LE RÉSEAU INTERNET

I) Généralités sur Internet

1) Internet, le réseau qui interconnecte les autres

Très vite dans l'histoire de l'informatique, on a cherché à relier entre eux des ordinateurs. Dès les années 60 différentes solutions techniques apparaissent permettant de créer des réseaux entre plusieurs ordinateurs mais ces solutions ne sont pas compatibles entre elles. Internet est né de la volonté d'interconnecter le plus de réseau possible et s'est progressivement imposé vers les années 1990 à 2000.

Quelques caractéristiques d'Internet aujourd'hui :

- Internet n'est pas un grand réseau homogène mais plutôt l'interconnexion d'un très grand nombre de réseau locaux.
- Internet permet de relier entre eux des terminaux de natures très différentes : ordinateurs, smartphones, imprimantes, montres connectées,…
- Internet utilise des moyens très différents pour faire transiter les données : câbles Ethernet, fibres, ondes Wi-Fi, 4G ou 5G, câbles sous-marin, liaisons satellite.
  Voici par exemple une carte des câbles sous-marins : https://www.submarinecablemap.com/
- Internet a une structure très décentralisée : Si certains équipements tombent en panne, d'autres prennent le relais automatiquement.

2) Réseaux LAN et WAN

Les **réseaux locaux** (souvent appelés **LAN** = Local Area Network) forment les briques de base du réseau internet. Un LAN peut contenir quelques terminaux (par exemple le réseau familial est un LAN) ou bien quelques milliers (réseaux d'universités ou d'entreprises par exemple).

Dans un LAN, les ordinateurs sont tous reliés entre eux via :

- Un ou plusieurs **switchs** (appelés en français **commutateurs**) qui permettent de connecter des ordinateurs avec des câbles **Ethernet** et des prises **RJ45**.
- Un ou plusieurs **points d'accès Wifi**.

Un LAN étant local :

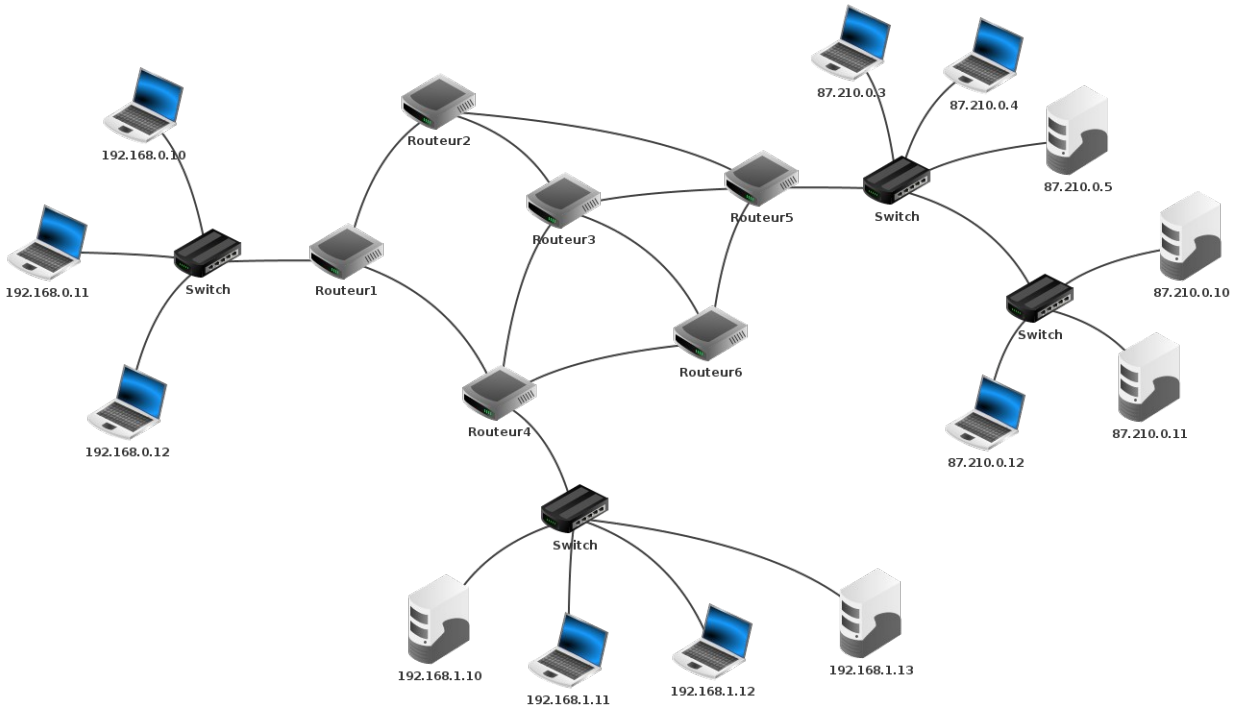
- Il a souvent des liaisons très rapides.
- Il est en général privé avec un enjeu de sécurité.
- Il y a une personne qui en maîtrise l'architecture globale (en général simple) et qui peut intervenir rapidement en cas de panne.

Communication entre deux ordinateurs :

- Si un ordinateur veut communiquer avec un ordinateur qui est dans le même LAN, cette communication peut se faire directement sans passer par d'autres intermédiaires que les switchs et les points d'accès wifi du LAN.
- En revanche, si cet ordinateur doit communiquer avec un ordinateur qui est sur un autre LAN, cette communication doit passer par la porte de sortie du LAN appelée **passerelle** ou **routeur**, puis sauter de routeur en routeur jusqu'à atteindre le routeur qui lui permettra d'entrer dans le LAN de l'autre ordinateur. Cette communication traverse alors ce que l'on appelle le **réseau étendu** (souvent appelé **WAN** = Wide Area Network).
- Les box familiales ont comme particularité de regrouper en un seul boîtier : un switch (souvent 4 ports LAN en RJ45), un point d'accès wifi et un routeur (1 port WAN en RJ45 ou fibre optique).

Livebox Play

Combien de LAN différents comptez-vous ci-dessous ? 3 ? 4 ? 12 ?
Y a-t-il un WAN ?



3) Adresses IP et adresses MAC

Sur internet, chaque **carte réseau** (appelée aussi **interface**) a deux adresses.

- Une adresse physique de 6 octets, en principe non modifiable, appelée **adresse MAC**.
  Ex : A4:26:49:F9:52:D1
- Une adresse logique de 4 octets, modifiable, appelée **adresse IP**.
  Ex : 192.168.0.163

Remarques :

- L'adresse MAC est définie par le constructeur de la carte réseau lors de sa fabrication de telle sorte qu'il n'y ait pas 2 cartes réseau qui aient la même adresse MAC.
- L'adresse IP est modifiable par l'administrateur de l'ordinateur. Sa structure permet aux routeurs de savoir dans quelle direction envoyer les données (un peu comme une adresse postale).
- Un ordinateur peut avoir plusieurs cartes réseau. Par exemple de nombreux ordinateurs portables ont à la fois une carte Ethernet avec prise RJ45 et une carte Wifi. Ces ordinateurs ont alors autant d'adresses IP et d'adresses MAC que de cartes réseau.
- Si votre smartphone est connecté au Wifi, alors vous trouverez son adresse IP et son adresse MAC dans les paramètres. En revanche, s'il est connecté sur le réseau GSM, vous verrez qu'il a toujours une IP (différente de celle du Wifi) mais pas d'adresse MAC car ce type de réseau utilise un autre identifiant unique (IMSI) lié à votre carte SIM.
- Les adresses IP à 4 octets (ipv4) permettent d'adresser un peu plus de 4 milliards de terminaux. Ce n'est plus assez ! Un certain nombre de techniques ont été mises en place pour retarder la pénurie (adresses privées avec NAT et PAT) mais surtout une nouvelle norme d'adresses IP à 16 octets (ipv6) se met en place progressivement.

Pourquoi deux adresses ?

- Les adresses MAC sont un peu comme des empreintes digitales. Elle sont uniques et permettent d'être certain que l'on s'adresse à la bonne personne.
- Les adresses IP sont un peu comme des adresses postales où l'octet le plus à gauche serait le pays, puis la ville, puis la rue et enfin l'octet le plus à droite le numéro de la maison. Elles permettent aux routeurs de savoir dans quelle direction acheminer les messages qu'ils reçoivent. Quand on « déménage » (changement d'abonnement internet, changement de service dans une entreprise,…), on change d'adresse IP.
  Pour voir par exemple les plages d'adresses IP attribuées à votre fournisseur internet : https://bgp.he.net/

4) Masques de sous-réseau

Quand on configure l'adresse IP d'une carte réseau, on précise en même temps un **masque de sous-réseau** et l'adresse IP de la passerelle qui permet de sortir du LAN.

Qu'est-ce qu'un masque de sous-réseau ?

- Un masque de sous-réseau est commun à tous les ordinateurs d'un même LAN. Il permet à chaque ordinateur de savoir si une adresse IP quelconque appartient à un ordinateur du même LAN que lui ou non. En effet, si un ordinateur veut envoyer un message à une IP du même LAN, il peut l'envoyer directement (les switchs du LAN sauront envoyer le message directement au bon ordinateur). Sinon, l'ordinateur doit faire transiter le message via la passerelle qui permet de sortir du LAN.
- Le masque de sous-réseau commence toujours en binaire par une série de 1 et il termine toujours par une série de 0. Les 1 permettent de délimiter la partie de l'adresse IP commune à tous les ordinateurs du sous-réseau.

Ex 1 : Supposons qu'un ordinateur A ait la configuration ci-dessous :

	En décimal :	En binaire :
Adresse IP :	192.168. 0 .7	1100 0000 . 1010 1000 . 0000 0000 . 0000 0111
Masque de sous-réseau	255.255.255.0	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
Passerelle	192.168. 0 .1	1100 0000 . 1010 1000 . 0000 0000 . 0000 0001

Dans l'exemple ci-dessus, les bits des 3 premiers octets du masque de sous-réseau sont à 1. Cela veut dire que tous les ordinateurs dont l'IP est de la forme 192.168.0.xxx appartiennent au même LAN que l'ordinateur A.
Remarque : La passerelle doit appartenir au même LAN que l'ordinateur A, sinon ce dernier ne pourrait rien lui envoyer.

Ex 2 : Supposons qu'un ordinateur B ait la configuration ci-dessous :

	En décimal :	En binaire :
Adresse IP :	192.100. 1 .7	1100 0000 . 0110 0100 . 0000 0001 . 0000 0111
Masque de sous-réseau	255.255.252.0	1111 1111 . 1111 1111 . ____ . 0000 0000
Passerelle	192.100. 0 .1	1100 0000 . 0110 0100 . 0000 0000 . 0000 0001

Compléter le tableau ci-dessus, puis préciser la plage d'adresses IP appartenant au même LAN.
La passerelle proposée est-elle visible par l'ordinateur B ?

Remarques :
- Pour l'ordinateur A, on voit que les 24 premiers bits du masque de sous-réseau sont à 1.
  Plutôt que d'écrire : 192.168.0.7 / 255.255.255.0, on préférera souvent écrire 192.168.0.7 / 24.
- Chez vous il est probable que personne ne se soit posé toutes ces questions car votre box familiale contient également ce que l'on appelle un **serveur DHCP** qui attribue automatiquement une adresse IP, un masque de sous-réseau et la passerelle à tous les ordinateurs que l'on branche sur le réseau familial. Un tel serveur existe aussi à l'école.

A faire :

Soit l'adresse IP : 172.16.5.10 / 28
- Quel est le masque de sous-réseau correspondant ?
- Combien peut-on mettre de machines différentes dans ce réseau ?

Soit l'adresse IP : 45.178.30.1 / 255.255.0.0
- Quelle est la plage d'adresses IP visibles par cette adresse ?
- Réécrire cette adresse IP plus simplement.

5) Ports

Sur un ordinateur, il y a souvent plusieurs applications différentes qui utilisent le réseau simultanément. Si on est par exemple en train de charger 2 pages web différentes tout en regardant une vidéo youtube et que le service de mise à jour de l'ordinateur se met en route, cela fait 4 « utilisations » simultanées d'internet. Pour que l'ordinateur sache à laquelle transmettre chaque paquet reçu, on attribue à chacune de ces utilisations un **port** spécifique sous la forme d'un entier sur 2 octets. Certains ports sont fixes (un serveur web utilise le port 80 ou le port 443) d'autres sont aléatoires (client web, client de messagerie,…)

6) Commandes réseau utiles

	Linux	Windows
Quelles sont mes adresses MAC et IP ?	`ip a`	`ipconfig /all`
Quelle est l'adresse IP de ma passerelle ?	`ip r`	`ipconfig /all`
Liste des adresses MAC que mon ordinateur connaît sur le LAN	`ip n`	`arp -a`
Tester la connexion entre mon ordinateur et le site tfontanet.free.fr	`ping tfontanet.free.fr`	`ping tfontanet.free.fr`
Liste des routeurs rencontrés pour atteindre le site tfontanet.free.fr	`traceroute tfontanet.free.fr`	`tracert tfontanet.free.fr`

A faire sur le chromebook :

- Utilisez les commandes ci-dessus pour déterminer l'adresse MAC et l'IP de l'interface réseau de votre machine virtuelle Linux, le masque de sous réseau associé, et l'IP de la passerelle.
- Quelle est la plage d'adresse IP qui est dans le même LAN que votre machine virtuelle ?
- Vérifiez que l'IP de votre passerelle en fait bien partie.

- Dans les paramètres du chromebook, sélectionnez la connexion wifi en cours et affichez l'adresse MAC et l'IP de votre carte wifi, le masque de sous réseau associé, et l'IP de la passerelle. Trouvez-vous les mêmes valeurs que ci-dessus ?
- Quelle est la plage d'adresse IP qui est dans le même LAN que votre chromebook ?
- Demandez à vos voisins de classe les IP de leurs cartes wifi. Sont-ils dans le même LAN que votre chromebook ?

- Envoyez un ping à un de vos voisins.
- Envoyez un ping au site www.youtube.fr. Quelle est l'adresse IP de ce site ?
- Combien de routeurs avez vous traversé pour atteindre ce site ? Est-ce que ce sont les mêmes que vos voisins ?

II) Modèle TCP/IP et protocoles

L'une des forces d'internet est sa souplesse. Cette souplesse a été rendue possible notamment grâce à une grande modularité et un bon découpage des tâches à accomplir. Pour chacune de ces tâches à accomplir, on a défini un certain nombre de règles de communication appelées **protocole** (Par exemple : HTTP, TCP, IP, DHCP, …). Puis, ces protocoles ont été répartis en couches successives bien identifiées communiquant les unes avec les autres.

1) Un découpage en couches successives

On distingue historiquement deux découpages en couches : le **modèle OSI** et le **modèle TCP/IP**. Nous nous intéresserons principalement au modèle TCP/IP.

OSI	TCP/IP	Tâches	Adresses	Protocoles	Données	Matériel
7-Application 6-Présentation 5-Session	Application			DNS, HTTP, FTP, POP, IMAP, SMTP, CIFS, NFS, SSH	Données Message	
4-Transport	Transport	Découpage des gros fichiers en morceaux Gestion des erreurs de transmissions Réassemblage final des gros fichiers	Ports	TCP, UDP	Segment	
3-Réseau	Internet	Routage des données d'une machine à l'autre jusqu'à la bonne destination	IP	IP, ARP, DHCP	Datagramme (Paquet)	Routeur
2-Lien	Lien	Communication entre 2 machines directement connectées ou via un switch (qui sont donc sur le même LAN)	MAC	Ethernet	Trame	Switch
1-Physique		Signaux électriques ou lumineux			Bits	Hub

2) Le protocole TCP (Transmission Control Protocol)

- Ce protocole permet à l'ordinateur de départ de créer une connexion avec l'ordinateur destinataire, de vérifier que ce dernier est prêt à recevoir des données et de garantir ensuite un échange fiable et sans pertes.
- Le TCP de l'émetteur découpe les gros envois de données en morceaux appelés segments qu'il numérote. Cela permet d'éviter de devoir tout renvoyer quand un segment est corrompu à l'arrivée et cela permet également de fluidifier les envois (si un petit fichier est envoyé après un très gros, le petit fichier n'est pas obligé d'attendre la fin de l'envoi du très gros).
- Le TCP du récepteur vérifie que chaque segment est bien arrivé. Au besoin, il redemande à l'émetteur les segments manquants ou corrompus, et les réassemble dans le bon ordre.

3) Le protocole IP (Internet Protocol)

- Ce protocole permet d'acheminer les données vers la bonne destination.
- Entre l'émetteur et le récepteur, il y a en général de nombreux **routeurs** connectés les uns aux autres formant comme une toile d'araignée. Le protocole IP va permettre que les données soient envoyées de routeur en routeur vers la bonne destination finale.
- En revanche, IP ne garantit pas l'ordre de réception des paquets, ni même qu'ils ne se perdent pas. Des paquets du même message peuvent emprunter des chemins différents selon l'encombrement du réseau.

4) Envoi d'un message et encapsulation des données

Supposons que je veuille afficher sur mon ordinateur la page d'accueil d'un site internet hébergé sur un ordinateur distant. Mon navigateur va formuler une demande qui va ensuite être formatée par mon système d'exploitation pour pouvoir traverser internet. Regardons ci-dessous les différentes étapes du processus :

Départ de mon ordinateur :

Mon navigateur va générer un message respectant le protocole HTTP (ci-dessous en bleu foncé à droite)
Puis ce message va traverser les différentes couches du modèle TCP/IP et recevoir à chaque fois un entête supplémentaire. On dit que l'on **encapsule** le message. A la fin la **trame Ethernet** ci-dessous est envoyée sur mon réseau local.

Couche Lien **Entête Ethernet**	Couche Internet **Entête IP**		Couche Transport **Entête TCP**			Couche application **Message initial HTTP**
Mac src : 40:E5:67:22:AB:81 Mac dest : 67:3F:65:B9:0C:56	IP src : 192.168.0.34 IP dest : 212.27.63.136	TTL 64	Port src : 52318 Port dest : 80	Msg n°1	Flag	GET / HTTP/1.1 Host: tfontanet.free.fr

Remarques :

- « IP src » et « Mac src » correspondent aux adresses IP et MAC de mon ordinateur et sont nécessaires pour que le serveur distant puisse me répondre quand il aura reçu le message.
- « IP dest » est l'IP du serveur distant. Si mon ordinateur ne la connaît pas, il doit faire au préalable une **requête DNS** pour savoir à quelle adresse IP correspond le site « tfontanet.free.fr ».
- Grâce à son masque de sous-réseau, mon ordinateur voit que « IP dest » n'est pas sur le même LAN que lui. Il doit donc envoyer la trame sur sa passerelle. « Mac dest » est donc l'adresse MAC de cette dernière. Si mon ordinateur ne la connaît pas, il doit faire au préalable une **requête ARP** pour savoir quelle est l'adresse MAC de la passerelle.

Traversée d'un switch :

Le switch est un équipement qui ne connaît que les adresses MAC du réseau local. Il a en général 8, 16 ou 24 ports (prises RJ45) et il tient à jour sa **table CAM** dans laquelle il enregistre quelle(s) adresses MAC sont accessibles via quels ports physiques.
Quand la trame arrive sur un switch, celui-ci lit « Mac dest » dans l'entête Ethernet et regarde dans sa table CAM sur quel port il doit envoyer cette trame.

Traversée d'un routeur :

Le routeur est un équipement qui interconnecte plusieurs réseaux locaux grâce à ses interfaces (= cartes réseau). Il met à jour en permanence sa **table de routage** et y enregistre quelles plages d'adresses IP envoyer à quelle interface.
Quand la trame arrive sur un routeur, celui-ci désencapsule l'entête Ethernet qui est obsolète, lit « IP dest » dans l'entête Internet et regarde dans sa table de routage sur quelle interface il doit l'envoyer. Il décrémente également le compteur TTL. Une fois TTL arrivé à 0, le paquet est détruit. Cela permet d'éviter que des paquets perdus n'encombrent inutilement le réseau.
Puis le routeur réencapsule le paquet avec son adresse MAC et celle du routeur de destination.

Arrivée sur le serveur :

L'ordinateur va désencapsuler adresses MAC, IP et ports, puis adresser le message HTTP initial au logiciel serveur web qui écoute le port destination. En réponse, ce logiciel va renvoyer un message beaucoup plus long qui contiendra le code html de la page d'accueil demandée. L'ordinateur va alors réencapsuler ce nouveau message en inversant par rapport à tout à l'heure les ports, IP et MAC sources et destination.

La même chose très bien expliquée en vidéo : https://www.youtube.com/watch?v=_0thnFumSdA

III) Pour aller plus loin

Quelques vidéos complémentaires :

- Récapitulatif de ce qui précède : https://www.youtube.com/watch?v=dCknqcjcItU
- Protocole ARP : https://www.youtube.com/watch?v=F3Jn_aqloVQ
- Masques de sous-réseau : https://www.youtube.com/watch?v=ImAtjunA_hI
- Serveur DNS : https://www.youtube.com/watch?v=qzWdzAvfBoo
- Serveur DHCP : https://www.youtube.com/watch?v=44ONmO8qDw8
- Adresses IP privées et translation d'adresses NAT et PAT : https://www.youtube.com/watch?v=jq3SLuhIyPI

Et un cours remarquable de l'EPFL qui reprend ce qui précède :

- https://www.youtube.com/watch?v=U6Uqf5xsaSI&list=PLOapGKeH_KhFkfZDf5B-AKXmNIXEPpn4a