

# Maintenance et mise en œuvre des réseaux TCP-IP



## OBJECTIFS

- 🌐 Comprendre l'organisation d'un réseau local sous TCP-IP.
- 🌐 Identifier le rôle de chaque composant pour maintenir un réseau industriel sous le protocole TCP-IP.

## METHODE PEDAGOGIQUE

- 🌐 Durant le stage, de nombreux travaux pratiques aborderont la configuration, la mise en œuvre et l'exploitation des Réseaux faisant appel au protocole TCP-IP.
- 🌐 50% théorique, 25% travaux dirigés ,25% de travaux pratiques.

## PREREQUIS

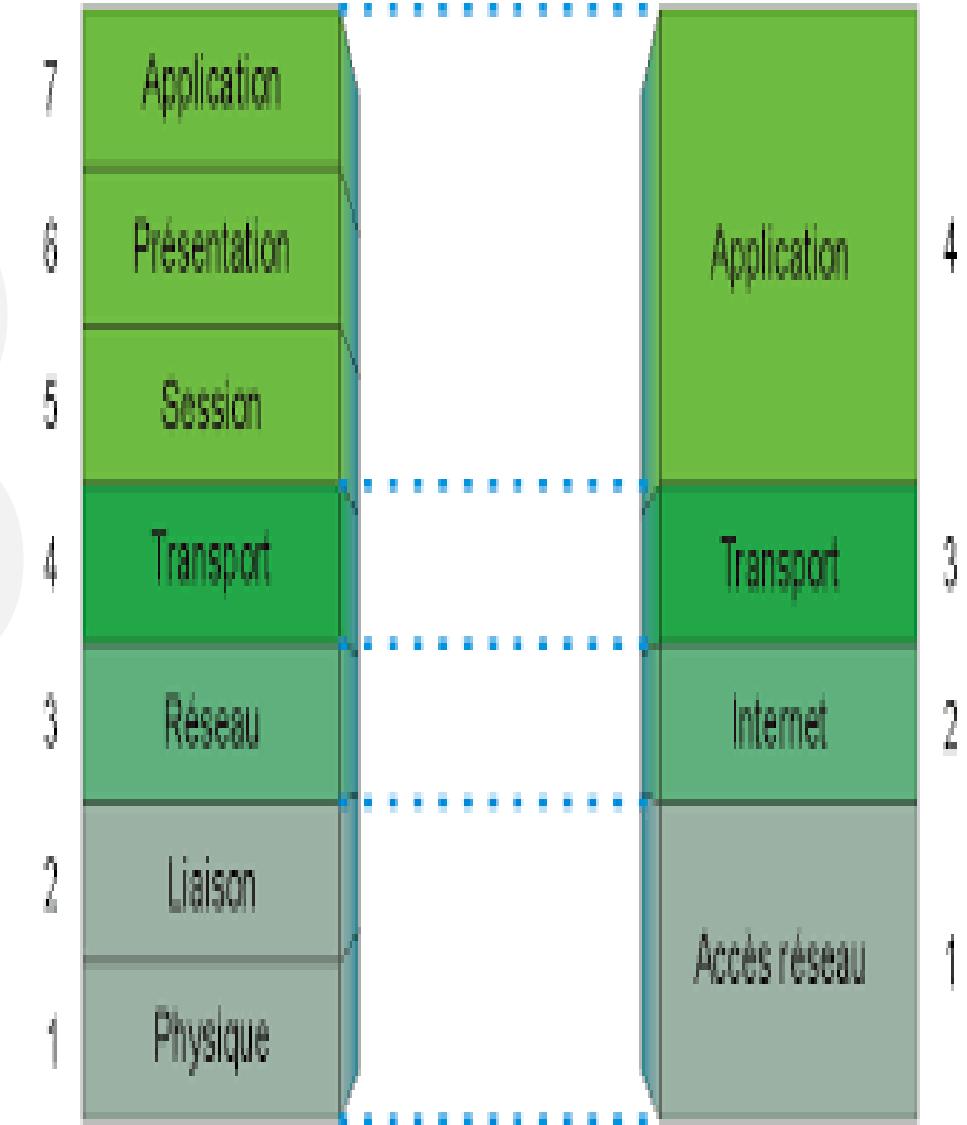
- 🌐 Connaissances de base de Windows, base calculatoire, binaire, .

## PUBLIC

- 🌐 Toute personne (maintenance, production, travaux neufs,...) impliquée dans la configuration et la maintenance des réseaux permettant d'interconnecter des PC et des systèmes industriels (API, Analyseur, ...).

# TABLE DES MATIERES

- 🌐 **Définition**
- 🌐 **Classification des RESEAUX**
- 🌐 **Modèle OSI & TCP/IP**
- 🌐 **MODELE TCP/IP**
- 🌐 **CARACTERISATION DES RESEAUX**
- 🌐 **COUCHE 1: physique**
- 🌐 **COUCHE 2: Liaison de données**
- 🌐 **Couche 3 : Réseau**
- 🌐 **Couche 4 : Transport**
- 🌐 **Couche 5 : Session**
- 🌐 **Couche 6 : Présentation**
- 🌐 **Couche 7 : Application**



# Classification des RESEAUX ➔

# Qu'est ce qu'un réseau de communication?

## Un ensemble des ressources:

- **Matériels** (modems, routeurs, commutateurs, câblage, cartes, ...)
- **Logiciels** (procédures, règles, protocoles, systèmes d'exploitation, ...)
- **Associés** à la transmission et l'échange d'information entre différentes entités (ordinateurs, individus, périphériques, processus, ...).

Les réseaux font l'objet d'un certain nombres de spécifications et de normes pour garantir leurs interfonctionnements.

.B



# Classification des RESEAUX(1/10)

## Type d'informations :

Les **réseaux de communications** peuvent donc être classés en fonction du type d'informations transportées et de la nature des entités impliquées. On distingue ainsi trois principales catégories de réseaux :

-  **Les réseaux de télécommunications:** réseau de télévision ;réseau informatique ;réseau de téléphonie mobile ; réseau téléphonique commuté ;
-  **Les réseaux de télédiffusion:** par satellites ou hertziens exemple TNT sonore
-  **Les réseaux Téléinformatiques ou réseau d'ordinateur**

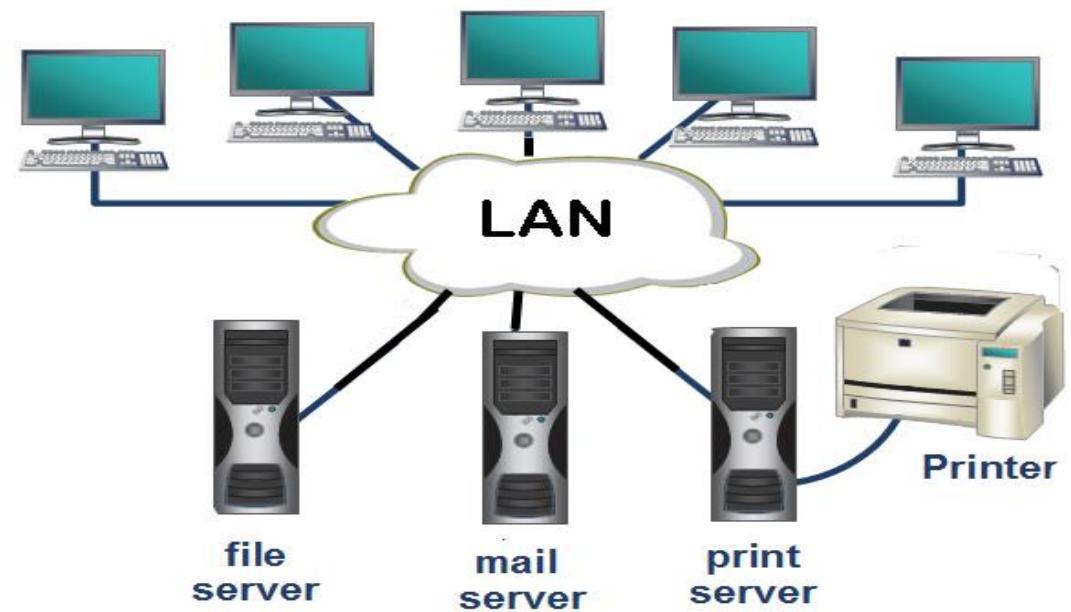
.B



# Classification des RESEAUX(2/10)

## LAN : Local Area Network

- ▣ **1 seule site**
- ▣ Couvrent une région géographique limitée,
- ▣ Permettent un accès multiple aux médias à large bande,
- ▣ Ils assurent une connectivité continue aux services locaux, (Internet, messagerie, etc.)
- ▣ Ils relient physiquement des unités Adjacentes.
- ▣ **Exemples:** école, laboratoire informatique,



.B



# Classification des RESEAUX(3/10)



## LAN : Local Area Network:2 types

### RESEAUX EGAL A EGAL (PEER TO PEER)

Les stations de travail munies tous du même logiciel réseau, peuvent partager ses ressources et gèrent elle-même sa sécurité. Dans cette configuration un serveur centralisé n'est pas requis.

-  Faible coût, pas de panne générale, facile à installer et à utiliser.
-  Difficulté de maintenir une sécurité, nombre de station limite, lent.

Exemples : Emule, BitTorrent, MTorrent

.B



# Classification des RESEAUX(4/10)



## LAN : Local Area Network:2 types

### **RESEAUX CLIENT-SERVEUR**

le serveur utilise des logiciels réseaux spéciaux avec une sécurité renforcée. Les ressources sur chaque station est non partageable et elles peuvent communiquer avec un ordinateur hôtes.

 Rapidité, sécurité, extension possible, excellente outils de gestion.

 Matériels coûteux, système d'exploitation chère, difficile à installer.

Exemples : consultation de pages sur un site web

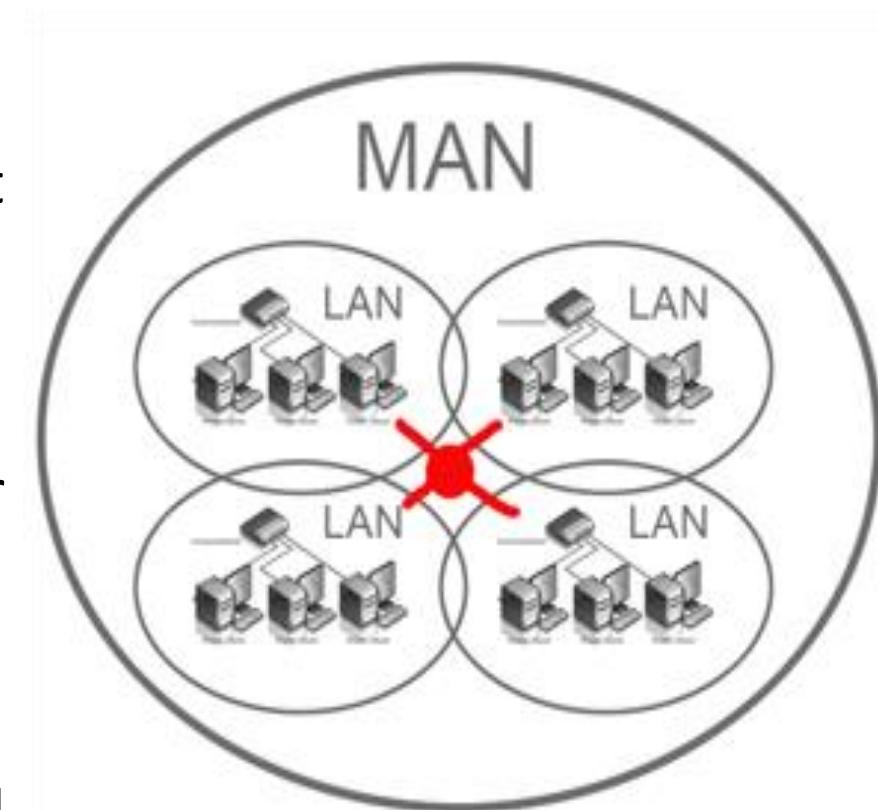
.B



# Classification des RESEAUX(5/10)

## MAN: Réseaux Métropolitain Area Network

- Interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres)
  
- Permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local,
  
- Formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).



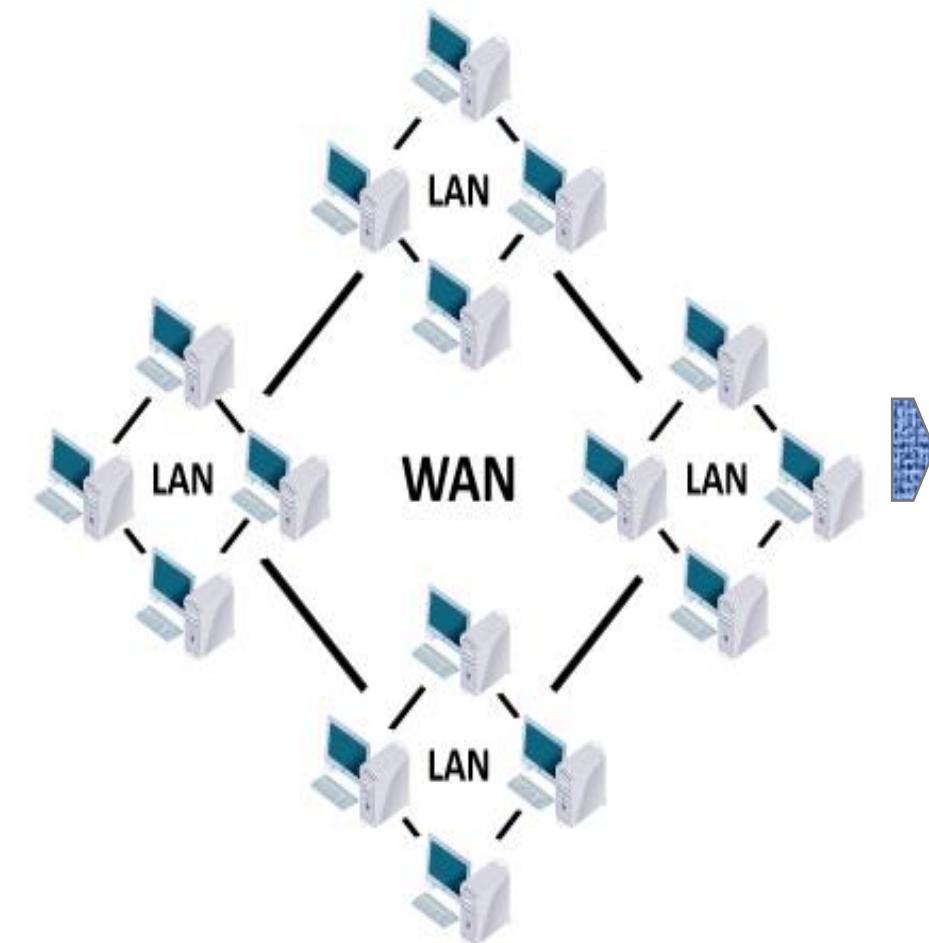
.B



# Classification des RESEAUX(6/10)

## WAN: Wide Area Network

- 🟡 Couvrent une vaste zone géographique,
- 🟡 Permettent l'accès par des interfaces séries plus lentes,
- 🟡 Assurent une connectivité pouvant être continue ou intermittente,
- 🟡 Relient des unités dispersées à une échelle planétaire.



.B



# Classification des RESEAUX(7/10)

## SAN :Storage Area Network

- 💡 Pour **désengorger le réseau de l'entreprise**, ce système a été inventé sous forme de réseau secondaire intégralement dédié au stockage,
- 💡 C'est un **réseau physique en fibre optique** ( Fibre Channel ou FC), dont le but est de permettre la mise en relation de serveurs avec des baies de disques,
- 💡 Il s'agit de dissocier le stockage des serveurs et de développer un réseau secondaire en parallèle, réseau exclusivement réservé à cette opération, ce qui permettra de désengorger le réseau local.
- 💡 Les sauvegardes se font par blocs de données, ce qui accélère la vitesse.
-  La Qualité de service (Qos) , La disponibilité, L'hétérogénéité, performances variables.
-  Le déploiement est souvent complexe.

.B



# Classification des RESEAUX(8/10)

## NAS :Network attached storage

- 💡 Le stockage NAS désigne la ressource de stockage qui est directement connectée au réseau Ethernet de l'entreprise.
- 💡 Les solutions NAS sont typiquement configurées comme des **serveurs de fichiers** accédés par des stations de travail et des serveurs au travers d'un **protocole réseau comme le TCP/IP**, et des **applications comme le NFS (network File System) ou CIFS (Common Internet File System)** pour l'accès aux fichiers.
- 😊 Administration simplifié, une interface WEB accessible , gestion des groupes d'utilisateurs, un coût très faible par rapport au SAN.
- 😢 le stockage NAS ne peut envoyer que des fichiers, et non des blocs de données,



.B



# Classification des RESEAUX(9/10)

## VPN :Virtual Private Network

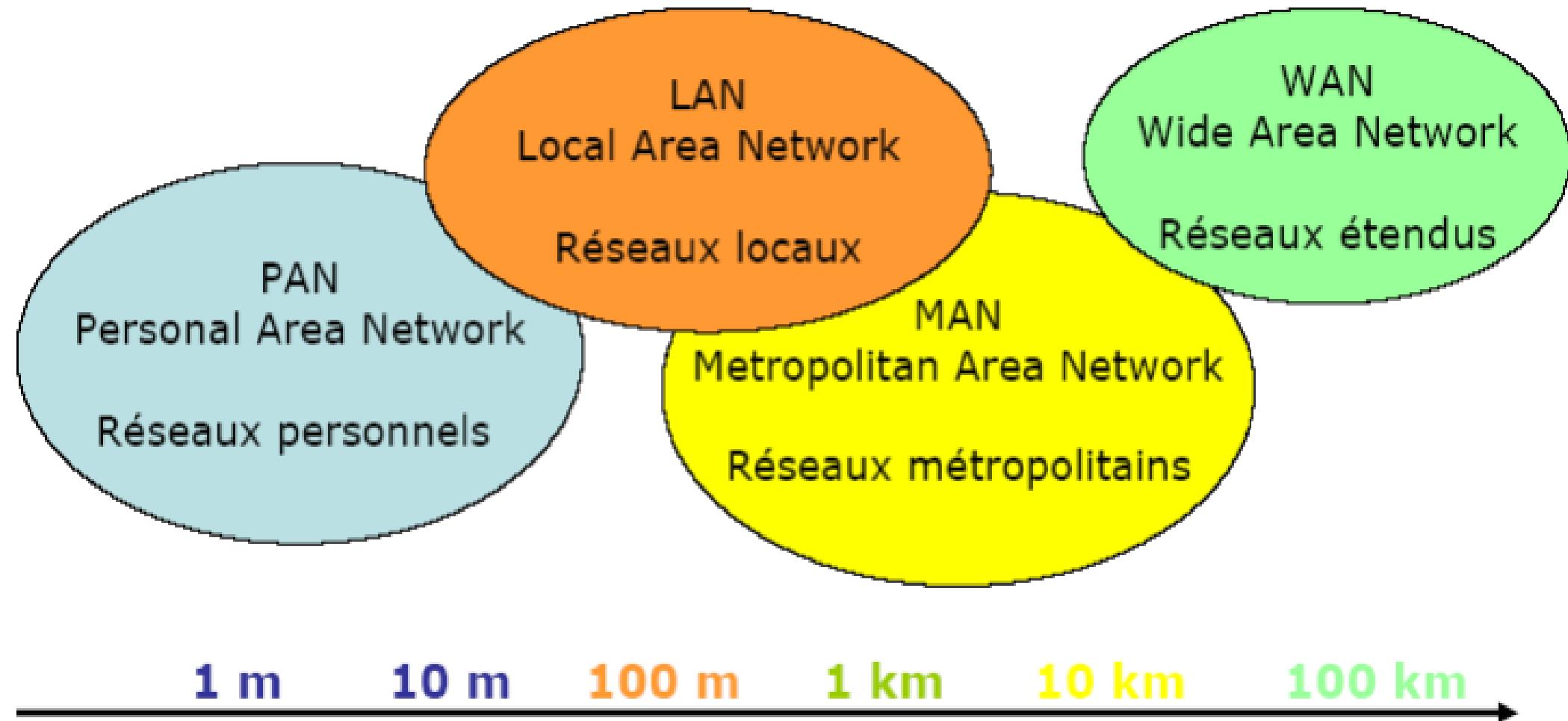
- 💡 Un réseau privé qui est construit dans une infrastructure de réseau public tel qu'Internet.
  
- 💡 **Extranet** : c'est un réseau privée (VPN) mais pas interne à une entreprise ouvert à des partenaires: clients, fournisseurs, filiale.
  
- 💡 **Intranet**: c'est aussi un réseau privé (VPN), mais à usage 100% interne de l'entreprise (réseau local interne) accessible avec ou sans connexion à internet .
  
- 💡 Par Internet, un tunnel sécurisé peut être mis en place entre le PC de l'utilisateur et d'un routeur VPN se trouvant au siège social de l'entreprise, afin que celui-ci accède de chez lui au réseau de son entreprise.

.B



# Classification des RESEAUX(10/10)

## RESUME:



.B



# Modèle OSI & TCP/IP



# ORGANISMES DE NORMALISATION (1/2)

## Les Organismes Internationaux :

Les organismes de normalisation internationaux cités ci-dessous sont sous l'égide de l'ONU et sont les plus actifs dans le domaine des réseaux et des télécommunications.

- **OSI** (Organisation Internationale de Standardisation) ou ISO (International Organisation for Standardisation);
- **UIT** (Union Internationale des Télécommunications) anciennement CCITT (Comité Consultatif International Télégraphique et Téléphonique).

.B



# ORGANISMES DE NORMALISATION (2/2)

## Les Organismes Multinationaux :

A ces organismes internationaux, s'ajoutent encore des organismes de différents continents comme l'Europe et les Etats-Unis :

- **IETF** (Internet Engineering Task Force);
- **IEEE** (Institute of Engineers in Electronic & Electrotechnic);
- **ETSI** European Telecommunication Standardization Institute);
- **EBU** (European Broadcasting Union).



IB



## LE MODELE DE REFERENCE ISO de L'OSI

Le Modèle de référence ISO pour Interconnexion des Systèmes Ouverts a été proposé en 1984 par l'OSI (Organisation de standardisation Internationale) :

- Modèle fondé sur un principe énoncé par Jules César :  
**« Diviser pour Régner »**
- Le principe de base est la représentation des réseaux sous la forme de couche de fonctions superposées les unes aux autres.  
**« Leur nombre, leur nom et leur fonction varient selon les réseaux »**
- L'étude du système de communication revient alors à l'étude de ses éléments élémentaires et offre une plus grande :  
**« Facilité d'étude ,Indépendance des couches, Souplesse d'évolution »**

.B



## Les 7 couches du modèle OSI

Le modèle OSI est un **modèle conceptuel**. Il a pour but d'analyser la communication en découplant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique :

- 💡 Quelles sont les informations qui circulent ?
- 💡 Sous quelle forme circulent-elles ?
- 💡 Quels chemins empruntent-elles ?
- 💡 Quelles règles s'appliquent aux flux d'informations ?



.B



## Les 7 couches du modèle OSI

### B Couche 1 : Couche physique

La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante...).

### B Couche 2 : Couche liaison de donnée

La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :

- o **La sous-couche MAC** (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de la gestion des communications entre les stations et interagit avec la couche réseau (MAC, DLCI).

- o **La sous-couche LLC** (Layer Link Control) s'occupe de fournir le contrôle de flux, l'accusé réception et la correction d'erreur.

### B Couche 3 : Couche réseau

Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.

.B



## Les 7 couches du modèle OSI

### **B Couche 4 : Couche transport**

La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.

### **B Couche 5 : Couche session**

La couche session établit, gère et ferme les sessions de communications entre les applications.

### **B Couche 6 : Couche présentation**

La couche présentation spécifie les formats des données des applications (encodage MIME, compression, encryptions).

### **B Couche 7 : Couche application**

Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur.

.B



# MODELE OSI(5/9)

## Les 7 couches du modèle OSI

| N° | Nom                | Description                         |
|----|--------------------|-------------------------------------|
| 7  | Application        | Communication avec les logiciels    |
| 6  | Présentation       | Gestion de la syntaxe               |
| 5  | Session            | Contrôle du dialogue                |
| 4  | Transport          | Qualité de la transmission          |
| 3  | Réseau             | Sélection du chemin                 |
| 2  | Liaison de données | Préparation de l'envoi sur le média |
| 1  | Physique           | Envoy sur le média physique         |



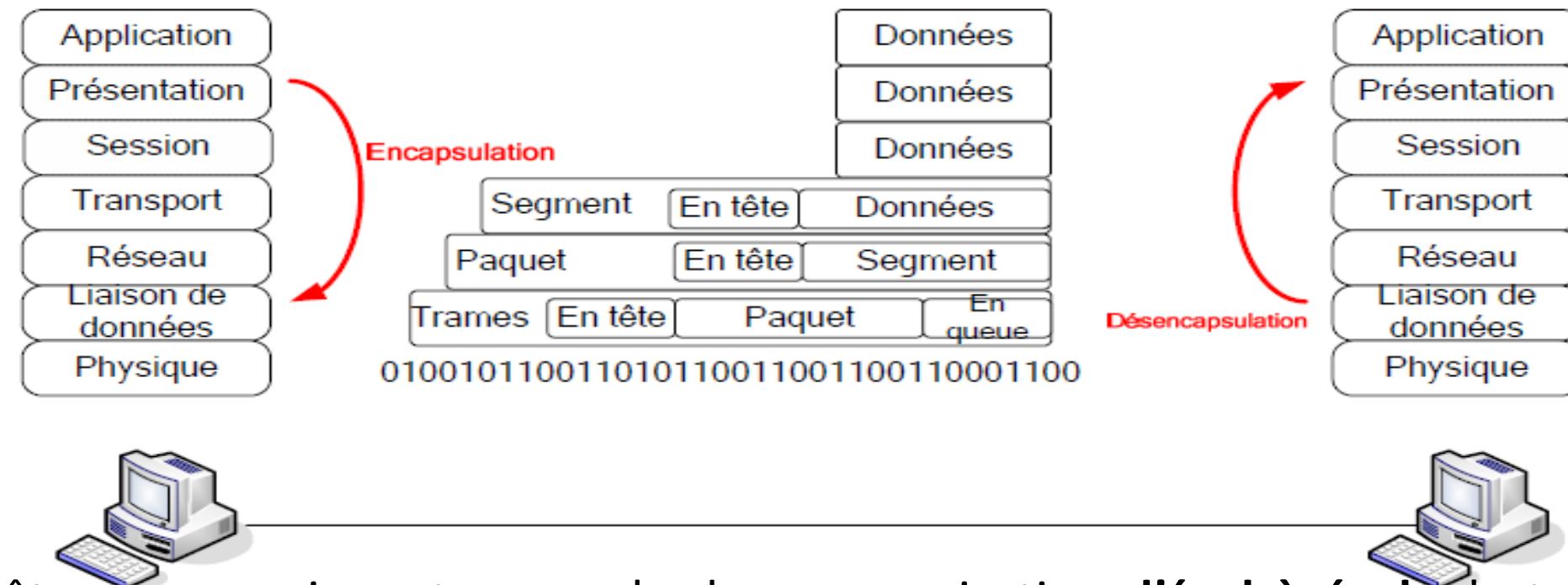
JB



# MODELE OSI(6/9)

## L' Encapsulation

Processus de conditionnement des données consistant à ajouter un en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure.



Lorsque 2 hôtes communiquent, on parle de communication **d'égal à égal**, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire.

Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU (Unité de données de protocole) est utilisée.

.B



## L' Encapsulation

### Organisation par capsulage

Chaque couche devra organiser la communication suivant un protocole particulier **en encapsulant les informations transmises de la couche supérieure**, avec des informations propres.



.B

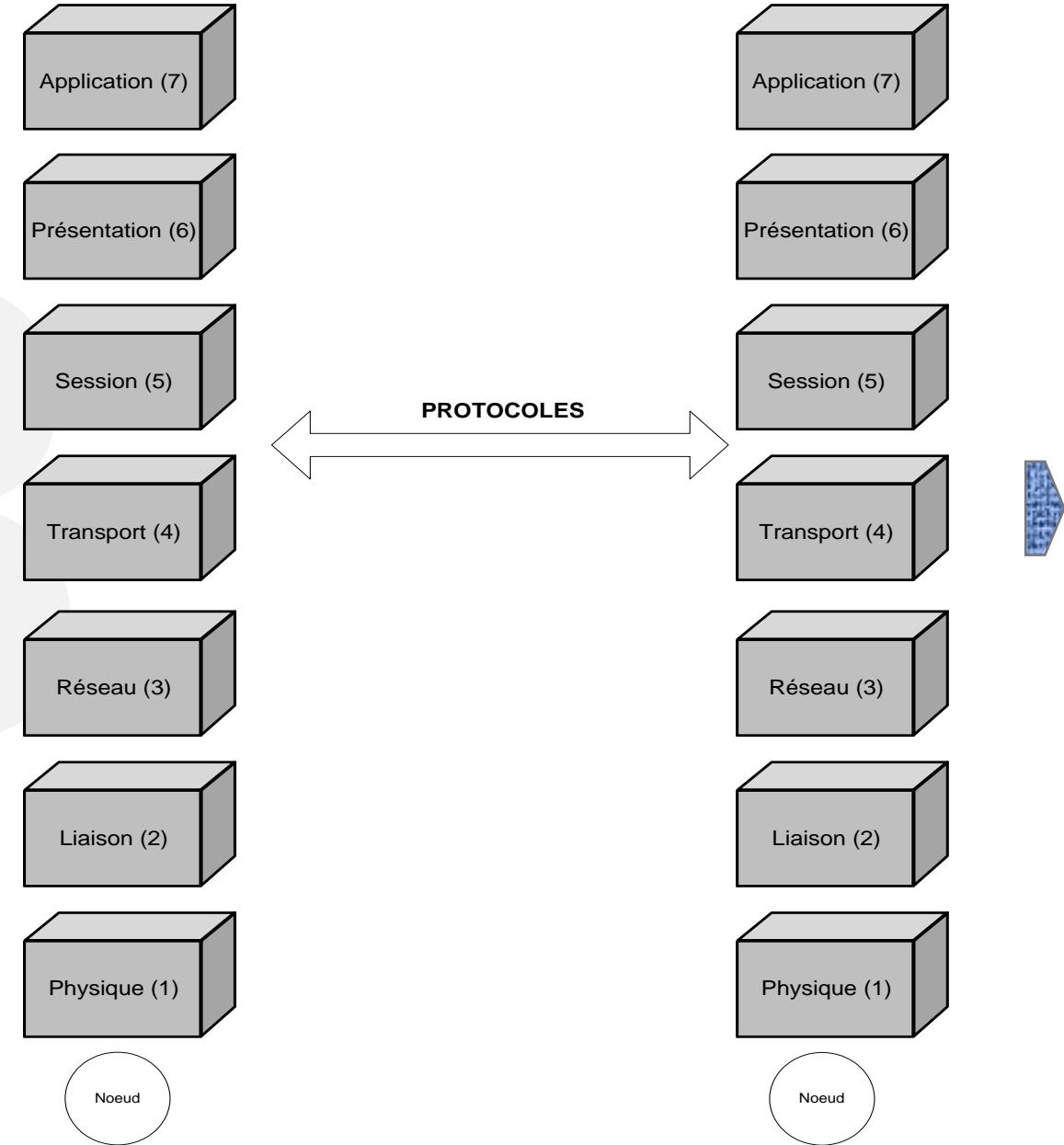


# MODELE OSI(8/9)

## L' Encapsulation

### Modèle de communication

Afin que tout utilisateur dans le monde puisse communiquer avec tout autre, sur tout type d'ordinateur, les principales organisations de standardisation ont publié une norme définissant l'organisation idéale logicielle d'un réseau suivant 7 couches.



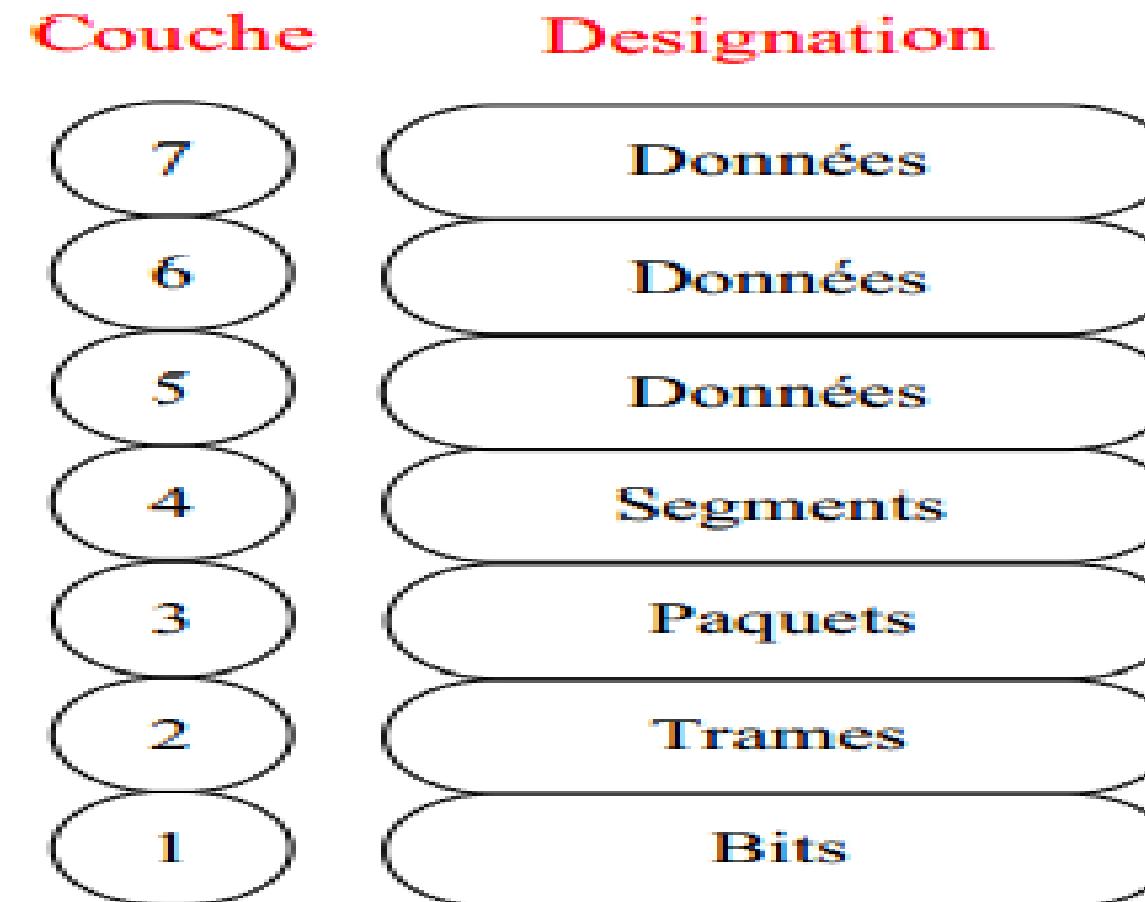
.B



# MODELE OSI(9/9)

## PDU (Unité de données de protocole)

Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU est utilisée.



.B



# MODELE TCP/IP(1/3)

## Un peu d'histoire

- La forme actuelle de **TCP/IP** résulte du rôle historique que ce système de protocoles a joué dans le parachèvement de ce qui allait **devenir Internet**.
- Internet est issu des recherches lancées par le **DOD (Department Of Defense)**, département de la défense américaine. À l'époque, les machines travaillaient pour la plupart de manière isolée ou encore en réseaux de **taille très modeste avec des protocoles incompatibles entre eux**, ceci rendant une **interconnexion impossible**.
- Les autorités militaires se sont alors demandées s'il était possible, pour ces machines aux profils très différents, de traiter des informations mises en commun et si c'était le cas, une telle **solution devrait être non centralisée**.
- Ses fonctions essentielles ne devaient en aucun cas se trouver en un seul point, ce qui le rendrait trop vulnérable. C'est alors que fut mis en place le **projet ARPANet** (Advanced Research Projects Agency Network du DOD), qui allait devenir par la suite le système d'interconnexion de réseau qui régit ce que l'on appelle **aujourd'hui Internet : TCP/IP**.

.B



# MODELE TCP/IP(2/3)

## Les 4 couches du modèle TCP/IP

| N° | Nom          | Description                              |
|----|--------------|--|
| 4  | Application  | Couches 7 à 5 du modèle OSI              |
| 3  | Transport    | Qualité de transmission                  |
| 2  | Internet     | Sélection du chemin                      |
| 1  | Accès Réseau | Reprend les couches 1 et 2 du modèle OSI |



.B



# MODELE TCP/IP(3/3)

## Comparaison entre le modèle TCP/IP et le modèle OSI

### Modèle OSI

| Couche           | Désignation             |
|------------------|-------------------------|
| Application      |                         |
| Présentation     | Couche Application      |
| Session          |                         |
| Transport        |                         |
| Réseau           | Couches flux de données |
| Liaison e Donnée |                         |
| Physique         |                         |

### Modèle TCP/IP

| Couche       | Désignation |
|--------------|-------------|
| Application  | Protocoles  |
| Transport    |             |
| Internet     | Réseaux     |
| Accès Réseau |             |

.B



# CARACTERISATION DES RESEAUX ➔

# CARACTERISATION DES RESEAUX(1/4)

## Comment transférer des données d'un point A à un point B ?

### Transfert en Mode circuit (1/2)

Toutes les données entre A et B transitent par un **même chemin** à travers le réseau. Ce chemin est appelé « **Circuit** » et est préétabli (calculé) pour satisfaire les contraintes de l'application (débit, délai, taux d'erreurs, taux de pertes ....).

Le circuit est calculé lors d'une phase de mise en connexion entre A et B (envoi d'un message de contrôle).

**Exemples:** Réseaux téléphoniques fixes et mobiles : RNIS, GSM, 3G



.B



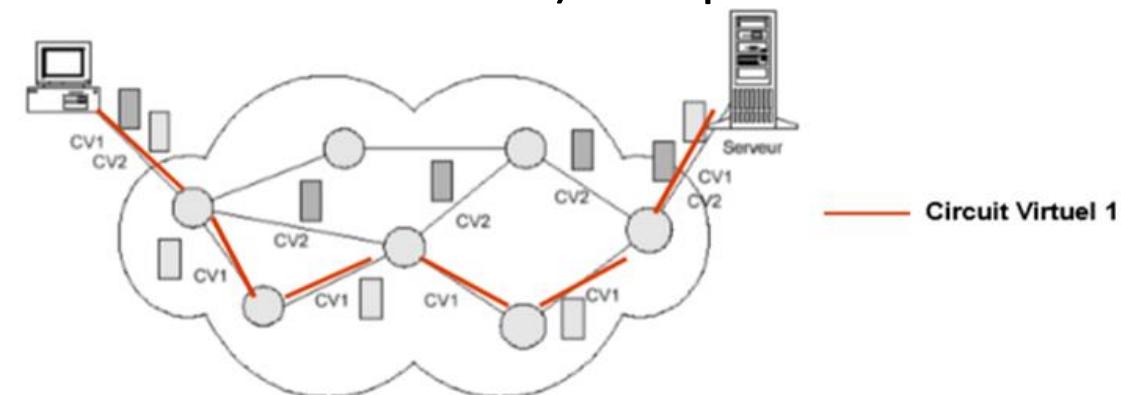
# CARACTERISATION DES RESEAUX(2/4)

## Comment transférer des données d'un point A à un point B ?

### B Transfert en Mode circuit (2/2)

Principe du service téléphonique:

1. Si le circuit est dédié aux communications entre A et B: on parle de circuit physique,
2. Si le circuit est partagé entre plusieurs entités(A,B,C...): on parle de circuit virtuel
3. Si le circuit est établi pour une longue période (mois, années) :on parle de circuit permanent.
4. si le circuit est établi pour une courte période (transfert de données): on parle de circuit commuté.



.B



# CARACTERISATION DES RESEAUX(3/4)

## Comment transférer des données d'un point A à un point B ?

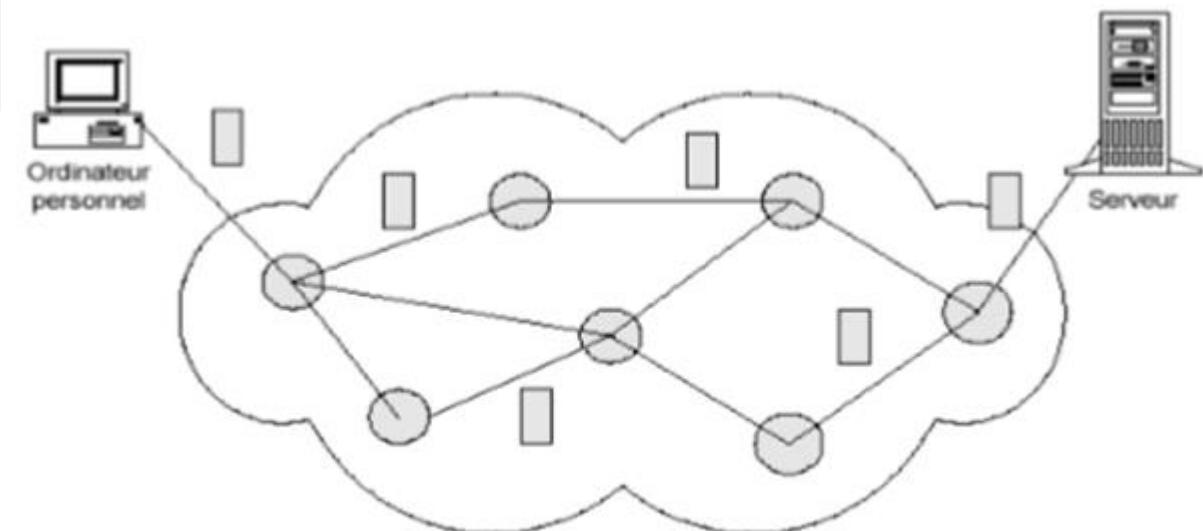
### **B Transfert en Mode datagramme**

Les données « peuvent » transiter entre A et B par des **chemins différents à travers le réseau**.  
Pas de phase de mise en connexion et de calcul d'un chemin entre A et B.

**Exemples :** Réseau Internet, réseaux 3G.

- Principe du courrier postal**

C'est aux équipements du réseau d'acheminer ces paquets individuellement par des chemins pouvant être différents, et en les temporisant si nécessaire.



.B



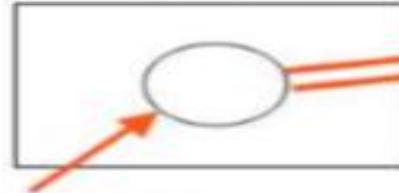
# CARACTERISATION DES RESEAUX(4/4)

## Comment transférer des données d'un point A à un point B ?

### B Mode de transfert des données

#### Mode orienté connexion

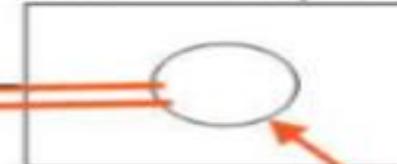
Hôte émetteur



réseau

circuit virtuel

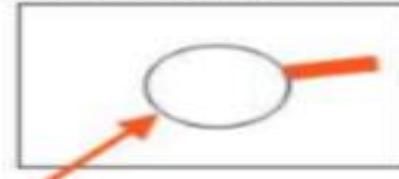
Hôte récepteur



processus  
récepteur

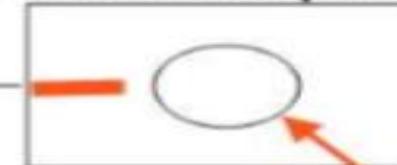
#### Mode sans connexion

Hôte émetteur



réseau

Hôte récepteur



processus  
récepteur

Paquets (Datagram)

.B



# COUCHE 1: Physique

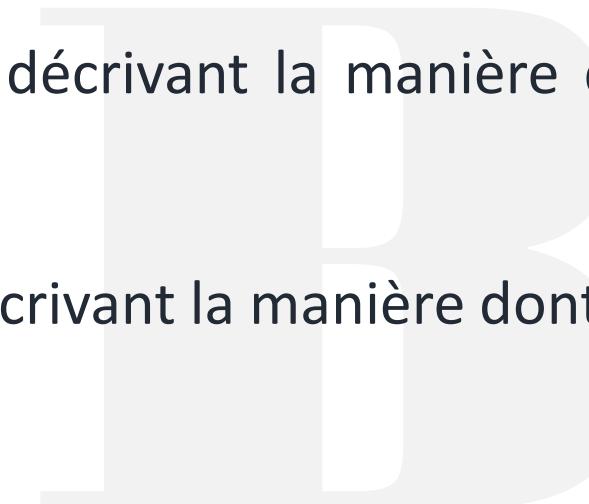


# Couche 1 (P): TOPOLOGIE DES RESEAUX 1/9

## Topologie

Décrit la manière dont les équipements réseau sont connectés entre eux. Nous en distinguerons deux types:

- Les **topologies physiques**, décrivant la manière dont les équipements sont reliés par des médias,
- Les **topologies logiques**, décrivant la manière dont les équipements communiquent.



.B

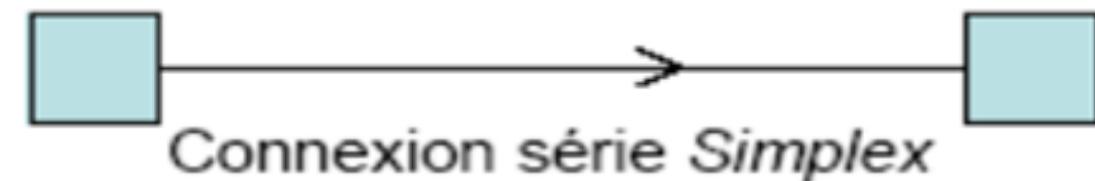


# Couche 1 (P): TOPOLOGIE DES RESEAUX 2/9

## Liaison entre deux équipements:

### B Connexion simplex ou unidirectionnelle:

- ✓ mode de communication *unidirectionnel*, dans lequel chaque appareil est soit *toujours* émetteur soit *toujours* récepteur.
- ✓ Utilisé pour la *diffusion*, c'est à dire lorsqu'un même émetteur exemple liaison entre un émetteur de télévision .
- ✓ Utilisé quand il n'est pas nécessaire pour l'émetteur d'obtenir une réponse de la part du récepteur  
exemple la télécommande de votre téléviseur.



.B



# Couche 1 (P): TOPOLOGIE DES RESEAUX 3/9

## Liaison entre deux équipements:

### B Connexion Half-duplex:

- ✓ Deux systèmes interconnectés sont capables d'émettre et de recevoir chacun leur tour.
- ✓ Un exemple de ce style de communication est le télégraphe Morse:
- ✓ talkie walkie.

IB



Connexion série Half-duplex

.B

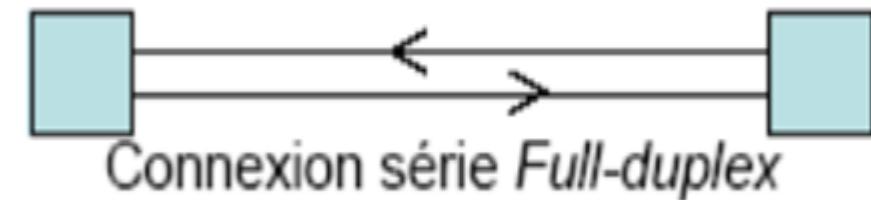


# Couche 1 (P): TOPOLOGIE DES RESEAUX 4/9

## Liaison entre deux équipements:

### B Connexion Full-duplex:

- ✓ Deux systèmes interconnectés sont capables d'émettre et de recevoir simultanément.
- ✓ Ce mode de communication exige aussi que chacun des deux systèmes soit capable de traiter à la fois des données entrantes et sortantes un exemple simple est le téléphone.
- ✓ Cette fonctionnalité requiert un bus de communication full-duplex comme SAS (Serial attached SCSI).



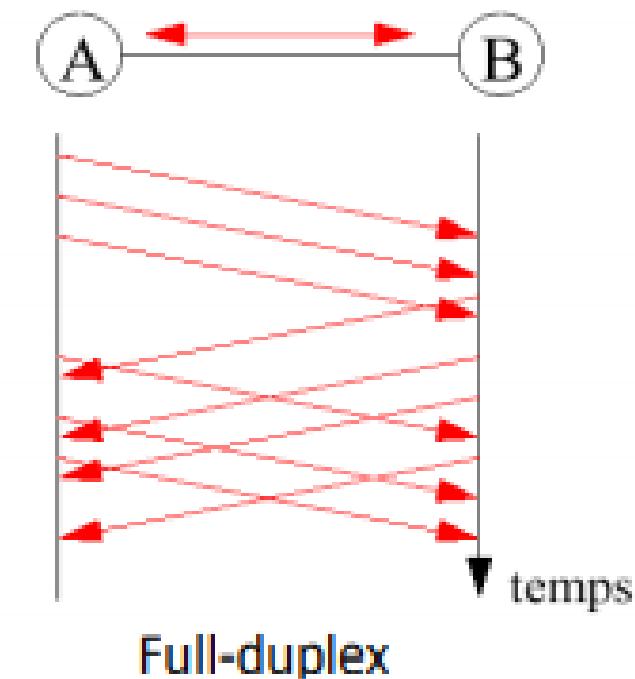
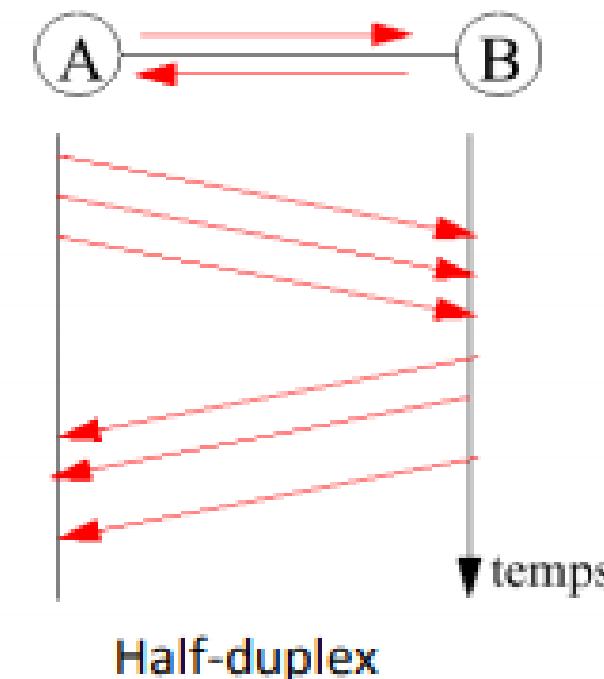
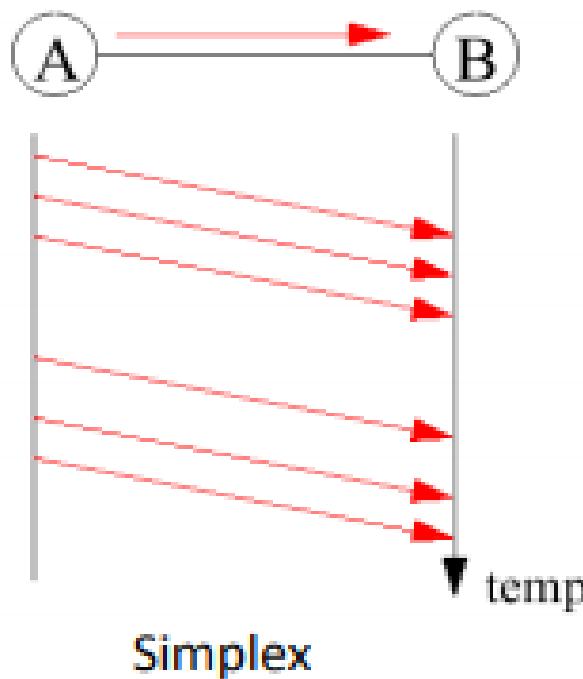
.B



# Couche 1 (P): TOPOLOGIE DES RESEAUX 4/9

## Liaison entre deux équipements:

- Unidirectionnel (simplex)
- Bidirectionnel à l'alternat (half-duplex)
- Bi-directionnel (full-duplex)



.B



# Couche 1 (P): TOPOLOGIE DES RESEAUX 5/9

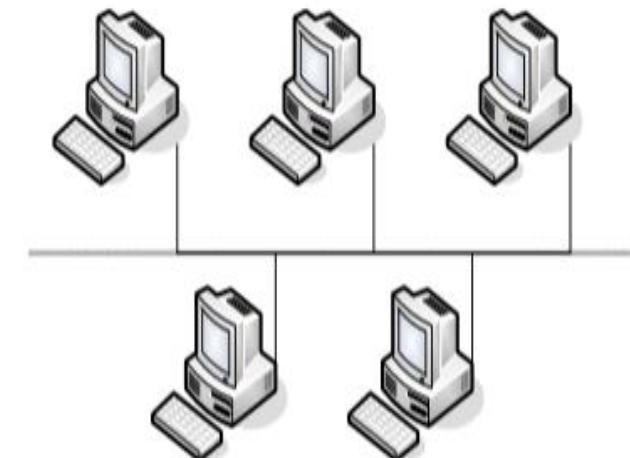
## Liaison entre deux équipements:



**BUS**

- ✓ **Perspective physique** : Tous les hôtes sont connectés directement à une liaison.
- ✓ **Perspective logique** : Tous les hôtes voient tous les signaux provenant de tous les autres équipements;
- ✓ **ADOPTÉE PAR LES RÉSEAUX :ETHERNET,APPLETALK,TOKEN BUS D'IBM**

- Extension aisée des équipements(1câble/équipement),
- L'ajout de terminaux n'interrompt pas le fonctionnement du système,
- La panne d'une station est sans conséquence,
- Economique en câblage.
- Temps d'attente imprévisible,
- Défaillance du réseau en cas de panne du support,
- Performances réduites en cas de charges importantes.



Topologie en bus

.B



# Couche 1 (P): TOPOLOGIE DES RESEAUX 6/9

## Liaison entre deux équipements:

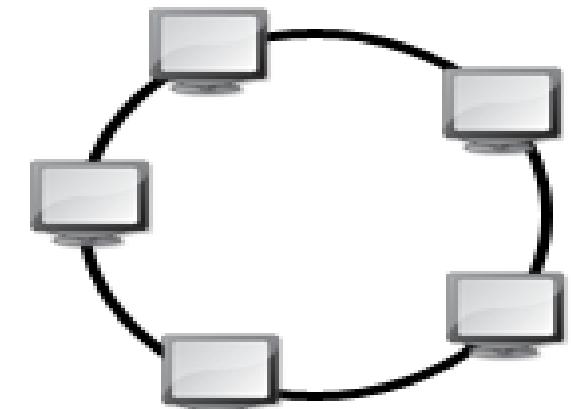
### B ANNEAU

- ✓ **Perspective physique :** Les éléments sont chaînés dans un anneau fermé.
- ✓ **Perspective logique :** Chaque hôte communique avec ses voisins pour véhiculer l'information.
- ✓ **ADOPTÉE PAR LES RÉSEAUX:**TOKEN RING, FDDI

### Remarque:

Une variante de cette topologie est le double anneau ou chaque hôte est connecté à 2 anneaux.

- Extension aisée des équipements (1 câble/équipement),
- Bonne performance avec forte charge.
- Défaillance du réseau en cas de panne du support ou de MAU(répartiteur).
- Performance réduite pour chaque nœud supplémentaire.



.B



# Couche 1 (P): TOPOLOGIE DES RESEAUX 7/9

## Liaison entre deux équipements:

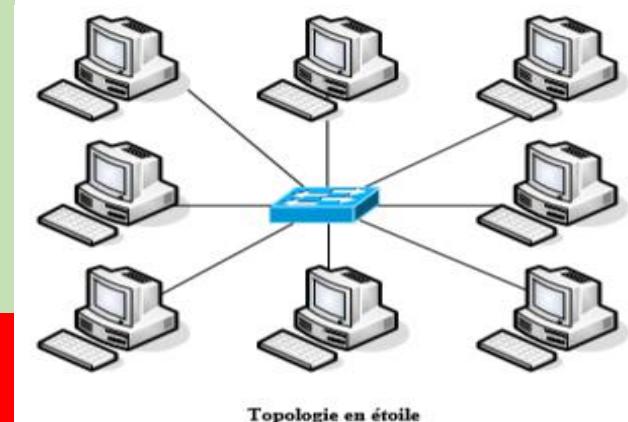
### ETOILE

- ✓ **Perspective physique** : Cette topologie comporte un nœud central d'où partent toutes les liaisons avec les autres nœuds.
- ✓ **Perspective logique** : Toutes les informations passent par un seul équipement, par exemple un concentrateur.
- ✓ **ADOPTÉE PAR LES RÉSEAUX** :STARLAN,ARCNET

### Remarque:

- ✓ La topologie en étoile étendue est identique à la topologie en étoile si ce n'est que chaque nœud connecté au nœud central est également le centre d'une autre étoile.

- Robustesse, pas de panne réseau en cas de défaillance,
- Performance en fonction du terminal et du nœud central,
- Diagnostic centralisé,
- Facilité de modification.
- Repose entièrement sur le nœud central
- Coût élevé pour les Wan.



.B

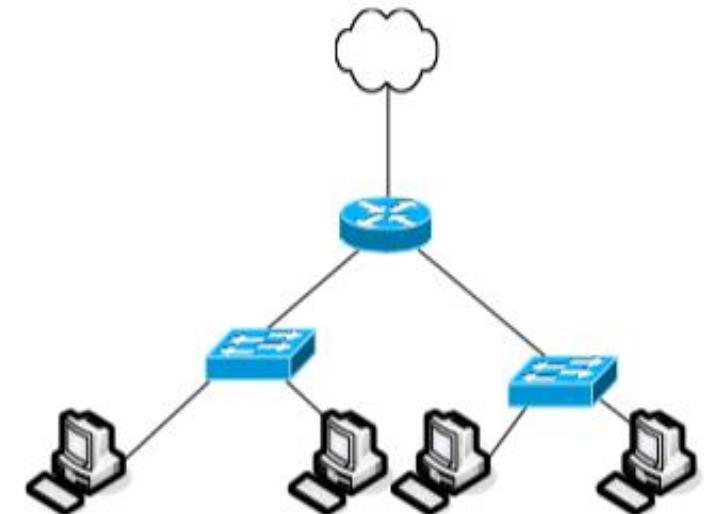


### Liaison entre deux équipements:

#### B ARBRE

- ✓ **Perspective physique** : Cette topologie ressemble à une topologie en étoile sauf qu'elle n'utilise pas de nœud central. Elle utilise un nœud de jonction à partir duquel elle se branche vers d'autres nœuds.
  
- ✓ **Perspective logique** : Le flux d'informations est hiérarchique
  
- ✓ **ADAPTÉ AUX RÉSEAUX A LARGE BANDE**

- Modulaire
- Planification aisée
- Equipements de base couteux.



Topologie hiérarchique

.B



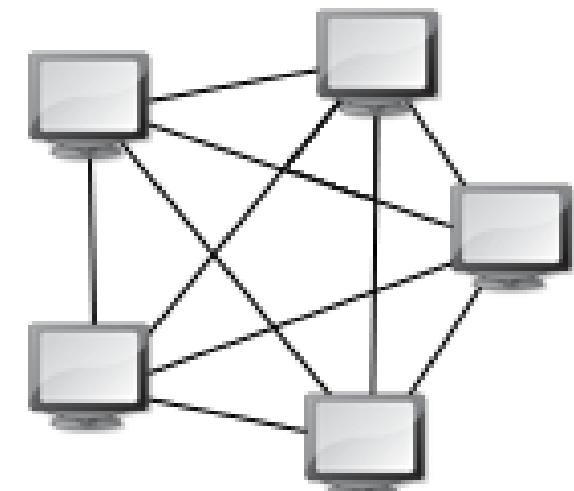
# Couche 1 (P): TOPOLOGIE DES RESEAUX 9/9

## Liaison entre deux équipements:

### B MAILLEE

- ✓ **Perspective physique** : Chaque nœud est connecté avec tous les autres
- ✓ **Perspective logique** : Dépend des équipements utilisés
- ✓ **ADAPTÉ AUX GRANDS RÉSEAUX DE DISTRIBUTION(INTERNET)**

- Autorisent un déploiement rapide et simplifié
- Grande évolutivité de la couverture,
- Une forte tolérance aux pannes et aux interférences.
- **Nombre** de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est .
- S'il y a N terminaux, le nombre de liaisons nécessaires est de:  
$$\frac{N \cdot (N - 1)}{2}$$



.B



# Couche 1 (P): Codage source et Normes 1/3

**Informations sous forme binaire 0 et 1 :**

**Nombres** → **Représentation sous forme binaire**

**Texte** → **Code ASCII**

**UNICODE**

**Code Vidéotex**

...

**Image** → **Noire et blanc (1 bit : 0 noir et 1 blanc)**

**Nuances de gris (8 bits par point)**

**Couleur (RVB, 8 bits par couleur → 24 bits par point)**

**Compression JPEG**

...

**Parole, Son et Vidéo** → **PCM (Pulse Modulation Code) pour un signal analogique**

**Compression DPCM (Son)**

**Compression MPEG (Vidéo)**

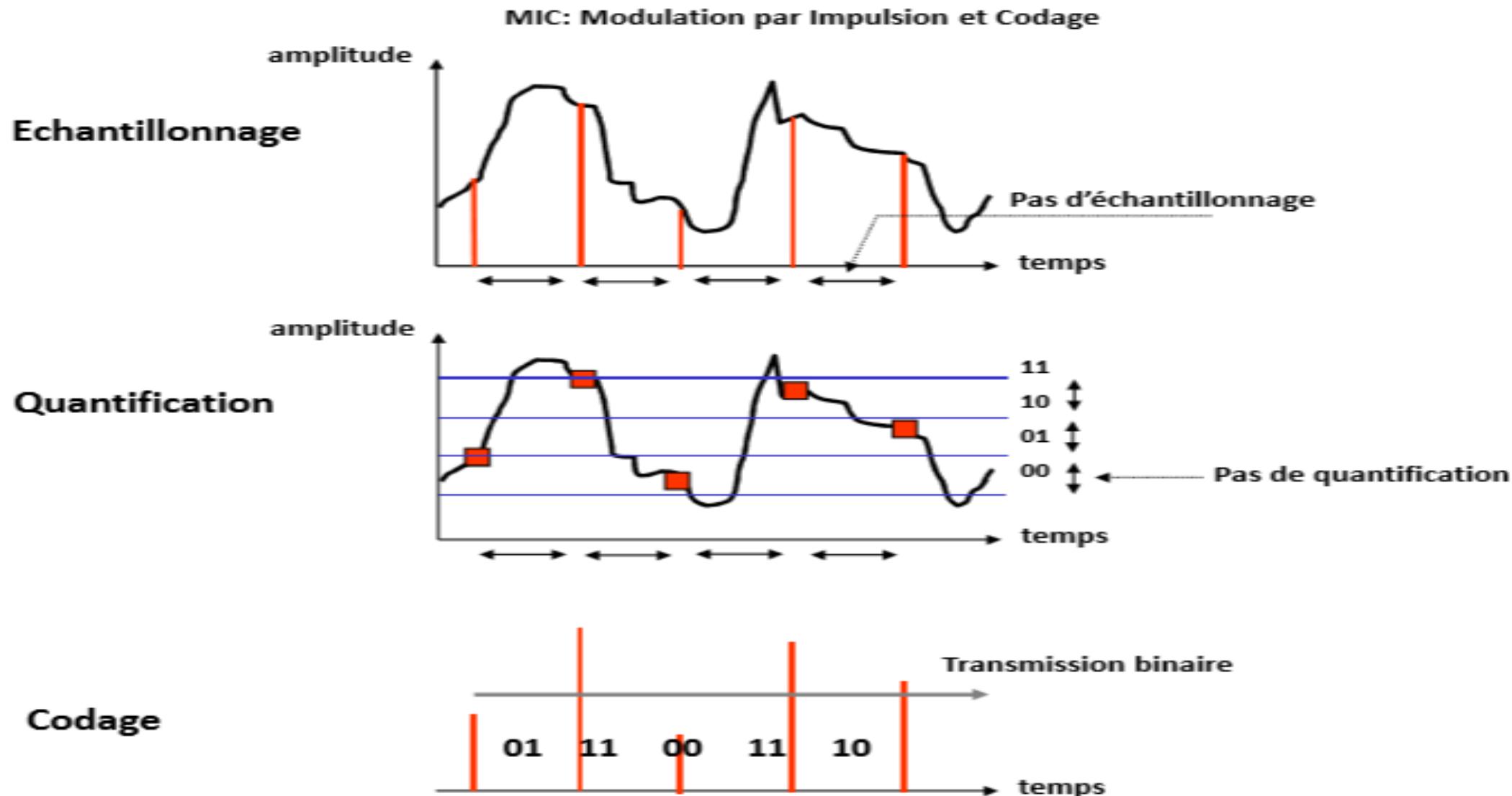


.B



# Couche 1 (P): Codage source et Normes 2/3

## La numérisation



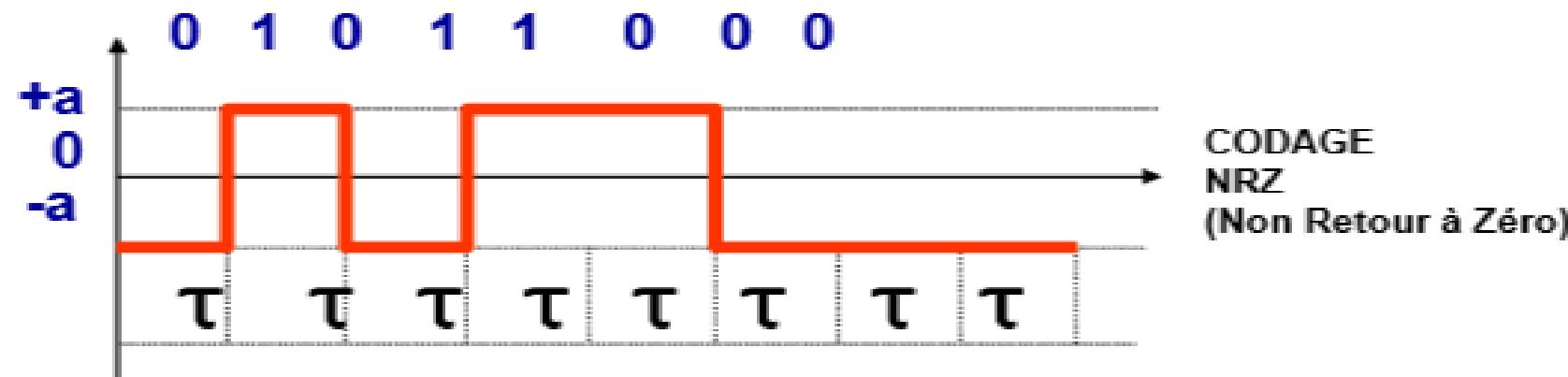
.B



# Couche 1 (P): Codage source et Normes 3/3

## La numérisation

- La couche physique est chargée de la transmission (émission et réception) effective d'un bit ou d'un train de bits continu sous la forme de signaux électriques ou optiques entre les interlocuteurs.
- Cette couche est chargée de la conversion entre bits et signaux électriques ou optiques.
- La transmission numérique (ou bande de base) consiste à convertir (ou coder) les bits en un signal à 2 niveaux : **0 → -a** et **1 → +a**

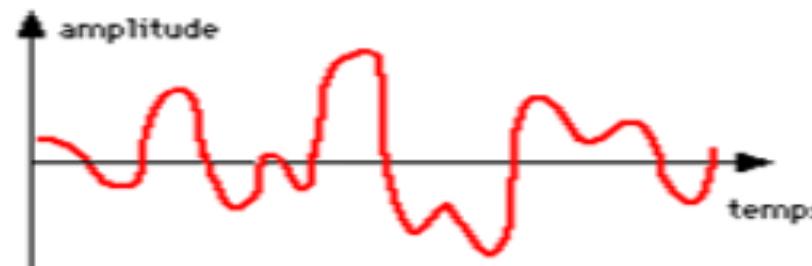


.B



# Couche 1 (P): Transmission 1/4

- L'**information** (analogique ou numérique) est véhiculée grâce à un signal physique. Ce signal peut être de nature analogique soit de nature digital (numérique).
- **Transmission analogique:** Un signal analogique est un signal **continu** qui peut prendre une infinité de valeurs.



- **Transmission numérique:** un signal **numérique** varie à des instants déterminés (discontinue) dans le temps et ne peut prendre que des valeurs distinctes dans un ensemble fini.



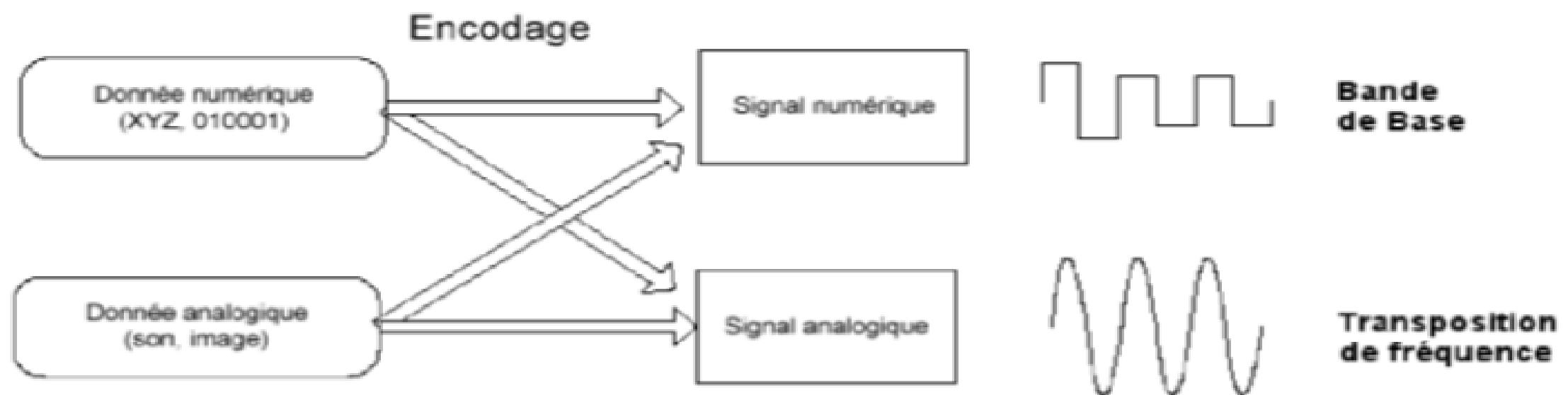
- **Remarque:** 4 combinaisons possibles entre les différents types d'information et les modes de transmission.

.B



# Couche 1 (P): Transmission 2/4

- **4 combinaisons possibles entre les différents types d'information et les modes de transmission:**
- Information Analogique – Transmission Analogique (voix sur RTCP)
- Information Analogique – Transmission Numérique (voix sur GSM ou Internet)
- Information Numérique – Transmission Analogique (données ordinateur sur RTCP via modem)
- Information Numérique – Transmission Numérique (données ordinateur sur LAN ou Internet)



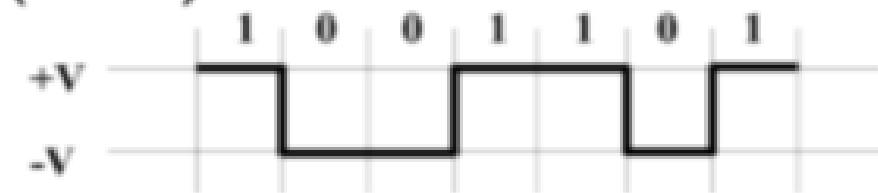
.B



## NUMERIQUE

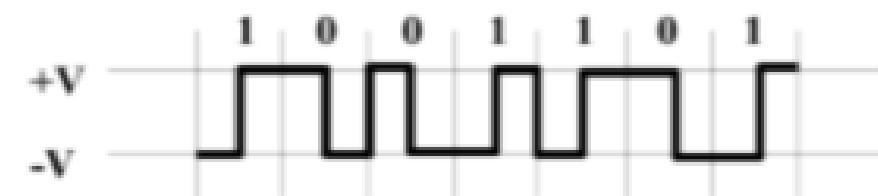
### ➤ Codage unipolaire sans retour à zéro (NRZ)

- Machine (horloge)



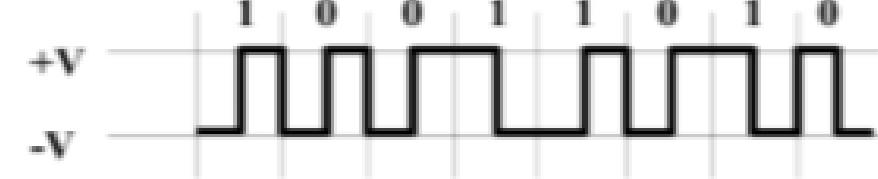
### ➤ Codage **Manchester** (simple)

- Inclus le signal d'horloge
- $\frac{1}{2}$  temps bit à l'inverse de la valeur  
+  $\frac{1}{2}$  temps bit à la valeur.



### ➤ Codage **Manchester différentiel**

- Bit 0 = Changement de polarité
- Bit 1 = Polarité du début temps bit identique à précédente



.B



## ANALOGIQUE

- Un signal est caractérisé par :
  - son amplitude **A**, sa fréquence **f** et sa phase **Φ**, tel que:
  - $y(t) = A \sin (2\pi ft + \Phi)$       avec       $f_{(\text{Hz})} = 1/T$  (T= période)
- Le signal est transporté sous la forme d'une onde adaptée aux caractéristiques physiques du support:
  - ddp électrique, onde radio-électrique, intensité lumineuse (fibre optique)
- Le signal se présente sous la forme d'une onde de base régulière appelée **porteuse**.
  - On fait subir des déformations (ou **modulations**) à cette porteuse pour distinguer les éléments du message (0, 1, 00, 01, 10, ....).
  - 4 types de modulations :
    - modulation d'**amplitude**
    - modulation de **fréquence**
    - modulation de **phase** (synchronisation)
    - modulation **combinée** (par exemple de phase et d'amplitude)



.B



- **Unités (Hz)**

- La fréquence d'un signal (**Hertz**), est le nombre de périodes (oscillations) par seconde
- kHz, MHz, GHz ...

- **Bandé Passante (Hz) :**

- La bande passante, c'est la bande de fréquences dans laquelle les signaux sont correctement reçus
- $W = F_{\max} - F_{\min}$

- **Rapidité de modulation (signal numérique):**

- $R \text{ (bauds)} = 1/\Delta$     ( $\Delta$ : durée d'un élément binaire)



.B



# Couche 1 (P): Définitions 2/2

- **Débit binaire:**
  - $D \text{ (bits/s)} = n \cdot R$  ( $n$ : *nombre de bits/intervalle de modulation*)
- **Valence:**
  - $V=2^n$  est appelé **Valence** du signal.
- **Capacité d'une voie de transmission (bit/s ou bps):** est le débit binaire maximal. C'est une fonction directe de la bande passante ( $W$ ) :
  - $C=D_{\max}=W \log_2(1+S/B)$  ( $S/B$  = Signal/Bruit)
  - En effet:
    - Selon Shannon:  $n_{\max} = 1/2 \log_2(1+S/B)$  (canal bruité)
    - Selon Nyquist:  $R_{\max} = 2W$  (canal sans bruit)
- **Remarque:** Lorsque  $V = 2$  (modulation simple), le débit binaire (bits/s) est égal à la rapidité de modulation (bauds). Par abus de langage on parle de débits en bauds ( $V \neq 2$ )



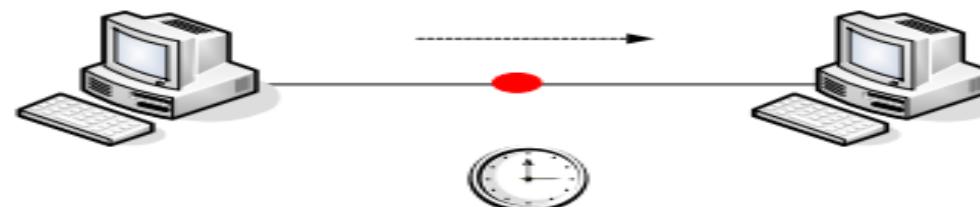
.B



## Les facteurs pouvant affecter un bit

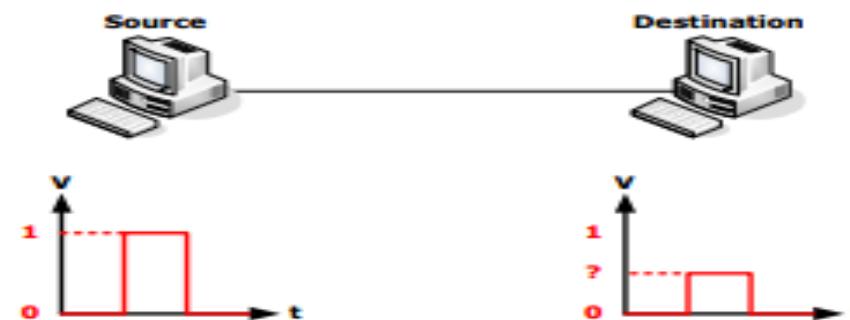
### B La propagation de signaux réseau :

Le terme de propagation fait référence au temps que met un bit, c'est-à-dire **une impulsion**, à se déplacer dans le média. Il est impératif que la propagation soit homogène dans le réseau.



### B L'atténuation du signal réseau :

Perte de la force du signal. Ce problème est limitable par un bon choix des médias réseau utilisés.



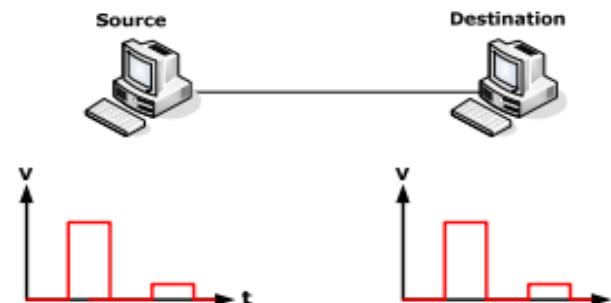
.B



## Les facteurs pouvant affecter un bit

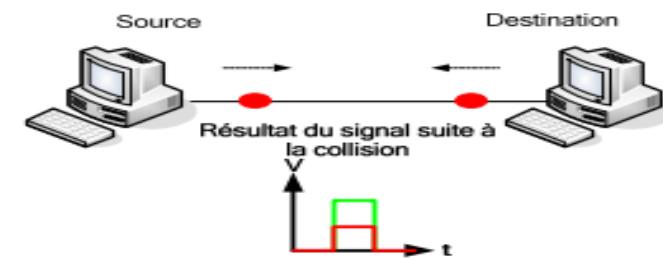
### La réflexion réseau :

Retour d'énergie causée par le passage des impulsions dans le média. Si ce retour est trop fort, il peut perturber le signal des impulsions suivantes. Le système binaire, et donc à 2 états, peut être perturbé par ces énergies supplémentaires se déplaçant dans le média.



### Les collisions :

Se produit lorsque 2 ordinateurs utilisant le même segment de réseau émettent en même temps. Les impulsions se mélangent, détruisant alors les données.



.B



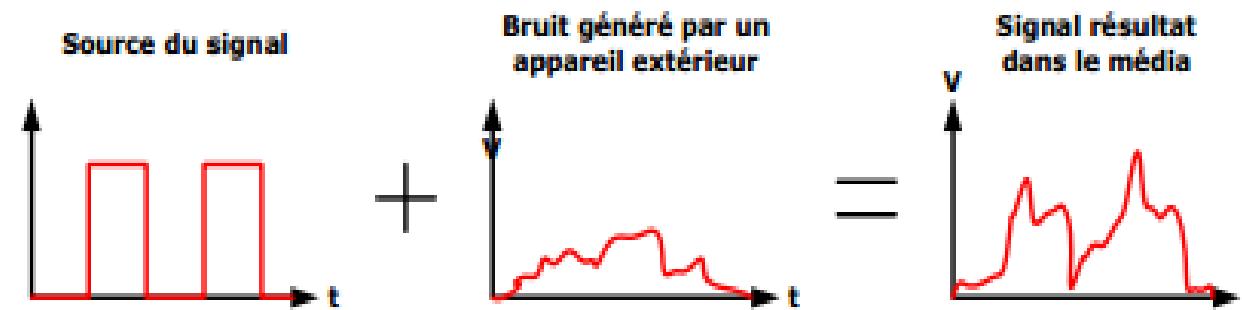
## Les facteurs pouvant affecter un bit

### B Le bruit :Ajout indésirable à un signal

**Diaphonie** : bruit ajouté au signal d'origine d'un conducteur par l'action du champ magnétique provenant d'un autre conducteur .

### B Paradiaphonie : diaphonie causée par un conducteur interne au câble .

Le bruit peut être causé par des sources d'alimentations externes, des variations thermiques, des interférences électromagnétiques ou encore des interférences de radio fréquences.



.B

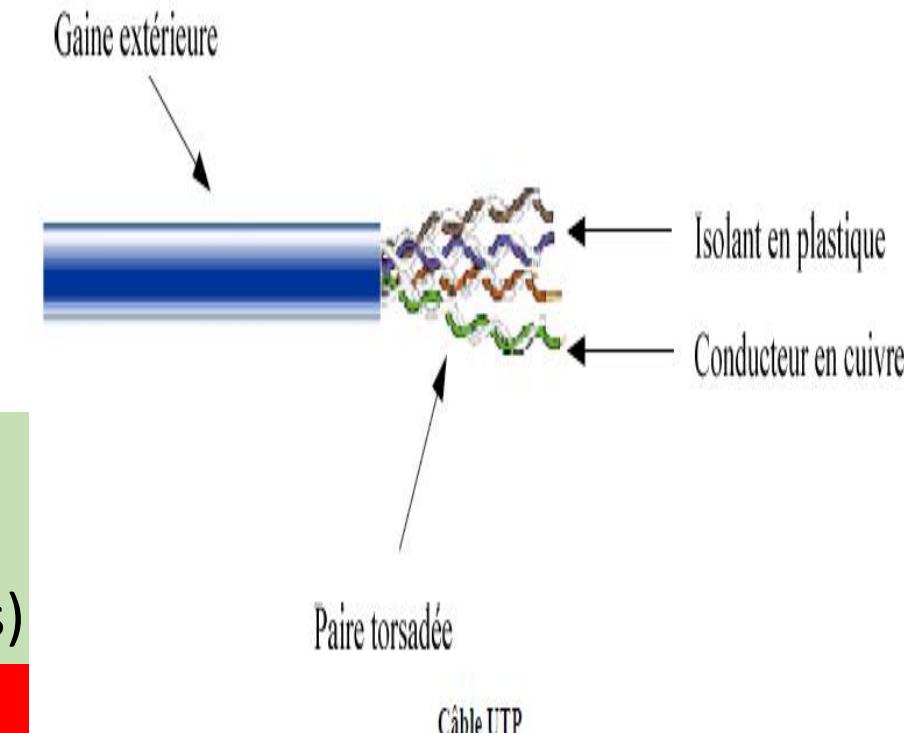


## CUIVRES

### **B Le câble à paires torsadées non blindées: UTP**

Le câble UTP est composé de **4 paires de fils torsadées 2 à 2**, chacune de ses paires étant isolées des autres. Ce câble compte uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal causée par une perturbation électromagnétique et une interférence radioélectrique.

**4 paires de fils torsadées 2 à 2.**



- Simple à installer
- Peu coûteux
- Petit diamètre (pour installation dans des conduits existants)
- Sensible aux interférences

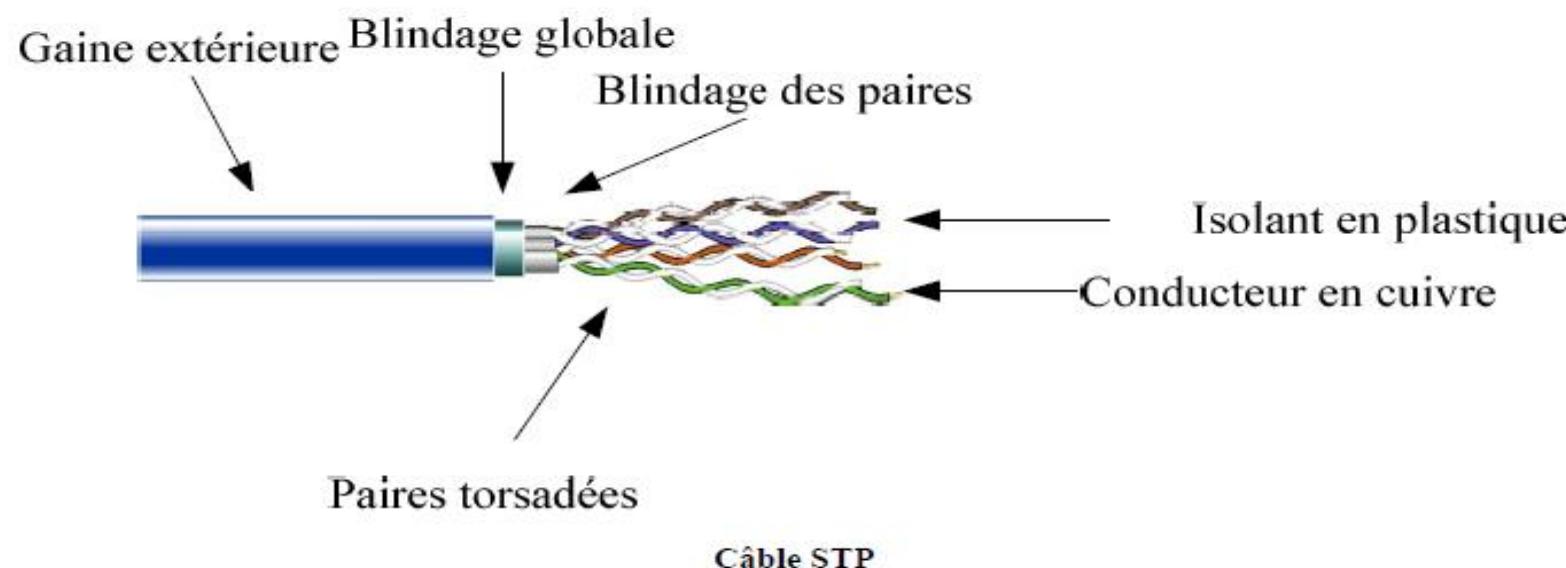
.B



## CUIVRES

### Le câble à paires torsadées blindées: STP

Le câble à paires torsadées et blindées, ou STP, ajoute aux spécifications de l'UTP une méthode de blindage, d'annulation et de torsion de câbles. offrent une résistance à l'interférence électromagnétique, ainsi qu'à l'interférence de radiofréquences, sans toutefois augmenter sensiblement la taille ou le poids du câble.



.B



## CUIVRES

### **Le câble coaxial**

Un câble coaxial est constitué d'un fil de cuivre entouré d'un isolant flexible, lui-même entouré d'une torsade de cuivre ou d'un ruban métallique qui agit comme le second fil du circuit et comme protecteur du conducteur intérieur. Cette deuxième couche ou protection peut aider à réduire les interférences externes. Une gaine de câble enveloppe ce blindage.

Le câble coaxial offre de nombreux avantages du fait de sa capacité à s'étendre sur une plus grande distance et de son coût parmi les plus faibles.



.B

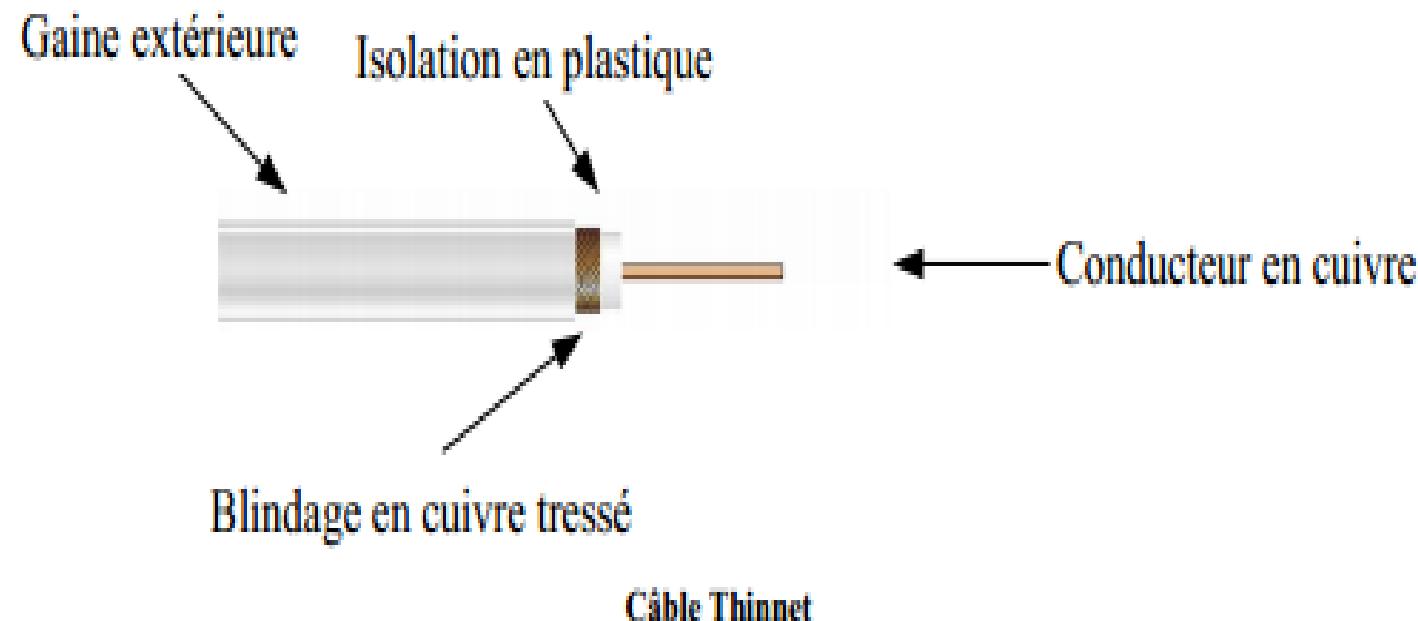


## CUIVRES

### B Le câble coaxial: Types de câble coaxial :

#### ✓ Thicknet :

Epais et raide à cause de son blindage, il est recommandé pour l'installation de câble fédérateur. Sa gaine est jaune.



.B

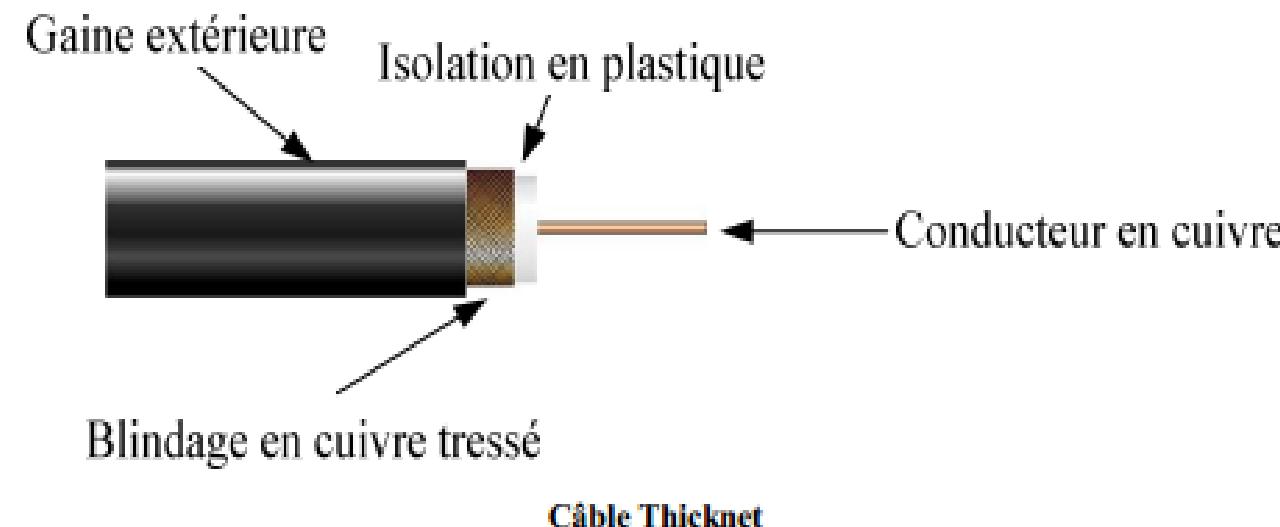


## CUIVRES

### Le câble coaxial: Types de câble coaxial :

#### ✓ **Thinnet** :

D'un diamètre plus réduit, il est plus pratique dans des installations comprenant des courbes. De plus, il est plus économique, mais dispose d'un blindage moins conséquent.



#### ✓ **CheaperNet** :

Version économique et de faible diamètre du câble coaxial.

.B



## CUIVRES

### Le câble coaxial: Connecteur Coaxial :



### Caractéristiques :



|           | Type de câble | Débit   | Longueur Max | Diamètre | Impédance | Stations max par segment |
|-----------|---------------|---------|--------------|----------|-----------|--------------------------|
| 10 Base 5 | Coaxial épais | 10 Mbps | 500 m        | 10 mm    | 50 ohms   | 100                      |
| 10 Base 2 | Coaxial fin   | 10 Mbps | 200 m        | 6 mm     | 50 ohms   | 30                       |

.B



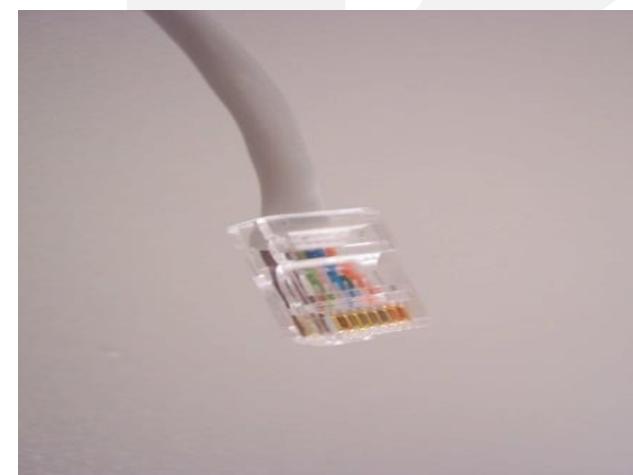
## CUIVRES

### Le câble coaxial: Les connecteurs RJ-45

Le raccordement **10BaseT** standard (le connecteur de point d'extrémité sans prise) est le RJ-45.

Il réduit les **parasites**, la **réflexion** et les problèmes de stabilité mécanique et ressemble à une prise téléphonique, sauf qu'il compte huit conducteurs au lieu de quatre.

Il s'agit d'un composant réseau passif, car il sert uniquement au passage du courant entre les quatre paires torsadées de câbles torsadés de catégorie 5 et les broches du connecteur RJ-45.



.B



## CUIVRES

Voici un tableau récapitulant les différents types de câbles ainsi que leur débit :

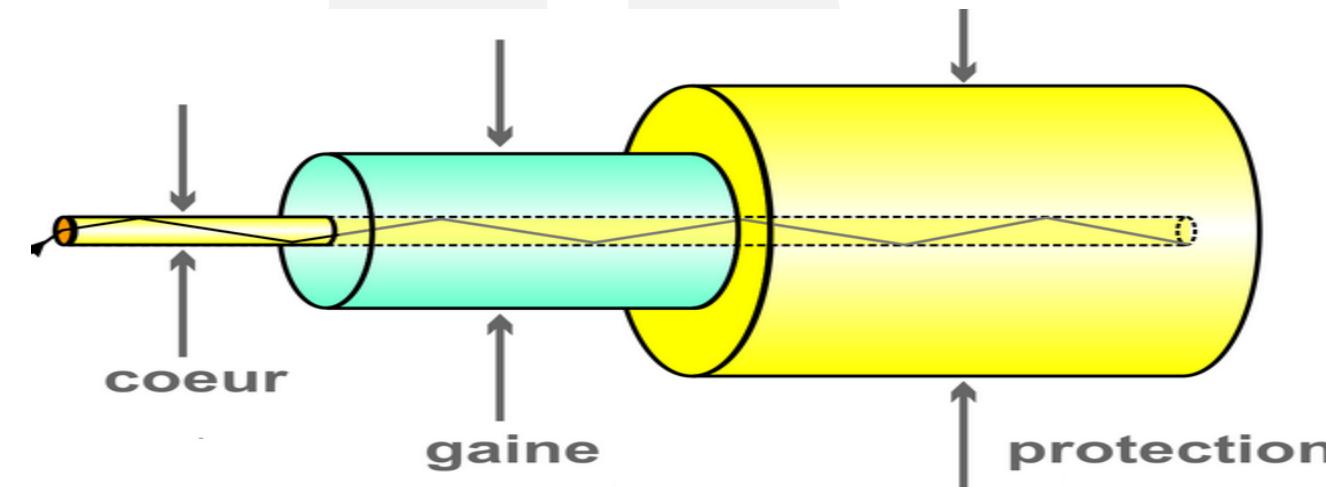
| Technologie          | Type de câble | Débit théorique | Longueur Max | Connecteur | Coût       |
|----------------------|---------------|-----------------|--------------|------------|------------|
| 10 Base 2 (Thinnet)  | Coaxial       | 10 Mbits/s      | 200 m        | BNC        | Peu cher   |
| 10 Base 5 (Thicknet) | Coaxial       | 100 Mbits/s     | 500 m        | BNC        | Peu cher   |
| 10 Base T            | UTP cat 5     | 10 Mbits/s      | 100 m        | RJ45       | Bon marché |
| 100 Base TX          | UTP cat 5     | 100 Mbits/s     | 100 m        | RJ45       | Bon marché |
| 10 Base FL           | Fibre optique | 10 Mbits/s      | 2000 m       | SC         | Elevé      |
| 100 Base FX          | Fibre optique | 100 Mbits/s     | 400 m        | SC         | Elevé      |

.B



## Fibres Optiques

Une fibre optique transmet des données dans **un sens seulement**. Aussi pour que deux entités communiquent en full duplex, un câble optique doit contenir deux fibres optiques : l'une pour transmission et l'autre pour réception. Un câble peut contenir de 2 jusqu'à 48 fibres.



**La lumière est guidée dans le centre de la fibre, appelé cœur.**

L'indice de réfraction est bien inférieur à celui du cœur. Cela permet justement à la lumière de se réfléchir.

.B

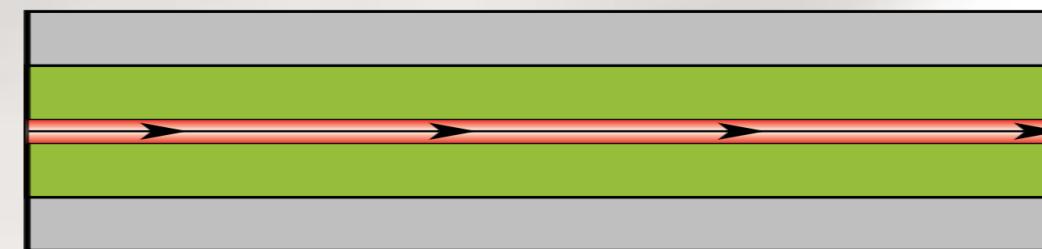
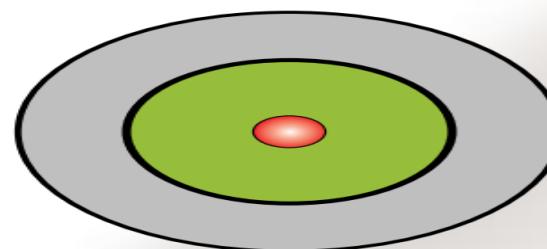


# Couche 1 (P): MEDIAS RESEAU 13/17

## Fibres Optiques

### les monomode

Dans ce cas, la fibre est dite « monomode » car, en raison de la très petite taille du cœur ( $9 \mu\text{m}$ ), il n'y a qu'un seul mode de propagation de la lumière.



### La fibre monomode

**9 / 125**

diamètre de la gaine en microns ( $\mu\text{m}$ )

diamètre du cœur en microns ( $\mu\text{m}$ )

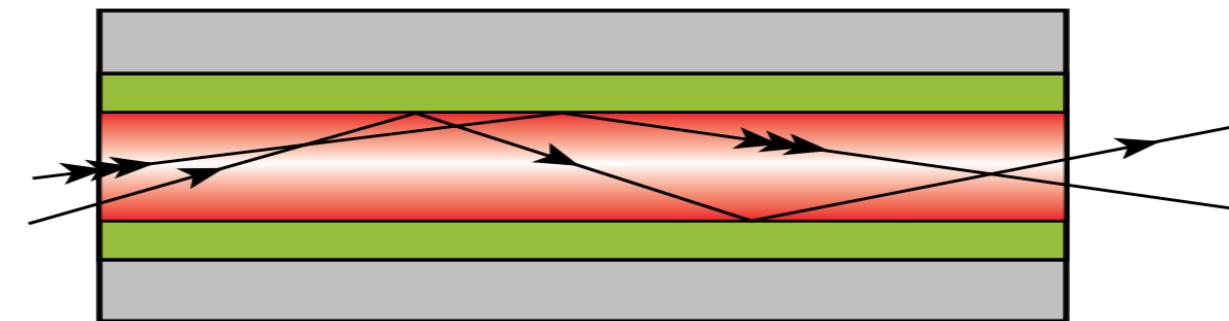
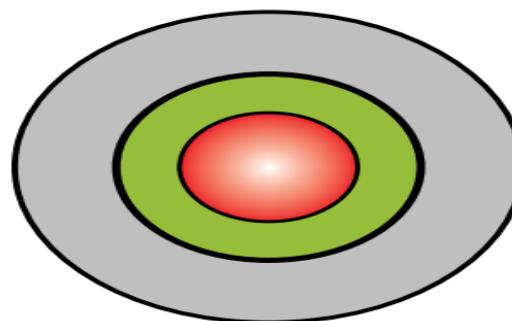
.B



## Fibres Optiques

### les multimodes:

Ce type de fibre est dit « multimode » car la lumière se propage suivant plusieurs « modes », C'est à dire qu'elle peut suivre plusieurs trajets à l'intérieur du cœur.



### La fibre multimode

**50 / 125 ou 62,5 / 125**

 diamètre de la gaine en microns ( $\mu\text{m}$ )  
 diamètre du cœur en microns ( $\mu\text{m}$ )

.B

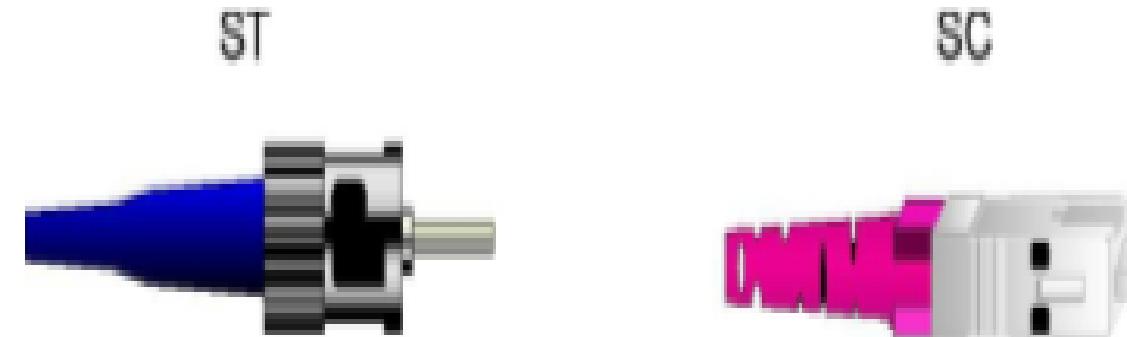


# Couche 1 (P): MEDIAS RESEAU 15/17

## Fibres Optiques

### Connecteurs fibre optique:

Les extrémités de fibre sont attachées aux connecteurs qui se branchent dans les prises des transmetteurs et récepteurs. Les connecteurs de type SC (Subscriber Connector) sont le plus souvent utilisés pour les fibres multimode et les connecteurs de type ST (Straight Tip) les plus fréquemment utilisés pour les fibres monomode. Le schéma ci-dessous montre les connecteurs ST et SC, respectivement.



Les deux connecteurs de fibre optique : ST et SC (simplex)

.B



## SANS FIL

### Fonctionnement d'un réseau sans fil

Les réseaux sans fils ou WLAN (pour Wireless LAN), réussissent à conjuguer tous les avantages d'un réseau filaire traditionnel comme Ethernet mais sans la limitation des câbles.

Un WLAN a également besoin, tout comme un LAN, d'un média. Au lieu de câbles à paires torsadées, les LANs utilisent des fréquences radio à **2,4 GHz et 5 GHz**.

.B



# Couche 1 (P): MEDIAS RESEAU 17/17

## SANS FIL

Les réseaux sans fils peuvent fonctionner à **deux bandes de fréquences**, selon la technologie utilisée. Soit aux alentours de 2400 Mhz (2,4 Ghz) pour le **802.11b** et **802.11g** soit aux alentours de **5000 Mhz pour le 802.11a**.

La bande la plus utilisée pour le moment est l'ISM (Industrial Scientific and Medical) cela correspond à la bande des 2,4 GHz avec une largeur de bande de 83,5 MHz. Soit des fréquences allant de 2,4 GHz à 2,4835 GHz.

|                    | <b>802.11b</b> | <b>802.11a</b> | <b>802.11g</b> |
|--------------------|----------------|----------------|----------------|
| Bande de fréquence | 2,4 Ghz        | 5 Ghz          | 2,4 Ghz        |
| Débit maximum      | 11 Mbps        | 54 Mbps        | 54 Mbps        |

**Tableau récapitulatif des fréquences et débits :**

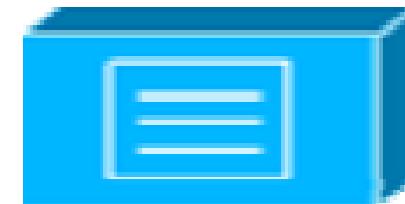
.B



# Couche 1 (P): EQUIPEMENTS D'INTERCONNEXION

## B Répéteur

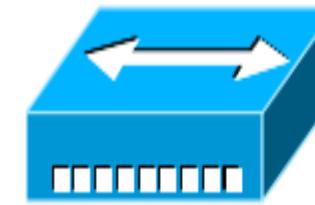
Le répéteur est un composant actif. Son rôle est de régénérer et de resynchroniser le signal afin de pouvoir étendre la portée des câbles.



Symbol d'un répéteur

## B Concentrateur

Le concentrateur, ou répéteur multi ports, reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité



Symbol d'un Concentrateur 10 Base T



Symbol d'un concentrateur 100 base T

## B Emetteur/récepteur

Un émetteur-récepteur (transceiver) convertit un signal en un autre. Il est souvent intégré aux cartes réseau.

.B



**Exercice 1.**

- a) Citer les codes ou alphabets que vous connaissez ! Quels sont les symboles représentables ?
- a) Comment représentons la parole, la musique, les images dans les applications usuelles : le téléphone, la télévision, le CD audio, ou le DVD ?
- a) Comment réalise t on la conversion de ces informations de l'analogique au numérique ?
- a) Quels sont les intérêts du numérique par rapport à l'analogique ?



 Solution Exercice 1.

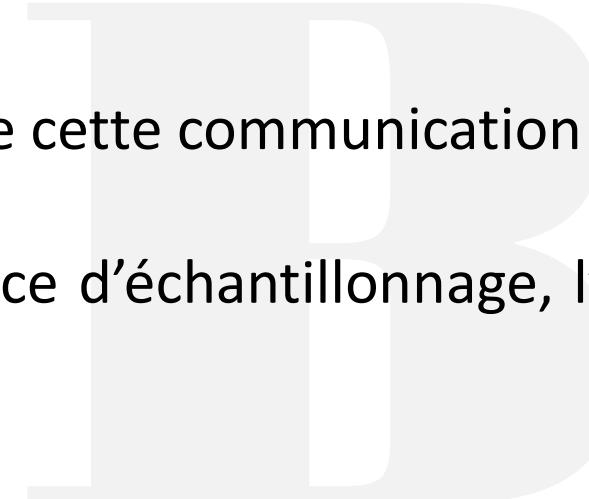
JB



### Exercice 2.

On considère un signal de parole de bande passante 4 KHz. On souhaite numériser ce signal et le transmettre sur le réseau NUMERIS en France.

- a) Quel sera le débit binaire de cette communication ?
  
- b) Veuillez préciser la fréquence d'échantillonnage, l'échelle de quantification, et la résolution de codage.



 **Solution Exercice 2.**

JB



### Exercice 3.

Soit à coder en binaire pour la transmission et le traitement informatique, une page A4 (A4 = 297 x 210 mm).

- a) on choisit de représenter chaque pixel par un bit (0 s'il est blanc, 1 s'il est noir). Sachant qu'il y a (pour le fax) 1728 pixels par ligne et 3,85 lignes par mm, quel est le volume de données binaires pour représenter ainsi une page (en mode portrait) ?
- b) Combien de temps faut il pour transmettre la page numérisée à 9600 bit/s, à 64 Kbit/s ?
- c) Mêmes questions si l'on veut transmettre la page avec 256 nuances de gris (possibles pour chaque pixel).
- d) Que peut on déduire quant à la méthode de codage utilisée dans un télécopieur classique ?



## Solution Exercice 3.

IB



## COUCHE 2: Liaison de données



## Couche 2 (LD): Liaison de données 1/6

### OBJECTIFS

- **Communication (fiable et efficace) entre deux machines adjacentes**
  - deux machines physiquement connectées par un canal de transmission
  - La couche liaison récupère des paquets de la couche réseau.
  - Pour chaque paquet, elle construit une (ou plusieurs) trame(s).
  - La couche liaison envoie chaque trame à la couche physique.
- **Liaisons de transmission ne sont pas parfaites :**
  - Débit binaire limité, le délai de propagation est non nul, il peut y avoir des erreurs de transmission
- **Cette couche doit assurer une transmission exempte d'erreurs sur un canal de communication.**
- **Elle doit aussi assurer un délivrance ordonnée des informations**



.B



## SERVICES OFFERTS

- Gestion (délimitation) de trames
- Contrôle d'erreurs
- Contrôle de flux
- Contrôle d'accès à un canal partagé (MAC)



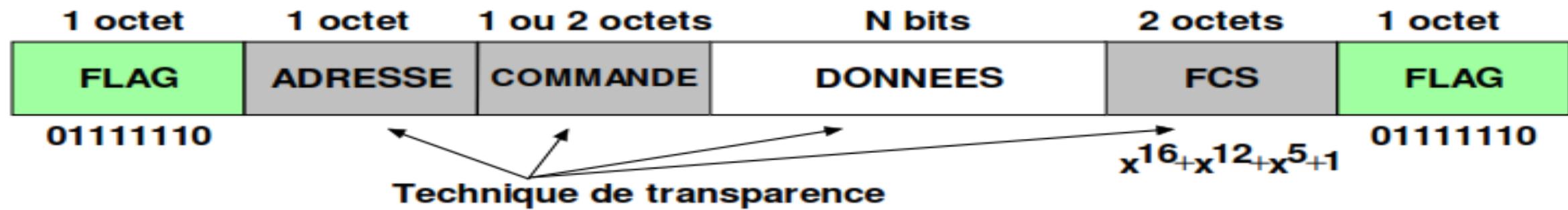
.B



SERVICES OFFERTS

## DELIMITATION DES DONNEES

exemple Trame HDLC



Le champ « DONNEES est généralement de taille constante.

N = 128 ou 256 octets

FCS : Frame Check Sequence (contrôle des erreurs binaires)

.B



## SERVICES OFFERTS

### CONTRÔLE DES ERREURS

#### 1- Vérification au récepteur de données

Vérification du format des trames :

- longueur, valeurs prédefinies de certains champs

Détection de la corruption des trames :

- champ de contrôle d'erreur → CRC-16 pour HDLC (champ FCS)

#### 2- Information de l'émetteur de données

- Soit implicitement par temporisateur
  - armé à chaque envoi de trame,
  - désarmé lors de la réception d'un acquittement positif
- Soit explicitement : par "Nack"
  - le **rejet total** : retransmission de toutes les trames à partir de celle spécifiée
  - le **rejet sélectif** : retransmission de la trame spécifiée

#### 3- Retransmission de la trame (perdue ou détruite) par l'émetteur



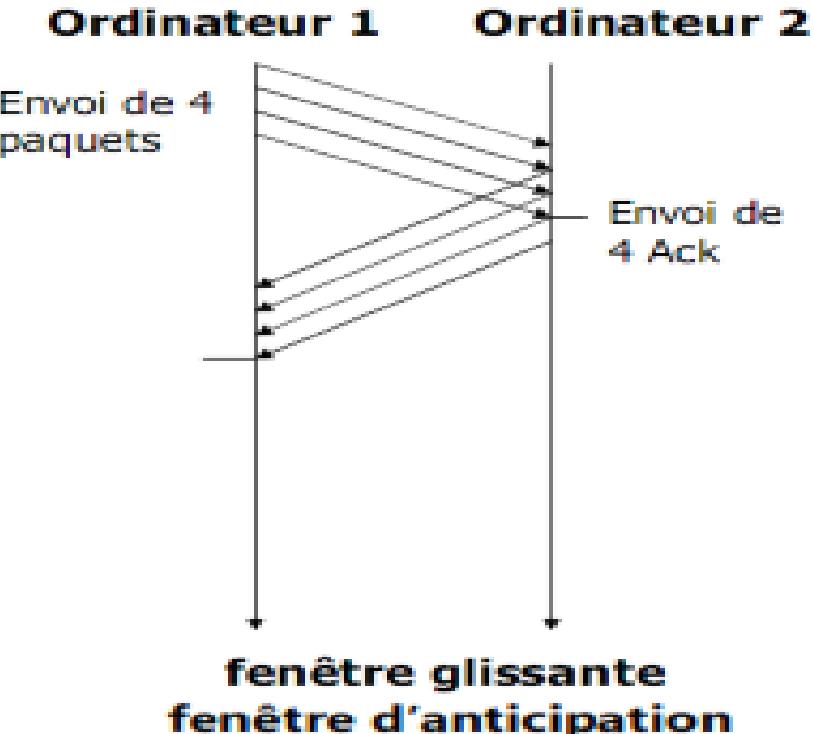
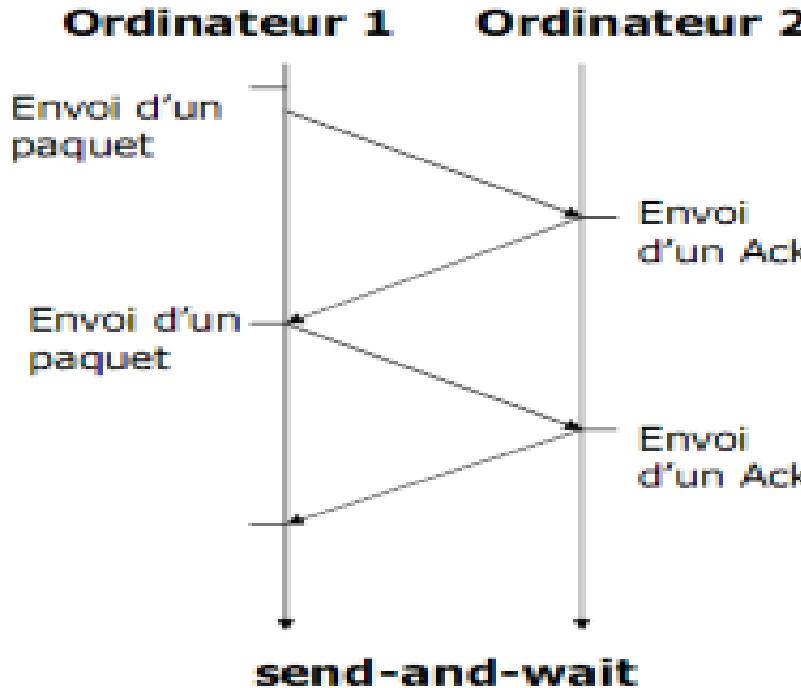
.B



## SERVICES OFFERTS

# CONTRÔLE DE FLUX

## 2 mécanismes



.B



## SERVICES OFFERTS

# CONTRÔLE DE FLUX avec mécanisme SIMPLE et UTOPIQUE « SEND & WAIT »

### Hypothèses :

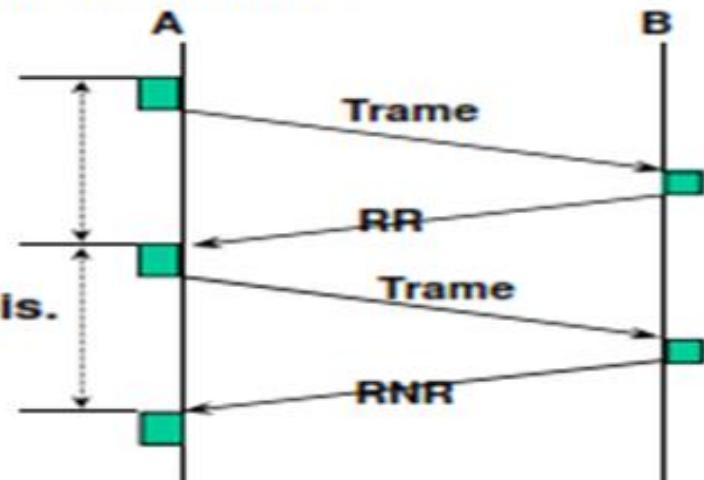
- Transmission de trames de données (I) dans un seul sens
- Canal de communication parfait (pas d'erreurs ni pertes)
- Taille finie des mémoires tampon

### Solution :

- Introduction de 2 trames de supervision (S), qui ne transportent aucune information utile et qui sont invisibles aux utilisateurs :
  - RR (Receiver Ready)
  - RNR (Receiver Not Ready)

### 2 variantes :

- Envoie d'une trame de supervision après chaque trame de données,
- Envoie d'une trame RNR si tampon plein, suivie d'une trame RR pour reprendre les envois.



.B



# Couche 2 (LD): Technologies Ethernet 1/16

## INTRODUCTION À ETHERNET

- 💡 Ethernet est la **technologie de base des réseaux LAN** la plus utilisée actuellement.
- 💡 Le principe repose sur le fait que toutes les machines sont reliées à une **même ligne de communication**.
- 💡 L'institut IEEE l'a normalisé et adapté dans son modèle IEEE 802.3.
- 💡 Ces deux technologies sont très similaires (elles diffèrent sur un champ de trame seulement).

.B



# Couche 2 (LD): Technologies Ethernet 2/16

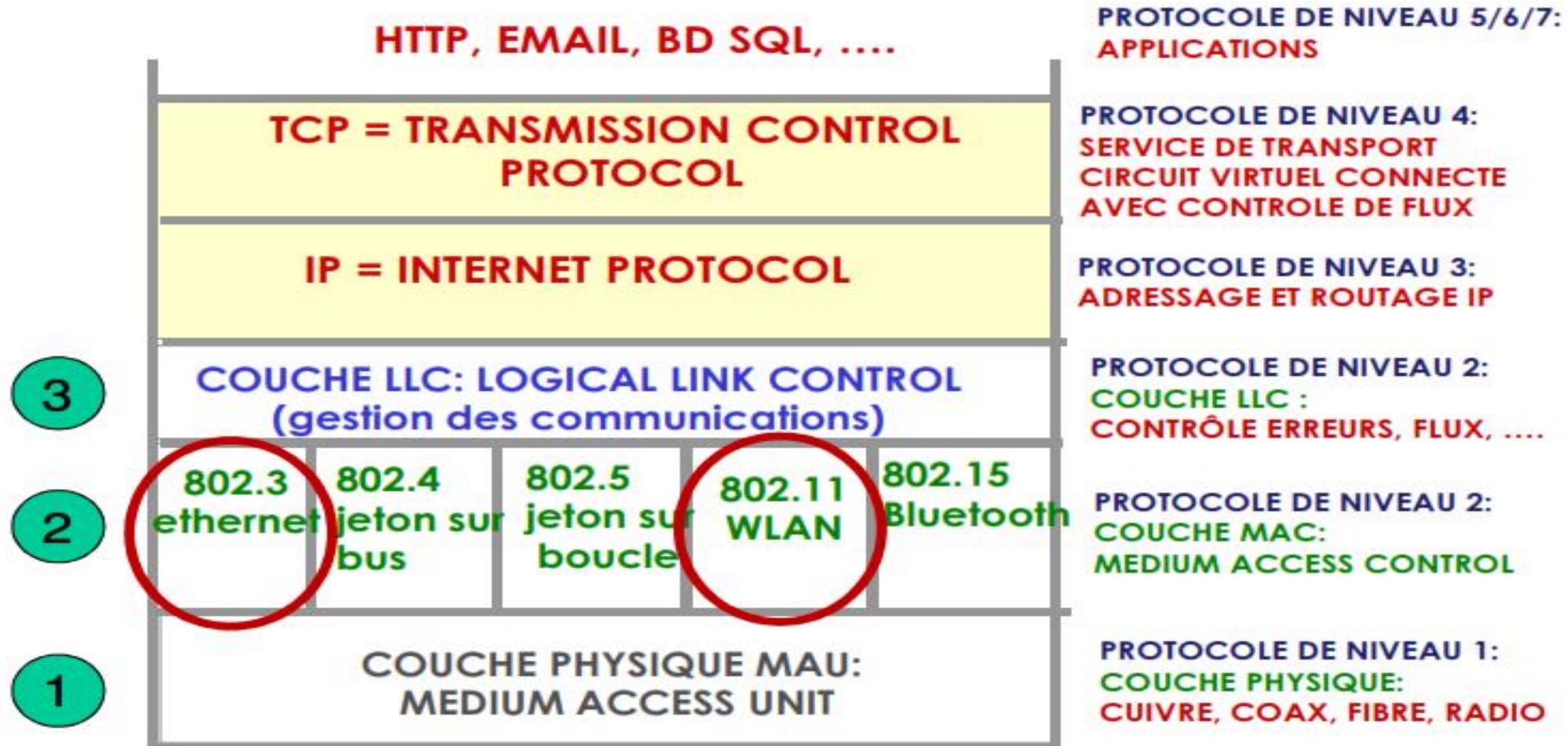
## Ethernet et le modèle OSI

- 💡 La technologie Ethernet opère au niveau de la **couche physique** et de la **couche liaison de données** (la couche MAC seulement).
  
- 💡 Lorsque plusieurs terminaux communiquent par le biais d'un média partagé, les données passent le plus souvent par un **répéteur** (accessoirement multi ports).
  
- 💡 Toutes les stations connectées à ce même média « voient » donc ce trafic.
  
- 💡 Elles communiquent entre elles également par ce même média.

.B



# Couche 2 (LD): Technologies Ethernet 3/16



.B



# Couche 2 (LD): Technologies Ethernet 4/16

## SPÉCIFICATIONS ET NORMES

L'IEEE a défini des normes pour les différentes technologies Ethernet :

| Norme   | Appellation         | Débit       | Média utilisé                 |
|---------|---------------------|-------------|-------------------------------|
| 802.3   | Ethernet            | 10 Mbps     | Coaxial / UTP / fibre optique |
| 802.3u  | Fast Ethernet       | 100 Mbps    | UTP / Fibre optique           |
| 802.3z  | Gigabit Ethernet    | 1000 Mbps   | Fibre optique                 |
| 802.3ab | Gigabit Ethernet    | 1000 Mbps   | Câble UTP                     |
| 802.3ae | 10 Gigabit Ethernet | 10 000 Mbps | Fibre Optique                 |

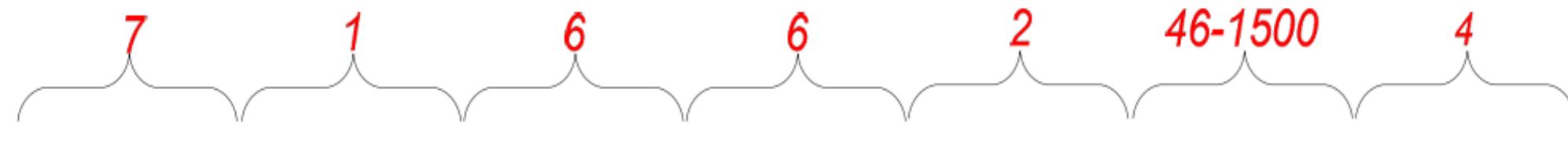


.B

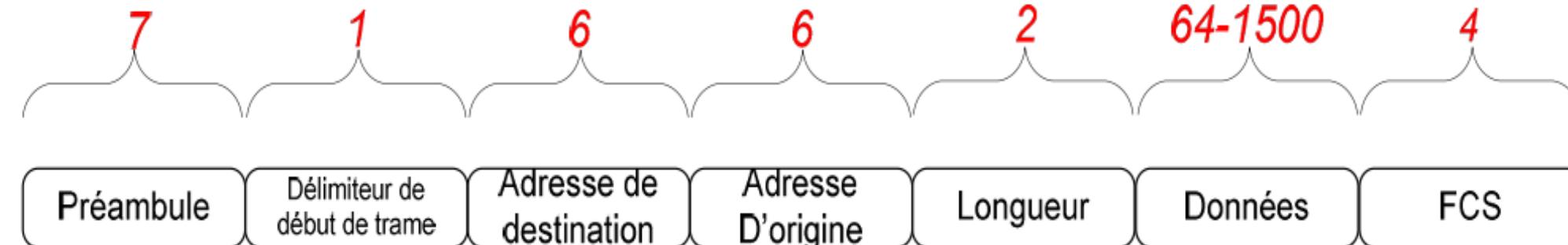


# Couche 2 (LD): Technologies Ethernet 5/16

## TRAMES ETHERNET ET IEEE 802.3



Trame Ethernet



Trame IEEE 802.3

.B



# Couche 2 (LD): Technologies Ethernet 6/16

## TRAMES ETHERNET ET IEEE 802.3

- **Préambule** : composé de 1 et de 0 en alternance, annonce si la trame est de type Ethernet ou 802.3.
- **Début de trame** : IEEE 802.3 : l'octet séparateur se termine par 2 bits à 1 consécutifs, servant à synchroniser les portions de réception des trames de toutes les stations.
- **Champ d'adresse de destination** : peut être de type unicast, multicast ou broadcast.
- **Champ d'adresse d'origine** : toujours de type unicast.
- **Type (Ethernet)** : précise le type de protocole de couche supérieure qui reçoit les données.
  
- **Longueur (802.3)** : indique le nombre d'octets de données qui suit le champ.
  - ✓ C'est sur cette partie que diffèrent les trames 802.3 et Ethernet : la valeur du champ permet de déterminer le type de trame : 802.3 ou Ethernet.
  - ✓ La trame est de type 802.3 si la valeur hexadécimale du champ est strictement inférieure à 0X600 ; La trame est de type Ethernet si la valeur hexadécimale du champ est égale à 0X600.

.B



## TRAMES ETHERNET ET IEEE 802.3

### **Données :**

- ✓ **Ethernet** : une fois le traitement de couche 1 et 2 terminé, les données sont transmises au protocole de la couche supérieure indiqué dans le champ type. On peut avoir recours à des octets de remplissage s'il n'y a pas assez de données pour remplir les 64 octets minimaux de la trame.
- ✓ **IEEE 802.3** : une fois le traitement de couche 1 et 2 terminé, les données sont transmises au protocole de la couche supérieure indiqué dans le champ donnée trame. On peut ici aussi avoir recours au remplissage.
- ✓ **FCS** : Séquence de contrôle de trame. Cette séquence contient un code de redondance cyclique permettant à l'unité réceptrice de vérifier l'intégrité des données transmises.

.B



## MAC :MEDIA ACCESS CONTROL

- Le principe utilisé pour partager l'accès à des ressources communes est appelé MAC pour Media Access Control (à ne pas confondre avec l'adresse MAC).
- Dans un environnement où plusieurs hôtes se partagent un média unique de communication, un **problème de priorité** doit être résolu.
- Dans un environnement Ethernet, c'est au niveau de la **sous-couche MAC** que l'on va utiliser un processus de **détection des collisions** : plusieurs hôtes émettent en même temps sur le même média.
- **Ethernet et 802.3** utilisent un principe d'accès au média non déterministe : **CSMA/CD** (Carrier SensMultiple Access with Collision Detection).
- Les hôtes se partagent donc le média. Si l'un d'eux désire émettre, il **vérifie au préalable que personne n'est en train de le faire**, puis commence à émettre (CSMA).

.B



 **MAC :MEDIA ACCESS CONTROL**

Si cependant **2 hôtes émettent en même temps**, il se produit alors une **collision**. La première station qui détecte une collision **envoie alors un signal de bourrage**, se traduisant par un **arrêt d'émission** de tous les hôtes. Les paquets concernés sont alors détruits.

Chaque hôte **calcule alors une valeur aléatoire définissant la durée avant de recommencer à émettre**, puis le mécanisme de CSMA se remet en fonction.



.B



## ERREURS POSSIBLES

### Collisions

Dans un environnement partagé, la première corruption rencontrée est de type collision. Lorsque deux hôtes ou plus émettent un signal au même instant sur le média, il se produit un **survoltage** qui ne signifie plus rien en terme de données. Ces collisions ne se produisent que dans **un environnement Half-Duplex**. (car dans un environnement Full-Duplex, chaque paire torsadée n'est utilisée qu'entre deux hôtes dans un seul sens de transmission.). L'algorithme CSMA/CD permet de détecter ces collisions et de les éviter.

Il existe trois types de collision :

-  **Collision locale**: La collision locale est de type survoltage.
-  **Collision distante**: Une collision distante résulte d'une trame ayant une longueur inférieure au minimum ou d'un FCS incorrect
-  **Collision de retard** :Une collision de retard n'est pas détectée par la couche liaison de données. En effet, elle est caractérisée par une erreur dans les données à partir du 64<sup>ème</sup> octet.

.B



 **ERREURS POSSIBLES** **Trames longues**

Ce type d'erreur est un simple dépassement de la taille maximale d'une trame.

- ✓ La taille du champ « Données » (variable) d'une trame ne doit pas excéder 1500 octets.
- ✓ Une trame a donc une taille maximale de **1526 octets**.
- ✓ Une trame de taille supérieure est donc considérée comme fausse.

 **Trames courtes**

- ✓ Comme pour les trames longues, l'erreur se situe au niveau du champ « données » qui doit avoir une taille minimale de **46 octets (ou 64 pour IEEE 802.3)**.
- ✓ Les trames courtes se caractérisent donc par une taille inférieure à 72 octets (ou 90 octets pour IEEE 802.3) mais avec un FCS valide : sinon elle serait considérée comme un fragment de trame, détruit lui aussi.



.B



 ERREURS POSSIBLES **Autres types d'erreur**

D'autres erreurs peuvent survenir du fait de la mauvaise qualité du média (ou d'interférences extérieures) :

- ✓ **FCS incorrect** : le résultat du FCS est faux quant aux données transmises
- ✓ **le champ longueur ne concorde pas** avec la taille du champ « données »
- ✓ **longueur de champ incorrecte** : le préambule ne fait pas 7 octets, ...



.B



## DOMAINE DE COLLISION

On appelle domaine de collision **la partie d'un réseau comprenant un environnement partagé.**

C'est dans ce domaine que les hôtes vont accéder en concurrence à une ressource. De ce fait, des collisions vont se créer sur cette partie du réseau. Le domaine de collision s'étend sur la plus grande partie du réseau contenant des équipements de couche 1 interconnectés.

.B



 **SEGMENTATION**

Le principe de la segmentation est de **n'envoyer des données que sur la portion de réseau concernée**. On va ainsi réduire le trafic inutile, ainsi que le nombre d'utilisateurs concurrents du même média.

Pour la segmentation, des **équipements de couche 2** sont nécessaires. C'est à ce niveau que l'on peu prendre des décisions d'adressage (sur quel média transmettre une trame).



.B



 **SEGMENTATION** **Segmentation par ponts**

Les ponts permettent de segmenter un réseau en n'envoyant les données que sur la partie du réseau concernée. Après avoir appris sur quelle portion se trouvent les hôtes (par leur adresse mac), un pont

filtrera le trafic suivant l'adresse de destination. Il laissera donc transiter les données vers la partie du réseau qui contient l'adresse de destination, et bloquera les paquets qui ne sont pas destinés à cette même partie.

.B



## SEGMENTATION

### Segmentation par commutateurs

Les commutateurs sont l'équivalent de **répéteurs multi ports intelligents**. Chaque hôte ou groupe d'hôtes connecté à un port du commutateur veut envoyer des données. Au lieu de retransmettre ces données sur chaque port, le commutateur ne va renvoyer que sur le port où se trouve la partie du réseau contenant le(s) destinataire(s).

Pour se faire, le commutateur va apprendre les adresses MAC de chaque hôte connecté à ses ports. Il saura ainsi quels hôtes se trouvent sur chacun de ses ports. Il stocke ces données dans une table d'adresses MAC.

Les commutateurs fonctionnent beaucoup plus vite que les ponts et créent des domaines sans collisions entre 2 ports en interne (par l'utilisation de circuits virtuels).

.B

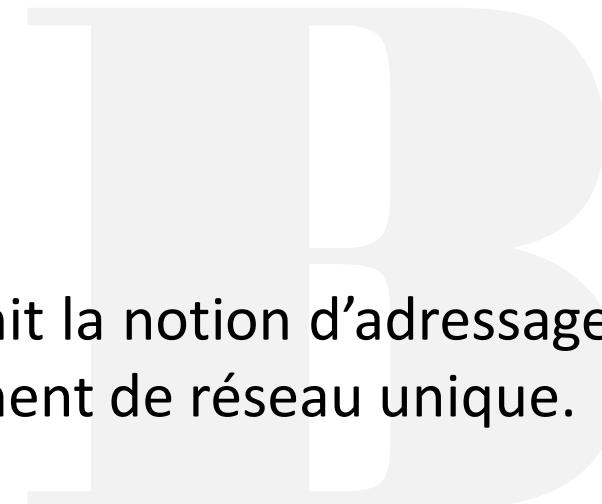


# Couche 3 : Réseau



 **PROTOCOLES ROUTABLES**

- 💡 **Protocole** : Ensemble formel de règles et de conventions qui régit l'échange d'informations entre des unités.
  
- 💡 **Un protocole routable** définit la notion d'adressage hiérarchique : un hôte est défini par une adresse unique sur un segment de réseau unique.
  
- 💡 **Un protocole de routage** (à ne pas confondre avec protocole routable), grâce à la structure du protocole routé, a toutes les informations nécessaires pour envoyer un paquet sur le segment spécifié à l'hôte spécifié.



.B



## PROTOCOLES ROUTABLES

### Protocoles orientés connexion:

- ✓ Un **protocole orienté connexion** définit un chemin unique entre l'hôte source et l'hôte de destination.
- ✓ Les **paquets empruntent alors le même chemin** et arrivent donc dans le **même ordre**.  
Pour ce faire l'hôte source établit en premier lieu une connexion avec l'hôte de destination.
- ✓ Une fois cette connexion établie, chaque paquet est envoyé par ce seul chemin. On appelle ce processus « commutation de circuits ».
- ✓ Le protocole **TCP** est un protocole orienté connexion.

.B



 **PROTOCOLES ROUTABLES** **Protocoles non orientés connexion :**

- ✓ Un protocole non orienté connexion **ne définit pas de chemin unique** pour acheminer les paquets d'un hôte source vers un hôte de destination.
- ✓ Les paquets peuvent alors **emprunter des chemins différent** suivant la topologie réseau existante entre ces deux hôtes.
- ✓ Cela implique une **durée de trajet différent** pour chaque paquet et donc un ordre d'arrivée différent de celui d'émission.
- ✓ **L'hôte de destination peut pas réordonner les paquets.**
- ✓ Le protocole **IP** est un protocole non orienté connexion.

.B



## PROTOCOLES ROUTABLES

-  **Protocoles routés :**
-  **Protocole routé :** c'est un protocole de communication de couche 3. Il **définit le format des paquets**, et notamment la manière de désigner le destinataire du paquet. Un protocole routé peut être routable ou non routable.
-  **Routable :** les messages envoyés à l'aide de ce protocole **peuvent sortir de leur réseau** (via un routeur). En effet, le format du paquet comprend une distinction entre la partie hôte et la partie réseau.
-  **Non routable :** les messages envoyés à l'aide de ce protocole **ne peuvent pas sortir de leur réseau**. En effet, le format du paquet ne comprend pas de mécanisme permettant à un élément réseau de faire suivre ces paquets au travers de différents réseaux.

.B



## PROTOCOLES ROUTABLES

### Protocoles routés :

La liste des protocoles routés suivante présente les protocoles les plus connus :

| Nom du protocole routé | Protocole routable ? |
|------------------------|----------------------|
| IP                     | Oui                  |
| IPX                    | Oui                  |
| Appletalk              | Oui                  |
| CLNP                   | Oui                  |
| NetBEUI                | Non                  |
| SNA                    | Non                  |

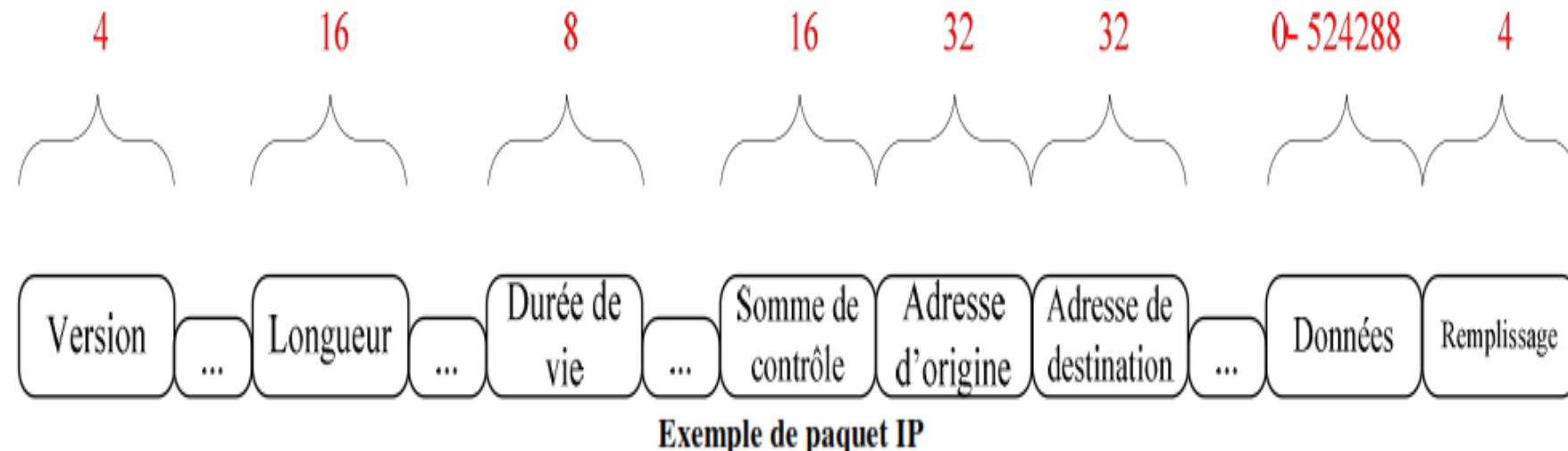
IB



## PROTOCOLE IP

### Paquet IP

Les informations provenant de la couche 4 sont encapsulées dans le PDU de couche 3 : **le paquet**, dont voici les principaux éléments :



JB



## PROTOCOLE IP

### Paquet IP

| Champs                 | Description  |
|------------------------|--|
| Version                | Indique la version de protocole IP utilisée (4 bits).  |
| Longueur totale        | Précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits).   |
| Durée de vie           | Un compteur qui décroît graduellement, par incrément, jusqu'à zéro. À ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle (8 bits). |
| Somme de contrôle      | Assure l'intégrité de l'en-tête IP (16 bits).  |
| Adresse d'origine      | Indique le nœud émetteur (32 bits).  |
| Adresse de destination | Indique le nœud récepteur (32 bits).   |
| Données                | Cet élément contient des informations de couche supérieure (longueur variable, maximum 64 Ko).   |
| Remplissage            | Des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP soit toujours un multiple de 32 bits.  |



IB

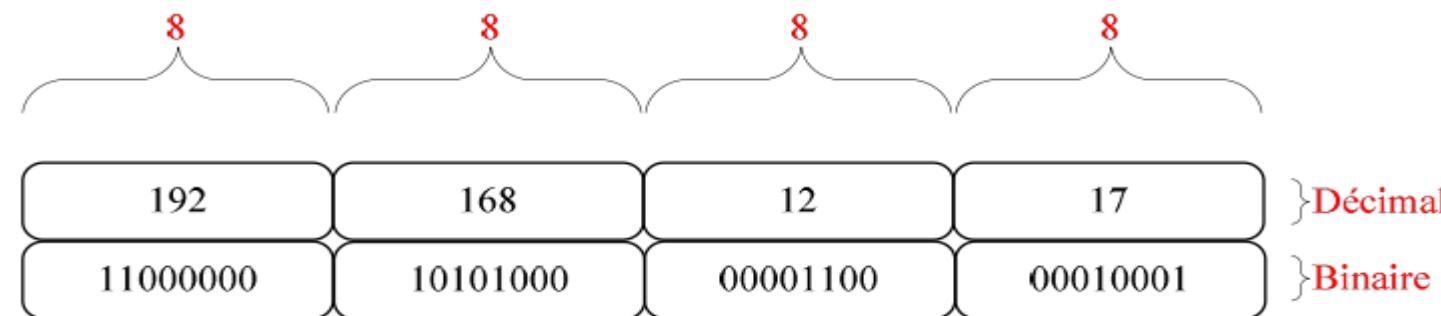


# Couche 3(R) : Protocole IP 8/19

## ADRESSAGE IP

Comme nous l'avons vu, une adresse IP est une adresse **32 bits** notée sous forme de 4 nombres décimaux séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- Une partie désignant le réseau (on l'appelle **netID**)
- Une partie désignant les hôtes (on l'appelle **host-ID**)



Exemple d'adresse IP

JB



## ADRESSAGE IP

### Classes d'adresses IP

L'organisme chargé d'attribuer les adresses IP publiques est l'InterNIC (Internet Network InformatioCenter).

#### Classe A de 1.x.x.x à 127.x.x.x

- ↳ 127 réseaux –
- ↳ 16777214 machines



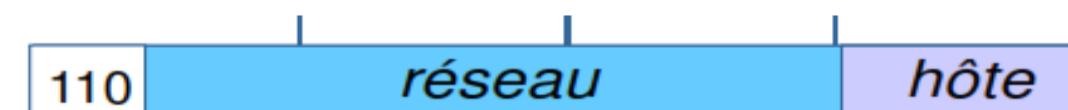
#### Classe B de 128.0.x.x à 191.255.x.x

- ↳ 16384 réseaux –
- ↳ 65534 machines



#### Classe C de 192.0.0x à 223.255.255.x

- ↳ 2097152 réseaux –
- ↳ 254 machines

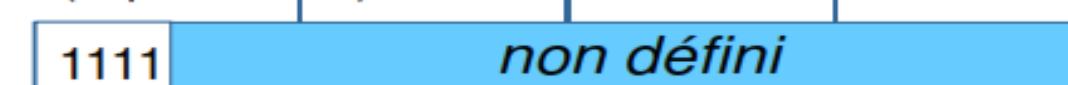


#### Classe D de 224.0.0.0 à 239.255.255.255

(multicast)



#### Classe E de 240.0.0.0 à 255.255.255.255 (Expérimentale)



JB



## ADRESSAGE IP

### Masque de réseau ou Netmask

- **Masque du réseau** : adresse IP particulière servant à identifier l'adresse du réseau à partir d'une adresse IP de machine.
  - Le masque d'un réseau de classe A = 255.0.0.0
  - Le masque d'un réseau de classe B = 255.255.0.0
  - Le masque d'un réseau de classe C = 255.255.255.0
  - Dans le cas d'un réseau découpé en sous-réseau : le masque est calculé en mettant tous les bits du préfix réseaux à la valeur binaire « 1 », et tous les bits associés au suffix à « 0 ».
- **Adresses réseau** : adresse IP dont la partie « hostid » ne comprend que des zéros;
  - => la valeur zéro ne peut être attribuée à une machine réelle : 192.20.0.0 désigne le réseau de classe C 192.20.0
- **Adresse machine locale** : adresse IP dont le champ réseau (netid) ne contient que des zéros;
  - Exemple 0.0.25.1



.B



## ADRESSAGE IP

### **Masque de réseau ou Netmask**

- Permet à une station de savoir si la station destination est dans le même réseau qu'elle ou s'il faut envoyer son paquet au routeur qui l'acheminera,
- Exemple station A veut envoyer un paquet à une station B :
  - @ IP A = 172.16.2.4
  - @ IP B = 172.16.3.5
  - @ netmask A : 255.255.0.0
- La station A doit réaliser 3 opérations :
  1. @ A AND @ netmask A = Res 1
  2. @ B AND @ netmask A = Res 2
  3. comparer Res 1 et Re 2
    - Si Res 1 = Res2 alors station sur le même réseau
    - Sinon station sur des réseaux distants



IB



## ADRESSAGE IP

| A | B | A AND B |
|---|---|---------|
| 0 | 0 | 0       |
| 0 | 1 | 0       |
| 1 | 0 | 0       |
| 1 | 1 | 1       |

## Netmask (2)

172 . 16 . 2 . 4 (@ IP A)  
10101100 . 00010000 . 00000010 . 00000100  
11111111 . 11111111 . 00000000 . 00000000 (mask A = 255.255.0.0)  
10101100 . 00010000 . 00000000 . 00000000 (@ du réseau classe B 172.16.0.0)

172 . 16 . 3 . 5 (@ IP B)  
10101100 . 00010000 . 00000011 . 00000101  
11111111 . 11111111 . 00000000 . 00000000 (mask A = 255.255.0.0)  
10101100 . 00010000 . 00000000 . 00000000 (@ du réseau B 172.16.0.0)

JB



ADRESSAGE IP

## Netmask (3)

**Autre exemple @ IP C = 125.128.96.12**

172 . 16 . 2 . 4 (@ IP A)  
10101100 . 00010000 . 00000010 . 00000100  
11111111 . 11111111 . 00000000 . 00000000 (mask A = 255.255.0.0 - classe B)  
10101100 . 00010000 . 00000000 . 00000000 (@ du réseau classe B 172.16.0.0)

125 . 128 . 96 . 12 (@ IP C)  
01111111 . 10000000 . 01100000 . 00001100  
11111111 . 11111111 . 00000000 . 00000000 (mask A = 255.255.0.0)  
01111111 . 10000000 . 00000000 . 00000000 (@ du réseau classe A 125.128.0.0)



JB



## IPV4 ET IPV6 (IPNG / IP NEXT GENERATION)

**Le protocole IPv4**, le standard actuel, était censé avoir une taille suffisante pour fournir des adresses IP ( $2^{32}$ , soit 4 294 967 296 adresses possibles). Néanmoins cette limite est en passe d'être atteinte.

Différentes solutions ont été mises en place, dans un premier temps afin de réduire cette consommation d'IP.

**IPv6 emploie 128 bits** à la place des 32 bits actuellement utilisés par IPv4. IPv6 emploie des nombres **hexadécimaux** pour représenter une adresse, alors qu'IPv4 utilise des nombres décimaux. IPv6 fournit  $3,4 \times 10^{38}$  adresse IP ( $2^{128}$ ). Cette version d'IP devrait donc fournir assez d'adresses pour les futurs besoins des nouveaux pays développés.

*Exemple d'une adresse IP v6 :*

Valeur

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Valeur

21DA:D3::2F3B:2AA:FF:FE28:9C5A

simplifiée:

Nombre d'octets utilisés : 16

*Exemple d'une adresse IP v4 :*

Valeur : 34.208.123.12

Nombre d'octets utilisés : 4

JB



## GESTION DES ADRESSES IP

### Méthodes d'obtention

On distingue 2 méthodes d'attribution d'adresses IP pour les hôtes :

-  **Statique** : chaque équipement est configuré manuellement avec une adresse unique
-  **Dynamique** : On utilise des protocoles qui attribuent des IP aux hôtes

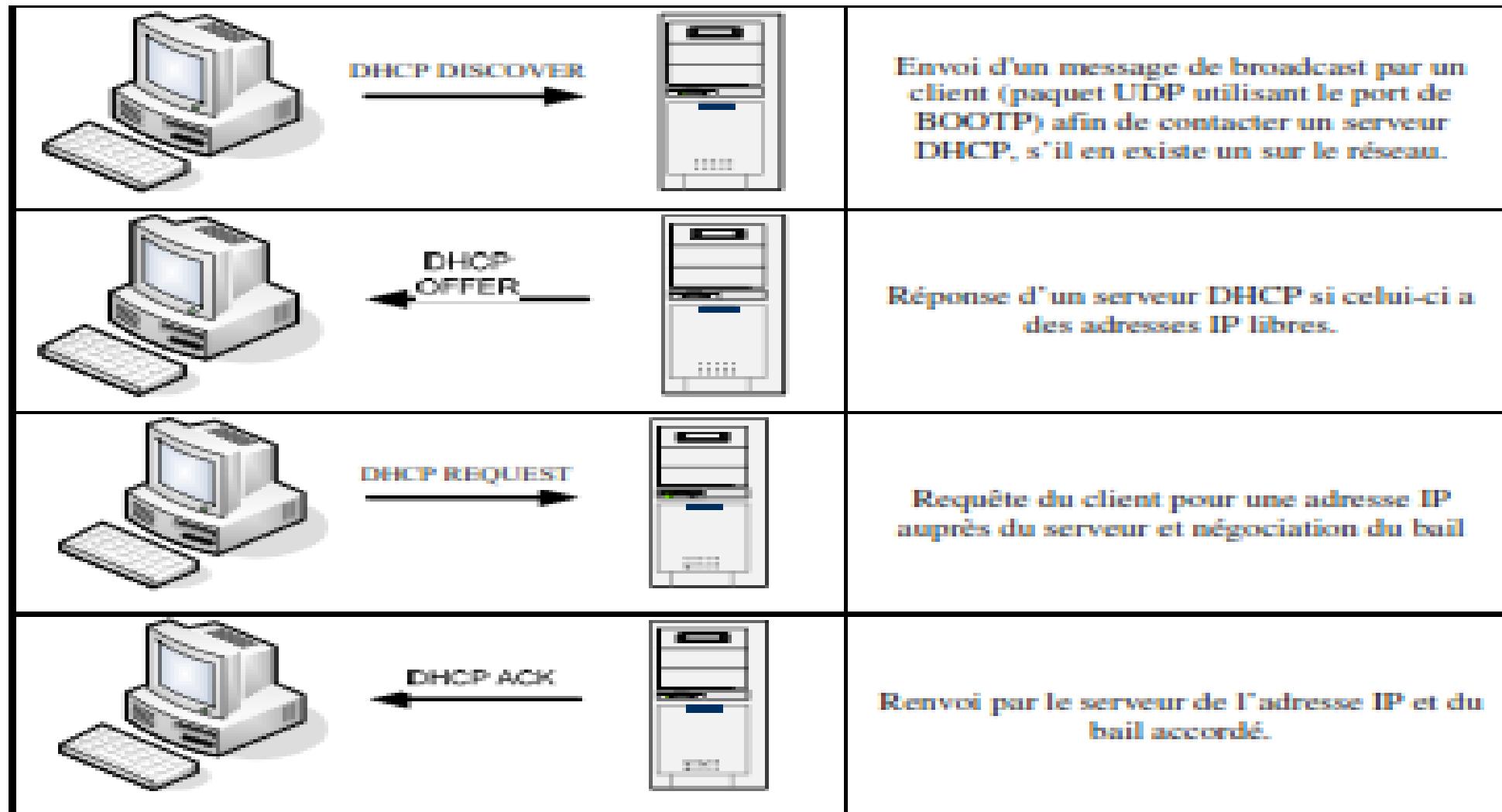
- ✓ **RARP** : Protocole associant les adresses MAC aux adresses IP. Il permet à de stations sans disque dur local connaissant leur adresse MAC de se voir attribuer un IP.
- ✓ **BOOTP** : Ce protocole permet à un équipement de récupérer son adresse IP au démarrage. L'émetteur envoi un message de broadcast (255.255.255.255) reçu par le serveur qui répond lui aussi par un broadcast contenant l'adresse MAC de l'émetteur ainsi qu'une IP.
- ✓ **DHCP** : Remplaçant de BOOTP, il permet l'obtention dynamique d'IP. Lorsqu'un ordinateur entre en ligne, il communique avec le serveur qui choisit une adresse et un masque de sous réseau et l'attribue à l'hôte. Il permet de plus d'obtenir des serveur DNS, la passerelle par défaut ainsi qu'optionnellement les adresses des serveur WINS.



JB



## GESTION DES ADRESSES IP



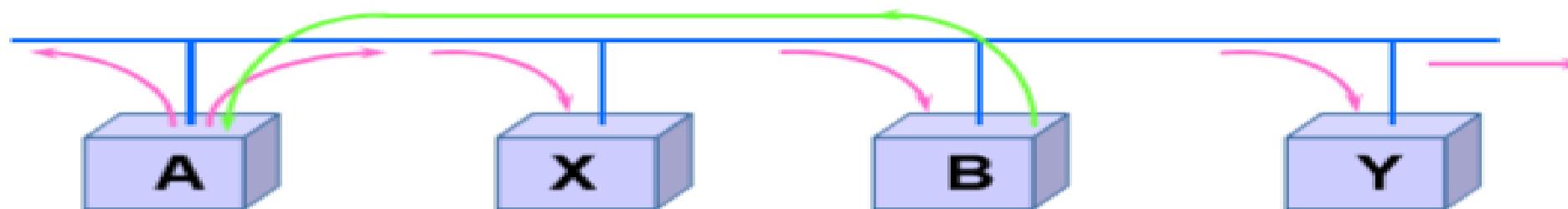
IB



## GESTION DES ADRESSES IP

# ARP

- L'association **adresse physique - adresse IP** de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache,



- Pour connaître l'adresse physique de B (PB) à partir de son adresse IP (IB), la machine A **diffuse une requête ARP** qui contient l'adresse IP de B (IB) vers toutes les machines;
- la machine B **répond avec un message ARP** qui contient la paire (IB, PB).
- Rem : champ type de la trame Ethernet: 0806 pour ARP

JB



## GESTION DES ADRESSES IP

### Le protocole RARP

Le protocole RARP (Reverse Address Resolution Protocol) **permet de connaître l'adresse IP d'un hôte, à partir de son adresse physique.**

Lorsqu'une machine ne connaît que l'adresse physique d'un dispositif, elle peut émettre une requête RARP afin d'avoir son adresse IP.



JB



## RÉSOLUTION D'ADRESSES

- **Le protocole ICMP**

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de **gérer les informations relatives aux erreurs générées au sein d'un réseau IP**. Etant donné le peu de contrôles que le protocole IP réalise, il permet, non pas de corriger ces erreurs, mais de **faire part de ces erreurs**.

Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour reporter une erreur (appelé Delivery Problem).

Un exemple typique d'utilisation du protocole ICMP est la **commande Ping**. Lors de l'exécution de cette commande, des informations précises peuvent être obtenues : le temps mis par un paquet pour atteindre une adresse, ou bien un éventuel problème de routage pour atteindre un hôte.

JB



# TCP/IP

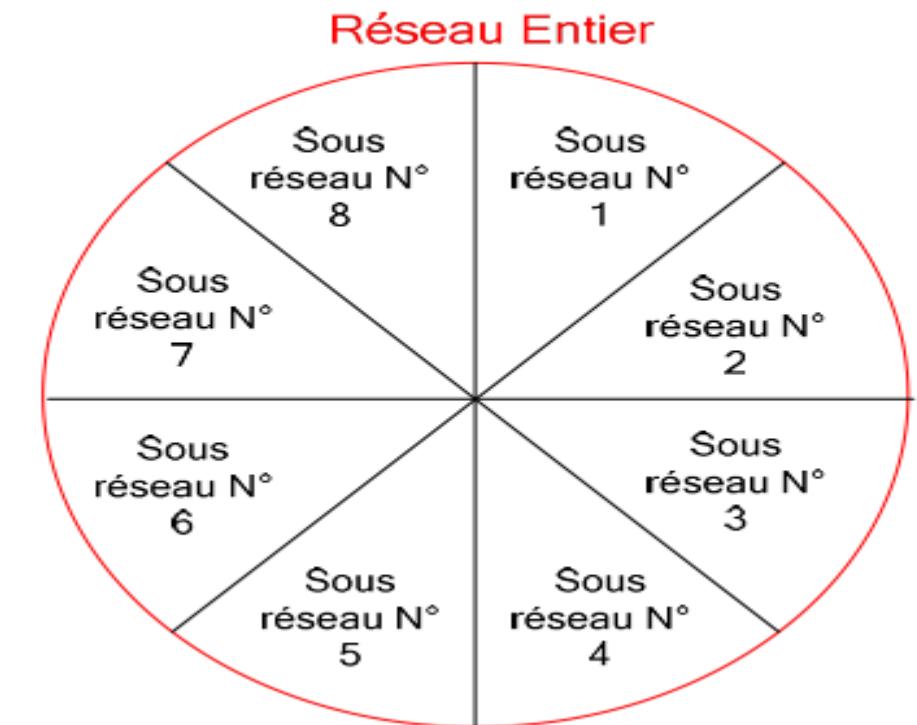
## Couche 3 (R) : Subnetting 1/7

### INTÉRÊT DU SUBNETTING

Afin d'augmenter les capacités de gestion de trafic dans un réseau, il est possible de subdiviser ce dernier en plusieurs sous réseaux afin de permettre une **segmentation des domaines de broadcast**.

Pour cela, on emprunte à la partie hôte des bits que l'on désigne comme champ de sous réseaux.

Le nombre minimal de bits à emprunter est de **2** et le nombre maximal est égal à tout nombre laissant 2 bits à la partie hôte.



.B

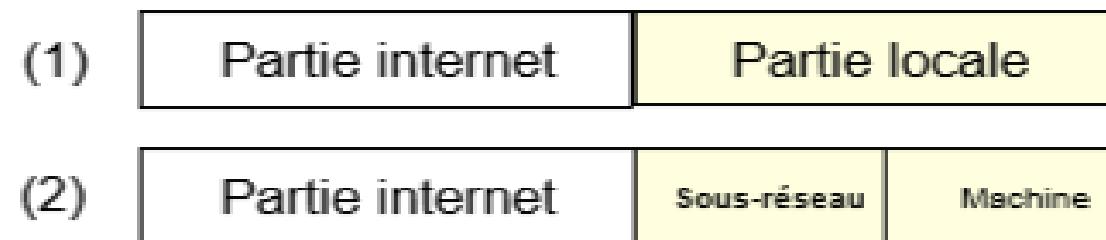




# Couche 3 (R) : Subnetting 2/7

## INTÉRÊT DU SUBNETTING

- **Constat** : Un site ne contient pas un réseau mais un ensemble de réseaux (exemple : UVSQ)
- **Solution** : scinder une classe en sous-réseaux (ou segment):
  - La partie numéro de machine devient le numéro de sous-réseau et le numéro de la machine dans ce sous-réseau,
  - Combien de bits (n) utiliser pour représenter les sous-réseaux ?
    - Si (p) sous-réseaux à représenter alors  $p \geq (2^n)$
  - Nombre de bits alloués au numéro de sous-réseau est configurable : c'est le « **sub-netmask** » ou simplement le « **netmask** » du sous-réseau



IB



## SUBNETTING: MÉTHODES DE CALCUL

### Méthode classique

On entend par méthode classique le fait de procéder sans formule spécifique, par la méthode calculatoire. Cette méthode se détaille en 6 étapes :

- ✓ Empruntez le nombre de bits suffisants
- ✓ Calculez le nouveau masque de sous réseau
- ✓ Identifiez les différentes plages d'adresses IP
- ✓ Identifiez les plages d'adresses non utilisables
- ✓ Identifiez les adresses de réseau et de broadcast
- ✓ Déterminez les plages d'adresses utilisables pour les hôtes.



JB



 SUBNETTING: MÉTHODES DE CALCUL

## Exemple

- Soit un réseau d'entreprise de classe B = 130.96.0.0 constitué de 8 sous-réseaux locaux.
- Pour identifier 8 sous-réseaux, combien de bits faut il prendre de la partie Host-id ?
  - 3 bits ? =>  $2^3 - 2 = 6$  (insuffisant !!!)
  - 4 bits ? =>  $2^4 - 2 = 14$  (Oui !!!)
- **Masque de sous-réseau** = 255.255.240.0
- **Exemple d'adresse de diffusion restreinte** = 130.96.175.255 pour le **sous-réseau** de net-id = 130.96.160.0



.B





# Couche 3 (R) : Subnetting 5/7

## SUBNETTING: MÉTHODES DU NOMBRE MAGIQUE

Cette méthode se détaille en 6 étapes :

- ❶ Calculer Le **nombre magique** est simplement un calcul fait à partir de l'octet significatif du masque.
  - ❷ **256 - octet significatif.**
- ❷ Il va nous permettre de calculer instantanément la première et la dernière adresse de notre plage.
- ❸ écrire tous les **multiples du nombre magique** (jusqu'à 256 bien sûr)
- ❹ La première adresse du réseau sera le **multiple du nombre magique**, inférieur ou égal à l'**octet correspondant dans l'adresse**.
- ❺ La dernière adresse du réseau sera le **multiple suivant, moins 1**.

.B





# Couche 3 (R) : Subnetting 6/7

## SUBNETTING: MÉTHODES DU NOMBRE MAGIQUE

**Exemple:**

Réseau d'entreprise d'adresse : 192.168.0.1/255.**224**.0.0

**Notre nombre magique vaut donc  $256 - 224 = 32$**

Allons-y pour les multiples de 32 ! 0, 32, 64, 96, 128, **160**, **192**, 224, 256

la première adresse du réseau sera donc le multiple du nombre magique, strictement inférieur à 168. En regardant la liste des multiples, on trouve très vite **160** !.

**donc 192.160.0.0**

La dernière adresse du réseau sera le multiple suivant, moins 1. Le multiple suivant est 192. Auquel on enlève 1 pour trouver **191**.

**donc 192.191.255.255**

La première adresse de la plage est donc **192.160.0.0** et la dernière **192.191.255.255**.

.B





# Couche 3 (R) : Subnetting 7/7

## SUBNETTING: MÉTHODES DU NOMBRE MAGIQUE

**Exemple:**

Réseau d'entreprise d'adresse : 10.45.**185**.24/255.255.**248**.0

**Notre nombre magique vaut donc  $256 - 248 = 8$**

Allons-y pour les multiples de 32 ! 160, 168, 176, 184, 192... STOP ! On est au dessus de 185.  la première adresse du réseau sera donc le multiple du nombre magique, strictement inférieur à 185. En regardant la liste des multiples, on trouve très vite **184** !. La dernière adresse du réseau sera le multiple suivant, moins 1. Le multiple suivant est 192. Auquel on enlève 1 pour trouver **191**.

Ce qui nous donne pour la première adresse **10.45.184.0**, et pour la dernière **10.45.191.255**.

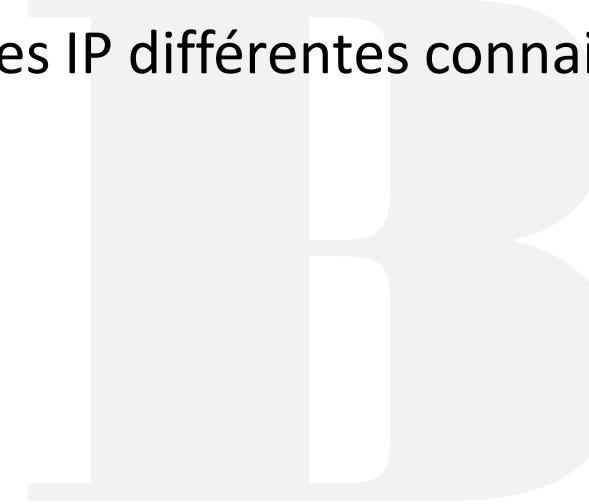
JB



# Couche 3 (R) : IP, Adressage 1/6

## Exercice 1. CLASSES D'ADRESSAGE

- a) Qu'est-ce que CIDR et VLSM ? pourquoi les a-t-on introduit à partir de 1994 ?
- b) Combien de types d'adresses IP différentes connaissez vous ? Citez les et donnez un exemple pour chacun d'eux.



# Couche 3 (R) : IP, Adressage 2/6

## [solution Exercice 1. CLASSES D'ADRESSAGE](#)

IB





## Couche 3 (R) : IP, Adressage 3/6

### Exercice 2: MASQUE DE RESEAUX

- a) Quelle est la fonction du masque de réseaux sur un terminal IP ?
- b) A quel moment le terminal fait il usage du masque ?
- c) Pour chacune des classes d'adresses globales (A, B et C) donner le masque de réseau associé.
- d) Soit une machine d'adresse IP 197.178.0.52/24. De quelle classe est cette adresse ? Quel est le masque du réseau ? Quelle est l'adresse du réseau ? Définir l'adresse de diffusion globale et l'adresse de diffusion restreinte pour ce réseau.
- e) Les adresses de diffusion traversent-elles les routeurs ?
- f) Soit la machine C possédant l'adresse 192.168.0.140/255.255.255.128. Nous voulons savoir si les machines A et B ayant respectivement pour adresses 192.168.0.20 (A) et 192.168.0.185 (B) sont sur le même réseau ?



# Couche 3 (R) : IP, Adressage 4/6

## solution Exercice 2: MASQUE DE RESEAUX

JB





## Couche 3 (R) : IP, Adressage 5/6

### Exercice 3: SUBDIVISION DE RESEAUX

a) Quelle est l'intérêt de la subdivision de réseaux ?

Vous êtes l'administrateur du réseau de votre entreprise, à qui l'on vient d'attribuer l'adresse IP 214.123.155.0. Vous devez créer 8 sous-réseaux distincts pour les 8 succursales de l'entreprise, à partir de cette adresse IP.

b) Quel est la classe de ce réseau ?

c) Quel masque de sous-réseau devez vous utiliser pour optimiser votre plan d'adressage ?

d) Combien d'adresses IP (machines ou routeurs) pourra recevoir chaque sous-réseau?

e) Quelle est l'adresse réseau et de broadcast du 5ème sous-réseau utilisable ?

f) Combien d'adresses IP distinctes est-il possible d'utiliser avec un tel masque, tous sous-réseaux possibles confondus ?





# Couche 3 (R) : IP, Adressage 6/6

## solution Exercice 3: SUBDIVISION DE RESEAUX

JB



# Couche 3 (R) : IPV6 1/24

## Pourquoi ipv6?

-  Espace d'adressage infini (on passe de 32 à 128bits)
-  Auto configuration des postes
-  Adresses multiples par interface
-  Adressage privé unique
-  Plus de broadcasts (remplacer par des multicast)
-  Intégration obligatoire du Ipsec
-  Entête IP moins gourmant /facilité de renumérotation du réseau
-  Diffusion multimédia facilitée
-  Mobilité facilité



## Fonctionnalités d'IPv6

IPv6 apporte un certain nombre de nouvelles fonctionnalités :

 **Un plus grand espace d'adressage:**

Permettra de déployer de nouvelles applications nécessitant des communications de bout en bout (téléphonie mobile, vidéoconférence, applications en temps réel).

- ✓ de 32 bits >> 128bits
- ✓ Plus besoin du NAT
- ✓ Plus besoin d'adresse de broadcaste



.B



## Fonctionnalités d'IPv6

IPv6 apporte un certain nombre de nouvelles fonctionnalités :

 **Un entête simplifié et efficace:**

l'entête IPv6 est de taille fixe

les extensions IPv6 ne seront gérées que par les équipements terminaux. Les équipements intermédiaires sont donc déchargés d'une partie des traitements. La gestion des paquets erronés est déléguée aux équipements d'extrémité et aux couches supérieures telles TCP ou UDP.

*En-tête IPv6 de base*

| Version                    | Traffic Class | Flow Label | Payload Length | Next Header | Hop Limit |
|----------------------------|---------------|------------|----------------|-------------|-----------|
| Source IPv6 (128bits)      |               |            |                |             |           |
| Destination IPv6 (128bits) |               |            |                |             |           |

- Version : version du protocole (4 bits).
- Traffic Class : gestion de qualité de service (8 bits).
- Flow Label : marquage de flux pour traitement différencié dans le réseau (20 bits).
- Payload Length : taille du contenu en octets (16 bits).
- Next Header : identification de l'entête suivant (8 bits).
- Hop Limit : durée de vie du paquet, décrémenté d'une unité à chaque passage par un routeur. Le paquet est détruit si la valeur tombe à 0 (8 bits).

JB



## Fonctionnalités d'IPv6

IPv6 apporte un certain nombre de nouvelles fonctionnalités :

### **L'auto-configuration:**

Elle met en œuvre un certain nombre de nouveaux protocoles associés à IPv6 (protocole de découverte des voisins, nouvelle version d'ICMP ...). L'auto-configuration permet à un équipement de devenir complètement "plug and play". Il suffit de connecter physiquement la machine pour qu'elle acquière une adresse IPv6 et une route par défaut.

### **Le support de la mobilité:**

Se caractérise par le fait d'être connecté et de disposer de son environnement tout en se déplaçant et ce, sans interruption de service tout en conservant la même adresse IPv6.

JB



## Couche 3 (R) : IPV6 5/24

### Principales caractéristiques d'IPv6

-  les **adresses IPv6 sont codées sur 128 bits** (1 milliard de réseaux).
  
-  le principe des numéros de réseaux et des numéros d'hôtes est maintenu.
  
-  IPv6 utilise un **adressage hiérarchique** (identification des différents réseaux de chaque niveau) ce qui permet un routage plus efficace.
  
-  IPv6 est prévu pour les systèmes mobiles : auto-configuration, notion de voisinage (neighbor).



JB



## Couche 3 (R) : IPV6 6/24

### Principales caractéristiques d'IPv6

-  IPv6 permet **l'authentification et le chiffrement** dans l'en-tête des paquets, ce qui permet de sécuriser les échanges. En effet IP v.6 intègre **IPSec** (protocole de création de tunnel IP avec chiffrement), qui garantit un contexte sécurisé par défaut.
-  IPv6 intègre la **qualité de service** : introduction de flux étiquetés (avec des priorités)
-  IPv6 prend mieux en charge le trafic en temps réel (garantie sur le délai maximal de transmission de datagrammes sur le réseau).



.B



## Allocation de l'espace d'adressage

L'adressage IPv6 est structuré en plusieurs niveaux selon un **modèle hiérarchique** dit "**agrégé**". Cette composition devrait permettre une meilleure agrégation des routes et une diminution de la taille des tables de routage. Un plan d'adressage hiérarchisé en trois niveaux a été défini pour les adresses IPv6 :



- **TLA (Top Level Aggregator):** délivré aux grands opérateurs internationaux
- **National: Sub-TLA(13bits):** permet aux opérateurs internationaux de fournir des adresses aux opérateurs nationaux,
- **Les 6 bits suivants sont réservés pour des utilisations futures.**
- **NLA (Next Level Aggregator) :** utilise les 13 bits suivants, il permet aux opérateurs de délivrer des adresses à leurs clients,
- **SLA (Site Level Aggregator):**ils sont sous la responsabilité du site et permettent de créer des sous-réseaux (donc 65534 sous-réseaux possibles par site).

Ils correspondent à l'identifiant unique de l'interface sur le réseau. Sur les réseaux Ethernet, ils sont généralement fabriqués à partir de l'identifiant unique de l'interface : l'adresse MAC, mais ils peuvent également être générés aléatoirement pour des raisons de confidentialité.

JB



# Couche 3 (R) : IPV6 8/24

## Représentation des adresses IPv6

128 bits de l'adresse sont divisés en 8 groupes de 16 bits représentés par 4 chiffres hexadécimaux et séparés par ":".

Exemple d'adresse : 5800:10C3:E3C3:F1AA:48E3:D923:D494:AAFF

Dans IPv6 les masques sont exprimés en notation CIDR.

- **Représentation des adresses IPv6 : forme préférée**

|       |       |       |       |       |       |       |      |
|-------|-------|-------|-------|-------|-------|-------|------|
| X     | X     | X     | X     | X     | X     | X     | X    |
| 2001: | 0660: | 7401: | 0200: | 0000: | 0000: | 0edf: | bdd7 |

- **Représentation des adresses IPv6 : forme abrégée**

|       |      |       |      |   |   |      |      |
|-------|------|-------|------|---|---|------|------|
| 2001: | 660: | 7401: | 200: | : | : | edf: | bdd7 |
|-------|------|-------|------|---|---|------|------|

JB

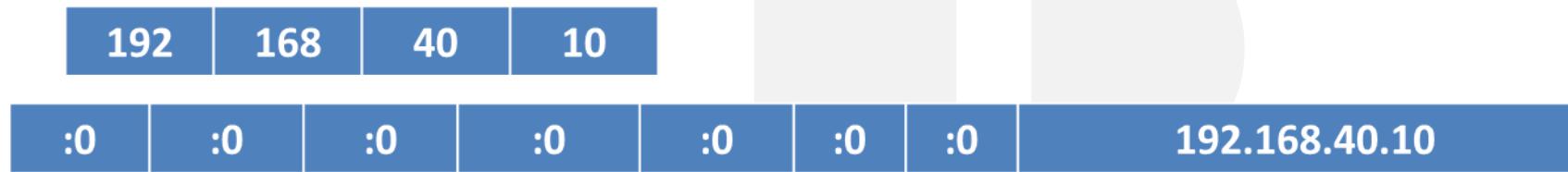


## Représentation des adresses IPv6 : forme mixte

## L'adresse IPv6 compatible IPv4

Elle est utilisée dans un contexte particulier : les tunnels 6 to 4 permettant de relier des réseaux IPv4 à des réseaux IPv6.

Soit une adresse IPv4 notée **a.b.c.d**, son équivalent IPv6 se notera  
**:0:0:0:0:0:a.b.c.d/96** ou en forme abrégée : **::a.b.c.d/96**



## Représentation des adresses IPv6 : forme abrégée



JB



# Couche 3 (R) : IPV6 10/24

## Représentation des adresses IPv6 : forme mixte

### L'adresse IPv4 mappée

Un hôte IPv6 étant capable de communiquer aussi bien avec un hôte IPv4 qu'avec un hôte IPv6, il utilise des adresses IPv4 mappées pour communiquer avec les autres machines IPv4 et utilise des adresses IPv6 normale pour communiquer avec les autres machines IPv6. Ces adresses sont de la forme **::ffff:a.b.c.d .**

|         |     |     |    |    |
|---------|-----|-----|----|----|
| ::ffff: | 192 | 168 | 40 | 10 |
|---------|-----|-----|----|----|

### L'adresse de bouclage qui correspond à 127.0.0.1 en IPv4

|       |       |       |       |       |       |       |      |
|-------|-------|-------|-------|-------|-------|-------|------|
| 0000: | 0000: | 0000: | 0000: | 0000: | 0000: | 0000: | 0001 |
|-------|-------|-------|-------|-------|-------|-------|------|

|    |   |
|----|---|
| :: | 1 |
|----|---|

JB



# Couche 3 (R) : IPV6 11/24

## Représentation des adresses IPv6 : forme mixte

### L'adresse indéterminée qui correspond à 0.0.0.0 en IPv4.

Elle caractérise l'absence d'adresse. Elle est utilisée lors de certaines phases d'initialisation. C'est une adresse transitoire. Elle se note **0:0:0:0:0:0:0:0 ou ::**

### Représentation des Masques de sous-réseaux

Leur notation classique comme en IPV4 est impossible avec 128 bits, c'est donc la notation CIDR, plus simplement appelée notation "slash" qui est utilisée.

Exemple l'adresse **fe80::20d:61ff:fe22:3476/64** a un masque de 64 bits , masque par défaut pour une adresse de type **lien-local**.



.B



## Types d'adresses: Les adresses unicast :

Elles désignent une et une seule machine >> interface unique

lien local (link-local)>> ne passent pas les routeurs

Global >> sont routables sur Internet

Site local >> ne sont pas routables sur Internet



JB



## Types d'adresses: Les adresses multicast :

Groupe d'interfaces appartenant généralement à des nœuds différents et pouvant être situés partout sur Internet.

Remplace le broadcast de IPV4

Le format des adresses multicast est le suivant :

ff01 : nœud local, les paquets ne quittent pas l'interface.

ff02 : lien local, les paquets ne quittent pas le lien .

ff05 : site local, les paquets ne quittent pas le site .



JB



## Types d'adresses: Les adresses anycast :

Anycast est un nouveau type d'adressage

Groupe d'interfaces, mais un paquet dont l'adresse de destination est une adresse anycast est acheminé à un élément du groupe et non à tous.

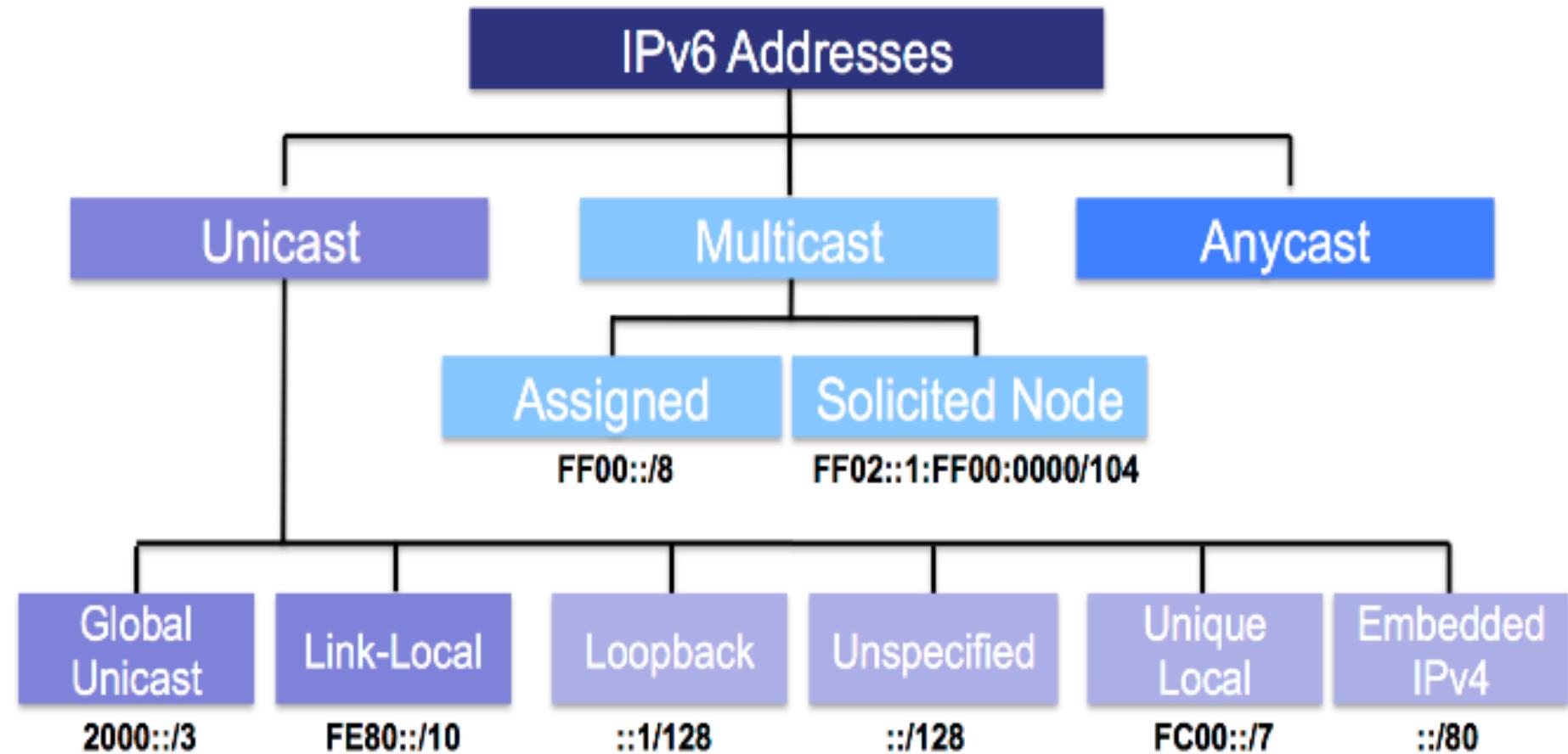
Pour l'instant, une seule adresse anycast est utilisée, elle est réservée au routeur mais dans l'avenir, d'autres pourraient être définies.



IB



## Types d'adresses:



IB



# Couche 3 (R) : IPV6 16/24

## Portée des adresses

La **portée** ou "scope" des adresses, est une nouvelle notion qui n'existe pas en IPv4. En fait une interface ne possède pas une seule adresse IPv6 mais peut en avoir plusieurs. Les quatre portées d'adresses sont :

|  |  |
|--|--|
| <b>Noeud-local (::1/128)</b>   | il s'agit de l'adresse de loopback   |
| Lien-local (préfixe <b>fe80::/64</b> )   | adressage commun aux machines d'un même lien physique reliées entre elles sans routeur intermédiaire, Seuls les équipements de la couche 2 du modèle OSI peuvent utiliser ces adresses pour communiquer entre eux. Cette adresse est obtenue par auto-configuration "sans état". |
| Site-local (préfixe <b>fec0::/48</b> suivi d'un champ de 16 bits permettant de définir des sous-réseaux) | adressage commun des machines d'un même site. Par exemple, un site qui n'est pas encore relié à Internet peut utiliser ce type d'adresse.(concept des adresses privées en IPv4)  |
| Globale (préfixe <b>2000::/3</b> )<br>On utilise <b>2xxx</b> ou <b>3xxx</b> .                            | ce sont des adresses dont le routage est effectué sans restriction.  |



JB



# Couche 3 (R) : IPV6 17/24

## Portée des adresses

**Le type d'adresse IPv6** est indiqué par les premiers bits de l'adresse qui sont appelés le "Préfixe de Format" (Format Prefix). L'allocation initiale de ces préfixes est la suivante :

| Allocation                      | Préfixe        | Usage   |
|---------------------------------|----------------|---|
| Adresses Unicast globales       | 010            | Adresses dont le routage est effectué sans restriction, utilisables sur Internet. |
| Adresses Unicast expérimentales | 001            |   |
| Adresses "Lien local"           | 1111 1110 1000 | Adresses d'un même lien physique, obtenues par autoconfiguration                  |
| Adresses "Site Local"           | 1111 1110 1100 | Adresses d'un même site   |
| Adresses Multicast              | 1111 1111      | Elles remplacent les adresses "broadcast" d'IPv4                                  |

**15 % de l'espace d'adressage est actuellement alloué. Les 85% restants sont réservés pour des usages futurs. En réalité sur les 128 bits, seulement 64 sont utilisés pour les hôtes (Interface ID).**

JB



# Couche 3 (R) : IPV6 18/24

## L'auto-configuration

 **L'auto-configuration** << l'autoconfiguration sans état « stateless » :

-  configuration automatique et autonome,
-  seul le préfixe est donné à l'équipement qui aura la charge de générer le suffixe de l'adresse,
-  L'adresse de type lien-local est automatiquement générée à partir de l'adresse MAC de l'interface.

JB



## L'auto-configuration

### Fonctionnement: Calcul de l'adresse

- ✓ Type link-local, le préfixe est toujours fe80::/
- ✓ L'adresse MAC est unique car fixée par le constructeur de l'interface
- ✓ L'adresse MAC ayant une longueur de seulement 48 bits, il est nécessaire d'ajouter 2 octets supplémentaires. Cela se fait en insérant la chaîne fffe (réservée par l'IEEE à cet usage) au milieu de ces 48 bits.
- ✓ **Exemple:** adresse Mac: 10:93:e9:0f:00:18  
**ID-interface Adresse IPV6 provisoire: 1093:e9ff:fe0f:0018**
- ✓ Différencier les adresses MAC uniques ou
  - MAC unique : le 7eme bit de l'octet le plus à gauche on le met à 1
  - Mac pas unique: le 7eme bit de l'octet le plus à gauche on le met à 0

IB



# Couche 3 (R) : IPV6 20/24

## L'auto-configuration

### Fonctionnement: Calcul de l'adresse

**L'auto-configuration** << l'autoconfiguration sans état « stateless »:

- ✓ **Exemple:** adresse Mac: 10:93:e9:0f:00:18

ID-interface Adresse IPV6 provisoire: 1093:e9ff:fe0f:0018

- ✓ Différencier les adresses MAC uniques ou
  - MAC unique : le 7eme bit de l'octet le plus à gauche on le met à 1
  - Mac pas unique: le 7eme bit de l'octet le plus à gauche on le met à 0
    - Notre octet ici c'est le 10
    - En binaire 0001 0000
    - 7eme bit à 1 00010010 >> 12
- **Adresse IPV6 definitive: fe80::1293:e9ff:fe0f:0018**



JB



# Couche 3 (R) : IPV6 21/24

## [Configurer @ IPv6](#)

### Rappel sur IPv4:

- Conf t
- Int fa0/0
- Ip address 192.168.1.1 255.255.255.0

### IPv6 :

- Conf t
- Int fa0/0
- Ipv6 address 2001::1 /64
- Ipv6 address FE80::1 /64 **link-local**
- Ipv6 address 2001:: /64 **eui-64**



JB



# Couche 3 (R) : IPV6 22/24

## Protocoles de routage

### Rappel sur IPv4:

- RIP
- OSPF
- EIGRP

### IPv6 :

- RIPvng
- OSPFv3
- EIGRP for IPv6



# Couche 3 (R) : IPV6 23/24

## Comment se relier au réseau IPv6 ?

Par un fournisseur d'accès :

Utiliser une connexion via un tunnel 6to4

Un tunnel "6to4" permet de relier un réseau Ipv4 au réseau IPv6.

Du côté du réseau IPv4 , les trames IPv6 sont encapsulées dans des trames IPv4 et sont envoyées vers le relais 6to4 qui est chargé d'en extraire les trames IPv6 et de les envoyer vers le réseau IPv6

Se relier à une passerelle ipv6

contrairement aux tunnels "6to4", vous ne vous enregistrez pas auprès d'un fournisseur qui redirigera pour vous tout le trafic IPv6 encapsulé dans des trames IPv4. Votre adresse IPv6 est calculée d'après votre adresse IPv4 publique, les trames IPv6 seront dirigées vers une passerelle "6to4". Pour connaitre les passerelles disponibles :

# Couche 3 (R) : IPV6 24/24

## Cohabitation IPV4-IPV6

- **Tunnel IPV6/IPV4**( encapsuler les paquets IPV6 sur des Paquets IPV4)
- **Dual STACK IPV4-IPV6** (installer ipv4 ou 6 sur le même nœud (poste ou routeur) et les activer et/ou les paramétrer ,
- **Translation IP** (NAT-PT,NAP-PT,NAT64&DNS64)
- **4.6PE**( réservé au opérateur qui vont utiliser MPLS basé sur IPV4 pour transporter des paquets IPV6)
- **ALG:** passerelle applicative ( utiliser un proxy doté à la fois de connexion IPV4 et IPV6



.B



# Couche 3 (R) : EXERCICES IPV6 1/8

## Exercice1 : simplifier les adresses IPV6 suivantes

- a) Fe80 :0000 : 0000 : 0000 : 0000 :4cff : fe4f :4f50
  
- b) 0000 :0000 :0000 :0000 :0000 :0000 :0000
  
- c) 2001 :0688 :1f80 :2000 :0203 :ffff :0017 :fe1a
  
- d) 3cd0 :0000 :0000 :0000 :0040 :0000 :0000 :0cf0



# Couche 3 (R) :EXERCICES IPV6 2/8

## Solution Exercice1 : simplifier les adresses IPV6 suivantes

.1B



# Couche 3 (R) :EXERCICES IPV6 3/8

## Exercice2 : mettez sous forme expansée les adresses IPV6 suivantes

- a) Fec0:0:0:ffff::1
  
- b) Fe80::1
  
- c) Fe80::4cd2:ffa1::1



# Couche 3 (R) :EXERCICES IPV6 4/8

 **Solution Exercice2 : mettez sous forme expasée les adresses IPV6 suivantes**

.1B



# Couche 3 (R) :EXERCICES IPV6 5/8

## Exercice 3: déterminer les types adresses en fonction de leur préfixe

- a) Fe80 ::4c00:fe4f:4f50
  
- b) 2001:618:1f80:2010:203:ffff:b118:ef1e
  
- c) Fec0:0:0:ffff::1
  
- d) Ff02::1



# Couche 3 (R) :EXERCICES IPV6 6/8

 **solution Exercice 3: déterminer les types adresses en fonction de leur préfixe**

.B



# Couche 3 (R) :EXERCICES IPV6 7/8

## Exercice4: Construire des adresses "lien local" et "lien global"

a) A partir des adresses Mac suivantes construire les adresses lien local auto configurées automatiquement

- ✓ **02-00-4c-4f-4f-50**
- ✓ **00-03-ff-18-cf-1e**
- ✓ **00:0C:29:88:F6:EE**
- ✓ **00:50:56:2C:C4:4C**
- ✓ **E4-02-9B-AC-E1-CF**



b) Quelles seraient les adresses "lien global" correspondantes si le préfixe global distribué par le fournisseur d'accès est 2a01:5d8:ccf1:4/64 ?

# Couche 3 (R) :EXERCICES IPV6 8/8

## Solution Exercice4: Construire des adresses "lien local" et "lien global"

IB



## PRINCIPES FONDAMENTAUX

Existe une grande différence entre commutation de trames et commutation de paquets (routage). La première distinction vient du fait que la **commutation de trames** s'effectue au niveau de **la couche 2 du modèle OSI**, alors que le **routage s'effectue au niveau de la couche 3 du modèle OSI**. Cela indique donc que les routeurs et les commutateurs ne prennent pas leur décision avec les mêmes informations.

Pour **joindre les hôtes non locaux**, une machine va faire une requête ARP pour avoir l'adresse MAC de la station de destination, si la destination n'est pas locale la requête ARP va échouer, la station enverra alors la trame à sa passerelle par défaut, c'est-à-dire au routeur.

Le routeur examine l'adresse de destination de la couche 3 du paquet, **effectue un ET logique binaire avec le masque de sous réseau pour identifier le réseau de destination et prendre la bonne décision de commutation.**

De la même manière qu'un commutateur garde une table des adresses MAC connues, un routeur garde une table des adresses réseaux dans sa table de routage. Il va ainsi être capable de commuter les paquets vers un réseau spécifique.

.B



## DOMAINE DE BROADCAST

Un domaine de broadcast est un **domaine logique** où n'importe quels hôtes connectés à un réseau **peuvent envoyer des données à une autre machine sans passer par des services de routage**.

Plus spécifiquement c'est un segment réseau composé d'hôtes et de dispositifs pouvant être atteint en envoyant un paquet à l'adresse de broadcast.

**Ces domaines de broadcast sont toujours séparés par des dispositifs de couche 3.**

IB



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### B Routeur :

Équipement de couche 3 permettant **d'interconnecter deux réseaux ou plus** en se basant sur les adresses de couche 3. Le routeur permet également une segmentation des domaines de broadcast et des domaines de collisions.



Routeur Cisco de type 2600



Symbole logique du routeur

Le routeur dispose d'une interface (une carte réseau) le reliant au réseau local. Celle-ci dispose d'une adresse IP.

IB

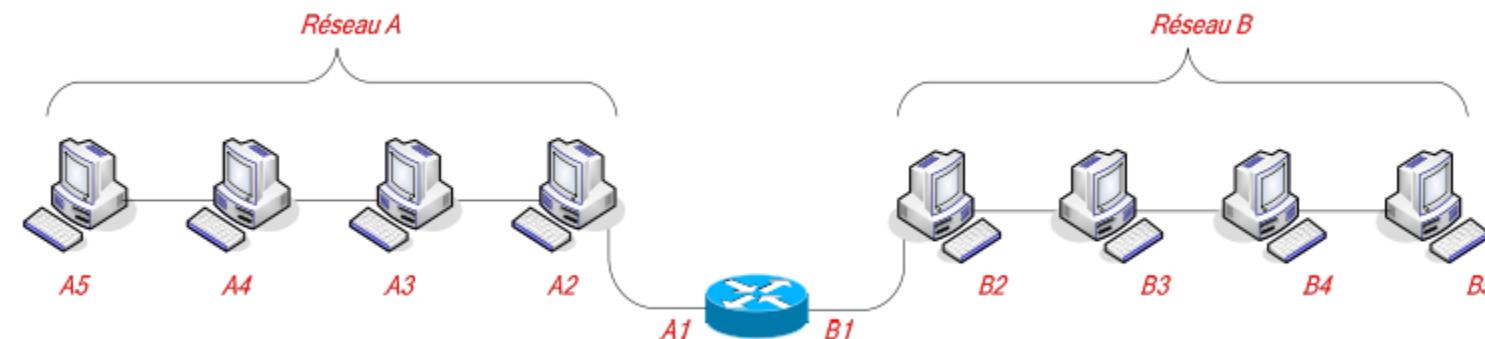


## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### Routeur :

Par exemple, sur le schéma ci-dessous, les adresses des hôtes sont A5, A4, A3 et A2, faisant partie du réseau A. On attribue A1 à l'interface du routeur, lui permettant ainsi de se connecter au réseau A.

Un autre réseau, B, est lui aussi connecté au routeur. Ce dernier dispose donc d'une interface ayant pour IP B1 afin de pouvoir communiquer avec le réseau.



JB



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### Routeur :

Supposons maintenant que l'on souhaite envoyer des données de A vers B :

- ✓ Le routeur reçoit la trame de couche 2, supprime l'en tête de liaison de données
  - ✓ Il examine l'adresse de couche 3 afin de déterminer le destinataire
  - ✓ Il effectue un ET logique entre l'adresse IP et le masque de sous réseau afin de déterminer le réseau de destination
- 
- Yellow icon: Il consulte sa table de routage pour déterminer l'interface par laquelle les données doivent être envoyées.

C'est pour cela que chaque interface du routeur doit être sur un réseau différent. Sinon le routeur ne pourra pas déterminer par quelle interface envoyer les informations. C'est le principe de commutation de paquets ou routage.

.B



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### Routeur :

Supposons maintenant que l'on souhaite envoyer des données de A vers B :

- Le routeur reçoit la trame de couche 2, supprime l'en tête de liaison de données
- Il examine l'adresse de couche 3 afin de déterminer le destinataire
- Il effectue un ET logique entre l'adresse IP et le masque de sous réseau afin de déterminer le réseau de destination
- Il consulte sa table de routage pour déterminer l'interface par laquelle les données doivent être envoyées.

C'est pour cela que chaque interface du routeur doit être sur un réseau différent. Sinon le routeur ne pourra pas déterminer par quelle interface envoyer les informations. C'est le principe de commutation de paquets ou routage.

IB



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### Détermination du chemin

Les méthodes de sélection du chemin permettent aux équipements de couche 3, les routeurs, de déterminer la route à suivre pour acheminer les informations au travers de différents réseaux.

Les services de routage utilisent les informations de topologie du réseau pour évaluer les chemins.

Ce processus est aussi appelé routage des paquets et prend en compte divers paramètres ou "métriques" comme :

- ✓ Densité du trafic
- ✓ Nombre de routeurs à franchir pour joindre la destination
- ✓ Vitesse des liaisons
- ✓ Etc.

.B



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### **Systèmes autonomes, IGP et EGP**

Un système autonome est un réseau ou un ensemble de réseaux sous un contrôle administratif commun. Un système autonome est composé de routeurs ayant les mêmes règles et fonctions.\*

Deux familles des protocoles de routage sont les protocoles IGP (Interior Gateway Protocol) et les protocoles EGP (Exterior Gateway Protocol).

Les IGP routent les données dans un système autonome, comme nous venons de le voir :

- RIP and RIPv2
- IGRP
- EIGRP
- OSPF
- IS-IS

EGP route les données entre les réseaux autonomes. Un exemple d'EGP est BGP.

IB



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### Routage statique et dynamique

| Nom du protocole | Type (IGP ou EGP) | Algorithme          | Métriques                                 | Mise à jour | Remarque  |
|------------------|-------------------|---------------------|---|-------------|---|
| RIP              | IGP               | Vecteur de distance | 15 sauts maximums                         | 30 sec      | 15 sauts maximums   |
| RIP v2           | IGP               | Vecteur de distance | 15 sauts maximums                         | 30 sec      | Inclus des préfixes de routage et les masques de sous réseau dans les informations de routage |
| IGRP             | IGP               | Vecteur de distance | Délais, charge, bande passante, fiabilité | 90 secondes | Choisi le meilleur chemin selon différent critères.<br>Propriétaires Cisco.                   |
| EIGRP            | IGP               | Hybride             | Délais, charge,                           | Instantanée | Propriétaire Cisco.   |



JB



## LES ÉQUIPEMENTS DE COUCHE 3 : LES ROUTEURS

### Routage statique et dynamique

|       |     |                      |   |  |  |
|-------|-----|----------------------|---|--|--|
|       |     |                      | bande passante,<br>fiabilité                  | à chaque<br>changement<br>topologique                | Meilleur<br>convergence et<br>moins de bande<br>passante utilisée.           |
| OSPF  | IGP | Etat de lien         | Le coût de la<br>route                        | Instantanée<br>à chaque<br>changement<br>topologique | Utilisé pour les<br>réseaux à grandes<br>échelles                            |
| IS-IS | IGP | Etat de lien         | Poids du lien                                 | Instantanée<br>à chaque<br>changement<br>topologique | Supporte de<br>multiples<br>protocoles routés<br>tel qu'IP.                  |
| BGP   | EGP | Vecteur de<br>chemin | Politique<br>réseau,<br>Attribut de<br>chemin |  | Protocole utilisé<br>par la plupart des<br>ISP et les grandes<br>compagnies. |



JB



# Couche 4 : Transport

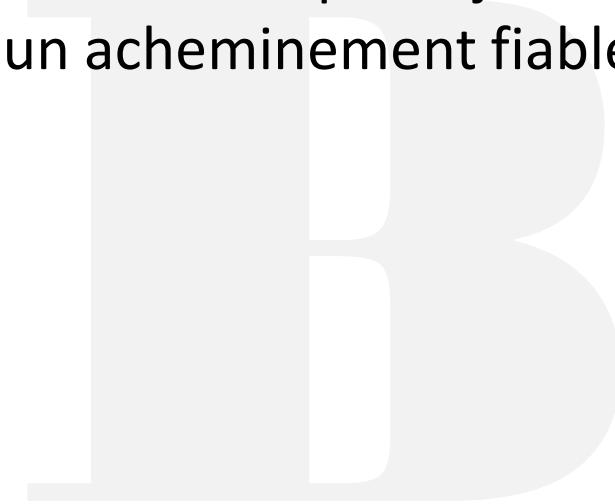




# Couche 4 : Transport

## INTRODUCTION

Nous avons vu dans les chapitres précédents comment TCP/IP envoie les informations de l'émetteur au destinataire. La couche transport ajoute à ce mécanisme la notion de « qualité de service », à savoir la garantie d'un acheminement fiable des informations au travers du réseau.





# Couche 4 : Transport 1/10

## TCP et UDP

La pile de protocoles TCP/IP comprend 2 protocoles de couche 4 : TCP et UDP

TCP est un protocole orienté connexion, c'est-à-dire qu'il associe au transport des informations, la option de qualité en offrant les services suivants :

- Fiabilité
- Division des messages sortants en segments
- Ré assemblage des messages au niveau du destinataire
- Ré envoi de toute donnée non reçue

Segments : PDU de couche 4



IB



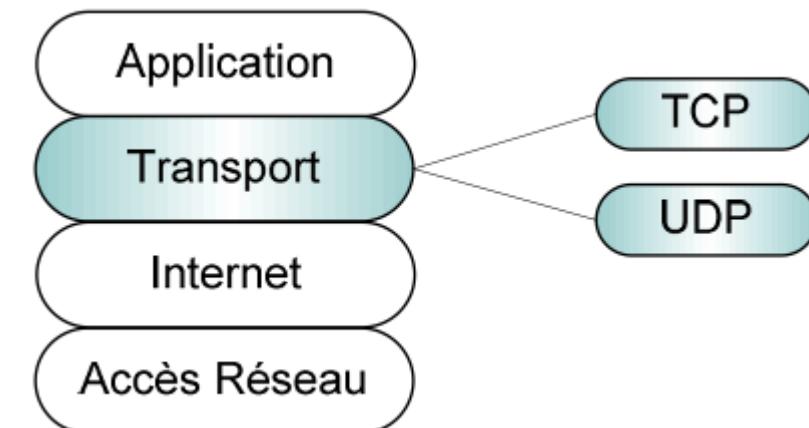
# Couche 4 : Transport 2/10

## TCP et UDP

UDP est lui un protocole non orienté connexion, c'est-à-dire qu'il n'offre pas de fonction de contrôle du bon acheminement :

- Aucune vérification logicielle de la livraison des messages
- Pas de réassemblage des messages entrants
- Pas d'accusé de réception
- Aucun contrôle de flux

Cependant, UDP offre l'avantage de nécessiter moins de bande passante que TCP. Il peut donc être intéressant d'utiliser ce protocole pour l'envoi de messages ne nécessitant pas de contrôle de qualité.



IB



# TCP/IP

## Couche 4 : Transport 3/10

### NUMÉROS DE PORTS

Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports. Des conventions ont été établies pour des applications .

| Protocole | n° de port | Description                         |
|-----------|------------|-------------------------------------|
| FTP data  | 20         | File Transfer (données par défaut)  |
| FTP       | 21         | File Transfer (contrôle)            |
| SSH       | 22         | Secure SHell                        |
| Telnet    | 23         | Telnet                              |
| SMTP      | 25         | Simple Mail Transfer                |
| DNS       | 53         | Domain Name System                  |
| HTTP      | 80         | World Wide Web HTTP                 |
| POP3      | 110        | Post Office Protocol - Version 3    |
| NNTP      | 119        | Network News Transfer Protocol      |
| IMAP2     | 143        | Interactive Mail Access Protocol v2 |
| NEWS      | 144        | News                                |
| HTTPS     | 443        | Protocole HTTP sécurisé (SSL)       |

Numéros de ports

.B





## Couche 4 : Transport 4/10

### NUMÉROS DE PORTS

Les ports sont attribués de la manière suivante :

#### Plage de ports

#### Utilisation

0 à 1023

réservés aux applications publiques

1023 à 65535

attribué aux entreprises pour les applications commerciales et utilisé par le système d'exploitation pour l'attribution dynamique des ports source.



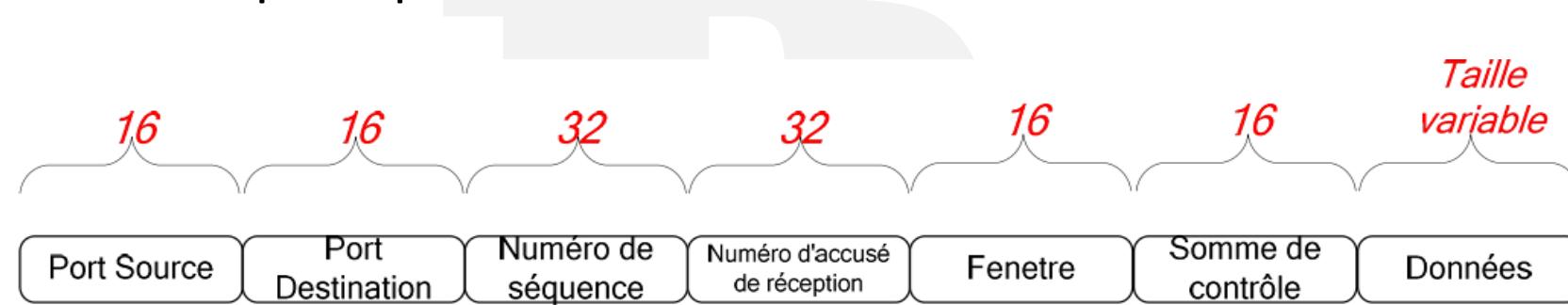
.B



# Couche 4 : Transport 5/10

## STRUCTURES D'UN SEGMENT TCP

Le protocole TCP encapsule les informations provenant de la couche supérieure dans des segments dont voici les principales informations :



| Champs                   | Descriptions  |
|--------------------------|---|
| Port source              | Numéro du port appelant   |
| Port de destination      | Numéro du port appelé   |
| Numéro de séquence       | Numéro utilisé pour assurer le séquençage correct des données entrantes |
| N° d'accusé de réception | Prochain octet TCP attendu  |
| Somme de contrôle        | Somme de contrôle calculée des champs d'en-tête et de données           |
| Données                  | Données du protocole de couche supérieure                               |

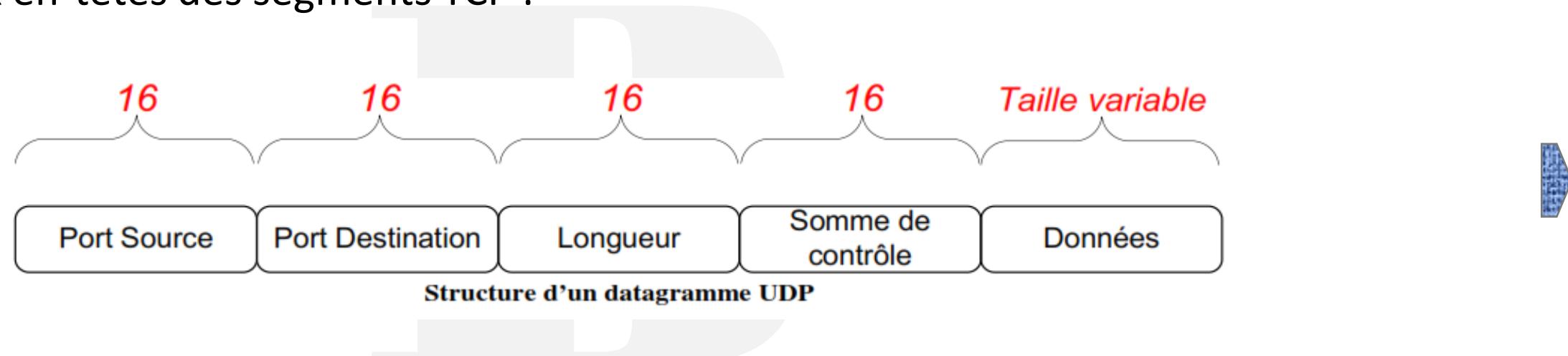
.B



# Couche 4 : Transport 6/10

## STRUCTURES D'UN SEGMENT UDP

UDP étant un protocole non orienté connexion, il dispose d'un en-tête de taille réduite par rapport aux en-têtes des segments TCP :



Le protocole UDP est conçu pour les applications ne devant pas assembler de séquences de segments.

Il laisse aux protocoles de la couche application le soin d'assurer la fiabilité.

.B





## Couche 4 : Transport 7/10

### MÉTHODE DE CONNEXION TCP

Un service orienté connexion comportent 3 points importants :

-  Un chemin unique entre les unités d'origine et de destination est déterminé
-  Les données sont transmises de manière séquentielle et arrivent à destination dans l'ordre,
-  La connexion est fermée lorsqu'elle n'est plus nécessaire



.B



# TCP/IP

## Couche 4 : Transport 8/10

### MÉTHODE DE CONNEXION TCP

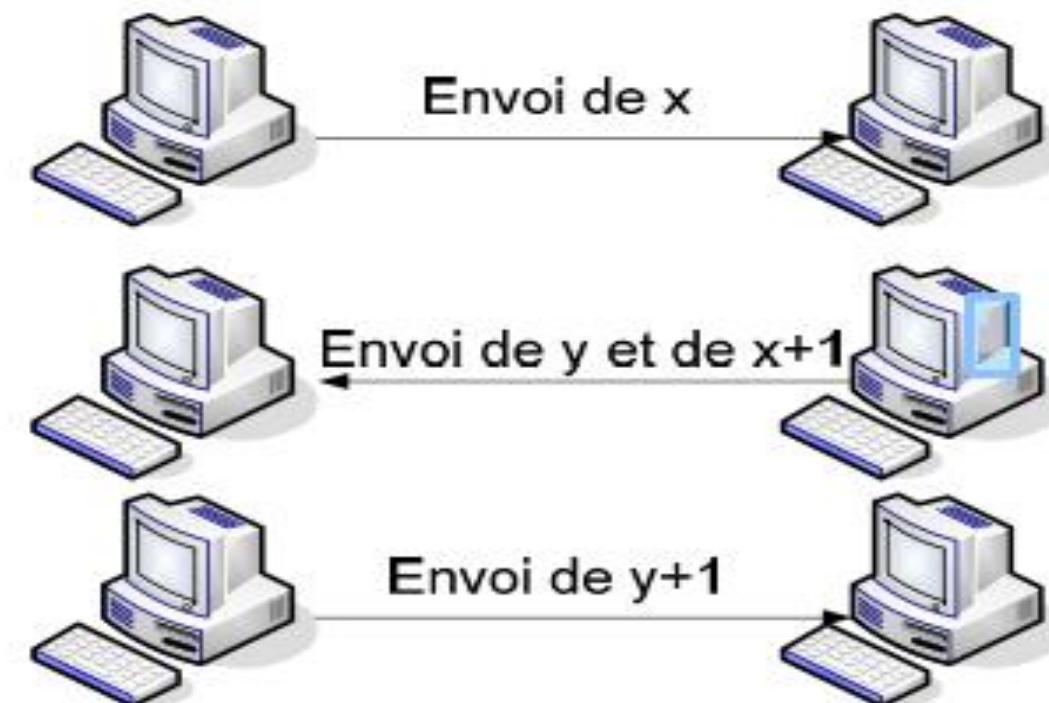
#### B Connexion ouverte/échange en 3 étapes

Les hôtes TCP établissent une connexion en 3 étapes, appelée aussi « connexion ouverte » :

L'émetteur envoie un paquet avec un numéro de séquence initial ( $x$ ) avec un bit dans l'en-tête pour indiquer une demande de connexion.

Le destinataire le reçoit, consigne le numéro de séquence initial, répond par un accusé de réception « $x+1$  » et inclut son propre n° de séquence ( $y$ ).

L'émetteur reçoit  $x+1$  et renvoie  $y+1$  pour dire au destinataire que la réception s'est bien passée.



JB





# Couche 4 : Transport 9/10

## MÉTHODE DE CONNEXION TCP

### **Positive Acknowledgement Retransmission**

La technique Positive Acknowledgement Retransmission ou PAR, consiste à envoyer un paquet, démarrer un compteur puis attendre un accusé de réception avant d'envoyer le suivant.

Si le compteur arrive à expiration avant l'arrivée de l'accusé, les informations sont alors retransmises plus lentement et un nouveau compteur est déclenché.

Cependant, cette technique est consommatrice de bande passante, c'est alors qu'intervient le mécanisme de fenêtrage.

JB



# Couche 4 : Transport 10/10

## MÉTHODE DE CONNEXION TCP

### Fenêtrage

Le Fenêtrage est un mécanisme dans lequel le récepteur envoi un accusé de réception après avoir reçu

un certain nombre de données. Si le destinataire n'envoie pas d'accusé, cela signifie pour l'émetteur que les informations ne sont pas parvenues correctement et dans ce cas sont retransmises.

La taille de la fenêtre détermine la quantité de données que l'on peut transmettre avant de recevoir un accusé de réception.

TCP utilise un système d'accusé de réception prévisionnel, ce qui signifie que le numéro d'accusé renvoyé indique la prochaine séquence attendue

IB



# Couche 5: Session ➔



## Couche 5 : Session 1/5

Comme nous l'avons vu précédemment, une session est un **ensemble de transactions entre deux unités réseau ou plus.**

Une analogie pour comprendre la couche session est une **communication entre plusieurs individus**. Si l'on souhaite que la conversation se déroule correctement, il est impératif de mettre en place diverses règles, afin que les interlocuteurs ne s'interrompent pas, par exemple.

Cette notion de contrôle du dialogue est le point essentiel de la couche session. Le rôle de la couche session est d'ouvrir, gérer et fermer les sessions entre les applications. Cela signifie qu'elle prend en compte :

- ✓ **le lancement des sessions**
- ✓ **la resynchronisation du dialogue**
- ✓ **l'arrêt des sessions**

Elle coordonne donc les applications qui communiquent au travers des différents hôtes.

IB



## Couche 5 : Session 2/5

Une communication entre ordinateurs suppose de nombreuses conversations courtes (commutation de paquets comme nous l'avons vu précédemment) avec en plus de cela d'autres communications pour **s'assurer de l'efficacité de la communication.**

Ces conversations nécessitent que les hôtes jouent à tour de rôles celui de client (demandeur de services) et de serveur (fournisseur de services).

Le contrôle du dialogue consiste en l'identification des rôles de chacun à un moment donné.



- Communication entre les hôtes
- Gestion des sessions

JB





## Couche 5 : Session 3/5

### CONTRÔLE DU DIALOGUE

La couche session décide si la conversation sera de type bidirectionnel simultané ou alterné. Cette décision relève du contrôle du dialogue.

- 💡 Si la communication bidirectionnelle simultanée est permise :
  - ✓ La gestion de la communication est assurée par d'autres couches des ordinateurs en communication.
  
- 💡 Si ces collisions au sein de la couche session sont intolérables, le contrôle de dialogue dispose d'une autre option : la communication bidirectionnelle alternée
  - ✓ Ce type de communication est rendu possible par l'utilisation d'un jeton de données au niveau de la couche session qui permet à chaque hôte de transmettre à tour de rôle.

.B





## Couche 5 : Session 4/5

### **SYNCHRONISATION DU DIALOGUE**

Cette étape est des plus importantes, elle permet aux hôtes communicants au travers d'un réseau de marquer une pause pour par exemple sauvegarder la communication en cours et resynchroniser le dialogue.

Pour cela ils utilisent un « point de contrôle », envoyé par l'un des interlocuteurs à l'autre pour enregistrer la conversation, vérifier l'heure de la dernière portion de dialogue effectuée, comme si vous aviez un double appel avec votre cellulaire. Ce processus est appelé la synchronisation du dialogue.

Comme dans le langage humain, il est important dans une discussion de montrer à son interlocuteur le début d'une conversation (« allo » dans le cas d'une conversation téléphonique) ainsi que de signifier que l'on se prépare à mettre fin à la conversation (« au revoir »). C'est pour cela que les deux contrôles principaux sont :

- ✓ Lancement ordonné de la communication
- ✓ Fin de la communication

IB





## Couche 5 : Session 5/5

### DIVISION DU DIALOGUE

La division du dialogue englobe le lancement, la gestion ordonnée et la fin de la communication.

Notre schéma représente une petite synchronisation. Au niveau du point de contrôle, la couche session de l'hôte A envoie un message de synchronisation à l'hôte B, et les deux hôtes exécutent la séquence qui suit :

- Sauvegarder les fichiers donnés.
- Sauvegarder les paramètres réseau.
- Sauvegarder les paramètres de synchronisation.
- Noter le point d'extrémité de la conversation.



JB



# Couche 6 : Présentation ➔

# Couche 6 : Présentation 1/5

Afin que deux hôtes communiquant puissent se comprendre, il est nécessaire qu'il parle le même langage : c'est à cette tâche qu'est dévolue la couche présentation.

## Fonctions et normes

L'un des rôles de la couche présentation est de présenter les données dans un format que le dispositif récepteur est capable de comprendre. La couche présentation peut être comparée à un traducteur lors d'une conférence internationale : elle s'occupe de « traduire » les données de manière à ce que l'hôte récepteur soit en mesure de comprendre.

La couche présentation, ou couche 6, assure trois fonctions principales, à savoir :

- ✓ **Le formatage des données (présentation)**
- ✓ **Le cryptage des données**
- ✓ **La compression des données**

Après avoir reçu les données de la couche application, la couche présentation exécute certaines ou toutes ces fonctions avant d'acheminer les données à la couche session.

IB



## Couche 6 : Présentation 2/5

Les normes de la couche 6 définissent également la présentation des graphiques. Les trois principaux formats graphiques sont :

- ▣ **BMP (BitMaP)** est un format ancien encore largement répandu, il est maintenant supplanté par le JPEG, qui fournit des fichiers avec un meilleur taux compression/taille
- ▣ **JPEG (Joint Photographic Experts Group)** - Format graphique le plus utilisé pour la compression des images fixes complexes et des photographies.
- ▣ **PNG (Portable Network Graphics)** est un format graphique en émergence sur Internet qui compresse les textures.

D'autres normes de la couche 6 concernent la présentation des sons et des séquences animées. Les normes suivantes appartiennent à cette catégorie:

- ▣ **MPEG (Motion Picture Experts Group)** - Format de compression et de codage de vidéo animée pour CD ou tout autre support de stockage numérique.
- ▣ **MP3 (MPEG Layer 3)** - Format de compression de musique le plus utilisé pour le moment. Il utilise l'étude de l'oreille humaine ainsi des algorithmes de compression.
- ▣ **Divx (MPEG 4)** format de compression créé à partir du format MPEG 4 développé par Microsoft et permettant une compression bien meilleure que le MPEG 1 ou 2 (exemple : faire tenir un film sur un CD au lieu d'un DVD).

.B



# Couche 6 : Présentation 3/5



## Représentation des données :

- Lisibilité des données par le destinataire
- Formatage des données
- Contrôle de la syntaxe



JB



# Couche 6 : Présentation 4/5

## LE CRYPTAGE DES DONNÉES

Le cryptage est défini par l'utilisation **d'algorithmes** permettant d'encoder le message de manière à ce que seul l'hôte à qui on l'adresse puisse le comprendre.

Le cryptage permet de **protéger la confidentialité des informations** pendant leur transmission.



Une clé de cryptage peut être utilisée pour crypter les données à la source en encodant les données avec elle, ce qui obligera l'hôte récepteur à posséder cette clé pour les décrypter. Un algorithme est donc utilisé pour rendre ces données incompréhensibles à quiconque ne disposant pas de la clé.

JB



# Couche 6 : Présentation 5/5

## LA COMPRESSION DES DONNÉES

La couche présentation assure également la compression des fichiers.

La compression applique des algorithmes (formules mathématiques complexes) pour **réduire la taille des fichiers**. L'algorithme cherche certaines séquences de bits répétitives dans les fichiers et les remplace par un« jeton »".

**Le jeton est une séquence de bits raccourcie qui est substituée à la séquence complète.**

Exemple : Remplacer« "Laboratoire Cisco »" par« Lab »"

On peut aussi utiliser un dictionnaire pour remplacer certains mots trop long : ils sont constitué des mots ou des séquences revenant le plus souvent ainsi que des séquences de remplacement, de manière à réduire considérablement les fichiers.

.B



# Couche 7 : Application



# Couche 7 : Application 1/17

## INTRODUCTION:

Le rôle de cette couche est **d'interagir avec les applications logicielles**. Elle fournit donc des services au module de communication des applications en assurant :

- ✓ **L'identification et la vérification de la disponibilité des partenaires de communication**
- ✓ **La synchronisation des applications qui doivent coopérer**
- ✓ **L'entente mutuelle sur les procédures de correction d'erreur**
- ✓ **Le contrôle de l'intégrité des données**

Dans le modèle OSI, la couche application est la plus proche du système terminal (ou la plus proche des utilisateurs).

Celle-ci détermine si les ressources nécessaires à la communication entre systèmes sont disponibles.

Sans la couche application, il n'y aurait aucun support des communications réseau. Elle ne fournit pas de services aux autres couches du modèle OSI, mais elle collabore avec les processus applicatifs situés en dehors du modèle OSI.

Ces processus applicatifs peuvent être des tableurs, des traitements de texte, des logiciels de terminaux bancaires.

JB



## Couche 7 : Application 2/17

De plus, la couche application crée une **interface directe avec le reste du modèle OSI** par le biais d'applications réseau (navigateur Web, messagerie électronique, protocole FTP, Telnet, etc.) ou une interface indirecte, par le biais d'applications autonomes (comme les traitements de texte, les logiciels de présentation ou les tableurs), avec des logiciels de redirection réseau.

Voici en détails les principaux protocoles utilisés par la couche transport :

.B





# Couche 7 : Application 3/17

## PRÉSENTATION DU PROTOCOLE DNS

-  Chaque station possède une adresse IP propre. Cependant il est nettement plus simple de travailler avec des noms de stations ou des adresses plus explicites comme par exemple <http://www.labocisco.com>, qu'avec des adresses IP.
-  Pour répondre à cela, le protocole **DNS permet d'associer des noms en langage courant aux adresses numériques.**
-  **Résolution de noms de domaines** : Corrélation entre les adresses IP et le nom de domaine associé.

IB



# Couche 7 : Application 4/17

## LES NOMS D'HÔTES ET LE « DOMAIN NAME SYSTEM »

Aux origines de TCP/IP, étant donné que les réseaux étaient très peu étendus, c'est-à-dire que le nombre d'ordinateurs connectés à un même réseau était faible, les administrateurs réseau créaient des fichiers appelés tables de conversion statique (fichiers généralement appelé hosts ou hosts.txt), associant sur une ligne, grâce à des caractères ASCII, l'adresse IP de la machine et le nom littéral associé, appelé nom d'hôte.



Ce système à l'inconvénient majeur de nécessiter la mise à jour des tables de tous les ordinateurs en cas d'ajout ou modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallu mettre en place un système plus centralisé de gestion des noms. Ce système est nommé Domain Name System, traduisez Système de nom de domaine.

Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.

IB



# Couche 7 : Application 5/17

## LES NOMS D'HÔTES ET LE « DOMAIN NAME SYSTEM »

On appelle **nom de domaine**, le **nom à deux composantes**, dont la première est un nom correspondant au **nom de l'organisation** ou de l'entreprise, le second à la **classification de domaine**. (**.fr, .com, ...**).

Chaque machine d'un domaine est appelée hôte. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré (le serveur Web d'un domaine porte généralement le nom **WWW**). 

L'ensemble constitué du nom d'hôte, d'un point, puis du nom de domaine est appelé adresse **FQDN (Fully Qualified Domain, soit Domaine Totalement Qualifié)**. Cette adresse permet de repérer de façon unique une machine. Ainsi, [www.cisco.com](http://www.cisco.com) représente une adresse FQDN.

.B



# Couche 7 : Application 6/17

## LES NOMS D'HÔTES ET LE « DOMAIN NAME SYSTEM »

Les machines appelées **serveurs de nom** de domaine permettent d'établir la correspondance entre **le nom de domaine et l'adresse IP sur les machines d'un réseau**. Chaque domaine possède ainsi, un serveur de noms de domaines, relié à un serveur de nom de domaine de plus haut niveau.

Ainsi, **le système de nom est une architecture distribuée**, c'est-à-dire qu'il n'existe pas d'organisme ayant à charge l'ensemble des noms de domaines. Par contre, il existe un organisme (l'InterNIC pour les noms de domaine en..com,.net,.org et .edu par exemple). Le système de noms de domaine est transparent pour l'utilisateur, néanmoins il ne faut pas oublier les points suivants.

Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette **machine est appelée Domain Name Server**. L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) peut également être introduite : il peut relayer le premier en cas de panne.

.B





# Couche 7 : Application 7/17

## CODES DES DOMAINES INTERNET

La classification du domaine, parfois appelées **TLD (Top Level Domain**, soit domaines de plus haut niveau), correspond généralement à une **répartition géographique**.

Toutefois, il existe des noms, créés pour les Etats-Unis à la base, permettant de classifier le domaine selon le secteur d'activité, par exemple :

-  **.com** correspond aux entreprises à vocation commerciales (désormais ce code de domaine ne rime plus à grand chose et est devenu international)
-  **.edu** correspond aux organismes éducatifs
-  **.gov** correspond aux organismes gouvernementaux
-  **.net** correspond aux organismes ayant trait aux réseaux
-  **.org** correspond aux entreprises à but non lucratif
-  **.biz** correspond aux entreprises en générale
-  **.info** réservé aux sites d'informations

IB



# Couche 7 : Application 8/17

## FTP

FTP est un **protocole fiable et orienté connexion** qui emploie TCP pour transférer des **fichiers entre les systèmes** qui supportent ce protocole. Le but principal du ftp est de **transférer des fichiers à partir d'un ordinateur à un autre en copiant et/ou en déplaçant des fichiers des serveurs aux clients**, et des clients vers les serveurs. Le protocole FTP est assigné au port 21 par défaut.

Quand des fichiers sont copiés d'un serveur, FTP établit d'abord une connexion de **contrôle entre le client et le serveur**. Alors une deuxième connexion est établie, qui est un lien entre les ordinateurs par lequel les données sont transférées. Le transfert de données peut se faire en mode Ascii ou en mode binaire. Ces modes déterminent le codage utilisé pour le fichier de données, qui dans le modèle OSI est une tâche de couche présentation, comme nous l'avons vu précédemment.

Après que le transfert de fichiers ait fini, la connexion de transfert de données se coupe automatiquement. La connexion de contrôle est fermé quand l'utilisateur se déconnecte et clôture la session.

IB





## Couche 7 : Application 9/17

### TFTP

TFTP est un service non orienté connexion qui emploie UDP. TFTP (Trivial FTP) est employé sur un routeur pour **transférer des dossiers de configuration et des images d'IOS de Cisco** et aussi pour transférer des fichiers entre les systèmes qui supportent TFTP. TFTP est conçues pour être léger et simple à utiliser. Néanmoins TFTP peut lire ou écrire des fichiers sur un serveur à distance mais il ne peut pas lister les répertoires et ne supporte pas une authentification utilisateur. Il est utile dans certains Lans parce qu'il fonctionne plus rapidement que le ftp.

JB



# Couche 7 : Application 10/17

## HTTP

Le protocole de transfert hypertexte (HTTP) fonctionne avec le **World Wide Web**, qui est la partie la plus utilisée et la plus importante d'Internet. Une des raisons principales de cette croissance extraordinaire est la facilité avec laquelle il permet l'accès à l'information.

Un navigateur web est une **application client/serveur**, qui implique l'existence d'un client et d'un serveur, composant spécifique installé sur les 2 machines afin de fonctionner.

Un navigateur web présente des données dans un format multimédia, c'est-à-dire un contenu réagissant aux actions de l'utilisateur. Le contenu peut être du texte, des graphiques, du son, ou de la vidéo.

Les pages web sont écrite en utilisant l'**HTML (HyperText Markup Language)** : un navigateur web reçoit la page au format HTML et l'interprète de manière à afficher la page d'une manière beaucoup plus agréable qu'un document texte.

JB



# Couche 7 : Application 11/17

## HTTP

Pour déterminer **l'adresse IP d'un serveur HTTP distant**, le navigateur utilise le protocole DNS pour retrouver l'adresse IP à partir de l'URL. **Les données qui sont transférées au serveur HTTP contiennent la localisation de la page Web sur le serveur.**

Le serveur répond à la requête par l'envoi au navigateur du code html ainsi que des différents objets multimédia qui agrémentent la page (son, vidéo, image) et qui sont indiqués dans les instructions de la page HTML. Le navigateur rassemble tous les fichiers pour créer un visuel de la page Web, et termine la session avec le serveur. Si une autre page est demandée, le processus entier recommence.

JB



# Couche 7 : Application 12/17

## SMTP

**Les serveurs d'email** communiquent entre eux en employant le *Simple Mail Transfer Protocol (SMTP)*

pour envoyer et recevoir du courrier. Le protocole SMTP achemine des messages email dans le format **Ascii en utilisant TCP**. On l'utilise souvent en tant que protocole d'envoi de mail, rarement en tant que protocole de récupération d'email, car il est peu sécurisé et surtout n'offre aucune authentification.



IB



## SNMP

Le **Simple Network Management Protocol (SNMP)** est un protocole de la couche application qui facilite **l'échange d'information de gestion entre les dispositifs d'un réseau**. Le SNMP permet à des administrateurs réseau de **contrôler l'état du réseau, détecter et résoudre des problèmes de réseau, et de prévoir le développement du réseau, si jamais celui-ci arrive à saturation**.

Le SNMP emploie le protocole UDP en tant que protocole de couche transport. Un réseau contrôlé par SNMP comprend les trois composants clés suivants:

IB



## Couche 7 : Application 14/17

- 💡 **Système de gestion de réseau (NMS / Network Management System) :** NMS exécute les applications qui supervisent et contrôle les dispositifs gérés. Un ou plusieurs NMS doivent exister sur n'importe quel réseau géré.
- 💡 **Dispositifs managés :** Les dispositifs managés sont des nœuds du réseau qui contiennent un agent SNMP et qui résident sur un réseau managé.  
Les dispositifs managés rassemblent et stockent des informations de gestion et rendent cette information disponible à NMS à l'aide des dispositifs SNMP. Les dispositifs managés, parfois appelés éléments de réseau, peuvent être des routeurs, des serveurs d'accès, des commutateurs, et des ponts, des concentrateurs, des ordinateurs hôtes, ou des imprimantes.
- 💡 **Agents :** Les agents sont des modules de logiciel réseau - gestion qui résident dans des dispositifs managés. Un agent a la connaissance locale d'information de gestion et traduit cette information en un format compatible avec SNMP.

JB



# Couche 7 : Application 15/17

## PRÉSENTATION DU PROTOCOLE TELNET

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client à un interpréteur de commande (côté serveur).

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet.

Il fournit ainsi un système orienté communication, bidirectionnel alterné (half-duplex), codé sur 8 bits facile à mettre en œuvre.

Le protocole Telnet repose sur trois concepts fondamentaux :

- ✓ Le paradigme du terminal réseau virtuel (NVT)
- ✓ Le principe d'options négociées
- ✓ Les règles de négociation

JB



## Couche 7 : Application 16/17

Ce protocole est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite **TCP/IP (FTP, SMTP, POP3, etc.)**.

Les spécifications de **Telnet ne mentionnent pas d'authentification**, car Telnet est totalement séparé des applications qui l'utilisent (le protocole FTP définit une séquence d'authentification au-dessus de Telnet).

En outre, le protocole Telnet est un **protocole de transfert de données non sûr**, c'est-à-dire que les données qu'il véhicule circulent en clair sur le réseau (de manière non chiffrée).

Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, **ce protocole est assigné au port 23**.

IB



# Couche 7 : Application 17/17

## LA NOTION DE TERMINAL VIRTUEL

Aux débuts d'Internet, le réseau (ARPANET) était composé de machines dont les configurations étaient **très peu homogènes** (claviers, jeux de caractères, résolutions, longueur des lignes d'affichage).

D'autre part, les sessions des terminaux possédaient également leur propre façon de contrôler les flux de données en entré/sortie.

Ainsi, au lieu de créer des adaptateurs pour chaque type de terminal afin qu'il puisse y avoir **une interopérabilité de ces systèmes**, il a été décidé de mettre au point une interface standard, appelée **NVT (Network Virtual Terminal, traduisez Terminal réseau virtuel)**, fournissant une base de communication standard, composée de :

-  Caractères ASCII 7 bits auxquels s'ajoutent le code ASCII étendu
-  Trois caractères de contrôle
-  Cinq caractères de contrôle optionnels
-  Un jeu de signaux de contrôle basique

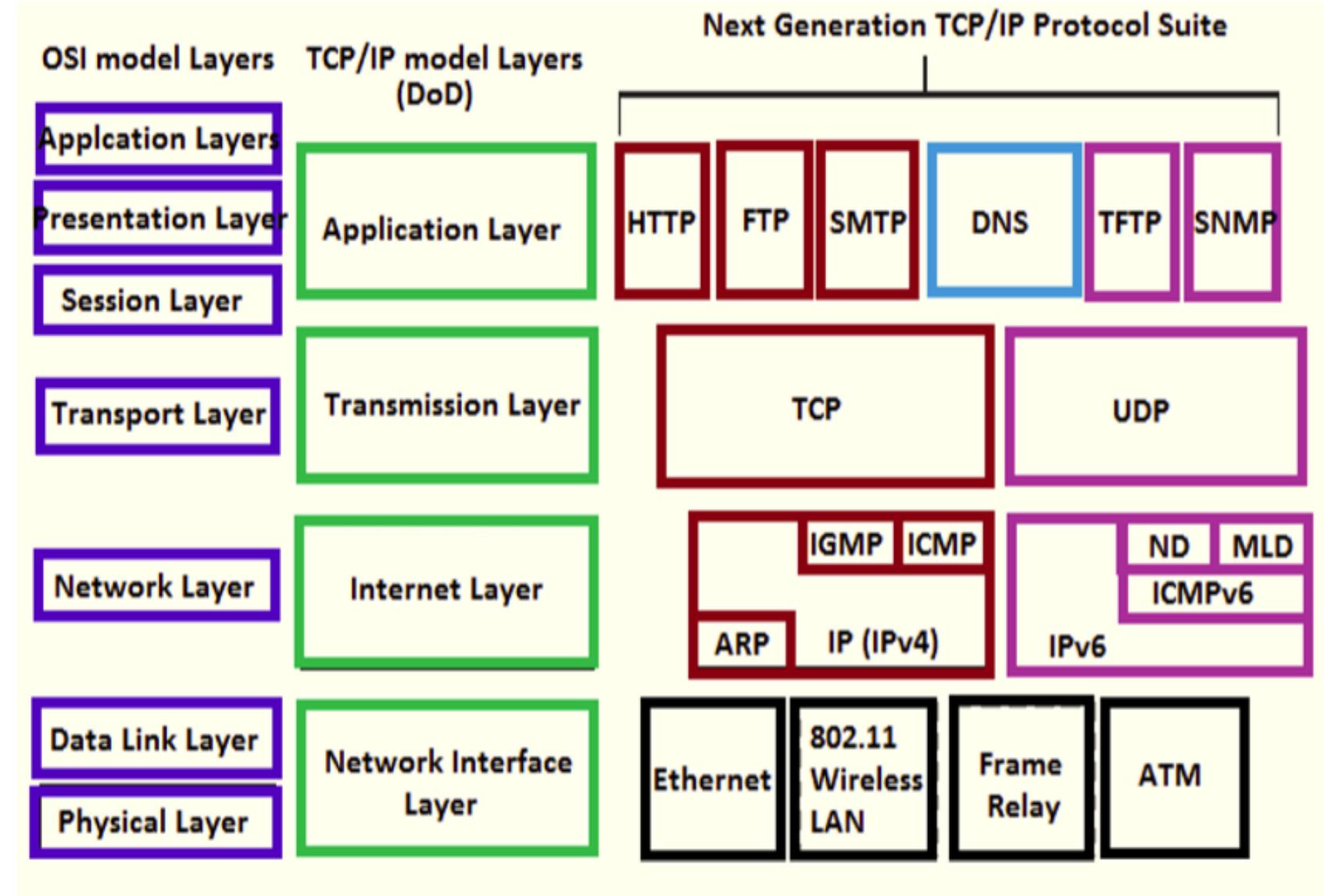
Le protocole Telnet consiste ainsi à créer une abstraction du terminal, permettant à n'importe quel hôte (client ou serveur) de communiquer avec un autre hôte sans connaître ses caractéristiques.

.B





# TCP/IP



## Droit d'auteur des ressources pédagogiques

Sauf consentement formel des auteurs, nous vous alertons que **tout partage partiel ou total d'un document fourni par vos enseignants** (quelle que soit sa nature) **est strictement interdit**, conformément au Code de la Propriété Intellectuelle (art. [L. 122-4](#) et art. [L. 335-3](#)).

**En cas d'enfreinte au règlement, vous vous exposez à une action en justice assortie d'une peine conséquente** (art. [L. 335-2](#)).

Sont concernés notamment les partages sur des plateformes publiques (Studocu, Stuvia, Facebook et assimilées) mais également toute cession de ressources pédagogiques, en tout ou partie.

