Proposition de support : Sciences numériques et technologie de seconde générale et technologique

Comprendre le fonctionnement d'Internet : Cours Débranché

Cette ressource regroupe 8 activités sur le thème Internet. Pour être complet sur ce thème, il faudrait traiter, en plus, les réseaux pair-à-pair et les réseaux physiques.

Conception	Jean-luc FERRAUD	Discipline : Sciences économiques et sociales	Académie de Grenoble
	Éric ROLLAND	Discipline : Sciences de la vie et de la Terre	Académie de Grenoble
	Patrice DUCROZ	Discipline : Mathématiques	Académie de Grenoble
	Antoine RUEZ	Discipline : Sciences Industrielles de l'Ingénieur	Académie de Grenoble
	Raphaël GROSBOIS	Discipline : Physiques et Chimie	Académie de Grenoble
	Zakari BERREMILI	Discipline : Eco-Gestion option (D) Informatique	Académie de Grenoble

Thématiques du programme

Internet

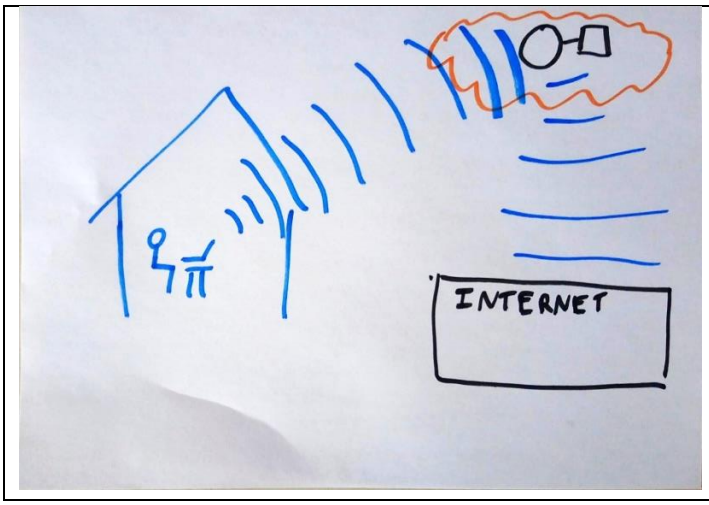
Contenus	**Capacités attendues**
Protocole TCP/IP : paquets, routage des paquets	Distinguer le rôle des protocoles IP et TCP. Caractériser les principes du routage et ses limites. Distinguer la fiabilité de transmission et l'absence de garantie temporelle.
Adresses symboliques et serveurs DNS	Sur des 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 ainsi que 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.

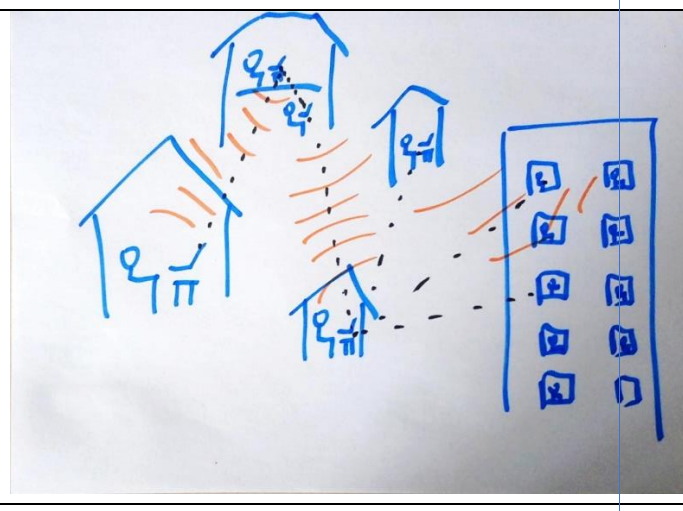
Comprendre le fonctionnement d'Internet

La rencontre avec le groupe d'élèves peut commencer par un partage de la représentation d'Internet.

Activité 1 : Dessiner Internet.

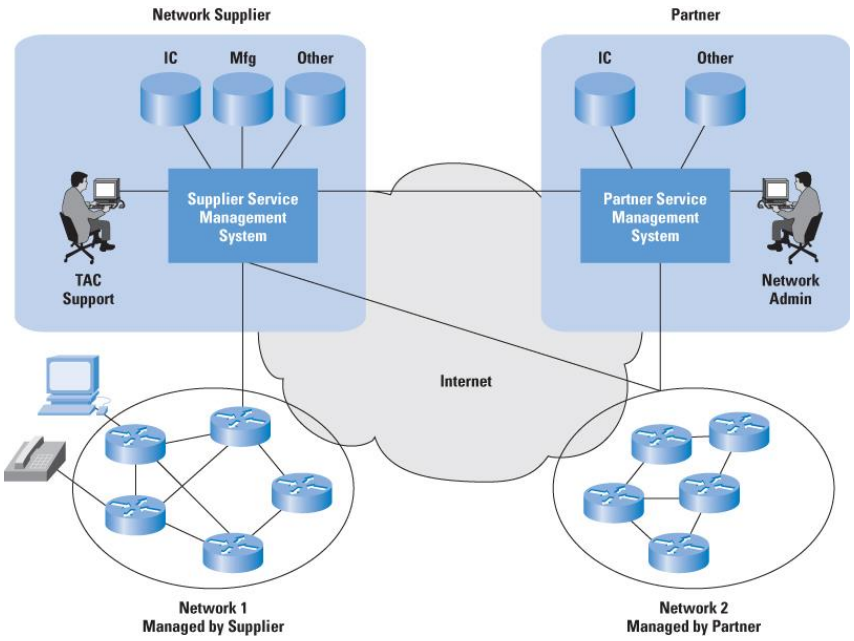
Au collège, la très grande majorité des élèves pense qu'Internet fonctionne avec les satellites. Il est donc possible d'obtenir le type de représentation ci-dessous.





Bilan : guider les élèves pour arriver à une représentation faisant apparaître des **supports de transmission** (ondes, câbles...), **périphériques finaux** (ordinateurs, smartphones, centres de données...) et **périphériques intermédiaires** (commutateurs « switch », routeurs, pare-feu, satellites...).

Exemple concret :



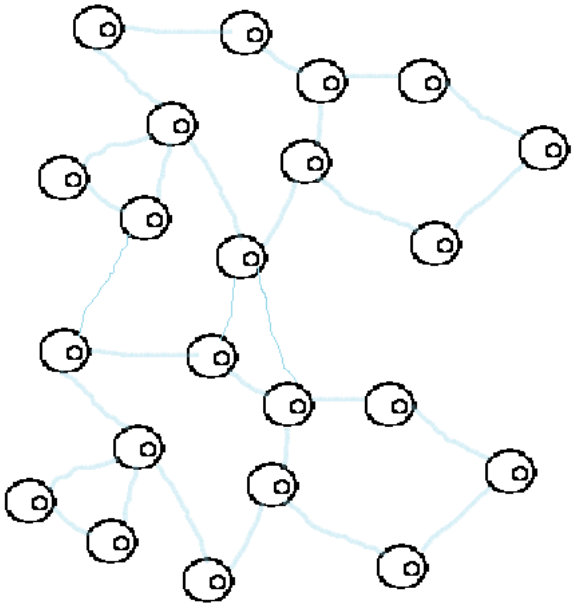
Activité 2 : Echanger des messages.

L'exercice demande de déplacer des chaises, les professeurs y sont habitués.

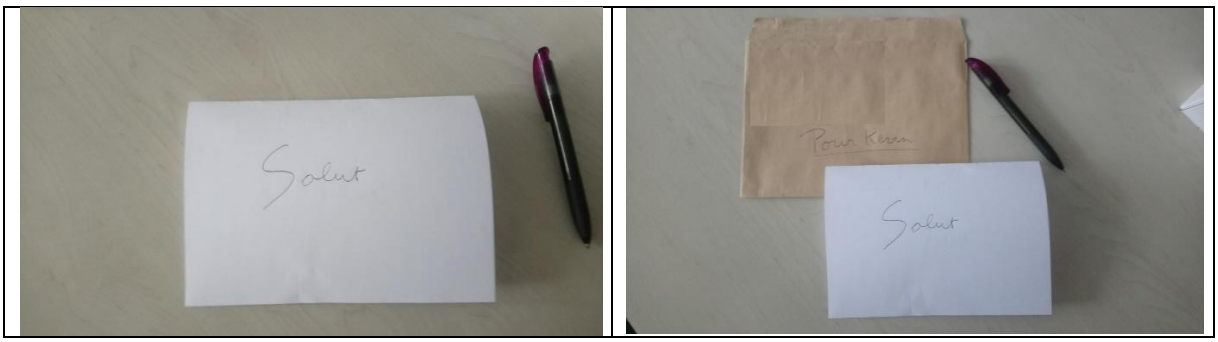
Chaque élève doit se placer où il veut à une longueur de bras minimum de chaque camarade. Il faut éviter de créer un grand cercle (anneau). Il peut y avoir plusieurs chemins pour aller au même endroit. En routage on appelle cela de la redondance.

Une fois les élèves en position :

Il faut leur expliquer qu'ils sont à présent des ordinateurs particuliers dotés de la capacité de transmettre des messages (de les router).
Toutefois ils ne peuvent envoyer une information (sous forme d'un petit mot) qu'à un voisin direct.



Demander à un élève (Farid) d'écrire un message à un camarade lointain (et éventuellement de le mettre dans une enveloppe).



Il ne peut le confier qu'à l'un de ses voisins directs.
Il est possible qu'il n'ait pas mis le destinataire (ce sera à exploiter)
Donc pour l'instant nous avons une enveloppe qui contient le message

En toute logique, l'enveloppe passe de main en main, la consigne est de ne jamais la renvoyer à quelqu'un qui l'aurait déjà eu en main. Pour une meilleure visualisation, on peut demander aux élèves, par qui est passé le message, de se lever.
Il y a de fortes chances que du premier coup « Kévin » reçoive l'enveloppe.

Pour l'instant nous pouvons modéliser l'objet ainsi :

L'enveloppe	Message
Destinataire	Salut

Question : À la classe. Est-ce que Kévin a bien reçu le message ?

OUI

Imaginons que Kévin et Farid soient à une distance de 100 ou 1000 km l'un de l'autre.

Farid peut-il savoir si Kévin a bien eu le message ?

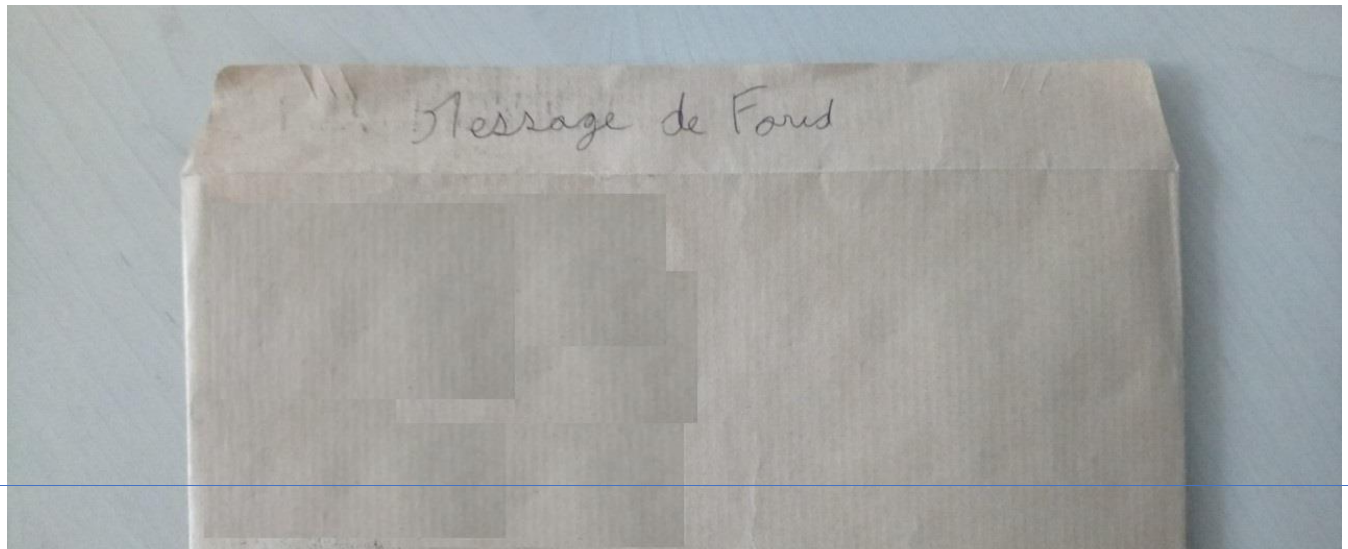
NON

COMMENT REMEDIER AU PROBLEME

Kévin doit accuser réception, dire qu'il a bien reçu le message.
C'est le mécanisme d'accusé de réception (acquittement, poignée de main, *acknowledgment*)

Oui mais comment va répondre Kévin ?

Il faut que Farid indique sur le message qu'il en est l'expéditeur.



Bilan et approfondissements :

Le message ne peut pas voyager seul, il lui faut un contenant avec des informations supplémentaires (expéditeur, destinataire, accusé de réception) pour s'assurer qu'il arrive à destination.

L'enveloppe		Message
Destinataire	Expéditeur	Salut

En réseau informatique, on appelle cela un paquet et les informations supplémentaires sont normalisées dans les protocoles IP et TCP.

Entête IP	@IP SOURCE	@IP DESTINATION	Données IP/ Message

La seule différence, c'est que le paquet est transporté de manière électromagnétique et selon un code composé que de 0 et de 1 appelé bits (Binary digIT).

Par exemple 1000001 veut dire A et 1011010 veut dire Z. C'est le code Ascii[1].

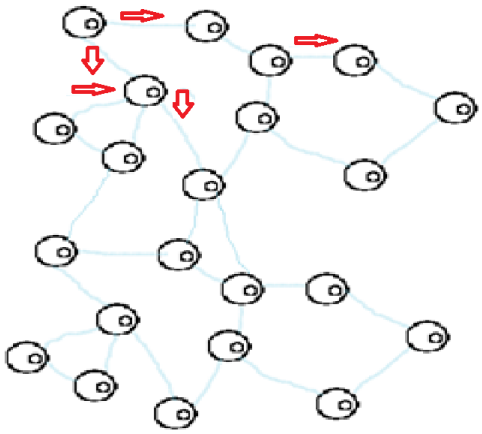
L'adresse IP est également transmise en binaire. Par souci de simplicité, on l'écrit souvent en « décimal pointé » x.x.x.x où x est compris entre 0 et 255. Ex : 172.31.0.1, 222.5.7.14. Ces adresses IP peuvent s'apparenter à un code postal : elles sont hiérarchiques et permettent de localiser le destinataire afin de lui envoyer des paquets.

Petit exercice pour aller plus loin sur les adresses IP en ANNEXE 2.

Activité 3 : Echangez des grands messages.

Le message est maintenant inscrit sur une feuille au format A4, trop grande pour être placée dans l'enveloppe (sans la plier). Idée des élèves (ou suggestion) : découper la feuille en morceaux plus petits qui tiennent dans l'enveloppe.

On met chaque morceau dans une nouvelle enveloppe et on relance le processus avec comme consigne aux participants de transmettre les enveloppes le plus rapidement possible, en utilisant notamment les divers chemins redondants à disposition.



On fera vite le constat qu'à l'arrivée on reçoit un *puzzle* qu'il est difficile de reconstituer.

[1] https://fr.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

Question : Comment aider le destinataire à reconstituer l'information ?

Numéroter les morceaux !

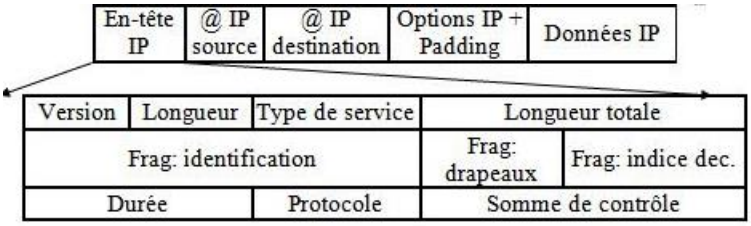
L'enveloppe Message

N°	Destinataire	Expéditeur	Morceau de la photo

Bilan et approfondissements :

Cette technique est utilisée par les protocoles TCP (création de segments...) et IP (fragmentation des paquets par certains routeurs) pour adapter les données aux capacités de transmission des réseaux physiques (MTU : Maximum Transmit Unit). Des champs spécifiques apparaissent dans les en-têtes IP et TCP.

Entête IP Avec N°	@IP SOURCE	@IP SOURCE	Fraction du message.



Activité 4 : réflexion sur la perte de paquets.

À ce moment de l'apprentissage, il est possible d'expliquer aux élèves que certains paquets peuvent se perdre où ne jamais arriver à destination (suite à la rupture d'un lien, mauvais routage...)

Question : Comment savez-vous qu'un paquet n'est jamais arrivé à destination ?

Réponse attendue : la source n'a pas reçu d'accusé de réception.

Oui mais au bout de combien de temps considère-t-on un paquet perdu dans les protocoles TCP/IP ?

Question : Que feriez-vous si un élément n'arrive pas à destination (pas d'accusé de réception) ?

Réponse *attendue :* *renvoyer* le paquet

Question : Que devient un paquet qui se perd et qui ne trouve pas sa destination, est-ce qu'il ère à l'infini sur la toile ?

Bilan et approfondissements :

Dans le protocole TCP/IP, la durée au-delà de laquelle on considère que le paquet est perdu est appelée RTT[2] et est comprise entre 0 et 90 ms. C'est très court à échelle humaine mais tout va très vite dans un câble, donc 90ms est un temps assez long pour considérer un paquet perdu.

[2] https://fr.wikipedia.org/wiki/Transmission_Control_Protocol

De plus, un paquet a une durée de vie TTL (Time To Live, 8 bits) : Ce champ est initialisé par l'émetteur puis diminué par chaque routeur traversé. Quand le TTL arrive à 0 (TTL de départ = 255 ou 127), le paquet est supprimé par le routeur qui avertit l'expéditeur (ex: principe de fonctionnement la commande *traceroute*).

Activité 5 : sécurité d'un message

Refaire le jeu de l'enveloppe. Demander à l'expéditeur d'envoyer un message personnel (quelque chose qui ne doit pas être connu par une tierce personne). Avant l'envoi, prévoir quelques complices sur le chemin de transmission dans le rôle de cyber-voyous (Hacker, Black-Hat: ils devront lire le message à haute voix s'il passe par eux).

Question : Comment faire pour éviter que l'information ne soit dévoilée ?

Réponse attendue : il faut *chiffrer* le message

Il est possible à ce moment-là de créer une séquence pour mettre en place des mécanismes ludiques de chiffrement (chiffre de César...).

Question : Est-il possible de faire des messages que seul le récepteur peut déchiffrer ?

OUI, s'il est le seul à disposer des informations pour le déchiffrer.

Il est possible d'évoquer les notions de chiffrement asymétriques, certificats... sans rentrer dans les détails

Pour aller plus loin :

Question : Pourquoi l'Etat a longtemps obligé les sociétés agréées fournissant des services de chiffrement sur le territoire français à procurer au service central de la sécurité des systèmes d'information les clés de chiffrement employées ?[3]

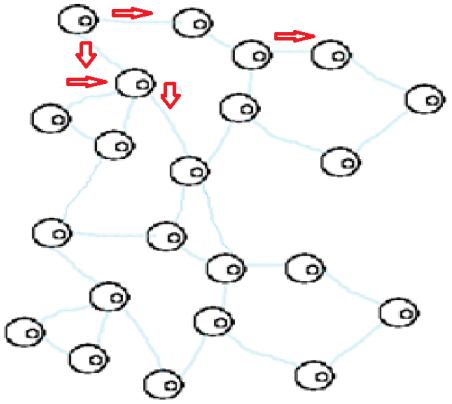
Les réponses doivent permettent aux élèves de comprendre grâce à une discussion qu'il est important qu'il y ait un régulateur. Sinon des personnes mal intentionnées pourraient en secret préparer des opérations illégales et dangereuses. Il faut préciser aussi que la grande majorité des conversations ne sont pas écoutées, c'est sous la direction d'un procureur et d'une enquête de police que se font les écoutes quand des indices permettent de suspecter des délits. La possibilité d'utiliser des mécanismes de chiffrement sans porte dérobée est encore en débat.

RTT ou RTD (Round-Trip Time ou Round-Trip Delay) : Il s'agit du délai exprimé en ms du temps de réponse. Ce délai indique le temps mis par le paquet pour atteindre sa destination et revenir. Plus ce délai est proche de 0, au plus la qualité de la connexion est bonne

[3] https://fr.wikipedia.org/wiki/Chiffrement

Activité 6 : sensibiliser au rôle du DNS.

On peut adapter le jeu de rôle initial en ajoutant une contrainte supplémentaire (analogie possible avec l'envoi de SMS) : la transmission du message à Kévin nécessite de connaître son adresse (son numéro de téléphone pour un SMS)



Question : Farid connaît-il par cœur le numéro de téléphone de Kévin ?

Réponse attendue : Non

Question : Comment peut-il l'obtenir ?

Réponse attendue : il cherche dans ses contacts

Question : et si le numéro de Kévin ne s'y trouve pas ?

Réponse attendue : il demande à un ami de Kévin s'il peut lui fournir son numéro

Bilan :

L'application *contacts* joue le rôle de serveur DNS[4]. : elle permet de retrouver le numéro de téléphone (adresse IP) d'une personne (nom de machine).

Activité 7 : calculer une métrique de routage

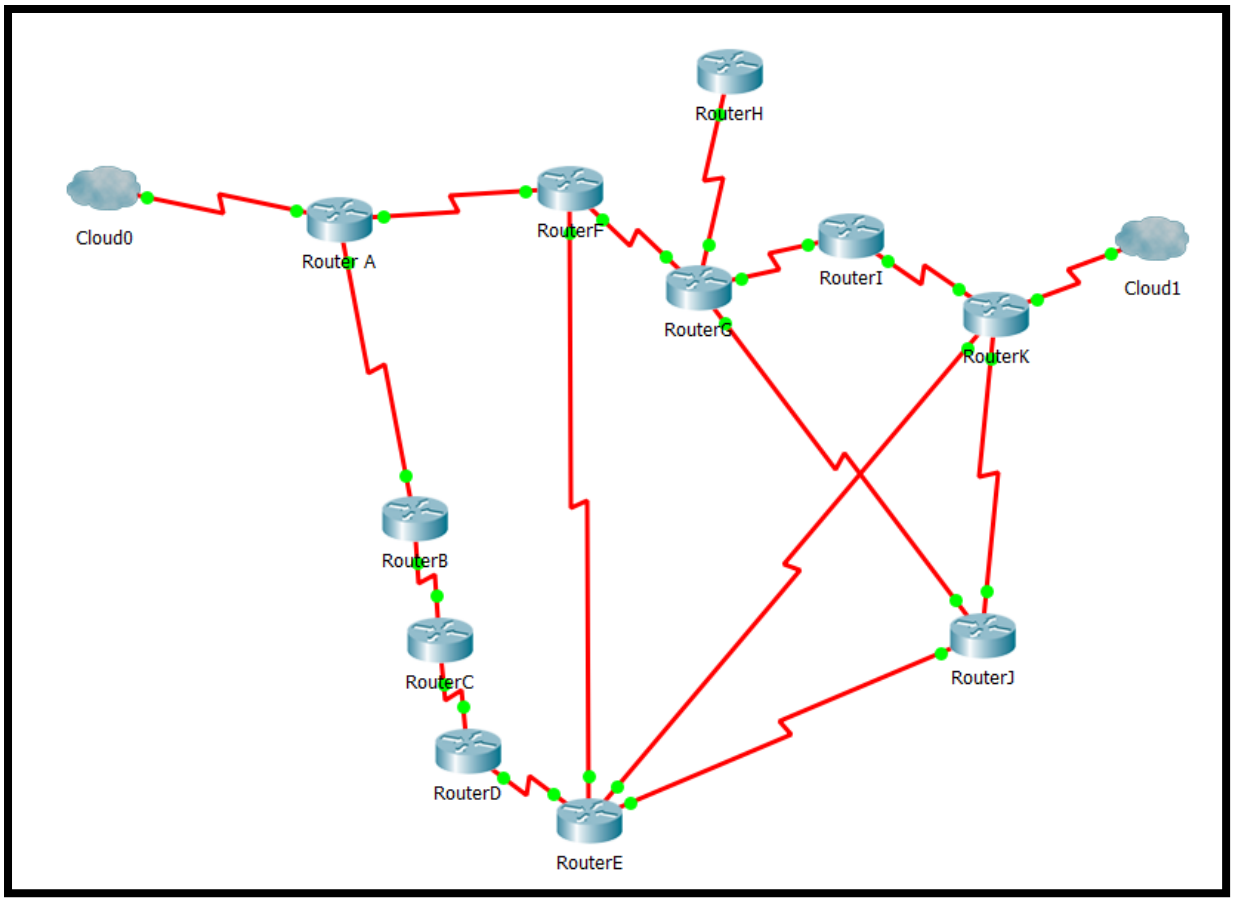
Un paquet suit un chemin sur le réseau, pour cela il doit utiliser les protocoles de routages. On peut voir le chemin parcouru par un paquet avec la commande traceroute (tracert, Cf ANNEXE 3)

Routing Information Protocol *(**RIP**, protocole d'information de routage) est un protocole de routage IP de type Vector Distance (à vecteur de distances) s'appuyant sur l'algorithme de détermination des routes décentralisé Bellman-Ford. Il permet à chaque routeur de communiquer aux routeurs voisins la métrique, c'est-à-dire la distance qui les sépare d'un réseau IP déterminé quant au nombre de sauts ou « hops » en anglais.* https://fr.wikipedia.org/wiki/Routing_Information_Protocol

Dans la vie courante, on calcule une distance en m (ou km), pour le protocole RIP c'est un peu ce que nous allons faire. Nous allons calculer les distances en nombre de routeurs à traverser (la longueur du câble n'a pas d'importance). Et choisir le chemin le plus court pour diriger/orienter nos paquets. Chaque paquet est envoyé au voisin faisant office de routeur ou étant uniquement un routeur voisin qui est sur le chemin le plus court.

Ici nous devons aller de cloud 0 à cloud 1.

[4] Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements. https://fr.wikipedia.org/wiki/Domain_Name_System



Question : Quel est le chemin le plus court ?

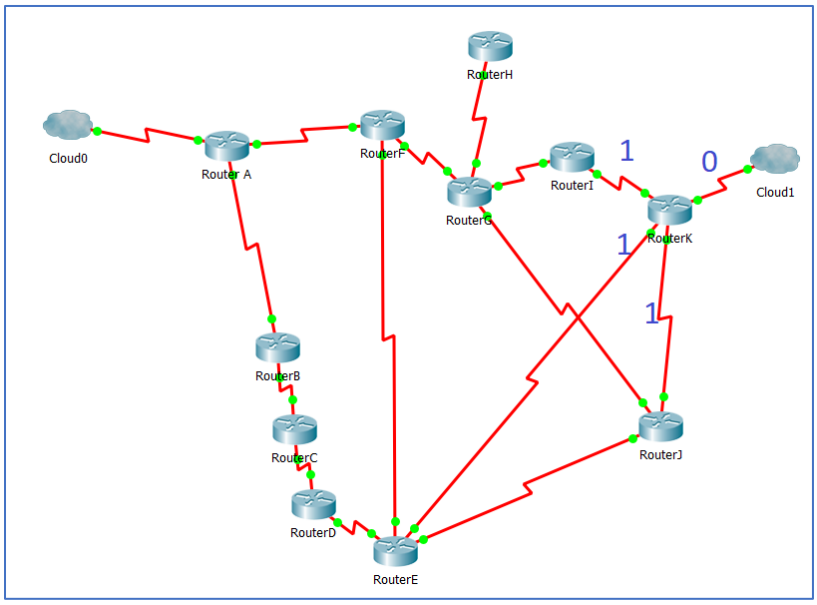
Cloud0 – A – F – E – K – Cloud1

Question : Comment le système le sait-il ?

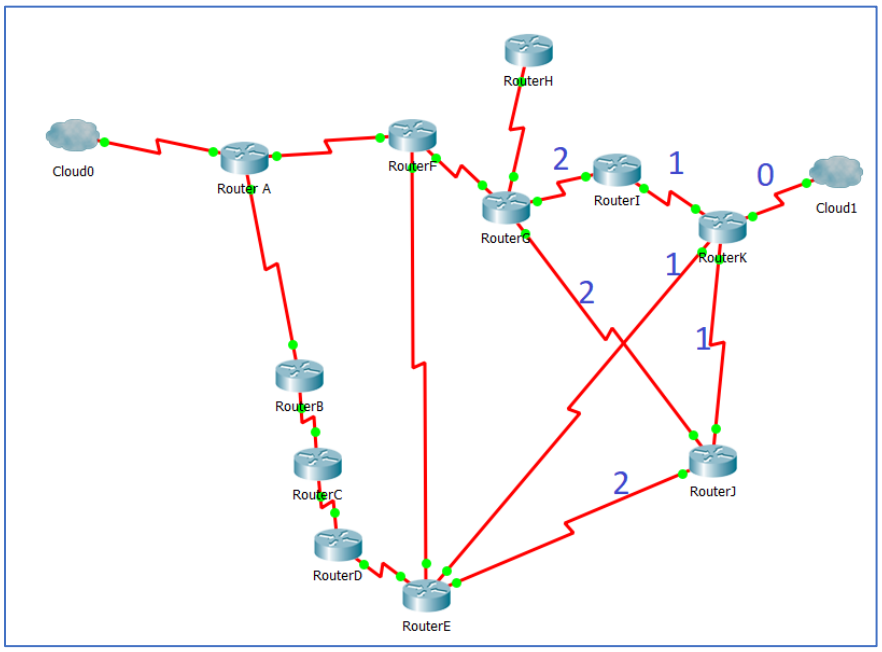
En faisant des calculs, une suite de calcul … Donc un Algorithme.

Voyons comment fonctionne l'algorithme de calcul qui est un des premiers protocoles de routage. Nous verrons celui-ci car il est simple mais sachez que les protocoles utilisés sur Internet sont un peu plus compliqués mais fonctionnent sur des principes similaires basés sur la distance et/ou le coût et appelé métrique.

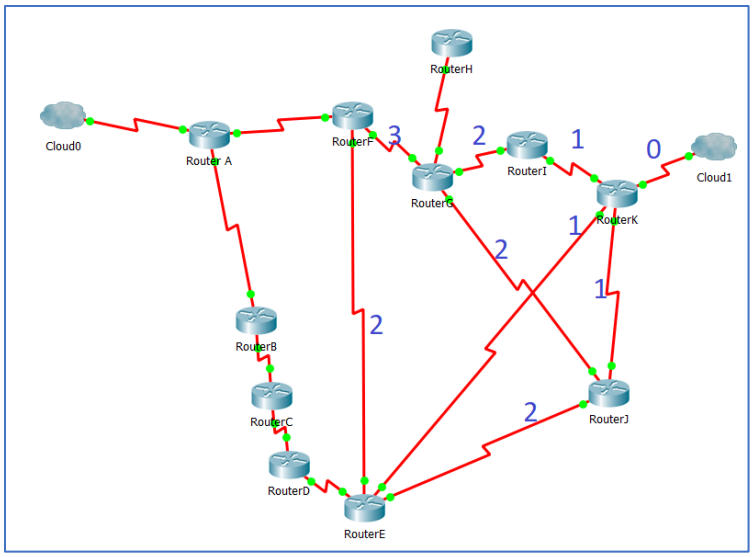
Partons de la destination et écrivons la distance qui nous en sépare.
Sur la dernière branche je suis à une distance 0 de l'arrivée.
Sur la branche juste après à une distance 1 du routeur.



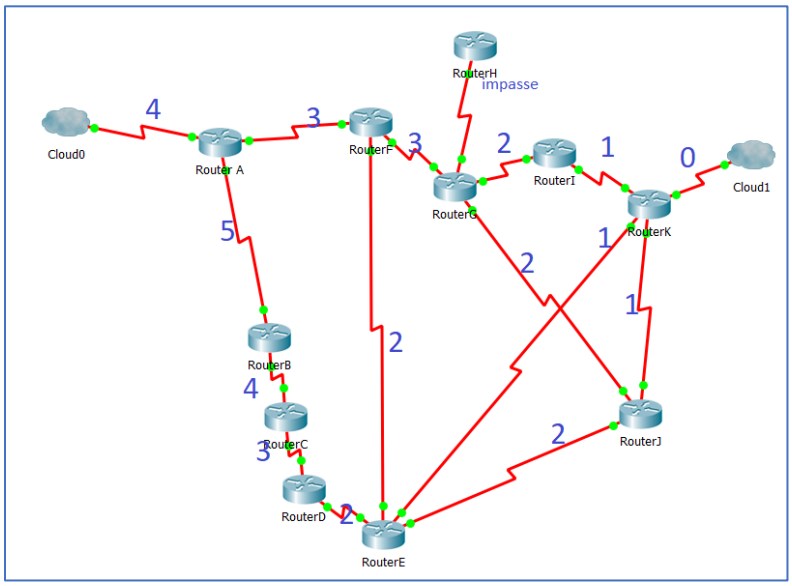
Je continue
1+1=2



Pour le tronçon entre G et F ce sera 3, 2+1=3
Par contre, pour le tronçon entre E et F j'ai le choix entre 1+1 = 2 et 2+1=3.
Je choisis le plus petit donc 2.



Et ainsi de suite

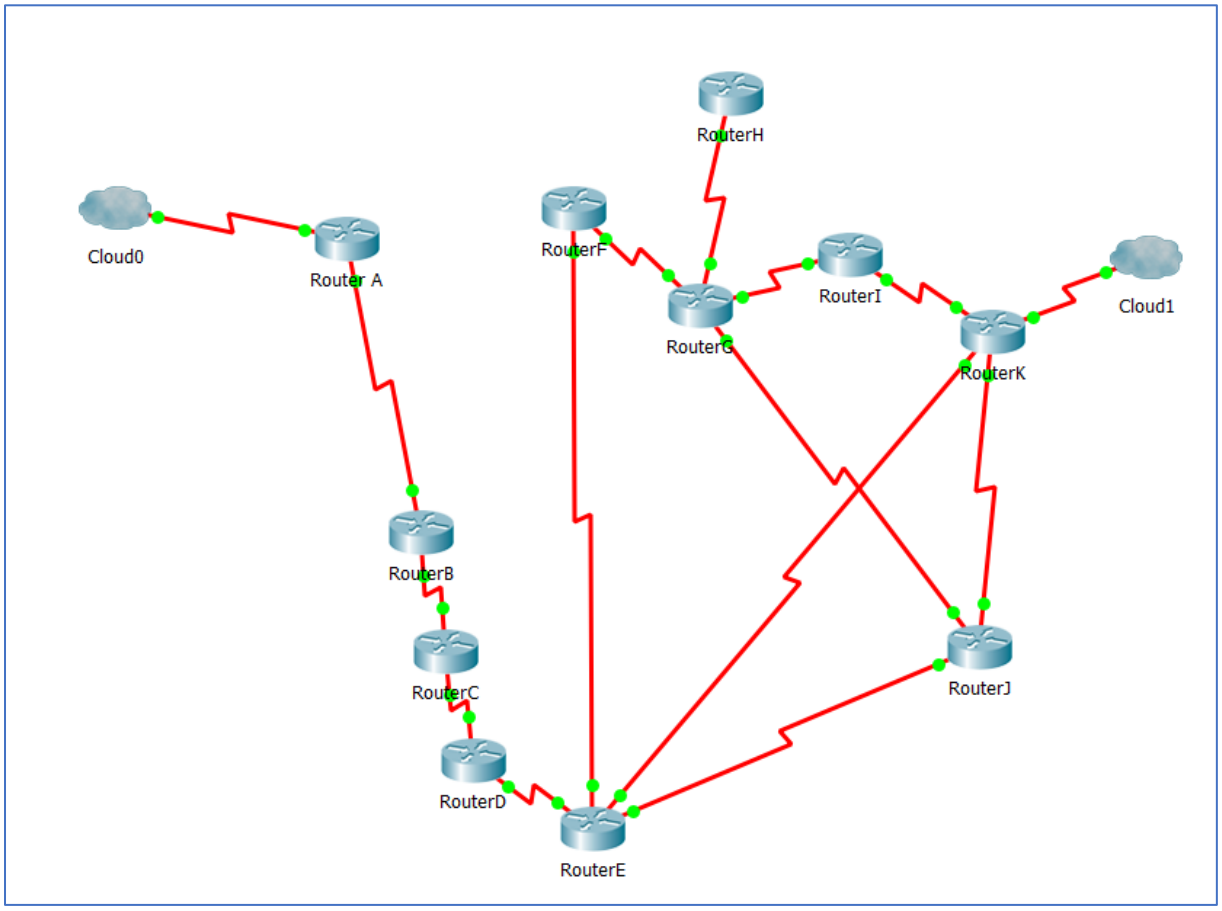


À présent le système a rempli ses tables de routage en destination de cloud 0.
Il prendra le chemin le plus court qu'il a calculé sans intervention humaine. Avec un Algorithme.

4 – 3 – 2 – 1

A – F – E – K

Et s'il y a un incident sur la ligne A-F !



Utilisez la même méthode pour calculer le nouveau chemin.

Le protocole IP fera la même chose automatiquement pour trouver un nouveau chemin.
Cela s'appelle de la tolérance aux pannes.

C'est du routage dynamique par opposition au routage statique qui ne se fait pas tout seul mais par le paramétrage d'un technicien.

Activité 8 : Réflexion sur la neutralité d'Internet

Nous avons abordé ici certains principes techniques qui régissent le web, la toile, Internet.
Est-ce que vous trouvez ces principes égalitaires ?

Faut-il que Internet soit égalitaire ?

Pensez-vous possible qu'un état puisse changer la règle de neutralité ? Comment ?

Qui garantit la neutralité d'internet en France et en Europe ?

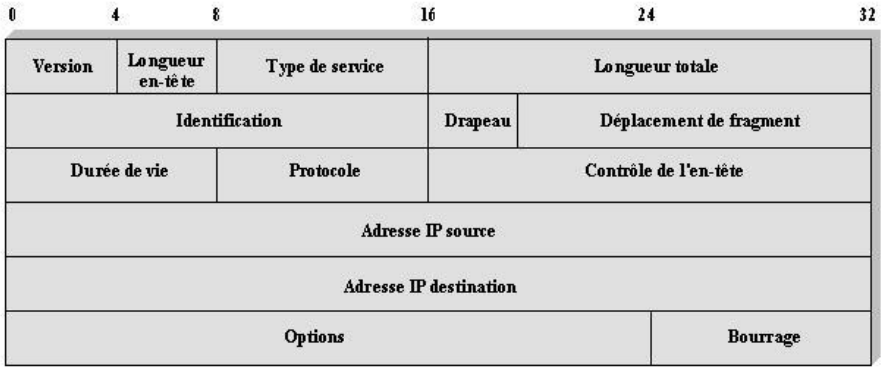
Ce point peut être le moment d'une évaluation.
Réaliser des exposés en utilisant un outil informatique de diaporama.
Possibilité de mettre en ligne ces diaporamas sous forme numérique (page HTML, WordPress, etc…)
Ces exposés doivent mettre en parallèle la technologie et les pratiques humaines.
Cf. ANNEXE 4.

ANNEXE 1

UN PAQUET

https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2002ttnfa03/Monnier-Philippe/2.3.htm

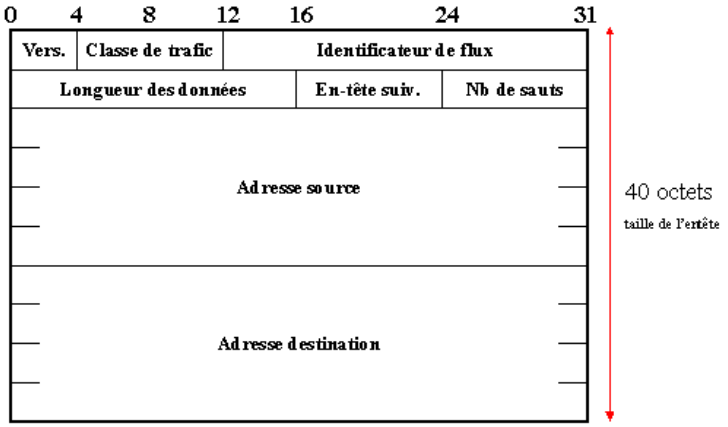
Voici le format de l'entête IPV4 :



Description des champs :

- Version (4 bits) : Dans notre cas 4 (IPv4)
- *Longueur entête (4 bits) :*
  - Longueur de l'entête en mots de 32 bits. La valeur minimale est 5 (20 octets sans option) et le maximum 15 (donc les options sont limitées à 40 octets).
- *Type de service (8 bits) :*
  - Ce champ permet en théorie de distinguer différentes qualités de service, et suppose que tous les paquets ne sont pas traités de la même façon. Ce champ se décompose en 3 bits de priorité (donc 8 niveaux) et trois indicateurs permettant de privilégier le débit, le délai ou la fiabilité. Ces champs sont rarement utilisés dans l'Internet actuel, mais pourraient être utilisés pour les mécanismes de qualité de service actuellement en cours de définition (Diffserv).
- *Longueur Totale (16 bits) :*
  - Il s'agit du nombre d'octets total du datagramme, entête IP compris. Il y a donc une limite de 2^{16}-1 octets.
- *Identificateur (16 bits) :*
  - Ce numéro est affecté par l'émetteur et sert en particulier à identifier les fragments d'un même paquet.
- Indicateurs (3 bits) :
  - Le premier bit est actuellement inutilisé. Deux indicateurs sont utilisés dans le cadre de la fragmentation:
  - *Don't frag* : le paquet ne doit pas être fragmenté si l'indicateur vaut 1.
    More Frag : le paquet est fragmenté et ce n'est pas le dernier fragment si l'indicateur vaut 1.
- *Position du fragment (offset) (13 bits) :*
  - Ce paquet est un fragment, et sa position par rapport au début du paquet initial est donnée en nombre de mots de 8 octets (tous les fragments sauf le dernier sont donc alignés sur des multiples de 8 octets).
- *Durée de vie ou TTL (Time To Live) (8 bits) :*
  - Ce champ est initialisé par l'émetteur puis diminué dans chaque routeur traversé (généralement 1). Quand le TTL arrive à 0, le paquet est abandonné (avec émission d'un message ICMP). Un fragment arrivé à destination voit aussi son TTL diminuer tant que le paquet n'est pas complet, et peut donc être abandonné (message ICMP).
- *Protocole (8 bits) :*
  - Donne le numéro du protocole (par exemple TCP=6, UDP=17, ICMP=1,...) de la couche au-dessus de IP.
- *Contrôle d'entête (16 bits) :*
  - Total de contrôle sur l'ensemble des octets de l'entête. Un paquet erroné est abandonné silencieusement. Il n'y a pas de contrôle sur les données du paquet.
- *Adresse source (32 bits) :*
  - Adresse IP de l'émetteur : adresse unicast, généralement celle de l'interface par laquelle le paquet est envoyé.
- *Adresse destination (32 bits) :*
  - Adresse IP du récepteur : peut être une adresse unicast, multicast ou broadcast.

Voici le format de l'entête IPV6 :



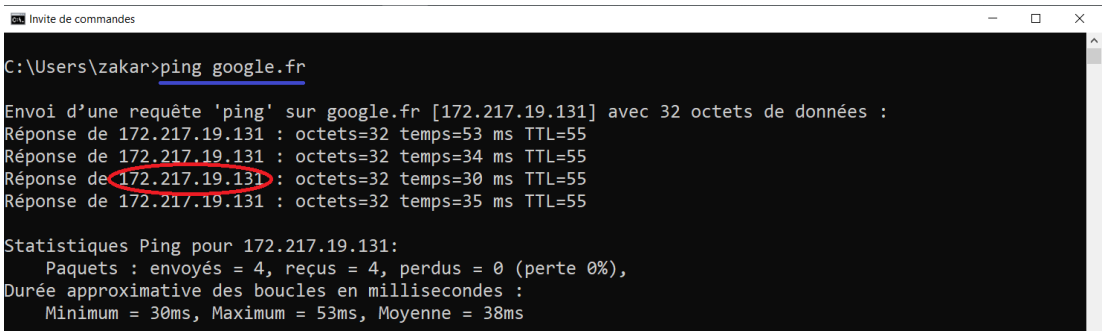
- Description des champs :
- *Version (4 bits) :*
  - Numéro de version. Dans notre cas 6 (Ipv6).
- *Classe de trafic (8 bits) :*
  - Priorité du paquet [RFC 2474].
- *Identificateur de flux (20 bits) :*
  - Qualité de service.
- *Longueur de données (16 bits) :*
  - Longueur du paquet sans prendre en compte les 40 octets de l'entête.
- *Entête suivant (8bits) :*
  - Type de l'entête suivant, du protocole de niveau supérieur ou extension.
- *Nombre de sauts (8 bits) :*
  - Nombre de sauts possibles avant que le paquet ne se détruise.
- *@ source :*
  - Adresse de l'élément qui envoie les données. Celle ci est codée sur 128 bits.
- *@ destination :*
  - Adresse de l 'élément qui va recevoir les données. Celle ci est codée sur 128 bit et peut être différente si l'option routing header est activée.

ANNEXE 2

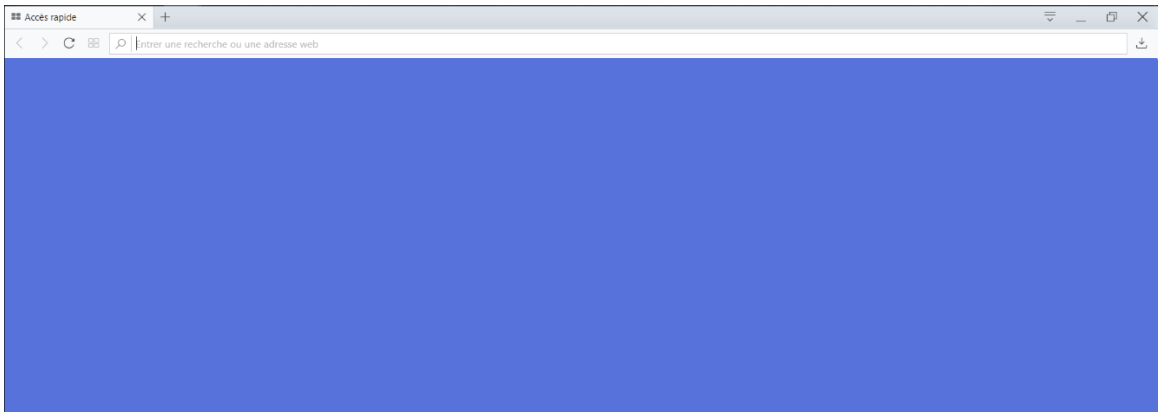
PING GOOGLE

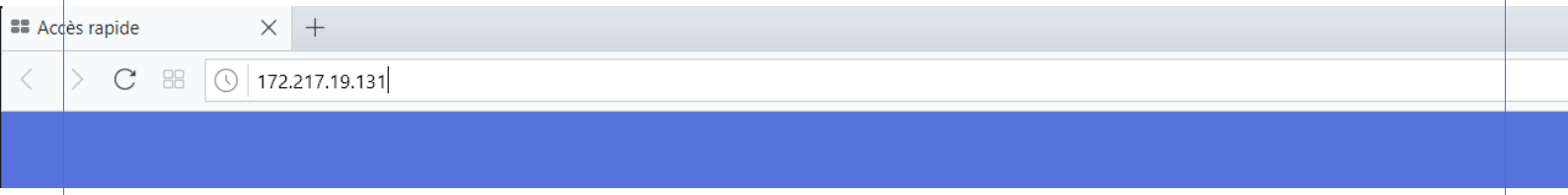
Ping est le nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau IP. La commande mesure également le temps mis pour recevoir une réponse, appelé round-trip time.

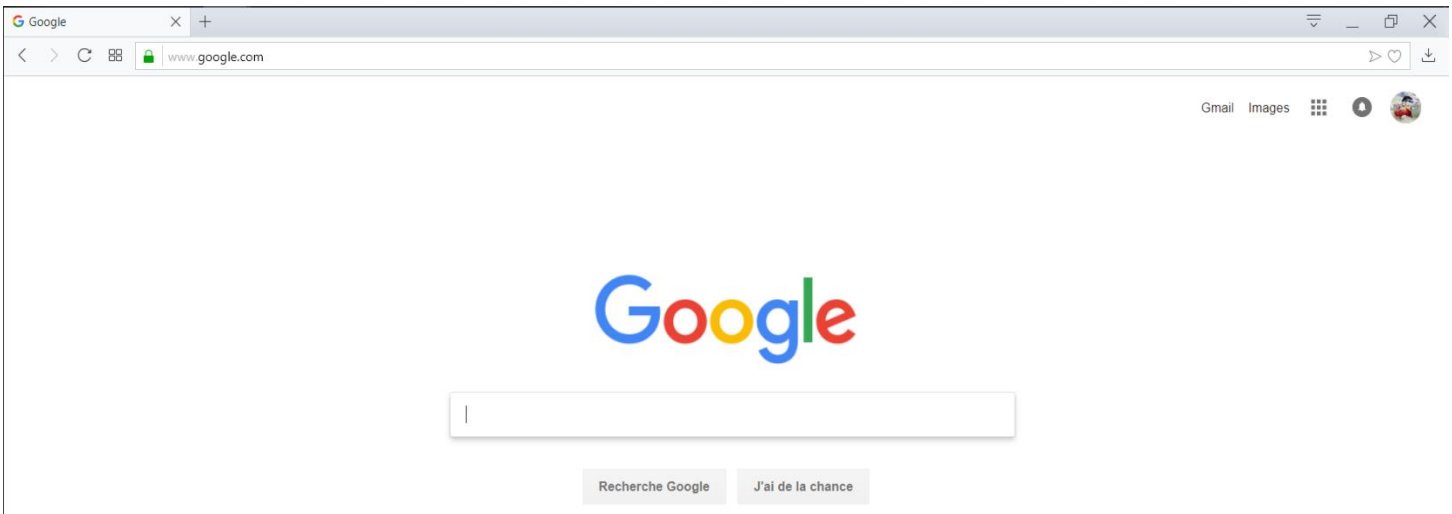
Si je pingue google.fr je vais pouvoir obtenir son adresse IP (ses coordonnées).



À présent je saisie cette adresse IP dans un navigateur.

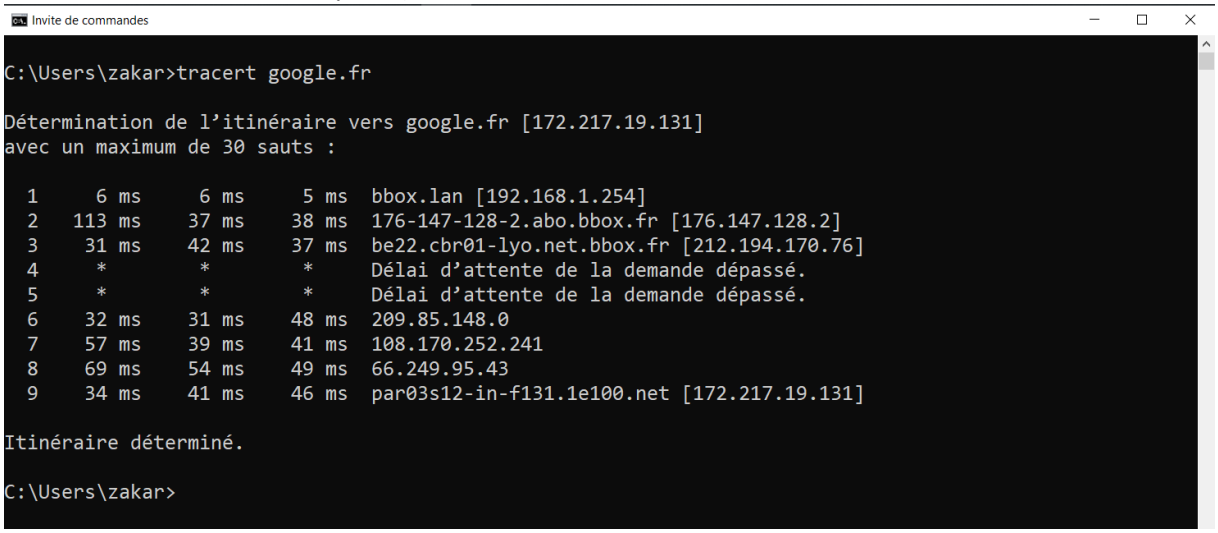






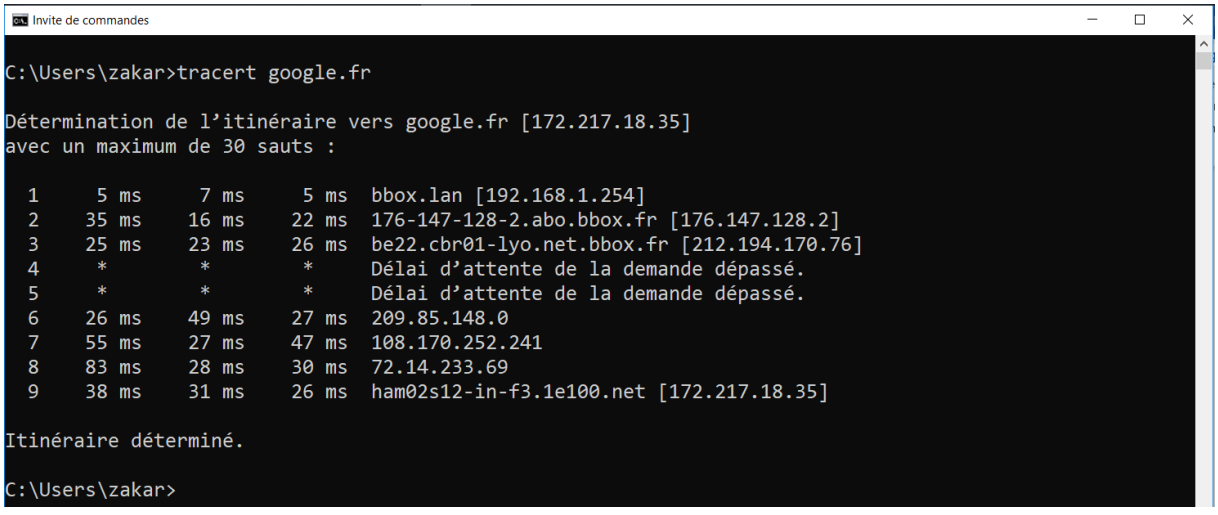
ANNEXE 3
TRACERT

Chaque étape est un routeur.
On peut repérer que l'on passe par la Box du fournisseur d'accès.
Les autres sont des routeurs d'Internet. Certains ne répondent pas à notre demande d'info (Délai d'attente de la demande dépassé).

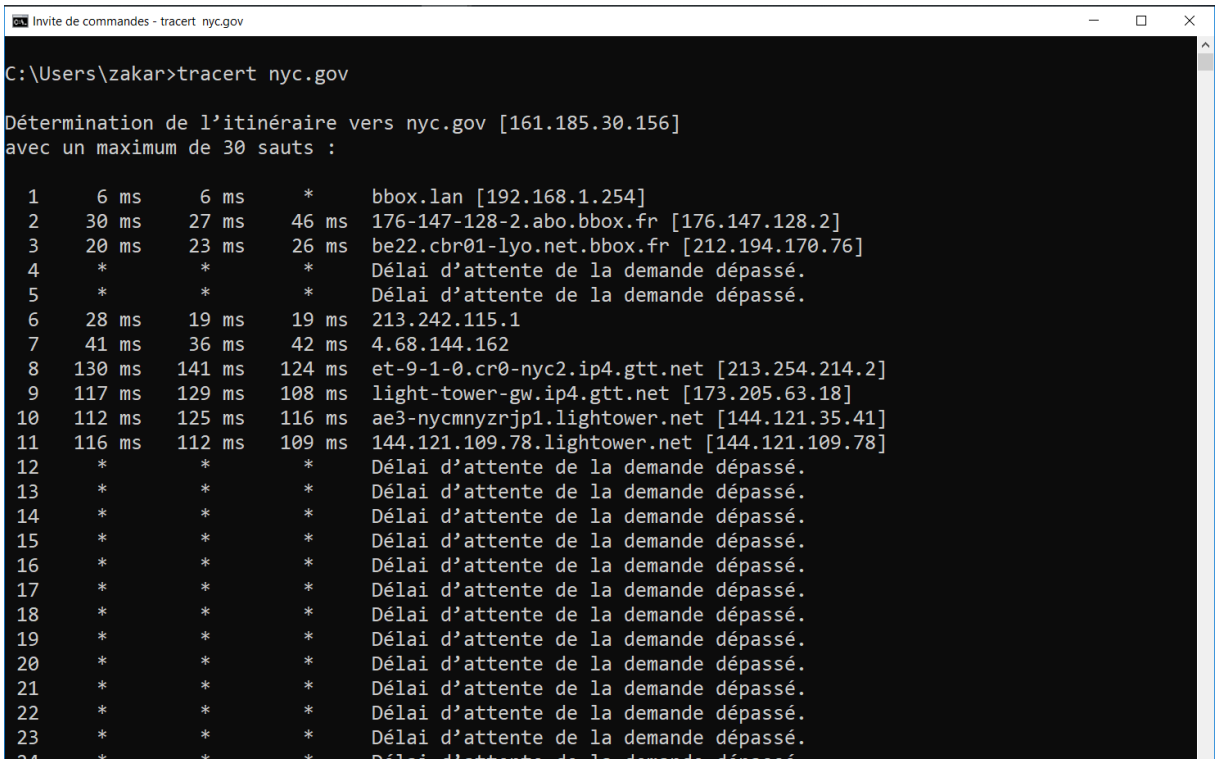


Pour aller encore plus loin. https://www.it-connect.fr/quest-ce-que-le-traceroute/

À noter que la même commande peut donner des adresses différentes. Cela veut dire en quelques sortes qu'il y a plusieurs ordinateurs google.fr. Toutefois le chemin est presque le même.



On peut voyager un peu en allant par exemple à la mairie de New York (USA).
Visiblement on passe par la light tower (il se peut que 30 sauts soit insuffisants).



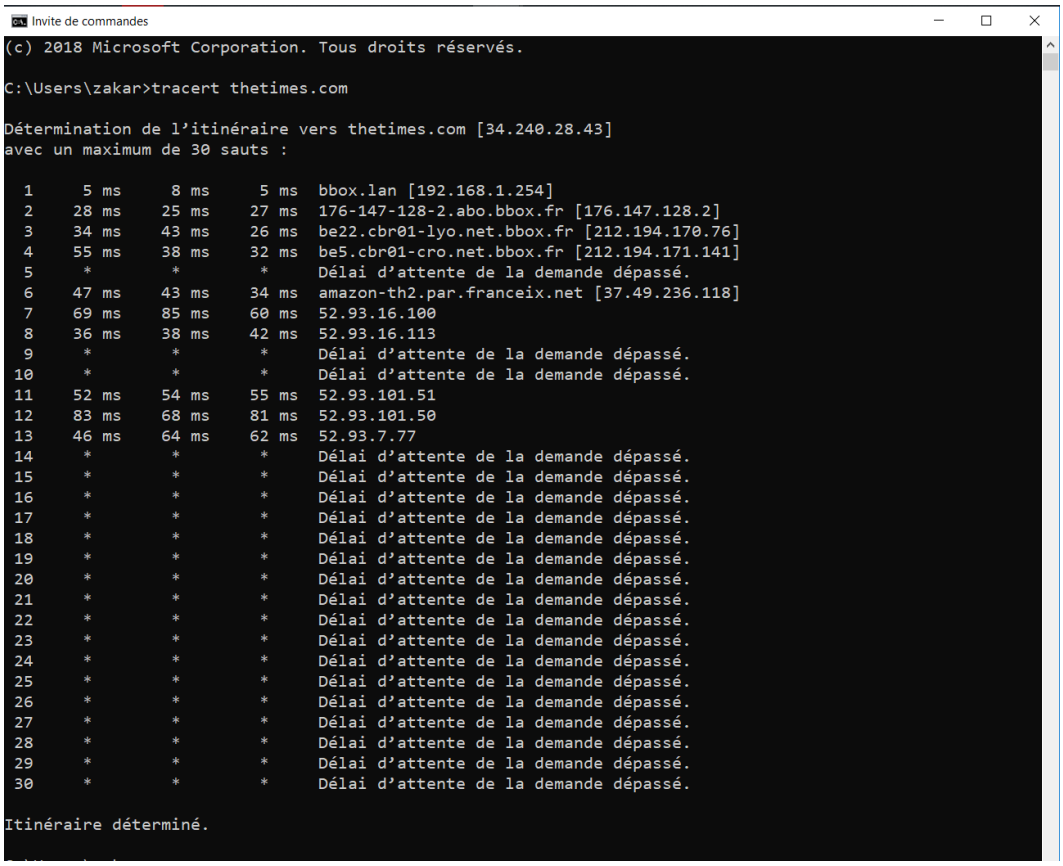
```
Invite de commandes - tracert  nyc.gov

C:\Users\zakar>tracert nyc.gov

Détermination de l'itinéraire vers nyc.gov [161.185.30.156]
avec un maximum de 30 sauts :

  1     6 ms     6 ms     *     bbox.lan [192.168.1.254]
  2    30 ms    27 ms    46 ms  176-147-128-2.abo.bbox.fr [176.147.128.2]
  3    20 ms    23 ms    26 ms  be22.cbr01-lyo.net.bbox.fr [212.194.170.76]
  4     *        *        *     Délai d'attente de la demande dépassé.
  5     *        *        *     Délai d'attente de la demande dépassé.
  6    28 ms    19 ms    19 ms  213.242.115.1
  7    41 ms    36 ms    42 ms  4.68.144.162
  8   130 ms   141 ms   124 ms  et-9-1-0.cr0-nyc2.ip4.gtt.net [213.254.214.2]
  9   117 ms   129 ms   108 ms  light-tower-gw.ip4.gtt.net [173.205.63.18]
 10   112 ms   125 ms   116 ms  ae3-nycmnyzrjp1.lightower.net [144.121.35.41]
 11   116 ms   112 ms   109 ms  144.121.109.78.lightower.net [144.121.109.78]
 12     *        *        *     Délai d'attente de la demande dépassé.
 13     *        *        *     Délai d'attente de la demande dépassé.
 14     *        *        *     Délai d'attente de la demande dépassé.
 15     *        *        *     Délai d'attente de la demande dépassé.
 16     *        *        *     Délai d'attente de la demande dépassé.
 17     *        *        *     Délai d'attente de la demande dépassé.
 18     *        *        *     Délai d'attente de la demande dépassé.
 19     *        *        *     Délai d'attente de la demande dépassé.
 20     *        *        *     Délai d'attente de la demande dépassé.
 21     *        *        *     Délai d'attente de la demande dépassé.
 22     *        *        *     Délai d'attente de la demande dépassé.
 23     *        *        *     Délai d'attente de la demande dépassé.
```

La commande tracert peut ne pas réussir à déterminer précisément tous les sauts sans pour autant échouer.



```
Invite de commandes
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\zakar>tracert thetimes.com

Détermination de l'itinéraire vers thetimes.com [34.240.28.43]
avec un maximum de 30 sauts :

  1     5 ms     8 ms     5 ms  bbox.lan [192.168.1.254]
  2    28 ms    25 ms    27 ms  176-147-128-2.abo.bbox.fr [176.147.128.2]
  3    34 ms    43 ms    26 ms  be22.cbr01-lyo.net.bbox.fr [212.194.170.76]
  4    55 ms    38 ms    32 ms  be5.cbr01-cro.net.bbox.fr [212.194.171.141]
  5     *        *        *     Délai d'attente de la demande dépassé.
  6    47 ms    43 ms    34 ms  amazon-th2.par.franceix.net [37.49.236.118]
  7    69 ms    85 ms    60 ms  52.93.16.100
  8    36 ms    38 ms    42 ms  52.93.16.113
  9     *        *        *     Délai d'attente de la demande dépassé.
 10     *        *        *     Délai d'attente de la demande dépassé.
 11    52 ms    54 ms    55 ms  52.93.101.51
 12    83 ms    68 ms    81 ms  52.93.101.50
 13    46 ms    64 ms    62 ms  52.93.7.77
 14     *        *        *     Délai d'attente de la demande dépassé.
 15     *        *        *     Délai d'attente de la demande dépassé.
 16     *        *        *     Délai d'attente de la demande dépassé.
 17     *        *        *     Délai d'attente de la demande dépassé.
 18     *        *        *     Délai d'attente de la demande dépassé.
 19     *        *        *     Délai d'attente de la demande dépassé.
 20     *        *        *     Délai d'attente de la demande dépassé.
 21     *        *        *     Délai d'attente de la demande dépassé.
 22     *        *        *     Délai d'attente de la demande dépassé.
 23     *        *        *     Délai d'attente de la demande dépassé.
 24     *        *        *     Délai d'attente de la demande dépassé.
 25     *        *        *     Délai d'attente de la demande dépassé.
 26     *        *        *     Délai d'attente de la demande dépassé.
 27     *        *        *     Délai d'attente de la demande dépassé.
 28     *        *        *     Délai d'attente de la demande dépassé.
 29     *        *        *     Délai d'attente de la demande dépassé.
 30     *        *        *     Délai d'attente de la demande dépassé.

Itinéraire déterminé.
```

ANNEXE 4

Neutralité d'Internet

Les enjeux économiques autour de la maîtrise du réseau : « pourquoi les américains ont-ils renoncé à la neutralité du net ? Doit-on faire pareil ? (Voir extrait de l'article ci-joint pour mieux comprendre cette question). Qui finance le net ? les entreprises, les utilisateurs, les pouvoirs publics ?...

Les enjeux politiques autour du réseau : Qu'est-ce que le grand firewall chinois ? Comment fonctionne-t-il ? Quelles sont les conséquences en matière de démocratie ? (voir extrait de l'article ci-joint qui illustre parfaitement le cours sur les méthodes pour contrôler Internet). Doit-on contrôler le réseau ? le réguler ?

Les enjeux sociaux autour du réseau : Comment préserver sa vie privée sur le réseau ? Mes informations sont-elles suffisamment sécurisées ? Est-ce que la vie privée est menacée ? La cyber criminalité : qu'est-ce que c'est ? l'espionnage industriel, le droit à l'oubli…

Extrait d'article : la neutralité du net (Les Echos, 2017)

Vous avez entendu parler ces dernières semaines de la neutralité du net, mais le sujet vous a paru technique et rebutant ? Pourtant, il est crucial pour le futur d'Internet, et pas si compliqué à comprendre. Décryptage alors que l'autorité de régulation américaine vient de se prononcer contre ce principe.

1 - C'est quoi la neutralité du net ?

Défendre la neutralité du net, c'est prôner l'égalité de traitement entre tous les flux de données sur Internet. "Il faut voir Internet comme des tuyaux par lesquels transitent des paquets de données", explique Serge Abiteboul, chercheur à l'Inria. "La neutralité du net, c'est dire que les gens qui contrôlent les tuyaux, c'est à dire les fournisseurs d'accès à Internet, n'ont pas leur mot à dire sur les contenus qui passent par les tuyaux".

En gros, tout le monde est logé à la même enseigne, et un fournisseur d'accès à Internet (FAI) comme SFR par exemple, ne peut pas offrir une connexion plus rapide à ceux qui se connectent pour lire le site web de Libération (qui appartient au même groupe) qu'à ceux qui lisent LesEchos.fr.

Il y a donc deux enjeux principaux autour de la neutralité du net. Le premier est lié à nos libertés individuelles fondamentales : chacun a le droit de lire et de publier du contenu sur Internet, en respectant la loi bien sûr, sans qu'un FAI ne décide de ce qui est prioritaire.

Le second aspect est celui de la concurrence économique. Comme dans l'exemple de SFR, garantir la neutralité du net c'est éviter qu'une entreprise donne un avantage à un service plutôt qu'un autre, sous prétexte qu'ils font partie du même groupe, ou que ce service a accepté de payer pour être prioritaire.

Bref, ce principe garantit la neutralité du réseau et évite qu'Internet ne devienne une sorte d'autoroute à plusieurs vitesses. Une comparaison qui a du sens car "les réseaux sont l'infrastructure du XXIème siècle", comme le rappelle Sébastien Soriano, le président de l'Autorité de régulation des communications électroniques et des postes (Arcep).

2 - Pourquoi on en parle maintenant ?

Depuis l'élection de Donald Trump, un nouveau patron a été nommé à la tête de la FCC, l'autorité de régulation américaine des télécoms, Ajit Pai. Cet ancien conseiller de l'opérateur Verizon a

rapidement enclenché un processus pour retirer une règle créée sous l'ère Obama qui garantit la neutralité du net aux Etats-Unis. La FCC a voté ce jeudi 14 décembre pour entériner sa décision.

Les patrons qui soutiennent Trump et ceux qui le critiquent

C'est une très mauvaise nouvelle pour les partisans de la neutralité du net qui tentent depuis cet été d'alerter et de mobiliser l'opinion publique américaine sur le sujet. "Il y a des grands noms qui se sont exprimés sur le sujet : la quasi-totalité des patrons de la Silicon Valley bien sûr mais aussi des célébrités d'Hollywood. Je ne pense pas hélas que cela aura un réel impact", regrette Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique.

3 - Quels sont les arguments des deux camps ?

> Du côté des antis neutralité du net, c'est-à-dire principalement le lobby des fournisseurs d'accès à Internet, c'est l'argument économique qui est le plus souvent avancé. Déployer des infrastructures, et en particulier la fibre, coûte cher. Et selon eux, assouplir les règles autour de la neutralité du net leur permettrait d'investir dans une meilleure qualité de service.

"Pour les FAI, il y a une captation inégale et injuste de la valeur par les producteurs de contenus, comme Google ou Netflix", explique Bernard Benhamou. Avec le développement des services de streaming vidéo, la consommation de data a en effet explosé ces dernières années, et les opérateurs ne voient pas pourquoi ils seraient les seuls à financer les investissements nécessaires dans les réseaux pour suivre les besoins croissants. La fin de la neutralité du net pourrait ainsi leur permettre de faire payer ces acteurs ou les gros consommateurs de vidéo, même si, officiellement, les opérateurs assurent que le vote de jeudi ne changera pas leur mode de fonctionnement.

> Du côté des pros neutralité du net, les motivations sont plus diverses. Il y a ceux pour qui la neutralité est un principe fondateur d'Internet et qui voient toute atteinte à celle-ci comme une attaque directe de nos libertés individuelles, et ceux qui avancent des arguments plus économiques, liés à la concurrence.

Les patrons qui soutiennent Trump et ceux qui le critiquent

"Ce qui est en train d'arriver aux Etats-Unis risque de renforcer les positions dominantes sur Internet", s'inquiète Bernard Benhamou de l'Institut de la souveraineté numérique. Les grands acteurs comme Google seront capables de payer les FAI pour être poussés de manière prioritaire, et les petits acteurs ne pourront pas suivre. "A terme, cela pourrait empêcher des startups d'émerger et de devenir le nouveau Netflix par exemple", détaille l'expert.

Enfin, il y a certains producteurs de contenus, comme Google, qui ne veulent pas verser de dîme aux fournisseurs d'accès et se sont donc mobilisés en faveur de la neutralité du net.

Extrait d'article : le great firewall chinois (Wikipédia)

Histoire

En 1998 le Parti communiste chinois craignait que le Parti démocrate chinois (PDC) monte un nouveau réseau puissant que les élites du parti ne pourraient pas contrôler[1]. Le PDC fut immédiatement interdit et des arrestations et emprisonnements s'ensuivirent[2]. Le projet Bouclier Doré commença la même année. La première partie du projet a duré huit années et fut achevée en 2006. La seconde partie a débuté en 2006 et s'est finie en 2008.

Le 6 décembre 2002, 300 personnes de 31 provinces et villes de Chine chargées du projet Bouclier Doré ont participé à l'inauguration de quatre jours intitulée « Exposition Étendue du Système d'Information Chinois »[3]. De nombreux produits occidentaux de haute technicité furent achetés à cette exposition (parmi lesquels des produits de sécurité internet, de surveillance vidéo ou de reconnaissance faciale). On estime qu'environ 30 000 agents de police sont employés dans le cadre de ce projet gigantesque

Ce projet a été surnommé le « Grand Firewall de Chine » en référence à son rôle de pare-feu informatique (« *Firewall* » en anglais, ou « pare-feu ») et à l'antique Grande Muraille de Chine. La majeure partie du projet concerne la capacité à bloquer du contenu en empêchant le routage d'adresses IP et est constituée de pare-feu classiques et de proxies placés aux passerelles Internet. Le système est aussi soumis à un Empoisonnement du cache DNS lorsque certains sites particuliers sont demandés.

Le gouvernement n'examine pas systématiquement le contenu d'Internet du fait que cette pratique est techniquement impossible[4]. Du fait de son isolement du reste du monde en termes de routage IP, le réseau contenu dans le Grand Firewall de Chine est nommé le « domaine de routage autonome chinois »[5].

Durant les Jeux olympiques 2008 les fonctionnaires chinois ont demandé aux fournisseurs d'accès à Internet de se préparer à débloquer l'accès depuis certains cybercafés, certaines prises d'accès dans des chambres d'hôtels et dans des centres de conférence où des étrangers étaient censés se rendre pour travailler ou séjourner[6].

Méthodes

La mise en œuvre de cette censure fait intervenir plusieurs méthodes[9].

Blocage d'adresse IP

L'accès à certaines adresses IP est refusé. Si le site web ciblé est hébergé sur un serveur mutualisé, alors tous les sites web sur ce serveur seront bloqués. Tous les protocoles qui dépendent d'IP sont alors affectés (en particulier TCP, c'est-à-dire HTTP, FTP ou POP). Une méthode de contournement classique consiste à trouver un proxy ayant accès au site web ciblé, bien que les proxies soient souvent congestionnés ou bloqués. Quelques gros sites web allouent des adresses IP supplémentaires afin de contourner le blocage, mais celui-ci est par la suite étendu afin de couvrir les nouvelles adresses.

Filtrage et redirection DNS

Les noms de domaine ne sont pas résolus, ou renvoient des adresses IP incorrectes. Tous les protocoles IP sont alors affectés : HTTP, FTP, POP, etc. Une méthode de contournement classique consiste à trouver un serveur DNS qui résolve les noms de domaine correctement, mais ces serveurs DNS sont aussi sujets au blocage (en particulier au blocage IP). Une autre solution consiste à éviter la résolution DNS si l'adresse IP peut être obtenue à partir d'autres sources et si elle n'est pas bloquée. Il est ainsi possible de modifier le fichier Hosts ou de taper directement l'adresse IP au lieu du nom de domaine dans le navigateur web.

Filtrage d'URL

L'URL saisie est scannée afin de détecter des mots-clés indépendamment du nom de domaine spécifié. HTTP est affecté. Les méthodes de contournement courantes consistent à utiliser des caractères d'échappement dans l'URL, ou d'utiliser des protocoles chiffrés comme VPN et SSL.

Filtrage de paquets

Les transmissions de paquets TCP sont interrompues lorsqu'un certain nombre de mots-clés controversés sont détectés. Tous les protocoles TCP sont affectés, mais les pages des moteurs de recherche sont aussi susceptibles d'être censurées. Les méthodes de contournement courantes consistent à utiliser des protocoles chiffrés comme VPN ou SSL, à échapper le contenu HTML, ou bien à réduire la MTU de la pile TCP/IP afin de réduire la quantité de texte contenu dans un paquet donné.

Réinitialisation de connexion

Si une connexion TCP a été précédemment bloquée par le filtre, les tentatives de connexion qui suivent des deux côtés seront bloquées durant au plus 30 minutes. Selon l'endroit du blocage, d'autres utilisateurs ou sites web peuvent aussi être bloqués si les communications sont routées en direction de l'endroit du blocage. Une méthode de contournement consiste à ignorer le paquet de réinitialisation envoyé par le firewall[10].

ANNEXE 5
Pour aller plus loin

Les protocoles CSMA/CD & CSMA/CA

À l'origine d'internet les ingénieurs qui l'ont créé ont cherché des moyens pour organiser la parole, la transmission sur les lignes. Et ont créé les techniques du jeton et CSMA/CD. Certaines sont encore utilisés notamment sur le wifi. Voyons comment ils fonctionnent.

Imaginez-vous sur une place du marché, nous dirons que c'est le marché de Brive-la-gaillarde.

À présent quand j'aurai fini de compter jusqu'à 3 vous parlerez tous en même temps.
1-2-3

Tout le monde parle en même temps, à moins d'être juste à côté on n'y comprend rien c'est du BRUIT. Le signal se diffuse mal ou en tout cas pas très loin.

À présent nous allons fonctionner avec un système de bâton de parole.

Le bâton va circuler dans l'ordre des participants, dès qu'il passe par vous vous pouvez parler à un destinataire qui attendra de l'avoir reçu à son tour pour vous dire « reçu »et libérer le bâton de parole si quelqu'un veut parler quand il passe par lui. (L'expérience est faisable en cours).

Inconvénient : c'est lent.

On appelle le CSMA/CA ou technique du jeton c'est efficace mais lent.

Faisons une nouvelle expérience. Prenons douze volontaires. Je vous donne à chacun un chiffre sur une carte.

3, 7, 11,17, 23, 29, 37, 41, 43, 47, 59, 61

À présent quand je compterai jusqu'à 3 chacun comptera jusqu'à son chiffre dans sa tête et écoutera rapidement si personne ne parle et parlera. Quand ça sera fini on s'échangera rapidement les cartes et on renouvellera l'expérience.

Ce système un peu « poli » marche bien même si parfois on constate des collisions. S'il y en a une, on envoie un signal (une sonnerie) pour dire à tous qu'il y a une collision qui cause du bruit et qu'on repart à 0 : on s'échange les cartes et on réessaye de dire ce qu'on a à dire.