

## Modele OSI et TCP/IP

### 1.1 Intro et rappel

On a vu (reseau 1) :

- le reseau local présente un système repartit avec des machines reliées souvent en étoile
- le reseau internet est un reseau de reseau ; c'est un système distribué, modélisé par un graphe
- les machines possèdent 2 type d'identifiants, MAC et IP (v4 et v6)
- des protocoles s'assurent de la bonne livraison des données sur internet, s'assurent qu'il n'y ait pas de collision des données
- l'un de ces protocoles est celui du bit alterné

video cookie connecté

### 1.2 Les données qui circulent sur internet

Internet manipule deux types d'information :

- les contenus envoyés
- des identifiants : les adresses du destinataire et de l'émetteur. Plus des identifiants numériques nécessaires au transport du paquet lui-même

Ces deux types d'information sont regroupées dans des *paquets de taille fixe*, de façon uniforme et *indépendante du type de données* transportées : texte, images, sons, vidéos, etc.

### 1.3 Principe du modèle OSI

Le modèle OSI est une norme qui préconise comment les ordinateurs devraient communiquer entre eux avec 5 *couches* technologiques adjacentes, numérotées selon leur *distance* au support d'émission (la couche n°1).

Les couches forment une hiérarchie qui va de l'application (HTTP, FTP etc...) jusqu'au support physique (cable coaxial, ondes etc...) :

Ce sont : **application (5, 6, 7), transport (4), reseau (3), liaison(2), physique (1).**

Ce modèle OSI (un modèle théorique) a été conçu pour cloisonner les différents processus, langages et technologies employés.

Combien de couches ? :

Selon le degré de description, on parle plutôt du modèle TCP/IP en 4 couches.

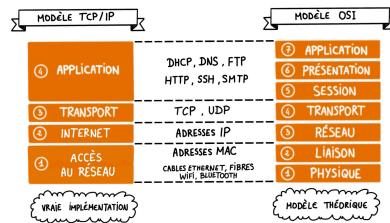


FIGURE 1 – illustration du TCP/IP - youtube - Cookie connecté

\*Quelles applications pour quelle couche ?:

Les 2 schémas ci-contre illustrent le découpage couche-application.

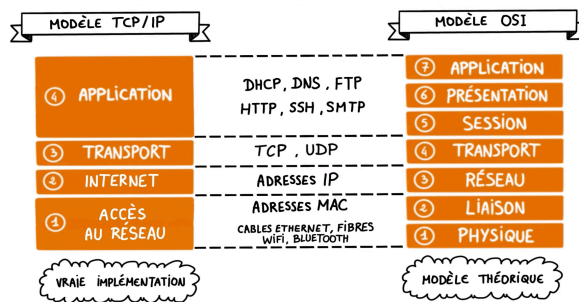


FIGURE 2 – couches - applications

SSH et SSL sont deux technologies qui permettent de chiffrer et d'authentifier les données qui passent entre deux ordinateurs. Ce sont des applications de la couche 5. Ces données sont chiffrées avant leur mise en forme pour le transport. Pour approfondir : différence entre SSH et SSL sur [kinsta.com](http://kinsta.com)

Quelles sont les liens entre couches ?

Le modèle OSI ajoute deux règles plus générales entre les couches :

- chaque couche est indépendante ;
- chaque couche ne peut communiquer qu'avec une couche adjacente.

Lors de l'émission d'une requête par une application, celle-ci doit traverser toutes les couches, depuis la 7 (application), puis de la 4 vers la 1 ; durant le trajet les données subiront des modifications et chaque couche rajoutera ce qu'elle voudra (généralement des en-têtes) pour mieux exercer sa fonction, mais pas seulement (la couche 1, de transport concerne... le transport).

Ce mécanisme s'appelle l'**encapsulation** : la trame de données numériques est constituée de plusieurs parties distinctes et mises dans un ordre particulier. Au final, ce qui va circuler sur le réseau est une trame de couche 2, qui contient le datagramme de couche 3 (qui lui-même contiendra l'élément de couche 4)

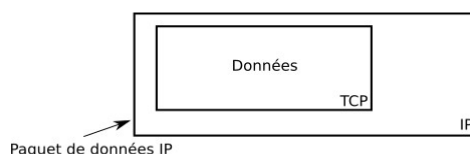


FIGURE 3 – encapsulation

Lors de la réception c'est exactement l'inverse qui se produit (désencapsulation).

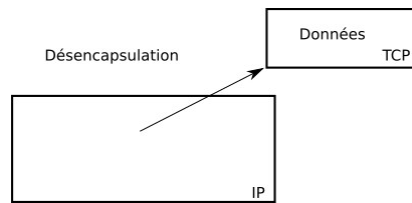
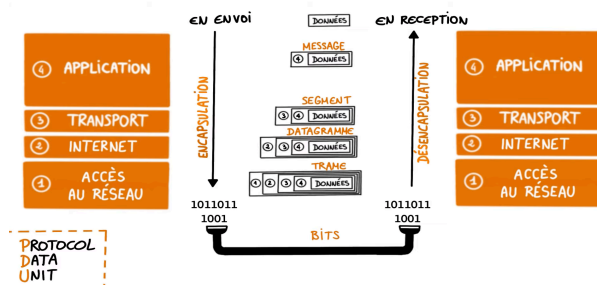


FIGURE 4 – désencapsulation

Prenons un exemple simple, vous demandez à votre navigateur de charger votre site préféré [www.informatix.fr](http://www.informatix.fr). Vous êtes reliés à un modem par un câble à paires torsadées.



#### 1.4 couche application

Le navigateur demande au système d'envoyer une requête HTTP (couche 7). Dans cette couche, le logiciel lui-même n'en fait pas partie. Cette couche concerne l'interface entre le logiciel et la couche de transport, et transporte l'information du **protocole application** utilisé (ici http par exemple, c'est à dire le protocole lié à l'affichage des pages html)

A ce moment, le paquet est un *message*

Sortie : [requête HTTP]

#### 1.5 couche de transport

La requête arrive dans TCP qui ajoute son en-tête. Le protocole TCP va mettre en forme les données à envoyer et ajouter son en-tête. Ici, les numéros d'identification sont

- les **port source et le port destination**, qui identifient les **applications** qui entrent en jeu dans la communication.
- le numéro de séquence initial, **ISN**, appelé aussi **SYN**
- et celui d'accusé de réception **ACK** (le numéro du prochain octet des données attendues). Ces numéros vont permettre d'établir une communication avec accusés de réception (pour TCP, pas UDP) et de s'assurer, en principe, de l'identité de la machine avec qui les données sont échangées (avec le numéro de séquence, nécessaire pour l'accusé de réception).
- L'en-tête contient aussi un *checksum*.

A ce moment, le paquet est un *segment TCP*

Sortie : [en-tête TCP][requête HTTP]

## 1.6 couche réseau

Le segment TCP arrive dans IP qui ajoute aussi son en-tête :

- **adresse IP** (pour le **routing**)
- celle du serveur demandé.
- La couche 3 indique à la couche 2 quel protocole a été utilisé (TCP, UDP...).
- Il y a aussi un numéro de connexions établies (IPID) sur le port en question
- et d'autres informations qui servent à l'éventuelle fragmentation du datagramme (les données ne peuvent pas excéder 1500 octets).
- Une autre valeur transportée est le **TTL** (time to live) qui évite que le paquet ne circule indéfiniment sur les réseaux.

A ce moment, le paquet est un *datagramme IP*

Sortie : [en-tête IP][en tête TCP][requête HTTP].

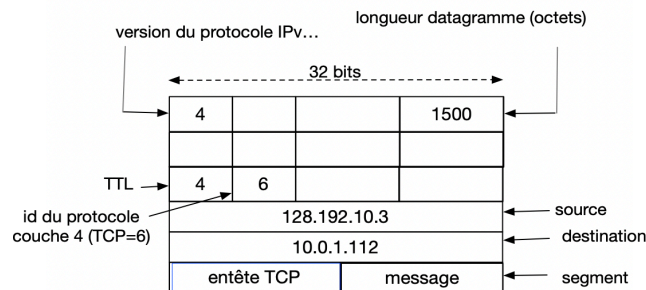


FIGURE 5 – modèle simplifié du datagramme

## 1.7 couche physique

Le paquet IP arrive dans Ethernet qui ajoute un en-tête (qui contient entre autres :

- votre **adresse MAC** - pour le **switch**
- et un **checksum** (vérification d'erreurs CRC).

La couche 2 peut alors former la *trame* et l'envoyer sur le réseau.

Il va ajouter l'adresse MAC de l'émetteur et du destinataire, qu'il aura résolu grâce aux tables de routage et la *table arp* (côté serveur).

Sortie : [en-tête Ethernet][en-tête IP][en tête TCP][requête HTTP][checksum Ethernet].

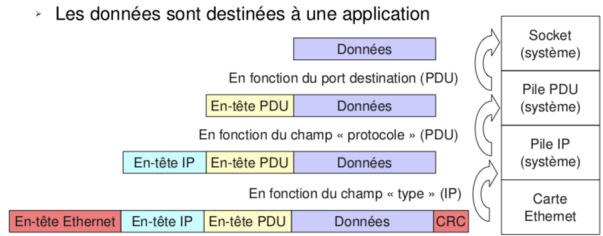
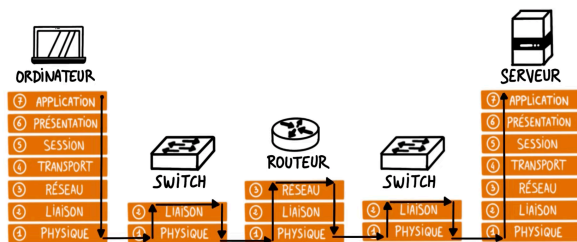


FIGURE 6 – en-tête Ethernet

Lors du transport, chaque machine va désencapsuler les informations de la partie Ethernet et les remplacer par de nouvelles informations pour assurer le transport jusqu'à la prochaine étape.



Seule la machine de destination va accéder au contenu.