À quoi ressemblera la résolution de noms dans l'Internet de demain ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 décembre 2011

https://www.bortzmeyer.org/resolution-de-demain.html

Dans tout réseau, il y a besoin d'un mécanisme de **résolution** des noms, traduisant les noms en identificateurs de plus bas niveau, plus proches du fonctionnement technique du réseau. C'est ainsi que, de 1983 à 2011, la résolution de noms sur l'Internet a surtout été assurée par le DNS, permettant ainsi de séparer des noms stables, comme www.example.org, des identificateurs moins stables <https://www.bortzmeyer.org/pourquoi-le-dns.html>, comme 2001:db8:af::1:567. Mais est-ce que cela sera toujours le cas demain ?

Car le DNS est aujourd'hui menacé. Pas par les vagues projets de construire un système « meilleur », tâche plus compliquée qu'elle n'en a l'air <https://www.bortzmeyer.org/no-free-lunch.html>. Mais par l'intérêt que portent des forces néfastes au DNS, et par les réactions que cela va entraîner. Aujourd'hui, avec le DNS, nous avons sur l'Internet un système d'une très grande fiabilité (les attaques DoS contre la racine ont toujours échoué <https://www.bortzmeyer.org/attaque-serveurs-racine.html>, par exemple), largement déployé, qui permet des identificateurs stables (mon blog est resté en www.bortzmeyer.org même lorsque je suis passé de Slicehost <http://www.slicehost.com/> à 6sync <http://www.6sync.com/>), et qui assure une signification unique pour les noms. Pas besoin de nuancer, de se renseigner, de demander quel réseau utilise son interlocuteur, on est sûr que tout le monde pourra utiliser www.bortzmeyer.org et avoir un résultat équivalent.

En raison de ces propriétés, le DNS est donc aujourd'hui à la base de toutes les transactions sur l'Internet, qui commencent toujours par une requête DNS (et parfois bien plus).

Ce rôle a évidemment attiré l'attention des méchants, notamment des censeurs. C'est ainsi que la loi LOPPSI en France permet d'imposer aux FAI de bloquer l'accès à certains sites, sur simple décision administrative (pour éviter que les citoyens puissent prendre connaissance de la liste des sites bloqués, et vérifier qu'ils sont bloqués pour de bonnes raisons). Un des mécanismes évidents pour mettre en œuvre ce blocage est le DNS (transformation du résolveur du FAI en DNS menteur <https://www.bortzmeyer.org/dns-menteur.html>, avec blocage du port 53 <https://www.bortzmeyer.org/port53-filtre.html>). Déjà, de nombreux commerciaux font le tour des acteurs de l'Internet pour promouvoir des solutions de filtrage DNS, qui est également possible dans des logiciels comme

BIND (avec la RPZ <https://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html>). La France dispose d'une grande avance technologique dans ce domaine, avec des entreprises comme Amesys, fournisseur de censure pour l'ex-dictature lybienne <http://owni.fr/2011/06/10/la-libye-sur-ec index.html>.

Les autres pays ne sont pas en reste et c'est ainsi que les États-Unis ont leur projet SOPA, équivalent de la LOPPSI, qui permet également d'obliger les FAI à bloquer l'accès à tel ou tel site. Comme, là encore, une implémentation évidente d'un tel système est via le DNS, SOPA a suscité des réactions vigoureuses <http://isoc.org/wp/newsletter/?p=4932> de la part des acteurs du DNS, ce qui explique en partie le recul des promoteurs du projet. Toutefois, la présence ou l'absence de cette loi ne sera pas forcément le facteur principal : un certain nombre d'opérateurs censurent déjà via le DNS (c'est donc une censure privée, contrairement à SOPA qui proposait une censure étatique).

Naturellement, cette censure ne restera pas sans réponse. Des tas de gens chercheront des contournements, des moyens de passer outre à la censure, comme cela s'est déjà produit pour Wikileaks <https://www.bortzmeyer.org/a-propos-wikileaks.html>. Comme le dit An dans les commentaires d'un blog : « Dans le temps, on s'échangeait des adresses de ftp warez. Dans un futur proche, on s'échangera peut-être des fichiers hosts contenant des listes :

```
warez1 @IP1
warez2 @IP2
etc...
```

et on lancera bien gentiment notre navigateur sur http://warez1, http://warez2 etc.. les sites webs auront été hackés et se verront ajouter un hostname warez1 qui servira des films de vacances d'été comme au bon vieux temps du ftp warez. Ça ne tiendra pas longtemps, ça sera difficilement traçable, et ça bougera bien trop rapidement pour être coincé. ». D'autres tentatives ont déjà été faites, de diffuser des listes d'adresses IP <https://docs.google.com/document/d/1aF-VyYGBsJ_zD1Cfv1bYZDl_nUlWVxFJxn-qS2kVB1E/preview?pli=1&sle=true>, suscitant de vives discussions <http://www.reddit.com/r/SOPA/comments/nf5p1/sopa_emergency_list/>. En d'autres termes, il s'agit de revenir aux anciennes listes genre hosts.txt distribuées, et jamais parfaitement à jour (comme le note Pierre Beyssac, ce sera du « "*hosts.txt, cloud-style*" »).

Autre solution, on verra apparaître des résolveurs DNS promettant de ne pas censurer comme ceux de Telecomix <http://dns.telecomix.org/>. Des outils apparaîtront pour permettre de changer de résolveur DNS plus facilement (comme le montre l'article de Korben <http://korben.info/outil-changer-dns.html>).

Ces réactions entraineront à leur tour des contre-réactions, vers davantage de contrôle, comme l'industrie du divertissement le prévoit déjà <http://reflets.info/quand-lindustrie-du-divertissement->.

Lors d'une discussion sur la liste FRnog <http://www.frnog.org/>, Ronan Keryell s'exclamait <http://www.mail-archive.com/frnog@frnog.org/msg16803.html> : « Je pense qu'il faut à la base arrêter de tuer Internet. C'était mieux avant (quand nous utilisions tous les 2 Internet dans les années 80... :-)). Doit-on vraiment revenir au bon vieux hosts.txt (RFC 952 [1] pour ceux qui ont oublié ou plus probablement ici n'ont jamais connu) face à tous ces délires de filtrage et de résolution de faux

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc952.txt

problèmes imaginaires pour le bonheur de l'utilisateur comme dans toute dictature qui se respecte ? Stop ! On s'arrête ! ».

Mais nous en sommes déjà là, à revenir à des systèmes mal fichus, dont le résultat varie selon l'utilisateur, et dont la fiabilité n'est pas garantie. Les gens qui font les lois comme LOPPSI ou SOPA se moquent bien de tuer l'Internet. Ce n'est pas par ignorance de la technique qu'ils décident des mesures qui vont gravement blesser l'Internet. Ils veulent le contrôle avant tout, même au prix de problèmes permanents pour les utilisateurs.

Petit à petit, ces utilisateurs vont se servir de systèmes de résolution « inhabituels ». Ce seront des résolveurs DNS avec des règles spéciales (comme le plugin Firefox <https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-piratebay-dancing/> de Pirate Bay) puis des infrastructures utilisant le protocole DNS mais avec des données différentes (comme les racines alternatives <https://www.bortzmeyer.org/racines-alternatives.html> sauf que cette fois, cela sera réellement adopté massivement, car il existe une forte motivation, qui manquait aux racines alternatives d'il y a dix ans, qui n'avaient rien à proposer aux utilisateurs).

On verra par exemple des « pseudo-registres » qui partiront des données des « vrais » registres puis les « corrigeront », ajouteront des termes ou d'autres, à partir d'une base à eux (contenant les domaines censurés).

Puis cela sera des systèmes de résolution nouveaux, comme Namecoin <http://dot-bit.org/Namecoin>, avec des passerelles vers le DNS (projet `.bit`).

Pour l'utilisateur, cela entrainera désordre et confusion. Des noms marcheront à certains endroits et pas d'autres. On verra des tas de discussions sur des forums avec des conseils plus ou moins avisés du genre « pour voir tous les `.fr`, utilise telle ou telle adresse de résolveur DNS, et pas ceux de X ou de Y qui sont censurés ».

À la fin de l'année 2011, ce scénario catastrophe semble difficilement évitable, sauf réaction vigoureuse contre les ayant-trop-de-droits et autres censeurs.