MR. Réseaux et modèles en couches

I/ Les réseaux informatiques

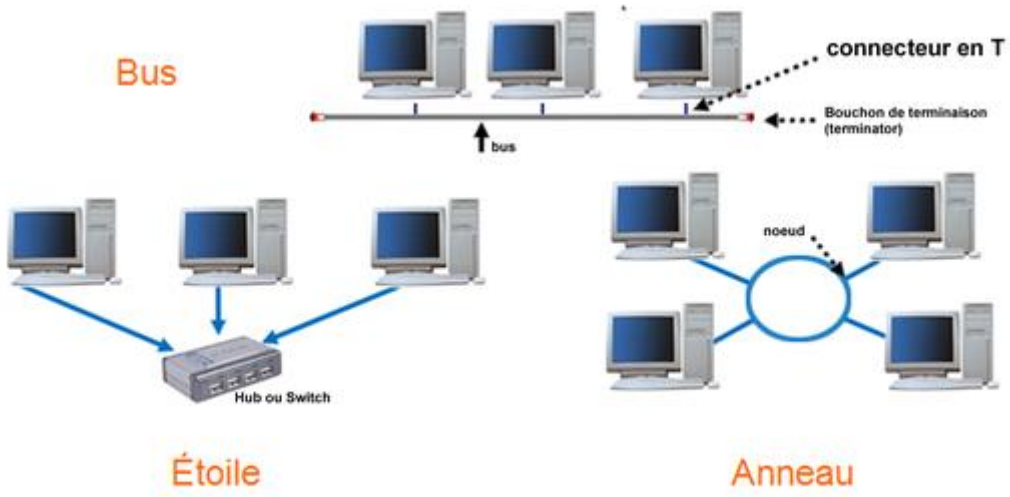
1/ Définition

Un **réseau** est un système composé d'éléments matériels (routeur, fibre optique …) et de logiciels (pilotes des interfaces, *firmwares* des équipements …) dont la fonction est le transport de flux d'informations. Il sert à mettre en œuvre des services (imprimante partagée, mise à disposition d'applications …).

2/ Etendue et topologie

Les réseaux se différencient en particulier par :

- Leur **taille** : PAN (Personnal Area Network), LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).
- Leur **mode** de fonctionnement : envoi de messages à tous les équipements (**broadcast**) ou à certains seulement (**multicast**), cela correspond à des réseaux de petites tailles. Dans le cas d'Internet, on communique à une seul équipement (**unicast**) via de nombreux supports (routeur, switch …).
- Leur **topologie** (configuration) : équipements en étoile, bus (en voie de disparition), anneau ...



A Saint-Jean, le réseau local de la salle d'informatique est en étoile.

II/ Les protocoles TCP/IP

1/ Historique

La DARPA (*Defense Advanced Research Projects Agency*) voit le jour en 1958, cette agence gouvernementale américaine a pour but de veiller à la constante suprématie des États unis en matière technologique et scientifique. Il ne faut pas oublier que l'on est en plein guerre froide et que l'URSS dispose à ce moment d'une avance marquée dans le domaine de la conquête spatiale.

En 1962 la DARPA soutient le projet du professeur Licklider qui a pour but de mettre en réseau les ordinateurs des universités américaines afin que ces dernières puissent échanger des informations plus rapidement (même à des milliers de kilomètres de distance).

En 1968, ARPAnet, 1er réseau informatique à grande échelle de l'histoire voit le jour. Le 29 octobre **1969**, le 1er message (le mot "login") est envoyé depuis l'université de Californie à Los Angeles vers l'université de Stanford via le réseau ARPAnet (les 2 universités sont environ distantes de 500 Km). C'est un demi-succès, puisque seules les lettres "l" et "o" arriveront à bon port.

A noter : **cette date est à connaître (réseau Arpanet).**

En 1972, 23 ordinateurs sont connectés à ARPAnet (on trouve même des ordinateurs en dehors des États unis). En parallèle au projet ARPAnet, d'autres réseaux voient le jour, problème, ils utilisent des protocoles de communication hétéroclites (UUCP, NCP ou encore X.25) et 2 ordinateurs appartenant à 2 réseaux différents sont incapables de communiquer entre eux puisqu'ils n'utilisent les mêmes protocoles.

En 1974 Vint Cerf et Bob Khan vont mettre au point **le protocole TCP** qui sera très rapidement couplé au protocole IP pour donner **TCP/IP**. TCP/IP, grâce à sa simplicité, va très rapidement s'imposer comme un standard : les différents réseaux (ARPAnet et les autres) vont adopter TCP/IP. Cette adoption va permettre d'interconnecter tous ces réseaux (2 machines appartenant à 2 réseaux différents vont pouvoir communiquer grâce à cette interconnexion). Internet était né (le terme Internet vient de "internetting" qui signifie "Connexion entre plusieurs réseaux").

A noter : **cette date est à connaître (mise au point du protocole TCP/IP).**

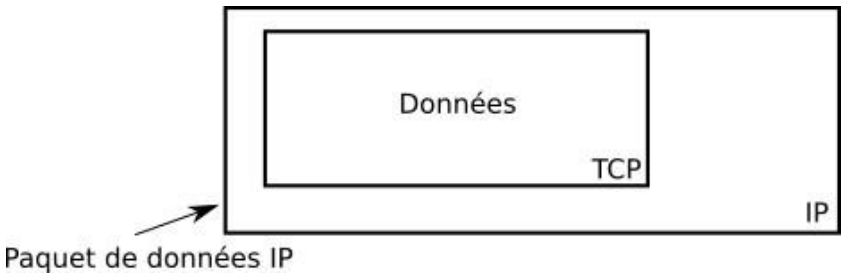
TCP/IP est donc au cœur d'Internet, voilà pourquoi aujourd'hui, la plupart des machines utilisent TCP/IP.

2/ Principes de ce protocole

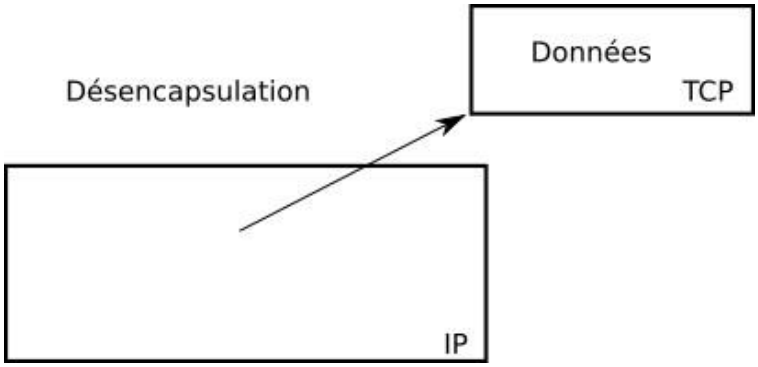
Voici le principe de base des protocoles TCP (*Transmission Control Protocol*) et IP (*Internet Protocol*).

Quand un ordinateur A "désire" envoyer des données à un ordinateur B, l'ordinateur A "utilise" le protocole TCP pour mettre en forme les données à envoyer.

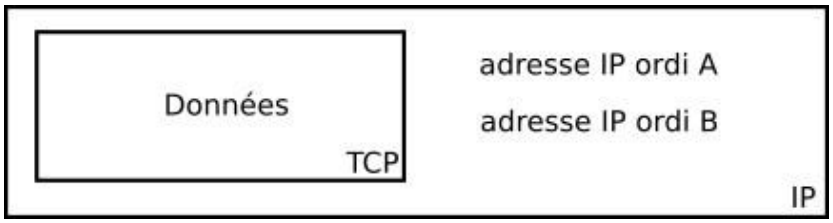
Ensuite le protocole IP prend le relai et utilise les données mises en forme par le protocole TCP afin de créer des paquets des données. Après quelques autres opérations qui ne seront pas évoquées ici, les paquets de données pourront commencer leur voyage sur le réseau jusqu'à l'ordinateur B. Il est important de bien comprendre que le protocole IP "encapsule" les données issues du protocole TCP afin de constituer des paquets de données.



Une fois arrivées à destination (ordinateur B), les données sont "désencapsulées" : on récupère les données TCP contenues dans les paquets afin de pouvoir les utiliser.

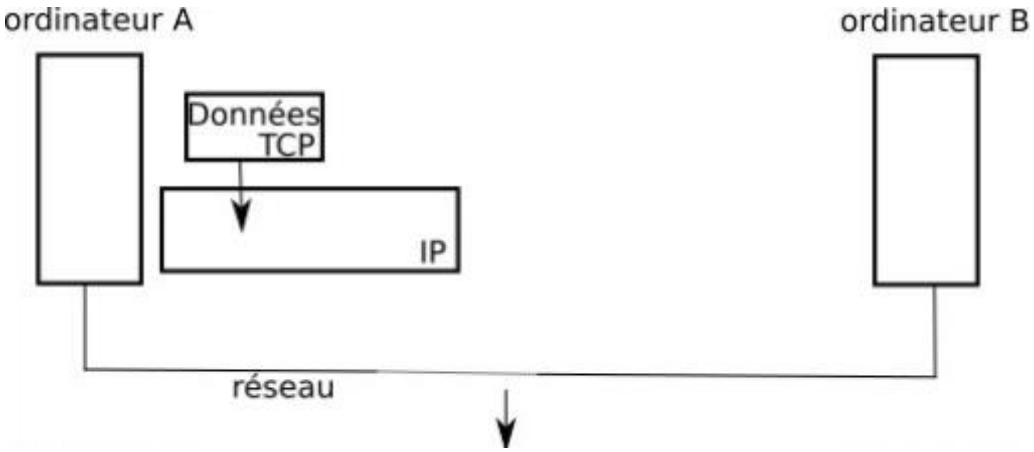


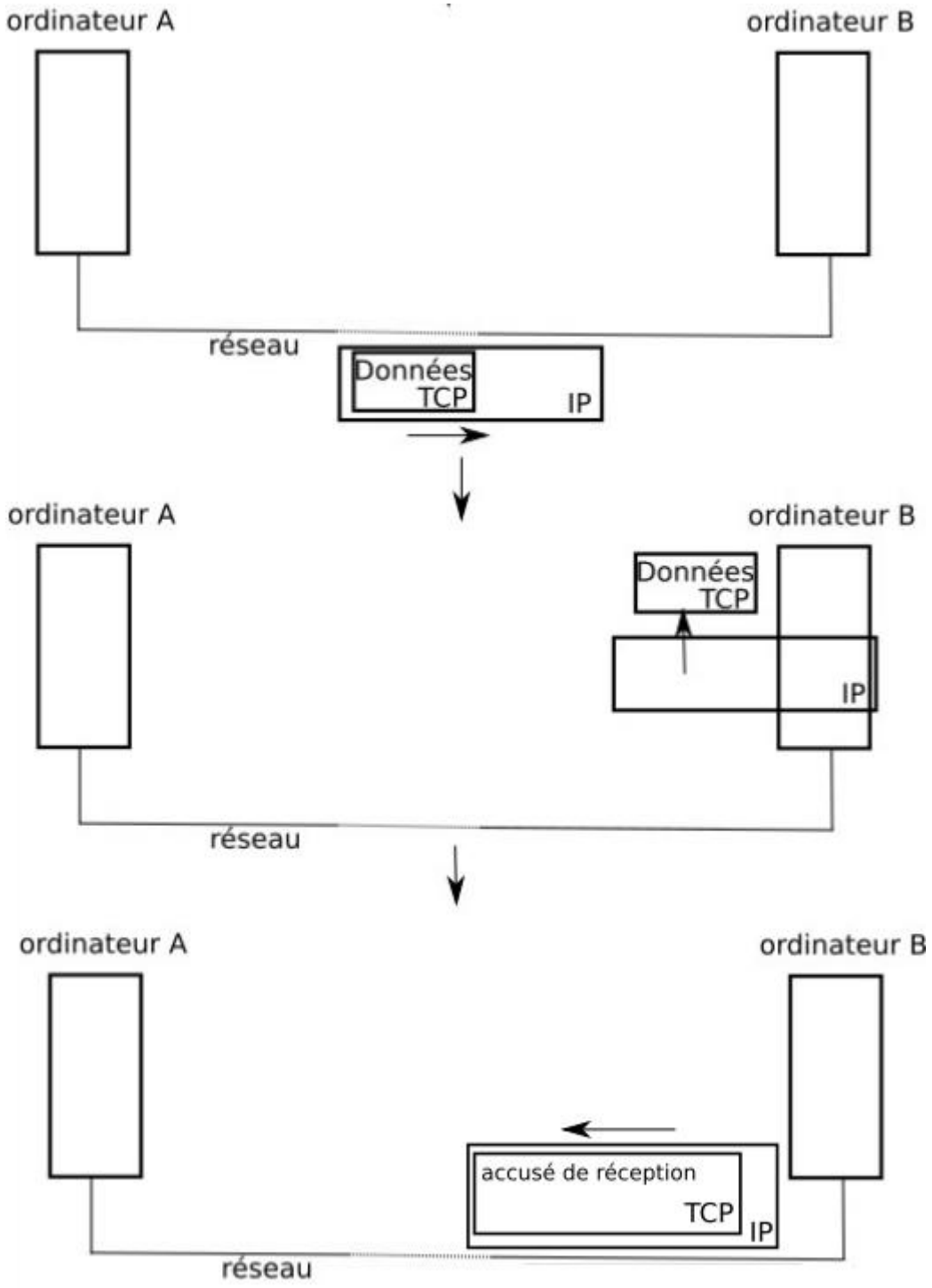
Le protocole IP s'occupe uniquement de faire arriver à destination les paquets en utilisant l'adresse IP de l'ordinateur de destination. Les adresses IP de l'ordinateur de départ (ordinateur A) et de l'ordinateur destination (ordinateur B) sont ajoutées aux paquets de données.



Le protocole TCP permet de s'assurer qu'un paquet est bien arrivé à destination. En effet quand l'ordinateur B reçoit un paquet de données en provenance de l'ordinateur A, l'ordinateur B envoie un accusé de réception à l'ordinateur A (un peu dans le genre "OK, j'ai bien reçu le paquet"). Si l'ordinateur A ne reçoit pas cet accusé de réception en provenance de B, après un temps prédéfini, l'ordinateur A renverra le paquet de données vers l'ordinateur B.

On peut donc résumer le processus d'envoi d'un paquet de données comme suit :





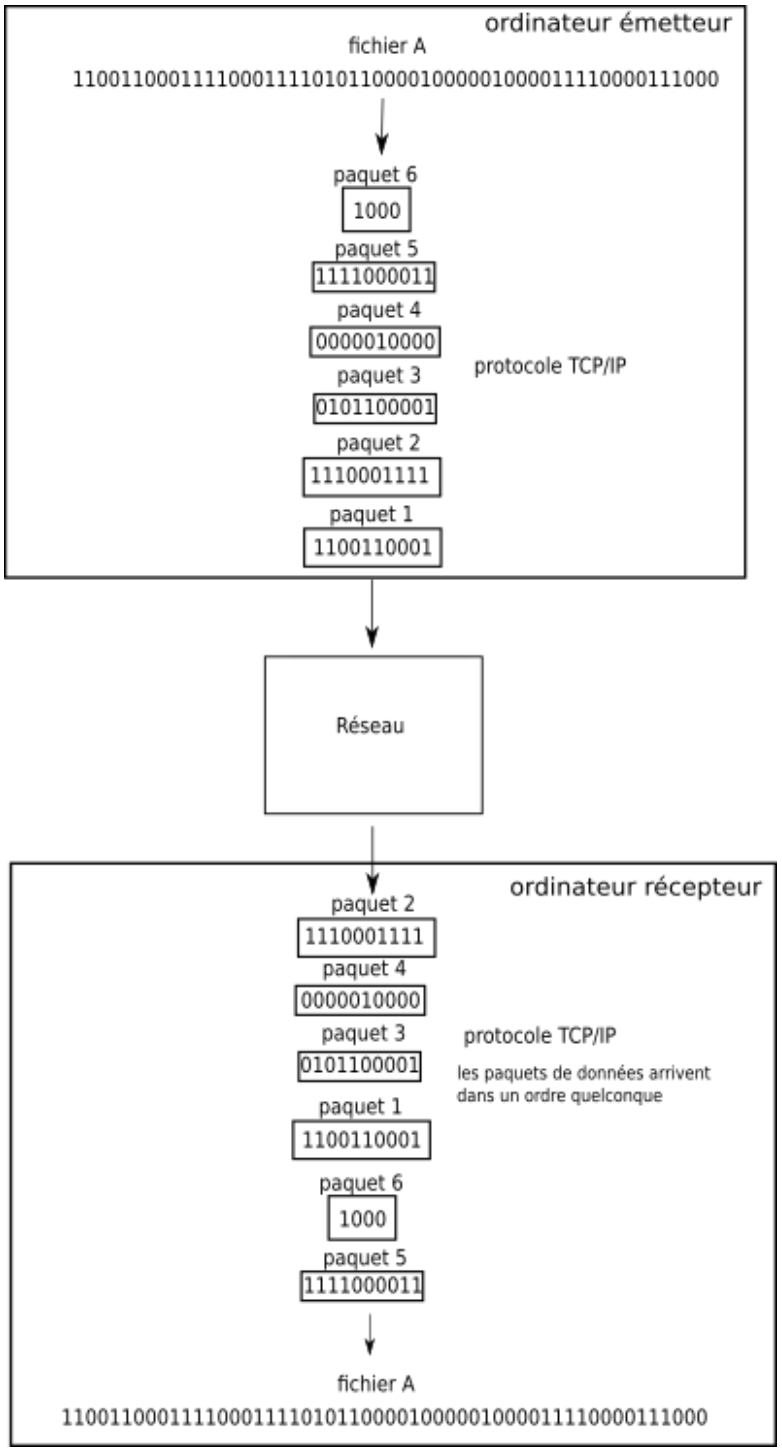
À noter qu'il existe aussi le **protocole UDP** qui ressemble beaucoup au protocole TCP. La grande différence entre UDP et TCP est que le protocole UDP ne gère pas les accusés de réception. Les échanges de données avec UDP sont donc moins fiables qu'avec TCP (un paquet "perdu" est définitivement "perdu" et ne sera pas renvoyé) mais beaucoup plus rapides (puisqu' il n'y a pas d'accusé de réception à transmettre).

UDP est donc très souvent utilisé pour les échanges de données qui doivent être rapides, mais où la perte d'un paquet de données de temps en temps n'est pas un gros problème (par exemple le streaming vidéo, certains jeux en ligne type MMORPG).

Il est très important de bien comprendre que TCP/IP repose sur la notion **de paquets de données**. Si par exemple on désire envoyer un fichier (son, photo, vidéo ou texte, peu importe, dans tous les cas on envoie une succession de bits) en utilisant TCP/IP, les données qui constituent ce fichier ne seront pas envoyées d'un seul tenant, ces données vont être "découpées" en plusieurs morceaux et chaque morceau sera envoyé dans un paquet différent.

Une fois tous les paquets arrivés à destination, le fichier d'origine pourra être reconstitué. Pour aller d'un ordinateur A à un ordinateur B, les **différents paquets** contenant les données qui constituent notre fichier, **ne passeront pas forcement par la même route** (en fonction de l'encombrement du réseau ou d'une panne subite d'un routeur), ils pourront emprunter des chemins très différents : en exagérant à peine, pour faire le trajet Paris-Los Angeles, certains paquets pourront passer par l'atlantique alors que d'autres passeront par le pacifique.

Si un des paquets n'arrive pas à destination, le fichier ne pourra pas être reconstitué, le paquet "perdu" devra être renvoyé par l'émetteur (voir le système d'accusé de réception décrit ci-dessus).

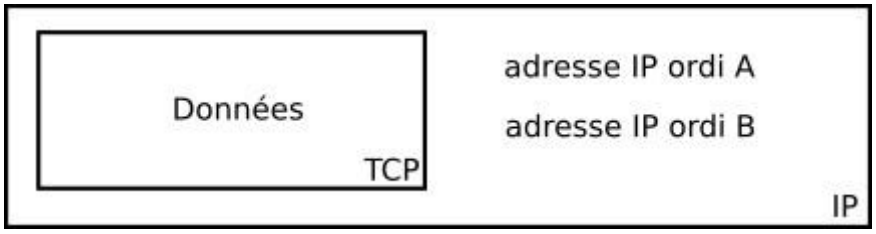


3/ Trame Ethernet

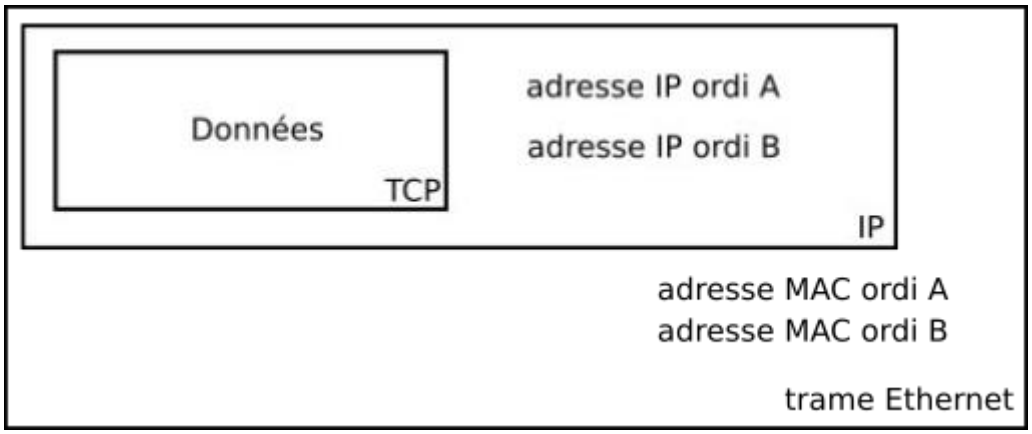
Les paquets IP ne peuvent en réalité pas transiter sur un réseau tel quel, ils vont eux aussi être encapsulés avant de pouvoir "voyager" sur le réseau. L'encapsulation des paquets IP produit ce que l'on appelle une **trame**. Il existe de nombreux types de trames : ATM, token ring, PPP, Ethernet, Wifi... On évoquera les 2 dernières : la **trame Ethernet** et la **trame Wifi**.

Dans un réseau filaire avec des câbles Ethernet (avec des prises RJ45), la trame sera de type Ethernet (ce qui est le cas pour le réseau du lycée Saint-Jean). Si vous utilisez un réseau sans fil Wifi, la trame sera de type Wifi. En fait, la trame Wifi ressemble beaucoup à la trame Ethernet, on peut même dire que la trame Wifi est la variante sans-fil de la trame Ethernet, afin de simplifier les choses, on évoquera uniquement la trame Ethernet en ayant à l'esprit que ce qui est dit sur la trame Ethernet et aussi valable pour la trame Wifi.

Le paquet IP contient les adresses IP de l'émetteur et du récepteur :



Le paquet IP étant encapsulé par la trame Ethernet, les adresses IP ne sont plus directement disponibles (il faut désencapsuler le paquet IP pour pouvoir lire ces adresses IP), on va donc trouver un autre type d'adresse qui permet d'identifier l'émetteur et le récepteur : **l'adresse MAC** (*Media Access Control*) aussi appelée adresse physique.



Au moment de l'encapsulation d'un paquet IP, l'ordinateur "émetteur" va utiliser un **protocole** nommé **ARP** (*Address Resolution Protocol*) qui va permettre de déterminer l'adresse MAC de l'ordinateur "destination", en effectuant une requête "broadcast" (requête destinée à tous les ordinateurs du réseau) du type : "j'aimerais connaitre l'adresse MAC de l'ordinateur ayant pour IP XXX.XXX.XXX.XXX".

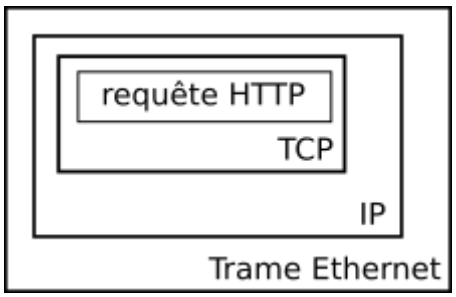
Une fois qu'il a obtenu une réponse à cette requête ARP, l'ordinateur "émetteur" encapsule le paquet IP dans une trame Ethernet et envoie cette trame sur le réseau.

4/ Couche application

Le protocole TCP permet de mettre en forme les données à envoyer :

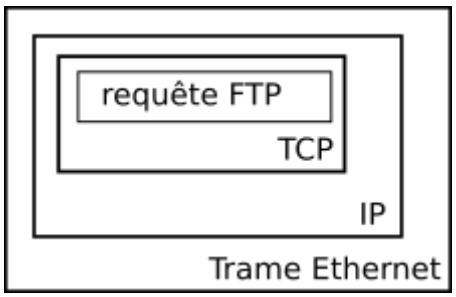
Quelle est la nature de ces données mises en forme par TCP ?

En fait, TCP effectue lui aussi une encapsulation, les données encapsulées par TCP peuvent être de plusieurs natures, par exemple celles issues d'une requêtes HTTP, elles sont encapsulés par TCP, au bout du compte et en résumé, on obtient alors ceci :



TCP encapsule aussi d'autres types de requêtes (et réponses), par exemple **FTP** (*File Transfer Protocol*) qui permet d'envoyer sur un réseau des fichiers (texte, son, image...), **SMTP** (Simple Mail Transfer Protocol) qui permet d'envoyer des emails, **DNS** (*Domain Name Server*) qui permet d'avoir la correspondance entre une adresse IP et une URL,...

Il est donc aussi possible d'avoir :



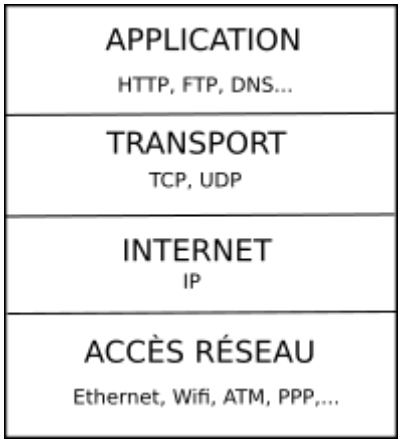
On dit que tous ces protocoles (HTTP, FTP, SMTP, DNS,...) appartiennent à la couche "Application" du modèle TCP/IP.

5/ Le modèle des couches TCP/IP

En effet, à chaque phase d'encapsulation on associe ce que l'on appelle une couche :

- comme nous l'avons vu les protocoles HTTP, FTP, SMTP, DNS,... sont associés à la couche "Application"
- les protocoles TCP et UDP sont associés à la couche "Transport"
- le protocole IP est associé à la couche "Internet"
- les trames Ethernet (ou Wifi) sont associées à la couche "Accès réseau"

On présente souvent ces différentes couchent sur ce type de schéma :



La couche du "dessous" encapsule la couche située "au-dessus". On nomme ce système de couche **"modèle de couches TCP/IP"** (car ce modèle repose principalement sur TCP et IP).

III/ Le modèle OSI

Le modèle OSI (*Open Systems Interconnection*) est une norme internationale permettant d'organiser la communication entre des systèmes informatiques, il date des années 1970.

A savoir : ce modèle contient 7 couches.

7. Application	Interface utilisateur (SMTP, HTTP, SSH...)
6. Présentation	Assure que les données sont présentées sous un format acceptable (ASCII, Unicode, JPEG...) s'occupe de compresser, coder, décoder le message
5. Session	Décide d'établir ou de terminer la connexion (*socket*), le « droit à la parole », la synchronisation...
4. Transport	Casse et reconstitue le message en segments numérotés et vérifie la fiabilité de la transmission (TCP, UDP)
3. Réseau	S'occupe du routage des paquets, du trajet entre source et destination, donne une adresse logique (IP)
2. Liaison	S'occupe des adresses physiques (MAC) des trames au niveau local (LAN)
1. Physique	Transmet de manière effective les bits (Ethernet, wifi...)

Couche 7,6,5 : le message est au bon format, doit être utilisé pour une certaine tâche et doit être transmis vers un destinataire qui peut être repéré par une adresse mail par exemple.

Couche 4 : le message est coupé en segments numérotés et avec un numéro de port qui correspond à l'application qu'il utilise (80 pour HTTP, 25 pour SMTP etc.). On vérifie si l'ordre est respecté, si chaque segment a été reçu, l'état de la connexion.

Couche 3 : les segments sont encapsulés dans des paquets IP qui contiennent en plus les adresses logiques (IP fournies selon la position dans le réseau) de la source et du destinataire, la longueur du paquet et sa durée de vie. On teste également si la source et le destinataire sont dans le même réseau.

Couche 2 : elle est atteinte lorsque le destinataire et le dernier routeur sont dans le même réseau. Une machine contient une carte physique associée à une interface réseau logique qui lui donne un nom et une adresse unique fournie par le fabricant (adresse MAC, *Media Access Control*). Le paquet, encapsulé dans une trame qui contient les adresse sources et destination à l'intérieur d'un LAN est souvent transmis à tous les membres de ce réseau.

Couche 1 : le message transite par ondes radio (Wi-Fi, bornes téléphoniques), câbles divers (RJ45,USB). Il peut être déformé en réception. Les couches supérieures vont alors effectuer des contrôles et corrections.

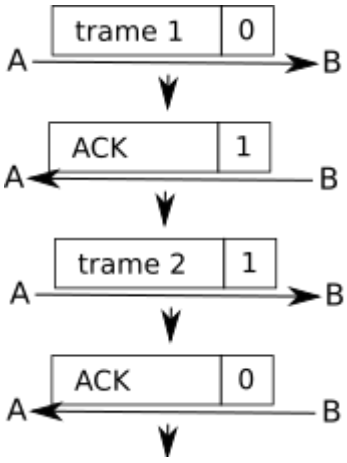
Remarque : les 4 première couches correspondent au modèle TCP/IP.

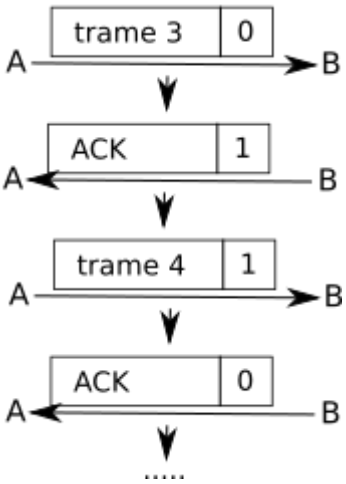
IV/ Le protocole du bit alterné

Le protocole TCP propose un mécanisme d'accusé de réception afin de s'assurer qu'un paquet est bien arrivé à destination. On parle plus généralement de **processus d'acquittement**. Ces processus d'acquittement permettent de détecter les pertes de paquets au sein d'un réseau, l'idée étant qu'en cas de perte, l'émetteur du paquet renvoie le paquet perdu au destinataire. Voici un protocole simple de récupération de perte de paquet : le **protocole de bit alterné**.

Le protocole de bit alterné est implémenté au niveau de la couche de "liaison de données" du modèle OSI (couche n°2), il ne concerne donc pas les paquets, mais les trames (on parle de paquets uniquement à partir de la couche "Réseau" (couche 3) du modèle OSI). Le principe de ce protocole est simple, considérons 2 ordinateurs en réseau : un ordinateur A qui sera l'émetteur des trames et un ordinateur B qui sera le destinataire des trames. Au moment d'émettre une trame, A va ajouter à cette trame un bit (1 ou 0) appelé drapeau (*flag* en anglais). B va envoyer un accusé de réception (*acknowledge* en anglais souvent noté ACK) à destination de A dès qu'il a reçu une trame en provenance de A. À cet accusé de réception on associe aussi un bit drapeau (1 ou 0).

La règle est relativement simple : la première trame envoyée par A aura pour drapeau 0, dès cette trame reçue par B, ce dernier va envoyer un accusé de réception avec le drapeau 1 (ce 1 signifie "la prochaine trame que A va m'envoyer devra avoir son drapeau à 1"). Dès que A reçoit l'accusé de réception avec le drapeau à 1, il envoie la 2e trame avec un drapeau à 1, et ainsi de suite...



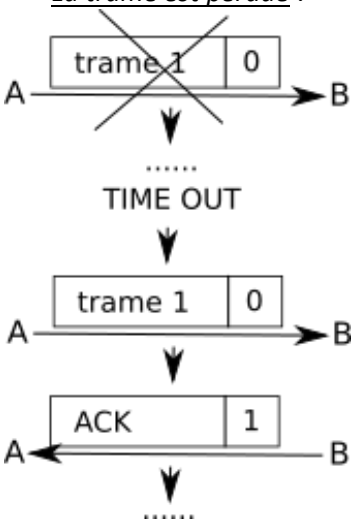


Le système de drapeau est complété avec un **système d'horloge** côté émetteur. Un "chronomètre" est déclenché à chaque envoi de trame, si au bout d'un certain temps, l'émetteur n'a pas reçu un acquittement correct (avec le bon

drapeau), la trame précédemment envoyée par l'émetteur est considérée comme perdue et est de nouveau envoyée.

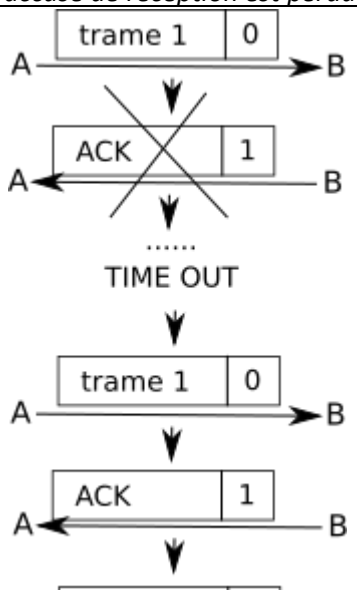
Voilà quelques cas :

La trame est perdue :



Au bout d'un certain temps ("TIME OUT") A n'a pas reçu d'accusé de réception, la trame est considérée comme perdue, elle est donc renvoyée.

L'accusé de réception est perdu :



A ne reçoit pas d'accusé de réception avec le drapeau à 1, il renvoie donc la trame 1 avec le drapeau 0. B reçoit donc cette trame avec un drapeau à 0 alors qu'il attend une trame avec un drapeau à 1 (puisqu'il a envoyé un accusé de réception avec un drapeau 1), il "en déduit" que l'accusé de réception précédent n'est pas arrivé à destination : il ne tient pas compte de la trame reçue et renvoie l'accusé de réception avec le drapeau à 1. Ensuite, le processus peut se poursuivre normalement.

Dans certaines situations, le protocole de bit alterné ne permet pas de récupérer les trames perdues, c'est pour cela que ce protocole est aujourd'hui remplacé par des protocoles plus efficaces, mais aussi plus complexes.