Internet

Internet est une infrastructure matérielle **réticulaire** (en réseaux) qui interconnecte des machines se situant partout dans le monde de sorte que chacune puisse communiquer avec toutes les autres.

Il s'est formé petit à petit par sur-ajout de connexions de machines sur sa structure. Il est donc hétérogène est assez complexe(Bref, c'est le bordel!!!).

On appelle **communication** le transport d'informations d'un émetteur à un récepteur.
Pour que le réseau d'organisation complexe qu'est Internet fonctionne correctement, il faut des règles.

On partira de l'étude des principes régissant la communication entre deux machines et de l'étude de la généralisation de ces principes à la communication entre un grand nombre de machines puis on étudiera l'utilisation du réseau Internet par diverses applications (avec lesquelles il ne faut pas confondre Internet) pour transporter de l'information.

I- Modes de connections entre machines.

1) Communication entre deux machines

Permise depuis 1958 : invention du premier modem pour communiquer entre deux ordinateurs.

Afin que deux machines communiquent, il faut : une **liaison physique** par laquelle transite l'information, des **programmes** permettant de traiter l'information afin qu'elle soit communicable, des **protocoles** réglant en les précisant le format des informations échangées et la manière de les échanger.

a. Liaisons physiques entre machines

Une liaison entre machines peut être **filaire** (fil ou câble) ou bien **hertzienne** (par onde radio).
La **portée** de la liaison peut varier de quelques mètres à des milliers de kilomètres.

Le **débit** de la liaison varie lui aussi selon la technologie employée. Il se mesure en bits par seconde (bit/s). Un bit est une information élémentaire : 0 ou 1. Ses multiples sont le kilobits, le mégabits, le gigabits. Le débit peut donc se mesurer en kbit/s, Mbit/s ou Gbit/s. (ou en octets/sec, on divise alors la valeur en bits/sec par 8… Logique!)

Tableau comparatif des liaisons physiques par ordre croissant de débit

Liaisons filaires	Liaisons hertziennes
Câbles téléphoniques (dits « paire cuivre »). Grâce à la technologie ADSL (Asymmetric Digital Suscriber Line – le débit descendant vers l'abonné est supérieur au débit montant, depuis l'abonné), ces câbles ne font pas qu'acheminer la voix mais transportent aussi des informations numériques. Débit : quelques Mbit/s.	**Bluetooth** : utilisé dans les connexions à courte distance, conçu au départ pour relier des **périphériques** sans fil

Câbles spécialisés de type RJ45. C'est la technologie **Ethernet** utilisée pour des réseaux locaux à l'échelle d'une salle ou d'un bâtiment. Débit usuel : 100 Mbit/s ou 1Gbit/s.	**WiFi** (wi : contraction de l'anglais *wireless*, sans fil) : permet de connecter des machines à une borne ayant une portée de quelques dizaines de mètres
Fibres optiques. Utilisées pour les communications à longue distance et à très haut débit.	**Réseaux de téléphonie mobile 3G, 4G, 5G** permettant la connexion à Internet en haut débit
	Liaisons radio satellitaires : permettent des connexions à longue distance via des satellites placés en orbite géostationnaire
	Lifi : comme le wifi mais utilise le spectre optique...

Chacun de ces points de liaison physique, que ce soit par liaison filaire ou hertzienne, est identifié par une **adresse MAC**. Une même machine, si elle est reliée au réseau par plusieurs points de liaison a donc plusieurs adresses MAC, une pour chaque point de liaison. Ces points de liaison seront nommés **routeurs.**

b. Programmes

Quand deux machines communiquent, il y a une machine **émettrice** et une machine **réceptrice**. L'émettrice envoie des informations. La réceptrice les reçoit.

Pour que la communication des informations ait lieu, il faut un programme qui dans la machine émettrice contienne des instructions pour écrire des informations sur la liaison.
Il faut aussi un programme sur la machine réceptrice qui contienne des instructions pour lire les informations venant de la liaison. → **les programmes traduisent les informations à chaque conversion.**

Si une machine écrit de l'information sur une liaison et que l'autre machine n'est pas préparée à la lire, alors l'information émise est perdue.

c. Protocoles

Pour que deux machines puissent communiquer, il faut que leurs programmes respectent les mêmes protocoles.
Un **protocole** est un ensemble de règles qui précise le format des informations échangées, la manière de les échanger, d'établir la communication et de la terminer.

Exemple :
IP= Internet Protocole. Ce protocole attribue notamment des adresses aux machines selon un code bien précis :
l'adresse IP= adresse de la machine

Exo test :(Attention, à ce stade adr IP= boîte noire...)
brancher **deux machines ouvertes en mode administrateur** ensemble par connexion filaire RJ45
grâce à la commande **ipconfig sur le tableau de commande cmd**, noter son adresse ipv4
pinger son voisin connecté : ping adrip ; exemple **ping** 192.168.25,.9
Rq : en configurant les OS, on peut même accéder aux disques durs des autres PC…
NOTER CES INSTRUCTIONS DANS VOTRE PENSE BÊTE..

2) Communication entre plusieurs machines

Le réseau Internet relie à l'échelle mondiale de nombreux réseaux locaux connectés entre eux par des liaisons. On peut considérer qu'il existe depuis 1969 avec l'invention d'ARPANET qui permettait de communiquer entre 4 machines.

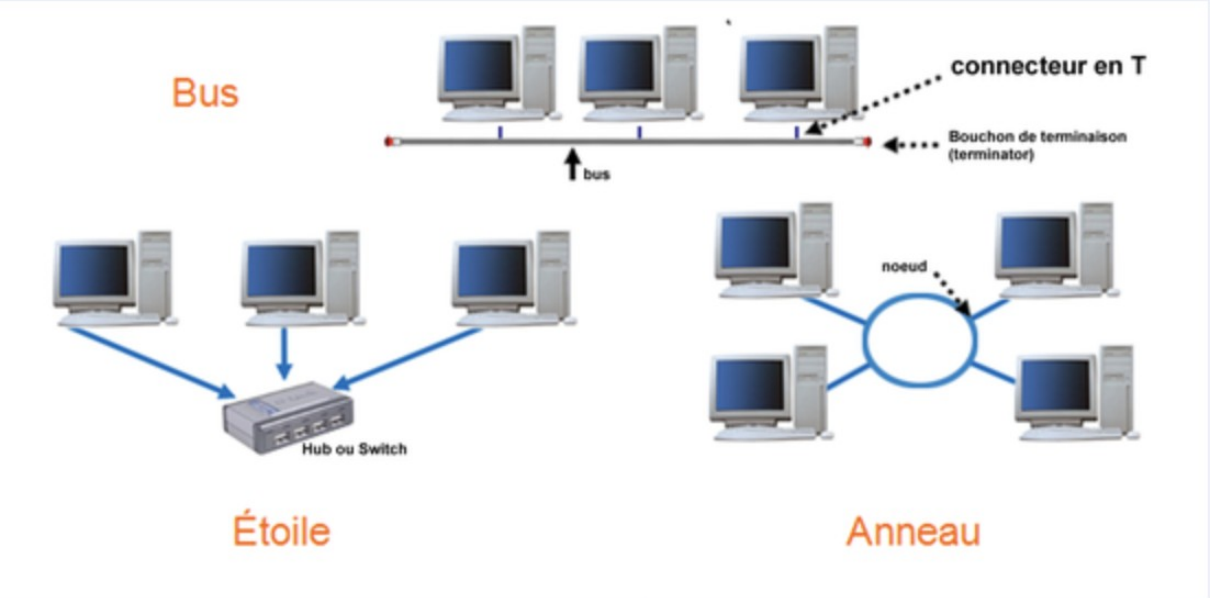
C'est 1982/83 que les protocoles de communication utilisés aujourd'hui (TCP/IP)sont créés et le nom internet est donné au réseau mondial en cours de formation.
Aujourd'hui, c'est 200 000 000 de serveurs et 3,5Milliards d'internautes.*(ouverture vers problème environnemental...)*

a. L'organisation du réseau

Un **réseau local** (ou **réseau LAN** – *Local Aera Network* en anglais) est un réseau entre un ensemble de quelques machines à l'échelle d'une d'une maison, d'un bâtiment, d'un lycée, d'une entreprise.

Les réseaux locaux sont organisés de manière à permettre à chaque machine du réseau de communiquer avec les autres et d'accéder à des ressources et informations partagées.
La plus efficace manière de connecter entre elles l'ensemble des machines du réseau local est de toutes les connecter à un même **commutateur** (**switch** en anglais).

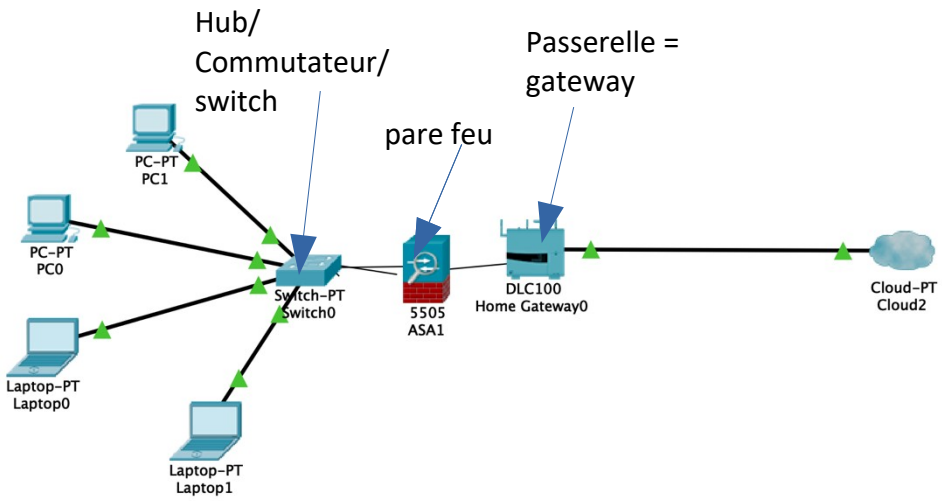
Commutateur avec des liaisons filaires RJ45



Topologies d'un réseau local

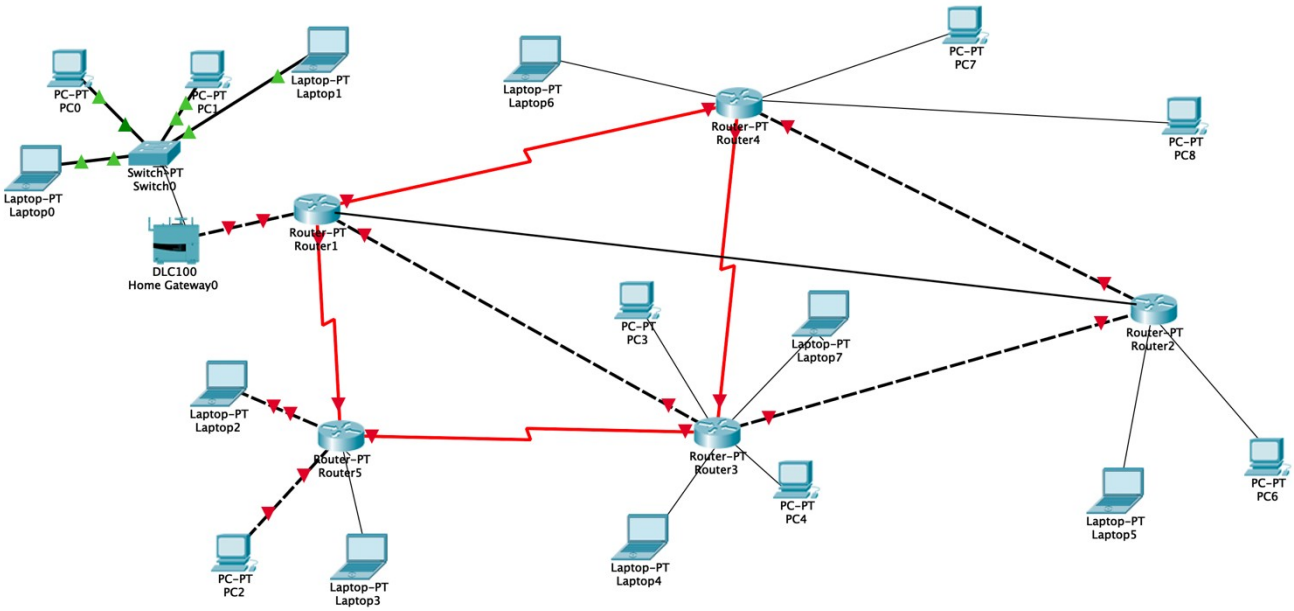
Un **réseau local peut être connecté au réseau Internet** par l'intermédiaire d'une **passerelle** (*gateway* en anglais) qui est une machine dédiée chargée de faire suivre les messages entre deux réseaux de natures différentes.

Cette **passerelle à une adresse ip commune avec toutes les machines qui y sont branchées.**
En plus de la passerelle, on trouve aussi souvent des **pare-feu** (*firewall* en anglais) qui sont des machines en charge de surveiller et filtrer les échanges d'informations entre un réseau local et Internet.



Un **routeur(qui possède une adresse MAC)** est une machine qui connecte deux ou plusieurs réseaux et qui exécute un programme permettant d'orienter les messages émis par le meilleur trajet pour atteindre la machine réceptrice destinataire.

Le réseau Internet est un ensemble de routeurs interconnectés entre eux auxquels sont connectées des machines émettrices et réceptrices. Toutes ces machines respectent le protocole IP.



Les routeurs contiennent un programme avec des instructions pour lire ou écrire sur une liaison.

Chacun possède son adresse : l'adresse MAC structurée comme suit :

Hors programme :
Une adresse MAC-48 est constituée de 48 bits (6 octets) et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point ou un tiret. Par exemple `5E:FF:56:A2:AF:15`.

Ces 48 bits sont répartis de la façon suivante :

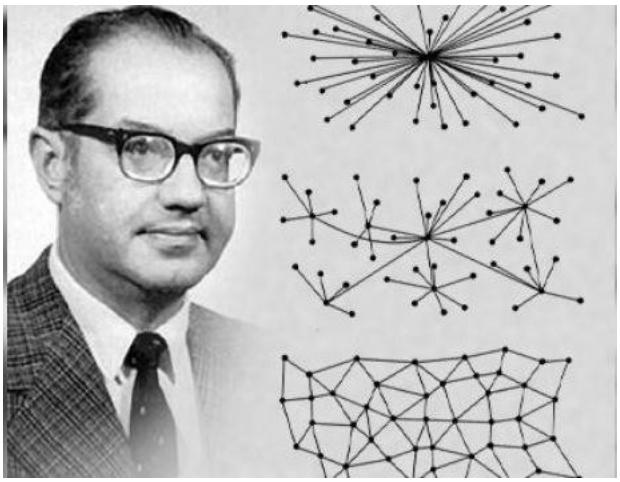
- 1 bit I/G : indique si l'adresse est individuelle, auquel cas le bit sera à 0 (pour une machine unique, unicast) ou de groupe (multicast ou broadcast), en passant le bit à 1 ;
- 1 bit U/L : indique 0 si l'adresse est universelle (conforme au format de l'IEEE) ou locale, 1 pour une adresse administrée localement ;
- 22 bits réservés : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur ;
- 24 bits : adresse unique (pour différencier les différentes cartes réseaux d'un même constructeur).

Il existe potentiellement 2^{48} (environ 281 000 milliards) d'adresses MAC possibles. L'IEEE donne des préfixes de 24 bits (appelés *Organizationally Unique Identifier* - OUI) aux fabricants, ce qui offre 2^{24} (environ 16 millions) d'adresses MAC disponibles par préfixe.

b. *La connexion des machines au réseau Internet*

Le réseau Internet est l'interconnexion des très nombreux réseaux locaux.
Il n'y a pas de machine centrale chargée de connecter toutes les autres et Internet n'est pas un réseau hiérarchisé du fait de sa construction progressive.

Pour connecter une machine à Internet, il suffit de la connecter à une autre machine déjà connectée à Internet (voilà par exemple pourquoi on peut connecter un ordinateur à Internet en utilisant un smartphone).



En 1962, Paul Baran distingue 3 formes de réseau : centralisé, décentralisé, distribué.

Une fois connectée au réseau Internet, une machine reçoit une adresse IP (Internet Protocol). Cette adresse est habituellement (pour la version 4 du protocole, nommée IPV4) un numéro à quatre nombres compris entre 0 et 255. Par exemple, une machine peut avoir l'adresse IP 172.16.254.1. Il y a donc 256^4 (plus de 4 milliards de possibilités) possibilités mais ce nombre **est** insuffisant , on arrive au bout ! Un protocole IPV6 a donc été créé.

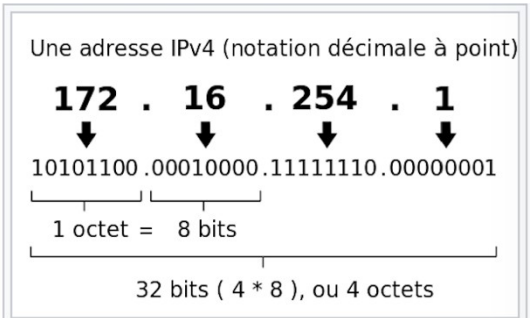
Les communications entre machines respectent des protocoles très précis. L'adressage en fait partie...

II- Des protocoles indispensables à la communication entre machines.

1- Le protocole IP :

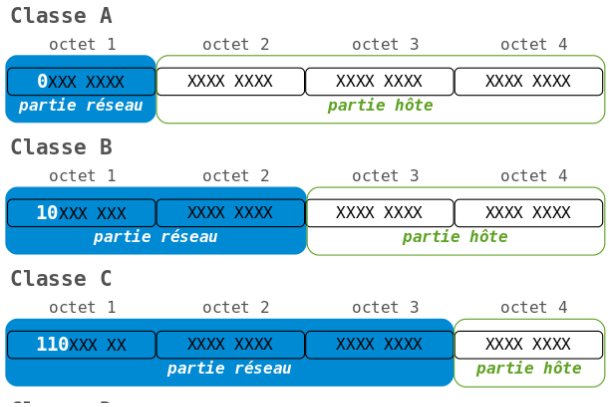
a- L'adressage des machines.

L'IPV4 :



Composition d'adresse IP selon la version de protocole IP V4

Limite HP :
Il existe **3 principales classes d'adresse IPV4** :
Classe A : premier octet entre 0 et 127 définit l'adresse du réseau(jusqu'à 126!), les trois autres les ordinateurs sui y sont branchés(jusqu'à 16,777216 Millions!!!)
Classe B : premier octet entre 128 et 191, les deux premiers octets définissent l'adresse du réseau(jusqu'à 16384!), les 2 autres les ordinateurs sui y sont branchés(jusqu'à 65534!!!)
Classe C : premier octet entre 192 et 223, les trois premiers octets définissent l'adresse du réseau(jusqu'à 2,097152millions!), le dernier les ordinateurs qui y sont branchés(jusqu'à 254 !!!)

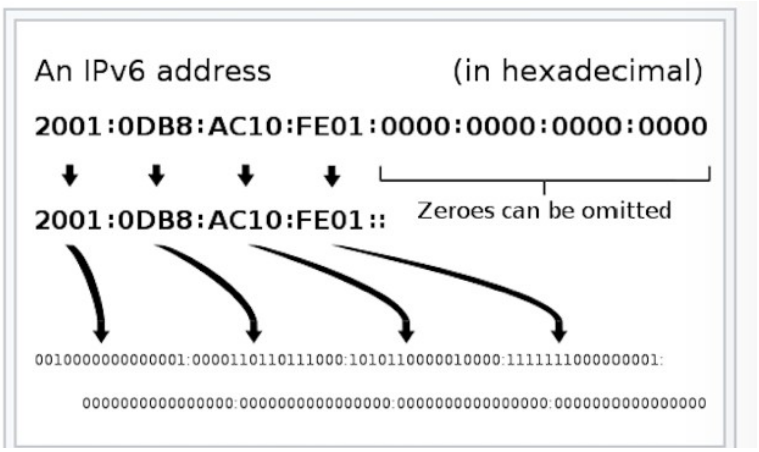


Adresse IP d'un ordinateur connecté à un réseau local (et possédant une adresse masque de sous-réseau) et utilisant une passerelle possédant elle-même une adresse IP

Parenthèse HP :
Ressources : Pour retrouver l'adresse ip de la passerelle de notre réseau : Exemple d'un réseau en **classe C**
Dans un **réseau LAN** de classe C, seul le dernier octet diffère entre les machines: exemple, **192.162.1**.1 et **192.162.1**.2, les 3 premiers octets pour le réseau LAN , le dernier pour l'ordi lui-même.
Prendre ensuite en compte le masque de sous réseau ci celui ci est 255.255.255.0, l'ip passerelle sera 192.162.1.0 *(c'est une association AND entre chaque bit de l'adresse ip de l'ordi et ceux du masque). Puis la même adresse de passerlle doit être donnée à chaque ordi (appareil) et au port du routeur sur lequell le réseau est branché….*
Fin de parenthèse...

L'IPV6 :
Pour lire l'IPV6, c'est simple : elle est écrite en hexadécimal ; Ce sont des adresses de 128bits séparés en groupes de 2octets.(2*8)*8=128. 64Bits sont réservés pour identifier le réseau, 64 pour les machines qui y sont connectées.

Le seul piège réside dans l'écriture des 0 :
- on les omet quand ils débutent un segment : « :00D6 : » → :D6 :
- on les réduits à 0 lorsque le segment est de valeur nulle : « :0000 : » → :0 :
- lorsque deux segments de valeurs nulles se suivent on écrit juste une série de ::: «:0000:0000 : » → ::



→ Activité : ATTENTION,
ordinateurs en mode administrateur !!!
On « ping » : dans la salle si on a un réseau branché vers l'extérieur…
1- découvrir son adresse ip : ipconfig dans la console(invit command)
2- envoyer un message test à une autre machine pour constater l'état de la liaison : ping 'adresse ip'
3- Alors on trace sa route : dans la console : instruction **tracert 'adresse ip'**

b- Le découpage en paquets :
Le **protocole IP** découpe l'information à envoyer en **paquets de taille constante**. La transmission d'un message sur un réseau nécessite donc un découpage en plusieurs paquets. Un **paquet** peut se définir comme l'entité transmise sur un réseau. Il inclut un en-tête contenant les informations nécessaires pour acheminer et reconstituer le message et **encapsule** une partie des données.

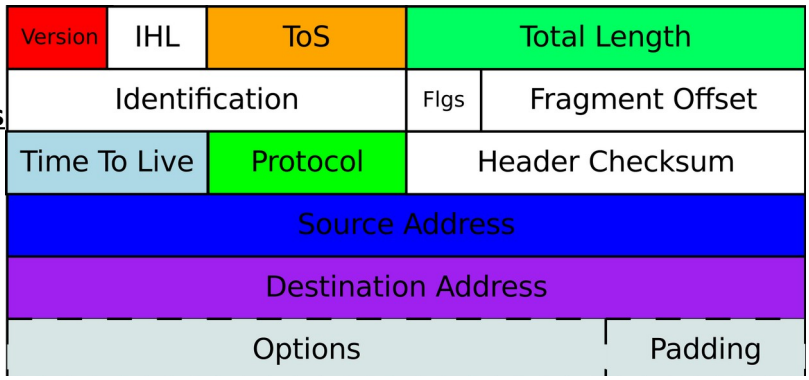
Chaque **paquet** contient :
-une en-tête contenant diverses informations dont les adresses de l'émetteur et du destinataire et le numéro du paquet(pour ranger ensuite)

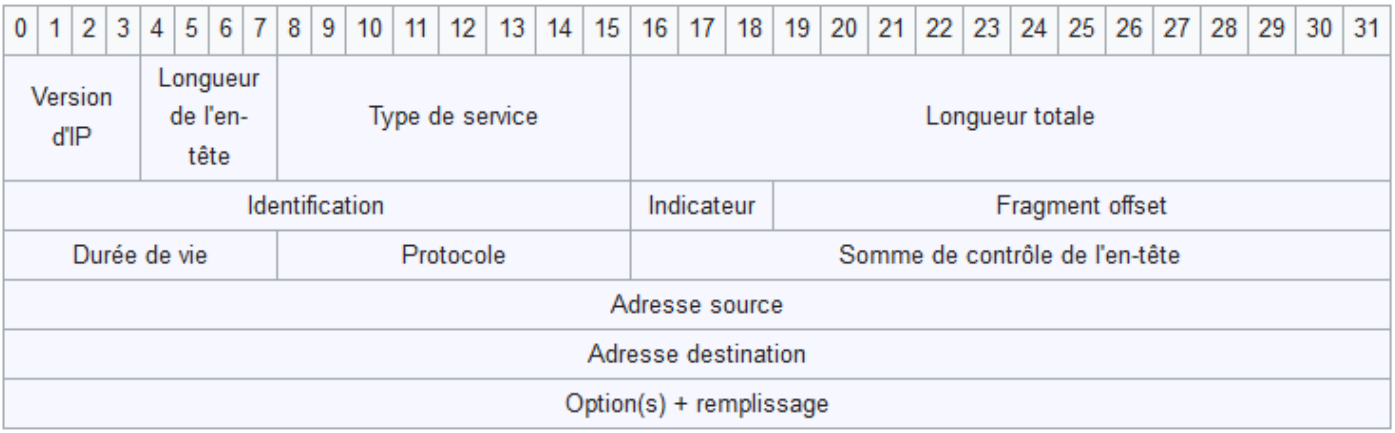
-**un paquet** = une partie de l'information à envoyer.

En tête v4 :

chaque ligne du schéma représente 32 bits d'info...(4 octets)
X 5lignes(hors options...)

En francais :





c- Le routage :

Le protocole Internet IP précise aussi comment acheminer un message d'une adresse à une autre.
Le **protocole IP** définit les règles de communication à respecter pour tous les algorithmes s'exécutant sur les routeurs et les différentes machines connectées au réseau. Sur chaque machine connectée on peut donc programmer l'envoi d'un message vers une autre machine en connaissant son adresse IP. Cet envoi n'est pas sécurisé à priori, **on n'est pas sûr qu'il parvienne à destination en intégralité**. Il est dit en **mode non connecté** car il ne demande pas si le destinataire est connecté, le message peut ne jamais arriver.

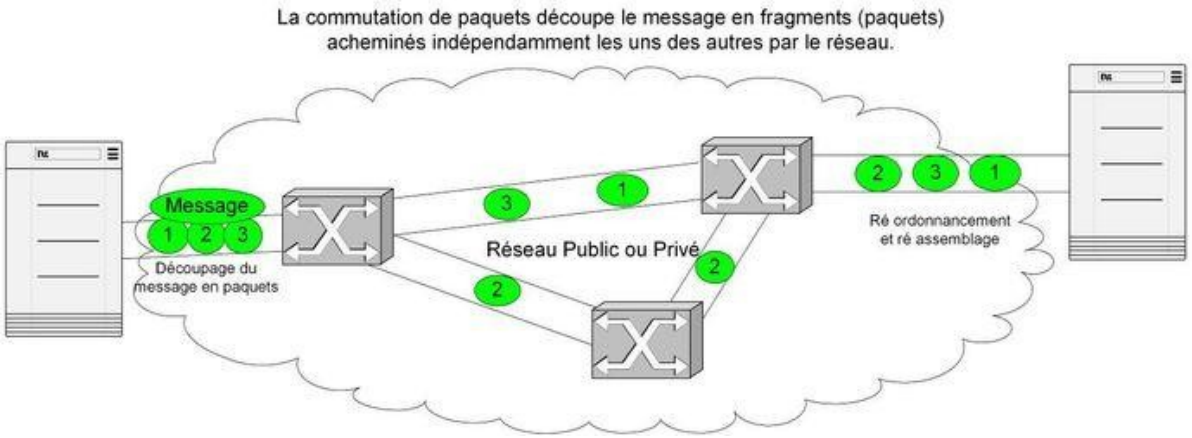
Il y a souvent plusieurs chemins possibles. On appelle **routage** le fait de chercher et trouver un chemin pour acheminer les informations d'un message d'une adresse à une autre. L'algorithme lit donc à chaque routeur **une table de routage** qui fait la liste des routeurs ou machines auxquels sont connectés ce routeur… Puis envoie le paquet vers le routeur le plus adapté…. Cela fonctionne par saut et recherches successives.
→ À chaque routeur, le routeur compare l'adresse destinataire avec celles des adresses auxquelles il est connecté(de sa table!) et envoie vers celle qui est la plus compatible(en lisant l'adresse de gauche à droite… Réseau puis ordi connecté...)
https://www.youtube.com/watch?v=dCknqcjcItU

Ce protocole IP a un routage qui repose sur un algorithme simple. Il n'assure pas la bonne réception des paquets.

Chaque routeur décide donc de la direction à faire prendre au message pour le rapprocher de son destinataire. Si un routeur tombe en panne, les messages empruntent un autre chemin, selon le principe de la **commutation de paquets**(La commutation de paquets est une technique d'acheminement des messages dans un réseau de communication dans laquelle la taille d'un message est limitée à une taille fixée : le paquet.)**.** Cela signifie que chaque routeur s'informe de l'état des routeurs voisins pour ne plus envoyer de

messages vers un routeur en panne ou bien vers un routeur ne supportant pas la taille du message envoyé.

Avec la **téléphonie IP** (par Internet donc, cf partie 3), si un paquet se perd à cause d'un routeur en panne, la voix devient hachée car les multiples paquets d'information composant un même message n'empruntent pas tous le même circuit.



Activité filius :

Annexe possible: https://pixees.fr/informatiquelycee/n_site/snt_internet_sim1.html

0- En utilisant le logiciel **Filius, créez un réseau de 4 machines** (M1, M2, M3 et M4). L'adresse IP de la machine M1 est "192.168.1.1", choisissez les adresses IP des machines M2, M3 et M4.
Effectuez un **"ping"** de la machine M2 vers la machine M4.

Ressources :

- installer d'abord sur chaque ordi le logiciel ligne de commande(sélection + flèche verte vers la gauche)
- commande sur l'ordi émetteur : **ping** *addresse ip visée*

→ donne le temps de l'aller retour et l'efficacité de la comm.

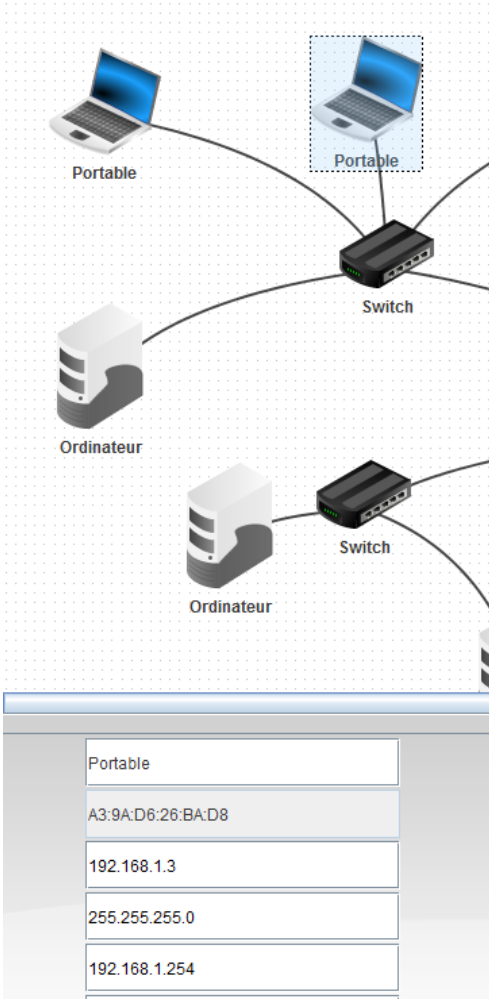
```
root /> ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3)
From 192.168.1.3 (192.168.1.3): icmp_seq=1 ttl=64 time=400ms
From 192.168.1.3 (192.168.1.3): icmp_seq=2 ttl=64 time=200ms
From 192.168.1.3 (192.168.1.3): icmp_seq=3 ttl=64 time=200ms
From 192.168.1.3 (192.168.1.3): icmp_seq=4 ttl=64 time=200ms
--- 192.168.1.3 Statistiques des paquets ---
4 paquets transmis, 4 paquets reçus, 0% paquets perdus
```

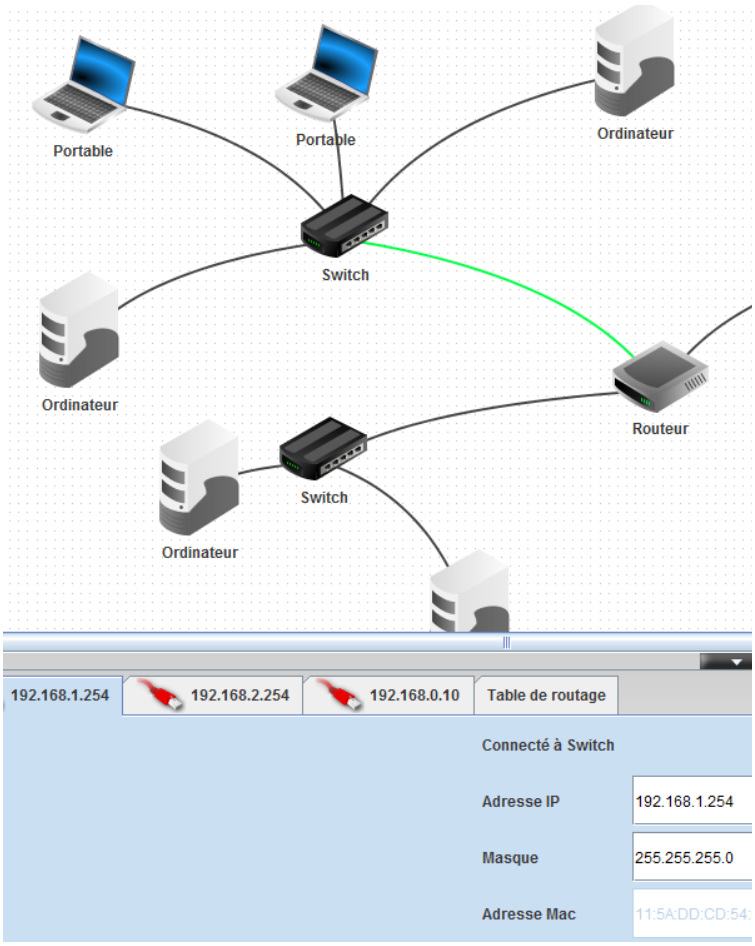
1- En utilisant le logiciel **Filius**, créez **3 réseaux de 2 machines chacun**. Ces 3 réseaux seront **reliés par un routeur**. Après avoir effectué toutes les opérations de configuration nécessaires, effectuez un **ping** entre deux machines de deux réseaux différents.

ex2filius.fls

Ressources :

- **attribuer une adresse ip à chaque ordi** de chaque réseau en adoptant une certaine logique(**seul le dernier octet varie dans chaque réseau local**(réseau de **classe C**)) : ex : dans un **réseau LAN** : **192.162.1**.1 et **192.162.1**.2, les 3 premiers octets pour le réseau LAN , le dernier pour l'ordi lui-même.
- **attribuer** pour chaque machine d'un réseau local(brancher au même swift) **le même ip de passerelle réseau qui doit être identique à l'ip correspondante du port du routeur qui y est branché…** Pour déterminer l'adresse ip de passerelle, il faut prendre en compte le masque, pour simplifier, ci celui ci est 255.255.255.0, l'ip passerelle sera **192.162.1**.0 . (En gros, l'adresse ip passerelle du réseau et celle du port du routeur associé doivent être identiques et dépendent du masque réseau)





2- Faites un **"traceroute"** entre l'ordinateur M14 et l'ordinateur M9 (n'oubliez pas de faire un "ipconfig" sur la machine M9 afin d'obtenir son adresse IP). Notez le chemin parcouru pour aller de la machine M14 à la machine M9 (remarquez au passage que le réseau R6 a des adresses IP de classe B et que cela ne pose aucun problème).
Supprimez le câble réseau qui relie le routeur F au routeur E (simulation de panne), refaites un "traceroute" entre M14 et M9. Que constatez-vous ? (ATTENTION : cela peut ne pas fonctionner du premier coup, car la mise à jour des tables de routage n'est pas immédiate : vous pouvez essayer de faire un ping entre M14 et M9, si cela ne fonctionne pas (timeout), attendez quelques secondes et recommencez. Une fois que le ping fonctionne, vous pouvez faire le traceroute).

Ressources :
- ouvrez le fichier : fichier snt_sim-res.fls
-repérez l'adresse ip de l'ordi visé, placer vous sur l'ordi émetteur et ouvrez la console. l'instruction s'écrit ici 'traceroute' et non 'tracert'.
- diminuez la vitesse de transmission des messages 

pour visualiser et décrivez les processus… Bon courage.

3- Traceroute en vrai : Il faut que les ordinateurs soient ouverts en mode administrateur...

(sur la console ‘cmd) réaliser une « tracert IP » : ça afficher le chemin suivi par l’information entre votre PC et la machine hébergeant le site associé à l’adresse IP :
- le site de l’université de Sydney.(ip = 129.78.5.8) → hébergé à Sydney
- le site doctolib.fr(ip= 104.20.116.110) → hébergé à Sevran en seine saint denis.

Comparer le nombre de serveurs qui relaient l’information et le temps de parcours de celle-ci.

Ressource :

Commande traceroute : **tracert** ‘adresse ip’

Autre exemple cedric.delepine.org

Rq: On peut localiser les machines avec leur adresse ip : https://www.mon-ip.co/

```
C:\WINDOWS\system32>tracert 104.20.116.110

Détermination de l'itinéraire vers 104.20.116.110 avec un maximum de 30 sauts.

  1    <1 ms    <1 ms    <1 ms  FREEBOX [192.168.1.254]
  2    24 ms    24 ms    24 ms  dan75-1-81-57-19-254.fbx.proxad.net [81.57.19.254]
  3    23 ms    25 ms    24 ms  78.254.0.126
  4    24 ms    24 ms    25 ms  gob75-1-v902.intf.nra.proxad.net [78.254.255.13]
  5    23 ms    24 ms    24 ms  bob75-1-v900.intf.nra.proxad.net [78.254.255.9]
  6    25 ms    25 ms    25 ms  mna75-1-v904.intf.nra.proxad.net [78.254.254.33]
  7    25 ms    25 ms    25 ms  th2-6k-2-1-po1.intf.nra.proxad.net [78.254.255.1]
  8    25 ms    25 ms    25 ms  194.149.171.65
  9    24 ms    26 ms    26 ms  194.149.166.33
 10    26 ms    25 ms    25 ms  194.149.166.50
 11     *        *        *     Délai d'attente de la demande dépassé.
 12    26 ms    27 ms    27 ms  212.73.205.22
 13    25 ms    25 ms    25 ms  104.20.116.110

Itinéraire déterminé.
```

```
C:\WINDOWS\system32>tracert 129.78.5.8

Détermination de l'itinéraire vers shared-addr.ucc.usyd.edu.au [129.78.5.8]
avec un maximum de 30 sauts :

  1    <1 ms    <1 ms    <1 ms  FREEBOX [192.168.1.254]
  2    23 ms    23 ms    24 ms  dan75-1-81-57-19-254.fbx.proxad.net [81.57.19.254]
  3    24 ms    25 ms    25 ms  78.254.0.126
  4    24 ms    25 ms    24 ms  gob75-1-v902.intf.nra.proxad.net [78.254.255.13]
  5    25 ms    24 ms    24 ms  bob75-1-v900.intf.nra.proxad.net [78.254.255.9]
  6    25 ms    24 ms    26 ms  mna75-1-v904.intf.nra.proxad.net [78.254.254.33]
  7    24 ms    25 ms    26 ms  th2-6k-2-1-po1.intf.nra.proxad.net [78.254.255.1]
  8    25 ms    24 ms    25 ms  ae2.mpr1.cdg11.fr.zip.zayo.com [64.125.14.37]
  9   163 ms   161 ms   162 ms  ae27.cs1.cdg11.fr.eth.zayo.com [64.125.29.4]
 10   162 ms   163 ms   162 ms  ae0.cs1.cdg12.fr.eth.zayo.com [64.125.29.84]
 11   161 ms   162 ms   161 ms  ae2.cs1.lhr11.uk.eth.zayo.com [64.125.29.25]
 12   162 ms   163 ms   175 ms  ae5.cs1.lga5.us.eth.zayo.com [64.125.29.126]
 13     *      162 ms   161 ms  ae3.cs3.ord2.us.eth.zayo.com [64.125.29.209]
 14   162 ms   161 ms   162 ms  ae2.cs1.sea1.us.eth.zayo.com [64.125.29.26]
 15   169 ms   168 ms   168 ms  ae27.mpr1.sea1.us.zip.zayo.com [64.125.29.1]
 16   162 ms   161 ms   161 ms  64.125.193.130.i223.above.net [64.125.193.130]
 17   303 ms   303 ms   302 ms  xe-0-2-1.pe1.bkvl.nsw.aarnet.net.au [202.158.194.120]
 18   303 ms   304 ms   304 ms  et-3-1-0.pe1.brwy.nsw.aarnet.net.au [113.197.15.146]
 19   305 ms   304 ms   304 ms  gw1.vl216.ae11.pe1.brwy-pe1.aarnet.net.au [138.44.5.47]
 20     *        *        *     Délai d'attente de la demande dépassé.
 21     *        *        *     Délai d'attente de la demande dépassé.
 22   304 ms   304 ms   304 ms  shared-addr.ucc.usyd.edu.au [129.78.5.8]

Itinéraire déterminé.
```

les temps indiqués sont des moyennes de temps cumulés, la moyenne finale correspond au temps de parcours total.
Évidemment : temps pour se rendre à Sydney> celui pour aller à Sevran en seine saint Denis.

Les gros sites web ont des duplicatas sur de nombreux serveurs sur tous les continents(cf google.fr) pour diminuer les temps de parcours et économiser les transmissions trans océaniques(sinon saturation très rapide!!!)

2- Le protocole TCP :

Le protocole qui permet de **sécuriser la transmission des messages** est le **protocole TCP** (Transmission Control Protocol). Il s'ajoute au protocole IP pour le rendre plus sûr.

Le protocole TCP découpe les messages trop longs pour être correctement sécurisés en plusieurs morceaux(segments). Chaque morceau est envoyé successivement en utilisant un programme de type « Envoyer message IP »→ paquet. Pour indiquer que le message a bien été reçu, le récepteur envoie un autre message appelé **accusé de réception**. Si l'expéditeur ne reçoit pas d'accusé de réception au bout d'un certain temps, il envoie à nouveau le même message.

Ce protocole adopte donc un **mode connecté** : il exige la connexion du destinataire pour envoyer le message. Il est donc plus fiable que le mode non connecté du protocole IP

Les différents morceaux du message initial sont envoyés tour à tour et peuvent prendre des chemins différents, ceux qui sont perdus peuvent être réexpédiés grâce à la procédure d'accusé réception. **Tous les morceaux finiront par arriver au bout d'un certain temps**, même si ce n'est pas dans le bon ordre. Les morceaux d'un message TCP étant **numérotés** et leurs accusés de réception l'étant aussi, ils peuvent facilement être **remis dans l'ordre** avant remise du message initial au destinataire.

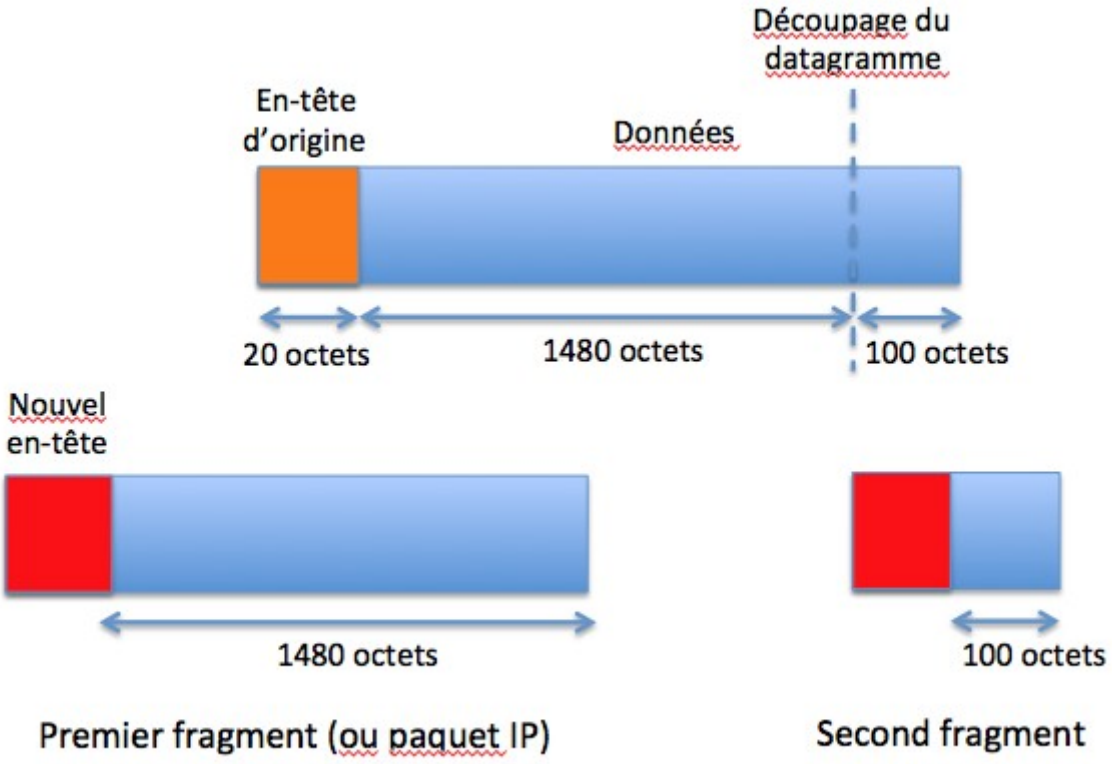
Finalement, pour envoyer un seul long message avec TCP, il y a beaucoup d'envois de messages IP contenant des morceaux du message initial, des accusés de réception, des réexpéditions de morceaux et d'accusés de réception de réexpédition, etc.

Le protocole TCP définit et remplit donc l'instruction « envoyer long message TCP à l'adresse IP abcd.efgh.ijkl.mnop » .

Un message envoyé selon le protocole TCP n'est pas limité en taille et est assuré d'arriver à son destinataire, mais sans assurance quant au temps qu'il lui faudra pour parvenir à ce destinataire.

Imaginons que notre machine souhaite envoyer un datagramme de 1600 octets. Une trame pouvant transporter un datagramme de 1500 octets il va falloir fragmenter ce datagramme.

Les fragments doivent toujours être **les plus gros possibles**.
Ainsi, nous allons faire un premier fragment de 1500 octets, et un autre de... 120 octets.
s 1500 + 120 ça ne fait pas 1600 ?
Vous avez oublié les 20 octets d'en-tête qui sont dans notre datagramme d'origine, il n'est pas nécessaire de les transporter puisque nous allons de toute façon fabriquer un nouvel en-tête pour chacun des fragments réalisés. Il faut aussi ajouter un nouvel en-tête à chacun de nos nouveaux fragments, voici un schéma qui explique cela:



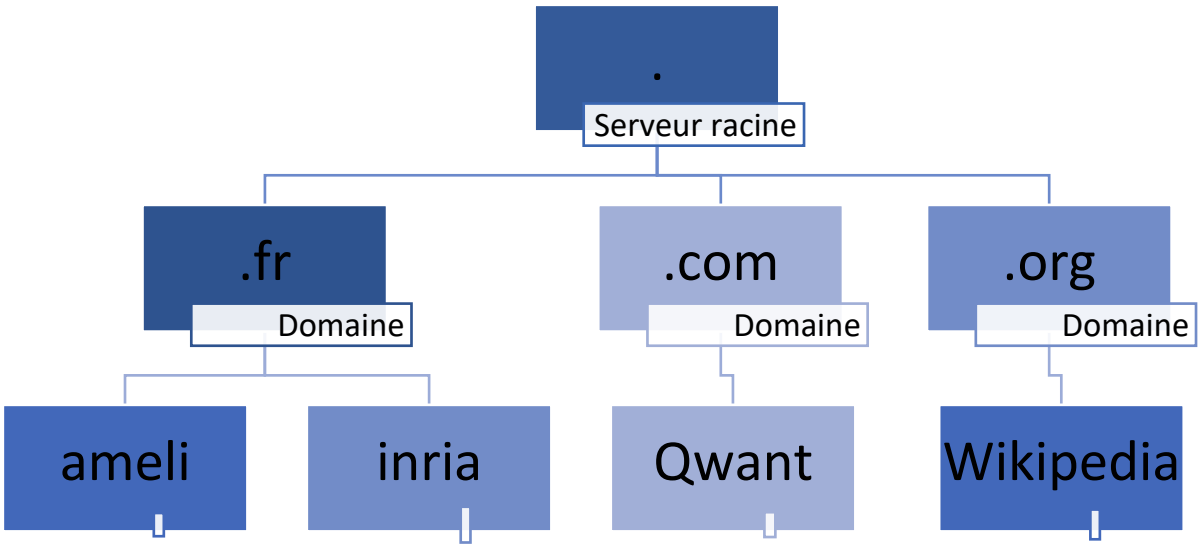
3) Applications/ Utilisations du réseau Internet

a. Le nommage des machines à l'échelle mondiale facilite la navigation sur le web...

Afin de simplifier l'envoi des messages avec les protocoles IP et TCP (selon une unique procédure qu'on appelle alors TCP/IP, indiquant par là qu'on utilise la combinaison des deux protocoles TCP et IP pour envoyer un message), un mécanisme de nommage symbolique est défini.

On appelle **DNS** (Domain Name System) le système des noms de domaines qui sont autant d'adresses symboliques auxquelles correspondent des adresses IP. DNS est aussi le nom du service qui organise et conserve et archive la correspondance entre **adresses symboliques** (par exemple http://www.quant.fr) et **adresses IP** (par exemple 194.153.205.26). Cette correspondance est établie car pour utiliser Internet il est beaucoup plus commode de désigner un destinataire par un nom que par une suite de chiffres.

Les serveurs DNS sont des machines connectées au réseau Internet qui conservent les tables de correspondance entre adresses IP et adresses symboliques. La mise à jour de ces serveurs s'effectue en permanence, car à chaque instant de nouvelles adresses IP ou symboliques sont créées (on peut ainsi créer ou acheter un **nom de domaine**, c'est-à-dire le faire enregistrer par un serveur DNS). Les serveurs DNS disposent de protocoles pour communiquer entre eux et se signaler les changements.



Hiérarchie DNS (partielle)

L'**ICANN** est l'organisme responsable des 13 serveurs DNS qui gèrent la racine du DNS.

Grâce à tous les protocoles vus précédemment (IP, TCP, DNS), une unique instruction (« envoyer message TCP/IP à l'adresse serveur.domaine ») permet de programmer toutes les applications développées pour utiliser le réseau Internet : courrier électronique (mail), web, réseaux sociaux, ...

Les applications du réseau Internet sont les différents services qui utilisent Internet pour répondre aux différents besoins des utilisateurs.

Il y a **deux grandes catégories d'applications d'Internet**, selon le principe de communication qu'elles utilisent : la catégorie **« Client-serveur »** et la catégorie **« Pair à pair ».**

b. Clients et serveurs

Le **mode « Client-serveur »** est un mode d'organisation d'une application sur Internet où un certain nombre de clients communiquent avec un serveur pour lui demander un service. Un **client** est un programme qui s'exécute sur la machine de son utilisateur. Un **serveur** est un programme situé sur une machine qui dispose d'assez de puissance de calcul et de mémoire pour rendre un ou plusieurs services.

Le protocole d'**envoi de courrier** SMTP (Simple Mail Transfer Protocol) ou le protocole IMAP (Internet Messaging Access Protocol) permettent à des clients de courrier électronique de communiquer avec des serveurs de courrier.
Le protocole FTP (File Transfer Protocol) permet à des clients de fichiers de communiquer avec un serveur de fichiers.

ABSOLUMENT HP:
*On appelle **port** le numéro permettant d'indiquer le service demandé à un serveur par Internet.*

L'envoi de courrier électronique par SMTP utilise le port 25 ; utiliser le web requiert le port 80 (Liste de ports Internet : https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels). Si le bon port n'est pas utilisé, les communications n'arrivent pas « à bon port » : si par exemple un serveur de fichier fonctionnant sous protocole FTP reçoit un message de client de courrier fonctionnant sous protocole SMTP ou IMAP, il n'en fera rien car ici serveur et client ne communiquent pas sous le même protocole (donc : ne communiquent pas du tout).

c. Réseaux pair à pair

Le **mode « pair à pair »** (« peer to peer » en anglais, P2P en abrégé) est le mode d'organisation d'une application sur Internet où toutes les **machines se comportent alternativement comme clients ou comme serveurs.**

C'est un mode d'organisation égalitaire (« pair à pair » signifie « d'égal à égal »). Aucune machine n'est distinguée soit comme client soit comme serveur. Certaines applications de partage de fichiers utilisent le P2P pour proposer de télécharger l'ensemble des documents mis à disposition sur l'ensemble des machines appartenant au réseau pair à pair.
Ce mode d'organisation a été utilisé pour diffuser illégalement des fichiers vidéos ou audio encore sous droit d'auteur.

Les applications internet se développe, on utilise à présent fréquemment internet pour :
- téléphoner : téléphonie IP, il existe deux technologies. ToIP(Telephone on IP) ou VoIP (Voice on IP)
- Regarder des films : VOD…
- Acheter…

d. Conséquences du développement de l'utilisation du réseau internet.

Tous ces transferts d'informations génèrent des flux très importants et des fonctionnements permanents de serveurs qui conduisent à une consommation d'énergie mondiale qui dépasse aujourd'hui celle du transport aérien mondial.
La **consommation énergétique d'Internet** est répartie en trois groupes, chacun utilisant une quantité élevée d'électricité. Ces groupes représentent :

- Les utilisateurs 30 %
- Le réseau 40 %
- Les centres de données 30 %

→ 10 % de l'électricité mondiale y passe selon l'ademe en octobre 2019..

Voici d'autres chiffres qui mettent en avant le côté énergivore d'Internet :

- l'envoi d'un mail d'1 Mo équivaut à l'utilisation d'une ampoule de 60 watts pendant 25 minutes
- Plus de 12 milliards de mails sont envoyés chaque heure dans le monde, émettant au total 50 Giga Watt Heure, soit la production électrique de 18 centrales nucléaires pendant une heure
- Une requête sur un moteur de recherche c'est, « *une ampoule basse consommation allumée pendant 1 heure*"
- Un grand centre de données consomme près de 100 millions de watts soit l'équivalent d'une ville européenne de 30 000 habitants
- En 2023, Les data centers chinois[2]consommeront autant d'énergie que l'ensemble de l'Australie, tous usages confondus
- les 3 milliards de vues de « Gangnan Style » ont consommé l'équivalent de la production annuelle d'une petite centrale

sources *Ademe : ICI et LA*[2]
http://www.newsroom-publicismedia.fr/linternet-un-tres-gros-consommateur-denergie/

Notions fondamentales et lexique – Capacités attendues

Contenus	Capacités attendues
Protocole TCP/IP : paquets, routage de paquets	Distinguer le rôle des protocoles IP et TCP Caractériser les principes du routage et de ses limites Distinguer la fiabilité de transmission et l'absence de garantie temporelle
Adresses symboliques et serveurs DNS	Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement
Réseaux pair-à-pair	Décrire l'intérêt des réseaux pair-à-pair Décrire les usages illicites qu'on peut en faire
Indépendance d'Internet par rapport au réseau physique	Caractériser quelques types de réseaux physiques : obsolètes ou actuels, rapides ou lents, filaires ou non. Caractériser l'ordre de grandeur du trafic de données sur Internet et son évolution.