

PARTIE 2 : Les réseaux informatiques



1. Introduction

Un réseau informatique est exactement la même chose qu'un réseau d'humains, sauf qu'il faut remplacer les humains par des machines. C'est aussi simple que cela. Dans les deux cas, humains ou machines s'échangent des informations.

Le reste n'est qu'une liste de règles qui régissent la communication.

Par exemple, là où on évoque le langage parlé, écrit, corporel ou encore langage des signes chez les humains, on évoquera le **protocole de communication** pour les machines.

Quel que soit le réseau considéré, nous aurons, au moins :

- Un émetteur,
- Un récepteur,
- Un canal pour acheminer l'objet de la communication, le **message**



2. Le réseau Internet

Le réseau Internet est le réseau permettant la communication entre différents ordinateurs connectés à Internet. Quand un ordinateur est connecté à ce réseau, on dit qu'il a accès à Internet. On confond parfois ce réseau avec le World Wide Web, alors qu'il y a une grande différence entre ces deux notions.

2.1. Le World Wide Web

Le World Wide Web, ou Web pour faire plus court, est l'ensemble des sites Web (appelés par abus de langage "sites Internet") présents sur le réseau Internet. La toile, comme on dit parfois en français, c'est donc l'ensemble de tous les sites Web que nous pouvons visiter grâce à notre navigateur Web (Firefox, Opera, ...).



2.2. Internet



Internet, par contre, c'est l'ensemble des nœuds (connexions, câbles, etc.) entre les machines qui nous donnent accès au web. Internet est donc l'ensemble des réseaux qui nous permettent de partager des données sur la toile (entre autres, car il n'existe pas que le web sur Internet). Donc, quand une personne vous demande si vous avez Internet, elle veut savoir si votre ordinateur a accès à Internet. Par ailleurs c'est encore un abus de langage que de dire que l'on a Internet : ce réseau gigantesque n'appartenant à personne, on ne peut qu'avoir accès à Internet.

3. La classification des réseaux informatiques

Il existe des réseaux adaptés à la nature des échanges et des équipements connectés. La distinction entre les réseaux se fait principalement en fonction de leur portée :

3.1. Le bus / réseau de terrain

Lorsque le réseau informatique est utilisé dans un terrain donné, on l'appelle bus de terrain ou réseau de terrain. Les technologies utilisées pour les réseaux de terrain peuvent varier des réseaux informatiques. En règle générale, on utilise des matériels dédiés à cette utilisation. On utilise aussi des protocoles moins sensibles aux perturbations extérieures.

Ces réseaux sont généralement utilisés pour interconnecter des capteurs, des actionneurs et des calculateurs ou automates industriels.

Exemples : bus CAN, bus I2C, bus DMX 512...

Bus CAN	Bus I2C	DMX 512
<p>CAN high speed (250kbit)</p> <p>CAN low speed (125 kbit)</p> <p>ECM, TCM, ETM, SAS, ABS, CEM, DDM, DIM, SWM, PSM, RTI, REM, SRS, CCM, AUM, PHM, UEM</p>	<p>Composants électroniques</p>	

3.2. Le réseau local (LAN)

Un réseau local, souvent désigné par l'acronyme anglais LAN de Local Area Network, est un réseau informatique tel que les terminaux qui y participent (ordinateurs, etc.) s'envoient des trames au niveau de la couche de liaison sans utiliser d'accès à internet. Au niveau de l'adressage IP, un réseau local correspond généralement à un sous-réseau IP (même préfixe d'adresse IP). On interconnecte les réseaux locaux au moyen de routeurs.

Une autre approche consiste à définir le réseau local par sa taille physique. C'est généralement un réseau à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise.

3.3. Le réseau métropolitain (MAN)

Un réseau métropolitain (en anglais Metropolitan Area Network, MAN) désigne un réseau composé d'ordinateurs habituellement utilisé dans les campus ou dans les villes. Le réseau utilise généralement des fibres optiques.

3.4. Le réseau étendu (WAN)

Un réseau étendu, souvent désigné par son acronyme anglais WAN (Wide Area Network), est un réseau informatique ou un réseau de télécommunications couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière. Le plus grand WAN est le réseau Internet.

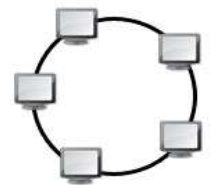
4. Les différentes typologies de réseau

Une topologie de réseau informatique correspond à l'architecture (physique ou logique) de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux.

Elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau (topologie physique). Elle peut aussi définir la façon dont les données transitent dans les lignes de communication (topologie logique).

4.1. Le réseau en anneau

Un réseau a une topologie en anneau quand toutes ses stations sont connectées en chaîne les unes aux autres par une liaison bipoint de la dernière à la première. Chaque station joue le rôle de station intermédiaire. Chaque station qui reçoit une trame, l'interprète et la réémet à la station suivante de la boucle si c'est nécessaire. La défaillance d'un hôte rompt la structure d'un réseau en anneau si la communication est unidirectionnelle.



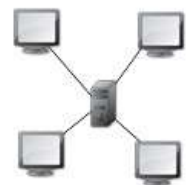
4.2. Le réseau en bus

Tous les postes sont directement connectés à un seul segment (limité par la longueur du câble). La défaillance d'un nœud (ordinateur) ne scinde pas le réseau en deux sous réseaux. Ces unités sont reliées de façon passive par dérivation électrique ou optique.



4.3. Le réseau en étoile

Aussi appelé Hub and spoke, c'est la topologie la plus courante actuellement. Omniprésente, elle est aussi très souple en matière de gestion et dépannage de réseau : la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central qui relie tous les nœuds constitue un point unique de défaillance : une panne à ce niveau rend le réseau totalement inutilisable. Le réseau Ethernet est un exemple de topologie en étoile. L'inconvénient principal de cette topologie réside dans la longueur des câbles utilisés.



4.4. Le réseau maillé

Une topologie maillée correspond à plusieurs liaisons point à point. (Une unité réseau peut avoir plusieurs connexions point à point possibles vers plusieurs autres unités.) Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est.

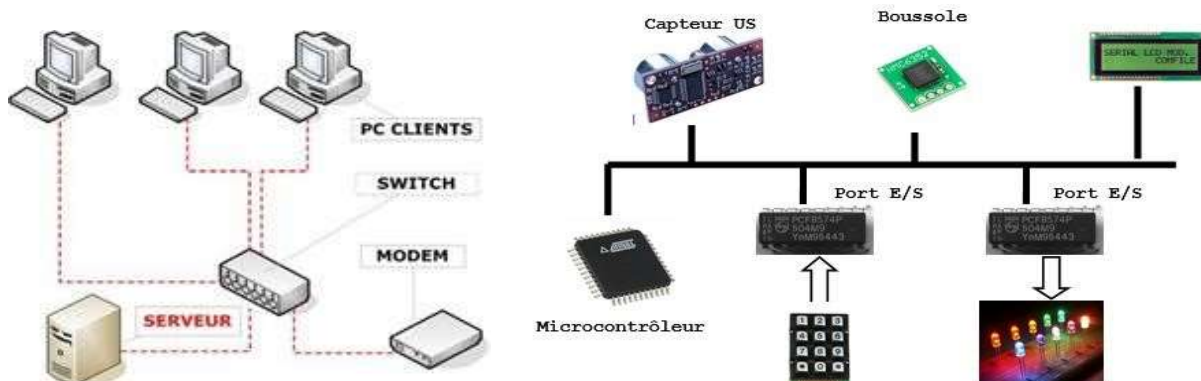
Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.



5. Les différents composants

5.1. Les terminaux

La fonction principale d'un équipement terminal est de permettre à l'utilisateur d'accéder aux ressources du réseau. La famille de terminaux comprend les ordinateurs (souvent appelées stations), les serveurs et l'ensemble des périphériques comme des imprimantes, des capteurs ou des actionneurs pouvant être reliés à un réseau.



5.2. Interface réseau

Pour pouvoir fonctionner en réseau, tous les terminaux doivent posséder une carte d'interface réseau. Certains terminaux sont fournis avec une carte réseau déjà installée. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau dans un ordinateur.

Elle possède une adresse physique (adresse MAC). Une seconde adresse IP lui est adressée et permet de s'affranchir de l'adresse physique. On peut donc changer de carte réseau (en cas de panne) donc d'adresse physique sans changer l'adresse IP.



5.3. Les concentrateurs ou hub (obsolète)

Un hub est un dispositif en réseau qui permet de mettre plusieurs ordinateurs en contact. On utilise quelque fois le terme de répéteur multiport, car il transfère, ou répète, tous les paquets qu'il reçoit sur un port à tous ses autres ports.



5.4. Les commutateurs ou switch

Un switch fonctionne à peu près comme un hub, sauf qu'il est plus discret et intelligent. Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire.

Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le switch se base sur les adresses physiques (adresses MAC) des cartes réseaux des terminaux.



5.5. Les routeurs / modems (ou passerelle)

Un routeur ressemble à un switch sur le plan de l'utilisation : en effet, il permet de mettre plusieurs ordinateurs en réseau. Mais cela va plus loin : il permet de mettre en contact 2 réseaux fondamentalement différents. Dans une petite installation, avec un ou plusieurs ordinateurs connectés à une "box" (qui est en fait un routeur), il est la frontière entre le réseau local et Internet.

Un routeur a plusieurs interfaces. Pour continuer dans notre exemple de frontière avec Internet, il possède une interface connectée à Internet (généralement, cela se traduit par un câble branché sur la prise téléphonique) et plusieurs autres interfaces sur lesquels se connectent des ordinateurs voulant accéder à Internet (ce qui se traduit généralement par des câbles Ethernet ou des connexions Wi-Fi).



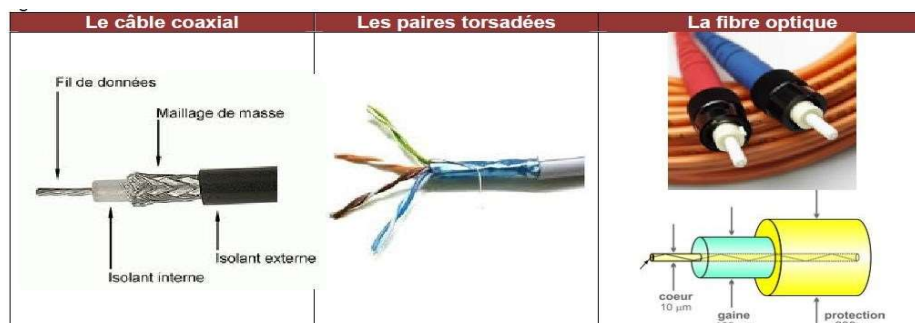
5.6. Les répéteurs

Un répéteur (repeater en anglais) agit un peu comme un hub, mais ce dernier n'a que 2 interfaces. Son intérêt est de renvoyer ce qu'il reçoit par l'interface de réception sur l'interface d'émission, mais plus fort. On dit qu'il régénère et réémet le signal.

En transmission sans fil (radio, téléphone) on parle aussi de relais. Un répéteur permet de couvrir des distances plus grandes que les distances maximales fixées par le matériel que l'on utilise : par exemple, dans un réseau sans fil (Wi-Fi), la portée maximale entre 2 appareils est d'environ 50 mètres en intérieur. En plaçant un répéteur peu avant ces 50 mètres, vous pouvez connecter 2 appareils à 100 mètres de distance. Le fait que les informations soient renvoyées "plus fort" peut dégrader la qualité du signal dans les réseaux sans fil.

5.7. Les supports de transmissions

Les supports physiques de transmission peuvent être très hétérogènes, aussi bien au niveau du transfert de données (circulation de données sous forme d'impulsions électriques, sous forme de lumière ou bien sous forme d'ondes électromagnétiques) qu'au niveau du type de support (paires torsadées, câble coaxial, fibre optique, ondes radio, ...).

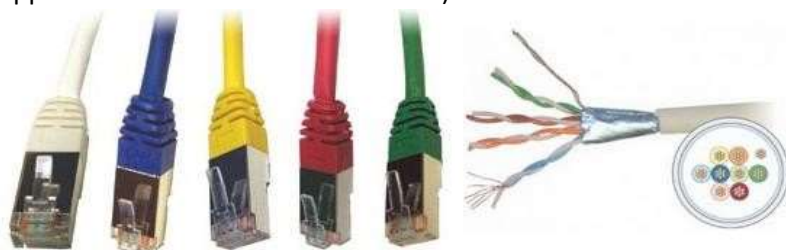


Le choix du support est fonction de critères interdépendants parmi lesquels : la distance maximum entre stations, les débits minimum et maximum, le type de transmission (numérique ou analogique), la nature des informations échangées (donnée, voix, vidéo ...), la connectique, la fiabilité, le coût ...

5.7.1. Le câble internet

Le câble Ethernet (à paires torsadées) est sûrement le type de câble le plus utilisé pour connecter des ordinateurs entre eux dans un réseau local. À moins que votre réseau soit entièrement sans-fil, vous en avez sûrement chez vous. Il relie généralement un ordinateur personnel à un routeur (ce que l'on appelle parfois une "box"). Le nom "scientifique" (si l'on peut appeler ça comme ça) du câble Ethernet est "câble UTP-CAT5 (Unshielded Twisted Pair Category 5)" ou "câble UTP-CAT6 (Unshielded Twisted Pair Category 6)". La différence entre les deux catégories ? Tout simplement le débit : le CAT5 permet un débit de 100 mégabits par seconde alors que le CAT6 supporte le gigabit par seconde.

Il existe deux types de câble Ethernet (à paires torsadées) : les câbles Ethernet droits et les câbles Ethernet croisés. Ces derniers permettent de relier directement entre eux deux équipements similaires (ex. deux ordinateurs ou deux switches) alors que les câbles droits servent à relier deux équipements différents (ex. un ordinateur à un autre appareil comme un hub ou un switch).



5.7.2. Le Bluetooth

Le Bluetooth est une technologie de réseau personnel sans fils, c'est-à-dire une technologie de réseaux sans fils d'une faible portée permettant de relier des appareils entre eux sans liaison filaire.

Contrairement à la technologie IrDa (liaison infrarouge), les appareils Bluetooth ne nécessitent pas d'une ligne de vue directe pour communiquer, ce qui rend plus souple son utilisation et permet notamment une communication d'une pièce à une autre, sur de petits espaces.

Il existe 3 classes en Bluetooth : la classe 1, la 2 et la 3. Ce qui les différencie est juste la portée. Dans la classe 1, la portée peut aller jusqu'à 100 mètres, dans la catégorie 2, elle est d'une dizaine de mètres, et dans la classe 3, elle est de quelques mètres seulement (moins de 10). C'est cette 3ème classe qui est utilisée dans les téléphones portables.



5.7.3. L'infrarouge

L'infrarouge est un autre moyen de transmission des données sans fil, qui exploite la lumière. Il est moins pratique que le Bluetooth car il faut que les périphériques qui communiquent entre eux soient à moins de 1,50m de distance. Ils doivent aussi être alignés : la lumière ne se propage pas dans les environs comme les ondes radio. Autrefois, beaucoup de téléphones utilisaient l'infrarouge, mais il s'est rapidement fait remplacer par le Bluetooth, bien que certains appareils utilisent les deux. Il existe toujours actuellement des télécommandes TV, imprimantes, souris, claviers sans fil utilisant infrarouge.



5.7.4. Le wifi

Le Wi-Fi est certainement le moyen de transmission de données sans fil le plus utilisé. Sa portée pouvant excéder les 200 mètres en espace ouvert et sa vitesse de débit théorique de plus de 100 mégabits par seconde (Mbps) ont permis une démocratisation de cette technologie qui est aujourd'hui très utilisée dans les réseaux locaux pour accéder à Internet. Il est impressionnant de constater le nombre de points d'accès Wi-Fi sécurisés ou non que l'on puisse capter un peu partout. "Wi-Fi" peut être considéré comme le nom commercial de la norme IEEE 802.11, norme qui régit cette technologie.



6. La communication dans un réseau

Tous les équipements connectés se partagent un même support de transmission doivent en conséquence respecter des règles appelées protocoles, régissant l'usage de ce support.



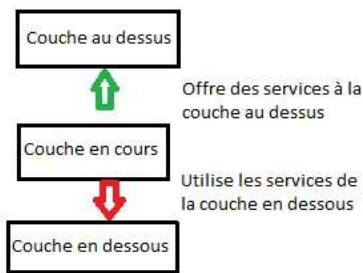
6.1. Les protocoles

Un protocole de communication est un ensemble de règles et de procédures permettant de définir un type de communication particulier. Les protocoles sont hiérarchisés en couches, pour décomposer et ordonner les différentes tâches. Il existe plusieurs familles de protocoles ou modèles, chaque modèle étant une suite de protocoles entre diverses couches. Parmi ces modèles on trouve le modèle OSI et le modèle TCP/IP.

6.2. Le modèle OSI

Le modèle OSI (Open Systems Interconnection : « interconnexion de systèmes ouverts ») a été développé à vocation normative, c'est-à-dire pour servir de référence dans le déroulement de la communication entre deux hôtes.

Le modèle OSI est une façon standardisée de segmenter en plusieurs blocs le processus de communication entre deux entités. Chaque bloc résultant de cette segmentation est appelé couche. Une couche est un ensemble de services accomplissant un but précis. La beauté de cette segmentation, c'est que chaque couche du modèle OSI communique avec la couche au-dessus et au-dessous d'elle (on parle également de couches adjacentes). La couche au-dessous pourvoit des services que la couche en cours utilise, et la couche en cours pourvoit des services dont la couche au-dessus d'elle aura besoin pour assurer son rôle. Voici un schéma pour illustrer ce principe de communication entre couches :



Ainsi le modèle OSI permet de comprendre de façon détaillée comment s'effectue la communication entre un ordinateur A et un ordinateur B. En effet, il se passe beaucoup de choses dans les coulisses entre l'instant t , où vous avez envoyé un mail (par exemple), et l'instant t_1 , où le destinataire le reçoit.

Exemple :

Pour comprendre le modèle OSI, nous allons inventer un scénario. Pierre garde une lettre dans son bureau. Il veut la donner au facteur, qui attend devant le portail de sa belle villa. La lettre est destinée à Jacques, mais Pierre n'a pas le droit d'entrer dans le bureau de Jacques. Jacques non plus n'a pas le droit de sortir de son bureau. Seul le facteur peut entrer dans le bureau de Jacques pour délivrer la lettre, mais il lui est interdit d'aller dans celui de Pierre pour la chercher.

La maison de Pierre est mal construite : il n'y a pas de couloir, juste un alignement vertical de pièces séparées par une porte. Pour aller du bureau au portail, Pierre doit traverser le salon et le jardin.

Dans le schéma ci-contre, chaque pièce de la maison peut être considérée comme une couche. Pierre doit quitter la couche la plus élevée pour se diriger vers la plus basse (le portail). Une fois la lettre remise au facteur, ce dernier devra faire l'inverse chez Jacques, c'est-à-dire quitter la couche la plus basse pour aller vers la couche la plus élevée (le bureau de Jacques).

Chaque pièce de la maison possède une fonction précise. Le bureau est généralement réservé au travail ; le salon, à la distraction (discussions, télévision, etc.). Le jardin, lui, nous offre sa beauté et son air pur. Quant au portail, il permet d'accéder aussi bien au jardin qu'à la maison.



Pierre



Le Facteur

Le modèle OSI a segmenté la communication en sept couches :

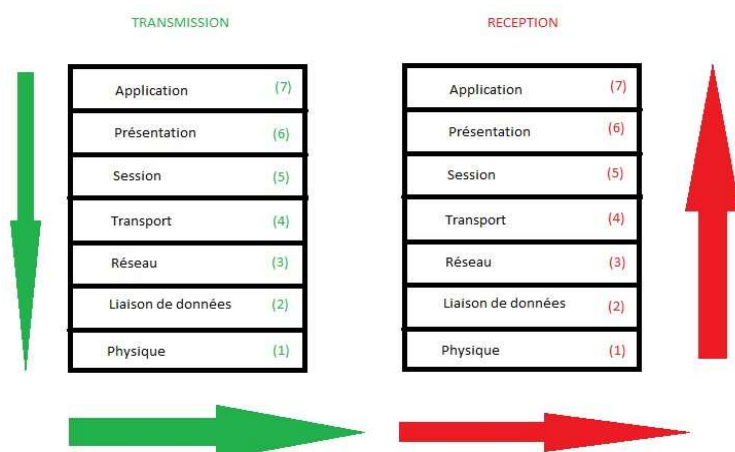


6.2.1. Les différentes couches du modèle

Position dans le modèle OSI	Nom de la couche	Rôle de la couche
7	Application	La couche applicative fait office d'interface pour vous donner accès à ces services, qui vous permettent notamment de transférer des fichiers, de rédiger un mail, d'établir une session à distance, de visualiser une page web...
6	Présentation	Elle s'occupe de tout aspect lié à la présentation des données : format, cryptage, encodage, etc.
5	Session	Responsable de l'initialisation de la session, de sa gestion et de sa fermeture.
4	Transport	Choix du protocole de transmission et préparation de l'envoi des données (TCP ou UDP par exemple). Elle spécifie le numéro de port utilisé par l'application émettrice ainsi que le numéro de port de l'application réceptrice. Elle fragmente les données en plusieurs séquences (ou segments).
3	Réseau	Connexion logique entre les hôtes (adresse IP). Elle traite de tout ce qui concerne l'identification et le routage dans le réseau.
2	Liaison de données	Établissement d'une liaison physique entre les hôtes (adresse MAC). Fragmente les données en plusieurs trames.
1	Physique	Conversion des trames en bits et transmission physique des données sur le média.

6.2.2. Processus de transmission / réception

Quand un hôte A envoie un message à un hôte B, le processus d'envoi va de la couche 7 (application) à la couche 1 (physique). En revanche, quand il s'agit de recevoir, le message emprunte le chemin inverse : il part de la couche 1 (physique) pour arriver à la couche 7 (application).

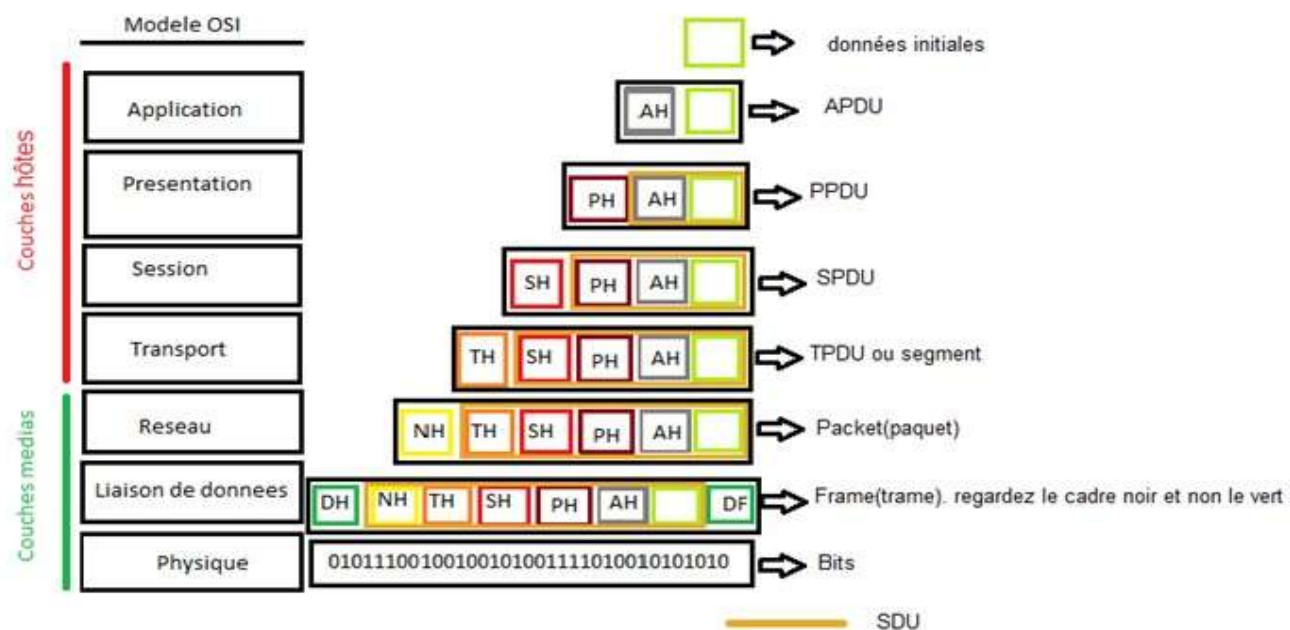


6.3. L'encapsulation

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. À chaque couche, une information est ajoutée au paquet de données, il s'agit d'un entête, ensemble d'informations qui garantit la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi à la réception, le message est dans son état originel.

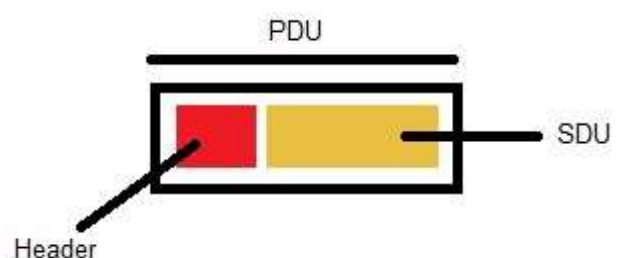
À chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé message au niveau de la couche application
- Le message est ensuite encapsulé sous forme de segment dans la couche transport
- Le segment une fois encapsulé prend le nom de paquet dans la couche réseau
- Enfin on parle de trame au niveau de la couche liaison
- Et de signal au niveau de la couche physique



Chaque couche du modèle OSI a une fonction déterminée. Cette corrélation indique bien que certaines informations peuvent se retrouver d'une couche à une autre. Cela n'est possible que grâce au principe d'encapsulation.

Les données sont enveloppées à chaque couche et portent le nom de PDU (Protocol Data Unit) et contiennent deux choses : la donnée en elle-même appelée SDU (Service Data Unit) et l'entête spécifique à cette couche. La partie « donnée » de ce paquet est composée de la donnée initiale, mais aussi des entêtes des couches qui la précèdent.



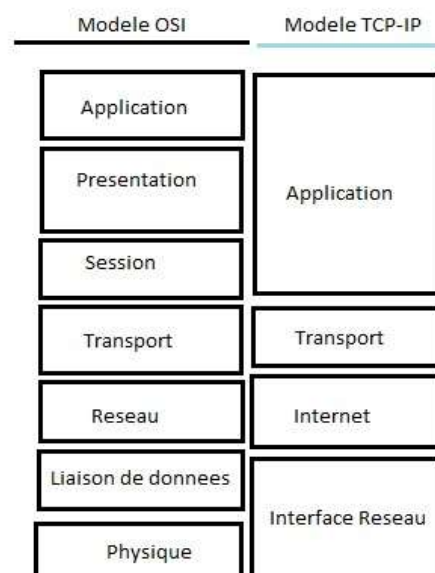
6.4. Le modèle TCP/IP

Le modèle TCP/IP a une vocation descriptive, c'est-à-dire qu'il décrit la façon dont se passe la communication entre deux hôtes. En d'autres termes, si vous voulez comprendre comment se déroule la communication « sur le terrain », prenez le modèle TCP/IP.

Le modèle TCP/IP n'est constitué que de quatre couches. Ce sont des couches d'abstraction, autrement dit des couches qui cachent les détails d'implémentation de la communication et leurs noms ne reflètent pas mot pour mot les fonctions qu'elles assurent. Les trois premières couches du modèle OSI correspondent à la couche applicative du modèle TCP/IP.

Le modèle TCP/IP est donc le modèle utilisé pour Internet.

Le nom de modèle TCP/IP est étroitement lié à deux protocoles : le protocole TCP (Transmission Control Protocol) et le protocole IP (Internet Protocol). Ceci est en partie dû au fait que sont les deux protocoles les plus utilisés pour Internet.



Position dans le modèle TCP/IP	Nom de la couche	Rôle de la couche
4	Application	La couche application est la couche située au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures.
3	Transport	<p>Les protocoles des couches précédentes permettaient d'envoyer des informations d'une machine à une autre. La couche transport permet à des applications tournant sur des machines distantes de communiquer. Le problème consiste à identifier ces applications.</p> <p>La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type de réseau emprunté (c'est-à-dire indépendamment des couches inférieures...), il s'agit des protocoles suivants :</p> <ul style="list-style-type: none"> ○ TCP, un protocole orienté connexion qui assure le contrôle des erreurs ○ UDP, un protocole non orienté connexion dont le contrôle d'erreur est archaïque
2	Internet	La couche Internet est la couche "la plus importante" (elles ont toutes leur importance) car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP.
1	Interface réseau	La couche interface réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

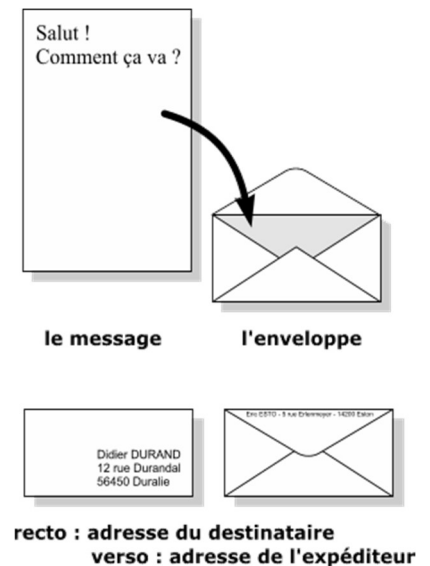
6.4.1. Le protocole IP

IP signifie Internet Protocol : littéralement "le protocole d'Internet". C'est le principal protocole utilisé sur Internet.

Faisons un parallèle avec la poste.

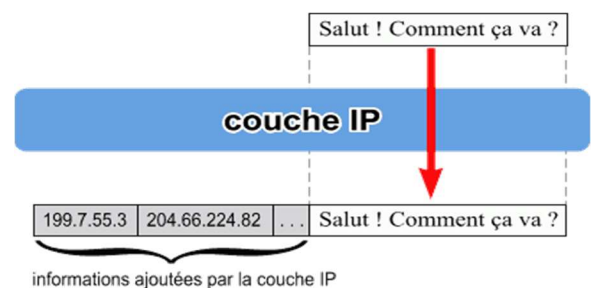
Quand vous voulez envoyer une lettre par la poste :

- 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 vôtre).



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 :

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



6.4.2. Les protocoles UDP et TCP

Les principaux protocoles utilisés par la couche transport du modèle TCP/IP sont l'UDP et le TCP

Le protocole UDP

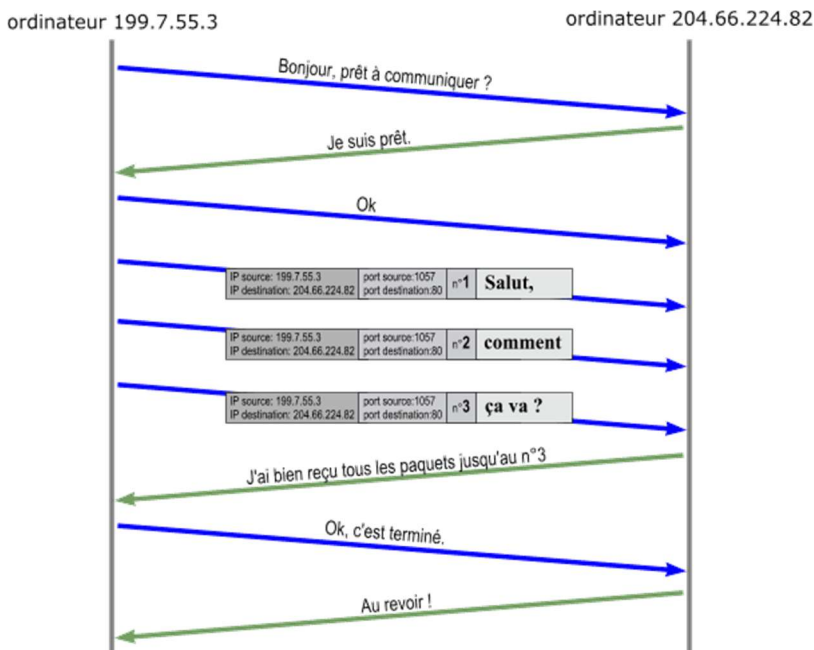
UDP est un protocole orienté "non connexion".

Pour faire simple, lorsqu'une machine A envoie des paquets à destination d'une machine B, ce flux est unidirectionnel. En effet, la transmission des données se fait sans prévenir le destinataire (la machine B), et le destinataire reçoit les données sans effectuer d'accusé de réception vers l'émetteur (la machine A). Ceci est dû au fait que l'encapsulation des données envoyées par le protocole UDP ne permet pas de transmettre les informations concernant l'émetteur. De ce fait, le destinataire ne connaît pas l'émetteur des données hormis son IP.

Le protocole TCP

Contrairement à l'UDP, le TCP est orienté "connexion". Lorsqu'une machine A envoie des données vers une machine B, la machine B est prévenue de l'arrivée des données, et témoigne de la bonne réception de ces données par un accusé de réception. Ici, intervient le contrôle CRC des données. Celui-ci repose sur une équation mathématique, permettant de vérifier l'intégrité des données transmises. Ainsi, si les données reçues sont corrompues, le protocole TCP permet aux destinataires de demander à l'émetteur de renvoyer les données corrompues.

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



6.5. L'adressage

Pour communiquer, il faut savoir à qui on veut s'adresser !

Il est temps de parler de l'identification et de la communication dans un réseau. Nous allons aborder 2 notions : il s'agit des adresses IP et des adresses MAC.

La différence primordiale entre les adresses IP et les adresses MAC est que les adresses IP sont routables. Elles peuvent communiquer avec des machines au-delà d'un sous-réseau, contrairement aux adresses MAC. L'élément central (switch, ...) se base donc sur les adresses MAC pour assurer la communication entre plusieurs machines appartenant à un même sous-réseau, mais utilise les adresses IP pour faire communiquer des machines de sous réseaux différents.

6.5.1. Les adresses MAC ou adresse physique

Une adresse MAC est un identifiant unique attribué à chaque carte réseau. C'est une adresse physique.

Concrètement, c'est un numéro d'identification composé de 12 chiffres hexadécimaux. Par convention, on place un symbole deux-points (:) tous les 2 chiffres. Une adresse MAC ressemble donc à cela : 01:23:45:67:89:AB.

6.5.2. Les adresses IP

Une adresse IP n'est "rien d'autre" que l'endroit où habite un ordinateur. Mais attention : cette adresse est relative au réseau. Une machine n'aura pas forcément la même adresse IP sur un réseau X et un réseau Y.

Les adresses IP sont le seul moyen d'identification des machines sur Internet. Mais il existe 2 versions du protocole Internet (la "manière" d'accéder à Internet en quelque sorte) : IPv4 et IPv6. Et chaque version utilise sa propre structure d'adresse IP.

Une "adresse IPv4" est constituée de 4 nombres correspondant à 4 octets compris entre 0 et 255, séparés par des points. De nos jours, ce sont les plus connues.

Exemple : **88.45.124.201**

Les "adresses IPv6" sont encore plus complexes : elles sont représentées par une suite de 8 groupes de 2 octets représentés en hexadécimal où les 8 groupes de 2 octets (16 bits par groupe) sont séparés par un signe deux points :

Exemple : **1fff:0000:0a88:85a3:0000:0000:ac1f:8001**

6.5.3. La structure des adresses IP

Les adresses IP sont des nombres de 32 bits qui contiennent 2 champs :

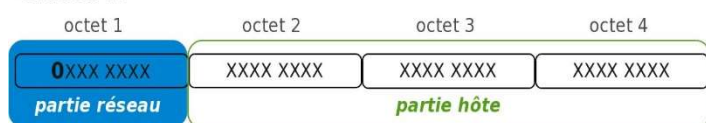
- **Un identificateur de réseau (NET-ID)** : tous les systèmes du même réseau physique doivent posséder le même identificateur de réseau, lequel doit être unique sur l'ensemble des réseaux gérés.
- **Un identificateur d'hôte (HOST-ID)** : un nœud sur un réseau TCP/IP est appelé hôte, il identifie une station de travail, un serveur, un routeur ou tout autre périphérique TCP/IP au sein du réseau.

6.5.4. Les classes d'adresse IPV4

Une classe en réseau est, en fait, un ensemble d'adresses IP. Chaque adresse IP appartient à une classe principale (on dit aussi une plage). Chaque classe a un masque de sous-réseau par défaut. Que vous le vouliez ou non, dès que vous donnez à votre carte réseau une adresse IP, votre système d'exploitation lui assigne directement un masque de sous-réseau par défaut selon la classe à laquelle appartient votre adresse IP.

Par convention, les créateurs du protocole IP disent qu'il existe 5 classes d'adresses IP. En d'autres termes, on peut choisir notre adresse IP dans ces cinq classes. Ces classes sont : A, B, C, D et E. Les classes les plus utilisées sont les classes A, B et C.

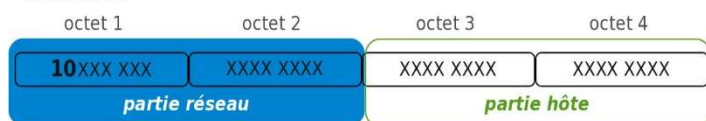
Classe A



Le premier octet d'une adresse IP permet de déterminer la classe de cette adresse.

Exemple : Soit l'adresse IP suivante : 142.62.149.4

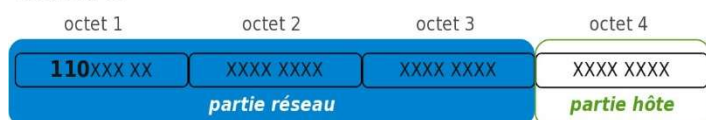
Classe B



142 en décimal = $(10001110)_2$ en binaire

Le mot binaire commence par les bits 10 donc il s'agit d'une adresse de classe B.

Classe C



S'agissant d'une adresse de classe B, les deux premiers octets identifient le réseau. Le numéro de réseau est donc : 142.62.0.0

Les deux derniers octets identifient l'équipement hôte

sur le réseau.

Finalement, cette adresse désigne l'équipement numéro 149.4 sur le réseau 142.62.

6.5.5. L'adressage CIDR

Une forme plus courte est connue sous le nom « d'adressage CIDR » (Classless Inter-Domain Routing) qui correspond à un adressage sans classes. Elle donne le numéro du réseau suivi par une barre oblique (ou slash, « / ») et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau.

Exemple : Soit l'adresse IP suivante : 91.198.174.2/19

La notation 91.198.174.2/19 désigne donc l'adresse IP 91.198.174, et signifie que les 19 premiers bits de l'adresse sont dédiés à l'adresse du sous-réseau, et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau.

6.5.6. Les masques de sous réseaux

Le rôle du masque de sous réseau (netmask) est d'identifier précisément les bits qui concernent le N° de réseau d'une adresse (il "masque" la partie hôte de l'adresse).

Un bit à 1 dans le masque précise que le bit correspondant dans l'adresse IP fait partie du N° de réseau ; à l'inverse, un bit à 0 spécifie un bit utilisé pour coder le N° d'hôte.

Ainsi, on a un masque dit "par défaut" qui correspond à la classe de ce réseau.

Exemple: dans un réseau de classe A sans sous-réseau, le premier octet correspond à l'adresse du réseau donc le masque de sous réseau commence par 11111111 suivi de zéros soit 255.0.0.0.

D'où le tableau suivant :

Classe	A	B	C
Masque de sous réseaux	255.0.0.0	255.255.0.0	255.255.255.0

Avec la notation CIDR, le masque de sous réseau peut prendre d'autres valeurs.

Exemple : Soit l'adresse IP suivante : 91.198.174.2/19

Le masque sera donc représenté par 19 bits à la valeur 1, suivis de 13 bits à la valeur 0. Soit 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000

6.5.7. Détermination de l'adresse réseau

Pour déterminer l'adresse du réseau auquel appartient un hôte, on effectue le masquage de son adresse IP par son masque de sous-réseau. Le masquage est obtenu en effectuant une opération ET (AND) bit à bit entre les deux adresses.

Exemple : Soit l'adresse IP suivante 172.16.4.1/24

&	@IP	10101100 . 00010000 . 00000100 . 00000001	172.16.4.1
	masque	11111111 . 11111111 . 11111111 . 00000000	255.255.255.0
	Résultat & bit à bit	10101100 . 00010000 . 00000100 . 00000000	172.16.4.0

L'adresse réseau (identifiant réseau) auquel appartient le poste est 172.16.4.0.

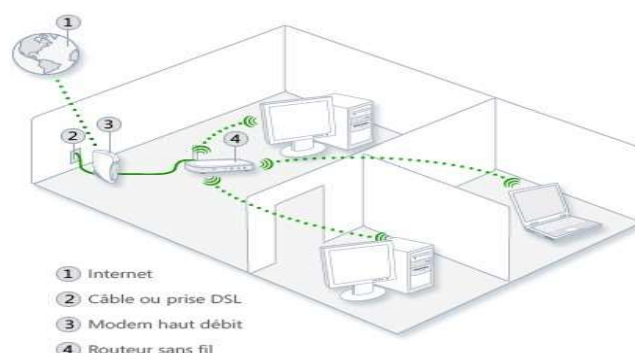
6.5.8. Les adresses publiques et privées

Dans un réseau domestique (réseau privé de votre maison), seule votre « BOX ADSL » (votre routeur) est identifiée par **une adresse IP publique**. Les autres périphériques de votre réseau domestique (ordinateur, tablette, ...) sont identifiés par **une adresse IP privée**.

L'adresse IP publique de votre BOX ADSL est une adresse IP fournie par votre Fournisseur d'Accès Internet (FAI), unique sur tout le réseau Internet.

C'est vous qui déterminez **Les adresses privées** que vous allez utiliser dans votre réseau domestique.

Pour cela, **vous pouvez piocher dans un lot d'adresses IP qui ont été sorties des adresses distribuables sur internet** pour un usage exclusif dans les réseaux privés.



- En classe A (masque 255.0.0.0) : de **10.0.0.0** à **10.255.255.255**
- En classe B (masque 255.255.0.0) : de **172.16.0.0** à **172.31.255.255**
- En classe C (masque 255.255.255.0) : de **192.168.0.0** à **192.168.255.255**

Les adresses privées ne sont pas routables (utilisable pour communiquer sur internet), elles ne sont utilisées que dans les réseaux privés (à la maison ou en entreprise) pour identifier les équipements informatiques. Ces adresses ne sont jamais attribuées par les fournisseurs d'accès internet. Les mêmes adresses IP peuvent donc être utilisées dans différents sous réseaux sans risques de conflits.

6.5.9. Les adresses réservées

Les adresses réservées ne peuvent désigner une machine TCP/IP sur un réseau.

L'adresse de bouclage (loopback) : l'adresse de réseau 127 n'est pas attribuée à une société, elle est utilisée comme adresse de bouclage dans tous les réseaux. Cette adresse sert à tester le fonctionnement de votre carte réseau. Un ping 127.0.0.1 doit retourner un message correct. Le paquet envoyé avec cette adresse revient à l'émetteur.

L'adresse de réseau est une adresse dont tous les bits d'hôte sont positionnés à 0 (ex 128.10.0.0 adresse de réseau du réseau 128.10 de classe B). Elle est utilisée pour désigner tous les postes du réseau. On utilise cette adresse dans les tables de routage.

L'adresse de diffusion (broadcast) est une adresse dont tous les bits d'hôte sont positionnés à 1 (ex : 128.10.255.255 adresse de diffusion du réseau 128 de classe B). Elle est utilisée pour envoyer un message à tous les postes du réseau.

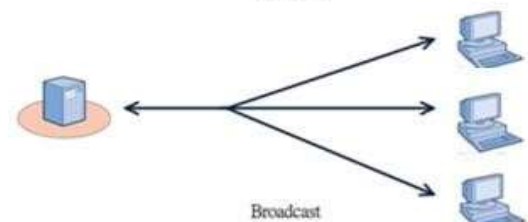
6.5.10. Les envois de données

Dans un réseau informatique, il y a plusieurs moyens d'envoyer des données.

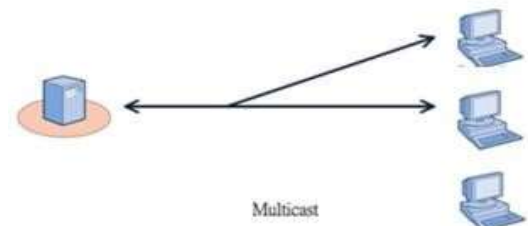
- **L'unicast** : dans ce cas, on envoie des données à un seul ordinateur ;



- **Le broadcast** : on envoie des données à tous les ordinateurs du réseau.



- **Le multicast** : l'envoi des données se fait vers un groupe d'ordinateurs ;



Ce qu'il faut savoir, c'est que l'adresse 255 dans les réseaux de la classe C est une adresse de broadcast réseau. En bref, si vous envoyez des données à cette adresse, les données seront envoyées à tous les ordinateurs du réseau !

7. Les principaux services réseaux

Nous avons vu qu'Internet s'appuyait sur le protocole TCP/IP. Il existe de nombreux autres protocoles en usage sur ce réseau, en particulier, les principaux services offerts par Internet qui sont le web, la messagerie électronique (email) les forums, le chat et le FTP, utilisent chacun un protocole différent.

On y trouve par exemple les services ci-dessous, mais il en existe pleins d'autres.

7.1. Les noms de domaines (DNS)

Le nom affecté à un matériel permet de l'identifier de manière plus simple par un utilisateur. Par exemple, delair.online.fr est plus significatif que 212.27.32.15. Un nom peut ainsi être associé à n'importe quelle interface réseau. Il est défini par l'administrateur du domaine dans lequel elle se situe.

Ce service s'est généralisé sur internet. Le DNS est un système hiérarchique comparable à l'organisation de répertoires.

Les domaines en haut de l'édifice sont découpés en deux catégories, celui géographique (fr, us, jp ...) et celui référençant le type d'organisations : com pour les organismes commerciaux, edu pour la formation, org...

7.2. La visualisation de pages Web (HTTP)

Le service le plus connu, le plus récent et maintenant le plus utilisé de consultation d'hyperdocuments. C'est LE service d'Internet. C'est ce service qui l'a rendu attrayant, et « commercialement utile ».

Un hyperdocument est un document électronique contenant des images, du son, du texte, parfois des petits morceaux de programme, mais surtout des liens vers d'autres hyperdocuments : des liens hypertextes. Ces liens apparaissent dans un style qui les distinguent, et une simple action de la souris sur un lien suffit à ouvrir le document lié. Les documents peuvent se trouver sur n'importe quelle machine (serveur) de l'Internet à des endroits parfois très éloignés et c'est ce qui donne l'impression à l'utilisateur de naviguer sur le réseau.

Il s'appuie sur le protocole HTTP, qui figure au début de l'adresse du serveur où vous vous connectez pour accéder à une page Web.

7.3. La messagerie électronique (SMTP et POP)

La messagerie électronique (e-mail ou encore mail), c'est utiliser l'Internet comme on utilise la poste. Il est possible de déposer un message dans la boîte aux lettres de son correspondant, qu'il soit ou non devant une machine. Ce dernier sera capable, à sa prochaine connexion, de consulter sa boîte aux lettres pour lire ou envoyer des messages à ses correspondants.

Les messages sont expédiés et reçus grâce à deux protocoles (SMTP et POP), mais ils peuvent aussi transiter par le Web.

7.4. Le transfert de fichier (FTP)

Le FTP, File Transfert Protocol, est un protocole de transfert de fichiers. Ce transfert s'effectue en établissant une connexion entre un serveur FTP et un client FTP situé sur votre ordinateur. Les fichiers échangés sont des fichiers informatiques de tous types (texte, images, sons, logiciels, ...)