

Tout le monde parle de Google DNS...

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 Décembre 2009. Dernière mise à jour le 8 Décembre 2009

<http://www.bortzmeyer.org/google-dns.html>

Alors, je vais en faire autant. Après Google Mail, Google Docs, Google Talk, Google Wave, Google DNS <<http://code.google.com/speed/public-dns/>> est la dernière vedette de la blogosphère, en attendant Google Power (pour distribuer l'électricité) et Google Airlines (gratuit, évidemment, pour battre les compagnies "low cost").

Google DNS <<http://code.google.com/speed/public-dns/>> est un résolveur DNS ouvert, accessible à tous gratuitement. On peut l'utiliser à la place des résolveurs fournis par le service informatique du réseau local, ou par le FAI. Les instructions pour cela sont disponibles chez Google (en gros, sur Unix, il suffit d'éditer son `/etc/resolv.conf`).

L'adresse à indiquer, 8.8.8.8, sera certainement dans très peu de temps une des plus connues de l'Internet. C'était une idée marketing géniale que d'utiliser une adresse simple à mémoriser (avec son alternative, 8.8.4.4, et ses équivalents IPv6, moins sxys, 2001:4860:4860::8888 et 2001:4860:4860::8844) même s'il n'est pas sûr que faire de l'"anycast" sur cette plage normalement allouée à Level 3 soit parfaitement conforme aux règles de l'ARIN. Mais ne chipotons pas.

Quel intérêt y a-t-il à utiliser un résolveur DNS distinct du résolveur habituel qu'on trouve sur n'importe quel réseau ? La seule raison valable, à mon avis, est le cas où ledit résolveur soit inexistant ou très lent (cela arrive avec certains FAI).

Mais Google met en avant d'autres raisons. En résumant : vitesse, sécurité et honnêteté. Commençons par la fin : contrairement à ses trois concurrents plus anciens (dont le plus connu, en raison de leur marketing agressif, est OpenDNS <<http://www.bortzmeyer.org/opensns-non-merci.html>>), les résolveurs de Google ne sont en effet pas des menteurs <<http://www.bortzmeyer.org/dns-menteur.html>>. Remarquons qu'on est tombés très bas : ne pas mentir devient si rare que c'est désormais cité comme argument commercial.

```
% dig @8.8.8.8 MX doesnotexist.fr
...
;; -->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 3712
```

On obtient bien le NXDOMAIN ("*No Such Domain*"), le DNS fonctionne normalement.

Et la vitesse ? A priori, l'essentiel du temps de réponse étant dû à la latence jusqu'au résolveur, Google DNS a peu de chances d'être plus rapide. À l'heure actuelle, Google DNS n'a apparemment pas d'instance en France et le serveur semble à Francfort. Mais mesurons, ne devinons pas. En utilisant `qtest <http://www.bortzmeyer.org/le-plus-rapide-dns.html>`, voyons, pour une machine française, trois résolveurs de son réseau local, les deux résolveurs d'OpenDNS et les deux de Google DNS :

```
% qtest -n3 "A a.gtld-servers.net" 127.0.0.1 192.134.7.248 192.134.4.162 208.67.222.222 208.67.220.220 8.8.8.8
0 127.0.0.1/127.0.0.1
0 192.134.4.162/192.134.4.162
0 192.134.7.248/192.134.7.248
```

Les résolveurs locaux gagnent nettement, comme prévu. Et si on compare les trois services de résolveur extérieurs :

```
% qtest -n3 "A a.gtld-servers.net" 208.67.222.222 208.67.220.220 8.8.8.8 8.8.4.4 156.154.70.1 156.154.71.1
11 8.8.4.4/8.8.4.4
11 8.8.8.8/8.8.8.8
17 208.67.220.220/208.67.220.220
```

Google l'emporte sur OpenDNS, non seulement en honnêteté mais aussi en vitesse. Il n'y a donc vraiment aucune raison pratique d'utiliser OpenDNS. (Il y a d'autres mesures sérieuses, avec le même résultat, par exemple "*Google DNS vs OpenDNS : Google Rocks for International Users*" `<http://www.manu-j.com/blog/opensns-alternative-google-dns-rocks/403/>` ou "*Divers Resolver DNS Services*" `<http://bark.no8.be/smokeping/smokeping.cgi?target=World.Resolver-DNS>`). Un autre outil de mesure, certes écrit par Google mais dont le source est disponible, si vous n'avez pas confiance, est l'excellent Namebench `<http://code.google.com/p/namebench/>`. Voyez aussi "*Domain Name Speed Benchmark*" `<http://www.grc.com/dns/benchmark.htm>` (ce dernier étant spécifique à Windows).

Et la sécurité ? Google promet `<http://code.google.com/speed/public-dns/docs/security.html>` que ses résolveurs mettent en œuvre toutes les bonnes pratiques actuelles, ce qui est la moindre des choses. La seule stratégie qui aurait été différenciatrice aurait été de faire la validation DNSSEC mais Google DNS ne le fait pas. Par rapport aux résolveurs locaux utilisant les logiciels libres actuels, à jour, comme Unbound ou BIND, Google DNS n'a qu'un avantage, l'utilisation de la variation de la casse, un "*hack*" amusant mais marginal.

Parlant de sécurité, notons un petit problème : il n'y a aucune authentification entre le client sur son poste de travail et Google DNS. Rien ne garantit qu'on parle bien aux machines de Google. D'habitude, cette sécurisation du dernier kilomètre n'était pas un problème car le résolveur DNS était proche : sur le même réseau local ou en tout cas sur le même FAI. Avec Google DNS, cela cesse d'être vrai et on pourrait imaginer de nombreux détournements possibles, par attaque sur le système de routage. Ces attaques pourraient être faites par un intermédiaire, ou bien par un FAI malhonnête, peu soucieux de voir ses

clients partir chez Google. Pour s'en protéger, il existe plusieurs solutions techniques mais aucune ne semble réaliste. Les seules solutions DNS (j'exclus IPsec et compagnie) possibles sont TSIG (RFC 2845¹), qui repose sur un secret partagé, et est donc inutilisable pour un service public comme Google DNS, et SIG(0) (RFC 2931), que personne n'a jamais déployé). Dans les deux cas, je ne crois pas qu'aucun "stub resolver" existant (par exemple la GNU libc) ne le gère, ce qui les rend complètement irréalistes et explique pourquoi Google n'offre pas ce service de sécurité.

Bref, il n'y a de raisons d'utiliser un service de résolveurs externe que si le « sien » est dramatiquement défaillant. Mais, dans ce cas, quelles sont les conséquences ? D'abord, il y a un problème spécifique à Google : l'existence d'une offre très vaste couvrant à peu près tout les services Internet. Si malhonnête que soit OpenDNS, quoi qu'ils fassent des données recueillies sur les utilisateurs, le fait qu'ils ne gèrent qu'un unique service limite les corrélations qu'ils peuvent établir et donc le mal qu'ils peuvent faire.

Au contraire, Google, ayant une offre complète, peut établir des relations, mettre en connexion des données, et représente donc un danger potentiel plus important. Externaliser son courrier à Gmail (ou son DNS à Google DNS), est une chose. Externaliser tous ses services en est une autre. Cela revient à avoir la même entreprise qui serait à la fois votre banque, votre médecin, votre épicier et votre garagiste...

Comment Google peut-il exploiter Google DNS, service gratuit ? Ici, je spécule, je n'ai pas d'informations précises. Google peut gagner de l'argent :

- en exploitant l'information recueillie pour améliorer le moteur de recherche,
- en vendant cette information (les noms les plus populaires, par exemple, une information qui intéressera les "domainers", surtout si la réponse est NXDOMAIN, indiquant que le domaine est libre),
- en hébergeant, dans le futur (ce service n'existe pas aujourd'hui), moyennant finances, des serveurs faisant autorité, qui profiteront de la proximité du résolveur pour de meilleures performances. Google, futur hébergeur de TLD ?
- Reconstituer la totalité d'un TLD, même lorsque celui-ci ne publie pas cette information, en comptant les noms dans les requêtes et les réponses obtenues.
- Ou, tout simplement, s'assurer que l'Internet fonctionne bien, pour que les clients puissent aller voir les autres services de Google (chez certains FAI, les résolveurs DNS marchent mal, ce qui gêne sans doute Google dans son cœur de métier).

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc2845.txt>