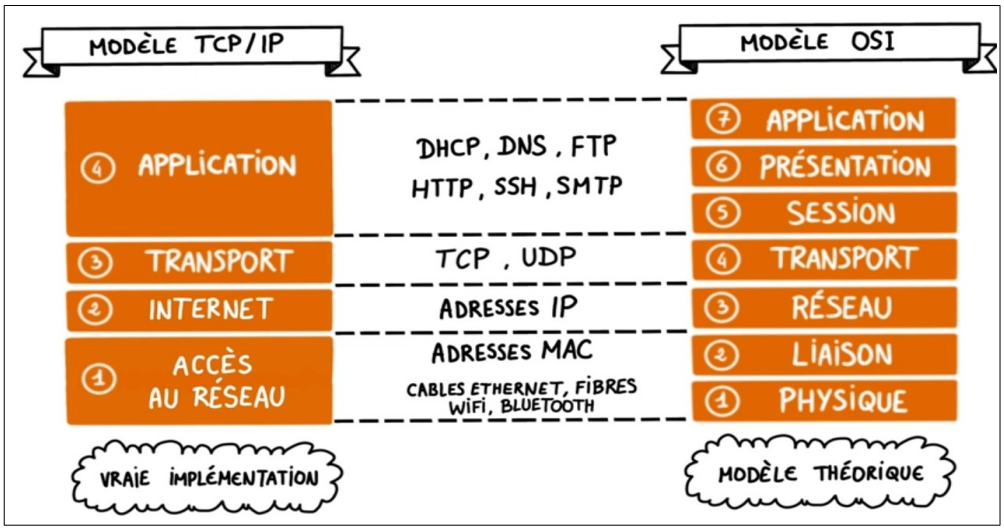
II. Le modèle TCP/IP (Transmission Control Protocol / Internet Protocol)

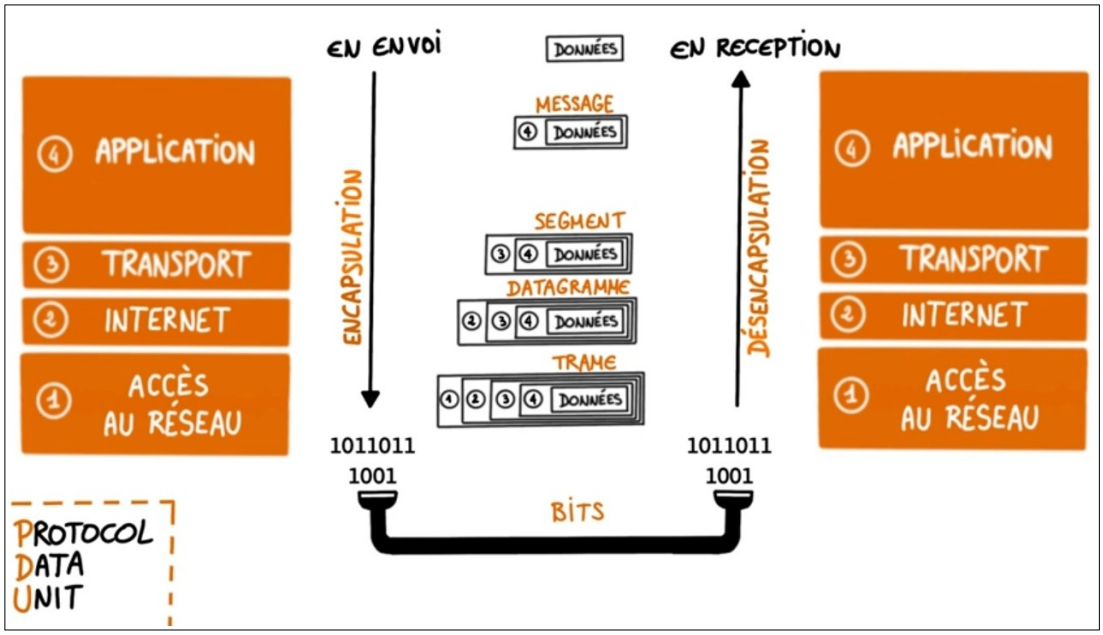
A noter que le modèle OSI est un modèle conceptuel, utilisé principalement pour la compréhension au niveau de la communication réseau des systèmes informatiques. Le problème c'est que cette modèle est très segmentée puisque certaine couche peut faire le travail des autres. D'où l'idée de la création de la modèle TCP/IP qui factorise les couches qui est (a peu près) le meme rôle (voir le schéma ci-dessous)

Le modèle TCP/IP simplifie le modèle OSI en 4 couches



MODÈLE TCP/IP	
Couche 4 - **Application**	Comme son nom l'indique, il s'agit des applications (les protocoles le plus utilisé dans cette couche sont : DHCP, DNS, FTP, HTTP, SSH et SMTP).
Couche 3 - **Transport**	Elle utilise la protocole TCP pour un transport fiable en mode connecté et UDP pour un service de transmission de datagrammes.
Couche 2 - **Internet**	Le protocole le plus utilisé de la couche Internet est l'IP (Internet Protocole) qui gère le routage, IP assure l'acheminement des paquets depuis une source vers une destination.
Couche 1 - **Acces au réseau**	Selon la modèle TCP/IP, cette couche s'occupe seulement la connexion physique entre 2 ou plusieurs terminaux.

Encapsulation | Desencapsulation | PDU



EXPLICATION	
Encapsulation (en émission) [couche 4 vers 1]	**Desencapsulation** (en réception) [couche 1 vers 4]
En émission, les données traversent chacune des couches au <u>niveau de la machine émettrice</u> et a chaque couche, une information est **ajoutée** au paquet de données, il s'agit **d'une entête,** ce dernière définit le protocole a utiliser dans la machine réceptrice	<u>Au niveau de la machine réceptrice</u>, lors du passage dans chaque couche, **l'entête est lue, interprétée et puis supprimée** puis a la fin (c'est a dire dans la couche application), les données sont dans son état de départ. => C'est la procédure inverse de l'encapsulation

PDU (**P**rotocol **D**ata **U**nit)

En passant par chaque couche, le paquet de données change d'aspect car on lui ajoute une entête. Ainsi les appellations change pour chaque aspect :

- **Données** : *aspect original lors de l'émission | aspect final lors de la réception*
- **Message** (c. application)
- **Segment** (TCP)
- **Datagramme** (c. internet)
- **Trame** (c. accès réseau)
- **Bits** (c. physique) : *aspect original lors de la réception*

Adressage

DHCP **(Dynamic Host Configuration Protocol)** **:** un serveur possédant un système qui assigne une adresse IP a chaque appareil connecte sur le réseau. (un routeur peut jouer le meme rôle)

Adresse IP **(Internet Protocol)** **:** un nombre binaire de 32bits, exprimées en 4 nombres en base 10, compris entre 0 et 255, séparés par des points qui sert a l'identification de manière unique d'une appareil dans un réseau TCP/IP.

1 adresse = 4octets = 4 * 8bits = 32bits

Adresse réseau (adresse du serveur) != Adresse IP (adresse du client/machine) != Adresse de diffusion (broadcast)

Classe de réseau :

Classe	Plage (1er octet)	Adresse IP (en base 10 pointé)	ID réseau	ID hôte	Masque de sous réseau
Classe A	1-127	0wwwwwww.xxxxxxxx.yyyyyyyy.zzzzzzzz	w.	x.y.z	255.0.0.0
Classe B	128-191	10wwwwww.xxxxxxxx.yyyyyyyy.zzzzzzzz	w.x.	y.z	255.255.0.0
Classe C	192-223	110wwwww.xxxxxxxx.yyyyyyyy.zzzzzzzz	w.x.y.	z	255.255.255.0

Les opérations basiques sur les adresses :

>> Calcul en binaire d'une adresse IP <<

Si Adresse IP = 192.168.21.10 *(Classe C)*

En binaire :

	128	64	32	16	8	4	2	1
192 →	1	1	0	0	0	0	0	0
168 →	1	0	1	0	1	0	0	0
21 →	0	0	0	1	0	1	0	1
10 →	0	0	0	0	1	0	1	0

=> Donc 192.168.21.10 = 11000000.10101000.00010101.00001010

>> Calcul d'hôte & calcul sous-réseau <<

Q°: Afin de disposer de sous-réseau, on utilise le masque ci-dessous, quel est la classe de l'adresse et combien d'hôtes porra-t'il y avoir pour un sous-réseau?

[Exemple 1] *Si Mask = 255.255.240.0* *(Classe B)*

On travail sur l'ID hôte du masque sous réseau

* ID hote (mask) = 240.0
* Conversion en binaire de la partie hôte : 240.0 = 11110000.00000000

Nombre d'hôte => nbr(0) = 12bits
Sous-réseau => nbr(1) = 4bits

=> nombre d'hôte = 2^{12} - 2 = 4094 **hôtes**
=> sous-réseau = 2^4 = 16 **sous-réseau**

Q°: Un réseau a comme masque 255.255.255.244, quel est la classe réseau et combien de machines peut-il y avoir sur un tel réseau?

[Exemple 2] *Si Mask = 255.255.255.224* *(Classe C)*

* ID hôte (mask) = 224
* Conversion en base 2 de 224: 11100000

nbr(0) = 5bits | nbr(1) = 3bits

=> nombre d'hôte = 2^5 - 2 = 30 **hôtes**
=> sous-réseau = 2^3 = 8 **sous-réseau**

>> Calcul adresse broadcast (adresse de diffusion) & calcul de l'adresse réseau <<

Q°: Un réseau a comme adresse 180.35.128.0 de masque 255.255.240.0. Quelle est l'adresse de diffusion ou broadcast ?

Adresse réseau = 180.35.128.0 (Classe B) => On conserve les 2 premiers octet (180.35) pour le résultat
Mask = 255.255.240.0

On travail sur l'ID hôte de l'adresse réseau et celle du masque sous réseau

* On sait que pour une adresse de Classe B, la masque sous réseau est 255.255.0.0
* Ici, on a 255.255.240.0 (on prend les 2 derniers octet => 240.0)
* Ainsi, pour l'adresse 180.35.128.0 => 128.0

On obtient:

L'ID hote (mask) sert pour référencer mais l'opération se fait sur l'ID hôte (IP)

* ID hote (mask) = 240.0 = 1111(0000.00000000) reference
* ID hote (IP) = 128.0 = (1000)0000.00000000 reste inchangé et les autres vers 1
(AND) 10001111.11111111 => 143.255 (2 dernier octet)

* On sait que la partie réseau de l'adresse = 180.35
=> Adresse broadcast = 180.35.143.255

Q°: Une machine a comme adresse IP de 150.56.188.80 et se trouve dans un réseau dont le masque est 255.255.240.0 Quelle est l'adresse réseau ?

Adresse IP = 150.56.188.80 (Classe B) => On conserve les 2 premiers octet (150.56) pour le résultat
Mask = 255.255.240.0

On fait juste une opération logique (AND) sur l'ID hote (mask) et l'ID hote (IP)

* ID hote (mask) = 240.0 => 11110000.00000000
* ID hote (IP) = 188.80 => 10111100.01010000
(AND) 10110000.00000000 => 176.0 (en décimal pointe)

=> Adresse réseau = 150.56.176.0

>> Découpage d'un réseau & nouveau mask <<

Q°: On découpe un réseau dont le masque est 255.255.224.0 en 8 sous-réseau. Quel est le nouveau masque?

* On cherche la puissance de 2 >= 8
* Ici, $8 = 2^3$ (Alors 3bits qui s'ajouteront a la partie hote du mask)
* On a, mask = 255.255.224.0

On travail sur l'ID hote (mask)

* ID hote (mask) = 224.0 => 111(000)00.00000000 (On ajoute alors 3bits de 1 après le dernier 1)
* On obtient, 11111100.00000000 => 252.0 (en décimal pointe)

=> New Mask = 255.255.252.0

>> Identification du mask par le nombre d'hôte <<

Q°: Une E/se veut utiliser l'adresse réseau 192.168.90.0 pour 4 sous-réseau.
Le nombre d'hôtes par sous-réseau étant de 25, quel masque de sous-réseau utiliseriez vous pour résoudre ce problème ?

* Adresse réseau = 192.168.90.0 (Classe C, pour trouver la mask par défaut)
* Mask = 255.255.255.0 (xxxxxxxx est le dernier bit a trouver)
* Nombre d'hôte = 25

Identification de la puissance de 2 ≥ au nombre d'hôte

La puissance de 2 >= 25 est 32 = 2^5

Remplacement du(des) bit(s) du dernier octet en fonction de la puissance de 2 obtenu

* Pour xxxxxxxx = 11100000 (les 5 derniers bit sont a 0, le reste a 1)
* 11100000 = 224 (en décimal pointe)

=> **New Mask = 255.255.255.224** **pour résoudre ce problème**

>> Identification du sous réseau de plusieurs adresses IP par une adresse réseau <<

Q°: Le réseau 192.168.130.0 utilise le masque de sous réseau 255.255.255.224
A quels sous réseaux appartiennent les adresses (ip) suivantes :
192.168.130.10 | 192.168.130.93 | 192.168.130.222

Identification de l'ID de sous réseau en comptant les 1 de l'ID hôte (mask) en base 2

* Adresse réseau = 192.168.90.0 (classe C)
* Mask = 255.255.255.224
* Identification de l'id du mask
* ID hôte (mask) = 224 => (111)0 0000 (3bits de 1)

=> **On a 3 bits pour les ID de sous réseau**

Identification de l'ID hote (IP) puis on met a 0 tous les bit hors de l'ID de sous réseau

[Pour *192.168.130.10*]
* ID hote (IP) = 10 => (000)0 1010
* Le champ hors de l'ID de sous réseau est égale a 0 => 0000 0000 = 0(en décimal pointe)

=> **Avec l'id réseau, on a 192.68.130.0 comme sous réseau**

[Pour *192.168.130.93*]
* ID hote (IP) = 10 => (010)1 1101
* Le champ hors de l'ID de sous réseau est égale a 0 => 0100 0000 = 64(en décimal pointe)

=> **Avec l'id réseau, on a 192.68.130.64 comme sous réseau**

[Pour *192.168.130.222*]
* ID hote (IP) = 222 => (110)1 1110
* Le champ hors de l'ID de sous réseau est égale a 0 => 1100 0000 = 192(en décimal pointe)

=> **Avec l'id réseau, on a 192.68.130.192 comme sous réseau**

>> Calcul du plage adressable d'un réseau <<

Si adresse réseau = 172.128.0.0
Si adresse broadcast = 172.128.63.255

Pour identifier la plage adressable :

Adresse réseau +1 (sur le dernier octet)
Adresse broadcast -1 (sur le dernier octet)

=> **172.128.0.1**
=> **172.128.63.254**

Nommage (DNS)

DNS (**D**omain **N**ame **S**ystem) : Service essentiel de l'Internet assurant la conversion des nom de domaine *(e.g. www.linux-france.org)* en adresse IP *(e.g. 212.208.53.35)*. L'intérêt essentiel est de disposer de noms de machines plus faciles à retenir.

Protocole TCP | UDP

TCP (Transmission **C**ontrol **P**rotocol**)** et **UDP (U**ser **D**atagram **P**rotocol**)** sont les deux protocoles principaux de la couche transport. Lors de la configuration d'un routeur ou d'une box internet, il n'est pas rare d'avoir à choisir entre les ports TCP et les ports UDP, par exemple dans les mécanismes de "Port forwarding".

UDP (User **D**atagram **P**rotocol**)**	**TCP (T**ransmission **C**ontrol **P**rotocol**)**
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 connait pas l'émetteur des données hormis son IP.	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.

Avantages et inconvénients

➔ Certains outils proposent de choisir entre TCP et UDP, c'est le cas par exemple de certains VPN, voici les avantages et inconvénients des deux protocoles :

➔ TCP est plus fiable que UDP, les connexions par TCP sont donc généralement plus fiables car le protocole garantit que les paquets sont bien arrivés ;

➔ TCP est plus courant que UDP, ce qui lui permet donc de fonctionner dans la plupart des situations, y compris à travers des firewalls, qui laissent par défaut un certain nombre de ports TCP ouverts (80, 443, etc.).

➔ UDP est plus rapide que TCP, puisque le protocole ne nécessite pas d'aller-retour pour vérifier la bonne livraison des paquets. Ce protocole est à privilégier s'agit d'un flux pouvant supporter une dégradation temporaire du service, ce qui est le cas par exemple du streaming.

Pour faire simple

UDP est plus rapide, plus simple et plus efficace que TCP mais il est moins robuste en terme de fiabilité

Tableau recaputilatif

	TCP	UDP
Fiabilité	fiable	peu fiable
Type de connexion	Orienté connexion	sans connexion
Type de transmission	orienté octets	Orienté messages
Séquence de transfert	strictement ordonné	désordonné
Contrôle de surcharge	oui	non
Tolérance aux erreurs	non	non