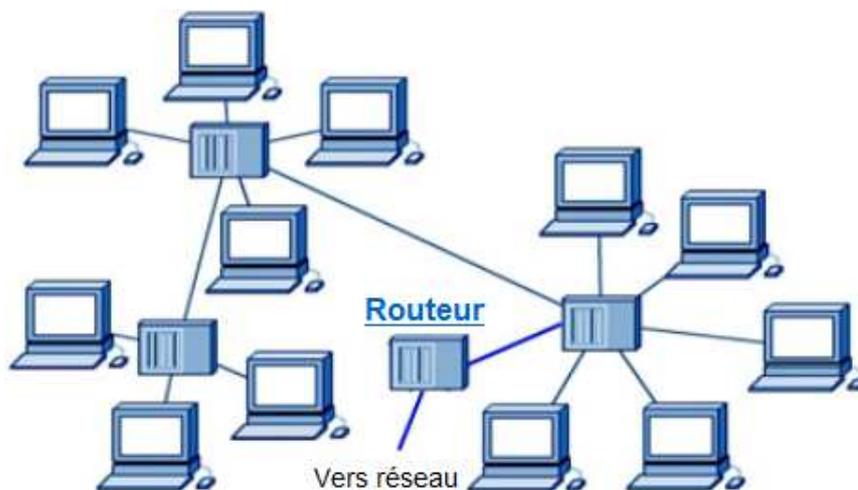


# Communication en réseau

## Cours - Synthèse



### Table des matières

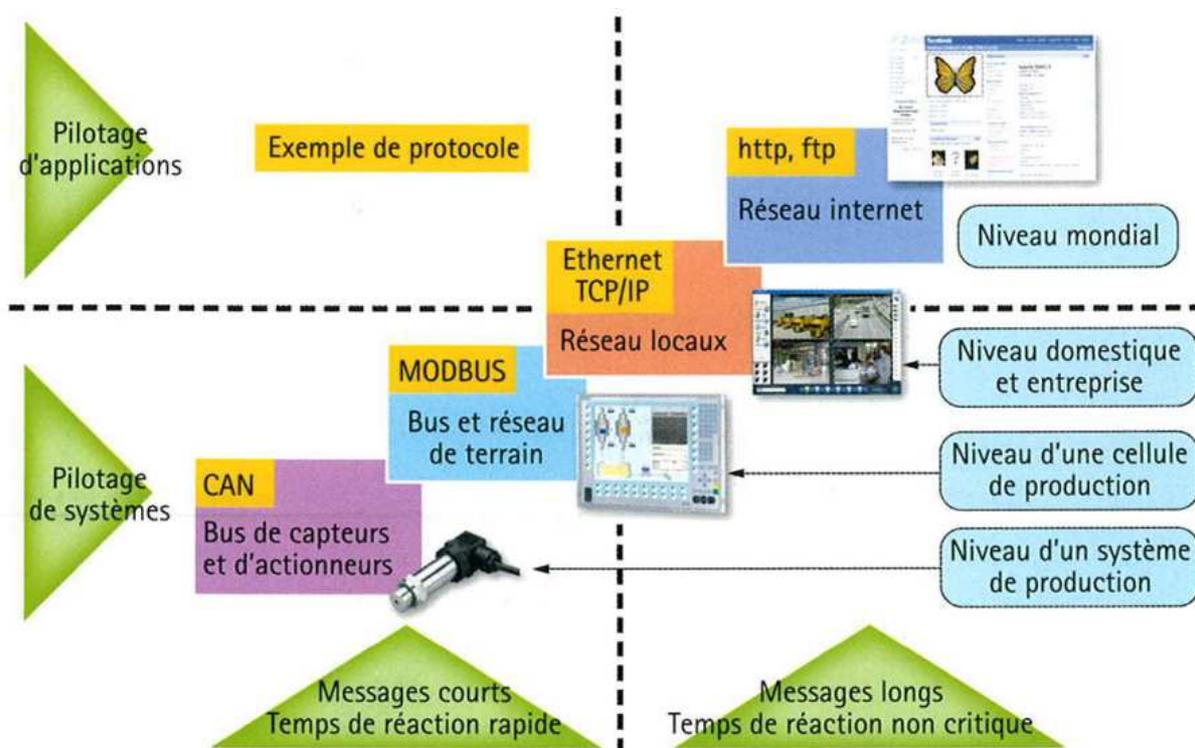
<b>1) Réseaux de terrain et informatique</b> .....	<b>2</b>
1.1) Les réseaux - généralités .....	2
1.2) Réseaux de terrain.....	3
1.3) Les réseaux informatiques.....	4
1.3.1) Présentation .....	4
1.3.2) Classification des réseaux informatiques .....	4
1.3.3) Architecture des réseaux informatiques .....	5
1.3.4) Topologie physique des réseaux informatiques.....	6
1.3.5) Topologie logique des réseaux informatiques .....	6
1.4) Support physique de transmission .....	7
1.5) transmission d'information sur un bus .....	8
<b>2) Modèle en couches / Multiplexage</b> .....	<b>9</b>
2.1) Le modèle TCP/IP.....	9
2.2) Multiplexage / Démultiplexage .....	11
2.3) Protocoles associés aux couches du modèle TCP/IP.....	11
<b>3) Adressage et Routage</b> .....	<b>12</b>
3.1) La communication informatique .....	12
3.2) Adressage IP (IPv4) .....	13
3.3) Masque de sous réseau .....	14
3.4) Adresse logique/physique, et table ARP .....	15
<b>4) Constituants d'un réseau sur Internet</b> .....	<b>17</b>

# 1) Réseaux de terrain et informatique

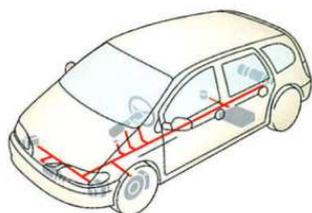
## 1.1) Les réseaux - généralités

Un réseau permet d'interconnecter entre eux différents hôtes afin d'échanger des informations. Les réseaux sont adaptés à la nature des échanges et des équipements connectés.

Il est possible d'interconnecter et de faire communiquer de nombreux équipements : capteurs et actionneurs industriels, caméras, imprimantes, ordinateurs avec différents systèmes d'exploitation.



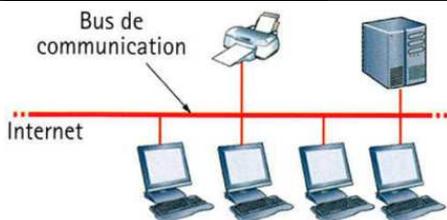
**On distingue deux types de réseau :**



**Réseaux de terrain :** (ou bus de terrain)

*Les bus de terrains sont utilisés sur un terrain précis (automobile par exemple), ils utilisent des technologies dédiées, afin de pouvoir communiquer de façon rapide et fiable.*

*Ils interconnectent généralement des capteurs, des actionneurs et des calculateurs.*



**Réseaux informatiques :**

*Ils mettent en liaison un ensemble d'équipements informatiques, et permettent de transmettre des données numériques parfois très complexes.*

## 1.2) Réseaux de terrain

Les réseaux de terrain permettent :

- Interconnexion entre plusieurs entités actives ou passives d'un même système;
- Réduction de la longueur des liaisons entre composants grâce au support commun de transmission ;
- Gain de place pour les systèmes d'électronique embarquée ;
- Transfert des informations de manière séquentielle : trames (paquet de bits) ;
- Insertion ou suppression d'éléments au sein d'un même système : modularité ...
- Diagnostique simplifié : connexion d'un système d'analyse pour identifier la panne ...

### 1.2.1) Exemples de protocoles de réseaux de terrain

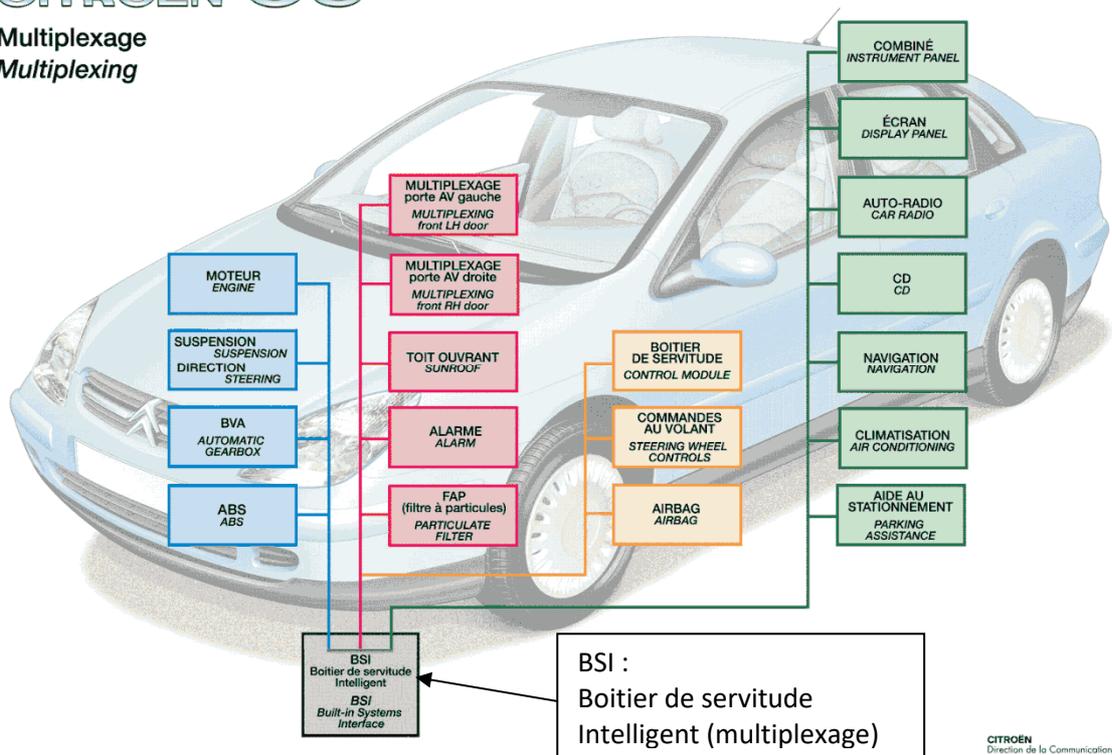
<b>Bus CAN</b>	Controller Area Network :	<i>Communication au sein des systèmes embarqués.</i>
<b>Bus I2C</b>	Inter Integrated Circuit :	<i>Communication entre composants électroniques.</i>
<b>Bus FIP</b>	Flux Information Process :	<i>Reseau de terrain industriel (électrotechnique)</i>
<b>Bus AS-i</b>	Actuator Sensor interface :	<i>Bus de terrain de type maître-esclave permettant de raccorder des capteurs et actionneurs en série.</i>

De nombreux autres réseaux (ou bus) de terrains industriels existent et ne sont pas décrits ici ...

### 1.2.2) Multiplexage en automobile :

CITROËN C5

Multiplexage  
Multiplexing



	<b>Circuit bleu</b>	<b>CAN (moteur, transmission, suspension et direction)</b>
	<b>Circuit rouge</b>	<b>VAN (carrosserie : portes avant, toit ouvrant, alarme et FAP)</b>
	<b>Circuit jaune</b>	<b>VAN (carrosserie : commandes au volant, airbag et divers)</b>
	<b>Circuit vert</b>	<b>VAN (confort : radio, GPS, climatisation,...)</b>

### 1.3) Les réseaux informatiques

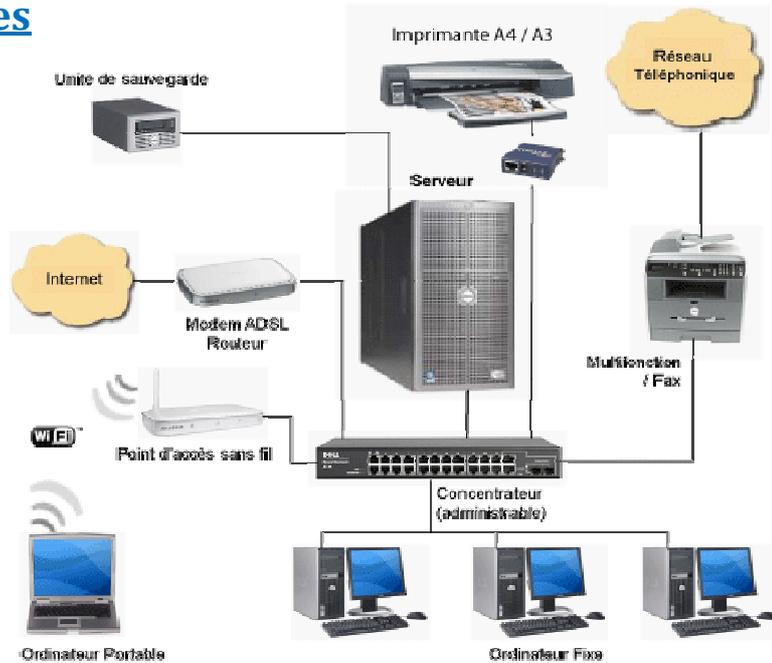
#### 1.3.1) Présentation

**Un réseau informatique est un ensemble d'équipements informatiques reliés entre eux pour échanger des informations et utiliser des ressources partagées.**

La mise en œuvre d'un réseau suppose les infrastructures suivantes :

- Liaisons physiques : câbles, ondes, etc...
- Equipements de transmission et d'interconnexion : carte réseau, routeur, switch...

Un réseau nécessite aussi la mise en œuvre de protocoles de communication permettant de définir la manière dont les informations sont échangées.



Un réseau informatique est généralement composé :

- d'un ou plusieurs serveurs : machines qui fournissent des ressources partagées aux utilisateurs ;
- de clients : machines qui accèdent aux ressources partagées ;
- de ressources partagées : fichiers, périphériques ou autres éléments utilisés par les usagers ;
- de supports de transmission : câbles Ethernet (RJ45), ondes WiFi, fibre optique... ;
- d'équipements de transmission et d'interconnexion : carte réseau, routeur, switch...

Un réseau nécessite aussi la mise en œuvre de protocoles de communication permettant de définir la manière dont les informations sont échangées.

#### 1.3.2) Classification des réseaux informatiques

La distinction entre différents réseaux se fait selon trois critères :

- le nombre d'éléments le constituant,
- la dispersion géographique,
- les technologies de transfert de données utilisées (supports physiques et protocoles).

LAN	MAN	WAN
<b>LAN :</b> Local Area Network ou réseau local	<b>MAN :</b> Metropolitan Area Network ou réseau métropolitain	<b>WAN :</b> Wide Area Network ou réseau étendu
Un LAN relie des équipements informatiques faiblement distants.	Un MAN interconnecte plusieurs LANs géographiquement proches.	Un WAN interconnecte des LANs ou MANs sur de grandes distances.
<u>Exemple :</u> Réseau d'une société	<u>Exemple :</u> Réseau urbain	<u>Exemple :</u> Internet
<u>Echelle :</u> lycée, entreprise, etc... S'étend de 1 mètre à 2 kilomètres. de 2 à plusieurs centaines d'abonnés.	<u>Echelle :</u> campus, ville, métropole. S'étend sur quelques dizaines de km, de 2 à quelques milliers d'abonnés.	<u>Echelle :</u> pays, continent, planète S'étend sur plus de 1000 kilomètres, plusieurs milliers d'abonnés.
Débit courant : 10 Mbits à 1 Gbits/s.	Débit courant : 10 Mbits à 1 Gbits/s.	Débit courant : 50 bits/s à 2 Mbits/s.

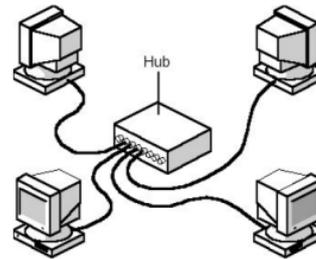
### 1.3.3) Architecture des réseaux informatiques

On distingue essentiellement trois types d'architectures réseau :

#### Architecture en GROUPE DE TRAVAIL (Workgroup)

Dans le cas d'un groupe de travail, les machines sont a priori toutes identiques (en puissance et en accès réseau). On se limite à de l'échange d'informations entre les postes.

Ce type d'architecture ne s'utilise que pour les réseaux de type LAN avec peu d'abonnés (quelques dizaines).



#### Avantages

- Très facile à mettre en œuvre,

#### Inconvénients

- Sécurité très faible,
- Aucune machine ne gère réellement le réseau.

#### Architecture CLIENT-SERVEUR

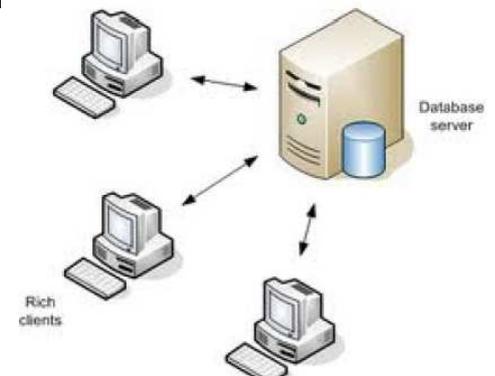
Ce type d'architecture s'utilise pour les réseaux de type LAN comportant généralement un nombre assez élevé d'abonnés (lycée, petite entreprise par exemple).

#### Deux types de machines :

Les serveurs : Machines dédiées à des tâches spécifiques

- un serveur de domaine : gestion des personnes et des postes,
- un serveur de données : stockage d'informations,
- un serveur d'impression : gestion des impressions sur le réseau...

Les postes clients : Sensiblement tous identiques (en puissance et en accès réseau) et à disposition des utilisateurs.



#### Avantages

- Le poste client peut être indifférencié : interface et ressources présentées de la même façon sur les postes clients,
- La centralisation des données offre une plus grande sécurité,
- Serveurs toujours en fonctionnement et données toujours disponibles.

#### Inconvénients

- La décentralisation entraîne un trafic conséquent sur le réseau et nécessite une bande passante importante,
- La mise en œuvre demande de bonnes connaissances pour bien administrer un tel réseau.

#### Architecture INTERNET - "Réseau des réseaux"

Il permet de mettre en relation des machines appartenant à des réseaux distincts au travers d'une « toile » ou du « web » (topologie de maille).

Un réseau privé utilisant l'architecture Internet peut être réalisé ; on parle alors d'intranet. (grandes entreprises par exemple).



#### Avantages

Grande diffusion d'informations en rendant accessible au public des services comme le courrier électronique et le World Wide Web.

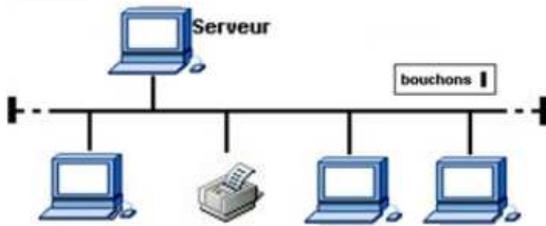
#### Inconvénients

Le fait d'interconnecter les réseaux demande une supervision importante de l'ensemble et une grande compétence technique dans la gestion des réseaux.

### 1.3.4) Topologie physique des réseaux informatiques

La topologie physique désigne l'organisation spatiale des éléments matériels constituant le réseau :

**en BUS (I2C, SPI, CAN...) :**



**BUS :**

**Avantage(s) :** La simplicité.

**Inconvénient(s) :**

Un seul ordinateur peut émettre des données.  
Tout le réseau est affecté dès qu'une liaison est défectueuse.

**en ANNEAU :**



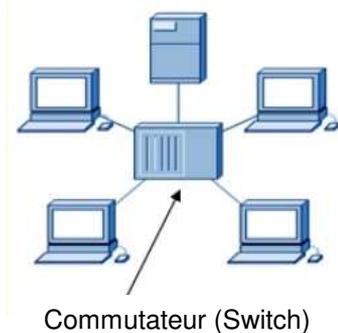
**ANNEAU :**

Des informations y circulent pour désigner pour désigner l'ordinateur qui a le droit d'émettre.  
L'ordinateur s'empare du jeton ou passe le tour (évite les collisions).

**Avantage(s) :** Collisions évitées.

**Inconvénient(s) :** Equipement couteux.

**en ETOILE (UART, broches I/O...) :**

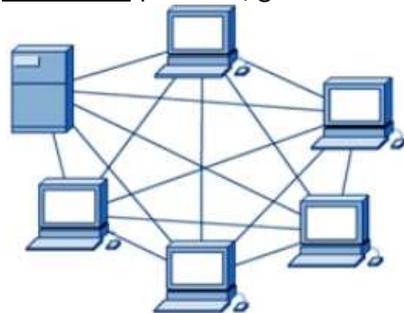


**ETOILE :**

**Avantage(s) :**

Un problème de connexion vers une machine n'affecte pas le reste du réseau.

**en MAILLE (Internet, grands réseaux...) :**



**MAILLE :**

C'est une évolution de la topologie en étoile.  
Chaque terminal est relié à tous les autres. Cette topologie se rencontre dans les grands réseaux de distribution (exemple : Internet).

L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.

**Avantage(s) :**

En cas de rupture d'un lien, l'information peut quand même être acheminée.

**Inconvénient(s) :**

Le nombre de liaisons nécessaires devient très élevé.

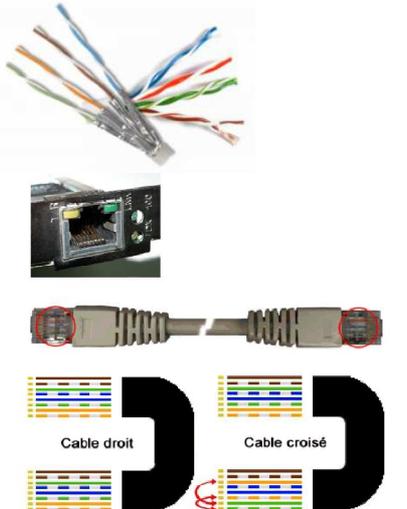
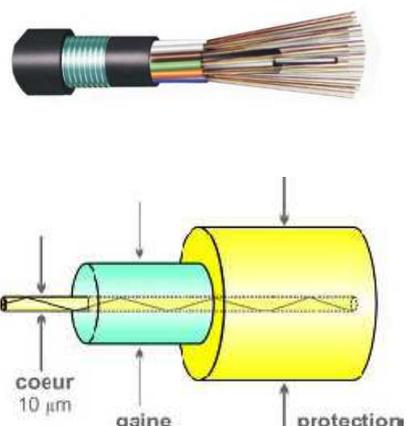
**NB :** la plupart des réseaux informatiques actuels utilise une topologie en étoile et/ou en maille.

### 1.3.5) Topologie logique des réseaux informatiques

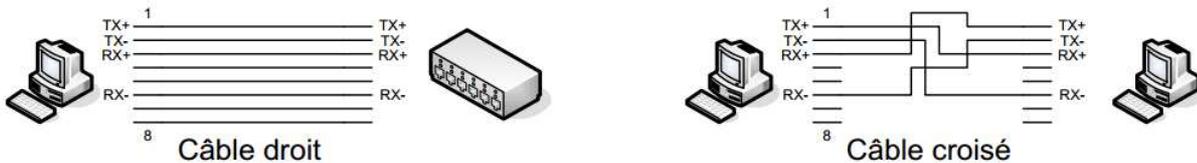
La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication.

- **Cas du protocole Ethernet :** Chaque machine peut envoyer des données sur le réseau à n'importe quel moment – Réémission de données en cas de collision après un temps d'attente.
- **Cas du protocole Token Ring :** Pour qu'une machine puisse envoyer des données sur le réseau, il faut que le jeton (token) passe devant cette machine.

## 1.4) Support physique de transmission

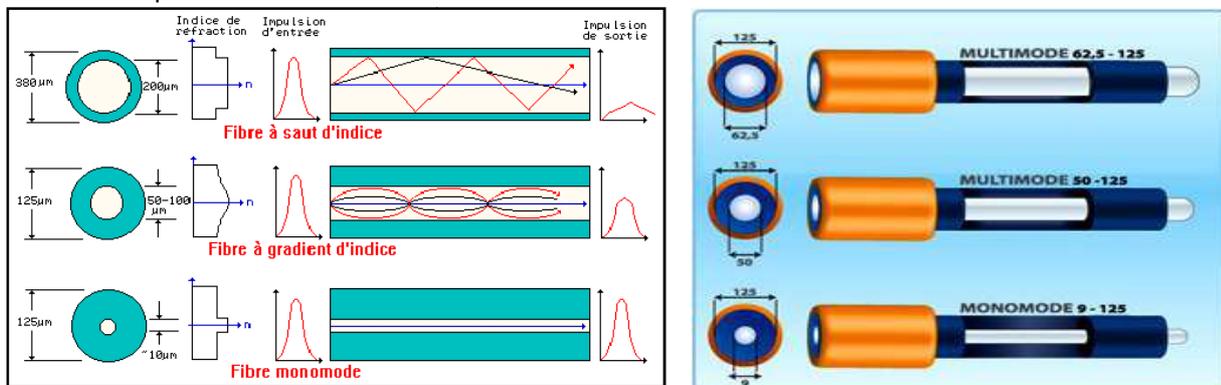
Câbles et connecteurs RJ45 (8 fils)	Fibre Optique	Ondes électromagnétiques
 <p>10Base-T, 100Base-TX, 100Base-FX, 1000Base-T</p> <p><b>Technique répandue sur de faibles longueurs (LAN)</b></p>	 <p>1000Base-SX, 1000Base-LX</p> <p><b>Technique utilisée pour les hauts débits</b></p>	 <p>Ondes radio, wifi, Bluetooth, ZigBee, GSM (3G, 4G) ...</p> <p><b>Technique répandue</b></p>

**Les câbles RJ45 (aussi appelés câbles réseau ou encore câble Ethernet)** sont droits ou croisés, cf. schéma ci-dessous. Aujourd'hui Windows détecte automatiquement le type de câble mais certains systèmes ont encore besoin de les différencier : le câble croisé pour relier directement deux ordinateurs entre eux (très peu utilisé aujourd'hui), ou câble droit pour relier un ordinateur à un concentrateur réseau (switch, hub, ou routeur).

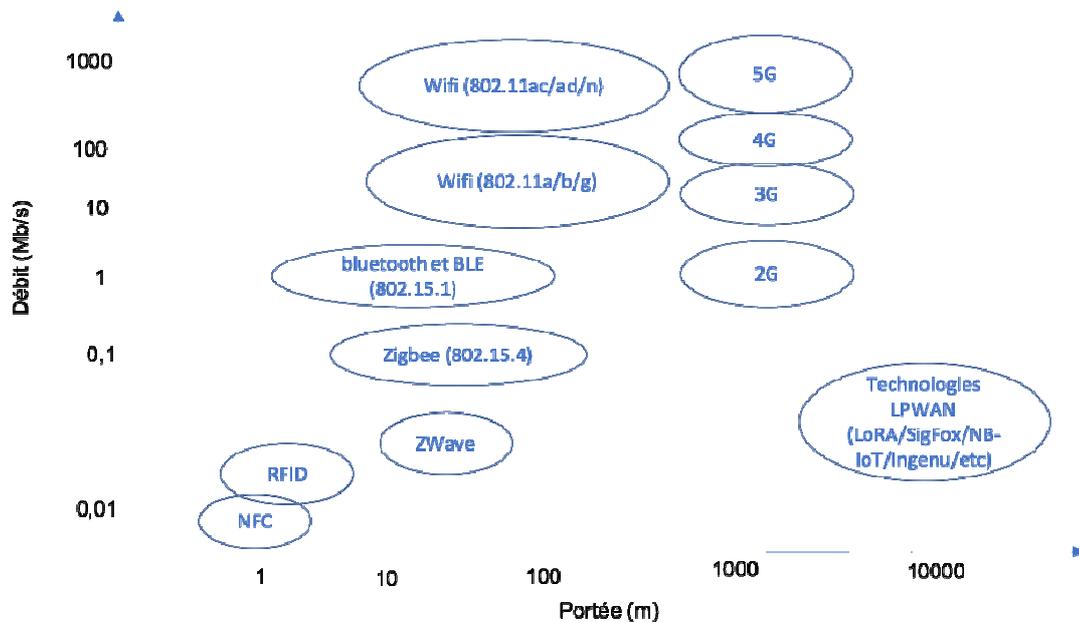


TX (Transmission) est utilisé pour l'écriture, et RX (Réception) pour la lecture. TX- et RX- sont les valeurs complémentaires des signaux TX+ et RX+, et ne servent qu'à vérifier la bonne transmission de ces-derniers. Seuls ces quatre fils sont utilisés dans le protocole TCP/IP (Ethernet, Internet...).

**La fibre optique** est un support unidirectionnel, il faut donc 2 fibres pour assurer une liaison bidirectionnelle. Deux types de fibres existent sur le marché : La fibre multimode et la fibre monomode. La fibre monomode offre de meilleurs performances mais coûte plus cher que le multimode, elle est essentiellement utilisée pour des distances importantes entre réseaux.



### Ondes électromagnétiques (principales technologies sans fil) :



### Transmission Simplex/Duplex :

Dans un seul sens : **simplex** (émission radio, TV...).

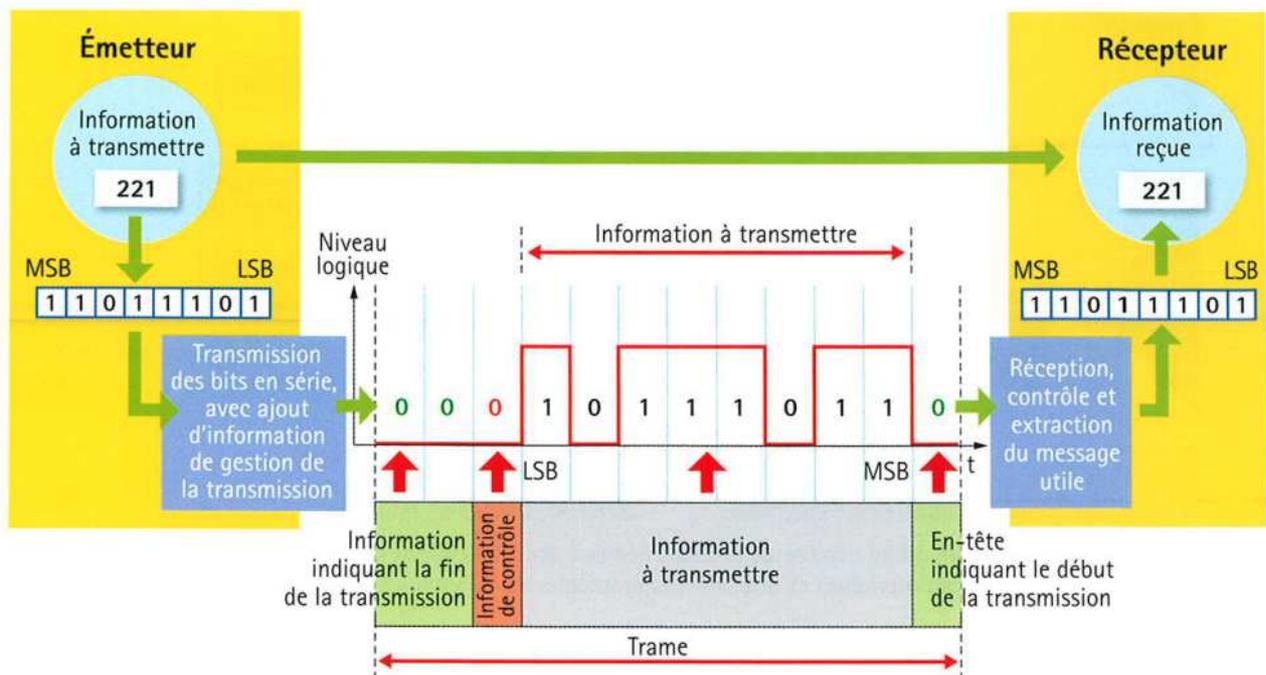
Dans les deux sens mais pas en même temps : **half – duplex** (Talkie Walkie, CB...).

Dans les deux sens et en même temps : **full – duplex** (téléphonie, Ethernet...).

## 1.5) transmission d'information sur un bus

Le point commun entre tous les réseaux réside dans le fait que tous les éléments sont reliés entre eux par un bus de communication commun. Il est donc nécessaire de gérer la façon dont les constituants vont échanger des informations sans interférences. Il convient pour cela de mettre en œuvre un langage commun aux différents éléments communicants, appelé protocole de communication.

### Transmission série d'une donnée utile de 8 bits :



### Principes basiques de la transmission d'informations sur un bus :

1. Les données numériques sont envoyées les unes après les autres en série, sous forme d'une succession de bits, à une cadence donnée,
2. On ajoute aussi les informations concernant l'identité de l'émetteur et celle du récepteur,
3. A ces informations, il est nécessaire d'ajouter celle qui vont gérer la transmission : « début de la transmission », « bonne transmission », « fin de la transmission » (a minima).

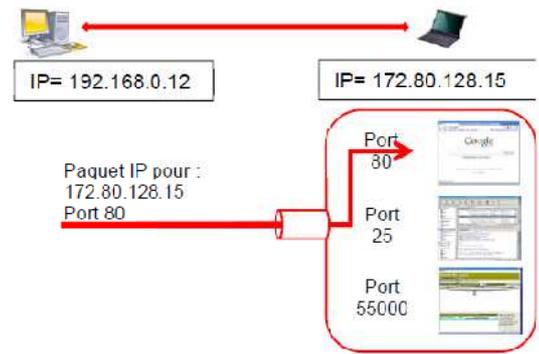
## 2) Modèle en couches / Multiplexage

Pour qu'une communication d'informations fonctionne, il faut établir quelques règles simples.

Dans le cas du réseau informatique, ces règles sont appelées **PROTOCOLE** : système de communication normalisé permettant aux machines de communiquer entre-elles.

Pour que l'ordinateur A puisse envoyer un message à l'ordinateur B, il doit connaître son adresse. Il s'agit de l'**adresse IP**.

Il peut y avoir plusieurs programmes qui fonctionnent en même temps sur l'ordinateur B : **A chaque logiciel correspond un numéro unique appelé PORT**. Ce numéro est transmis avec l'adresse IP.



### 2.1) Le modèle TCP/IP

#### 2.1.1) Présentation

TCP/IP est en fait une **suite de protocoles**. Cette appellation vient des noms des deux principaux protocoles de la suite, à savoir :

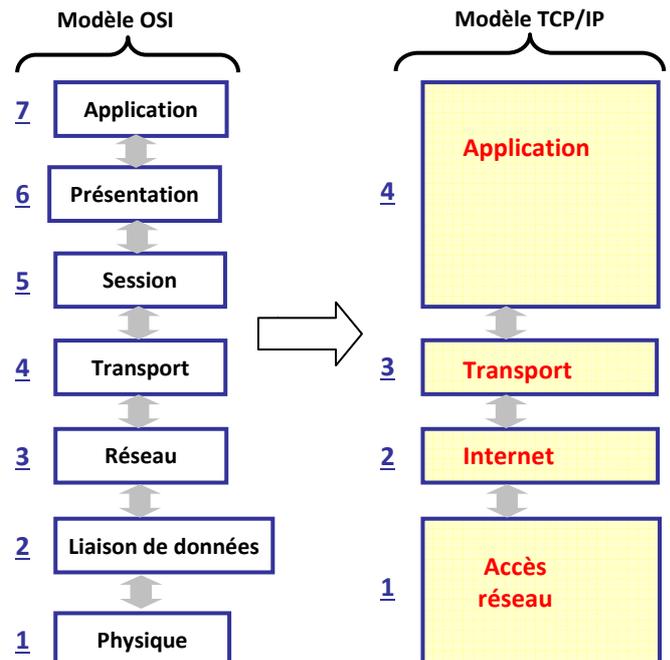
**TCP – Transmission Control Protocol**

**IP – Internet Protocol**

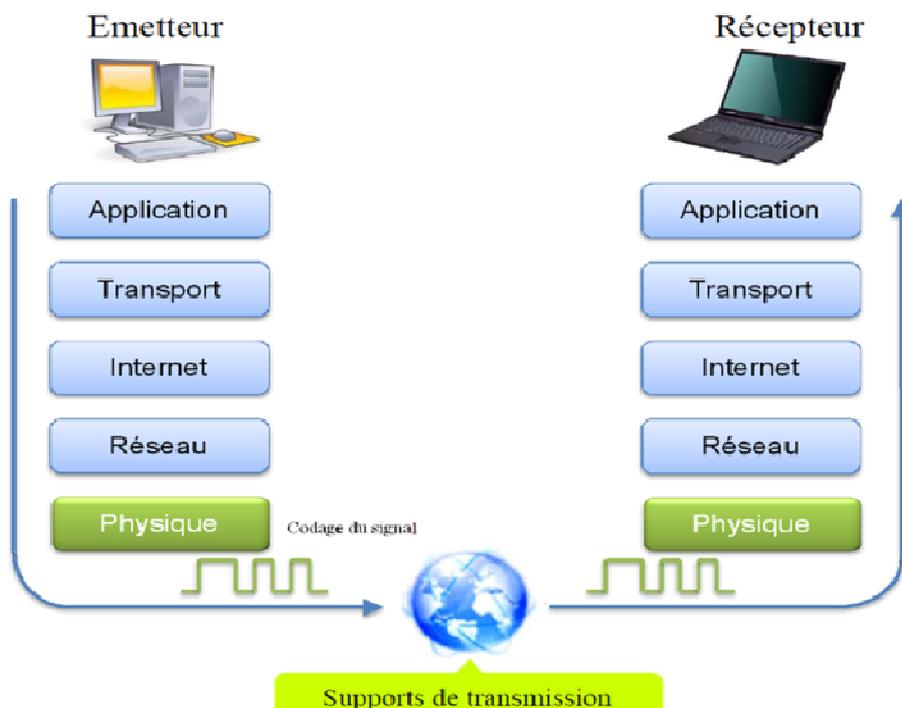
Le modèle TCP/IP fournit un cadre de référence pour le développement des protocoles utilisés sur Internet.

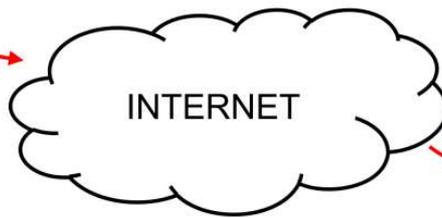
Il se compose de 4 couches, qui exécutent les fonctions nécessaires pour préparer les données à une transmission sur le réseau.

Il est basé sur le modèle normalisé international OSI, mais simplifié.



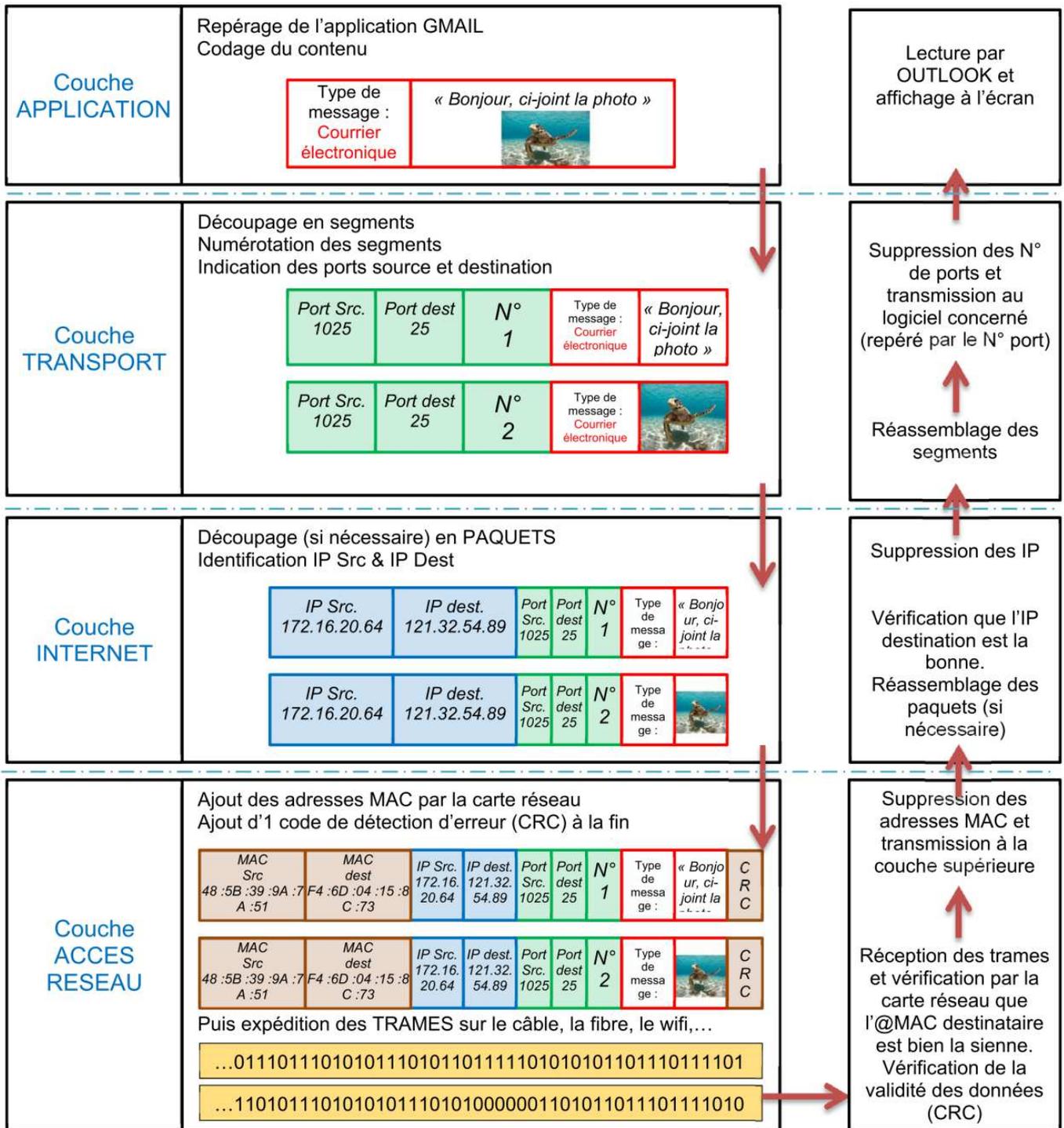
#### 2.1.2) Fonctionnement simplifié par "Couches" du modèle TCP/IP





**Expéditeur**  
 Logiciel : messagerie GMAIL  
 @IP : 172.16.20.64  
 @MAC : 48 :5B :39 :9A :7A :51

**Destinataire**  
 Logiciel : messagerie OUTLOOK  
 @IP : 121.32.54.89  
 @MAC : F4 :6D :04 :15 :8C :73

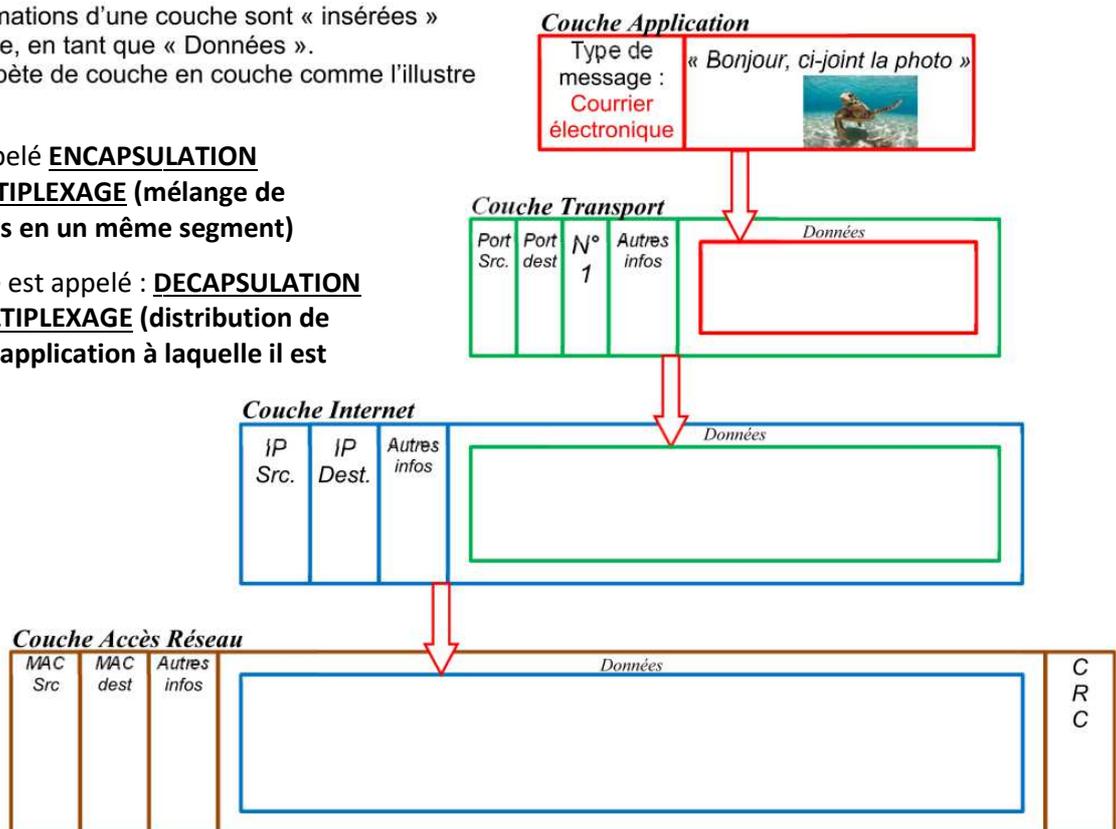


## 2.2) Multiplexage / Démultiplexage

A l'émission, es informations d'une couche sont « insérées » dans la couche voisine, en tant que « Données ».  
Ce phénomène se répète de couche en couche comme l'illustre le schéma ci-contre.

Ce processus est appelé **ENCAPSULATION**  
Cela permet le **MULTIPLXAGE** (mélange de différents protocoles en un même segment)

Le processus inverse est appelé : **DECAPSULATION**  
et permet le **DEMULTIPLXAGE** (distribution de chaque segment à l'application à laquelle il est destiné)



Le multiplexage/démultiplexage est possible grâce à un code indiquant quel protocole ou quel port est utilisé dans la couche suivante (encapsulée). Cela permet le mélange de différents protocoles.

En fin de démultiplexage, les **numéros de ports** contenus dans les en-têtes TCP et UDP permettent de connaître l'**application** à laquelle il faut restituer les données.

### Multiplexage temporel ou fréquentiel :

Le multiplexage dans le protocole Ethernet filaire est un multiplexage temporel, séparant dans le temps les bits appartenant aux différents protocoles.

Il existe aussi des techniques de multiplexage fréquentiel (utilisés dans les lignes téléphoniques, ADSL, et fibre optique), permettant la transmission de plusieurs protocoles simultanément, dans des plages de fréquence différentes.

## 2.3) Protocoles associés aux couches du modèle TCP/IP

<b>Couche 4: APPLICATIONS</b>						
FTP	SMTP	POP	IMAP	SSH	RPC	etc...
<b>Couche 3: TRANSPORT</b>						
TCP	UDP					
<b>Couche 2: INTERNET</b>						
IP	ARP	RARP	ICMP	IGMP		
<b>Couche 1: RESEAU</b>						
ATM	X25	Ethernet	Token ring	FDS	FDDI	etc...

Sur cette couche circulent des :  
**Données** appelées aussi **messages**

Sur cette couche circulent des :  
**Segments TCP** ou bien **Paquets UDP**

Sur cette couche circulent des :  
**Datagrammes**

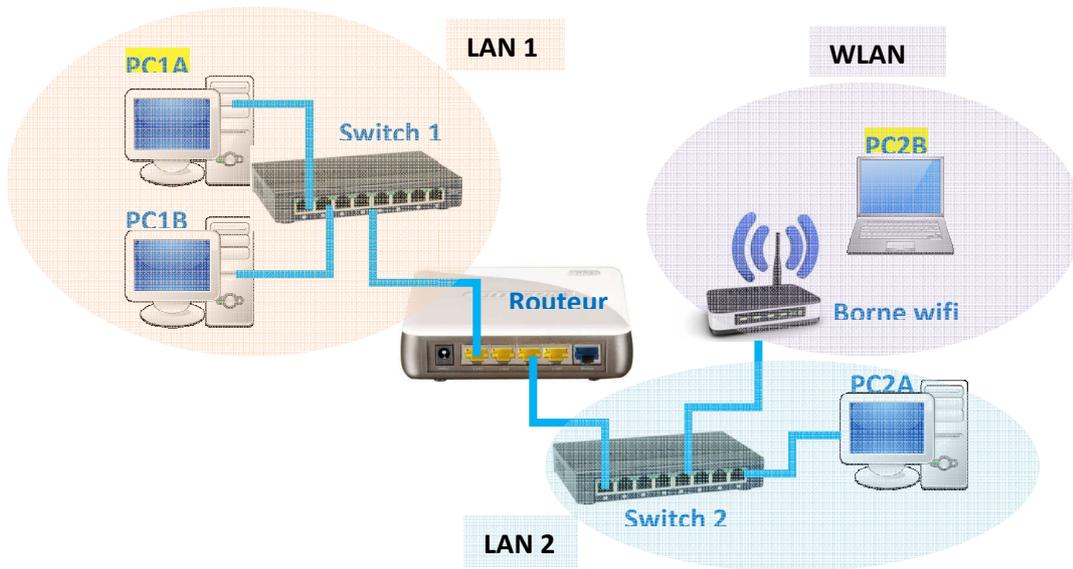
Sur cette couche circulent des :  
**Trames**

### 3) Adressage et Routage

#### 3.1) La communication informatique

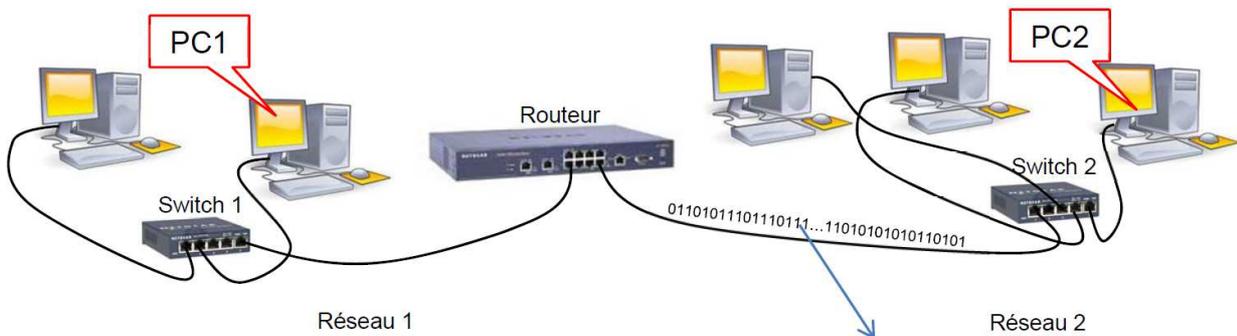
##### 3.1.1) Introduction

La communication entre deux ordinateurs peut être comparée à l'envoi d'un courrier postal entre un expéditeur et un destinataire. Dans les deux cas, il est nécessaire de connaître l'adresse. Si PC1A veut envoyer un message à PC2B, il a besoin d'une adresse réseau : **l'adresse IP (Internet Protocol)**.



##### 3.1.2) Protocole Internet

Le protocole internet a été conçu pour interconnecter les réseaux informatiques, il assure la transmission des paquets de données appelés datagrammes entre un ordinateur source et un autre de destination.



Chaque datagramme circulant sur le réseau possède un en-tête qui contient l'ensemble des informations nécessaires à son acheminement vers sa destination.

En-tête IPv6 :

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

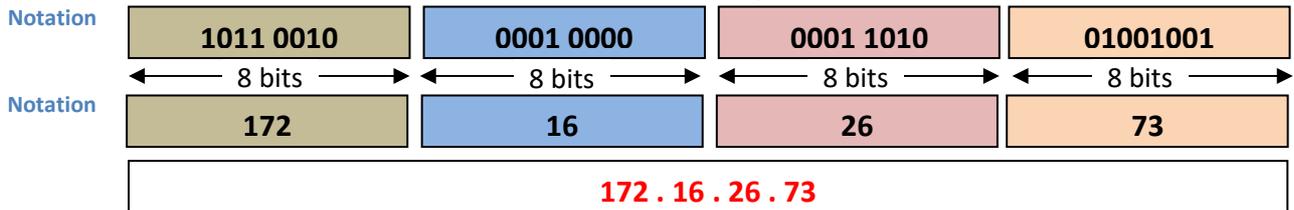
En-tête IPv4 :

Version	IHL	ToS	Total Length	
Identification			Flgs	Fragment Offset
Time To Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

## 3.2) Adressage IP (IPv4)

### 3.2.1) Notation

Une adresse **IPv4** est constituée de 4 octets, soit un nombre binaire de 32 bits (1 octet = 8 bits). Pour faciliter la lecture de l'adresse IP, celle-ci est notée sous la forme décimale pointée.



**IPv6** : En IPv4 il peut exister  $2^{32} = 4.10^9$  adresses différentes possibles (moins les adresses privées), et le réseau aurait saturé en 2011. C'est pourquoi les adresses IPv6, standardisées en 2017 remplacent progressivement la norme IPv4. Les adresses IPv6 fonctionnent sur le même principe mais sont constituées de 128 bits (16 octets), soit  $2^{128} = 3.10^{38}$  adresses différentes possibles (moins les adresses privées). Elles s'écrivent sous la forme de 8 groupes de 2 octets, séparés par un signe deux-points :

**2001:0db8:0000:85a3:0000:0000:ac1f:8001**

ou encore, en enlevant les 0 non significatifs : 2001:db8:0:85a3:0:0:ac1f:8001

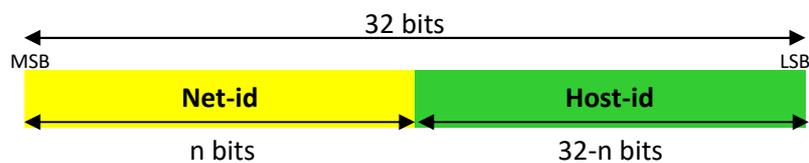
ou encore (suppression d'une suite de groupes à 0) : 2001:db8:0:85a3::ac1f:8001

Comme beaucoup de machines utilisent encore IPv4, on illustrera ce cours avec la norme IPv4, plus simple.

### 3.2.2) Structure

L'adresse IPv4 d'un élément du réseau est composée de 2 parties :

- Le numéro d'identification du réseau (NETID)
- Le numéro de l'hôte sur ce réseau (HOSTID). L'hôte désigne un appareil connecté.



La partie NETID peut être codée sur 1, 2 ou 3 octets (soit  $n=8$ ,  $n=16$  ou  $n=24$ ). Le nombre de bits restants est alors dédié à la partie HostID. Ce nombre détermine alors le nombre de machines pouvant être connectées sur le réseau.

Exemple : si la partie HOSTID est constituée de 16 bits, cela signifie qu'il existe de  $2^{16}$  combinaisons possibles pour créer un numéro d'hôte. On peut connecter en théorie 65 536 machines sur ce réseau.

### 3.2.3) Classification des adressages

Il existe plusieurs **classes** d'adresse IP. En fonction de cette classe, la taille du hostID varie (soit le nombre d'équipement connectable au réseau).

**Adresses réservées** : Il existe deux adresses réservées, donc non attribuables à un équipement :

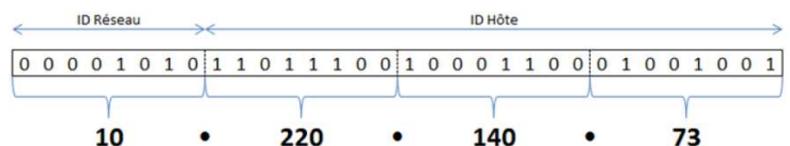
- **L'adresse réseau** est une adresse IP avec tous les bits de la partie Host-id à 0.
- **L'adresse de broadcast** (adresse de diffusion) est une adresse IP avec tous les bits de la partie Host-id à 1. Elle sert à cibler tous les hôtes du réseau.

Si la partie HOSTID est constituée de 16bits, cela signifie qu'il existe de  $(2^{16}-2)$  combinaisons possibles pour créer un numéro d'hôte. On peut donc connecter en réalité 65 534 machines sur ce réseau.

**Exemple :**



Adresse IP  
**10.220.140.73**



Classe A	
ID Réseau: 00001010 (10)	Adresse réseau: 00001010 00000000 00000000 00000000 (10.0.0.0)
ID Hôte: 11011100 10001100 01001001 (220.140.73)	Adresse de diffusion: 00001010 11111111 11111111 11111111 (10.255.255.255)

### 3.3) Masque de sous réseau

Le masque de sous réseau est constitué de 4 octets. Il permet d'identifier dans une adresse IP la partie **net-id** et la partie **host-id**.

Pour cela, il est nécessaire d'effectuer une opération logique de type ET entre chaque bit de l'adresse IP et chaque bit du masque de sous-réseau.

Les masques de sous réseau sont par défaut :

- En classe A : **255.0.0.0**
- En classe B : **255.255.0.0**
- En classe C : **255.255.255.0**

Pour déterminer l'adresse du réseau à partir d'une adresse IP, on effectue l'opération logique suivante:

$$\text{Adresse réseau} = (\text{Adresse IP}) \text{ ET } (\text{masque})$$

**Exemple 1 :** L'adresse IP de la machine est la suivante : 192.168.1.11 (ou encore 192.168.1.11/24)

Le masque est le suivant : 255.255.255.0 (24 bits à 1)

L'opération ET logique bit à bit est donc la suivante :

<b>Adresse IP</b>	192	168	1	11
	1100 0000	1010 1000	0000 0001	0000 1011
<b>Masque</b>	255	255	255	0
	1111 1111	1111 1111	1111 1111	0000 0000
<b>Résultat du ET</b>	<b>1100 0000</b>	<b>1010 1000</b>	<b>0000 0001</b>	<b>0000 0000</b>
Soit l'adresse réseau	<b>192</b>	<b>168</b>	<b>1</b>	<b>0</b>

**Exemple 2 compliqué :** L'adresse IP de la machine est la suivante : 192.168.1.166 (ou encore 192.168.1.166/25)

Le masque est le suivant : 255.255.255.128 (25 bits à 1)

L'opération ET logique bit à bit est donc la suivante :

<b>Adresse IP</b>	192	168	1	166
	1100 0000	1010 1000	0000 0001	1010 0110
<b>Masque</b>	255	255	255	128
	1111 1111	1111 1111	1111 1111	1000 0000
<b>Résultat du ET</b>	<b>1100 0000</b>	<b>1010 1000</b>	<b>0000 0001</b>	<b>1000 0000</b>
Soit l'adresse réseau	<b>192</b>	<b>168</b>	<b>1</b>	<b>128</b>

#### Notation CIDR :

Il existe une notation qui permet d'écrire à la fois l'adresse IP et le masque. Il suffit d'indiquer à la fin de l'adresse IP le nombre de bits à 1 contenus dans le masque : notation CIDR.

Exemple :

- L'adresse IP de la machine est la suivante : 192.168.1.166
- Le masque est le suivant : 255.255.255.128 (soit **25 bits à 1**)
- La notation CIDR est la suivante : 192.168.1.166 / **25**

### 3.4) Adresse logique/physique, et table ARP

Il existe deux types d'adresse :

- L'adresse dite logique : adresse IP (Internet Protocol)
- L'adresse dite physique : adresse MAC (Media Access Control)

#### 3.4.1) Adresse physique : adresse MAC

Tous les équipements réseau ont une adresse MAC. Cette adresse est non modifiable et correspond au numéro d'identification de la carte réseau.

L'adresse physique est composée de 48 bits soit 6 octets. Les 3 premiers octets sont attribués par l'IEEE (Institute of Electrical and Electronics Engineers) à chaque constructeur de matériel réseau et les 3 autres sont définis par le constructeur.

Adresse MAC					
8bits	8bits	8bits	8bits	8bits	8bits
00	04	20	1A	B9	87
ID constructeur			Affectés par le constructeur		

**Une adresse MAC est un nombre de 48 bits représenté en hexadécimal par 6 octets.**

Exemple d'adresse MAC : **00 : 04 : 20 : 1A : B9 : 87**



#### 3.4.2) Table ARP

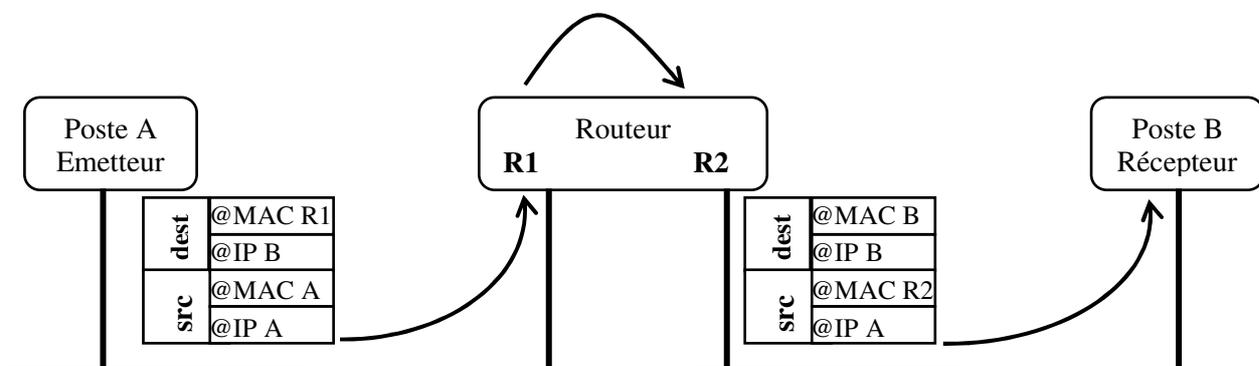
L'adresse MAC est une adresse de bas niveau, qui permet d'identifier une machine avec certitude. Cependant les applications réseau évitent d'utiliser directement cette adresse, car si on change la carte réseau d'une machine, la machine ne sera plus reconnue. C'est pourquoi, les applications travaillent avec une adresse logique (adresse IP) et maintiennent à jour une **table de correspondance** entre adresse physique (MAC) et adresse logique (IP) : **c'est la table ARP**.

#### 3.4.3) Adresse logique : adresse ip

L'adresse IP est, quand à elle, affectée à chaque machine :

- soit manuellement par l'administrateur réseau. On parle d'adressage statique.
- soit automatiquement. C'est le serveur **DHCP** (Dynamic Host Configuration Protocol) qui assigne l'adresse IP de son choix (adresse disponible). On parle alors d'adressage dynamique.

#### 3.4.4) Exemple d'adressage via un routeur



### 3.5) Adresses publiques / adresses privées

**Les adresses IP privées** sont des adresses IP de classe A, B et C. Elles peuvent être utilisées uniquement dans un réseau local (LAN). Elles ne sont pas utilisées (routées) sur Internet. En IPv4 :

- Les adresses privées de la **classe A** : **10.0.0.0 à 10.255.255.255** (10.0.0.0/8, soit  $2^{(32-8)}$ -2 possibles)
- Les adresses privées de la **classe B** : **172.16.0.0 à 172.31.255.255** (172.16.0.0/12, soit  $2^{(32-12)}$ -2 possibles)
- Les adresses privées de la **classe C** : **192.168.1.0 à 192.168.255.255** (192.168.1.0/16, soit  $2^{(32-16)}$ -2 possibles)

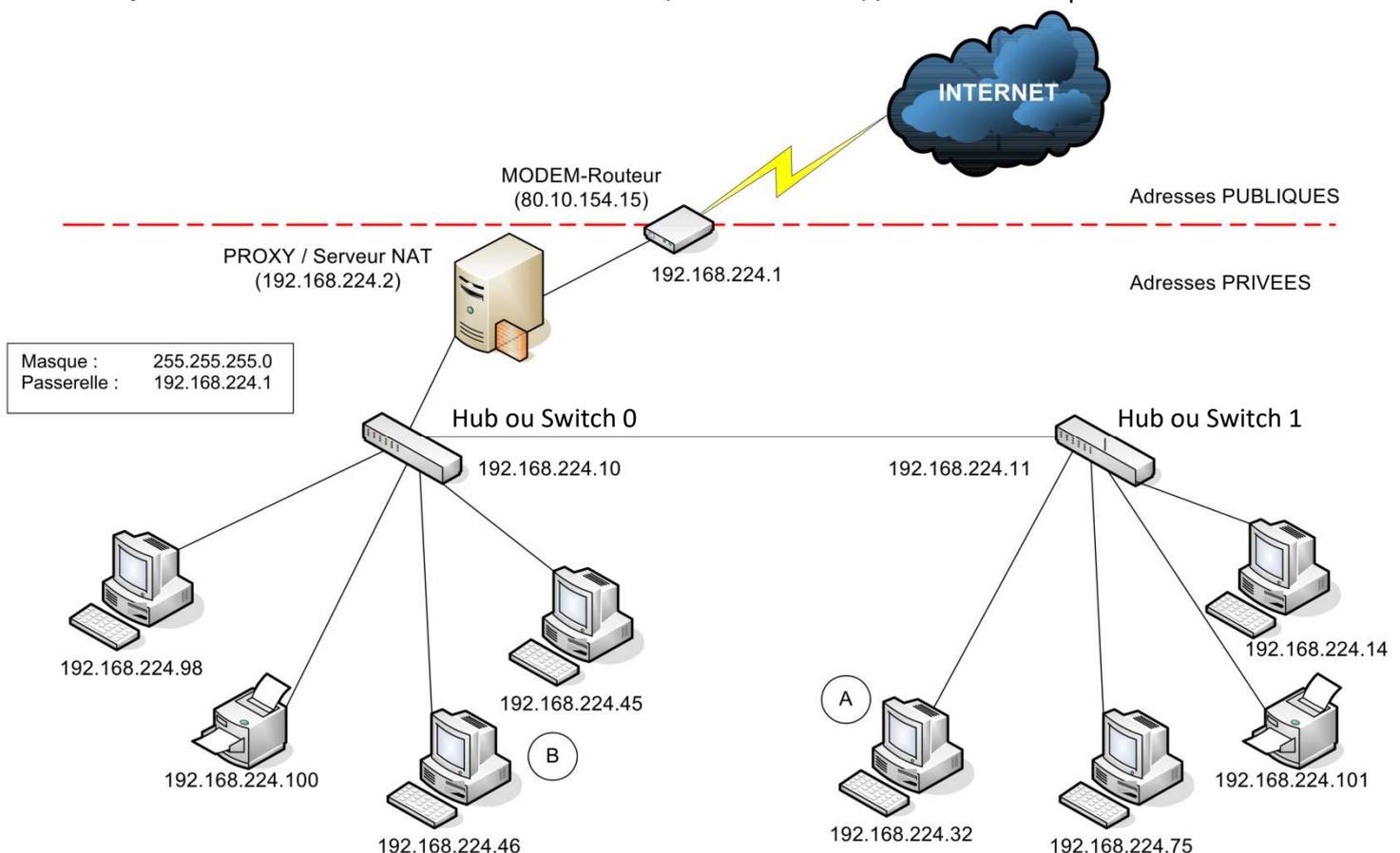
La classification est très différente en IPv6 et plus complexe (offrant plus de possibilités).

**Les adresses IP publiques** ne sont pas utilisées dans un réseau local mais uniquement sur Internet. Le routeur (qui est la box Internet chez les particuliers) dispose d'une adresse IP publique ce qui le rend visible sur internet, ainsi qu'une adresse locale pour communiquer avec toutes les machines connectées en local au routeur.

Le routeur sert de **passerelle** entre le réseau public et le réseau local (une seule passerelle max par réseau local). Les adresses IP publiques sont attribuées au routeur par un organisme (L'IANA) auprès de qui il faut s'enregistrer. C'est le fournisseur d'accès Internet qui s'en charge chez les particuliers.

Les adresses IP sont par défaut des **IP dynamiques** (elle change à chaque reconnexion), attribuées par le DHCP (routeur pour un réseau local, ou serveur DHCP du fournisseur d'accès pour les adresses publiques). Or il peut être utile d'avoir une **IP fixe** (si l'ordinateur est utilisé comme serveur par exemple). Pour cela il faut soit configurer le routeur pour avoir une IP fixe, soit passer par un serveur particulier capable de délivrer des IP fixes.

**Exemple** : Une seule adresse est visible sur l'internet, celle du routeur, jouant le rôle de passerelle.



## 4) Constituants d'un réseau sur Internet

### Répéteur

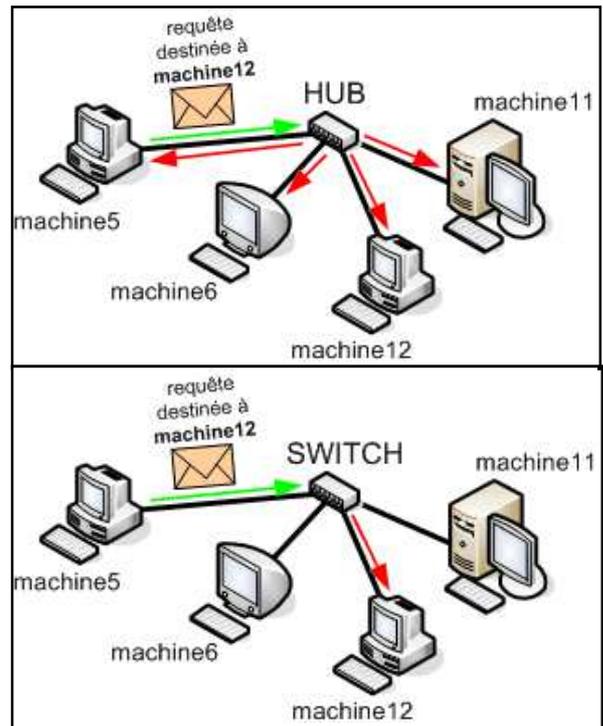
Equipé d'un port d'entrée et d'un port de sortie, il régénère les signaux réseau et les resynchronisent au niveau du bit pour leur permettre de voyager sur de plus longues distances dans le média (on place un répéteur après 100m de câble).

### Hub, ou répéteur, ou concentrateur :

C'est un répéteur multipoint permettant la connexion de plusieurs appareils sur une même ligne de communication. Il redistribue l'information à toutes les machines connectées. La machine destinataire se reconnaît et peut ainsi traiter la requête. Les autres machines, qui ne sont pas concernées, ignorent simplement la requête. Il est de moins en moins utilisé, au profit du switch.

### Switch, ou commutateur :

C'est un répéteur multipoint « intelligent ». Si l'information passe par un switch, celui-ci est capable d'identifier le destinataire de la requête. Il peut ainsi la relayer à la machine concernée uniquement.



**Routeur :** transmet l'information en déterminant la route la plus efficace.



Pour réaliser le routage, un routeur dispose d'une **table de routage**, lui permettant de définir les passerelles associées à chaque sous-réseau connecté au routeur.

Si le destinataire du message n'est pas directement dans un des sous-réseaux connecté, le routeur envoie par défaut celui-ci vers un autre routeur et ainsi de suite. Il y a donc systématiquement, dans la table de routage d'un routeur, un "chemin" par défaut correspondant à l'adresse d'un autre routeur. C'est la **passerelle par défaut**.

**Serveur PROXY :** solution plus sophistiquée qu'un routeur d'accès partagé à l'Internet qui offre également une sécurité renforcée du fait de l'utilisation de méthodes de filtrage complexes. Il peut mettre en cache les sites les plus fréquemment visités pour optimiser les performances et réduire la quantité d'accès à l'Internet.

**Serveurs Internet :** Identifiés par une adresse unique, ils proposent un service (consultation de pages web, téléchargement ftp, chat, envoi de courrier, ...). Ils sont disséminés partout dans le monde.

Les communications dans un réseau s'articulent autour de **demandes** ou de **requêtes**. A l'origine, il y a toujours une requête de l'un à l'autre. Par exemple :

- une machine peut demander à une autre de lui envoyer des informations ou des données.
- elle peut aussi demander à une imprimante d'imprimer un travail.
- elle peut encore demander à un routeur de transmettre des informations à une troisième machine.

Dans tous les cas cités ci-dessus, il y a un **client** (qui va commander un service ou une requête quelconque) et un **serveur** (qui va rendre le service ou accéder à la requête). Pour cette raison, on dit que la communication est basée sur une **architecture client/serveur**.

Une deuxième forme d'architecture, appelée point à point ou **peer-to-peer**, littéralement client à client, implique que les deux nœuds en communication endossent chacun leur tour le rôle du serveur et le rôle du client.

**Serveur DNS** (« *Domain Name System* », ou « système de noms de domaine ») :

Il établit la correspondance entre une adresse IP et un nom de domaine. Le service DNS est souvent fourni par le fournisseur d'accès. S'il ne connaît pas la réponse, il transmet la requête à un autre serveur.

Le Domain Name System (ou **DNS**, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations, notamment en adresses IP de la machine portant ce nom. Ce service a aussi été créé pour simplifier les recherches sur internet puisqu'un nom (ex: wikipedia.org) est plus facile à retenir qu'une série de chiffre qui constitue une adresse IP (ex: 2620:0:862:ed1a::1).

### Principe d'une requête DNS

