Un DNS en pair-à-pair ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 décembre 2010

https://www.bortzmeyer.org/dns-p2p.html

D'innombrables électrons ont été agités sur toute la planète pour écrire des articles de blogs (ou leurs commentaires), des "*tweets*" ou des messages sur les listes de diffusion, au sujet du projet de Peter Sunde d'un « DNS pair-à-pair ». Je le reconnais, j'écris cet article en mode grognon : je suis jaloux de Peter Sunde, à qui il suffit de parler vaguement en 140 caractères <http://twitter.com/brokep/status/8779363872935936> d'un projet à peine défini pour obtenir aussitôt l'attention de tous. Cela illustre malheuresement le fonctionnement de l'« économie de l'attention » lorsque le vedettariat s'en mêle. Mais revenons à ce projet. En quoi consiste-t-il et que peut-on en dire ?

D'abord, un peu de contexte. Les insatisfactions quant à la manière dont est géré le système de noms de domaines sont anciennes. Étant hiérarchique (et non pas centralisé, comme beaucoup d'ignorants l'ont écrit), ce système prête à l'attention de gens peu recommandables et d'innombrables problèmes ont surgi autour du contrôle de ce système, pour lequel de très nombreuses réunions dans des destinations touristiques se sont déjà tenues. Le pouvoir sur la racine de ce système, géré par le gouvernement des États-Unis via l'ICANN a ainsi souvent été contesté, et l'ICANN affublée de divers noms d'oiseaux. Plus récemment, le scandaleux projet de loi COICA aux États-Unis a attiré l'attention sur le risque d'un contrôle de l'Internet via le DNS, au profit, dans le cas de COICA, de l'industrie du divertissement. Sans même attendre un éventuel vote de COICA, le gouvernement états-unien a procédé en novembre 2010 à la destruction d'un certain nombre de noms de domaines <http://www.justice.gov/iso/opa/ag/speeches/2010/ag-speech-101129.html>, au nom de la défense de ladite industrie. Le problème n'est évidemment pas spécifique aux États-Unis et, en France, le projet de loi LOPPSI prévoit un filtrage obligatoire de noms qui déplaisent au gouvernement, filtrage dont la mise en œuvre pourrait se faire via le DNS (au début, ce filtrage serait limité aux cas de pédopornographie mais l'histoire monte qu'un tel pouvoir de contrôle est toujours généralisé par la suite). La pression des titulaires de propriété intellectuelle existe aussi dans ce pays et une récente proposition de loi <http://www.assemblee-nationale.fr/13/pdf/amendements_commissions/eco/2789-01.pdf> pour remplacer celle que le Conseil Constitutionnel avait cassée en octobre 2010 <http://blog.dalloz.fr/2010/10/%C2%AB-tout-citoyen-peut-parler-ecrire-imprimer-librement-C2%BB%E2%80%A6-ainsi-qu%E2%80%99enregistrer-et-utiliser-des-noms-de-domaine/> prévoit d'interdire l'enregistrement d'un nom correspondant à une marque (même sans intention malhonnête : si cette loi était adoptée et appliquée strictement, un M. Michelin ne pourrait pas enregistrer de domaine à son propre nom puisque c'est aussi une marque). (Un lecteur attentif me fait remarquer

que ma présentation de cette proposition est résumée au point d'être à la limite de l'inexact. Mais mon but est de parler du projet « P2P DNS » et d'introduire cette discussion par un exemple des pressions existant sur le DNS. Pour la proposition de loi sur la gestion de `.fr`, le mieux est de la lire directement, de consulter les bons auteurs qui l'ont commentée <http://domaine.blogspot.com/2010/12/discussion-legislative-autour-du-fr.html>, de la mettre en perspective - la jurisprudence - et d'écrire à votre député ensuite <http://www.lioneltardy.org/archive/2010/12/01/noms-de-domaine-sur-internet.html>.)

Depuis l'annonce du projet de Peter Sunde, l'affaire WikiLeaks <https://www.bortzmeyer.org/a-propos-wikileaks.html> a d'ailleurs très bien illustré ces pressions contre la liberté d'expression, et les risques qu'il y a mettre tous les œufs dans le même panier (`wikileaks.org` est en panne depuis des jours car il n'y avait qu'un seul hébergeur DNS.)

On voit donc que les frustrations sont nombreuses et légitimes. Historiquement, elles ont mené à divers projets (et la plupart des articles sur le projet de Peter Sunde ne les mentionnent pas, probablement par ignorance de l'histoire), soit de créer des racines alternatives <https://www.bortzmeyer.org/racines-alternatives.html> permettant de court-circuiter l'ICANN, voire les registres existants, soit de mettre au point des systèmes de résolutions de noms n'utilisant pas la hiérarchie du DNS, par exemple à base de DHT comme le très intéressant projet CoDoNS <http://www.cs.cornell.edu/people/egs/beehive/codons.php> ou d'autres méthodes comme le ANDNA de Netsukuku <https://linuxfr.org/comments/1180007.html> ou comme Askemos <http://www.askemos.org/>. Avant toute mise en route d'un nouveau projet, il faudrait donc commencer par s'informer et se demander pourquoi ces projets, dont certains (comme CoDoNS ou comme la racine alternative ORSN <https://www.bortzmeyer.org/orsn-vraiment-fini.html>) étaient très sérieux, n'ont jamais connu de déploiement significatif. Sinon, on agitera beaucoup d'air pour se retrouver face au même échec.

Maintenant, place au projet « P2P DNS ». Si on n'est pas un "*fanboy*", il est difficile de l'analyser, de l'approuver ou de le critiquer, car il est très peu défini. Il y a de vagues idées, des propositions dont on ne sait pas si elles seront retenues ou pas, des grandes déclarations, bref, pour l'instant, c'est du niveau de l'idée de bistrot. Certes, beaucoup de grandes idées sont nées dans un bistrot mais, au bout d'un moment, elles en sont sorties et se sont confrontées au réel. Pour l'instant, avec le projet « P2P DNS », toutes les remarques critiques sont reçues par l'argument que rien n'est encore défini. Je vais donc devoir me contenter de remarques générales.

D'abord, il y a deux services fondamentaux que rend le DNS : l'**enregistrement** de noms et la **résolution** de noms. Historiquement, le terme de « "*Domain Name System*" » désignait les deux, comme si elles étaient forcément liées. Mais ce n'est pas le cas, même si le service d'enregistrement de noms et le protocole de résolution (le DNS, normalisé dans les RFC 1034 [1] et RFC 1035) ont des interactions (tous les deux utilisent un mécanisme arborescent, par exemple). Le mécanisme d'enregistrement assure l'**unicité** des noms (une de ses fonctions les plus importantes) et celui de résolution permet à une machine d'obtenir des informations (par exemple des adresses IP) en échange d'un nom de domaine. On pourrait donc envisager de ne remplacer que l'un d'eux, ce qui est exactement ce que faisait CoDoNS (qui remplaçait la fonction de résolution par une DHT, en gardant le mécanisme d'enregistrement). Changer le mécanisme de résolution, quoique une tâche colossale (il faudrait modifier des centaines de milliers de machines) reste possible. Il existe d'ailleurs déjà aujourd'hui des mécanismes alternatifs (comme des fichiers de noms locaux). Changer le système de nommage et d'enregistrement, que tant d'utilisateurs (bien plus compliqués à mettre à jour que les logiciels) connaissent paraît franchement irréaliste.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1034.txt`

Or, on ne sait pas à quelle fonction veut s'attaquer le projet « P2P DNS ». Le message original de Peter Sunde mentionnait juste la création d'une racine alternative, donc un changement du mécanisme d'enregistrement. Mais d'autres parlent de créer un nouveau TLD, `.p2p`, d'autres de remplacer le DNS par BitTorrent. Difficile d'y voir clair. On a l'impression qu'il y a en fait plusieurs projets différents, chacun avec un cahier des charges distincts et n'ayant en commun que leur insatisfaction du système actuel.

Car ces discussions sur le projet parlent rarement de ce qui devrait être le principal problème : **quels services rend-t-on ?**. Le DNS fournit des noms **uniques**, relativement mémorisables par un humain et qui peuvent être résolus par un programme (cette résolution était traditionnellement faite de manière assez peu sûre <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>, ce que DNSSEC arrangera peut-être). Et il fonctionne depuis plus de vingt ans, malgré les changements considérables qu'a connu l'Internet. L'enregistrement d'un nom nécessite de passer par les règles d'enregistrement d'un registre et, bien qu'ils aient fâcheusement tendance à se copier les uns les autres (la pensée unique frappe ici aussi), cela laisse un certain choix à l'utilisateur (d'autant plus que le registre n'est pas forcément un TLD, il existe des registres à tous les niveaux comme `eu.org`).

Plusieurs articles sur le sujet ont mentionné la participation d'une des organisations qui font encore tourner une racine alternative, OpenNIC, qui vend des noms dans des TLD bidons comme `.free`. OpenNIC pourrait être le registre de `.p2p` et il existe déjà une page Web décrivant le projet <http://wiki.opennicproject.org/dotP2PTLD>. Dans ce cas, les problèmes qu'on a actuellement avec l'ICANN, l'AFNIC ou Verisign seraient simplement déplacés vers OpenNIC. Comme toujours en politique, il n'y a pas de raccourci simple : si on transfère le pouvoir d'un acteur à l'autre, on n'a résolu aucun problème. Quelle politique suivra ce nouveau registre ? La page ci-dessus ne permet pas d'être optimiste, avec comme seule idée, celle de privilégier les gros, ceux qui sont premiers dans le classement d'Alexa : « *"To prevent domain fraud on commonly used domains (eg : google.*) alexa top1000 will be locked to the owner of the highest ranking domain that appears on the alexa rankings."* ».

D'autres possibilités d'un nouveau registre ont été émises, du genre « *"A widely distributed group of trustworthy individuals [...] Sure it's "centralized" to a small group of people, but they are not ICANN or the RIAA."* ». Elles sont, politiquement, tout aussi contestables : les individus honnêtes ne le restent pas quand on leur donne un tel pouvoir.

Si on veut passer à un autre système, il faut voir ce qu'on va abandonner. **Il n'existe pas de solution magique qui résoudrait tous les problèmes en n'ayant aucun inconvénient.** Ce problème, quoique ignoré par la plupart des admirateurs qui tombent en pâmoison devant toute déclaration de Peter Sunde, est pourtant bien connu dans le milieu du pair-à-pair. Ainsi, pour trouver un fichier dans un réseau pair-à-pair, soit on utilise un système hiérarchique (c'est le cas du BitTorrent classique où la récupération du fichier `.torrent` passe par un URL donc un nom de domaine), soit on fonctionne de manière complètement pair-à-pair et, dans ce cas, il n'y a plus d'**unicité** : le même nom peut désigner deux fichiers totalement différentes (une énorme différence avec les URL). C'est ce qui se produit avec les racines alternatives : s'il n'existe pas de racine unique (RFC 2826), alors le même nom (par exemple `stopthecavalry.jona-lewie.mp3`, exemple relativement réaliste puisqu'il existe effectivement plusieurs TLD `.mp3` différents dans plusieurs racines alternatives) peut être enregistré par deux entités différentes et avoir des contenus complètement différents.

Est-ce si grave ? Cela dépend. On peut estimer que le plaisir d'être débarassé de l'ICANN, des registres et de toute cette cuisine vaut bien qu'on supporte quelques inconvénients. C'est un choix possible. Mais je ne l'ai vu mentionné explicitement et clairement que dans un seul <http://techcrunch.com/2010/11/29/peter-sunde-seconds-the-idea-of-an-alternative-root-dns/> des articles consacrés au projet « DNS P2P » (« *"And yes, it's not going to be secure and authenticated like*

the present system. We're just going to have to deal with that." ≫), les autres semblaient tout simplement ignorants du problème.

(Un point technique : je connais au moins un algorithme, dû à Emin Gun Sirer, d'enregistrement de noms uniques en pair-à-pair, sans registre central, à condition que toutes les parties coopèrent. Il n'est pas utilisable en pratique pour cette raison mais je suis preneur d'algorithmes plus astucieux.)

Et si on change le système de résolution, que gagne-t-on et que perd-t-on ? D'abord, il faut préciser que le DNS actuel est fondé sur plus de vingt ans d'expérience avec le monde réel. Tout mécanisme autre (et ceux à base de DHT sont techniquement très intéressants, et méritent certainement l'attention de tout informaticien ambitieux) mettrait sans doute des années avant d'être au point et une longue coexistence est à prévoir. On est loin des vantardises de "*geeks*" qui se voient remplacer les opérateurs DNS actuels en trois mois. Ensuite, il reste des problèmes colossaux à résoudre. L'un d'eux est la sécurité de la résolution de noms. Actuellement, dans la très grande majorité des cas, la confiance dans le résultat de la résolution vient du fait qu'on s'est adressé à un serveur connu. En pair-à-pair, ce mécanisme de validation disparait. N'importe qui peut mettre n'importe quoi dans la DHT et il n'y a plus de serveur faisant autorité. CoDoNS résolvait le problème en imposant DNSSEC ce qui était techniquement correct mais on retombe alors sur le fait qu'on a juste changé le système de résolution (CoDoNS visait surtout la résistance aux DoS, quitte à exagérer <https://www.bortzmeyer.org/dns-vulnerabilites.html>). L'infrastructure d'enregistrement reste la même, avec ses défauts (DNSSEC utilise l'arborescence du DNS pour la validation des signatures.) Il est du reste très probable qu'il ne peut pas y avoir de sécurité dans un système **purement** pair-à-pair (c'est-à-dire sans aucun composant privilégié).

Voici pour les objections pratiques. Mais il y a aussi un problème plus de fond : la question d'origine est à 100 % politique, elle porte sur le contrôle, la liberté, la censure. Il n'existe jamais de solution technique à des problèmes politiques. À un moment, il faut affronter le système et le changer. Autrement, celui-ci trouvera toujours un moyen de vous écraser. Si vous n'utilisez pas le DNS, ce sera via BGP ou via le filtrage IP. Malgré les déclamations ostentatoires et ridicules (comme ≪ "*Internet treats censorship as a damage and routes around it*" ≫), il est illusoire de croire qu'on puisse résoudre des problèmes aussi graves que les atteintes aux libertés fondamentales via des astuces techniques.

Quelques articles intéressants :

— Censure via le DNS aux États-Unis <http://torrentfreak.com/us-government-responds-to-doma
>,
— Le projet ".p2p" <http://dot-p2p.org/>,
— Un court article de Christian Huitema exposant de manière très sommaire à quoi pourrait ressembler un DNS pair-à-pair <http://huitema.wordpress.com/2011/01/03/a-simple-p2p-dns-propo
>,
— Si vous aimez le remue-méninges, une discussion ouverte et riche <http://dns-p2p.openpad.me/1?> entre certains des participants au projet ; brut de fonderie mais techniquement intéressant, avec de bonnes remarques.