

---

## - Architectures matérielles et systèmes d'exploitation -



---

# LE MODÈLE INTERNET ET LE MODÈLE OSI

---

## Plan du chapitre

---

### I. HISTORIQUE

### II. LES ÉCHANGES DE DONNÉES SUR INTERNET VIA LES PROTOCOLES TCP/IP

1. *La fragmentation des données*
2. *L'encapsulation des données*
3. *Le transport des données sur le réseau*
4. *La désencapsulation des données*
5. *L'assemblage des données des paquets TCP.*

### III. LE MODÈLE DES COUCHES INTERNET (modèle TCP/IP)

1. *La trame Ethernet – Nécessité d'une adresse MAC*
2. *Le protocole ARP*
3. *Couche application*
4. *Le modèle des couches internet*

### IV. LE MODÈLE DES COUCHES OSI

## I. HISTORIQUE

---

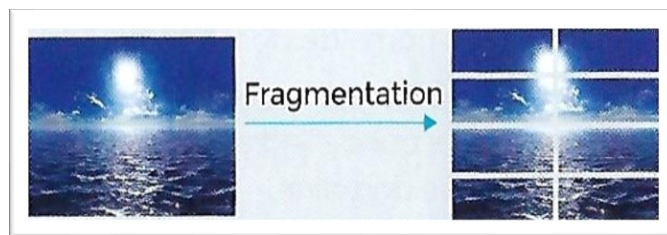
- 1958 : En pleine guerre froide, Eisenhower crée l'agence gouvernementale américaine DARPA (Defense Advanced Research Projects Agency) dont le but de veiller à la constante suprématie scientifique et technologique des États-Unis.
- 1962 : La DARPA soutient le projet du professeur Licklider qui a pour 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).
- 1968 : naissance d'ARPAnet, le 1er réseau informatique à grande échelle de l'histoire. Le 29 octobre 1969, le 1er message (le simple mot "login") est envoyé depuis l'université de Californie à Los Angeles vers l'université de Stanford via ce réseau.
- début des années 1970 : Le réseau Arpanet comporte une vingtaine d'ordinateurs et d'autres réseaux voient le jour en parallèle. Le souci est que 2 ordinateurs appartenant à 2 réseaux différents sont incapables de communiquer entre eux car ils n'utilisent pas les mêmes protocoles : il s'agit de règles communes de communication entre plusieurs machines.
- 1974 : Afin de résoudre ce problème, Vint Cerf et Bob Khan mettent au point le protocole TCP qui sera très rapidement couplé au protocole IP pour donner TCP/IP. Grâce à sa simplicité, il va très rapidement s'imposer comme un standard. Les différents réseaux peuvent alors être interconnectés : Internet est né ! (le terme Internet vient de "internetting" qui signifie "Connexion entre plusieurs réseaux"). TCP/IP est donc au cœur d'Internet, voilà pourquoi aujourd'hui, la plupart des machines utilisent TCP/IP.

[Retour au plan](#)

## II. LES ÉCHANGES DE DONNÉES SUR INTERNET VIA LES PROTOCOLES TCP/IP

### 1. La fragmentation des données

Sur internet, avant d'être envoyées les données (par exemple une photographie, un morceau de musique...) sont fragmentées, c'est-à-dire découpées en morceaux de plus petite taille. C'est le **protocole TCP** qui est chargé de cette tâche. Grâce à cette fragmentation, la taille des données envoyées n'est pas limitée.



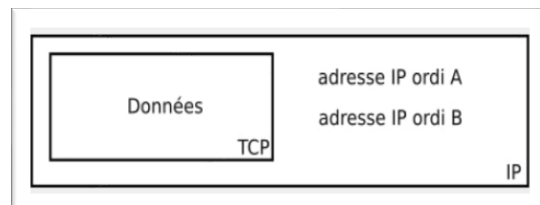
[Retour au plan](#)

### 2. L'encapsulation des données

Les fragments doivent être numérotés (eh oui, à la réception, il faudra bien être en capacité reconstituer l'image finale !). Les données (data) seront alors encapsulées dans un **paquet de données TCP** qui comportera un en-tête indiquant le n° du paquet (et d'autres informations : nombre total de paquets, délai avant destruction ...).

Ensuite ce paquet est de nouveau encapsulé dans un **paquet de données IP** qui lui contiendra dans son en-tête l'adresse IP de l'émetteur (ordinateur A) et l'adresse IP du récepteur (ordinateur B). C'est le **protocole IP** qui est chargé de cette tâche. Un paquet de données IP (en-tête compris) a une taille moyenne de 128 ou 256 octets.

*Remarque :* quand on envoie un courrier par la poste, on l'encapsule aussi dans une enveloppe sur laquelle est inscrite l'adresse du récepteur mais aussi de l'expéditeur.



[Retour au plan](#)

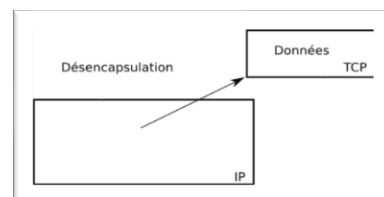
### 3. Le transport des données sur le réseau

Les paquets de données pourront alors commencer leur long voyage sur le réseau jusqu'à l'ordinateur B. Nous verrons plus tard que sur Internet les paquets peuvent emprunter des chemins différents, c'est pourquoi ils sont généralement réceptionnés par l'ordinateur B dans le désordre. C'est le protocole IP (Internet Protocol) qui est chargé de l'acheminement des données à leur destinataire.

[Retour au plan](#)

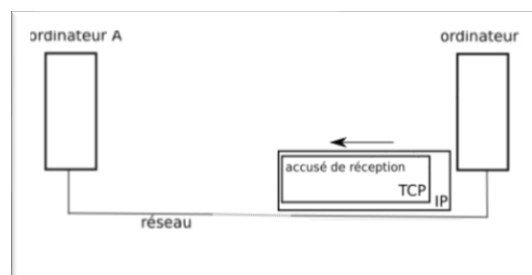
### 4. La désencapsulation des données

Une fois arrivées à destination (ordinateur B), le paquet IP est "désencapsulé" : on récupère alors le paquet TCP qui sera désencapsulé à son tour afin de récupérer les données.



Le protocole TCP (Transmission Control Protocol) permet de s'assurer que l'ensemble des paquets est bien arrivé à destination (l'en-tête du paquet TCP comporte le nombre total de paquets). A chaque réception d'un paquet, l'ordinateur B renvoie un accusé de réception à l'ordinateur A. 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. Un éventuel paquet perdu sera détruit au bout d'un temps déterminé indiqué dans l'entête du paquet TCP.

Grâce au protocole TCP, l'envoi des données est **fiable** : le message finira arriver, mais **sans aucune garantie temporelle**. Il existe un protocole UDP très proche du protocole TCP, mais celui-ci ne gère pas les accusés de réception. Les échanges de données avec UDP sont donc plus rapides mais moins fiables qu'avec TCP (un paquet "perdu" ne sera pas renvoyé). On utilise ce protocole par exemple pour le streaming vidéo où la perte d'un paquet n'a pas une importance capitale.

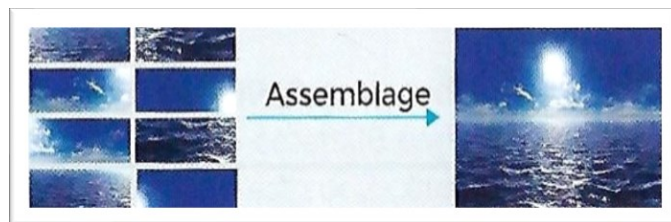


[Retour au plan](#)

## 5. L'assemblage des données des paquets TCP.

Grâce à la numérotation des paquets TCP, le protocole correspondant va être en mesure de réassembler dans l'ordre la globalité des données.

[Retour au plan](#)



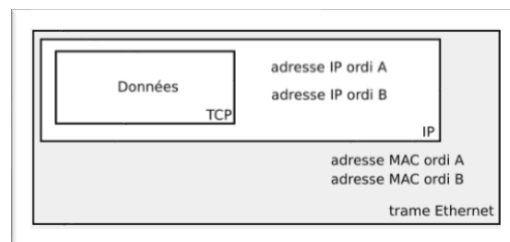
## III. LE MODÈLE DES COUCHES INTERNET (modèle TCP/IP)

### 1. La trame Ethernet – Nécessité d'une adresse MAC

Nous venons de voir que les données sont encapsulées par le protocole TCP, puis de nouveau encapsulées par le protocole IP. En fait, les paquets IP ne peuvent pas transiter sur un réseau tel quel, ils vont eux aussi devoir 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... Nous allons uniquement évoquer les 2 dernières : la trame Ethernet (pour les réseaux filaires) et la trame Wifi (pour les réseaux wifi). La trame Wifi est la variante sans-fil de la trame Ethernet, ce qui sera dit sur la trame Ethernet sera aussi valable pour la trame Wifi.

Les paquets IP étant encapsulés par les trames Ethernet, les adresses IP ne sont plus directement disponibles, c'est-à-dire qu'il faudra désencapsuler le paquet IP pour pouvoir lire ces adresses IP. Il est donc indispensable d'utiliser un autre type d'adresse qui permet d'identifier l'émetteur et le récepteur : l'adresse MAC (Media Access Control) aussi appelée adresse physique.



Les adresses MAC sont codées sur 6 octets. Elles sont généralement écrites en hexadécimal, chaque octet est séparé par 2 points (exemple d'adresse MAC : 00:E0:4C:68:02:11). Les adresses MAC sont liées au matériel, chaque carte réseau (Ethernet ou Wifi) possède sa propre adresse MAC, il n'existe pas dans le monde 2 cartes réseau qui possèdent la même adresse MAC. Les 3 premiers octets d'une adresse MAC ("00:E0:4C" dans l'exemple ci-dessus) désignent le constructeur du matériel, par exemple, "00:E0:4C" désigne le constructeur "realtek semiconductor corp".

[Retour au plan](#)

### 2. Le protocole ARP

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 connaître 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.

[Retour au plan](#)

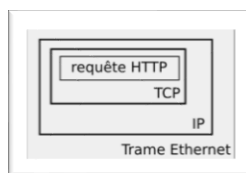
### 3. Couche application

Nous avons vu que le protocole TCP permet de mettre en forme les données à envoyer :  
Quelle est la nature de ces données mises en forme par TCP ?

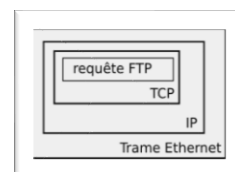


En fait, TCP effectue lui aussi une encapsulation des données qui peuvent être de plusieurs natures :

- Une requête http (voir cours sur le web) ;



- Une requête FTP (File Transfer Protocol) qui permet d'envoyer sur un réseau des fichiers (texte, son, image...) ;



- Une requête SMTP (Simple Mail Transfer Protocol) qui permet d'envoyer des emails ;
- Une requête DNS (Domain Name Server) qui permet d'avoir la correspondance entre une adresse IP et une URL
- ...

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

[Retour au plan](#)

#### 4. Le modèle des couches internet

À chaque phase d'encapsulation on associe ce que l'on appelle une couche :

- Les protocoles HTTP, FTP, SMTP, POP, IMAP, 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 "Réseau", parfois appelée "couche internet"
- Les trames Ethernet (ou Wifi) sont associées à la couche "Liaison", encore appelée couche "accès réseau".

On présente souvent ces différentes couches avec le modèle suivant, nommé "modèle des couches internet " ou encore "modèle TCP/IP" :

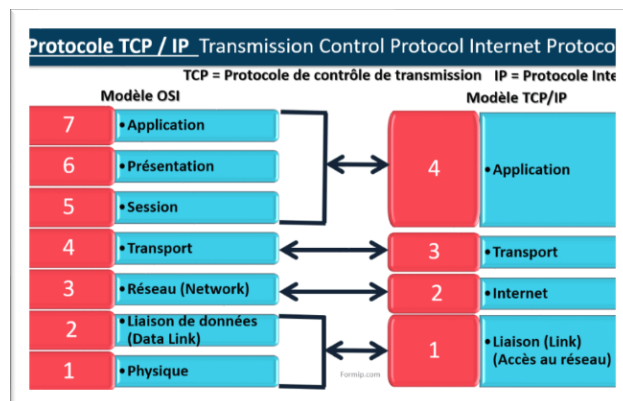
4	Couche application HTTP, FTP, SMTP, POP, IMAP, DNS...
3	Couche Transport TCP, UDP ...
2	Couche réseau (couche Internet) IP, ARP
1	Couche liaison (couche accès réseau) Trames Ethernet, Wifi...

[Retour au plan](#)

## IV. LE MODÈLE DES COUCHES OSI

Il existe un autre modèle de couche, le modèle OSI (Open Systems Interconnection), ce système est antérieur au modèle TCP/IP puisqu'il date des années 1970. Ce modèle est principalement théorique et a permis de poser les bases des communications réseau. Ce modèle est composé de 7 couches, alors que le modèle TCP/IP est composé de seulement 4 couches.

Il existe des liens entre le modèle OSI et le modèle TCP/IP (voir schéma ci-contre), mais parfois comparer les 2 modèles peut être délicat.



[Retour au plan](#)

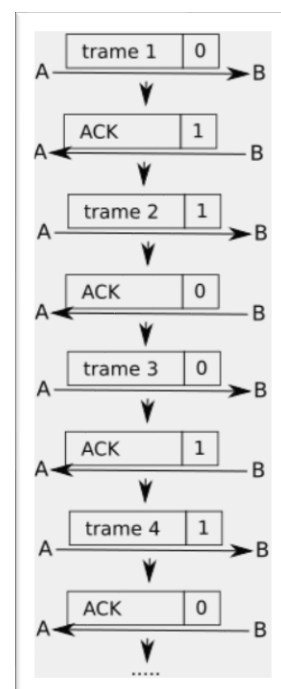
## V. LE PROTOCOLE DE BIT ALTERNÉ

Le protocole TCP propose un mécanisme d'accusé de réception (processus d'acquittement) afin de s'assurer qu'un paquet est bien arrivé à destination. Ce processus détecte 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.

Le protocole de bit alterné est implémenté au niveau de la couche de "liaison" (couche 1) du modèle internet, il ne concerne donc pas les paquets, mais les trames.

**Principe :** Considérons 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 : 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 la trame en provenance de A. À cet accusé de réception B va associer un bit drapeau de 1 (cela signifie que la prochaine trame envoyée par A devra avoir le drapeau 1)
- Dès que A reçoit l'accusé de réception avec le drapeau à 1, il envoie la 2<sup>ème</sup> 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 (avec le même drapeau que la précédente).

Ce protocole est aujourd'hui remplacé par des protocoles plus efficaces, mais aussi plus complexes.