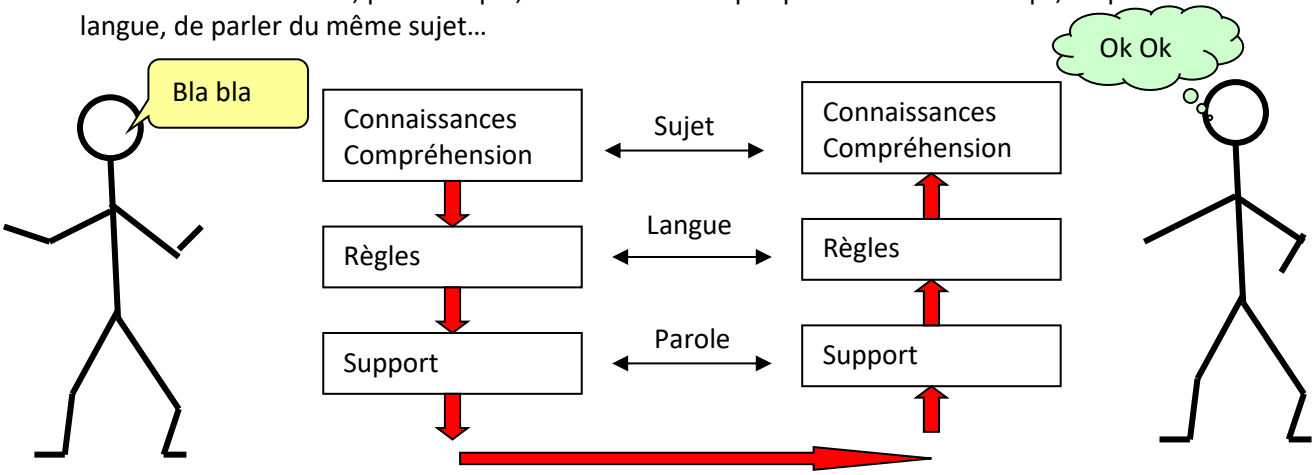
1 Introduction : l'ordinateur, un système communicant

L'unité centrale d'un ordinateur a besoin de **communiquer** avec l'homme ainsi qu'avec différents périphériques et réseaux informatiques (internet, intranet…). Pour cela on utilise en fonction du besoin différents supports et protocoles de communication. On rencontre les vocables suivants : RS232, USB, Bluetooth, ADSL, TCP/IP, HTML, Fibre optique, bauds, L.A.N., Internet, Modbus, V24, liaison full Duplex, IP V6, …. Etc…

2 La communication

2.1 Principe

Pour qu'une communication d'informations fonctionne il faut établir quelques règles.
Dans une conversation, par exemple, il convient de ne pas parler en même temps, de parler la même langue, de parler du même sujet…

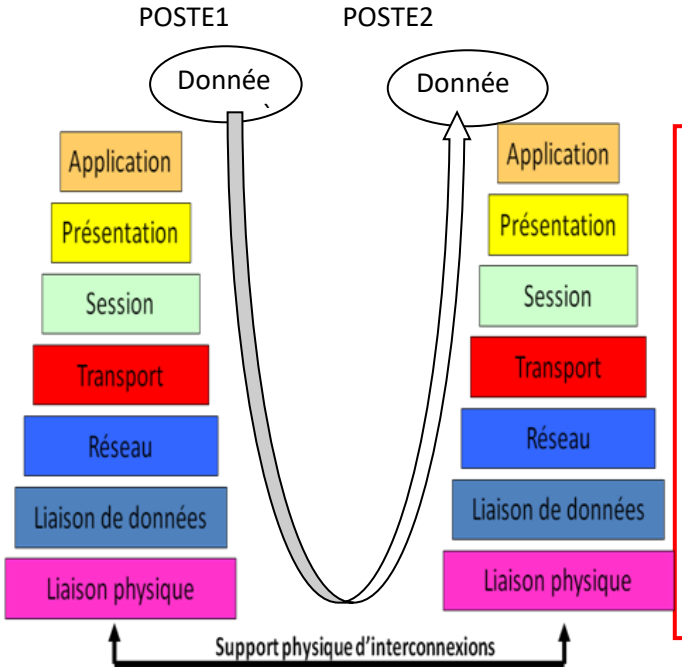


Les principes ainsi définis constituent un ensemble :

- de couches (connaissance, règles, support),
- de protocoles (sujet, langue, parole).

2.2 Normalisations des couches et des protocoles :

Le modèle OSI (open system interconnexion) : il définit en 7 couches les différentes étapes pour établir un transfert de données entre un émetteur et récepteur.

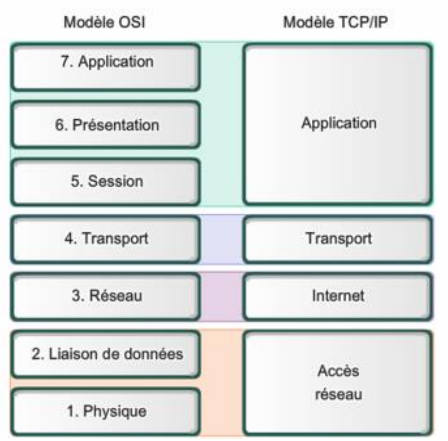


Couches	
7	7 : Partie logicielle, environnement nécessaire aux traitements et transmission des données. DHCP · DNS · FTP · HTTP · POP3 · SMTP · SSH Telnet VoIP Ici on parle de données. (PDU)
6	6 : Codage informatique de l'information (ascii etc…), taille, sens d'envoi, cryptage.
5	5 : Déclaration du principe de communication. Gestion des ouvertures/fermetures de sessions entre hôtes distants NetBios, ... Ici on parle toujours de données. (PDU)
4	4 : Corrige les erreurs de transmission et vérifie le bon acheminement des informations. Gestion de la tr TCP · UDP Ici on parle de segments (TCP/UDP) et de datagrammes. (PDU) transmission de segments.
3	3 : Identification des ordinateurs (MAC) et points de connexion du réseau et détermine par où les informations doivent être dirigées. (Routage) ICMP · IPv4 · IPv6 Ici on parle de paquets. (PDU)
2	2 : Les données numériques sont traduites en signal. Les bits de données sont organisés en trames. Un en-tête est créé dans lequel on peut identifier l'émetteur et le destinataire par leur adresse physique Ethernet · MAC · ARP · PPP · Wi-Fi · (Cartes réseau · switch - hub)
1	1 : Conversion des données informatiques en données électriques (codage électrique : Manchester, NRZ, NRZI…)

Principe de l'encapsulation de données.

Donnée à transmettre	Données	Éléments d'encapsulation
7. Application	Données	Adresse de nœud
6. Présentation	Données	Information de codage
5. Session	Données	Informations de communication
4. Transport	Données	Entête somme de contrôle
3. Réseau	Données	Taille du paquet ou de la séquence
2. Liaison	Données	Somme de contrôle de trame / fin de message
1. Physique	flux de bits	Le paquet est émis : séquence de bits

Le modèle TCP/IP : appelé également modèle Internet, il a été établi en 1976 donc avant le modèle OSI établi lui en 1984. Il présente aussi une approche modulaire (utilisation de couches) mais en contient uniquement quatre. Il fonctionne également sur le principe de l'encapsulation des données. Les 4 couches sont :



3 Les réseaux

On appelle ***RESEAU*** (network) un ensemble d'ordinateurs et de périphériques connectés les uns aux autres.
Il est caractérisé par la distance, le médium (support) et la bande passante (capacité)

3.1 Utilité d'un réseau

- Partage des ressources

Les réseaux permettent de rendre accessible un certain nombre de ressources (logiciels, bases de données, matériel...) indépendamment de la localisation géographique des utilisateurs.

- Augmentation de la fiabilité et des performances

- Réduction des coûts

Les ordinateurs individuels coûtent bien moins cher que les gros systèmes centralisés (1000 fois moins environ), et ce pour une baisse des performances d'à peine un facteur 10.

- Accès à l'information et au courrier

Avec les réseaux et en particulier Internet, il est très facile de s'informer sur toute sorte de sujets très rapidement.

3.2 Que signifie réseau

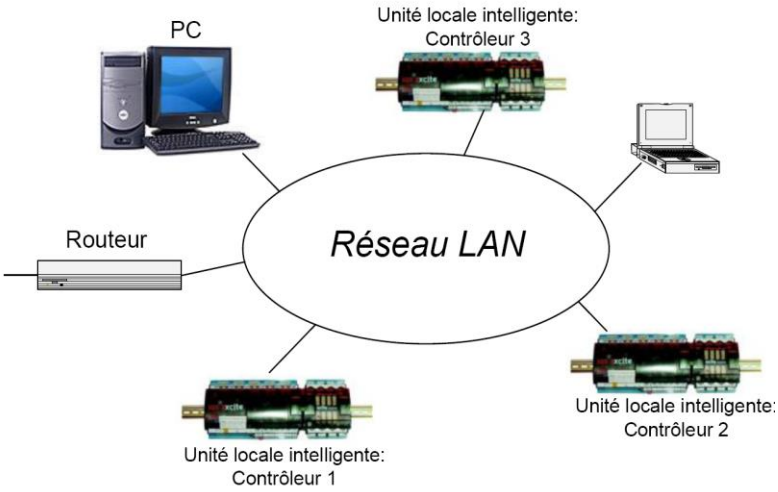
Le terme réseau en fonction de son contexte peut désigner plusieurs choses.
1 Il peut désigner l'ensemble des machines, ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui 'est le cas lorsque l'on parle de Internet.

2 Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées. C'est le cas lorsque l'on dit que les machines d'un site (sur un réseau local) sont sur un réseau Ethernet, Token Ring, réseau en étoile, réseau en bus.

3 Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent. On peut parler de réseau TCP/IP, NetBus (protocole Microsoft) DecNet (protocole DEC), IPX/SPX,...

3.3 Différents types de réseaux

Il existe différents types de réseaux ; suivant la localisation, les distances entre les systèmes informatiques et les débits maximum, on peut distinguer trois types de réseaux.



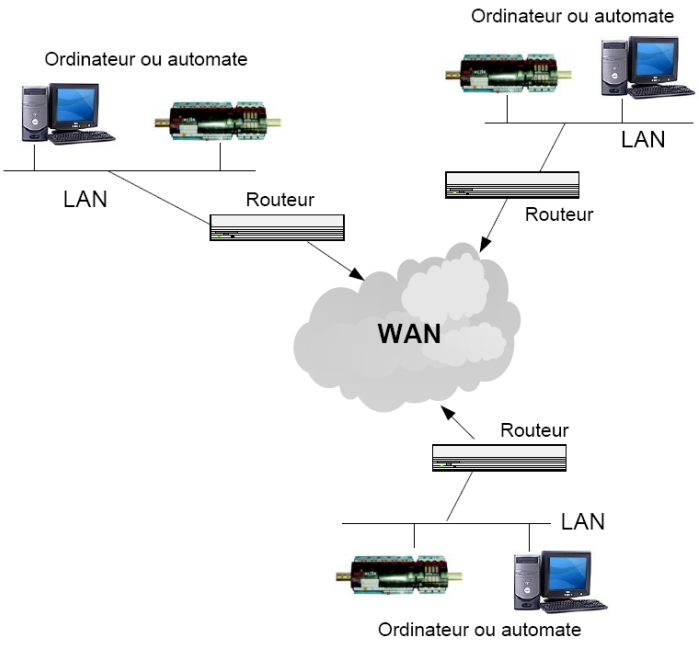
- BUS

Les bus que l'on trouve dans un ordinateur pour relier ses différents composants peuvent être considérés comme des réseaux dédiés à des tâches très spécifiques. (<1m)

- **Les réseaux locaux ou LAN** (Local Area Network) qui correspondent par leur taille aux réseaux intra-entreprise et qui permettent l'échange de données informatiques ou le partage de ressources (Ethernet, Token ring, ATM).

- Les *réseaux métropolitains* ou MAN (Metropolitain Area Network)

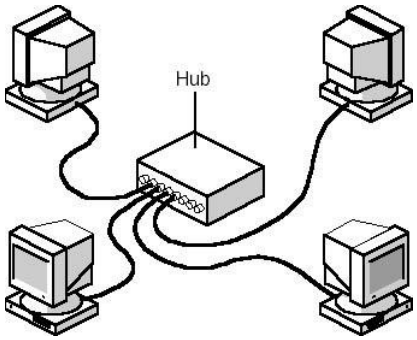
  - **Les *réseaux longues distances* ou WAN** (**W**ide **A**rea **N**etwork), généralement publics (Renater), et qui assurent la transmission des données numériques sur des distances à l'échelle d'un pays. Le support utilisé peut être terrestre (réseau maillé de type téléphonique ou ligne spécialisée) ou hertzien (transmission par satellite). Types de réseaux **Wan** : ADSL Dans une grande entreprise, un réseau est généralement une combinaison plus ou moins complexe de **Lan** et de **Wan.**

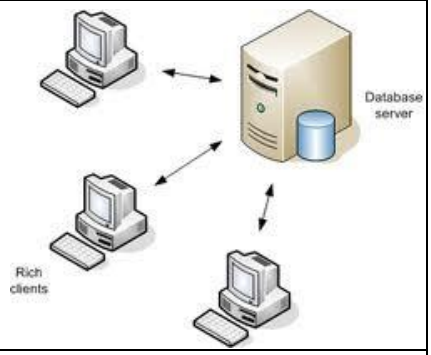


3.4 Spécifications d'un réseau ou architecture :

Les spécifications d'un réseau regroupent l'ensemble des éléments mis en œuvre pour permettre l'échange des informations. Ces spécifications comportent :
- la topologie du réseau
- le type de câblage ou de support physique utilisé
- les éléments d'interconnexion
- les machines connectées
- le modèle et sa pile de protocoles
- les systèmes d'exploitation ou OS (Operating System, ex : Windows seven) ainsi que les applications informatiques (messageries par ex) utilisés

On distingue essentiellement trois types d'architectures:

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. On parle alors de partage de fichiers ou de ressources. Ce type d'architecture ne s'utilise que pour les réseaux de type LAN avec peu d'abonnés (<qques dizaines)	
Avantages	
Très facile à mettre en œuvre	
Inconvénients	
Sécurité très faible Aucune machine ne gère réellement le réseau	

Architecture CLIENT-SERVEUR	
deux types de machines : ***Les serveurs*** : machines dédiées à des tâches spécifiques. On trouvera entre autres : • un serveur de domaine : gestion des personnes et des postes connectés • 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	Inconvénients
Le poste client peut être indifférencié. C'est à dire que quelle que soit la machine utilisée, l'utilisateur retrouve immédiatement la même interface, les ressources présentées de la même façon,... La centralisation des données offre une plus grande sécurité. Serveurs toujours en fonctionnement et données toujours disponibles	La décentralisation entraîne une augmentation du trafic sur le réseau et nécessite une bande passante importante. La mise en œuvre demande de bonnes connaissances pour bien administrer un tel réseau. Ce type d'architecture s'utilise pour les réseaux de type LAN comportant généralement un nombre assez élevé d'abonnés (lycée par exemple).

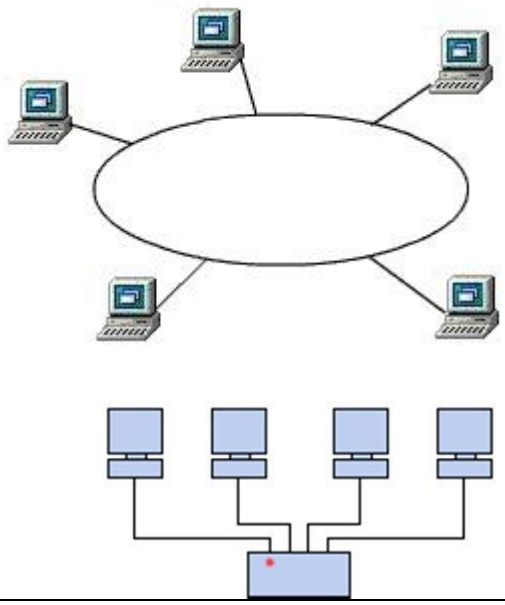
Architecture INTERNET

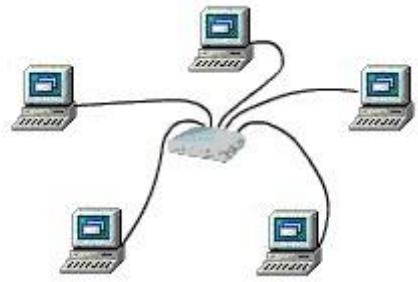
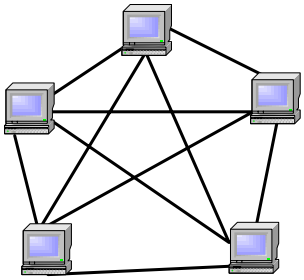
Appelé « réseau des réseaux », mondialement répandu. Il permet de mettre en relation des machines appartenant à des réseaux distincts au travers d'une « toile » ou « web » (topologie de maille).

Il est maintenant possible de réaliser un réseau privé utilisant l'architecture Internet, et qui soit efficace et souple. On parle alors d'« intranet ».

Avantages	Inconvénients
grande diffusion d'informations en rendant accessible au public des services comme le courrier électronique et le World Wide Web. Sécurité.	Le fait d'interconnecter les réseaux demande une supervision importante de l'ensemble et une grande compétence technique dans la gestion des réseaux.

3.5 Topologie de réseaux :

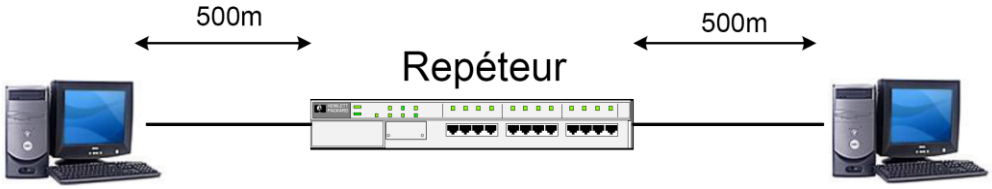
Topologie en BUS	
	Un seul câble relie toutes les machines. C'est le cas des réseaux Ethernet "10Base2" aussi appelé thinnet qui utilisent un câble coaxial fin (thin) raccordé à une carte réseau de chaque PC par un raccord en 'T'. Toutes les transmissions se font donc par un seul lien sur lequel un seul ordinateur a le droit d'émettre des données à la fois. L'avantage de ce type de réseau est sa simplicité. A part les cartes réseau, il n'est pas nécessaire d'utiliser d'autres équipements. L'inconvénient est que ce type de liaison est assez fragile car tout le réseau est affecté dès qu'une connexion quelconque est défectueuse.
Topologie en ANNEAU	
	Le " token ring " est un système inventé et utilisé par IBM. Le câble qui relie les ordinateurs forme une boucle fermée, un anneau. Des informations (le jeton - token) y circulent pour désigner l'ordinateur qui a le droit d'émettre. Les ordinateurs s'emparent du jeton où le passe au suivant selon qu'ils ont des données à transmettre ou qu'ils peuvent passer leur tour. Cette organisation permet d'éviter les collisions. Il permet des transferts allant jusqu'à 16 Mbits par seconde. L'inconvénient de ce type de réseau est qu'il n'est pratiquement plus employé que par IBM et que les équipements Token ring sont assez coûteux En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.
Topologie en ETOILE	

	Au lieu d'avoir comme dans les deux configurations précédentes un câble qui passe d'un ordinateur à l'autre, chaque machine est connectée à un concentrateur (HUB) ou un commutateur (SWITCH) situé au centre de "l'étoile". S'il y a une interruption de la connexion vers une machine, celle-ci sera la seule à être déconnectée. Le reste du réseau continue de fonctionner normalement.
Topologie maillé	
	Dans le maillage régulier l'interconnexion est totale ce qui assure une fiabilité optimale du réseau, par contre c'est une solution coûteuse en câblage physique. Si on allège le plan de câblage, le maillage devient irrégulier et la fiabilité peut rester élevée.

4. Les Composants actifs d'un réseau

4.1. Répéteur

Un ***répéteur*** reçoit des informations et les retransmets en régénérant un signal. Un répéteur permet de connecter 2 segments Ethernet dans un LAN.



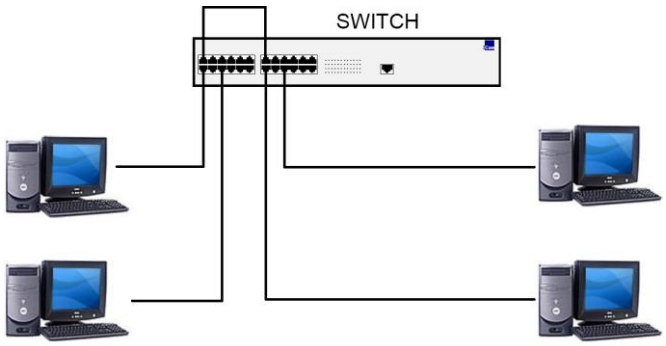
Un réseau 10Base T peut utiliser des « ***HUB***s » comme répéteurs.

4.2. HUB

Un Hub récupère les trames Ethernet en provenance d'un port et les renvoie vers tous les autres ports. Toutes les trames en provenance d'une interface Ethernet sont envoyées à toutes les autres interfaces présentes sur ce HUB. Ainsi on est 'sur' que le destinataire recevra l'information. Inconvénients : toutes les interfaces pour lesquelles la trame n'est pas destinée la recevront également. Cela génère beaucoup de trafic inutile sur le réseau, il y a risque de saturation.

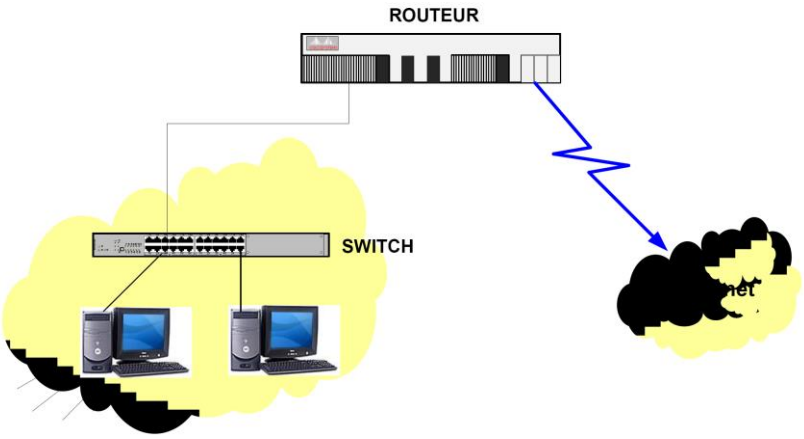
4.3. Switch

Alors que les Hubs ne font que transférer, de façon aveugle, les trames à travers le réseau, les switchs sont capables de connaître la destination en consultant dans chaque trame l'adresse MAC de l'expéditeur et du destinataire. En conservant la trace de ces adresses MAC dans sa table d'adresse, un switch est capable de transférer exactement la trame sur le port où est raccordé le destinataire (sauf les trames de Broadcasts).



Nota : Le broadcast est un terme anglais définissant une diffusion de données à un ensemble de machines connectées à un réseau. En français on utilise le terme diffusion

4.4. Routeur



C'est une passerelle entre le LAN (réseau local) et un autre réseau (Internet par exemple). Ils sont employés pour relier 2 réseaux ensemble et diriger le trafic des réseaux basés sur les adresses IP. Beaucoup de routeurs sont employés pour créer Internet.
Le routeur contient une base de données appelée « Routing Table » qui détient des chemins d'accès aux différents réseaux. Les routeurs sont en général utilisés au niveau réseau de l'Entreprise, pour relier différentes unités ou différents sites. Ils sont parfois associés à des fonctions de sécurité de type pare-feu « (Firewall) » pour filtrer les accès distants. Un routeur doit être configuré pour pouvoir connaître où router les messages. Les mécanismes de routage sont basés sur l'adresse IP. Les stations sont regroupées sur un même sous-réseau selon leurs adresses IP et leur masque de sous-réseau. Chaque message adressé à un réseau distant sera transmis au routeur qui assurera le routage vers la bonne destination

4.5 Carte Réseau

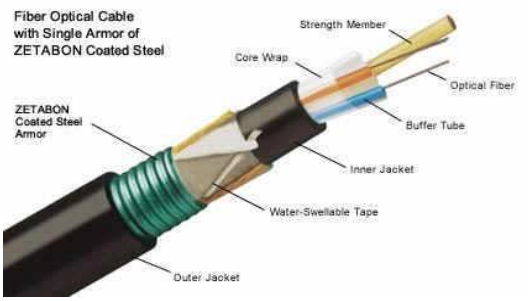
La **carte réseau** (appelée *Network Interface Card* en anglais et notée **NIC**) constitue l'interface entre l'ordinateur et le câble du réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau.
La carte réseau possède généralement deux témoins lumineux (LEDs) :
La LED verte correspond à l'alimentation de la carte ;
La LED orange (10 Mb/s) ou rouge (100 Mb/s) indique une activité du réseau (envoi ou réception de données).
Pour préparer les données à envoyer, la carte réseau utilise un **transceiver** qui transforme les données parallèles en données séries. Chaque carte dispose d'une adresse unique, appelée **adresse MAC(adresse physique)**, affectée par le constructeur de la carte, ce qui lui permet d'être identifiée de façon unique dans le monde parmi toutes les autres cartes réseau.

5 Supports physiques de transmission et câblage

Pour relier les diverses entités d'un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés.
Une de ces possibilités est l'utilisation de câbles. Il existe de nombreux types de câbles, mais on distingue généralement :

- Le câble de type coaxial : quasiment abandonné.

- La double paire torsadée : technique la plus répandue.



-
- •La fibre optique : utilisée pour les très hauts débits. Longues distances, insensible à l'environnement de déploiement et haute capacité (>100 Mbit/s)

En plus de ses capacités de transmission, ses grands avantages sont son immunité aux interférences électromagnétiques et sa plus grande difficulté d'écoute, contrairement aux supports électriques, ce qui la rend également attrayante dans les contextes où la confidentialité est requise.

D'autres techniques de liaison sont disponibles telles que :

- CPL (courants Porteurs en Ligne) utilisant des lignes d'alimentation électriques : techniques réservée le plus souvent aux réseaux domestiques (« indoor »).
- Par ondes électromagnétiques : liaisons RF (Radio Frequency) permettant de réaliser des réseaux locaux sans fils ou WLAN (Wireless Local Area Network). On rencontre la technique :
  - Wi-Fi (Wireless Fidelity) : ses protocoles sont régis par la norme IEEE 802.11 et ses déclinaisons.
  - Bluetooth avec son service RFCOMM

  Très sensible à l'environnement : affaiblissement, évanouissement, multi-chemin, interférences au niveau physique et bande passante faible

5.1 La paire torsadée non blindée UTP (Unshielded Twisted Pair)

C'est le type de paire torsadée le plus utilisé pour les réseaux locaux.

Longueur maximale d'un segment : 100 mètres
Composition : 2 fils de cuivre isolés

Les normes UTP comportent cinq catégories de câbles parmi lesquelles on retient :

Catégorie 1 : Câble téléphonique traditionnel (transfert de voix mais pas de données)
Catégorie 4 : 16 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre
Catégorie 5 : 100 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre
Catégorie 5e : 1000 Mbit/s maximum

L'inconvénient du câble UTP réside dans sa sensibilité aux interférences (signaux d'une ligne se mélangeant à ceux d'une autre ligne) conduisant à la nécessité d'utiliser des câbles blindés.

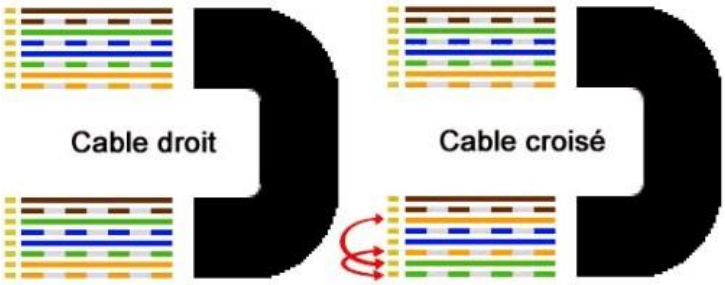
5.2 La paire torsadée blindée (STP)

Le câble STP (Shielded Twisted Pair) utilise une gaine de cuivre de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP. Il contient une enveloppe de protection entre les paires et autour des paires. Dans le câble STP, les fils de cuivre d'une paire sont eux-mêmes torsadés, ce qui fournit au câble STP un excellent blindage, c'est-à-dire une meilleure protection contre les interférences). D'autre part il permet une transmission plus rapide et sur une plus longue distance.

5.3Connecteur RJ45

Dans un câble RJ-45 croisé on permute deux à deux les paires Transmission de données (TX) et Réception de données (RX), c'est-à-dire les conducteurs Blanc-Vert (TX+) et Blanc-Orange (RX+), Vert (TX-) et Orange (RX-).

Le câble croisé est utilisé pour connecter deux appareils identiques ensemble et ainsi s'affranchir d'un *hub* ou d'un *switch*



Le câble droit est utilisé pour connecter l'appareil à un *hub* ou un *switch*.

Remarque : Certains appareils et certaines cartes réseau sont capables d'analyser si le câble est croisé ou non (natif pour les cartes gigabit).

6. TCP/IP

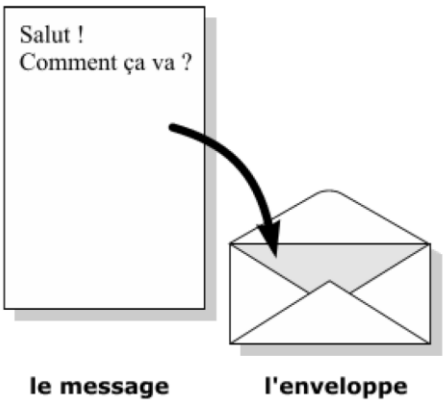
TCP/IP est un **protocole**, c'est à dire des **règles de communication**.

- TCP signifie Transmission Control Protocol : littéralement Protocole de Contrôle de Transmission *(couche)*
- ***IP*** signifie ***Internet Protocol*** : littéralement "le protocole d'Internet". C'est le principal protocole utilisé sur Internet (couche 3). ***{que nous verrons sur l'explication du Modèle O.S.I.}.***

6.1. IP

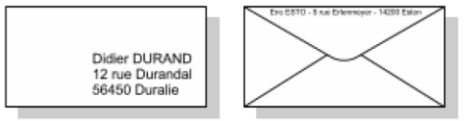
Internet signifie ***Inter-networks***, c'est à dire "entre réseaux". Internet est l'*interconnexion des réseaux* de la planète. Le protocole **IP** permet aux ordinateurs reliés à ces réseaux de dialoguer entre eux.
C'est un service
- **Non Fiable** La Fiabilité assurée par les protocoles supérieurs
- **Non Connecté** : pas d'information d'état de la connexion ; iIndépendance des paquets

Faisons un parallèle avec la poste.
Quand vous voulez envoyer une lettre par la poste:



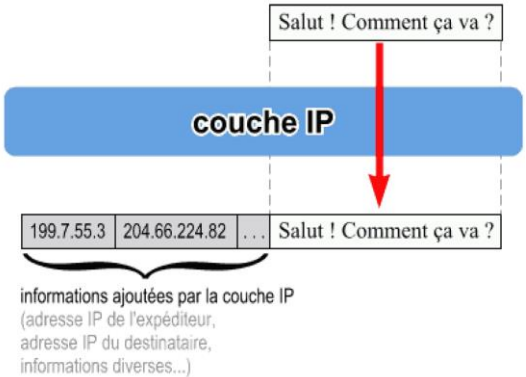
- vous placez votre lettre dans une **enveloppe,**
- sur le recto vous inscrivez l'**adresse du destinataire,**
- au dos, vous écrivez l'**adresse de l'expéditeur** (la votre).

Ce sont des règles utilisées par tout le monde. C'est un **protocole**.
Sur Internet, c'est à peu près la même chose: chaque message (chaque petit paquet de données) est enveloppé par IP qui y ajoute différentes informations:



recto : adresse du destinataire
verso : adresse de l'expéditeur

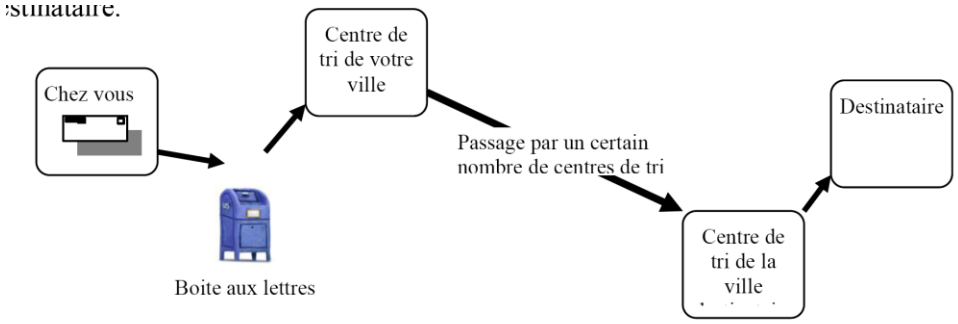
- l'adresse de l'expéditeur (vôtre adresse IP),
- l'adresse IP du destinataire,
- différentes données supplémentaires (qui permettent de bien contrôler l'acheminement du message).



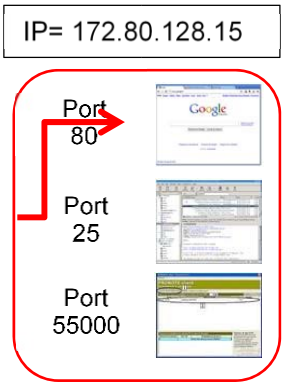
L'**adresse IP** est une adresse **unique** attribuée à chaque ordinateur sur Internet (c'est-à-dire qu'il n'existe pas sur Internet deux ordinateurs ayant la même adresse IP). De même, l'adresse postale (nom, prénom, rue, numéro, code postal et ville) permet d'identifier de manière unique un destinataire. Tout comme avec l'adresse postale, il faut connaître au préalable l'adresse IP de l'ordinateur avec lequel vous voulez communiquer. L'adresse IP se présente le plus souvent sous forme de 4 nombres (entre 0 et 255) séparés par des points. Par exemple: 204.35.129.3

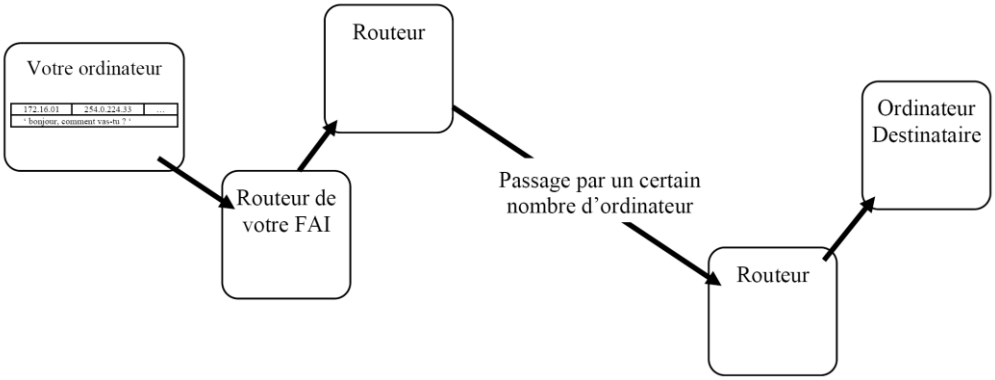
6.2 Le routage IP

Pour envoyer votre lettre, vous la postez dans la boîte-aux-lettres la plus proche. Ce courrier est relevé, envoyé au centre de tri de votre ville, puis transmis à d'autres centres de tri jusqu'à atteindre le destinataire.



C'est la même chose sur Internet !
Vous déposez le paquet IP sur l'ordinateur le plus proche (celui de votre fournisseur d'accès en général). Le paquet IP va transiter de routeur en routeur jusqu'à atteindre le destinataire.





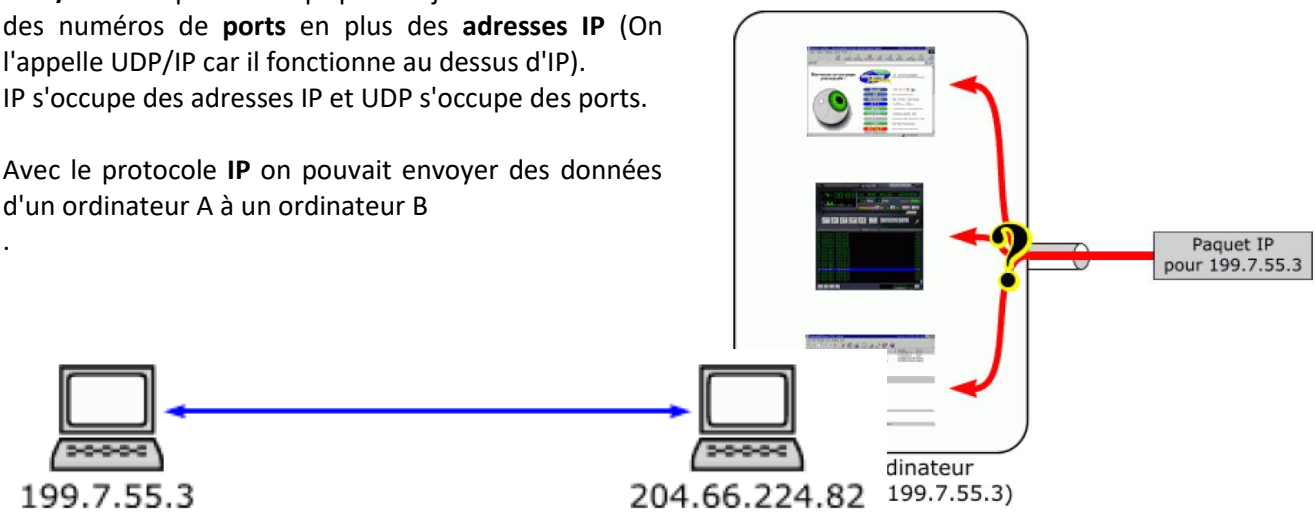
6.3. Les ports

Avec IP, nous avons de quoi envoyer et recevoir des paquets de données d'un ordinateur à l'autre. Imaginons maintenant que nous ayons plusieurs programmes qui fonctionnent en même temps sur le même ordinateur : un navigateur, un logiciel d'email et un logiciel pour écouter la radio sur Internet. Si l'ordinateur reçoit un paquet IP, comment savoir à quel logiciel donner ce paquet IP ?

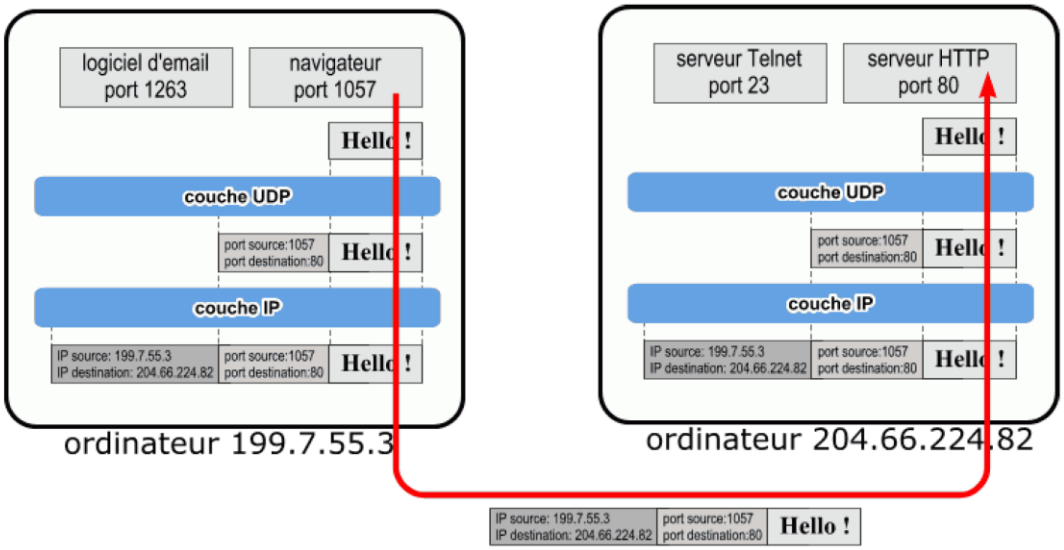
6.4 UDP (User Datagram Protocol)

UDP/IP est un protocole qui permet justement d'utiliser des numéros de **ports** en plus des **adresses IP** (On l'appelle UDP/IP car il fonctionne au dessus d'IP).
IP s'occupe des adresses IP et UDP s'occupe des ports.

Avec le protocole **IP** on pouvait envoyer des données d'un ordinateur A à un ordinateur B
.



Avec **UDP/IP**, on peut être plus précis : On envoie des données d'une **application x** sur l'**ordinateur A** vers une **application y** sur l'**ordinateur B**. Par exemple, votre navigateur peut envoyer un message à un serveur HTTP (un serveur Web):



Chaque couche (UDP et IP) va ajouter ses informations. Les informations de **IP**vont permettre d'acheminer le paquet à destination du bon **ordinateur**. Une fois arrivé à l'ordinateur en question, la couche **UDP** va délivrer le paquet au bon **logiciel** (ici au serveur HTTP), mais il ne garantit pas l'exactitude des informations qu'il remets à la couche application, mais cela permet d'accélérer les échanges.
L'émetteur ne reçoit aucune confirmation de réception.
Les deux logiciels se contentent d'émettre et de recevoir des données ("**Hello !**"). Les couches UDP et IP en dessous s'occupent de tout.

Ce couple (199.7.55.3:1057, 204.66.224.82:80) est appelé un **socket**. Un socket identifie de façon unique une communication entre deux logiciels. Parmi les usages les plus connus du mode sans connexion (UDP), notons:

- La résolution des noms ou la résolution inverse des adresses (DNS)
- La recherche d'une adresse IP dynamique (DHCP)
- La plupart des jeux en réseau.
- Le streaming (gros volumes d'informations tel que vidéo, chansons) où la perte d'information n'est pas dommageable.

6.5. TCP

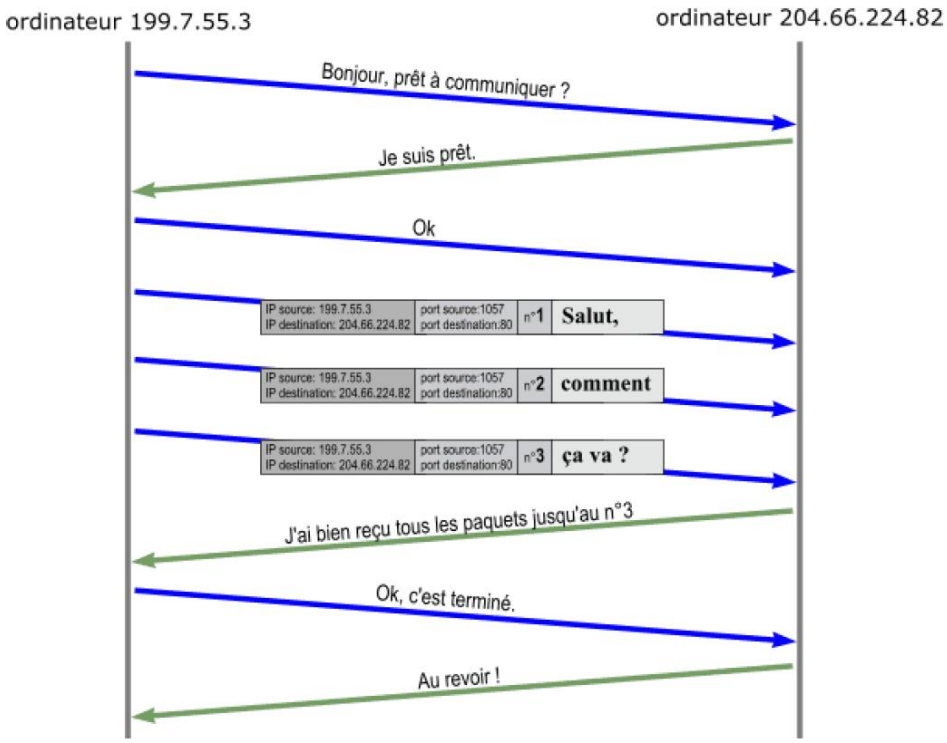
Bon... on peut maintenant faire communiquer 2 logiciels situés sur des ordinateurs différents. Mais il y a encore de petits problèmes:
Quand vous envoyez un paquet IP sur Internet, il passe par des dizaines d'ordinateurs. Et il arrive que des paquets IP se perdent ou arrivent en double exemplaire.

- Ça peut être gênant : imaginez un ordre de débit sur votre compte bancaire arrivant deux fois ou un ordre de crédit perdu !
- Même si le paquet arrive à destination, rien ne vous permet de savoir si le paquet est bien arrivé (aucun accusé de réception).
- **La taille des paquets IP est limitée** (environ 1500 octets). Comment faire pour envoyer le fichier qui fait 62000 octets ? C'est pour cela qu'a été conçu TCP.

TCP est capable:

- de faire tout ce que UDP sait faire (ports).
- de vérifier que le destinataire est prêt à recevoir les données.
- de **découper** les gros paquets de données en paquets plus petits pour que IP les accepte
- de **numéroter** les paquets, et à la réception de **vérifier** qu'ils sont tous bien arrivés, de **redemander** les paquets manquants et de les **réassembler** avant de les donner aux logiciels. Des accusés de réception sont envoyés pour prévenir l'expéditeur que les données sont bien arrivées. Il garantit que toutes les données sont acheminées. Mais les échanges se voient ralentis.

  Par exemple, pour envoyer le message "**Salut, comment ça va ?**", voilà ce que fait TCP (Chaque flèche représente 1 paquet IP):



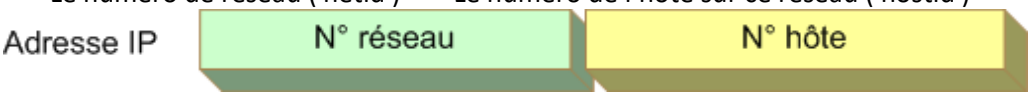
A l'arrivée, sur l'ordinateur 204.66.224.82, la couche TCP reconstitue le message "**Salut, comment ça va ?**" à partir des 3 paquets IP reçus et le donne au logiciel qui est sur le port 80.

7. Adresse IP

7.1 Constitution d'une adresse IP

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

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



La taille du *netid* dépend de **la classe d'adresse IP** utilisée. Il existe plusieurs classes d'adresses IP dédiées à des usages différents.

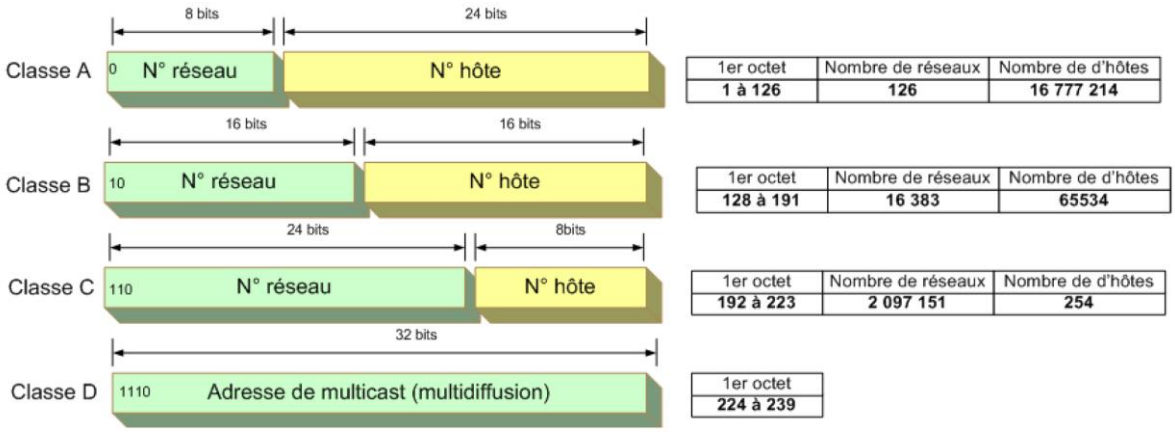
7. 2 Les classes d'adresses :

Il existe 3 classes d'adresses IP : x 0 ou 1

Classe A	0xxx xxxx	Octet 3	Octet 2	Octet 1
Classe B	10xx xxxx	Octet 3	Octet 2	Octet 1
Classe C	110x xxxx	Octet 3	Octet 2	Octet 1

Etendue de chaque classe :

Classe	***Première adresse***	***Dernière adresse***
A	0.0.0.1	127.255.255.254
B	128.0.0.1	191.255.255.254
C	192.0.0.1	223.255.255.254



Les classes d'adresses IP

Il y a quelques adresses que l'on ne peut attribuer à un hôte :

-l'adresse d'hôte = 0 (exemple : 192.168.1.0 dans la classe C) est réservée à l'identification du réseau.

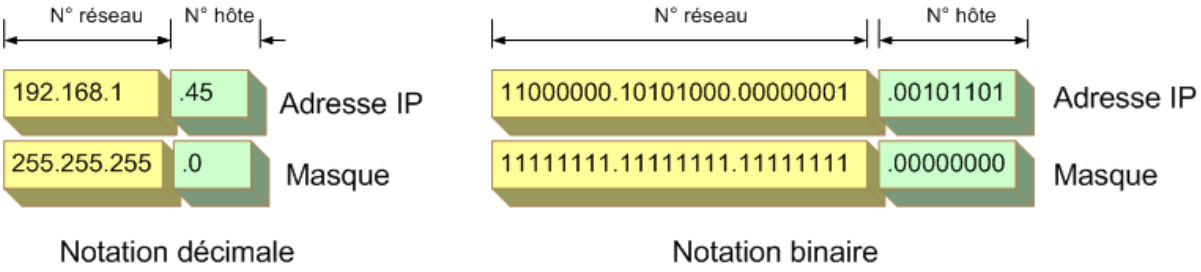
- l'adresse d'hôte avec tous ses bits à 1 (exemple : 192.168.1.255) cette adresse comprenant tous les hôtes du réseau 192.168.1.0. Par convention, cette adresse signifie que tous les hôtes du réseau 192.168.1.0 sont concernés (Adresse de broadcast IP).

nombre d'hôtes sur ce réseau sera petit.

7.3 Le masque de sous réseau :

Le ***masque de sous réseau*** est un ensemble de 4 octets destiné à isoler :

- soit ***l'adresse de réseau*** en effectuant **un ET logique** bit à bit entre **l'adresse IP** et le **masque**
- soit ***l'adresse de l'hôte*** en effectuant en ET logique bit à bit entre l'adresse IP et le complément **du masque.** Tous les bits à 1 du masque permettent de définir chaque bit correspondant de l'adresse IP comme un bit faisant partie du n° de réseau. Par opposition, tous les bits à 0 du masque permettent de définir chaque bit correspondant de l'adresse IP comme un bit faisant partie du n° d'hôte.

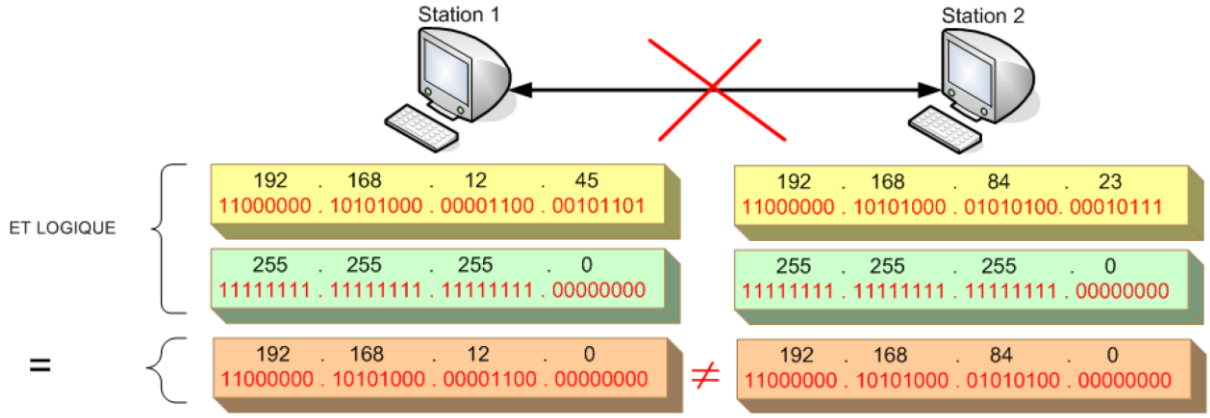


Le masque servant à faire la séparation en deux parties sur une adresse IP, il est donc indissociable de celle-ci. Une adresse seule ne voudra rien dire puisqu'on ne saura pas quelle est la partie réseau et quelle est la partie machine.

Les masques de sous réseau ont **par défaut** :

Classe	Masque par défaut	Nombre d'octets pour l'hôte
A	255.0.0.0	3
B	255.255.0.0	2
C	255.255.255.0	1

Exemple



Exemple d'application du masque

7.4 Le masque de sous réseau :

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255[2]	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0

7.5 Adresse IP particulière : adresse de diffusion (broadcast)

L'adresse de diffusion (autrement nommée « broadcast ») est utilisée pour envoyer un message à toutes les machines du réseau. Cette adresse ne peut pas être attribuée à un hôte.

L'adresse de broadcast d'un réseau à sa partie « host-ID » entièrement à 1 :

Exemple d'adresse IP de broadcast :

192 . 168 . 1 . 255

1100 0000 . 1010 1000 . 0000 0001 . 1111 1111

7.6 Les adresses privées

Les adresses IP privées représentent toutes les adresses IP de classe A, B et C que l'on peut utiliser dans un réseau local (LAN) c'est-à-dire dans le réseau de votre entreprise ou dans le réseau domestique. De plus, les adresses IP privées ne peuvent pas être utilisées sur internet (car elles ne peuvent pas être routées sur internet), les hôtes qui les utilisent sont visibles uniquement dans votre réseau local. Les classes A, B et C comprennent chacune une plage d'adresses IP privées à l'intérieur de la plage globale.

Plage d'adresses IPv4	Masque de réseau
10.0.0.0 - 10.255.255.255	10.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0

7.7 Les exceptions

- Le réseau **127.0.0.0** est réservé pour les tests de boucle locale avec notamment l'adresse **IP 127.0.0.1 qui est l'adresse « localhost » c'est-à-dire de boucle locale de votre PC.**

On peut ainsi vérifier que la pile TCP/IP d'une machine est opérationnelle en utilisant le programme ping pour le <<localhost>> ou ping 127.0.0.1.

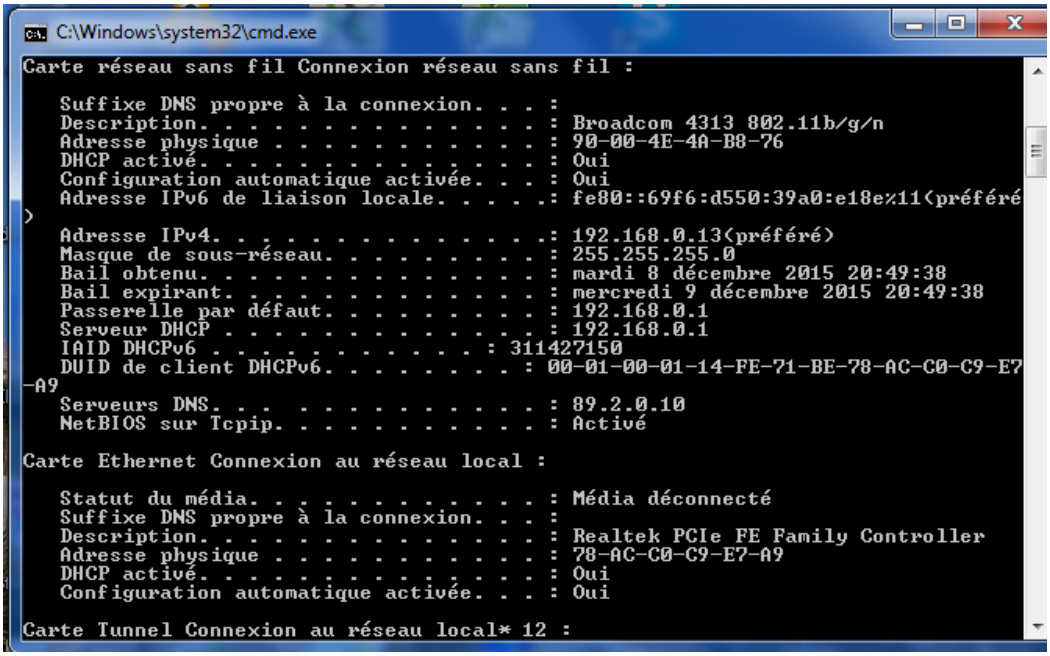
- Le réseau **0.0.0.0** est lui aussi réservé (et utilisé notamment pour définir une route par défaut sur un routeur).

7.8 L'adressage physique : l'adresse MAC (Media Access Control)

A chaque carte réseau est associée une adresse qu'on appelle adresse MAC ou adresse physique. Cette adresse est fixée par le constructeur du matériel et est propre à chaque matériel informatique. Elle permet ainsi d'adresser un message à un ordinateur précis (trame « unicast »).
3 octets pour identifier le constructeur (OUI) + 3 octets pour identifier les machines.
Exemple d'adresse MAC : F4-6D-04-AF-64-62

8 Commandes Microsoft DOS associées :

Sous une fenêtre MS-DOS (commande cmd dans menu démarrer), l'exécution de la commande « ipconfig /all » permet de lister tous les paramètres réseaux de votre ordinateur.
La commande « ping » permet quant-à elle de vérifier si un hôte (un PC, un routeur, un serveur, une serrure biométrique,…) est joignable sur le réseau IP.

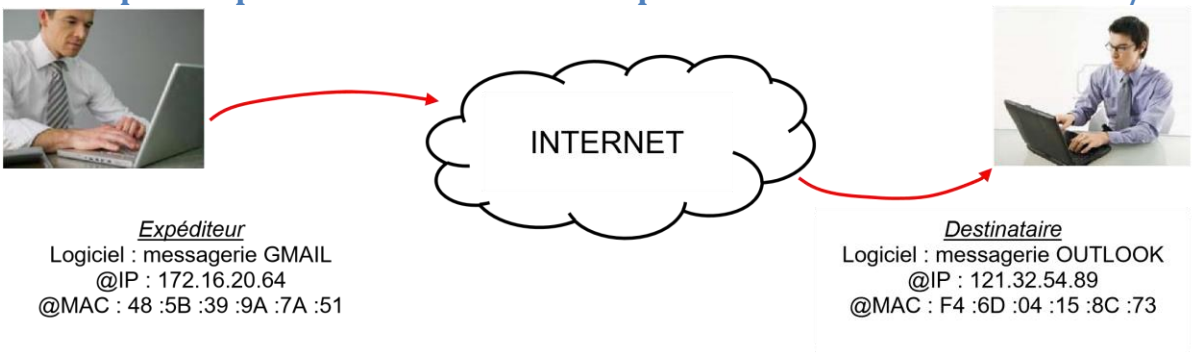


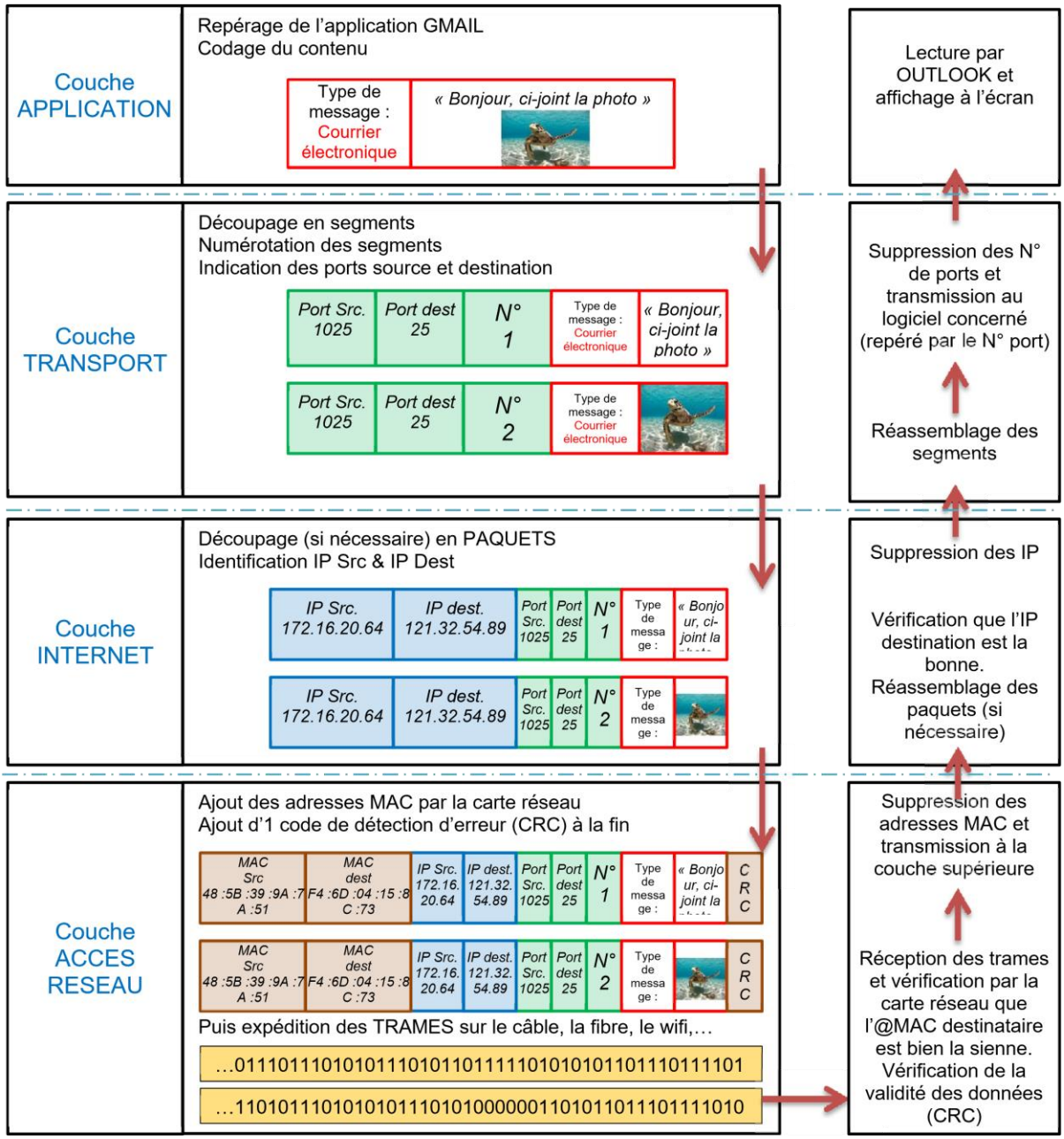
Principales informations

Serveur DHCP : Obtenir une adresse IP automatiquement

Passerelle par défaut : c'est l'adresse IP à laquelle il faut transmettre les paquets IP destinés à des hôtes situés hors du réseau local, pour qu'ils soient routés vers le réseau local de leur destinataire ;
Serveur DNS (*Domain Name System*) mise en relation de l'adresse *www.google.fr* écrite en clair et l'adresse IP de Google en décembre 2015 : *216.58.211.67/,* par exemple.

9 Exemple simplifié du fonctionnement par « Couches » du modèle TCP/IP





Le schéma précédent montre que chaque couche ajoute des informations à celles fournies par la couche précédente. En réalité, chaque couche ajoute d'autres informations en plus des adresses IP, N° de ports,…