Peut-on vraiment parler de « propagation » DNS ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 février 2012. Dernière mise à jour le 15 février 2012

http://www.bortzmeyer.org/dns-propagation.html

On trouve souvent, sur les forums en ligne, des allusions à une « propagation » des informations stockées dans le DNS. Par exemple, une phrase comme « Les informations ont été modifiées au registre, il faut maintenant attendre 24 à 48 heures leur **propagation** ». Ce terme est-il correct ?

Je ne pense pas. « propagation » fait penser à un mouvement qui se déroule tout seul, une fois la source modifiée. C'est effectivement le fonctionnement de certains protocoles réseau comme BGP (RFC 4271 [1]) ou bien Usenet (RFC 5537) où, une fois injectées dans le système, les nouveautés se propagent en effet, sans autre intervention, de machine en machine, jusqu'à atteindre tout l'Internet.

Mais le DNS (RFC 1034) ne fonctionne pas comme cela. Il est "*pull*" et pas "*push*", c'est-à-dire que l'information ne se propage pas toute seule mais est demandée par les clients, les **résolveurs**. Ceux-ci la gardent ensuite dans leur cache et reviennent aux serveurs faisant autorité lorsque la durée de séjour dans le cache arrive à son terme. Si un résolveur n'avait pas l'information dans son cache, il la demande et il aura tout de suite l'information à jour, sans « propagation ». S'il l'a dans son cache, attendre une hypothétique propagation ne changera rien, l'information nouvelle n'arrivera pas avant l'expiration des données.

Notez au passage que cette expiration est commandée par la source : celle-ci indique dans les données le TTL, c'est-à-dire la durée de vie des données. La source (le serveur faisant autorité) peut donc parfaitement commander le processus de mise à jour, contrairement à ce qui se passe pour BGP, où le routeur d'origine n'a aucune influence sur la propagation. C'est parce que la source (le domaine faisant autorité) choisit le TTL qu'il est possible (et même recommandé), lors d'un changement de données (par exemple migration d'un serveur Web vers un nouvel hébergeur, avec une nouvelle adresse IP) d'abaisser le TTL à l'avance <http://www.bortzmeyer.org/changement-adresse-et-dns.html>, de manière à ce que la transition soit sans douleur, puis de le remonter après.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4271.txt

Donc, le terme « propagation » est mauvais, car il fait penser à un modèle de mise à jour qui n'est pas celui du DNS. Il vaut donc mieux utiliser un autre terme. Il n'en existe pas de standard alors j'adopte un terme proposé par Michel Py : « réjuvénation ». Il existe dans le dictionnaire <http://fr.wiktionary.org/wiki/r%C3%A9juv%C3%A9nation> et sonne bien. Je souhaite qu'on dise désormais des choses comme « L'AFNIC vient de modifier `.fr`, il faut maintenant attendre la réjuvénation des données. »

Avec un outil de déboguage DNS comme dig, on peut bien voir ce processus de réjuvénation :

```
% dig A www.cfeditions.com
...
;; ANSWER SECTION:
www.cfeditions.com. 43 IN A 178.33.202.53
```

La réponse a été trouvée et le temps restant à vivre dans le cache est de 43 secondes (le second champ). Si on recommence deux minutes plus tard, ce temps aura été dépassé et le résolveur devra réjuvéner les données :

```
% dig A www.cfeditions.com
...
;; ANSWER SECTION:
www.cfeditions.com. 120 IN A 178.33.202.53
```

Et voilà, on est reparti pour une durée de 120 secondes, celle déterminée par le serveur faisant autorité. Vérifions en lui demandant directement :

```
 % dig @ns6.gandi.net A www.cfeditions.com
...
;; ANSWER SECTION:
www.cfeditions.com. 120 IN A 178.33.202.53
```

Cette durée est extrêmement basse (beaucoup trop) mais c'était pour illustrer le fait qu'elle était sous le commandement exclusif du gestionnaire du domaine. Autrefois, les TTL typiques étaient de 24 à 48 heures, d'où la légende « le temps de propagation dans le DNS est de 24 à 48 h ». Aujourd'hui, les durées les plus courantes sont de 4 à 12 h bien que certains abusent et indiquent des durées ridiculement courtes.

Alors, bien sûr, les experts DNS parmi mes lecteurs vont dire que c'est plus compliqué que cela. Il existe d'autres causes aux délais de mise à jour comme la réactivité de l'hébergeur DNS lorsqu'on modifie une zone via le panneau de contrôle, la réactivité du registre lorsqu'on lui envoie des modifications (il fut un temps où il était courant que les TLD ne soient modifiés qu'une ou deux fois par jour), la synchronisation entre les serveurs faisant autorité (en général quasi-instantanée depuis le RFC 1996 mais il peut y avoir des problèmes), etc. Ceci dit, les délais les plus longs sont bien en général dus aux caches des résolveurs.

D'autres termes à proposer à la place ? J'ai entendu « actualisation » mais je le trouve moins joli. « mise à jour » ? « expiration du cache » (trop technique et pas assez littéraire) ? « rébiscoulation » (le verbe « rébiscouler » est utilisé dans le Sud-Ouest de la France au sens de « remonter, requinquer ») ? « regain » ? « rafraîchissement » (trop de risques de confusion avec le champ "*Refresh*" de l'enregistrement SOA, qui a un autre sens) ? « reviviscence » (qu'on peut aussi écrire « réviviscence ») ?

Un outil intéressant pour regarder la fraîcheur des informations DNS en demandant à des résolveurs DNS ouverts (accessibles à tous) est <http://www.migrationdns.com/>. Un autre, qui offre plusieurs possibilités intéressantes (demander à des résolveurs ouvertes, demander aux serveurs faisant autorité, etc) est <http://www.preshweb.co.uk/cgi-bin/dns-propagation-tracker.pl>. Citons enfin <http://www.whatsmydns.net/>.

Et pour finir, un bon résumé par Wesley George pendant une réunion IETF : « if you need to pull it, put it in DNS, if you need to push it, put it in BGP ».