Chapitre VIII : Réseaux et Internet

I - Transmission de données

a) Généralités

Internet est un réseau de réseaux de machines dans lesquelles circulent des données.

En 1969, quatre centres de recherche réussissent à échanger des données, c'est le projet ARPANET (*Advanced Research Projects Agency Networks*). Son évolution a donné naissance à Internet en 1974.

L'idée est de découper l'information en paquets indépendants muni de l'adresse du destinataire et de l'envoyeur. À l'arrivée, l'information est reconstituée à partir des paquets reçus.

La communication entre deux appareils s'établit à l'aide de **protocoles**. Les plus connus sont TCP (*Transfert Control Protocol*), IP (*Internet Protocol*) et HTTP (*Hypertext Transfert Protocol*).

Ce sont les protocoles qui régissent Internet et le Web.

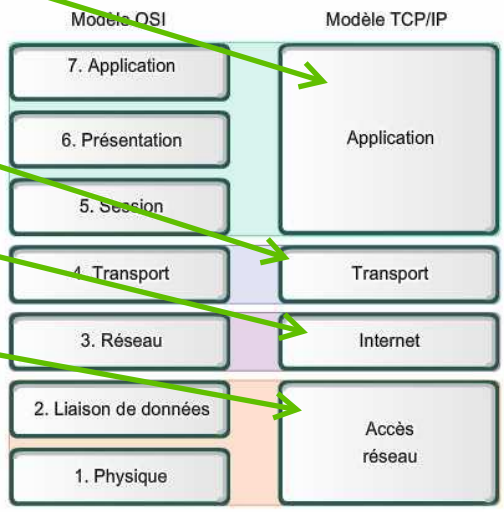
Un réseau informatique est un ensemble de nœuds composés d'équipements informatiques (ordinateurs, routeurs, concentrateurs, ...) reliés par des câbles de cuivre, de la fibre optique, des ondes radio, ...

Le protocole TCP/IP permet de transférer des données dans un réseau (notamment le réseau Internet) de façon fiable. Il a été mis en place en 1974 et est toujours utilisé aujourd'hui même s'il a subi des évolutions.

b) Le modèle TCP/IP

Le modèle TCP/IP propose quatre couches, qu'on présente en général de haut en bas :

- la **couche application** avec le protocole HTTP (ou HTTPS). On y trouve également des protocoles comme DHCP, DNS, FTP, SMTP, POP, ...
  DHCP permet d'attribuer des adresses IP dans un LAN (*Local Area Network*, réseau local)
  FTP est un protocole de transfert de fichier, SMTP, POP servent pour les mails
- la **couche transport** avec le protocole TCP (il existe également le protocole UDP à ce niveau)
  UDP sert notamment pour le transfert de vidéos, mais aussi pour le DNS
- la **couche Internet** avec le protocole IP (IPv4 ou IPv6)
- la **couche accès** au réseau avec les protocoles Ethernet, Bluetooth, Wi-fi, mais aussi ARP (*Adress Resolution Protocol*) pour connaitre une adresse physique MAC (*Media Acces Control*) d'un matériel à partir de l'adresse IP.



Ce modèle s'inscrit dans un modèle plus général appelé **modèle OSI** comme le montre l'image ci-contre.
La correspondance des couches n'est cependant pas aussi nette que semble le montrer cette image.

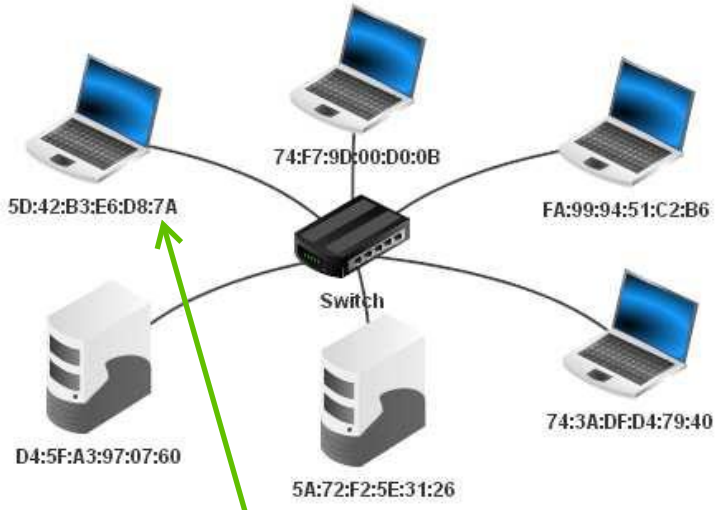
Principe général de communication dans un réseau : À RETENIR !!!

Pour demander une simple page Web, un navigateur prépare une requête HTTP (message de demande). Cette requête est mise en forme dans un ou plusieurs paquet(s) par le protocole TCP. TCP s'occupe de la couche **transport** entre l'émetteur et le récepteur mais il s'assure également **de la bonne réception des paquets et de leur mise en ordre**, ce qui permettra d'afficher correctement la page Web.
Ces paquets sont encapsulés dans des paquets munis d'**adresses IP** pour circuler dans différents nœuds du réseau.
Ces paquets IP sont à leur tour encapsulés dans des **trames Ethernet ou Wi-fi**. Ces trames ajoutent les adresses MAC c'est-à-dire les adresses physiques des appareils.

Le processus inverse est ensuite réalisé chez le récepteur jusqu'à récupérer le contenu du message de demande HTTP. Il répond suivant le même principe en envoyant le code de la page Web.

c) Réseau local et réseau Internet

On peut différencier un réseau local **LAN (*Local Area Network*)** et le réseau Internet.



– Dans un réseau local, toutes les machines sont reliées entre elles à un commutateur (switch).

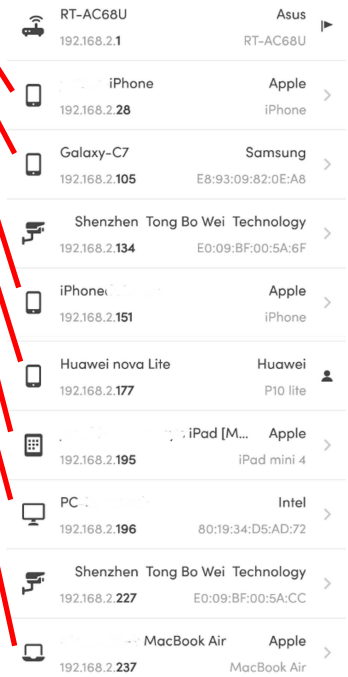
Chaque machine possède une adresse dite adresse MAC sur 6 octets écrite en hexadécimal (en séparant chaque octet), par exemple 5D:42:B3:E6:D8:7A sur la figure ci-contre.
On peut l'obtenir sur n'importe quel ordinateur à l'aide d'une invite de commande.

Sous Windows, il suffit d'écrire ..ipconfig /all... qui donnera l'adresse physique des différents réseaux.

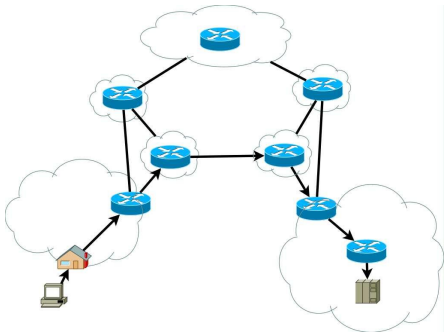
Sous linux, on écrit ..ip a.....

Sur Androïd, il suffit d'aller dans Paramètres, Onglet Général → À propos de l'appareil → État. L'application mobile fing permet de lister les appareils connectés au même réseau local que l'appareil.
Voici ce que cela peut donner (sous deux formes) :

State	Host	MAC Address	Vendor	Hostname
UP	192.168.2.1	B0:6E:BF:3C:65:A8	ASUSTek	router.asus.com
UP	192.168.2.28	F4:5C:89:D5:5C:D4	Apple	-iPhone
UP	192.168.2.105	E8:93:09:82:0E:A8	Samsung	Galaxy-C7
UP	192.168.2.134	E0:09:BF:00:5A:6F	Shenzhen Tong Bo Wei Technology	IPCAM
UP	192.168.2.151	1C:5C:F2:5D:BD:59	Apple	iPhone
UP	Huawei nova Lite (192.168.2.177)	50:04:B8:93:08:C6	Huawei	HUAWEI_P10_lite
UP	192.168.2.195	AC:E4:B5:42:F6:E5	Apple	32021SOU
UP	192.168.2.196	80:19:34:D5:AD:72	Intel	PC
UP	192.168.2.227	E0:09:BF:00:5A:CC	Shenzhen Tong Bo Wei Technology	
UP	192.168.2.237	30:35:AD:C7:4A:06	Apple	C
DOWN	192.168.2.36	3C:95:09:56:ED:47	Liteon Technology	DESKTOP-O3NP1NI
DOWN	192.168.2.64	78:CA:39:40:1F:18	Apple	
DOWN	192.168.2.102	BC:54:36:0B:31:05	Apple	
DOWN	192.168.2.119	30:35:AD:CD:C7:F4	Apple	
DOWN	192.168.2.207	C4:B3:01:0C:52:D5	Apple	Iphone



– Chaque machine présente sur Internet possède également une adresse MAC.
Dans un réseau, les machines s'identifient cependant grâce à leur adresse IP (le protocole IP permettant l'encapsulation des adresses du destinataire et de l'envoyeur).



Pourtant, lorsqu'on demande une page Web, on n'écrit pas l'adresse IP de la machine hébergeant cette page mais une URL (*Uniform Resource Locator*).

Le protocole ..DNS (*Domain Name System*)..... permet d'identifier l'adresse IP de la machine de destination et fonctionne un peu comme un annuaire.

II - Détail des rôles des différents protocoles de communication

a) Couche Application

Le navigateur envoie une requête HTTP à l'adresse IP d'une machine d'un réseau (par exemple pour avoir la page d'accueil d'un site).
Les échanges sur Internet pouvant être sensibles (échange sur un site marchand, avec sa banque, ...), il ne faudrait pas que les données soient interceptées au cours du transport. Une nouvelle couche intervient alors, c'est la couche de sécurisation effectuée avant le transport, c'est le protocole HTTPS. Elle permet l'échange avec le serveur de clés de chiffrement assurant la sécurisation du transport.

DNS est un autre protocole de la couche application. Il permet de maintenir des annuaires qui font correspondre des noms symboliques (par exemple `http://www.qwant.fr`) à des adresses IP (`217.70.184.55`) en plusieurs étapes :

1. Le serveur DNS du fournisseur d'accès interroge un serveur racine qui enverra l'adresse du serveur .fr appelée extension TLD (ce peut aussi être .com, .net, ...).
2. Un deuxième serveur renvoie vers le serveur qui connait l'adresse IP souhaitée (celle du nom de domaine : qwant).
3. Ce dernier serveur contacte ensuite les serveurs connaissant les adresses des sous-domaines (www ici) et renvoie l'adresse IP.

Le site https ://www.whois.com/whois permet d'identifier les serveurs DNS utilisés pour joindre le site `http://www.qwant.fr`.

b) Transport

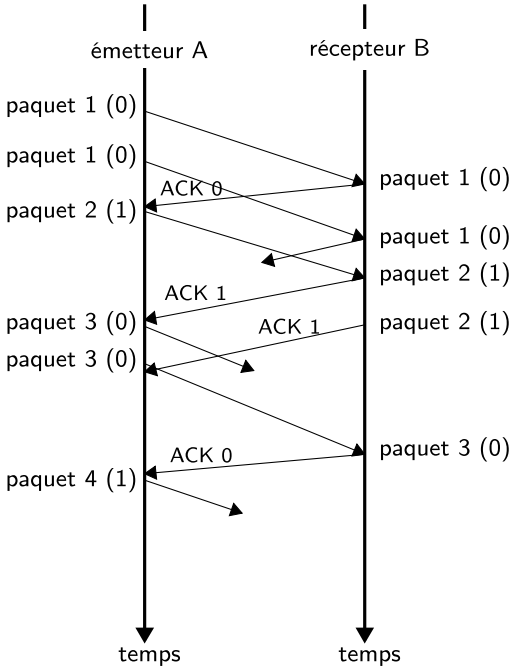
Le **protocole TCP** décompose le contenu de la requête en paquets en respectant une taille maximale pour chaque paquet (1500 octets par défaut pour une liaison Ethernet).

Protocole de bit alterné
Le protocole TCP propose un mécanisme d'accusé de réception afin de s'assurer qu'un paquet est bien arrivé à destination. 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. Nous allons ici étudier un protocole simple de récupération de perte de paquet : le **protocole de bit alterné**.

Des paquets sont envoyés par un émetteur A à un récepteur B.
Chaque paquet contient des données et un bit (0 ou 1).
B renvoie à A un message qui est un accusé de réception et le même bit que le message reçu.

Des paquets pouvant être perdus ou corrompus, on doit pouvoir les retransmettre. Ainsi :

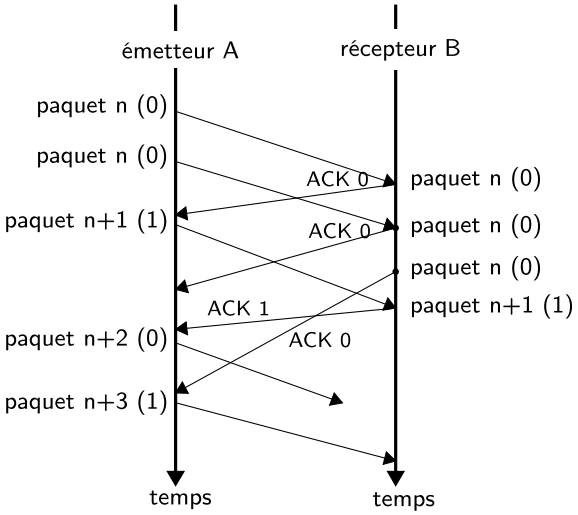
- Quand A envoie un paquet, il le renvoie à intervalles réguliers avec le même bit jusqu'à ce qu'il reçoive l'accusé de réception (appelé *acknowledgement* - ACK) de récepteur B
- Quand B reçoit un message non corrompu de A, il envoie à intervalles réguliers l'accusé de réception avec le même bit jusqu'à ce qu'il reçoive de A un message avec un bit différent.
- A peut continuer à recevoir un accusé de réception avec un bit 1 alors qu'il a déjà envoyé le nouveau paquet avec le bit 0. Il est dans ce cas ignoré.



Une vidéo expliquera ce principe. Vous devez le connaître !

Des problèmes subsistent, en voici un exemple.
Un paquet n est envoyé plusieurs fois. L'un de ses paquets (ou son accusé de réception) s'est un peu perdu et arrive après l'accusé de réception du paquet n+1 (comme ci-contre). Dans ce cas, le paquet n+2 a été envoyé avec le même bit que le paquet n.
L'émetteur reçoit alors un accusé de réception avec le bit 0, il va donc croire que c'est celui du paquet n+2 qui sera peut-être perdu.

Le protocole TCP a donc été amélioré pour éviter ce problème.



Maintenant, tout paquet envoyé contient un nombre appelé TTL (*Time To Live*) auquel on enlève 1 à chaque passage par un routeur. Quand ce nombre arrive à 0, on détruit le paquet pour éviter l'encombrement du réseau. C'est le protocole IP qui contient cette information.

Remarque : Il est existe également le protocole UDP (*User Datagram Protocole*).
Lorsqu'une application communique avec une autre application sur une machine distante par le protocole UDP, elle spécifie l'adresse IP de la machine qui reçoit et lui envoie un datagramme UDP (paquet de données dans un réseau). Ce datagramme est encapsulé dans un paquet IP, lui même encapsulé dans une trame (par exemple Ethernet).
Le protocole UDP ne propose pas de vérification pour être certain que le datagramme a bien été reçu. Il ne permet pas non plus de garantir que les datagrammes arrivent dans le même ordre que celui d'envoi.

c) La couche Internet et le protocole IP

L'adresse IP est une adresse numérique permettant d'identifier les appareils connectés à un réseau. Il en existe deux versions : IPv4 et IPv6 (IPv6 a été mis en œuvre pour augmenter le nombre d'adresses disponibles, le nombre d'adresses dans la version IPv4 devenant insuffisant suite à la multiplication des appareils connectés).

Dans la version IPv4, l'adresse IP est représentée par 4 octets notés en décimal (entre 0 et 255) et séparés par des points.
On peut tester si une machine distante est bien accessible depuis notre machine à l'aide de la commande .ping..
Dans un terminal de commande, pour vérifier qu'on a accès au site www.qwant.fr on peut écrire :
..... ping www.qwant.fr ..... ou ..... ping 217.70.184.55 ..... et on aura la réponse :

```
Envoi d'une requête 'Ping' 217.70.184.55 avec 32 octets de données :
Réponse de 217.70.184.55 : octets=32 temps=15 ms TTL=55
Réponse de 217.70.184.55 : octets=32 temps=15 ms TTL=55
Réponse de 217.70.184.55 : octets=32 temps=15 ms TTL=55
Réponse de 217.70.184.55 : octets=32 temps=15 ms TTL=55

Statistiques Ping pour 217.70.184.55:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 15ms, Maximum = 15ms, Moyenne = 15ms
```

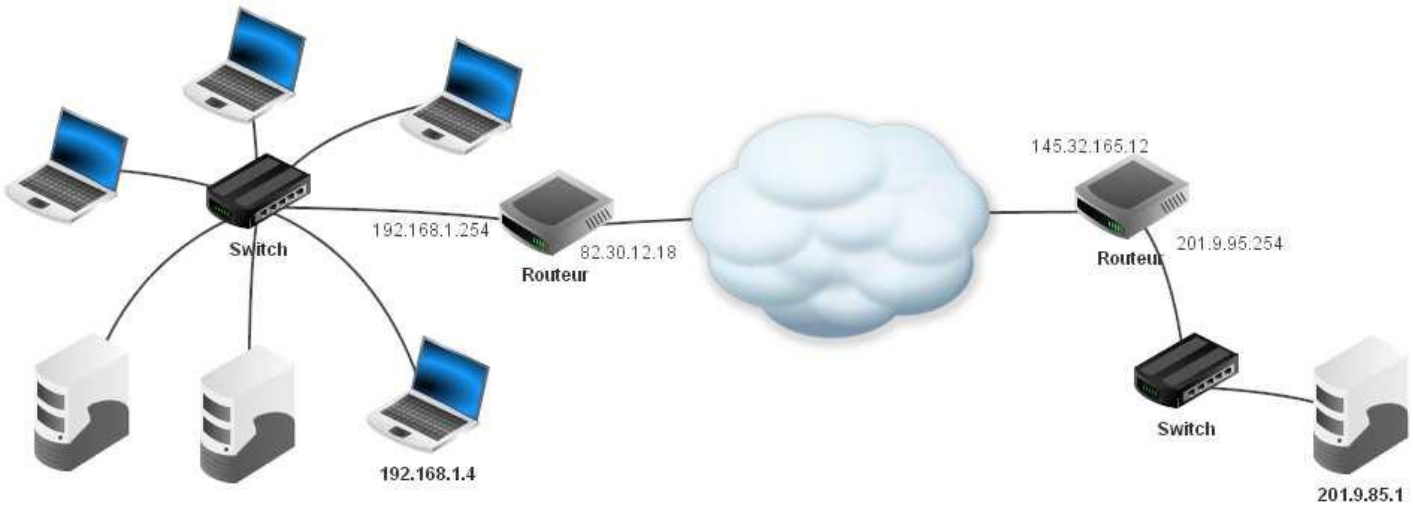
Sous Windows ..... tracert 217.70.184.55 ....., sous Linux ..... traceroute 217.70.184.55 .....
donne la liste des différents routeurs traversés pour arriver à la machine.

Dans le schéma ci-dessous, on distingue un réseau local dont l'adresse IP d'une des machines est 192.168.1.4. Ce réseau local possède une « porte de sortie » appelée passerelle (*gateway*) qui possède une table de routage c'est-à-dire la liste des adresses joignables depuis cette interface.

Par exemple, la machine d'adresse IP 192.168.1.4 veut envoyer des données à la machine d'IP 201.9.85.1. Voici les différentes étapes :

- elle cherche d'abord la machine dans le réseau local, ne la trouvant pas, elle envoie les données au routeur de son réseau ;
- on passe alors par lapasserelle d'IP 192.168.1.254 et le routeur propage sur la passerelle d'IP 82.30.12.18 ;
- de proche en proche, les paquets sont propagés jusqu'à arriver au routeur de passerelle 201.9.95.254 donnant accès à la machine souhaitée.

La machine d'adresse IP 201.9.85.1 reçoit chaque paquet et le protocole TCP/IP les désencapsule pour reconstituer le message d'origine.



Remarque : Les adresses IPv6 sont de plus en plus utilisées. Elles utilisent 16 octets, ce qui permet d'obtenir 2^{128} adresses.

d) Architecture d'un réseau

On distingue deux modèles de réseaux :

- le modèle client-serveur : le client (programme qui s'exécute sur la machine d'un utilisateur) communique avec un serveur (programme situé sur une machine disposant de puissance de calcul) pour lui demander un service.
- le modèle pair-à-pair (*peer to peer*) : ce modèle définit un réseau informatique où tous les ordinateurs agissent d'égal à égal. Ils distribuent et reçoivent des données ou des fichiers.
  Dans ce type de réseau, chaque client devient lui-même un serveur.
  Le pair-à-pair facilite et accélère les échanges entre plusieurs ordinateurs au sein d'un même réseau.

Chez un particulier, un ordinateur, ainsi que d'autres appareils sont connectés à une box louée par un FAI (fournisseur d'accès Internet). Les appareils et la box forment un réseau local et chaque machine a une adresse IP. La box a par exemple l'adresse 192.168.1.1 et elle affecte des adresses à tous les autres appareils connecté, dans une certaine plage avec un masque de sous-réseau 255.255.255.0.
Les adresses de tous les appareils connectés sont dynamiques et attribuées par un serveur DHCP. La box est reliée physiquement au réseau Internet par un câble DSL ou la fibre optique. Elle a enregistré des adresses de serveurs DNS qui sont proposées aux demandes des appareils.