage fréquentiel (FDMA : "Frequency division multiple access") :**

Principe

Découpe la bande passante (large) en plusieurs sous bande (étroite).

Chaque sous bande est affectée à une voie de transmission. Cette répartition en fréquence est bien adaptée aux transmissions analogiques.



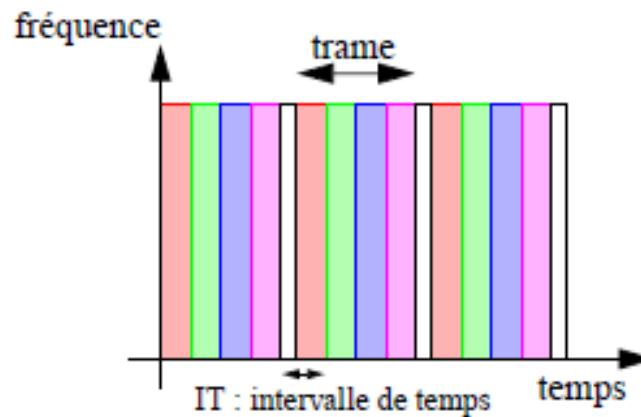
# 4. Le multiplexage

Multiplexage temporel (TDMA : "Time division multiple access"):

Principe

Des bits (ou des octets) sont prélevés successivement sur les différentes voies reliées au multiplexeur pour construire un train de bits (ou d'octets) qui constituera le signal composite.

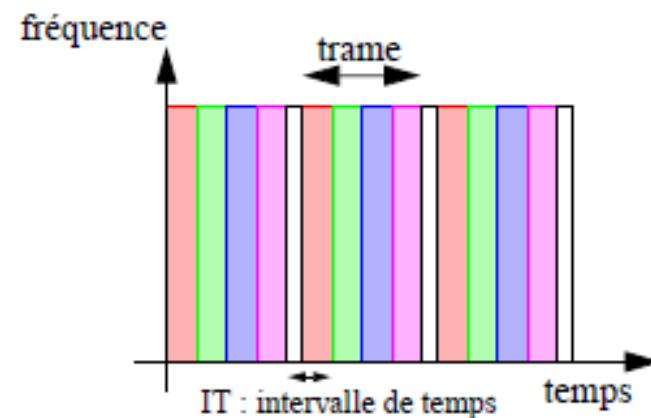
A chaque voie est affecté un intervalle de temps (IT), intervalle pendant lequel elle envoie. Cette répartition en temps est uniquement adaptée pour les données numériques.



# 4. Le multiplexage

Le multiplexage temporel est plus efficace puisqu'il fait une meilleure utilisation de la bande passante

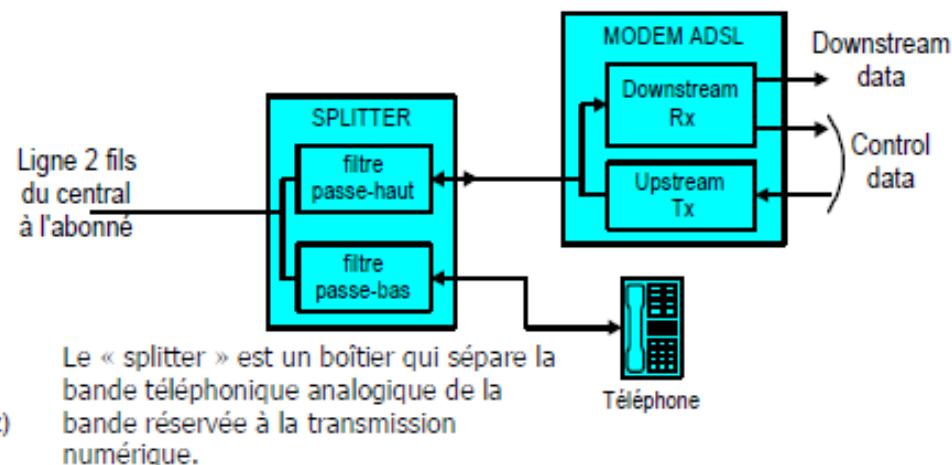
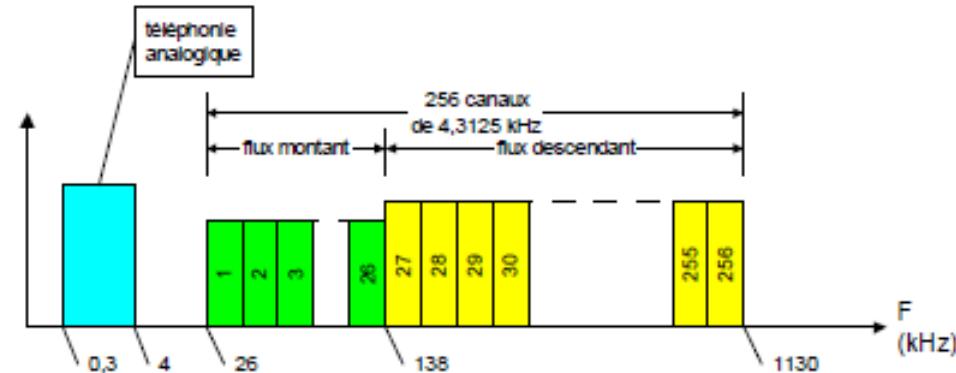
**Problème-** Des données sont prêtes sur une voie, mais ce n'est pas son tour? Il faut donc mémoriser ces données en attendant son tour!  
Attente peut être lente!! Multiplexeur doit avoir donc une mémoire tampon!!



# 5. Modulation ADSL

## Modulation ADSL (Asymmetric Digital Subscriber Line)

- Elle est utilisée sur les lignes téléphoniques avec une bande passante de 1MHz
- 3 plages de fréquences indépendantes :
  - Voie téléphonique ordinaire: Bande de 0 à 4 KHz
  - En émission numérique : Bande de 4 KHz à 50 KHz
  - En réception numérique : Bande de 50 KHz à 1 MHz



# 5. Modulation ADSL

En émission et réception : Multiplexage en fréquence sur des canaux de 4 KHz et utilisation des techniques des anciens modems sur chaque canal

- Aujourd'hui : offre théorique jusqu'à 20 Mbits/s en réception et jusqu'à 1 Mbit/s en émission.
- Possibilité de téléphoner tout en surfant sur le Web (impossible avec les modems standards)

La bande passante effective (montante et descendante) dépend de plusieurs paramètres

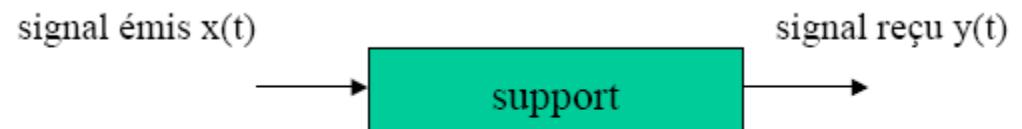
- Distance entre les modems
- Degré d'interférence électrique

Sans interférence :

- Débit descendant :
  - 8 Mbps si distance < 3 km
  - 2 Mbps si distance = 6 km
- Débit montant :
  - entre 16 Kbps et 1 Mbps

# 6. Les supports de transmission

## Défauts du support



**MAIS**, en fait il y a :

- Affaiblissement du signal en amplitude
- Bruits impulsifs : interférences entre signaux, diaphonie

**-CONSEQUENCES :**

- Affaiblissement => le support se comporte comme un filtre et ne laisse pas passer toutes les fréquences
- bruits => erreurs de transmission

Bandé Passante (Hz) : Caractérise tout support de transmission, c'est la bande de fréquences dans laquelle les signaux sont correctement reçus

- BW = Fmax - Fmin
- L'oreille humaine est sensible dans la bande 15-15000 Hz
- Téléphone : [300, 3400]Hz

# 6. Les supports de transmission

L'ensemble des caractéristiques que nous venons de voir fait que la capacité d'un support de transmission est limitée.

Capacité Maximale = la quantité Maximale d'information transportée par unité de temps.  $\text{CapMax} = W \log_2(1 + \frac{S}{B})$

où W est la largeur de la bande passante exprimée en Hertz, S/B est la valeur du rapport puissance du signal à puissance du bruit, la base deux du logarithme servant pour exprimer l'information en bits.

Exemple:

sur une liaison téléphonique dont la bande passante a une largeur de W=3100 Hz, avec un rapport S/B correspondant à 32 dB (valeurs courantes),

on obtient :

$$10 \log S/B = 32, \text{ donc } \log S/B = 3.2 \text{ soit } S/B = 1585$$

$$\text{CapMax} = 3100 \log_2 (1 + 1585)$$

$$\text{soit avec } 1586 = 2^{10,63}$$

$$\text{CapMax} = 3100 \times 10,63 = 33000 \text{ bit/s.}$$

# 6. Les supports de transmission

## Critères de choix d'un support de transmission

En théorie : propriétés physiques

En pratique :

- Cout : media, Connecteurs, émetteurs et récepteurs, Installation : pose (tirer des câbles), ...
- Immunité aux perturbations : Foudre, électromagnétiques, ...
- Longueur maximale possible entre deux équipements actifs
- Débits possibles (surtout débit max) : bit/s

## Les supports de communication:

Deux grandes classes de supports de transmission :

les supports **à guide physique**

- les paires torsadées, les câbles coaxiaux, les fibres optiques, ...

les supports **sans guide physique**

-les ondes hertziennes, radioélectriques,...

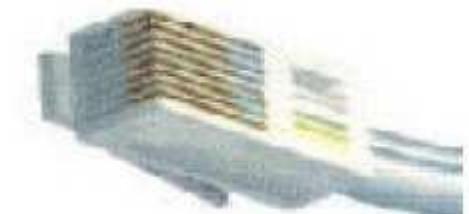
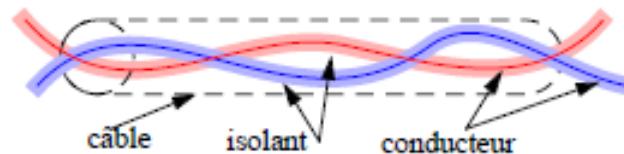
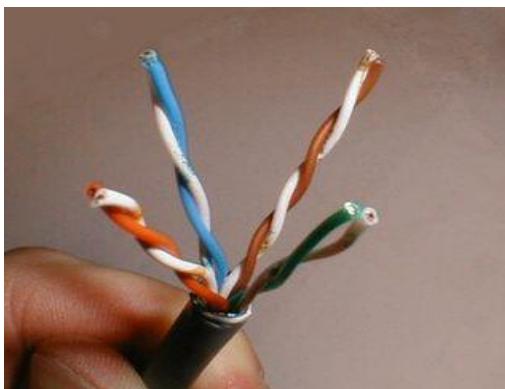
Chaque type de câble nécessite des connecteurs, ou prises, d'un format spécifique.

# 6. Les supports de transmission

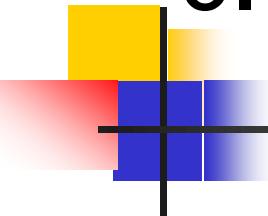
Ainsi le câblage en paire torsadée utilise généralement des connecteurs de type RJ45, alors que le câblage coaxial utilise des connecteurs en T

## Paire torsadée : téléphonie, LAN

- Une paire de conducteurs (alliage de Cu) en spirale entourés d'un isolant (plastique).
- utilisée depuis très longtemps pour le téléphone
- une paire → un lien de communication, plusieurs paires → un câble
- répéteur tous les 2-3 km
- Accès point à point ou multipoint



# 6. Les supports de transmission



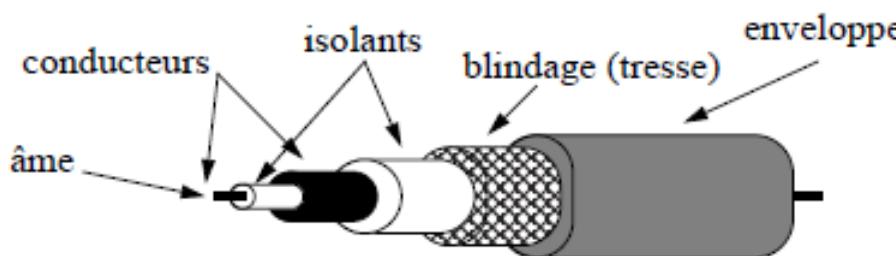
plusieurs catégories de paires torsadées, c'est le média le plus utilisé à l'intérieur des bâtiments

- Catégorie 1: n'a aucune contrainte, sert pour les communications bas débit.
- Catégorie 2 : fréquence de 2 Mhz, 2 à 25 paires. Dédié au transport de voix et bas débit.
- Catégorie 3 : référence pour les RL Ethernet et Token Ring, fréquence de 16 Mhz
- Catégorie 4 : complément du précédent pour une plus grande sécurité, 20 Mhz, peu utilisé
- Catégorie 5 : jusqu'à 125 Mhz, le plus répandu actuellement : câbles de 4 paires de pas de torsades différents.

# 6. Les supports de transmission

## Le câble coaxial

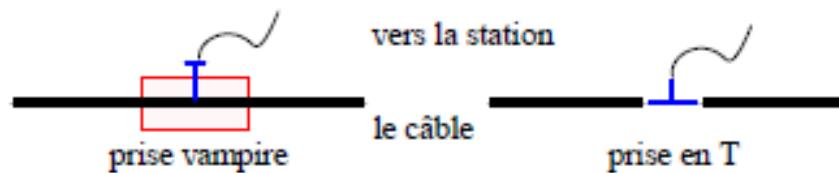
- Deux conducteurs cylindriques, ayant le même axe, séparés par un isolant .
- offre un meilleur blindage vis-à-vis des paires torsadées
- Réduit les distorsions électromagnétiques
- Avantages : moins sensible aux bruits, fréquences plus élevées => débits plus importants (Gbits/s)
- Inconvénient : coût élevé



# 6. Les supports de transmission

Connecteurs :

- prise vampire: perce le câble
- prise en T : nécessite la coupure du câble (prise BNC)



Caractéristiques :

-impédance :

- 50 Ohm - type Ethernet,
- 75 Ohm - type TV (CATV : "Community Antenna TeleVision")

- débit : quelques 100 Mbit/s

- encombrant : diamètre > 1 cm, et peu flexible

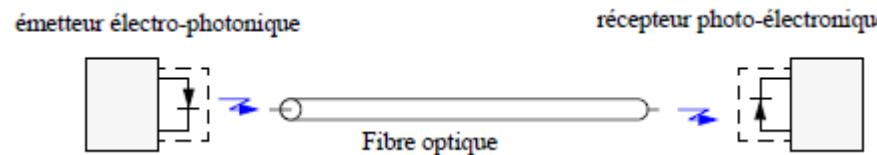
- coût plus élevé

# 6. Les supports de transmission

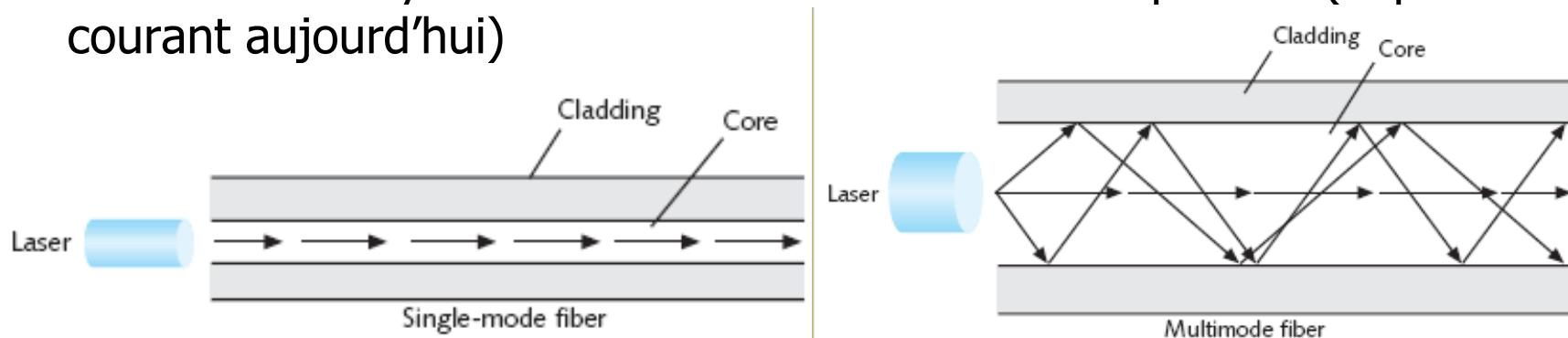
## La fibre optique

- guide cylindrique de diamètre de quelques microns, en verre ou en plastique qui conduit un rayon optique

Principe d'émission/réception



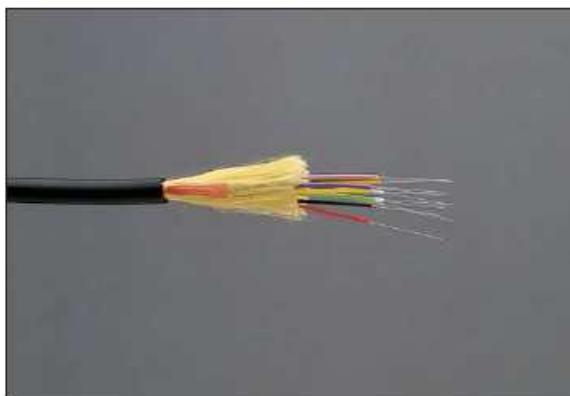
- 2 types : monomode / multimode
  - Monomode : rayons lumineux « en ligne droite »
  - Multimode : rayons lumineux avec réflexions : dispersion (le plus courant aujourd'hui)



# 6. Les supports de transmission

## La fibre optique

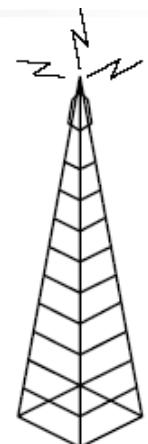
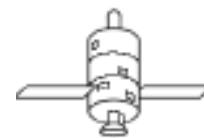
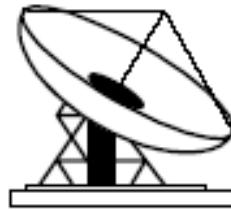
- largeur de bande varie entre 25 000 et 30 000 Ghz.
- Avantages :
  - interconnecte des réseaux éloignés (centaines de km)
  - Peu sensible aux bruits, pas d'erreurs ( $< 10^{-12}$ )
  - confidentialité
  - C'est le support le plus utilisé en interconnexion en MAN et WAN
- Inconvénient : cher, connexion point à point seulement



# 6. Les supports de transmission

## Transmission à travers l'atmosphère

- Pas de support physique
- Ondes radioélectriques : 10 kHz – 500 kHz
- Les faisceaux hertziens : 500 kHz – 20 GHz
  - utilisée pour les transmissions de données
  - transmission terrestre - portée : 50 à 1000km
- Liaison satellite - (géostationnaire ou à défilement, hauteur:36000 ou 800 km)
  - fréquences montantes : 3.4 – 4.2 GHz & 7.25 – 7.75 GHz
  - fréquences descendantes : 5.725 – 6.425 GHz & 7.9 – 8.4 GHz



# 6. Les supports de transmission

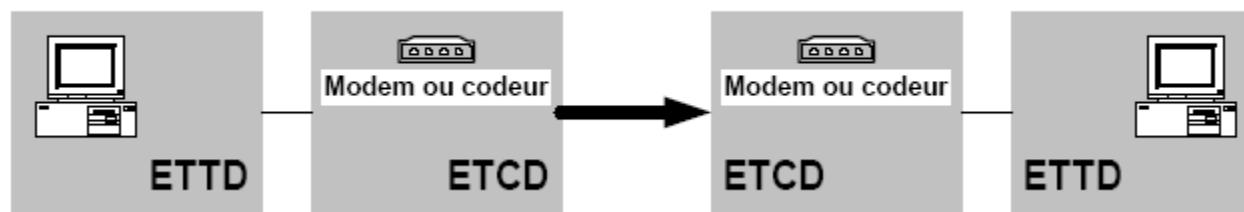
## En résumé

Types	Bandes Passantes	Utilisation
Paire Torsadée (TP)	>100 KHz	Téléphonie, LAN (UTP, STP)
Câble coaxial	>100 MHz	Télévision, LAN, (MAN?)
Fibre Optique	>1 GHz	LAN, MAN et WAN (Monomode #60 Km, Multimode #2 Km)
Faisceaux Hertziens	Variable ( dépend nature et fréquence)	MAN, LAN
Satellites	Plusieurs canaux > 10 MHZ	WAN

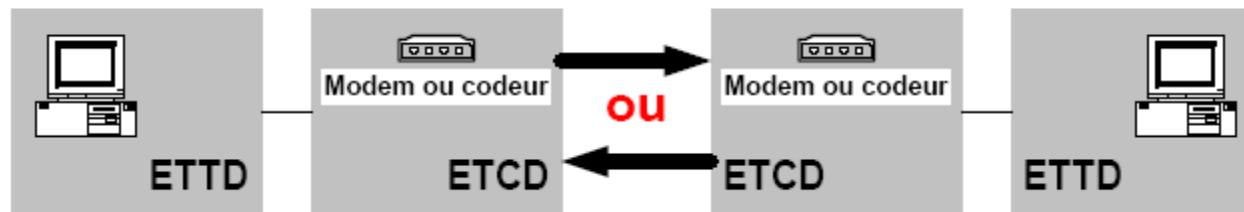
# 7. Les modes de transmission

Le mode de transmission concerne l'organisation des échanges entre les entités communicantes:

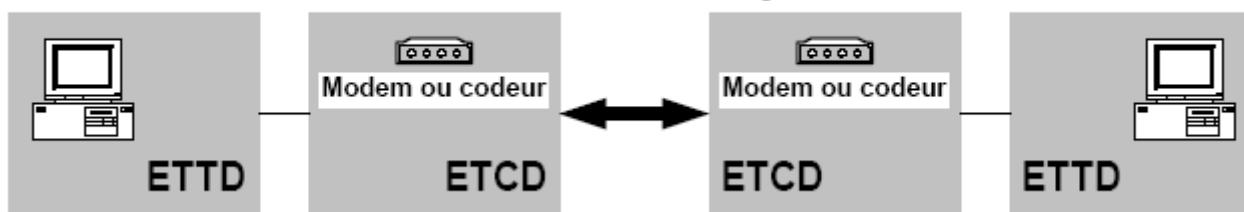
**Liaison simplex**

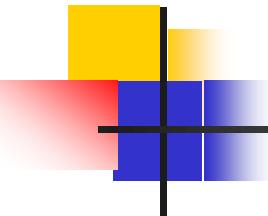


**Liaison half duplex (à l'alternat)**



**Liaison full duplex**



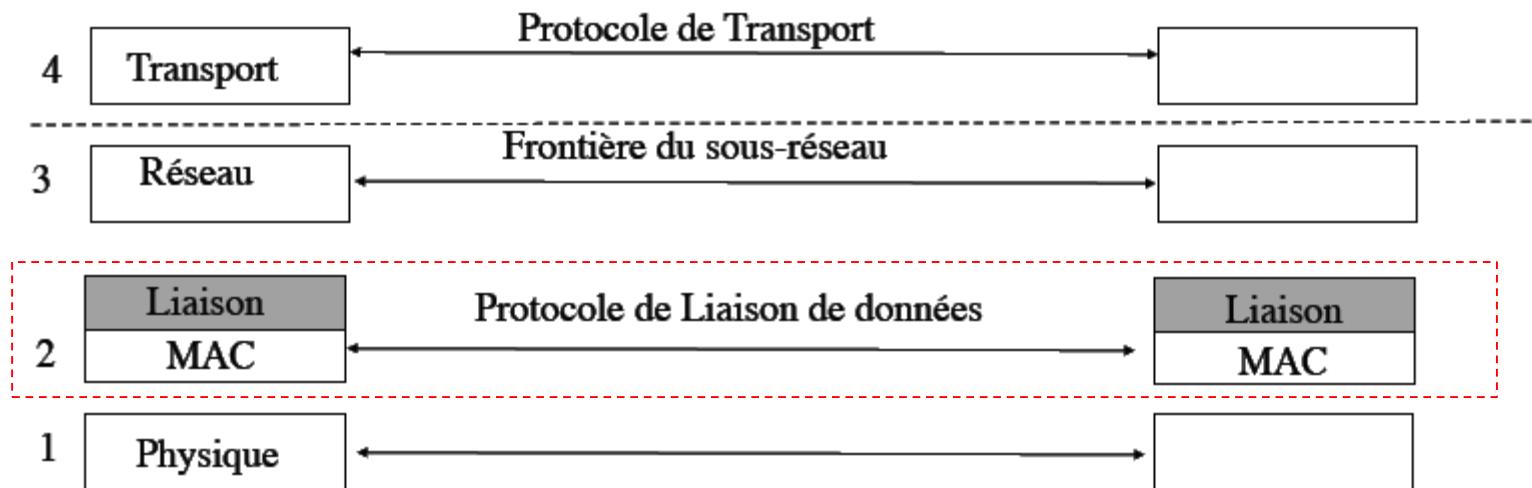


## **Chapitre -4-**

# **Couche liaison et réseaux locaux**

# 1. Etude de la couche Liaison de données

## La couche liaison de données



# 1. La couche liaison de données

## Service fournis à la couche réseau

- Découpage en trame
- Un transfert fiable: détection et correction des erreurs
- Contrôle de flux et récupération d'erreur
- Accès multiples à un support (fait par la sous couche MAC: Medium Acces Control): exemple le protocole Ethernet
- Une grande partie de ces problématiques est en fait souvent réalisé dans la couche transport (en particulier pour les réseaux locaux)
- Dans Ethernet la couche Liaison se résume à la couche MAC, à la délimitation des trames et à la détection des erreurs: c'est un service sans connexion , ni acquittement
- Le reste (contrôle de flux et récupération d'erreur) est fait dans TCP

# 1. La couche liaison de données

## Le contrôle d'erreur

- Les données peuvent être modifiées ou perdues pendant le transport
  - un service primordial pour certaines applications
  - exemple: transfert de fichiers
- La détection d'erreur
  - Comment se rendre compte de la modification ou perte des données à l'arrivée du trame?
- La correction d'erreur: deux techniques
  - Comment corriger à l'arrivée les données erronées? La correction à l'arrivée des paquet.
  - Faire en sorte que l'émetteur, renvoie les trames erronées ou perdues: la récupération d'erreur

# 1. La couche liaison de données

## Notion de trame

Une trame est une suite binaire de taille bornée contenant des informations de types " données " et/ou des informations de contrôle nécessaires pour réaliser les fonctions de ce niveau.

Le flot de données (bits) entrant doit être segmenté en blocs appelés trames

- But: fixer une unité pour le contrôle d'erreur.

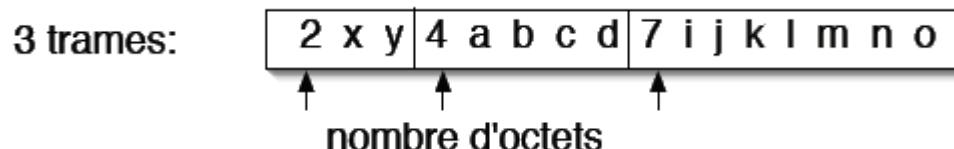
## Pourquoi?

- Si une erreur se produit lors de la transmission, l'unité de transmission sera la trame (au lieu de retransmettre toute l'information on renvoie simplement la trame)
- Certains types de réseaux imposent une limite sur la taille de trames

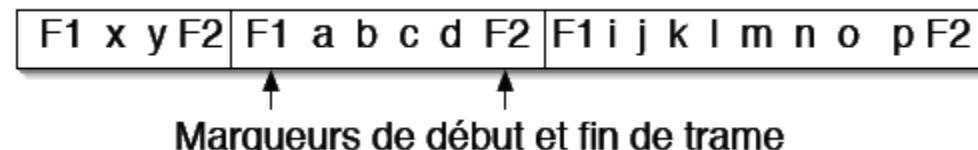
# 1. La couche liaison de données

- Techniques de découpage en trame

1. Compter les caractères

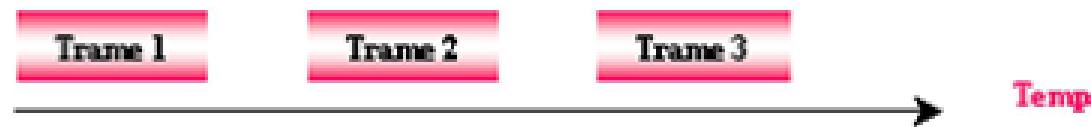


2. Utiliser des marqueurs de début et de fin de trame



3. Changer le codage utilisé dans la couche physique

Introduire un silence inter trames



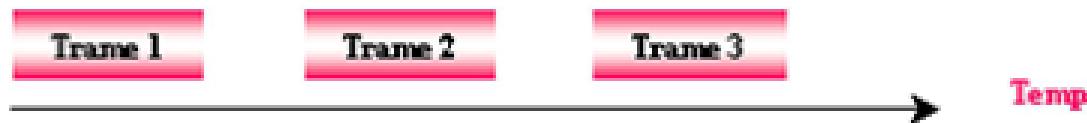
# 1. La couche liaison de données

Exemple : Ethernet un marqueur de début de trame et arrête le codage Manchester à la fin de trame (Silence inter trame de  $9,6\mu s$  pour le 10 Mb/s)

## Problème

- Comment délimiter une trame (le récepteur doit être capable de savoir le début et la fin de chaque trame)?

## Insérer des silences entre les trames

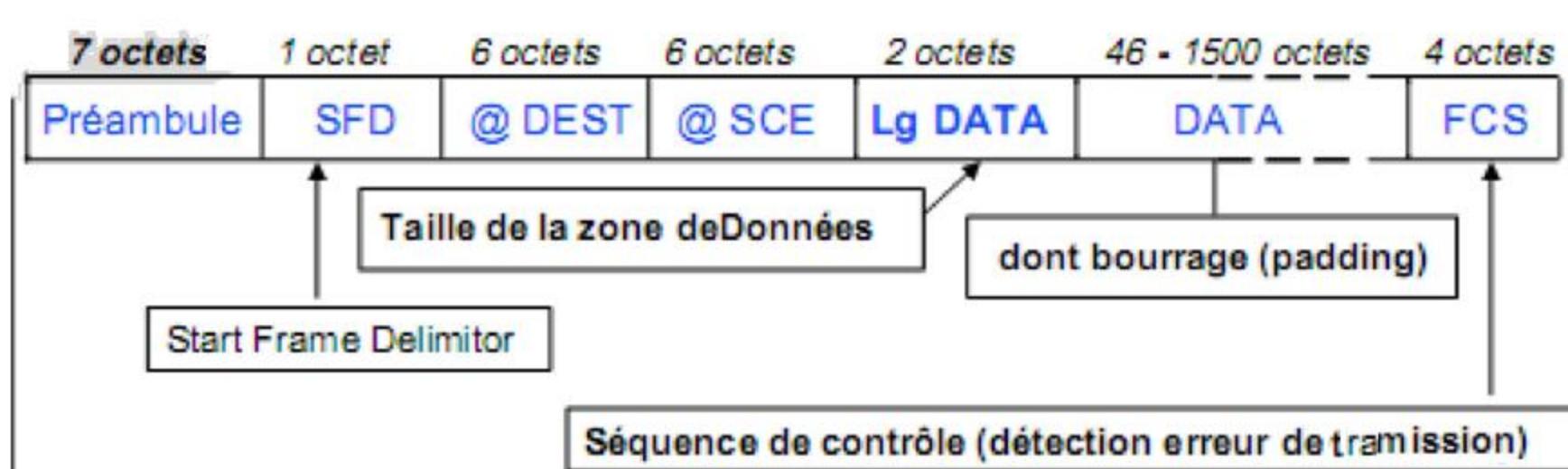


## Inconvénient

Les réseaux garantissent rarement les délais ➔ Possibilité de destruction de certains temps de silence ou de créer d'autres à l'intérieur des trames.

## 2. Analyse syntaxique

Format d'une trame IEEE 802.3



FORMAT D'UNE TRAME ETHERNET



## 2. Analyse syntaxique

### Format d'une trame IEEE 802.3

**Préambule:** Représente le début de chaque trame et elle est composée de 7 octets positionnés à 10101010 (AA en hexadécimal). Cette amorce permet de synchroniser les stations réceptrices.

**Marqueur de début de trame (Start Frame Délimiter) :** Cet octet représente le début de la trame et a pour valeur 10101011.

**Adresse destination-Adresse source :** Ce sont les adresses physiques du réseau codées sur 6 octets.

**Longueur du champ d'information (Length) :** Ce champ indique sur 2 octets la longueur des données LLC. Ce nombre est compris entre 0 et 1500 octets.

## 2. Analyse syntaxique

**Données** (Data) : Champ de données LLC (Logical Link Control) contenant entre 0 et 1500 octets.

**Bourrage** (PAD) : Octets de bourrage ajoutés si la trame ne contient pas 46 octets pour satisfaire la taille minimale d'une trame 802.3.

**FCS** (Frame Control Sequence) : Constitué d'un mot de 32 bits, ce champ représente le code de vérification d'erreur sur la trame. Sa portée s'effectue sur tous les champs exceptés :

- le délimiteur de début de trame,
- le FCS.

Polynôme générateur d'une trame 802.3 est :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1.$$

## 2. Analyse syntaxique

### Jeton sur anneau

Définition: Un jeton est une trame particulière et unique

#### Principe

- Les stations sont connectées sur un anneau logique unidirectionnel
- Le jeton circule d'une station à une autre
- Une station a le droit d'émettre une trame si elle possède le jeton.
- Une trame envoyée par une station est retirée de l'anneau par la station émettrice.

#### Problèmes

- L'existence du jeton, L'unicité du jeton et absence de famine

#### Solution

- Une station particulière dite station de **surveillance** se charge de vérifier l'existence et l'unicité du jeton.
- Des règles d'échange du jeton doivent être définies afin d'éviter la famine de certaines stations .

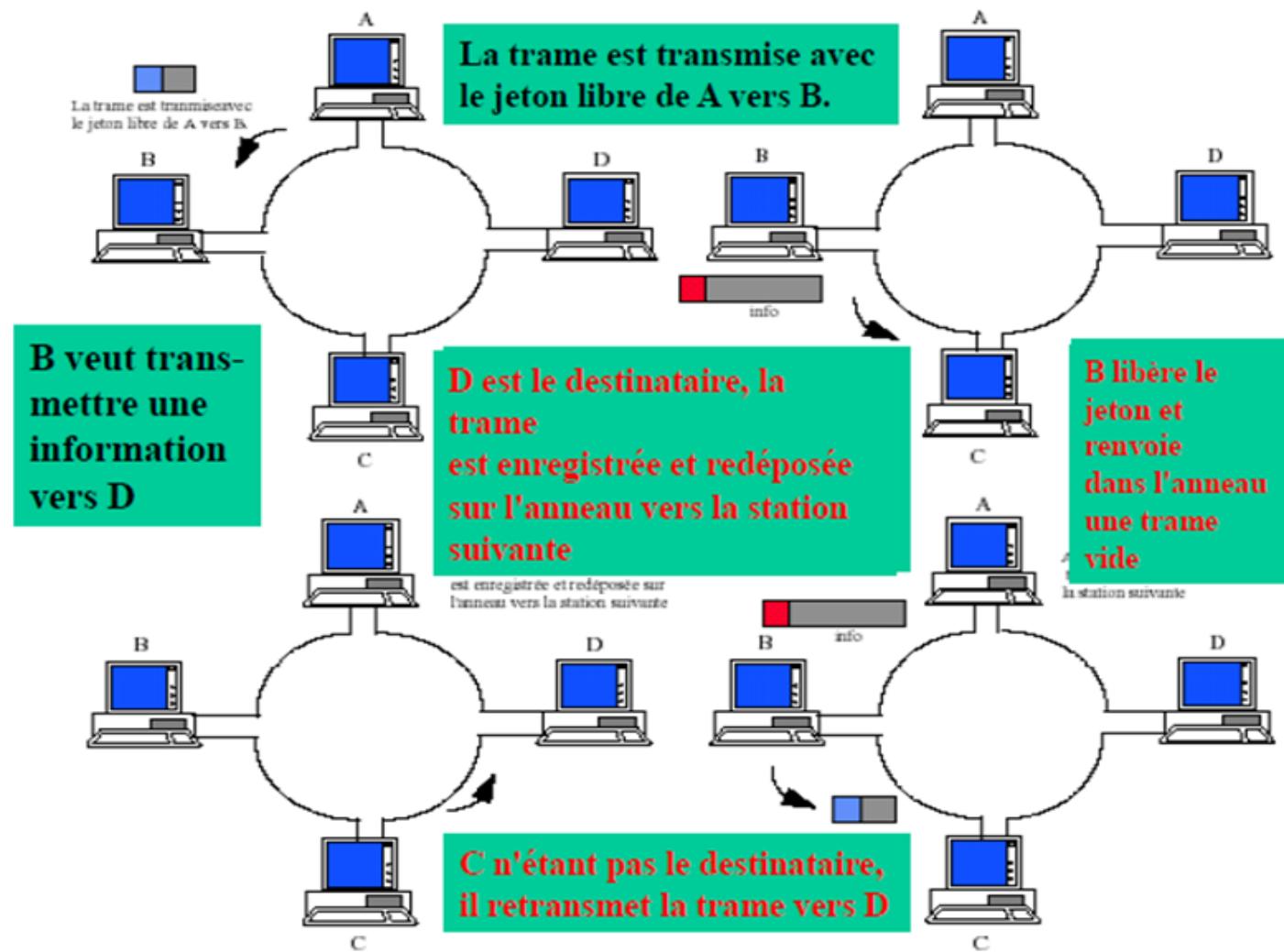
## 2. Analyse syntaxique

### Jeton sur anneau : Principe de fonctionnement :

- Une trame vide circule de station en station sur l'anneau avec un jeton positionné à libre.
- Une station recevant la trame avec le jeton libre souhaite transmettre de l'information; Elle positionne le jeton à occupé, elle remplit la trame avec les données à transmettre, elle indique le destinataire, et renvoie la trame vers la station suivante.
- La trame circule de station en station jusqu'à ce quelle atteigne le destinataire
- La station destinatrice recopie les données nécessaires, et renvoie la trame dans l'anneau après avoir positionné certains indicateurs.
- La station émettrice reçoit la trame, la vide, remet le jeton à libre et redépose la trame dans le réseau.
- La trame circulera dans l'anneau jusqu'à ce qu'une station le capture pour transmettre quelque chose.

## 2. Analyse syntaxique

Jeton sur  
Anneau  
(exemple)



## 2. Analyse syntaxique

**Jeton sur anneau : Format du trame 802.5**

Trame sans données (Jeton Libre)



Trame avec données (Jeton occupé)



**SD** : (Starting delimiter), codé sur 1 octet, il sert à délimiter le début d'une trame ou d'un jeton. Son format est représenté par la valeur : JK0JK000 avec J et K ont des valeurs binaires ne représentant ni un 0 ni un 1.

**AC** : (Access Control) 1 octet dont la structure est de la forme suivante :

PPP : Indique la priorité de la trame (de 0 à 7)

T : Permet aux stations d'accéder au support pour les transferts d'information.

T=0 jeton libre

T=1 jeton occupé

## 2. Analyse syntaxique

### Jeton sur anneau : Format du trame 802.5

M : Monitor bit, positionné par la station 'moniteur' du réseau. Il permet d'éviter que les trame fasse plusieurs fois le tour du réseau.

RRR : Bits de réservation de plus grande priorité pour augmenter la priorité du prochain jeton.

**FC** : (Frame Control) 1 octet permettant de définir le type de la trame.

**@D** (Destination Address) **@S**(Source Address) : Ce sont les adresses physiques du réseau codées sur 6 octets.

**RI** : (Routing Information) Ce champ comportant de 2 à 30 octets permettent le routage de la trame vers la station destinatrice.

**INFO** (Data) : Ce champ peu être vide ou contenir un ou plusieurs octets. La taille max n'est pas définie formellement.

**FCS** (Frame Control Check) : Codé sur 4 octets il permet de vérifier l'intégrité de transmission de la trame.

Polynôme générateur d'une trame 802.5 :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1$$

# 3. Erreur de transmission

- Détection et retransmission (Codes détecteurs).

**Techniques:**

- Bit de parité
- Détection d'erreur par checksum
- La plus utilisée CRC (Code Reduncy Cyclic)

- Détection et Correction (Code Correcteurs):

indispensable pour les supports physiques de mauvaise qualité ou pour des applications qui demande le transport de données précieuses.

**Plusieurs techniques-**

- Envoyer 3 fois la même information et on choisit la plus probable,

# 3. Erreur de transmission

## Détection et Correction d'erreurs

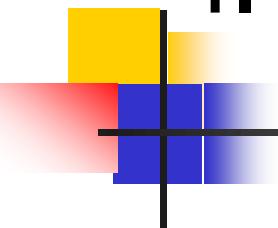
Avant 2004:

Détection et Correction d'erreurs gérées au niveau trame (couche2) du fait que la qualité lignes physiques était insuffisante pour obtenir des taux d'erreurs acceptables.

Actuellement le problème est différent:

- Le taux d'erreurs en lignes est devenu satisfaisant (moins que  $10^{-9}$ )
- Cela provient des techniques de codages et de la fibre optique
- Les applications multimédias ne tolèrent pas la perte de temps associés aux reprises sur erreurs.
- D'où détection et retransmission est la plus utilisée en ce moment

## 4. Le contrôle d'erreur

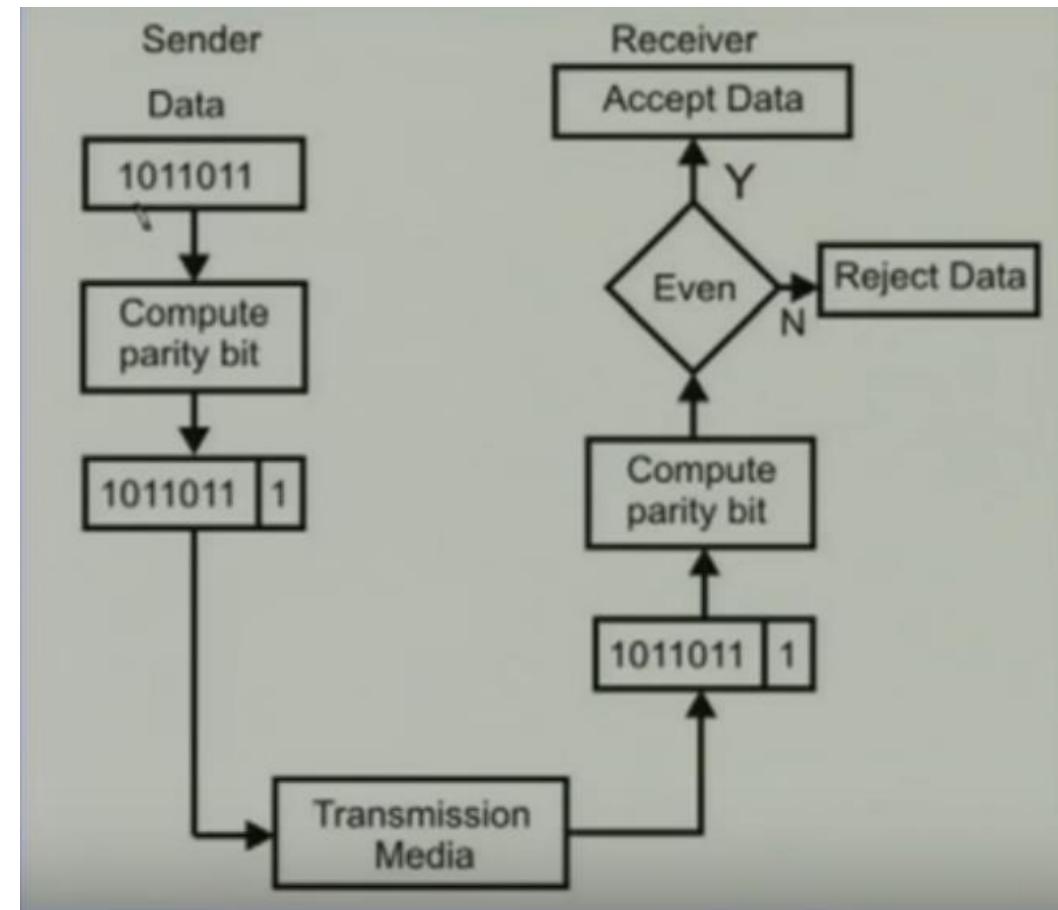


## La détection /correction d'erreur

# 4. Le contrôle d'erreur

## Bit de parité

Algorithme et exemple



# 4. Le contrôle d'erreur

## Bit de parité

Réception : la règle de codage est appliquée et la parité du résultat est comparée au 8eme bit reçu

Exemple : 1 1 0 0 1 0 1 **1** => incorrect (le 8eme bit devrait être 0)

## Remarques

on ne sait pas d'où vient l'anomalie

•Lorsque le nombre de bits erronés est pair, il n'y a pas de détection  
exemple : si 1 1 0 0 1 0 1 0 devient 0 0 1 1 0 1 0 1 la communication semble correcte et pourtant 8 erreurs.

•La détection d'anomalies ne permet pas de détecter le nombre d'anomalies

ex emple: si 1 1 0 0 1 0 1 0 devient 0 0 1 1 0 1 0 0, on ne pas savoir qu'il y a eu 7 erreurs

❑code parité => code détecteur d'un nombre impair d'erreurs mais ne permet pas de corriger des erreurs!

# 4. Le contrôle d'erreur

## Code de parité croisé

Bloc : suite de L caractères => suite de 7L bits

Codage : les L caractères sont rangés dans un tableau de L lignes et 7 colonnes. On ajoute une parité horizontale et une parité verticale.

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$
$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$	$a_{2,8}$
...	...	...	...	...	...	...	...
$a_{L,1}$	$a_{L,2}$	$a_{L,3}$	$a_{L,4}$	$a_{L,5}$	$a_{L,6}$	$a_{L,7}$	$a_{L,8}$
$a_{L+1,1}$	$a_{L+1,2}$	$a_{L+1,3}$	$a_{L+1,4}$	$a_{L+1,5}$	$a_{L+1,6}$	$a_{L+1,7}$	

# 4. Le contrôle d'erreur

Code de parité croisé

Décodage

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$	0
$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$	$a_{2,8}$	0
...	...	...	...	...	...	...	...	0
$a_{L,1}$	$a_{L,2}$	$a_{L,3}$	$a_{L,4}$	$a_{L,5}$	$a_{L,6}$	$a_{L,7}$	$a_{L,8}$	...
$a_{L+1,1}$	$a_{L+1,2}$	$a_{L+1,3}$	$a_{L+1,4}$	$a_{L+1,5}$	$a_{L+1,6}$	$a_{L+1,7}$	$a_{L+1,8}$	0
0	0	0	0	0	0	0	0	

Un 1 indique une erreur

# 4. Le contrôle d'erreur

Code de parité croisé

Décodage

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$	0
$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$	$a_{2,8}$	0
...	...	...	...	...	...	...	...	0
$a_{L,1}$	$a_{L,2}$	$a_{L,3}$	$a_{L,4}$	$a_{L,5}$	$a_{L,6}$	$a_{L,7}$	$a_{L,8}$	0
$a_{L+1,1}$	$a_{L+1,2}$	$a_{L+1,3}$	$a_{L+1,4}$	$a_{L+1,5}$	$a_{L+1,6}$	$a_{L+1,7}$	$a_{L+1,8}$	0
0	0	0	1	0	0	1	0	

Pour 2 erreurs sur une même ligne ou même colonne : détection mais pas de correction possible (quelle ligne ?)

# Le contrôle d'erreur

Code de parité croisé

Décodage

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$	$a_{1,8}$	0
$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$	$a_{2,8}$	1
...	...	...	...	...	...	...	...	0
$a_{L,1}$	$a_{L,2}$	$a_{L,3}$	$a_{L,4}$	$a_{L,5}$	$a_{L,6}$	$a_{L,7}$	$a_{L,8}$	1
$a_{L+1,1}$	$a_{L+1,2}$	$a_{L+1,3}$	$a_{L+1,4}$	$a_{L+1,5}$	$a_{L+1,6}$	$a_{L+1,7}$	$a_{L+1,8}$	0
0	0	0	1	0	0	1	0	

Pour 2 erreurs sur des lignes distinctes : détection mais pas de correction possible (2 possibilités)

# 4. Le contrôle d'erreur

## Code de parité croisé

Exemple

Soit le Message HELLO! à envoyer:

H	1001000	0
E	1000101	1
L	1001100	1
L	1001100	1
O	1001111	1
!	0100001	0
LRC	1100011	0

Le message transmis est:

10010000 10001011 10011001 10011001 10011111 01000010 11000110

Cette méthode permet de détecter toutes les erreurs simples, doubles ou triples.

# 4. Le contrôle d'erreur

## Détection d'erreur par checksum

Données considérées comme n mots de K bits

Le Checksum de contrôle = complément à 1 de la somme des n mots. A la réception la somme des n mots de données plus le checksum ne doit pas contenir de 0.

Utilisé dans UDP, TCP

$$\begin{array}{r} k=8 \\ \hline \begin{array}{c} 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1 \\ +\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\ +\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0 \\ \hline =\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0 \end{array} \end{array} \quad n=3$$

Complément à 1

Checksum

1	0	1	0	0	0	0	1
---	---	---	---	---	---	---	---

# 4. Le contrôle d'erreur

Détection d'erreur par checksum

Exemple

Example:

$$k=4, m=8$$

10110011

10101011

01011110

1

01011111

01011010

10111001

11010101

10001110

1

Sum : 10001111

Checksum 01110000

Example: Received data

10110011

10101011

01011110

1

01011111

01011010

10111001

11010101

10001110

1

10001111

01110000

Sum: 11111111

Complement = 00000000

Conclusion = Accept data

# 4. Le contrôle d'erreur

## Détection d'erreur par CRC (Cyclic Redundancy Code)

Sont nommés aussi codes polynomiaux: il sont basés sur le traitement des suites de bits comme étant une représentation polynomiale avec les coefficients 0 et 1.

- Principe

on considère une suite de bits par exemple : 110111

A cette suite on fait correspondre le polynôme suivant :

$$(1.x^5)+(1.x^4)+(0.x^3)+(1.x^2)+(1.x^1)+1 \rightarrow x^5+x^4+x^2+x+1$$

Remarque : Les calculs sont faits en binaire (modulo 2 :  $1+1=0$ ;  $X+X=0$ ;  $X=-X$ ) [par exemple,  $(x^7 +x^3 )+ (x^3 +x) = x^7 + x$  ]

- Etape 1 :

On définit un polynôme connu de l'émetteur et du récepteur appelé polynôme générateur, soit r son degré :

$G(x) = x^r + \dots + 1$  ; il faut que les termes des deux extrêmes soient non nuls ( $x^r, x^0$ )

## 4. Le contrôle d'erreur

Codes normalisés  $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

IEEE 802, Ethernet

Etape 2 :

soit  $M$  le message à transmettre (de  $m$  bits) dont le polynôme correspondant est  $(M(x))$  de degré  $m-1$ .

On ajoute au message  $M$ ,  $r$  bits (appelés bits de contrôle, CRC (ou FCS) pour envoyer une trame  $P$  de  $n$  bits ( $n=m+r$ ) dont le polynôme correspondant  $P(x)$  de degré  $n-1$  est divisible par  $G(x)$

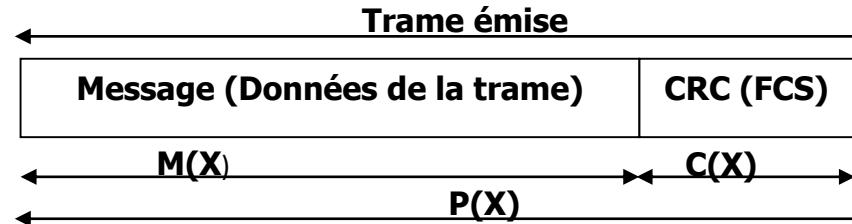
$P(x)$  est calculé suivant la méthode suivante :

on multiple  $M(x)$  par  $x^r$  : on a le polynôme  $x^r \cdot M(x)$  Ceci équivaut à un décalage de  $M(X)$ , de  $r$  positions vers la gauche.

on divise  $x^r \cdot M(x)$  par  $G(x)$ , soit :  $x^r \cdot M(x) = Q(x)G(x) + C(x)$ ,  $C(x)$  est le reste de cette division. Par définition son degré est  $r-1$

on envoie le mot  $P$  (de  $n=m+r$  bits) composé de  $m$  bits du message  $M$  suivie des  $r$  bits de FCS dont le polynôme correspondant est  $C(x)$ .

# 4. Le contrôle d'erreur



## En réception

- Le récepteur effectue la division du mot reçu par  $G(x)$ . Si le résultat est nul, il conclut qu'il n'y a pas d'erreur.

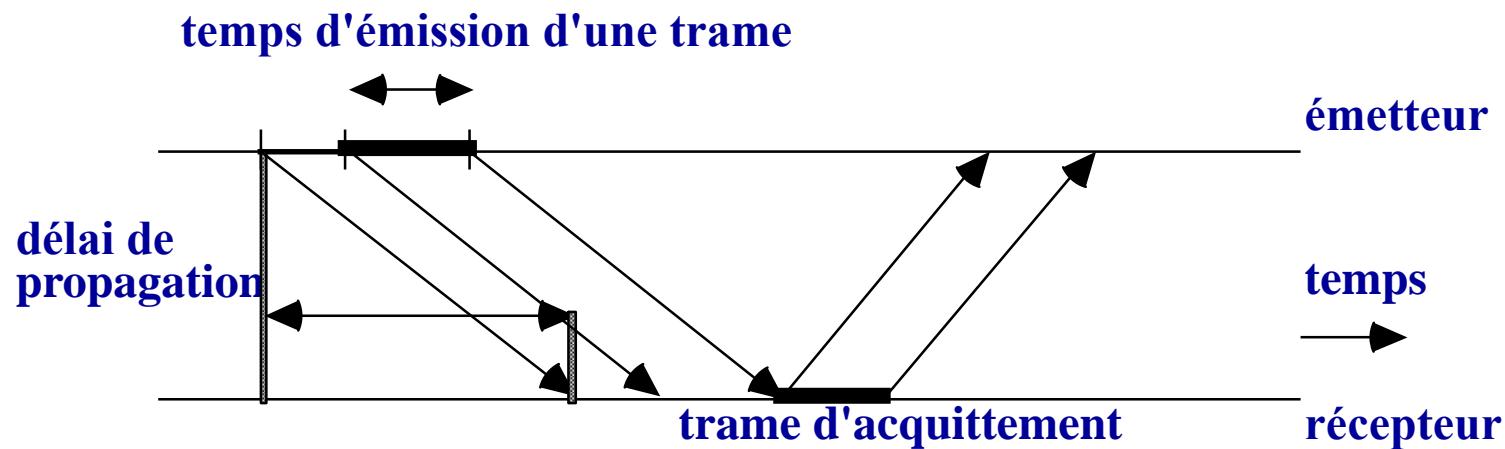
### ■ Problème

Les erreurs qui produisent un polynôme multiple de  $G(x)$  ne sont pas détectées.

### ■ Exemple CRC :

- Polynôme générateur :  $x^2+x+1$
- Message : 110111
- Division de 11011100 par 111 : reste 11
- Message transmis : **11011111**
- Décodage : division de 11011111 par 111.
- On contrôle si le reste est nul.

# 5. Contrôle de flux



Deux techniques:

- stend & wait
- Slinding window

# 5. Contrôle de flux

**Stend & wait : envoyer et attendre**

•Hypothèses:

- Les données utiles circulent dans un seul sens.
- Les trames envoyés contiennent l'information nécessaire (CRC par exemple) pour que le récepteur puisse détecter les erreurs éventuelles.

•Côté récepteur:

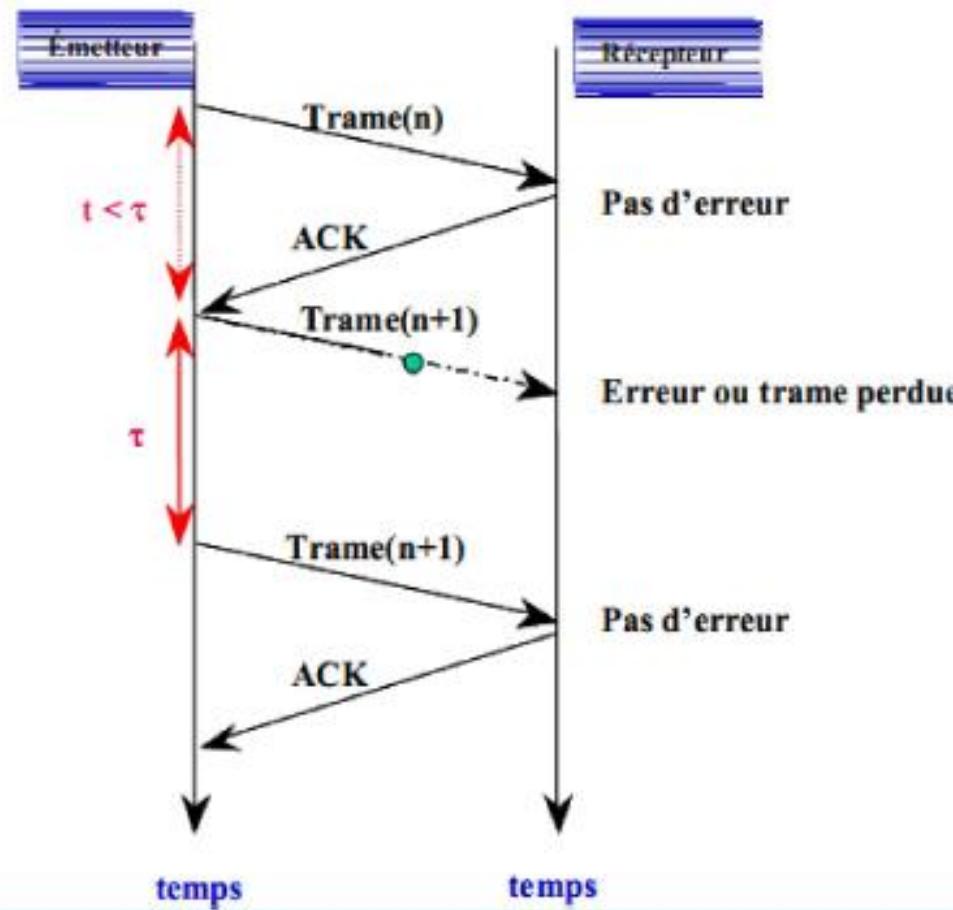
- Si la trame reçue ne contient pas d'erreur, il envoie un message d'acquittement ACK.
- Si la trame reçue content des erreurs, il n'envoie rien.

•Côté émetteur:

- Il envoie une trame et il attend une durée T ( T>= au temps requis pour qu'une trame fasse un aller-retours).
- Si au bout de T unité de temps , il ne reçoit pas un acquittement ACK, il retransmis la trame.

# 5. Contrôle de flux

Stend & wait : envoyer et attendre

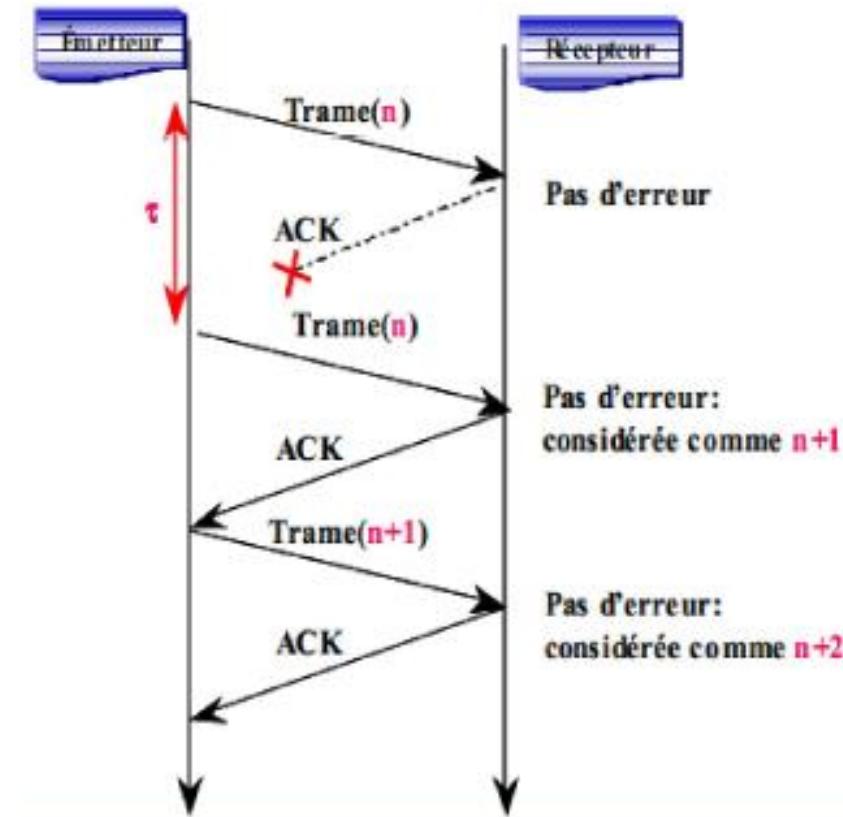


# 5. Contrôle de flux

Send & wait : envoyer et attendre

Problème:

Si l'acquittement d'une trame est perdu, l'émetteur va la retransmettre mais le récepteur va la considérer comme une nouvelle trame !.



## 5. Contrôle de flux

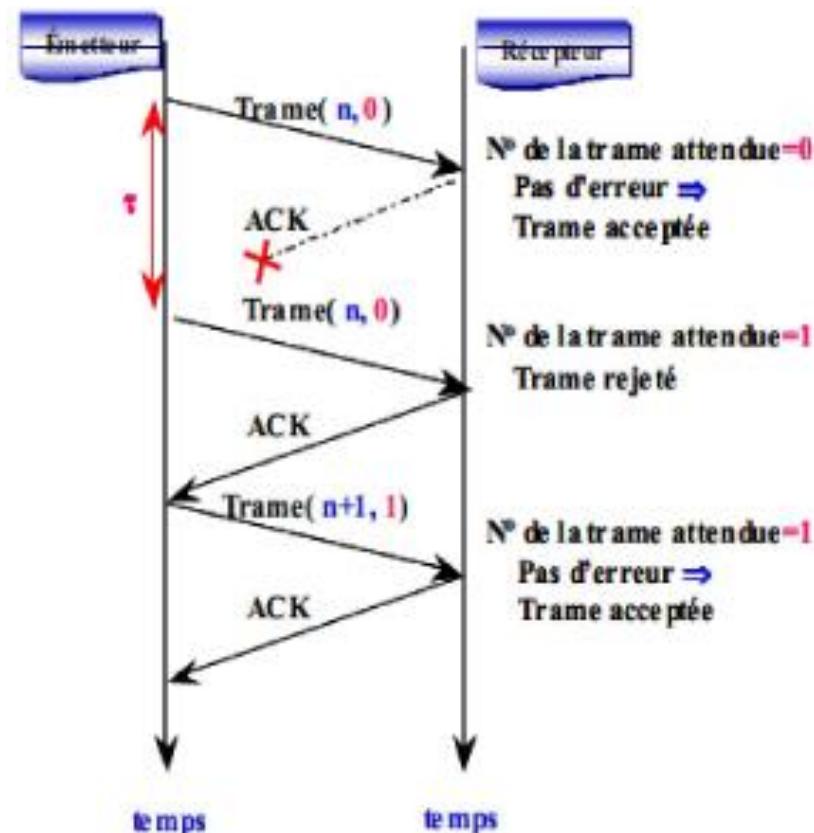
## **Stend & wait : envoyer et attendre**

**Solution:** Il suffit de numérotter les trames pour résoudre le problème précédent. A cette fin, on va ajouter un champ dans l'en-tête de chaque trame pour mettre leurs numéros.

**Question:** Quelle est la longueur du champ numéro?

## Réponse:

La seule ambiguïté du côté de récepteur est de savoir s'il s'agit de la trame précédente ou d'une nouvelle trame, donc un seul bit suffira pour la numérotation des trames. La première trame porte le numéro 0, la deuxième 1, le troisième 0, la quatrième 1, etc.



# 5. Contrôle de flux

**Stend & wait : envoyer et attendre**

**avantages:**

- Simplicité: Facile à comprendre et à implémenter
- Il ne demande pas beaucoup de mémoire: le récepteur utilise un tampon qui peut contenir une seule trame.
- Contrôle de flux: l'émetteur n'envoie pas plus que ce que le récepteur peut traiter. Il envoie une trame et il s'assure qu'elle a été traitée par le récepteur avant d'envoyer la suivante.

**Inconvénients:**

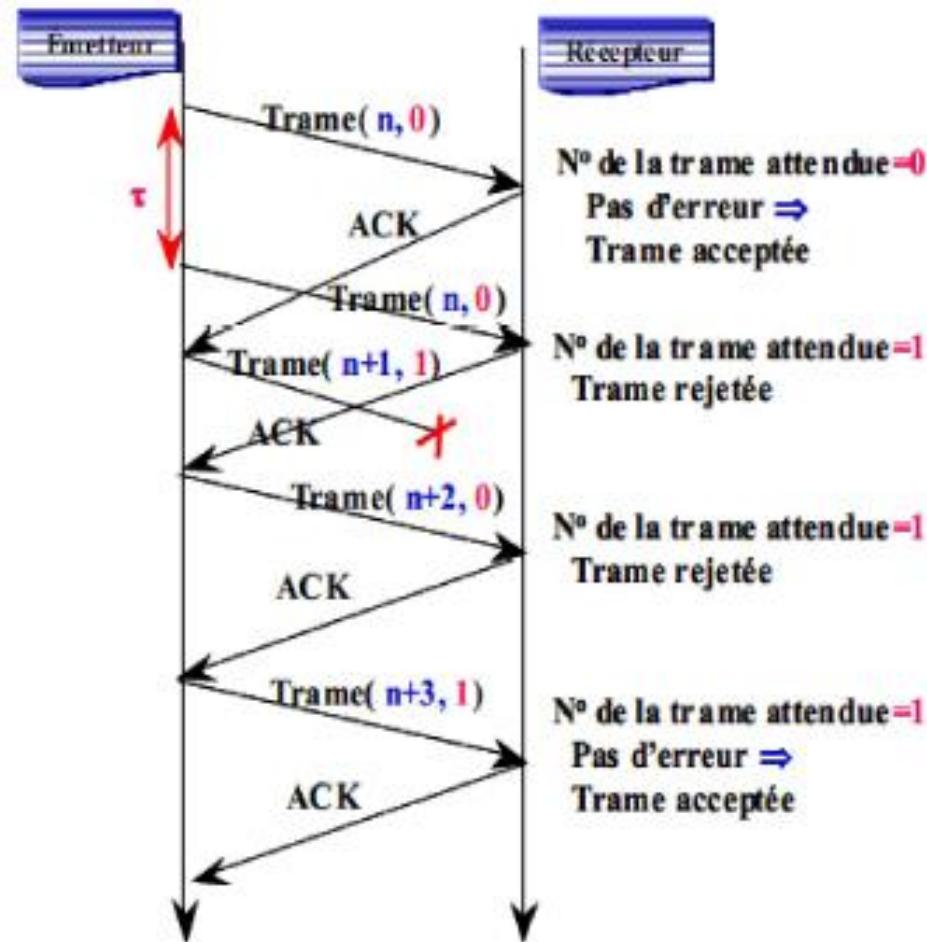
Les données utiles circulent dans un seul sens.: le canal de transmission n'est pas exploité comme il faut. Durant à peu près la moitié du temps. L'émetteur chôme.

# 5. Contrôle de flux

**Send & wait : envoyer et attendre**

Robustesse :

Avec le protocole précédent, si l'émetteur ne règle pas convenablement son temporisateur (plus petit que la valeur convenable). Il y aura la possibilité que le récepteur rejette des trames en les croyant des retransmissions.



# 5. Contrôle de flux

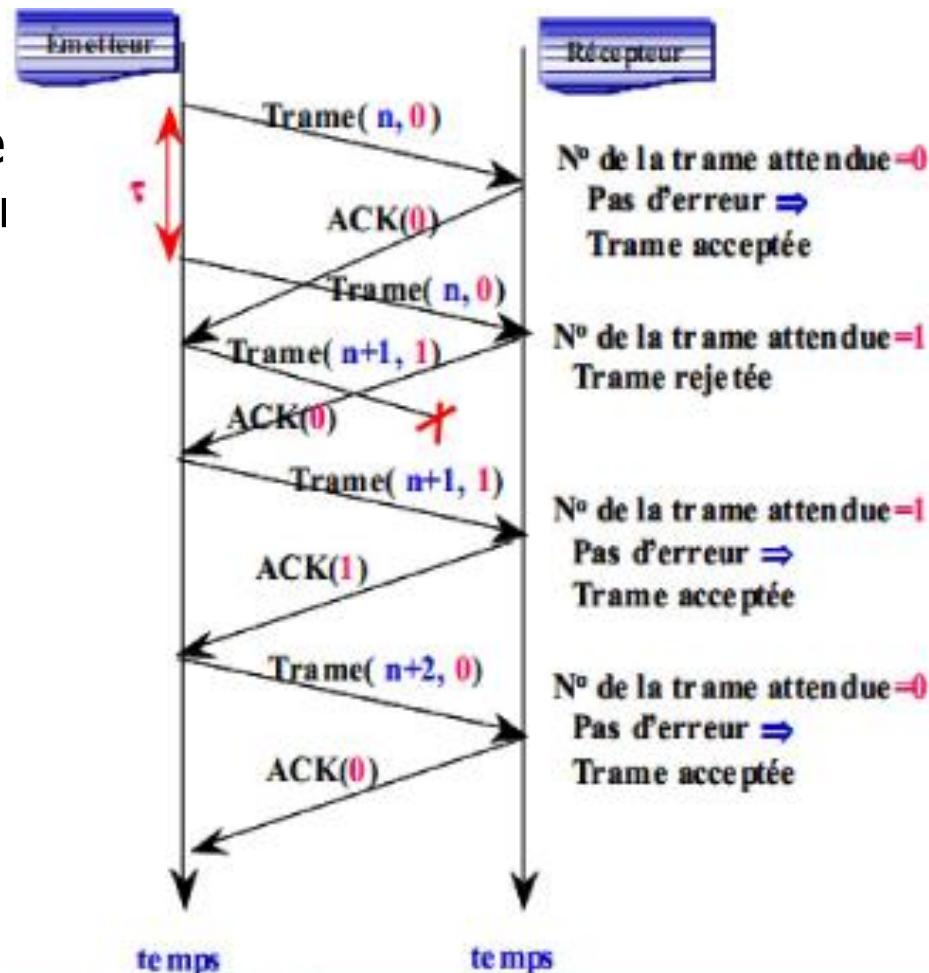
**Send & wait : envoyer et attendre**

Protocole plus robuste :

On veut un protocole qui fonctionne convenablement même si l'émetteur ne règle convenablement son temporisateur.

Solution:

Numérotter les acquittements.

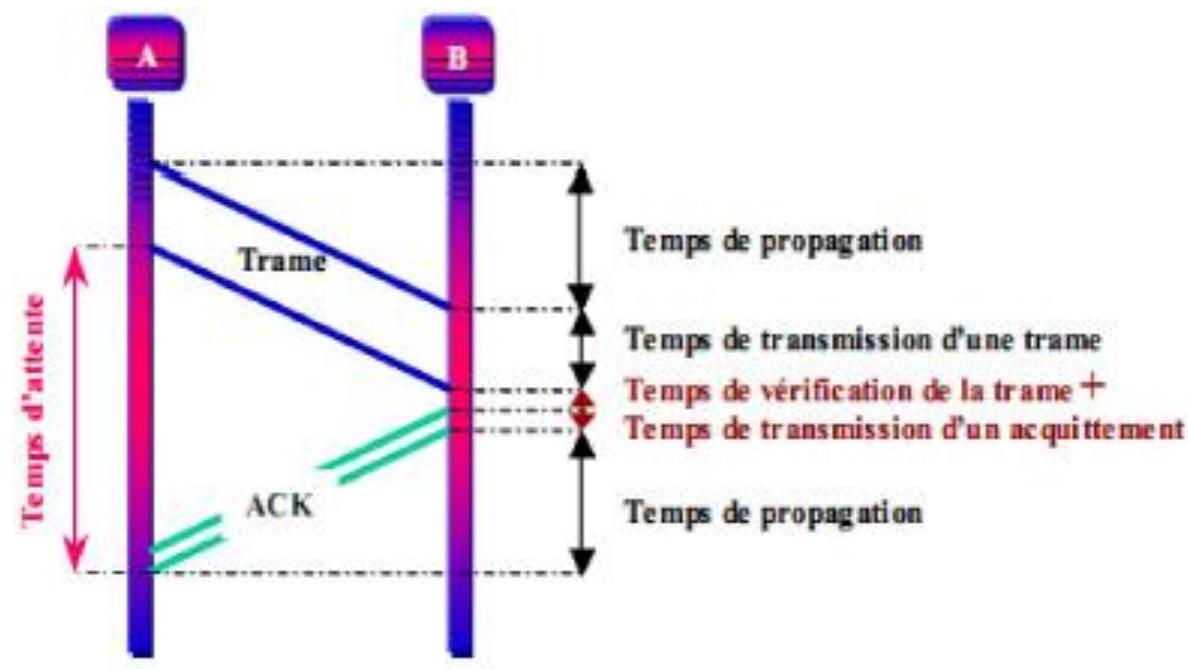


# 5. Contrôle de flux

## Sliding Window: Protocoles avec fenêtre d'anticipation

Amélioration :

Pour permettre une meilleur utilisation de la bande passante du canal de transmission, on va permettre à un émetteur d'envoyer plusieurs trames avant de recevoir un acquittement.



# 5. Contrôle de flux

## **Slinding Window: Protocoles avec fenêtre d'anticipation**

but:

Pour permettre une meilleur utilisation de la bande passante du canal de transmission, on va permettre à un émetteur d'envoyer plusieurs trames avant de recevoir un acquittement.

# 6. le contrôle d'accès multiple au canal

Réseaux particuliers à diffusion:

- Bus,
- radio, ...

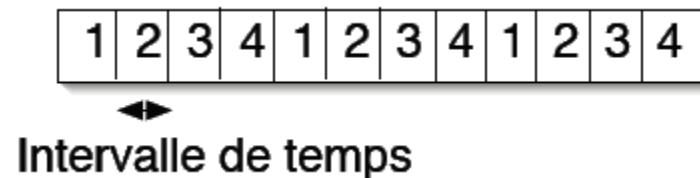
Ces réseaux sont intéressants pour leurs faible coût.

■ Problème :

- Réseau à diffusion implique un support unique pour n émetteurs / récepteurs
- Il existe différentes solutions pour réaliser ces accès multiples:
  - Par partage strict du support: le support est divisé soit dans le temps soit physiquement
  - Par accès aléatoire: on parle quand on veut
  - Par accès séquentiel: on parle à tour de rôle

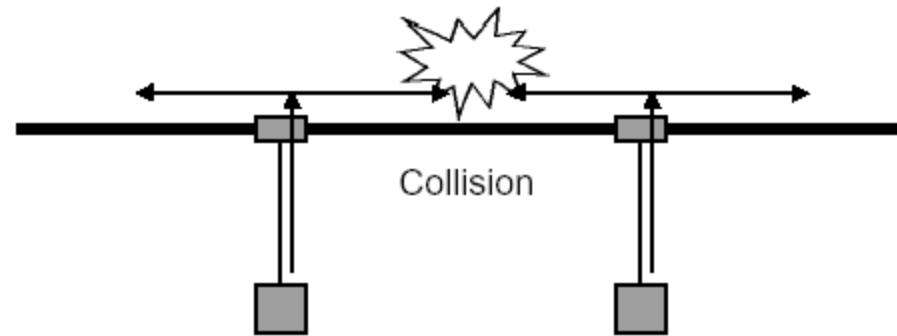
# 6. le contrôle d'accès multiple au canal

- Multiplexage en fréquences: découpage et allocation permanent des plages de fréquences,
  - Exemple de radio FM
  - Problèmes de l'allocation des plages de fréquences
- Multiplexage temporel: découpage dans le temps de l'allocation de la totalité de la bade passante à chaque entité



# 6. le contrôle d'accès multiple au canal

- Ethernet et WiFi (Wireless Fidelity)
- Une seule fréquence: possibilités de collisions



- 2 trames se percutent : c'est la collision
  - Plus le réseau est grand (nombre de stations), plus la probabilité d'apparition de collisions est grande

## Gestion de collisions

Deux grandes approches : Approche optimiste et Approche pessimiste

# 6. le contrôle d'accès multiple au canal

Approche optimiste

- Envoyer
- Déetecter s'il y a eu collision
- Si oui appliquer une méthode de résolution de conflit

Approche pessimiste

- Donner à chaque machine le droit exclusif d'émettre pendant une durée limitée du temps.
- Il faut prévoir un mécanisme de négociation de droit d'émission entre les machines.

**La Méthode d'accès CSMA/CD** Carrier Sens Multiple Access/ Collision Detection

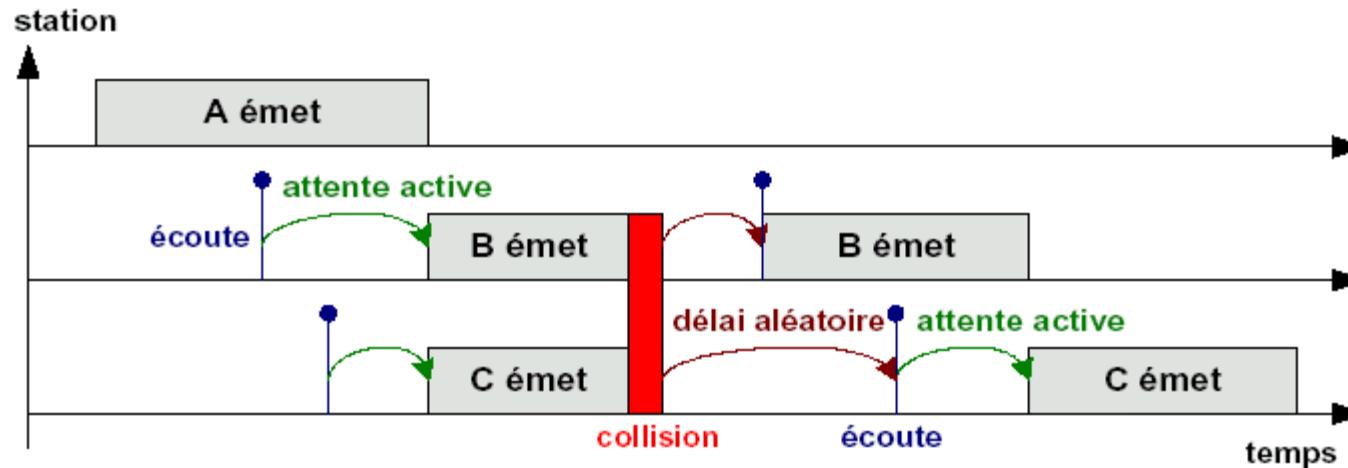
▪ Approche optimiste

▪ Principe :

- Ecouter le trafic sur le réseau
- Si pas de trafic Alors
  - Emettre une trame
  - Si la trame provoque une collision Alors
    - Ressayer ultérieurement d'envoyer la même trame

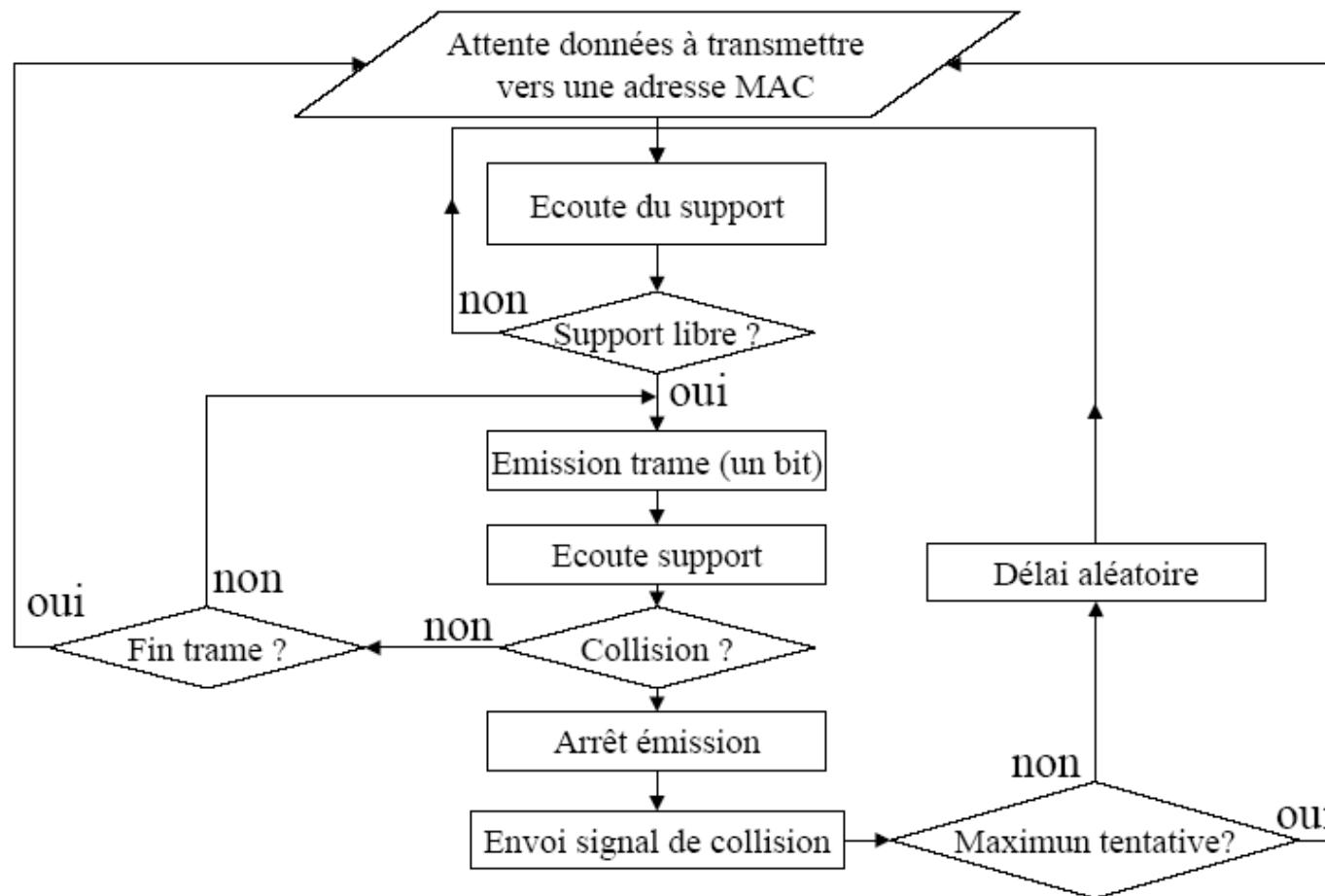
# 6. le contrôle d'accès multiple au canal

La Méthode d'accès CSMA/CD (gestion des collisions)



# 6. le contrôle d'accès multiple au canal

## La Méthode d'accès CSMA/CD algorithme

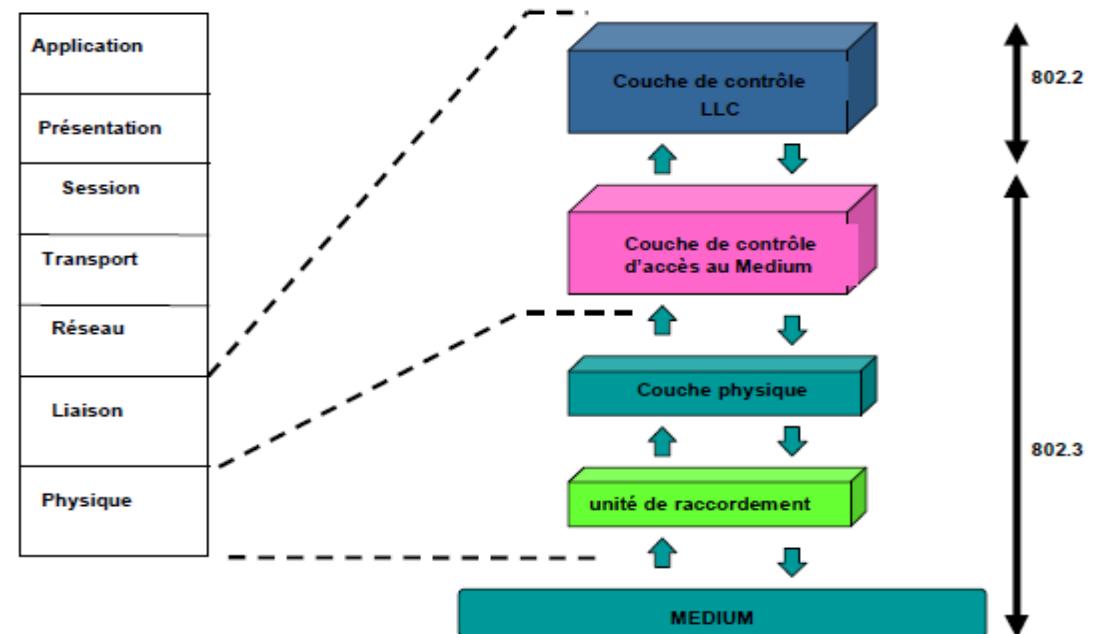


# 7. Les normes couche liaison de données

141

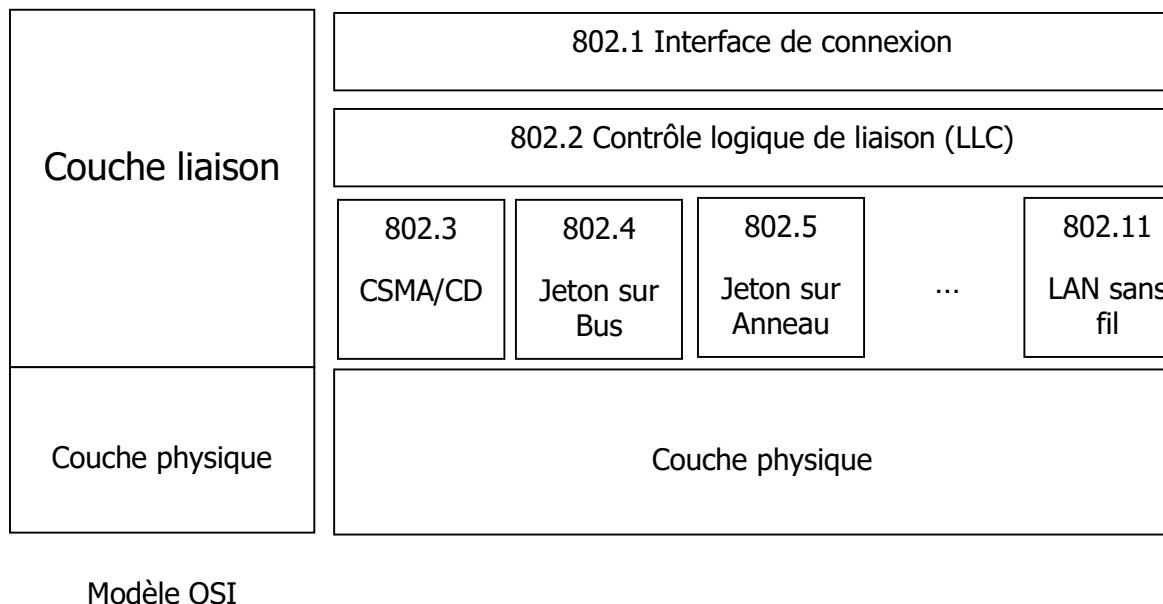
Le comité 802 d'IEEE a eu la charge de normaliser l'architecture de communication des réseaux locaux. Il s'est intéressé aux services offerts au niveau le plus bas (physique et liaison de données).

- Le modèle IEEE 802 contient 3 couches correspondants aux 2 couches (1 et 2) du modèle OSI.
- La couche 2 a été subdivisé en deux sous-couches pour prendre en compte d'une part le contrôle d'accès au Support et d'autre part la gestion communicantes

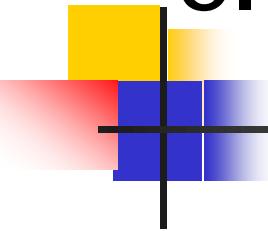


# 7. Les normes couche liaison de données

1980 : début de normalisation par l'IEEE  
Normalisation par le groupe du travail 802.



# 8. Les réseaux Locaux



On trouve généralement Les mots réseau et local indiquent une architecture distribuée mais localisée généralement. Qu'est ce qu'un réseau local ?

C'est un ensemble de **moyens autonomes de traitement** (ordinateurs, stations de travail, imprimantes, fax, téléphones, ...) reliés entre eux pour s'échanger des informations et partager des **ressources matérielles** (imprimantes, photocopieurs, scanners, graveurs, espaces disque, ...) ou **logicielles** (programmes, fichiers, ...)

On trouve généralement dans un réseau local  
un serveur de fichiers, d'impressions, de messagerie, de gestion des comptes utilisateur, de licences, de routage sécurisé vers Internet, web ...

# 8. Les réseaux Locaux

## Caractéristiques

- Un même média partagé (même câble par exemple)
  - il faut gérer l'accès au médium (différentes méthodes)
- Rayon de couverture : quelques kilomètres,
- Une bande passante élevée (10 Mb/s, 100 Mb/s, 1 Gb/s), partagée par tous les hôtes,
- Faible taux d'erreurs ( $10^{-10}$  erreur/bit)
- La capacité de faire du "broadcasting" (diffusion) et du "multicasting",
- Des relations entre les machines placées sur un mode d'égalité, (et non par exemple sur un mode Maître/Eclave).
- Une mise en œuvre qui reste du domaine privé, c'est à dire qui ne dépend pas d'un opérateur officiel de télécommunications.

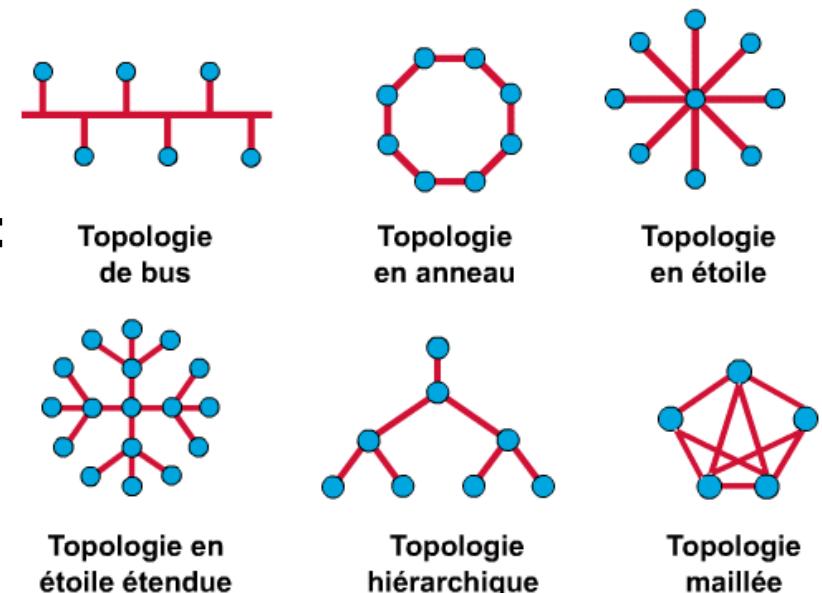
# 8. Les réseaux Locaux

La topologie définit la structure du réseaux: Il existe deux forme :

**La topologies physiques :**

c'est l'arrangement physique des stations, c'est-à dire la configuration spatiale du réseau. On distingue généralement les topologies suivantes :

- topologie en bus,
- topologie en anneau,
- topologie en étoile,
- topologie en étoile étendue,
- topologie en arbre,
- topologie maillée



**La topologie logique :** par opposition à la topologie physique, elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

# 8. Les réseaux Locaux

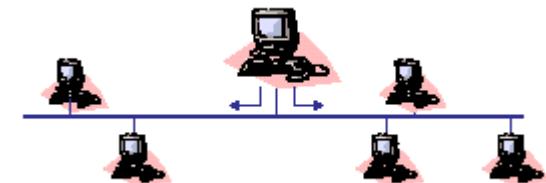
## Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

les messages sont reçus par l'ensemble des stations connectées (diffusion). une station peut accéder à tout moment au support  
→ problème si deux stations décident d'émettre en même temps (collision)

802.3 (Ethernet) : une station vérifie avant d'émettre qu'aucune autre station n'est déjà en train d'émettre

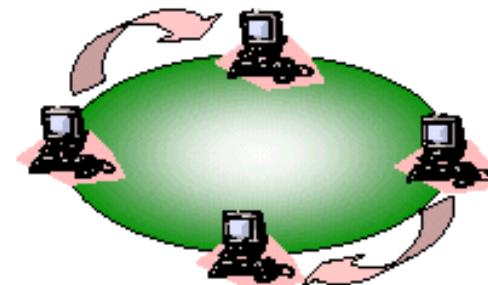
802.4 (Token Bus) : chaque station se voit attribuer tour à tour le droit d'émettre (circulation d'un jeton)



# 8. Les réseaux Locaux

## Topologie en anneau

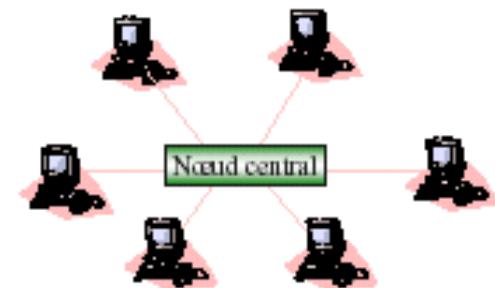
circulation unidirectionnelle du message de proche en proche jusqu'à atteindre le Destinataire



802.5 (Token Ring) : le droit d'émettre est transmis par l'intermédiaire d'un jeton qui circule de station en station sur l'anneau

## Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (hub) ou commutateur (Switch).



Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

# 9. Les réseaux Ethernet

## Historique

1970 : 1er Ethernet par Xerox

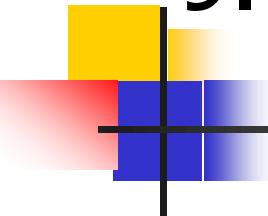
1975 : Normalisation (Xerox, DEC & Intel)

1985 : Normalisation par l'IEEE 802.3

## Caractéristiques

- Architecture logique :
  - Le support de transmission est un Segment = bus.
  - Il n'y a pas de topologie particulière (boucle, étoile, etc. . .).
- Un équipement est raccordé sur un câble On parle alors d'une station Ethernet, celle-ci a une adresse unique.
- Sur le câble circulent des trames.
  - Rayon de couverture : quelques KM
- Méthode d'accès : (CSMA/CD)
- Débits 10Mbits/s , 100Mbits/s , 1Gbits/s

# 9. Les réseaux Ethernet



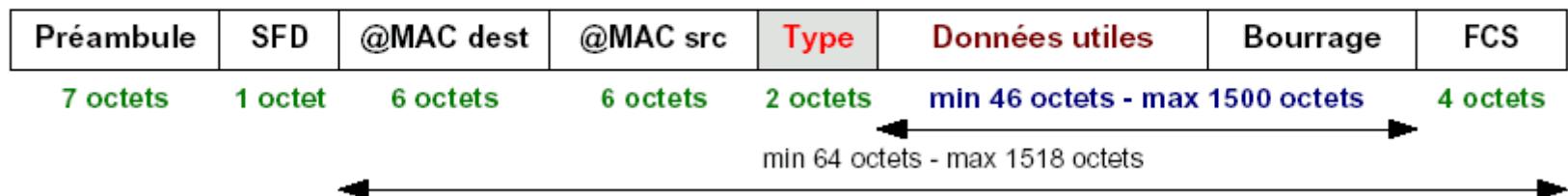
Un réseau Ethernet est un réseau à caractère probabiliste car il n'y a pas de chef d'orchestre pour synchroniser les émissions. Cette absence conduit à dire que c'est un réseau égalitaire.

Les quatre éléments de base d 'Ethernet sont:

- La **trame** qui est un ensemble standardisé de bits utilisé pour transporter des données à travers le système.
- Le **protocole de contrôle d 'accès au média**, qui consiste en un ensemble de règles intégré dans chaque interface Ethernet et qui permet à plusieurs ordinateurs d accéder de façon équitable au canal Ethernet commun.
- Les **composants de signalisation**, qui consistent en des dispositifs électroniques standardisés pour l émission et la réception des signaux sur le canal Ethernet.
- Le **Médium physique**, constitué des câbles et autres matériels utilisés pour transporter les signaux Ethernet numériques entre les ordinateurs connectés au réseau

# 9. Les réseaux Ethernet

## Trame Ethernet



Longueur minimale de trames Ethernet 64 octets

Si la trame < 64 octets on ajoute des bits de bourrage.

Longueur maximale de trames Ethernet 1518 octets

# 9. Les réseaux Ethernet

- Préambule : 7 fois 10101010 pour la synchronisation des bits, AA en hexadécimal.
- SFD (Start Frame Delimiter) : 10101011, AB en héxadécimal.
- FCS sur 4 octets pour la détection d'erreur
- Le champ "type" est deux octets qui désignent le type des données encapsulées:
- Type Données

Type	Données
0x0800	IP
0x0860	ARP
0x0835	RARP

- L'adressage MAC est sur 6 octets, 48 bits.  
L'adresse MAC est divisée en deux parties:
  - les trois premiers octets désignent le constructeur,
  - les trois derniers désignent le numéro de carte.

# 9. Les réseaux Ethernet

L'IEEE assure l'unicité des numéros de constructeurs, par tranche de  $2^{24}$  cartes.

Chaque constructeur assure l'unicité du numéro de chaque carte fabriquée. En gros  $2^{24}$  cartes par classe d'adresses.

On parle alors d'adresse physique, ou "hardware address". Pour le bon fonctionnement d'un LAN il est absolument indispensable que toutes les stations aient une adresse physique différente.

Exemple d'adresse physique en représentation hexadécimale :

08 :00 :09 :35 :d5 :0b

08 :00 :09 est attribuée à HP.

35 :d5 :0b est l'adresse de la carte

D'autres constructeurs, saisis au hasard des réseaux : liste

00 :00 :0C (Cisco), 08 :00 :20, (Sun)

AA :00 :04, (DEC), 00 :10 :5A (3Com)

# 9. Les réseaux Ethernet

## Différentes versions d'Ethernet

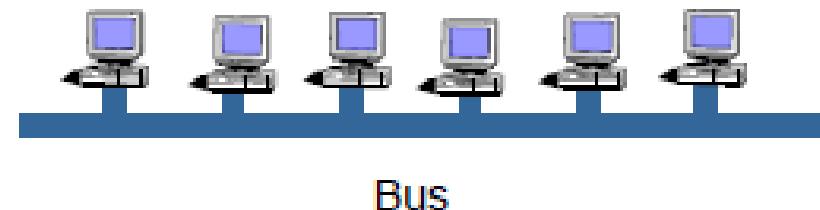
Pourquoi différentes versions ?

- Protocoles évolutifs
  - 2Mbit/s, 10Mbit/s, 100Mbit/s, 1Gbit/s
  - coaxial, paires torsadées, fibres optiques
- Les appellations normalisées IEEE 802.3 sont désignées par un code qui indique :
  - le débit
  - le type de modulation (bande de base ou large bande)
  - la longueur maximale d'un segment pour un câble coaxial ou une lettre donnant le type du support (T pour la paire torsadée, F pour la fibre optique)
- Exemple :
  - 10Base5 = 10Mbit/s en bande de base sur câble coaxial d'une longueur maximale par segment de 500m

# 9. Les réseaux Ethernet

## Ethernet, IEEE 802.3 10base5

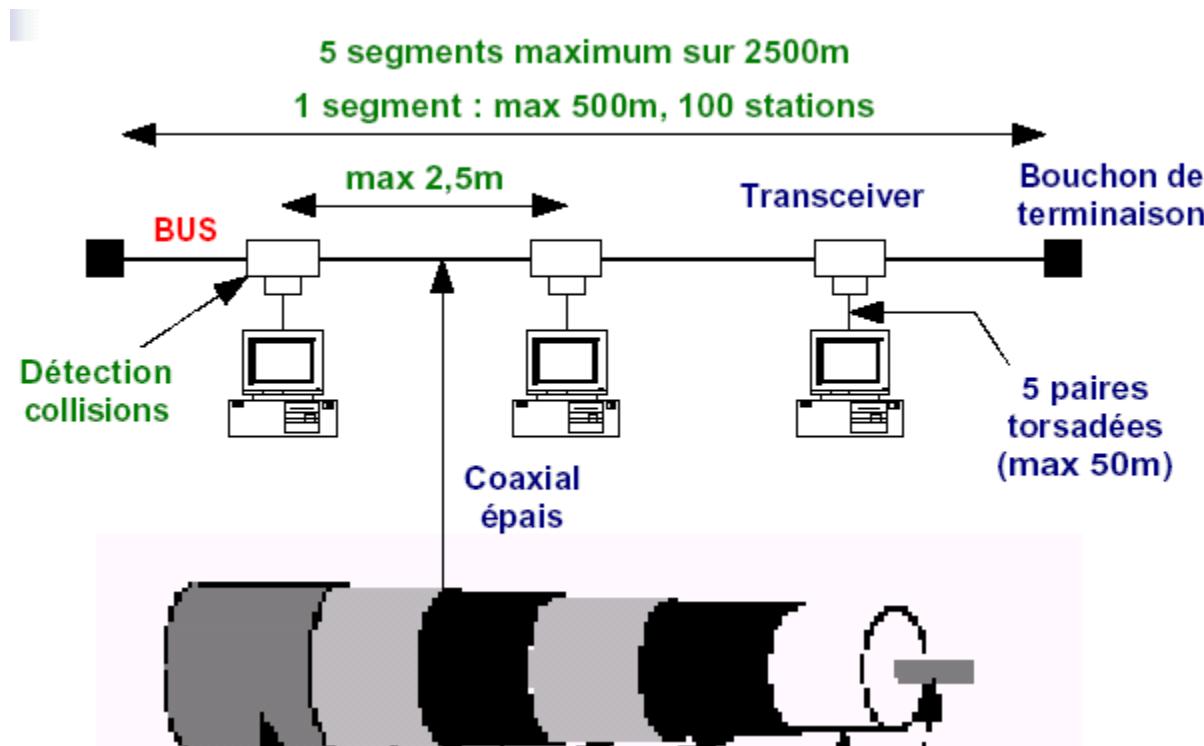
- Première version d'Ethernet normalisée (1985)
- une "vieille" technique très bien normalisée mais dépassée.
- 10Mbit/s en bande de base sur câble coaxial d'une longueur maximale par segment de 500m pour un maximum de 100 stations.
- Coût non négligeable.



- Matériel
  - codage Manchester
  - topologie physique = bus
  - câble coaxial épais (10mm), câble de liaison,
  - bouchons de terminaison (limite échos), connecteur DB15, répéteurs entre deux segments
  - transceiver (ou MAU) : conversion des signaux, détection collisions
  - carte Ethernet : gère l'algorithme CSMA/CD, ...

# 9. Les réseaux Ethernet

Ethernet, IEEE 802.3 10base5

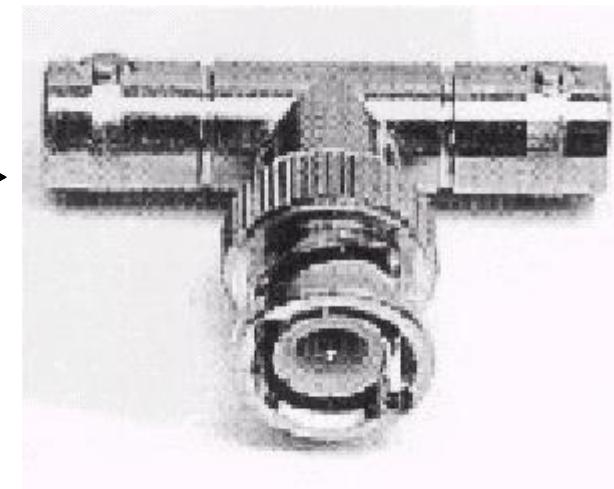
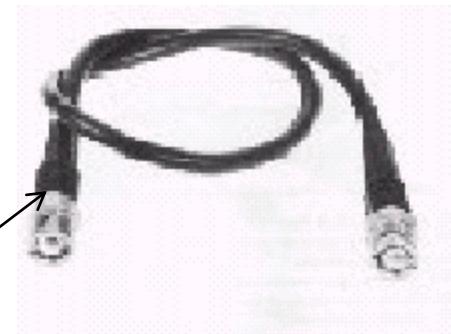


Pour les câblages rapides on préfère le 10Base2

# 9. Les réseaux Ethernet

## Ethernet fin, IEEE 802.3 10base2

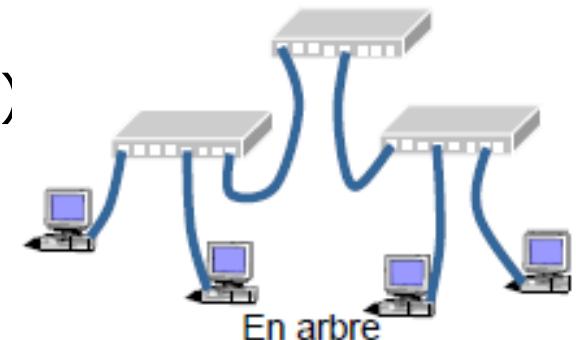
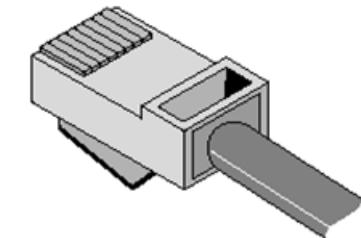
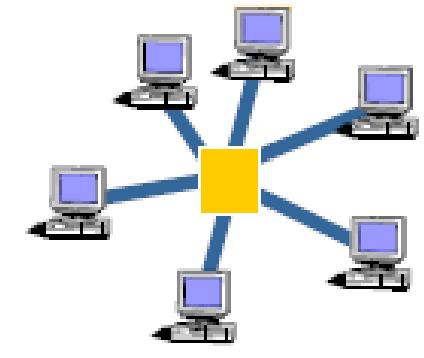
- Moins coûteux et plus facile d'installation
- Architecture la plus économique pour des petits réseaux (dizaines de stations)
- Matériel
  - codage Manchester
  - topologie physique = bus
  - câble coaxial fin (5mm),
  - bouchons de terminaison (limite échos),
  - connecteur BNC en T,
  - répéteurs entre deux segments
  - 30 stations max par segment)
  - longueur maximale d'un segment : 185m
  - distance entre 2 nœuds : 0,5m
  - transceiver intégré à la carte Ethernet



# 9. Les réseaux Ethernet

## Ethernet, IEEE 802.3 10baseT

- Une double paire torsadée de câble suffit.
- Topologie physique en étoile, La longueur maximale entre le moyeu et la station est de 100 m.
- Un Hub (ou Switch) émule un bus
  - Le raccordement au Hub se fait à l'aide d'une prise du type RJ45,
  - diffusion des messages sur tous les ports
  - détection des collisions avec émission d'un signal de collision à l'ensemble des stations
- Liaison Hub/Station ou Hub/Hub en paires torsadées (1 pour l'émission, 1 pour la réception)



# 9. Les réseaux Ethernet

## FastEthernet IEEE 802.14 100baseT

- Aujourd'hui le 100BaseT équipe la majeur partie des équipements professionnels,
  - 100 comme 100 Mbits/s.
  - Hub et cartes avec ports 10/100Mbitps
  - le port et la carte s'auto-configurent (permet la mixité 10/100)
  - Entièrement compatible avec 10BASE-T
    - Topologie en étoile : hub ou commutateur avec paires torsadées
    - Protocole CSMA/CD
    - Même format de trame
    - Ce sont le codage du signal et la catégorie des câbles qui changent.
- Trois types de câblages autorisés
  - 100baseT4 (4 paires, câble catégorie 3,4)
  - 100baseTX (2 paires, câble catégorie 5),
  - 100baseFX (fibre optique)

# 9. Les réseaux Ethernet

- Pourquoi des extensions pour Ethernet ?

- Accroissement du trafic sur les réseaux d'entreprise
- Nouvelles applications, consommatrices en débit (multimédia)
- La norme Ethernet est utilisée comme techniques d'accès à Internet

- Les extensions sont destinées à améliorer les débits disponibles

- Ethernet commuté (= Ethernet Full Duplex ou Switched Ethernet)
- Fast Ethernet (100 Mbit/s)
- Gigabit Ethernet
- 10Gigabit Ethernet

# 9. Les réseaux Ethernet

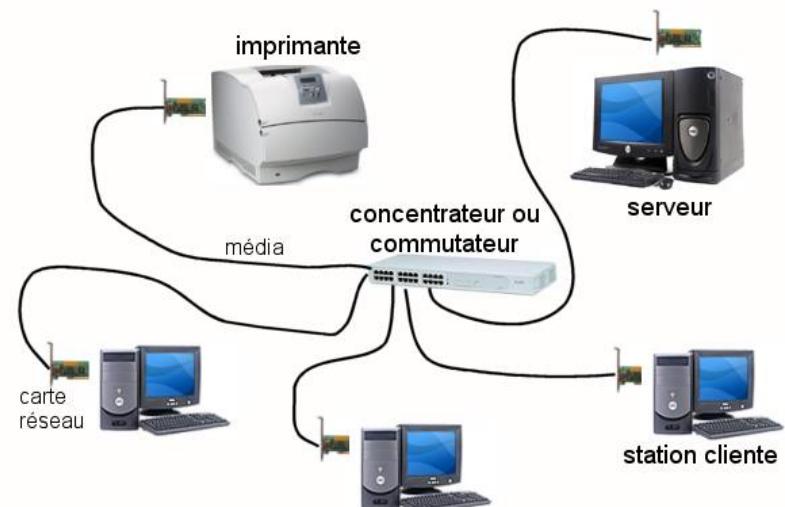
## Ethernet commuté

- Ethernet commuté (= Ethernet Full Duplex ou Switched Ethernet)
- **Hub** vs **Commutateur**

**Hub** : La topologie physique est une étoile, mais la topologie logique est le bus

**Commutateur** (switch) : l'équipement analyse l'adresse physique de destination d'une trame et la retransmet uniquement sur le brin contenant la machine destinatrice.

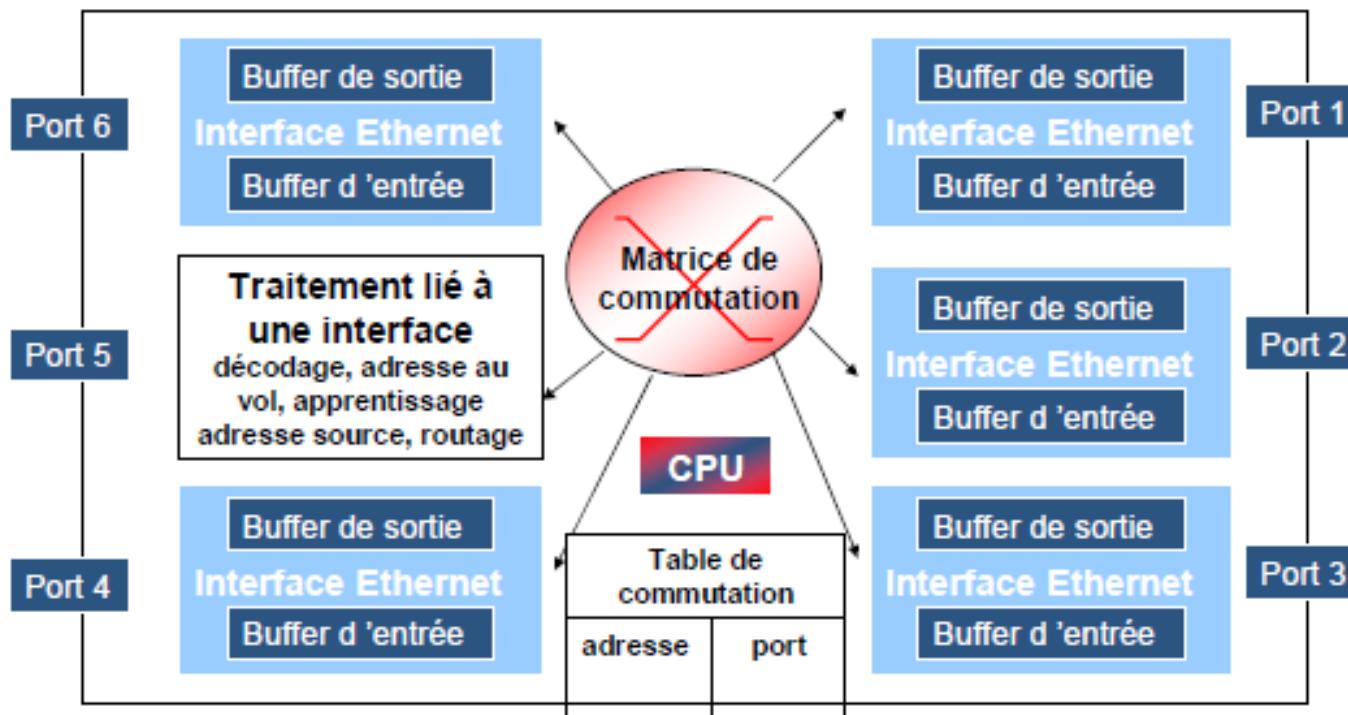
- Le commutateur permet en plus de regrouper dans un même segment les stations liées par des trafics importants :
  - plusieurs serveurs sur une dorsale
  - un serveur et des stations d'un même groupe de travail



# 9. Les réseaux Ethernet

## Ethernet commuté

Architecture interne d'un commutateur



# 9. Les réseaux Ethernet

## Ethernet commuté

### Deux techniques de commutation

- Commutation à la volée (cut through)

- accepte la trame et commence à détecter l'adresse destination pour la transmettre directement sur le port sortant
  - pas de contrôle → peut transmettre des trames erronées
  - doit bufférer si le port est occupé

- Commutation store and forward

- accepte la trame entrante, la stocke temporairement, la vérifie, la retransmet sur le port sortant

Problème de congestion du réseau - Pas de contrôle de flux.

# 10. Les réseaux Token-ring

## Principales caractéristiques

### ▪ Historiques

- Développé en 1969: boucle de Newhall
- Normalisé en 1983 (IEEE 802.5) soutenu par IBM

### ▪ Principe

- Une structure en anneau permet de faire circuler un jeton unique donnant le droit d'émettre à au plus une station

### ▪ Amélioration

- par rapport à Ethernet, offre à service de transmission des données prioritaires

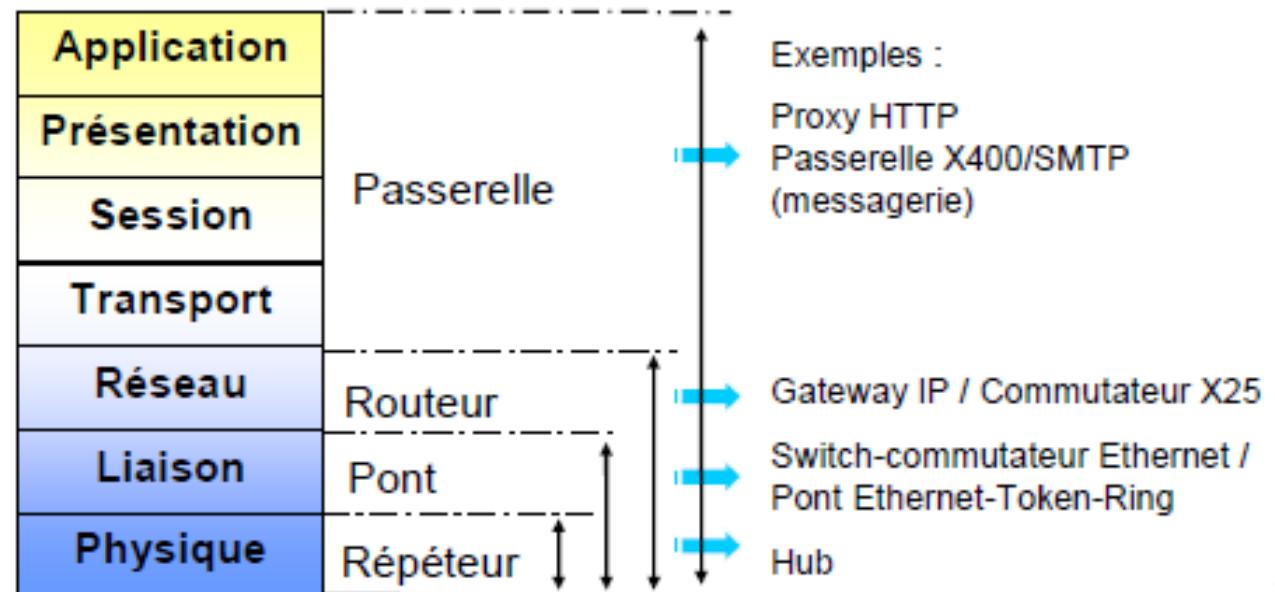
### ▪ Méthode d'accès: a priori (surcoût de gestion)

### ▪ Débit: 1, 4, 16 Mbit/s

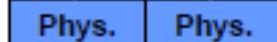
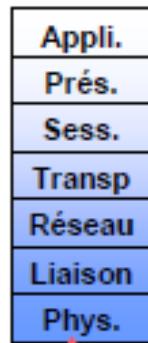
# 11. Interconnexion des réseaux

**But** : Permettre à des stations appartenant à différents LAN de communiquer.

**Pourquoi** ? Pour s'affranchir des limites imposées sur les LAN en termes de rayon de couverture et de nombre de stations et de répartir un LAN en plusieurs domaines de collisions distincts pour des raisons de sécurité, de performances ou d'administration.

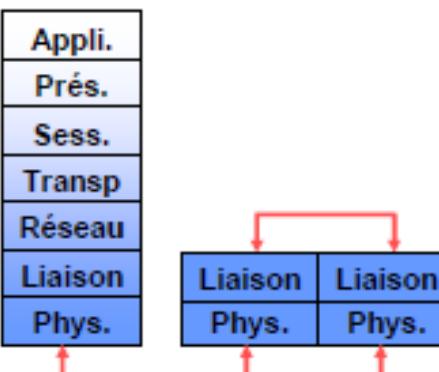


# 11. Interconnexion des réseaux

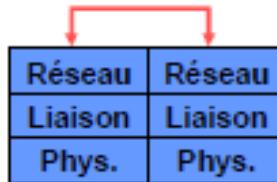


## Répéteur ou Hub

- Amplification du signal pour augmenter la taille du réseau éventuellement conversion
- Répétition du signal vers N ports

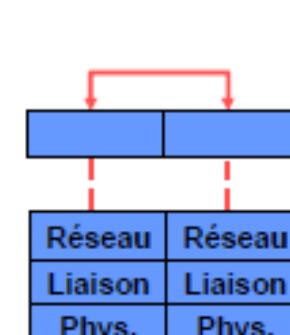


Pont ("Bridge"), commutateur  
Conversion de format des trames  
(couche 2)



## Routeur ("Router")

- Conversion de format des paquets et @
- Routage des paquets

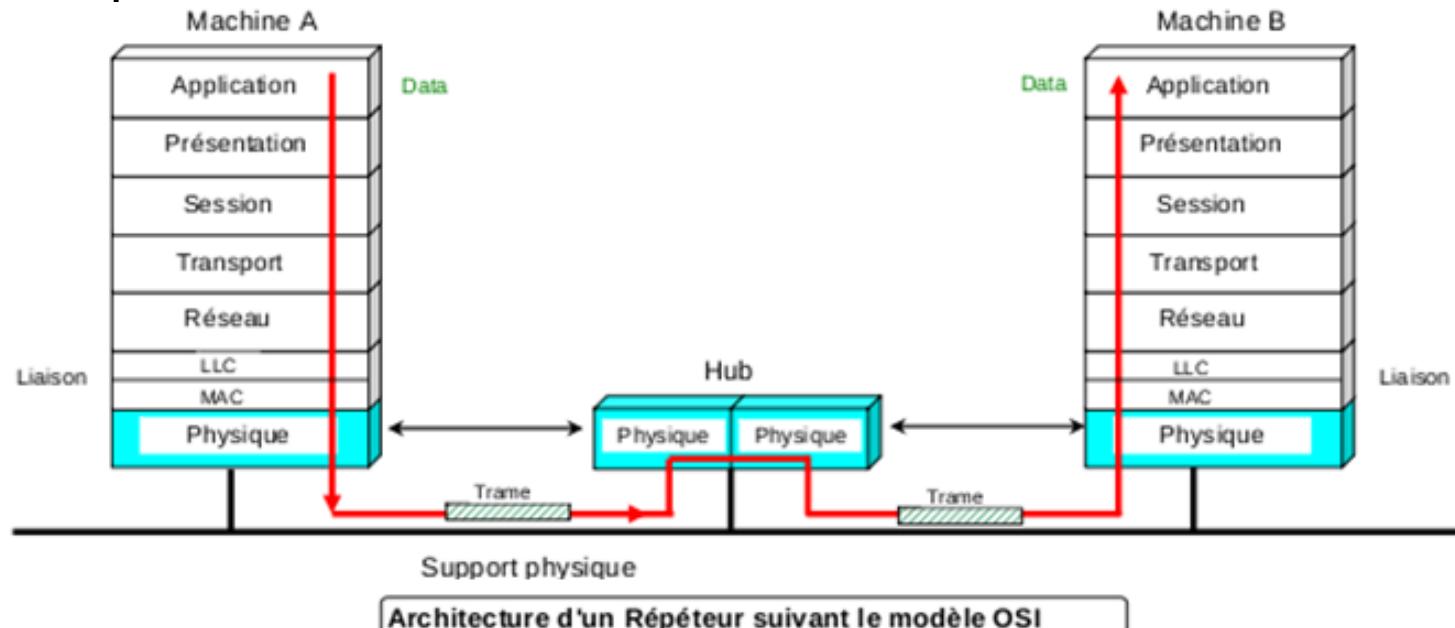


## Passerelle ("Gateway")

- Conversion de format de messages d'une des couches supérieures (4 à 7)

# 11. Interconnexion des réseaux

Un **répéteur** agit uniquement au niveau de la couche 1 du modèle OSI, c'est un "amplificateur de ligne" avec ses avantages et aussi l'inconvénient de transmettre le bruit sans discernement : il n'y a aucun filtrage sur le contenu. Il relie deux brins d'une même technologie en un seul LAN car les trames sont reproduites à l'identique. En 10Base5, l'usage d'un répéteur fait passer la limite des 500 m à 1000 m...



# 11. Interconnexion des réseaux

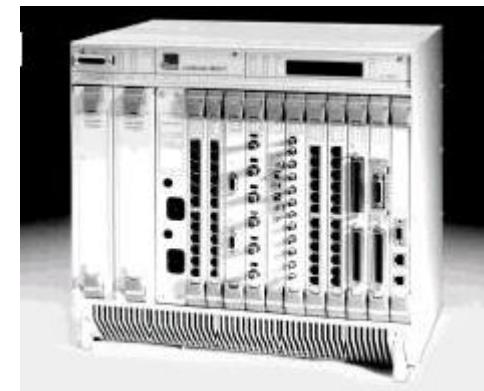
## Concentrateur (ou "HUB")

Un hub répète simplement les informations d'un port vers tous les autres ports.

Le Hub ne limite pas les collisions et n'améliore pas l'usage de la bande passante. Son seul intérêt est de permettre le branchement ou le débranchement des stations sans perturber le fonctionnement global du réseau.



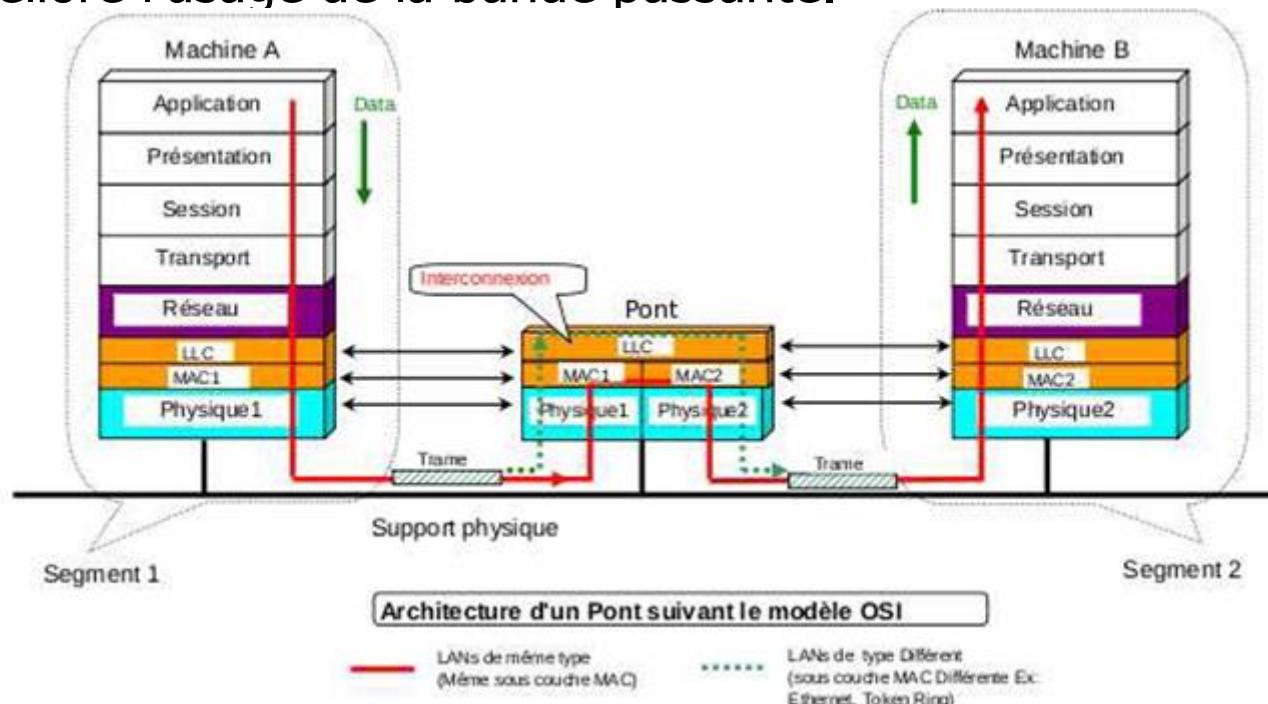
Mini hubs (Hewlett Packard)



Hub multi Protocole (3com)

# 11. Interconnexion des réseaux

La technologie CSMA/CD atteint vite ses limites quand le réseau est encombré. Une amélioration possible quand on ne peut pas changer de technologie (augmentation du débit) est d'utiliser un ou plusieurs **ponts** ("bridges") qui réduit le taux de collisions en réduisant le trafic inutile, donc améliore l'usage de la bande passante.



# 11. Interconnexion des réseaux

## Commutateurs (Switch)

Aligner des stations sur un même réseau local constitue une première étape simple et de faible coût pour un réseau local d'entreprise.

L'inconvénient d'une telle architecture est que le nombre de collisions croît très vite avec le trafic, d'où une baisse très sensible de la rapidité des échanges due à ce gaspillage de la bande passante.

Depuis plusieurs années est apparue une nouvelle technologie nommée "Intelligent Switching Hub" (ISH) – commutateur intelligent – qui utilise le concept de commutation parallèle.

Le switch établit une connexion entre un port d'entrée et un port de sortie en fonction des adresses MAC.

Un commutateur fonctionne par apprentissage pour établir sa carte des adresses mais il peut aussi travailler à partir d'une table préconfigurée



# 11. Interconnexion des réseaux

## Commutateurs (Switch)

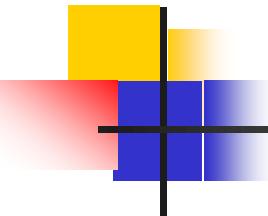
Un commutateur peut fonctionner par port (une seule station Ethernet par port) ou par segment (plusieurs stations Ethernet par port).

**Domaine de collision** : segment de réseau dans lequel toutes les machines partagent la même bande passante (plus il y a de stations, plus il y a de collisions)

- Equipement de niveau 2 (pont, switch) utilisé pour séparer les domaines de collision (analyse des adresses MAC qui évite la propagation des collisions)

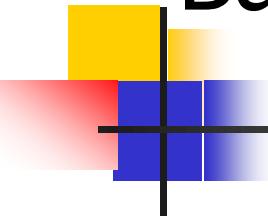
**Domaine de broadcast** : ensemble des éléments du réseau recevant le trafic de diffusion

- Equipement de niveau 3, routeur qui bloque les broadcasts



## **Chapitre -5- Principes des réseaux TCP/IP**

# Bases des réseaux TCP/IP

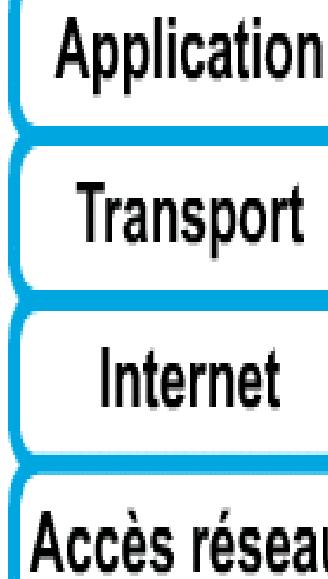


"TCP/IP" fait référence à une multitude de protocoles de communication. Il tient son nom de deux de ses protocoles: Le "Transmission Control Protocol" et le "Internet Protocol".

## Architecture TCP/IP

- Résultat de recherches conduites sur ARPANET, financés par DARPA (Department of Defence USA)
- Coeur de l'Internet
- Les protocoles sont indépendants des architectures matérielles et des systèmes d'exploitation.
- Le mode d'adressage est commun à tous les utilisateurs de TCP/IP quelle que soit la plate-forme qui l'utilise.
- La majeure partie des informations relatives à ces protocoles sont publiées dans les RFCs (Requests For Comments).

# Bases des réseaux TCP/IP



Contient la logique nécessaire au support d'applications usagers (ftp, telnet, http etc.) Chaque application requière un module différent

Sûreté de la transmission/réception (contrôle d'erreur, séquençage, contrôle de flux)

Fonctions de routage à travers des réseaux multiples. Implémenté aussi bien dans les systèmes terminaux que les routeurs

Couvre l'interface physique au réseau. Caractéristiques Mécaniques, électriques, fonctionnelles et procédurales du médium physique

# Les protocoles de l'architecture TCP/IP

## Niveau applicatif (La couche application)

- HTTP - HyperText Transport Protocol
- FTP - File Transfer Protocol
- TELNET - TELetypewriter Network Protocol
- SMTP - Simple Mail Transfer Protocol
- DNS - Domain Name System
- SNMP - Simple Network Management Protocol

## La couche transport : Protocoles de transport de données

- TCP (Transmission Control Protocol) : transfert fiable de données en mode connecté
- UDP (User DatagramProtocol) : transfert non garanti de données en mode non connecté

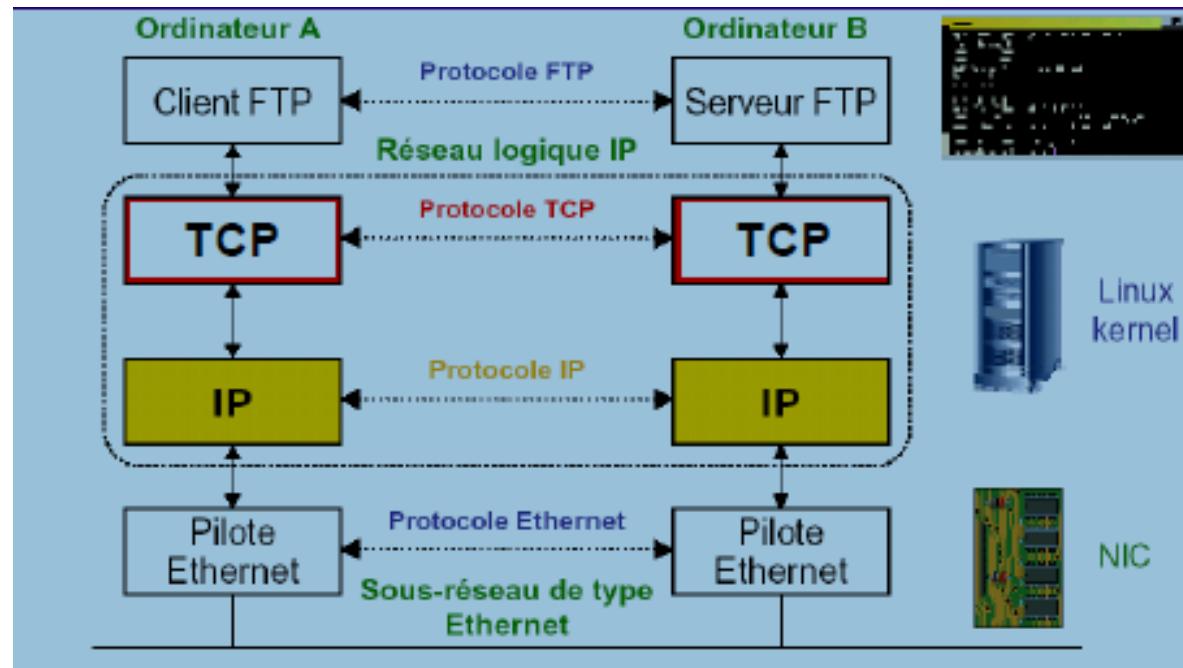
## La couche Réseau : Protocole IP et Protocoles de contrôle de l'Internet

- IP (Internet Protocol) : gère la circulation des paquets à travers le réseau en assurant leur routage.
- ICMP (Internet Control and error Message Protocol)
- ARP/RARP (Address Resolution Protocol)/(Reverse ARP)

# Concept de l'interconnexion

## Communications sans routeur

- Deux machines sur un même sous réseau

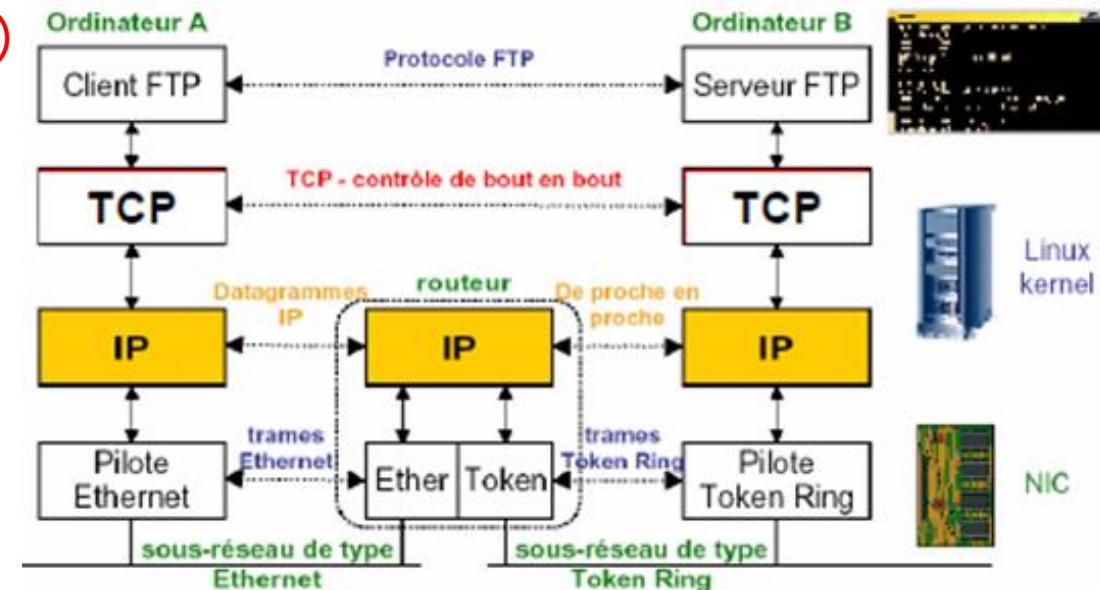


L'architecture TCP/IP permet de faire fonctionner un réseau local : par exemple sur un réseau Ethernet reliant un ordinateur client A qui interroge un serveur FTP

# Concept de l'interconnexion

## Communications avec routeur (s)

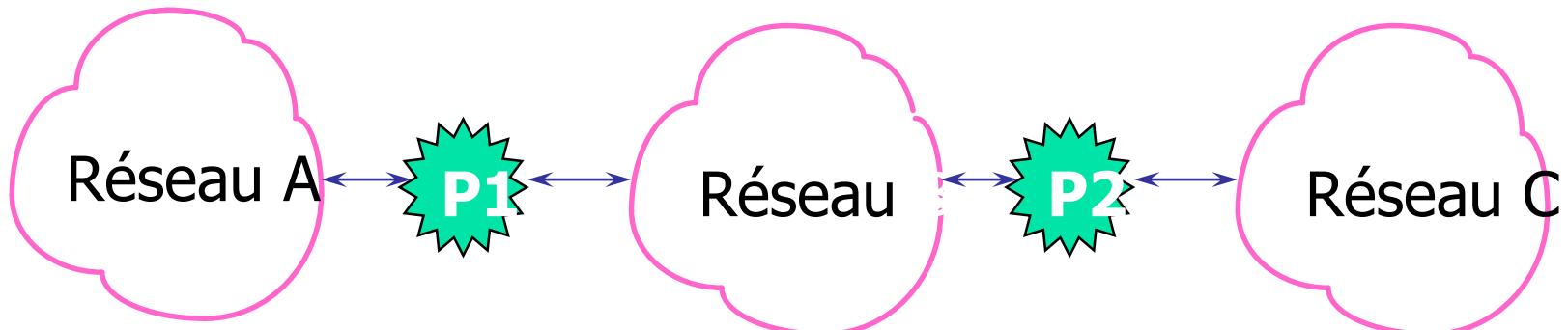
- Prise en compte de l'hétérogénéité



L'architecture TCP/IP permet surtout de constituer un Internet, c. a. d. une interconnexion de réseaux éventuellement hétérogènes comme illustré dans la figure. Ici les ordinateur A et B sont des systèmes terminaux et le routeur est un système intermédiaire. La remise du paquets nécessite l'utilisation de deux trames différentes, l'une du réseau Ethernet entre la machine A et le routeur, l'autre du réseau Token-Ring entre le routeur et la machine B.

# Concept de l'interconnexion

Communications avec routeur (s)

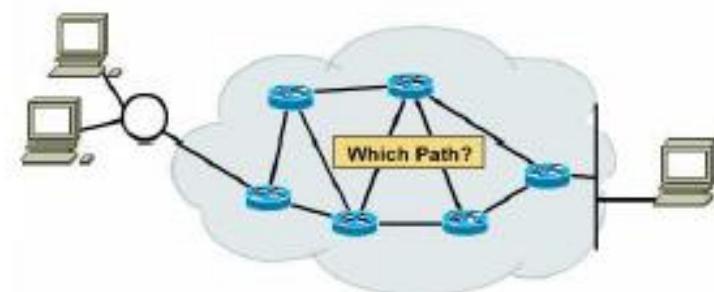


- Les données transitent depuis un réseau vers un autre réseau par des nœuds spécialisés appelés passerelles (*gateway*) ou routeurs (*router*).
- Chaque routeur a une vue « local » du réseau global.
- Exemple: le routeur p1 sait comment atteindre directement les réseaux A et B, mais pour atteindre le réseau C il envoie les données au routeur p2.

# Protocole IP (Internet Protocol)

## Caractéristiques du protocole IP

- Implémente la couche réseaux par rapport au modèle OSI.
- Définit l'adressage logique des machines ainsi que le routage des données entre les nœuds.
- C'est un protocole non fiable car il ne garanti pas la remise des données à la destination final (best effort).
- C'est un protocole sans connexion car il n'y a pas de circuit établi au préalable et les paquets sont acheminés indépendamment les uns des autres.
- Le protocole IP définit :
  - L'unité de donnée transférée dans les interconnexions (le paquet).
  - La fonction de routage.



# Protocole IP (le paquet)

Le paquet IP: L'unité de transfert de base dans un réseau Internet est le paquet qui est constituée d'un en-tête et d'un champ de données:

Le paquet est une suite d'éléments binaires dont on ne peut distinguer le début et la fin. Pour transporter un paquet, il faut l'encapsuler dans une trame. Adjonction de fonctions supplémentaires dans l'en-tête et la zone de fin de paquet : contrôle d'erreur, contrôle de flot, etc.

TCP/IP s'appuie sur les adresses physique, chaque carte Ethernet ou Token Ring a une adresse **unique** qui est imprimée dans le matériel.

L'adressage MAC est sur 6 octets, 48 bits.

L'adresse MAC est divisée en deux parties:

- les trois premiers octets désignent le constructeur(HP, Cisco, DEC, Sun, 3Com),
- les trois derniers désignent le numéro de carte.

Les adresses IP, adresses réseau, sont assignées par l'administrateur et sont configurées **logiquement** dans les équipements.

Deux grandes fonctionnalités à satisfaire:

Adressage et Routage.

HRD

Data

# Protocole IP (le paquet)



# Protocole IP (le paquet)

- **VERS** : numéro de version de protocole IP, (IPv4 ou IPv6).
- **HLEN** : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (sans d'options)
- **Type de service** : indique comment le paquet doit être géré: traitement normal, haute priorité, haut débit, haute fiabilité.
- **Longueur totale** : longueur totale du paquet (en-tête + données).
- **Identification, Flags, Fragment Offset** : informations utilisées par IP pour la reconstitution d'un paquet IP fragmenté.
- **IDENTIFICATION** : entier qui identifie le paquet initial (utilisé pour la reconstitution à partir des fragments qui ont tous la même valeur).
- **FLAGS** contient un bit appelé "do not fragment" (01X)
- un autre bit appelé "More fragments" (FLAGS = 001 signifie d'autres fragments à suivre) permet au destinataire final de reconstituer le paquet initial en identifiant les différents fragments (milieu ou fin du paquet initial).

# Protocole IP (le paquet)

- **Durée de vie** : Ce champ indique en second, la durée maximale de transit du paquet sur Internet. Chaque passerelle diminue la valeur du TTL d'au moins 1 avant de le router.
- **Protocole** : Ce champ identifie le protocole de niveau supérieur dont le message est porté par le champs données du datagramme :

6 : TCP

17 : UDP

1 : ICMP

- **Somme de contrôle de l'en-tête** : Ce champ permet de détecter les erreurs survenant dans l'en-tête du paquet, et par conséquent l'intégrité du paquet. Le total de contrôle d'IP porte sur l'en-tête du paquet et non sur les données véhiculées.

• **@IP source** : l'adresse IP de la machine source.

• **@IP destination** : l'adresse IP de la machine destinataire.

• **OPTIONS** : Le champ OPTIONS est facultatif et de longueur variable. Les options concernent essentiellement des fonctionnalités de mise au point. Une option est définie par un champ octet.

# Adressage IP

**But** : fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion.

Une machine doit être accessible aussi bien par des humains que par d'autres machines.

Une machine doit être identifiée par :

Un nom (mnémotechnique pour les utilisateurs), Nom d'hôte (Internet)  
serveur.stage.priv

Une adresse qui doit être un identificateur universel de la machine, Adresse IP  
(protocole IP) (V4 ou V6) 192.168.1.10

• Une route précisant comment la machine peut être atteinte.

**Solution** : Un adressage binaire assurant un routage efficace et qui utilisent:

• des noms pour identifier des machines (réalisée à un autre niveau que les protocoles de base)

## Les classes d'adressage

• Une adresse IPv4 est constituée de 32 bits dite « Internet address » ou "IP address" constituée d'une paire (net-id, host-id) où **net-id** identifie un réseau et **host-id** identifie une machine sur ce réseau.

# Adressage IP

## Structure d'une adresse IP



- **La partie réseau:** est un identifiant commun pour un groupe de machines connectées sur le même réseau physique et/ou logique.
- **La partie host:** identifie une machine donnée dans le réseau physique et/ou logique, identifié par l'identifiant réseau.

Cette paire est structure d'une manière à définir 5 classes d'adresses IP. Nous nous intéressons seulement aux classes A, B et C.

	0	7	15	23	31
Classe A	0	Net-Id		Host-id	
Classe B	0	7	15	23	31
Classe C	10	Net-Id		Host-id	
	0	7	15	23	31
	110		Net-Id		Host-id

# Adressage IP

Exemple d'IP des classes A, B, C

	1er octet	2ème octet	3ème octet	4ème octet
Classe A	10	70	123	40
Classe B	131	24	245	20
Classe C	192	168	12	34

# Adressage IP

## Notation décimale

L'interface utilisateur concernant les adresses IP consiste en la notation de quatre entiers décimaux séparés par un point, chaque entier représentant un octet de l'adresse IP :

10000000 00001010 00000010 00011110 est écrite :

128.10.2.30

Les adresses réseaux sont distribuées par un organisme international à but non lucratif : ICANN (Internet Corporation for Assigned Names and Numbers) puis décentralisé au niveau de chaque pays.

Commande ipconfig/ ifconfig.

# Adressage IP

## Adresses particulières:

- **Adresse réseau** : adresse IP dont la partie host-id ne comprend que des zéros : 191.20.0.0 désigne le réseau de classe B 191.20.
- **Adresse machine locale** : adresse IP dont le champ réseau (net-id) ne contient que des zéros: 0.0.1.2
- **Netid = 0 et hostid = 0** ( $\Rightarrow$  tout à zéro), l'adresse est utilisée au démarrage du système afin de connaître son adresse IP (DHCP).
- **Adresse de diffusion limitée** : Net-id = 1 et host-d = 1 ( $\Rightarrow$  tout à 1) : l'adresse constituée concerne uniquement le réseau physique associé. (255.255.255.255)
- **L'adresse de diffusion dirigée** : net-id est une adresse réseau spécifique et host-id = 1 (broadcast) la diffusion concerne toutes les machines situées sur le réseau spécifié : 192.20.255.255 désigne toutes les machines du réseau 192.20.
- **Adresse de boucle locale** : l'adresse réseau 127.0.0.1 (localhost) est réservée pour la désignation de la machine locale, c'est à dire la communication intra-machine. Elle permet de tester la pile TCP/IP.

# Adressage IP: Notion de masque

Le masque réseau est un entier sur 32 bits, constitué d'une suite de 1 suivi par une suite de 0.

Exemple

11111111 11111111 11111111 00000000

- Le masque sert à identifier l'adresse Réseau qui correspondant à une adresse IP donnée.
- En appliquant un **and** logique entre une adresse IP quelconque et le masque associé on obtient la partie réseau de l'adresse (l'adresse réseau).  
@ip-machine **AND** Masque = @network

Par exemple le masque associé a une adresse de classe A est:

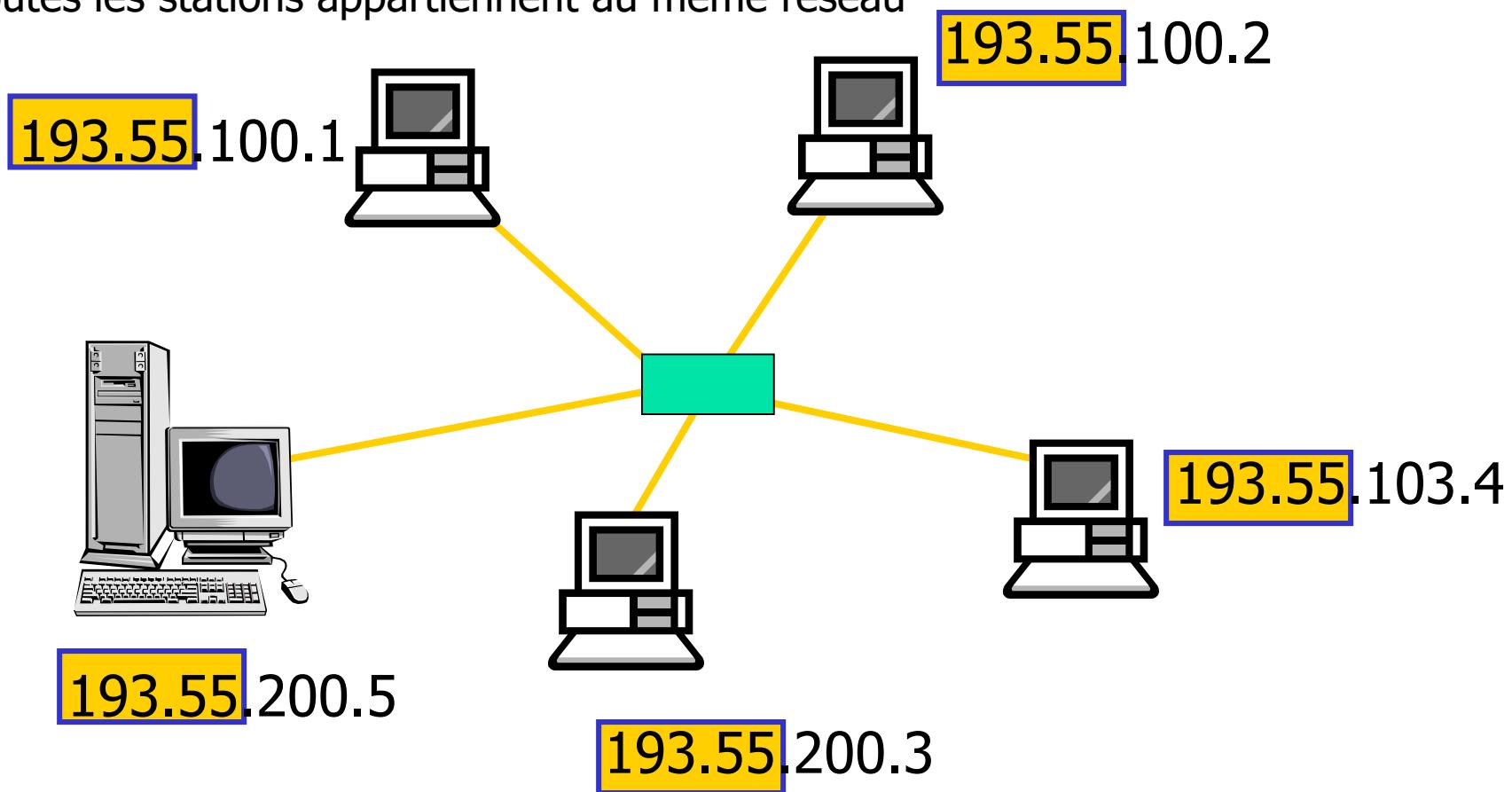
1111 1111 0000 0000 0000 0000 0000

Ce qui correspond en notation décimal : 255.0.0.0 /8.

# Adressage IP: Notion de masque

Si le masque est 255.255.0.0 :

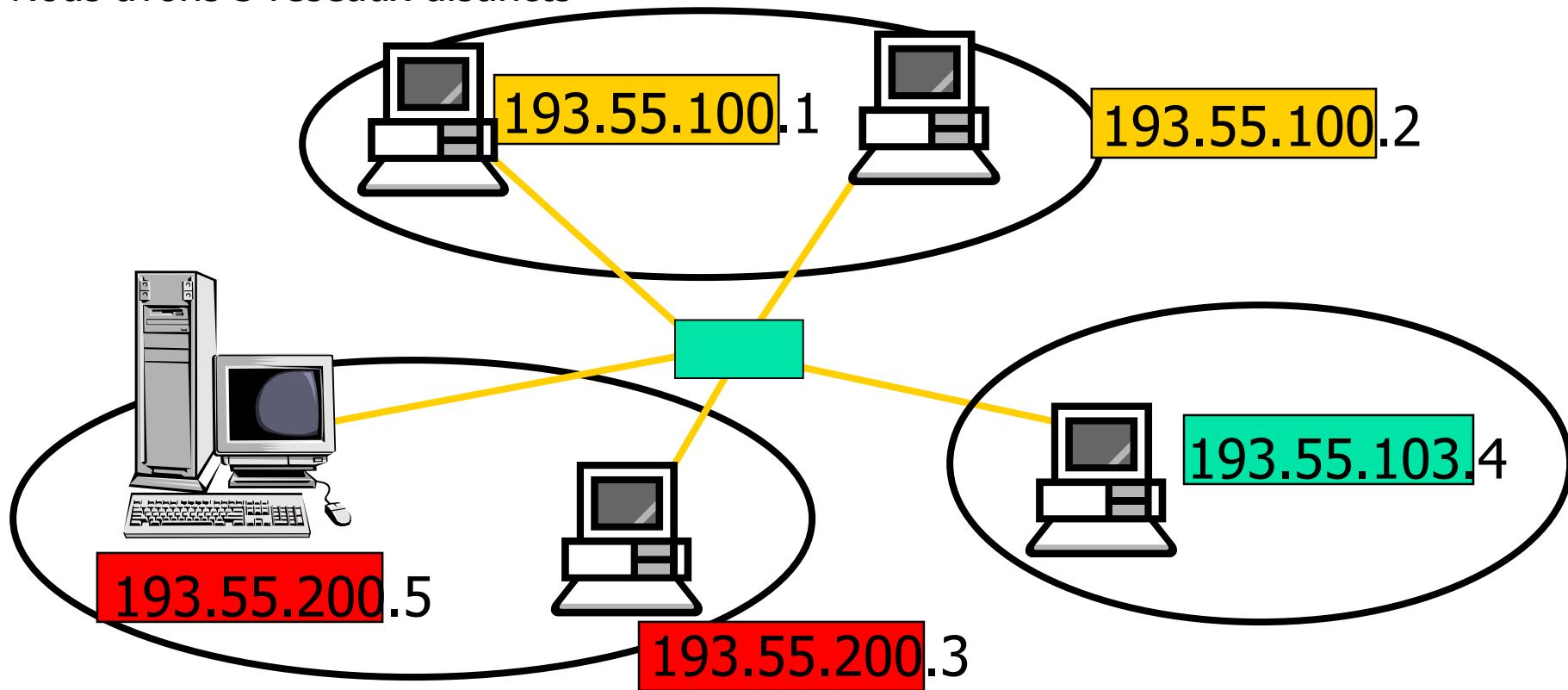
Toutes les stations appartiennent au même réseau



# Adressage IP: Notion de masque

Si le masque est 255.255.255.0 :

Nous avons 3 réseaux distincts



# Adressage IP: Notion de masque

Le masque par défaut associé à une adresse de classe B est:

1111 1111 1111 1111 0000 0000 0000 0000

Ce qui correspond en notation décimal : 255.255.0.0 /16.

Le masque par défaut associé à une adresse de classe C est:

1111 1111 1111 1111 1111 1111 0000 0000

Ce qui correspond en notation décimal : 255.255.255.0 /24..

En récapitulant, une @IP est constitué de 4 nombres correspondant à 2 parties

- Numéro du réseau (network ID=identifie le réseau)
- Numéro de la station (host ID=identifie une machine sur ce réseau)

Masque de sous-réseau permet de distinguer le numéro du réseau et le numéro de l'hôte.

# Adressage IP

## Comment interpréter une adresse IP

- 0.0.0.0 Un hôte inconnu (source)
- 255.255.255.255 Tous les hôtes (destination)
- 193.75.199.3 Hôte 3 du réseau 193.75.199
- 193.75.199.0 Hôte inconnu du réseau 193.75.199
- 193.75.199.255 Tous les hôtes du réseau 193.75.199
- 0.0.0.4 L'hôte 4 de ce réseau (source)
- 127.0.0.1 Cet hôte Loopback

# Limites de l'adressage IP classique

## Problèmes (fin des années 80)

- Problèmes d 'allocation des adresses:
  - 1- épuisement de la classe B :  
254 machines < sites << 64K machines
  - 2- utilisation rapide des classes C
  - 3- accroissement et explosion des tables de routages

## – Solutions =>

- Allouer exactement la quantité nécessaire
- sous adressage
- super adressage ou bien CIDR et adressage privé)
- Agrégation d'adresses dans les tables de routage

# Adressage IP: Subneting

Le subneting (sous adressage) est une extension du plan d'adressage initial. Devant la croissance du nombre de réseaux de l'Internet, il a été introduit afin de limiter la consommation d'adresses IP .

## Principes

- A l'intérieur d'une entité associée à une adresse IP de classe A, B ou C, plusieurs réseaux physiques partagent cette adresse IP.
- On dit alors que ces réseaux physiques sont des sous-réseaux (subnet) du réseau d'adresse IP initial.
- Le principe est qu'une adresse de réseau d'une classe A, B ou C peut être découpée en plusieurs sous-réseaux.

Réseau vu de l'extérieur:

Partie Réseau

Partie locale

- En interne, découpage en pseudo classes

Partie Réseau

Identifiant sous réseau

Identifiant host

# Adressage IP: Subneting

Avec le subnetting (sous adressage) une adresse IP comporte désormais 3 partie:

- l'identifiant réseau «Partie Réseau» (Net-Id) : il a la même signification que celui du plan d'adressage initial.
- l'identifiant du sous-réseau : identifie un segment ou un sous-réseaux.
- l'identifiant de la machine : identifie la machine sur le segment ou le sous-réseaux.
- La somme des longueurs de l'identifiant sous-réseau et l'identifiant de la machine doit toujours donner la longueur de la partie hôte dans l'adressage classique initiale.
- Les champs «sous Réseau» et «identifiant host» sont de taille variable.

# Adressage IP: Subneting

## Algorithme de calcul des sous-réseau:

- Déterminer le nombre de bits dans la partie sous-réseau qui permet d'avoir le nombre de sous réseaux voulu.
- Déterminer le nombre de bits dans la partie machine qui permet d'avoir le nombre de machines.
- Déterminer le masque qui va être utilisé pour ses sous-réseaux.
- Écrire sous forme binaire l'adresse IP initial.
- Écrire sous forme binaire le masque initial( par défaut).
- Écrire sous forme binaire le nouveau masque.
- Déduire les adresses des sous-réseaux en incrémentant la partie de sous-réseau dans l'adresse initial.
- Déduire l'adresse du broadcast en remplaçant par des 1 tous les bits de la partie machine de l'adresse IP.
- Enfin déduire les adresses utilisables.

# Adressage IP: Subnetting

## Exemple:

Nous voulons découper le réseau de classe C 192.168.64.0/24 en 8 réseaux de 30 machines pour chaque réseau. Le nombre de réseaux doit être une puissance de 2, or  $8=2^3$  donc nous avons 3 bits dans la partie sous-réseau.

- 1) Masque réseau par défaut 255.255.255.0

En notation binaire/décimal 255.255.255.00000000

On veut 8 sous réseaux, on utilise 3 bits de host qu'on va attribuer aux sous réseaux → masque sous réseau 255.255.255.11100000

255.255.255.224 ou /27

- 2) Les @IP des 8 sous réseaux:

@IP initiale 192.168.64.0 en notation binaire	192.168.64.00000000
---	---------------------

1 <sup>er</sup> sous réseau	192.168.64.00000000	192.168.64.0
-----------------------------	---------------------	--------------

2 <sup>ème</sup> sous réseau	192.168.64.00100000	192.168.64.32
------------------------------	---------------------	---------------

3 <sup>ème</sup> sous réseau	192.168.64.01000000	192.168.64.64
------------------------------	---------------------	---------------

4 <sup>ème</sup> sous réseau	192.168.64.01100000	192.168.64.96
------------------------------	---------------------	---------------

8 <sup>ème</sup> sous réseau	192.168.64.11100000	192.168.64.224
------------------------------	---------------------	----------------

# Adressage IP: Subnetting

## Exemple (suite):

- 3) Les @IP du broadcast:

1 <sup>er</sup> sous réseau	192.168.64. <b>000</b> 11111	192.168.64.31
2 <sup>ème</sup> sous réseau	192.168.64. <b>001</b> 11111	192.168.64.63
3 <sup>ème</sup> sous réseau	192.168.64. <b>010</b> 11111	192.168.64.95
4 <sup>ème</sup> sous réseau	192.168.64. <b>011</b> 11111	192.168.64.127
⋮	⋮	⋮
8 <sup>ème</sup> sous réseau	192.168.64. <b>111</b> 11111	192.168.64.255

- 4) Les adresses utilisables: nous avons 5 bits dans la partie hôte. Le nombre de machines doit être une puissance de 2,  $32 = 2^5$ ,  $32-2=30$  @ dans chaque sous réseau

1 <sup>er</sup> sous réseau	192.168.64. <b>1</b>	-	1 192.168.64. <b>30</b>
2 <sup>ème</sup> sous réseau	192.168.64. <b>33</b>	-	192.168.64. <b>62</b>
3 <sup>ème</sup> sous réseau	192.168.64. <b>65</b>	-	192.168.64. <b>94</b>
4 <sup>ème</sup> sous réseau	192.168.64. <b>97</b>	-	192.168.64. <b>126</b>
⋮	⋮	⋮	⋮
8 <sup>ème</sup> sous réseau	192.168.64. <b>225</b>	-	192.168.64. <b>254</b>

# Adressage IP: Subneting

Adresse réseau	Adresse broadcast	Adresses utilisable	
192.168.64. 000 00000 (192.168.64.0)	192.168.64.00011111 (192.168.64.31)	192.168.64.0000001 192.168.64.1	192.168.64.0001110 192.168.64.30
192.168.64. 001 00000 (192.168.64.32)	192.168.64.00111111 (192.168.64.63)	192.168.64.0010001 192.168.64.33	192.168.64.0011110 192.168.64.62
192.168.64. 010 00000 (192.168.64.64)	192.168.64.01011111 (192.168.64.95)	192.168.64.0100001 192.168.64.65	192.168.64.0101110 192.168.64.94
192.168.64. 011 00000 (192.168.64.96)	192.168.64.01111111 (192.168.64.127)	192.168.64.0110001 192.168.64.97	192.168.64.0111110 192.168.64.126
192.168.64. 100 00000 (192.168.64.128)	192.168.64.10011111 (192.168.64.159)	192.168.64.1000001 192.168.64.129	192.168.64.1001110 192.168.64.158
192.168.64. 101 00000 (192.168.64.160)	192.168.64.10111111 (192.168.64.191)	192.168.64.1010001 192.168.64.161	192.168.64.1011110 192.168.64.190
192.168.64. 110 00000 (192.168.64.192)	192.168.64.11011111 (192.168.64.223)	192.168.64.1100001 192.168.64.193	192.168.64.1101110 192.168.64.222
192.168.64. 111 00000 (192.168.64.224)	192.168.64.11111111 (192.168.64.255)	192.168.64.1110001 192.168.64.225	192.168.64.1111110 192.168.64.254

# Adressage IP: CIDR

CIDR: Classless Inter Domain Routing

## Le besoin:

- Au début de l'Internet, Les adresses IP allouées pour les Grands FAI et les grandes firmes étaient des adresses de classe B.
- Au début des années 90 ce types d'adresses commençaient à devenir rares, et les adresses de classe C étaient insuffisantes pour ce type d'organisations.

## La solution:

- L'introduction par l'IETF de la notion de CIDR RFC 1338-1518-1519. Ca consiste à allouer exactement le nombre de classes C nécessaires pour un organisme donné. Les adresses de classes C doivent être contiguës, en parle alors de super réseaux.

Par exemple les adresses de classe C qui commencent de 192.168.64.0 jusqu'à 192.168.95.0 forment un seul bloc d'adresses de 32 classes C contiguës.

On note ce bloc par 192.168.64.0/19 car le nombre de bits commun pour toutes les classes d'adresse qui forment ce bloc est 19.

Un réseau de 4 classe C consécutif est souvent appelé « slash 22 ou /22».

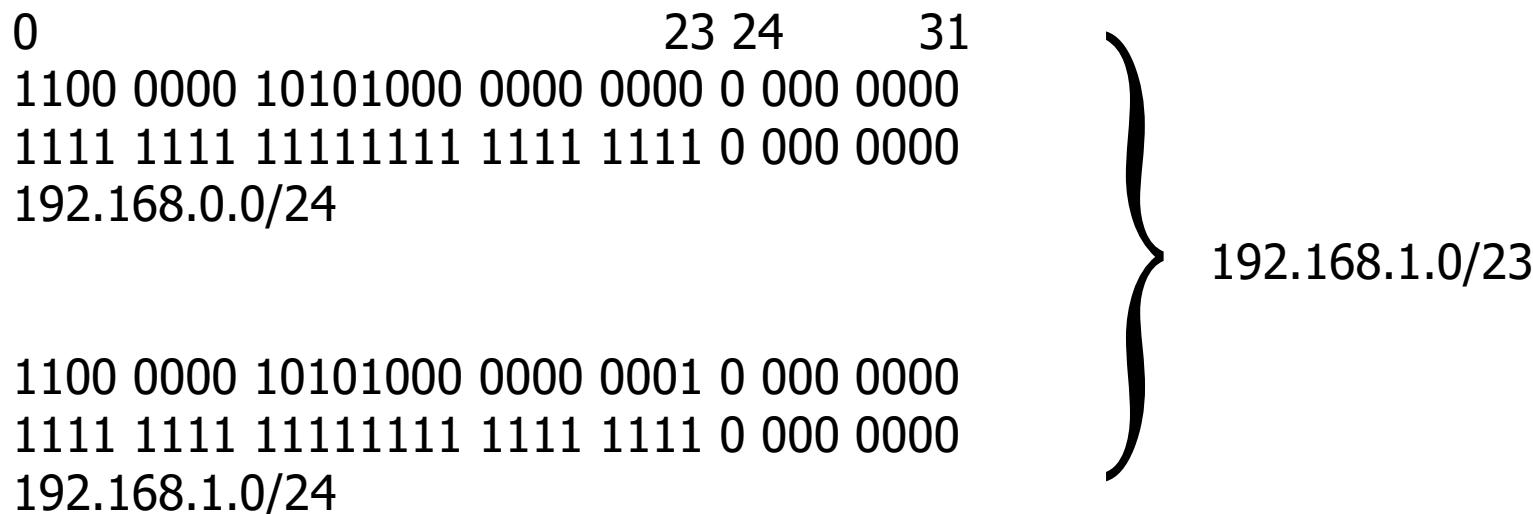
# Adressage IP: CIDR

Au niveau des routeurs une seule entrée dans la table de routage désigne tout le bloc d'adresses.

On parle alors d'agrégation des adresses, et ça représente l'avantage de soulager la table de routage au niveau des routeurs.

Exemple 1:

- Le bloc 192.168.0.0/23 permet d'assigner 2 classes C à l'utilisateur.
- 192.168.0.0/23



# Adressage IP: CIDR

Exemple 2:

Le bloc 193.194.64.0/19 regroupe les classes adresses allant de 193.194.64.0 jusqu'à 193.194.95.0

0        8        16    19        24        31

1100 0001 1100 0010 010 0 0000 0000 0000 : 193.194.64.0

1111 1111 1111 1111 **111** 0 0000 0000 0000 : 255.255.224.0

1100 0001 1100 0010 **010** 0 0000 0000 0000 : 193.194.64.0

1100 0001 1100 0010 010 0 0001 0000 0000 : 193.194.65.0

1100 0001 1100 0010 010 0 0010 0000 0000 : 193.194.66.0

1100 0001 1100 0010 010 0 0011 0000 0000 : 193.194.67.0

1100 0001 1100 0010 010 0 0100 0000 0000 : 193.194.68.0

1100 0001 1100 0010 010 0 0101 0000 0000 : 193.194.69.0

⋮

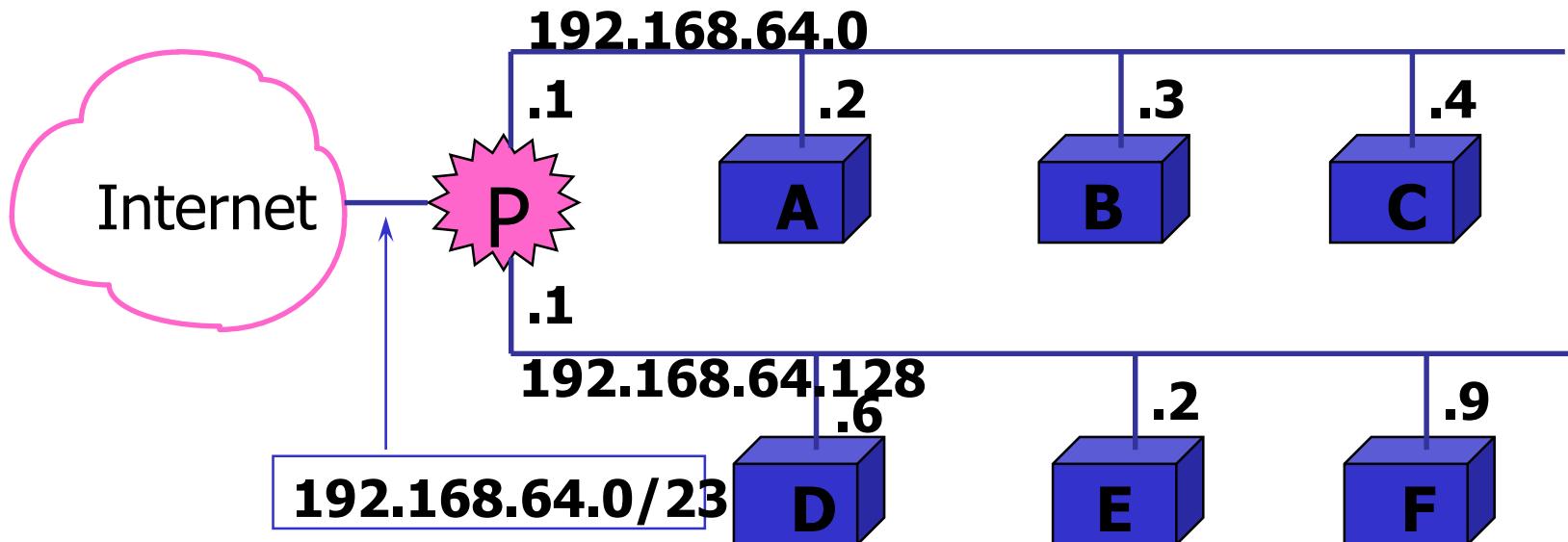
1100 0001 1100 0010 010 1 1111 0000 0000 : 193.194.95.0

} 193.194.64/19

# Adressage IP: CIDR

CIDR: un exemple pratique

Les réseaux 192.168.64.0 et 192.168.64.128 sont notés seulement avec le Net-Id, les machines seulement avec le Host-id ;



Un site avec deux réseaux physiques utilisant le super adressage de manière à ce que ses deux réseaux soient couverts par une seule adresse IP.

La passerelle P accepte tout le trafic destiné au réseau 193.194.64.0/23 et sélectionne le sous-réseau en fonction du troisième octet de l'adresse destination.

# Protocole DHCP

L'adresse IP de chaque machine est gérée par l'administrateur réseau.

- Il existe deux possibilités pour faire cela :
  - fixer une valeur à chacun des postes
  - utiliser un serveur d'adresses IP (DHCP)

Des protocoles (ARP et RARP) vont ensuite convertir l'adresse logique (IP) en adresse physique (MAC) et réciproquement

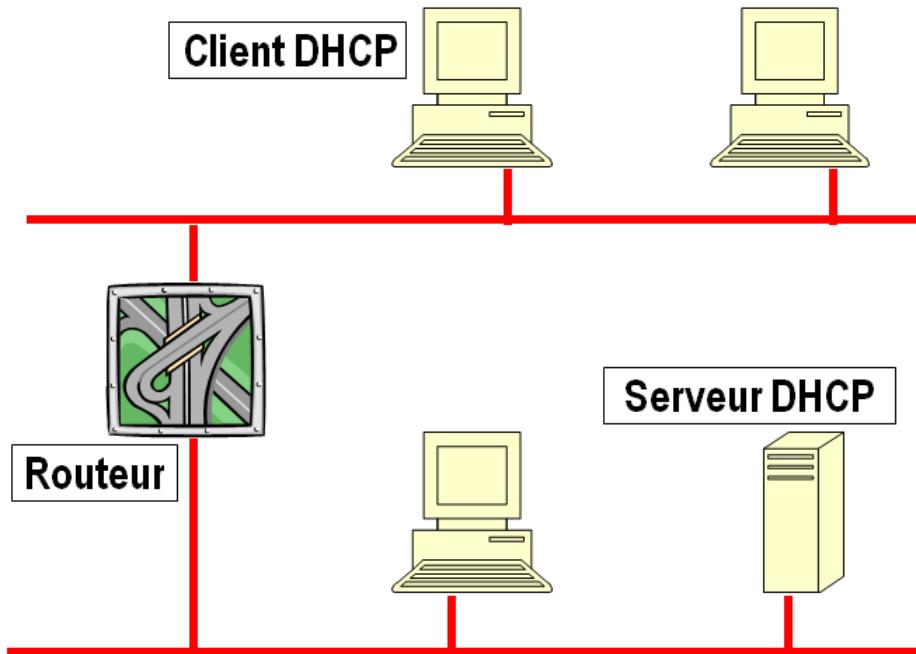
**DHCP: Protocole de Configuration Dynamique des Hôtes**

Les adresses sont allouées dynamiquement à partir d'un groupe lorsqu'un ordinateur demande l'accès au réseau.

- Simplifie la distribution des adresses IP
- Permet à un réseau de supporter plus d'utilisateurs de TCP/IP qu'il n'y a d'adresses IP.

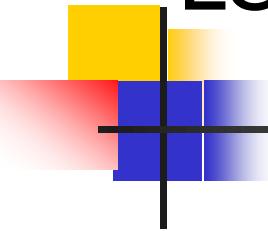
# Protocole DHCP

Comment travaille DHCP



- 1) Le client émet un message de découverte qui est envoyé vers le serveur DHCP sur le réseau.
- 2) Le serveur DHCP répond en offrant une adresse IP.
- 3) Le client sélectionne une des adresses IP et envoie une demande d'utilisation de cette adresse au serveur DHCP.
- 4) Le serveur DHCP accorde réception de la demande et accorde l'adresse en bail.
- 5) Le client utilise l'adresse pour se connecter au réseau.

# Le routage des paquets



Le routage est le processus permettant à un paquet d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur. Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le paquet.

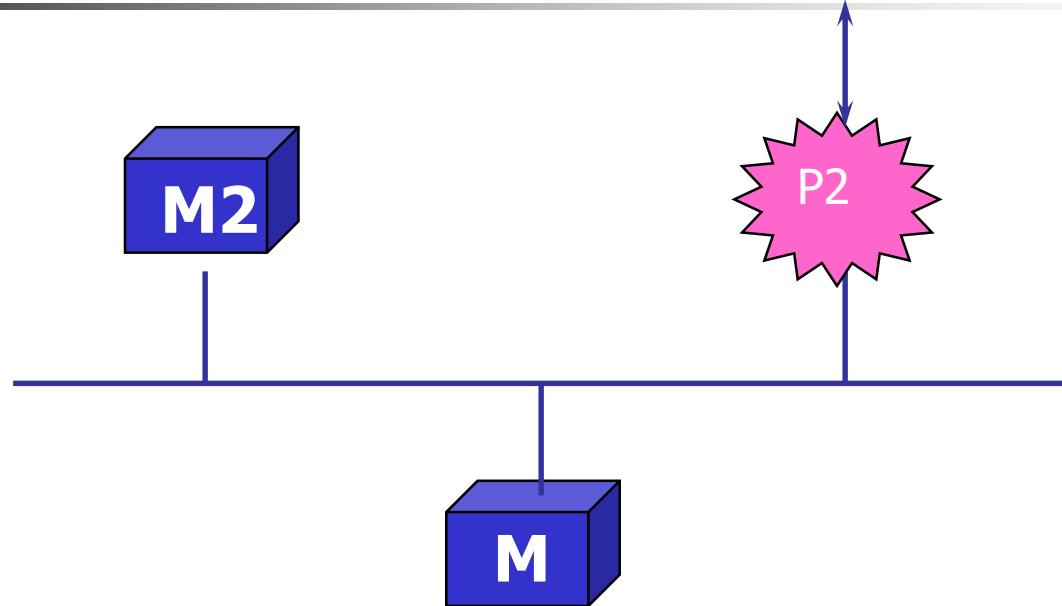
Les routeurs forment une structure coopérative de telle manière qu'un paquet transite de passerelle en passerelle jusqu'à ce que l'une d'entre elles le délivre à son destinataire.

Un routeur possède deux ou plusieurs connexions réseaux tandis qu'une machine possède généralement qu'une seule connexion.

Les Machines et routeurs participent au routage :

- les machines doivent déterminer si le paquet doit être délivré sur le réseau physique sur lequel elles sont connectées (routage direct) ou bien si le paquet doit être acheminé vers une passerelle; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée.
- les passerelles effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.

# Le routage des paquets



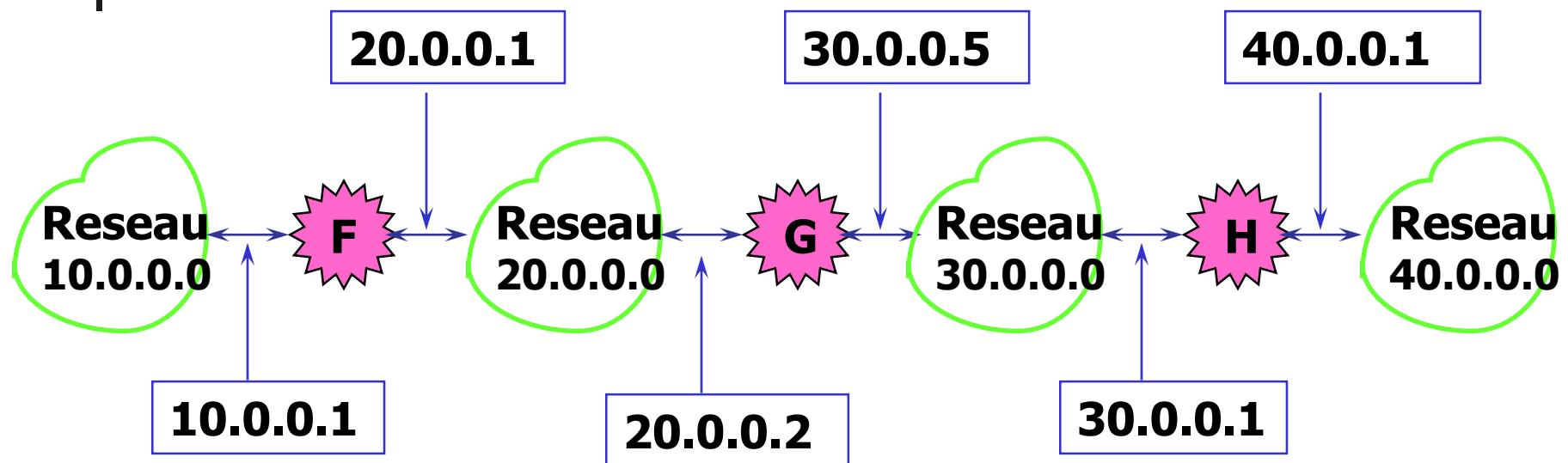
- **Le routage directe** : consiste à remettre les paquets directement à la destination lorsque celle-ci est connectée au même réseau physique.
- **Le routage indirecte** : repose sur une table de routage IP, présente sur toute machine et passerelle, indiquant la manière d'atteindre un ensemble de destinations.

# Le routage : La route par défaut

- La route par défaut est l'adresse d'un routeur à qui on va remettre les paquets lorsque aucune entrée dans la table de routage n'indique la destination voulue.
- Elle est utilisée par les machines pour pouvoir accéder à tous les réseaux de l'Internet.
- Utilisé également par les routeurs lorsque ceux-ci ne possèdent qu'un seul connexion vers Internet.
- Les tables de routage IP, renseignent seulement les adresses réseaux et non pas les adresses machines.
- Typiquement, une table de routage contient des couples (R, P) où R est l'adresse IP d'un réseau destination et P est l'adresse IP de la passerelle correspondant au prochain saut dans le cheminement vers le réseau destinataire.
- La passerelle ne connaît pas le chemin complet pour atteindre la destination.

Commande route print.

# Le routage : La table de routage



R	P
20.0.0.0	direct
30.0.0.0	direct
10.0.0.0	20.0.0.1
40.0.0.0	30.0.0.1

Table de routage de G

# Fin du cours

