Peut-on ≪ débrider ≫ sa connexion YouTube avec le DNS ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 février 2013

https://www.bortzmeyer.org/debrider-avec-dns.html

Une société <https://speed-dns.eu/> vient de clamer qu'elle pouvait ≪ débrider gratuitement l'accès à certains sites comme Youtube qui est bridé par votre fournisseur d'accès à internet ≫. Est-ce possible ? Et, si oui comment font-ils ?

On comprend le modèle d'affaires de cette société. Un grand nombre d'internautes sont en effet très mécontents du peu de fluidité des flux vidéo avec certains services comme YouTube. En effet, le conflit entre les fournisseurs de service comme Google (propriétaire de YouTube) et les FAI (comme Free ou Orange) autour du problème ≪ qui va payer ? ≫ amène parfois à ne pas augmenter la capacité du réseau qui relie le fournisseur de services au FAI, voire à restreindre délibérement cette capacité (≪ bridage ≫). (C'est l'une des facettes de la question dite de ≪ neutralité du réseau <https://www.bortzmeyer.org/neutralite.html> ≫.) Depuis de nombreux mois, par exemple, regarder des vidéos YouTube depuis Free est très pénible, avec des arrêts soudains, des dizaines de secondes passées à regarder tourner un indicateur de chargement, etc. Les dirigeants de Free clamant bien fort qu'ils ne résoudront le problème que lorsque Google aura cédé et les paiera, il est logique que les ≪ freenautes ≫ cherchent des solutions, ce que leur FAI ne fait pas.

La société Speed-DNS <https://speed-dns.eu> prétend qu'elle a une telle solution, qu'elle peut ≪ [garantir] une vitesse de streaming aussi importante que chez les autres opérateurs. ≫. Or, Speed-DNS est simplement un service de **résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html>**. Elle fournit deux résolveurs, identifiés par leurs adresses IP, 178.33.182.34 et 5.135.158.150, qu'on peut utiliser à la place de ceux normalement fournis par son FAI (voir la documentation de Speed-DNS <https://speed-dns.eu/use.php>). Quel est l'intérêt ? Un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> DNS est un composant quasi-indispensable d'un accès à l'Internet. C'est le serveur auquel on donne un nom de domaine comme www.bouletcorp.com ou www.ati.tn et qui répond par l'adresse IP du serveur correspondant, adresse qui sera utilisée par les machines pour communiquer. Normalement, un résolveur en vaut un autre, car ils donnent tous la même réponse. L'internaute typique se sert donc de ceux fournis par son FAI, configurés automatiquement via la "*box*". Toutefois, depuis quelque temps, deux facteurs ont mené à l'apparition de services de **résolveurs DNS publics**, distincts de ceux du FAI. Le plus connu est Google Public DNS <https://www.bortzmeyer.org/google-dns.html>. D'abord, certains FAI offrent un service médiocre, en fiabilité ou en temps de réponse, poussant certains à aller voir ailleurs un meilleur service (souvent sans mesurer <https://

www.bortzmeyer.org/le-plus-rapide-dns.html>, en faisant une confiance aveugle à la publicité du service). Mais certains FAI font pire. Normalement, un résolveur DNS n'est qu'un relais : il transmet les questions de l'utilisateur aux serveurs DNS faisant autorité (par exemple, pour www.ati.tn aux serveurs de l'ATI) et relaie les réponses vers l'utilisateur. Or, certains FAI modifient les réponses DNS dans le résolveur, pour servir aux utilisateurs de fausses informations. Ce sont les DNS menteurs <https://www.bortzmeyer.org/dns-menteur.html>. Un exemple est le service AdGate <https://www.bortzmeyer.org/free-adgate.html> de Free (désormais désactivé par défaut, donc ne mentant que si l'utilisateur l'a explicitement réclamé). Ce mensonge peut être imposé par la loi, à des fins de censure, comme le fait l'ARJEL <https://www.bortzmeyer.org/arjel.html>. Utiliser un résolveur DNS public situé dans une autre juridiction peut donc permettre de contourner ces mensonges. (Mais attention, certains résolveurs DNS publics ont leurs propres mensonges.)

Et qu'est-ce que cela change pour YouTube ? Faisons un petit détour vers le fonctionnement de YouTube. Lorsque l'utilisateur se connecte à YouTube, le point de départ est le nom de domaine youtube.com. Via le résolveur DNS, il est ensuite traduit en un groupe d'adresses IP, le navigateur Web va alors se connecter à une de ces adresses (en utilisant HTTP), récupérer une page contenant à son tour des informations sur la source du flux vidéo (où on trouve des noms comme r12---sn-25g7rn7l.c.youtube.com), le navigateur se connectera à ces sources et recevra la vidéo. Le résolveur DNS ne peut rien faire sur le flux vidéo lui-même qui ne passe **pas** par le DNS. Un résolveur DNS comme celui de Speed-DNS n'a pas de possibilité d'action ici. Que peut-il donc faire ? Speed-DNS répond <https://twitter.com/SpeedDnsTeam/status/300687825576267776> « on ne va pas dévoiler nos systèmes internes en public ». Qui peut être assez naïf pour avaler un tel argument ? « J'ai mis au point un système pour faire des recherches sur le Web dix fois plus vite qu'avec Google. Je ne vais pas le dévoiler car je ne veux pas me faire piquer l'idée mais il me faut 20 M€ pour le financer, merci de m'envoyer un chèque. »

Pourtant, un résolveur DNS a des possibilités : il peut mentir (pour la bonne cause), en donnant comme adresse IP de YouTube une autre adresse IP que l'officielle. Quel intérêt ? Cette adresse IP pourrait être, par exemple, celle d'un service de relais, comme il en existe déjà pour contourner les bridages.

J'ai mis tout cela au conditionnel : en effet, il faut d'abord tester que l'interrogation des résolveurs DNS de Speed-DNS montre un tel effet. Par exemple, depuis Free, en utilisant l'outil de déboguage dig, la réponse renvoyée par le résolveur standard (dans la Freebox) est (j'ai abrégé pour simplifier) :

```
% dig youtube.com
...
;; ANSWER SECTION:
youtube.com. 74.125.230.229
youtube.com. 74.125.230.225
youtube.com. 74.125.230.230
youtube.com. 74.125.230.231
youtube.com. 74.125.230.233
youtube.com. 74.125.230.224
youtube.com. 74.125.230.227
youtube.com. 74.125.230.228
youtube.com. 74.125.230.232
youtube.com. 74.125.230.226
youtube.com. 74.125.230.238

;; Query time: 40 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)          <--- Le résolveur dans la Freebox
;; WHEN: Mon Feb 11 08:44:20 2013
```

Alors que celle renvoyée par le résolveur de Speed-DNS est :

```
% dig @178.33.182.34 youtube.com
...
;; ANSWER SECTION:
youtube.com. 173.194.41.78
youtube.com. 173.194.41.64
youtube.com. 173.194.41.65
youtube.com. 173.194.41.66
youtube.com. 173.194.41.67
youtube.com. 173.194.41.68
youtube.com. 173.194.41.69
youtube.com. 173.194.41.70
youtube.com. 173.194.41.71
youtube.com. 173.194.41.72
youtube.com. 173.194.41.73
...
;; Query time: 58 msec
;; SERVER: 178.33.182.34#53(178.33.182.34)
;; WHEN: Mon Feb 11 08:52:08 2013
```

D'autres adresses, miraculeusement plus rapides ? Non. Comme on peut le tester avec whois, ces adresses sont également chez Google et une recherche de leur connectivité avec traceroute montrent qu'on les atteint par la même route, en passant par les mêmes tuyaux. L'adresse donnée par le résolveur de Free :

```
% traceroute  74.125.230.229
traceroute to 74.125.230.229 (74.125.230.229), 30 hops max, 60 byte packets
 1  192.168.2.254 (192.168.2.254)  0.460 ms  0.469 ms  0.380 ms
 2  88.189.152.254 (88.189.152.254)  22.790 ms  23.970 ms  24.443 ms
 3  78.254.1.62 (78.254.1.62)  25.469 ms  25.563 ms  25.525 ms
 4  rke75-1-v900.intf.nra.proxad.net (78.254.255.42)  26.754 ms  26.797 ms  28.618 ms
 5  cev75-1-v902.intf.nra.proxad.net (78.254.255.46)  28.611 ms  29.653 ms  29.885 ms
 6  p16-6k-1-po12.intf.nra.proxad.net (78.254.255.50)  30.920 ms  26.093 ms *
 7  th2-crs16-1-be1002.intf.routers.proxad.net (212.27.57.217)  27.883 ms  25.887 ms  29.845 ms
 8  cbv-9k-1-be1002.intf.routers.proxad.net (212.27.59.9)  31.298 ms  31.328 ms  32.510 ms
 9  74.125.50.116 (74.125.50.116)  91.574 ms google-pni-3.routers.proxad.net (212.27.40.102)  92.001 ms 74.125.5
10  72.14.238.228 (72.14.238.228)  34.098 ms  35.280 ms  35.603 ms
11  209.85.242.51 (209.85.242.51)  49.916 ms  50.083 ms  49.745 ms
12  par08s10-in-f5.1e100.net (74.125.230.229)  38.188 ms  39.238 ms  23.775 ms
```

Et celle donnée par Speed-DNS :

```
% traceroute  173.194.34.8
traceroute to 173.194.34.8 (173.194.34.8), 30 hops max, 60 byte packets
 1  192.168.2.254 (192.168.2.254)  0.578 ms  0.467 ms  0.419 ms
 2  88.189.152.254 (88.189.152.254)  24.557 ms  25.586 ms  25.731 ms
 3  78.254.1.62 (78.254.1.62)  27.030 ms  27.066 ms  27.057 ms
 4  rke75-1-v900.intf.nra.proxad.net (78.254.255.42)  28.425 ms  28.408 ms  29.838 ms
 5  cev75-1-v902.intf.nra.proxad.net (78.254.255.46)  29.904 ms  30.903 ms  30.968 ms
 6  * p16-6k-1-po12.intf.nra.proxad.net (78.254.255.50)  60.155 ms *
 7  th2-crs16-1-be1002.intf.routers.proxad.net (212.27.57.217)  60.847 ms  25.848 ms  34.256 ms
 8  cbv-9k-1-be1002.intf.routers.proxad.net (212.27.59.9)  34.233 ms  35.785 ms  35.815 ms
 9  google-pni-3.routers.proxad.net (212.27.40.102)  94.137 ms 72.14.216.98 (72.14.216.98)  95.981 ms google-pni
10  72.14.238.234 (72.14.238.234)  38.538 ms  109.822 ms  39.354 ms
11  209.85.242.45 (209.85.242.45)  42.286 ms  42.052 ms  42.013 ms
12  par03s02-in-f8.1e100.net (173.194.34.8)  42.321 ms  23.875 ms  23.746 ms
```

On voit qu'on suit la même route, on passe par les mêmes endroits (`google-pni-3.routers.proxad.net` est à l'interconnexion de Google et de Free, PNI veut dire "*Private Network Interconnection*" et elle est toujours surchargée). Et la cible se trouve probablement dans le même bâtiment (dans `par03s02-in-f8.1e100.net`, `par` désigne sans doute Paris, vus les temps de réponse en milli-secondes indiqués ensuite).

Mais attention, rappelez-vous la description du fonctionnement de YouTube : ce n'est pas lors de la connexion avec le serveur Web de YouTube que des problèmes peuvent se produire, c'est lors de l'envoi de la vidéo, qui se fait sur une connexion différente et via des noms différents. Testons ceux-ci. Sans Speed-DNS :

```
% dig A r12---sn-25g7rn7l.c.youtube.com
...
;; ANSWER SECTION:
r12---sn-25g7rn7l.c.youtube.com. --->r12.sn-25g7rn7l.c.youtube.com.
r12.sn-25g7rn7l.c.youtube.com. 173.194.20.49
...
;; Query time: 34 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)
;; WHEN: Mon Feb 11 09:11:29 2013
```

Et avec Speed-DNS :

```
% dig @178.33.182.34 A r12---sn-25g7rn7l.c.youtube.com
...
;; ANSWER SECTION:
r12---sn-25g7rn7l.c.youtube.com.  178.33.182.34
...
;; Query time: 37 msec
;; SERVER: 178.33.182.34#53(178.33.182.34)
;; WHEN: Mon Feb 11 09:12:37 2013
```

Cette fois, on voit un effet, l'adresse IP renvoyée est chez OVH, pas chez Google (c'est la même adresse que le serveur de noms de Speed-DNS). Si on configure sa machine pour utiliser les serveurs de noms de Speed-DNS, et qu'on examine son trafic avec tcpdump, on voit en effet que, lors du visionnage d'une vidéo YouTube, un important trafic TCP sur le port 80 a lieu avec `178.33.182.34` : le trafic vidéo a été détourné vers la machine de Speed-DNS à OVH, contournant ainsi le bridage. Rien de miraculeux ou d'innovant, donc, c'est exactement la même chose que les services de VPN qu'on achète ou qu'on fait soi-même.

Maintenant, est-ce que cela accélère les choses ? Une seule machine à OVH, qui sert aussi bien de serveur DNS que de relais vidéo ne va pas pouvoir encaisser beaucoup de trafic. Ça marche pour l'instant car il y a peu de clients, mais, en pratique, il reste à voir si cela tiendra la charge.

Il y a d'autres choses à raconter sur Speed-DNS, sur l'état de leur réseau ou sur les autres caractéristiques de leurs résolveurs mais, ici, je me suis focalisé sur leur prétention à accélérer YouTube.