

Que veut dire synchroniser deux domaines ?

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 juillet 2010. Dernière mise à jour le 24 août 2010

<https://www.bortzmeyer.org/domaines-synchrones.html>

À la réunion <<http://www.ietf.org/meeting/78/index.html>> de Maastricht de l'IETF, le 28 juillet, un sujet brûlant a été discuté, le "*DNS aliasing*" ou la synchronisation de domaines.

Quel est le problème à résoudre? Eh bien justement, une bonne partie de la difficulté est qu'on ne sait pas trop. Pour la convocation de la réunion du 28, Andrew Sullivan a fait un résumé <<http://www.ietf.org/mail-archive/web/ietf/current/msg62280.html>> de la situation. Avant de voir l'état actuel de la discussion, prenons un peu de hauteur sur cette question.

Le DNS fonctionne en comparant des noms de domaine. Si on interroge un serveur DNS faisant autorité en lui demandant des informations sur `www.france.fr`, il va chercher si ce nom est dans sa base et répondre si c'est le cas. La norme du DNS (RFC 1034¹, section 3.1) précise que cette recherche se fait de manière insensible à la casse donc on aurait pu demander `Www.France.FR` et avoir le même résultat. À part l'insensibilité à la casse, le serveur n'essaie pas de faire des recherches approximatives, de trouver un nom « ressemblant ». Il fonctionne de manière littérale.

Mais, parfois, les humains trouvent que c'est trop littéral et voudraient que deux noms « identiques » (pour eux) soient reconnus comme tels par le DNS. Par exemple, un français qui tape `www.saint-ennemond.fr` s'attend peut-être à ce que `www.st-ennemond.fr` (une abréviation courante) lui donne le même résultat (le site Web de la commune). Bien sûr, les informaticiens riront de sa naïveté mais sa demande que les deux noms soient « *aliasés* » ou « synchrones » est tout à fait raisonnable. De même un australien trouvera peut-être que `theatre.com` (orthographe anglaise) et `theater.com` (orthographe états-unienne) devraient être « le même domaine ». Bien sûr, les IDN fournissent encore d'autres possibilités d'« égalité » entre noms. Si Unicode ne fournit que des équivalences simples, via ses algorithmes de canonicalisation, cela laisse bien des cas où un humain voudrait des équivalences que ne fournit pas Unicode. Un exemple typique est la différence entre les TLD `.` [Caractère Unicode non

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

montré ²] [Caractère Unicode non montré] et . [Caractère Unicode non montré] [Caractère Unicode non montré] (Taïwan, en sinogrammes traditionnels et simplifiés).

On le voit, **déterminer** que deux noms sont « équivalents » n'est pas faisable par un algorithme. Alors, simplifions le problème. Supposons que des humains aient déterminé par un processus quelconque que deux noms sont équivalents et que les domaines qu'ils représentent devraient être « synchronisés ». Existe-t-il un moyen technique de le faire? Et, si non, l'IETF doit-elle en développer un?

D'abord, et c'est une grande partie de la difficulté, il faut déterminer ce que veut dire « synchronisés ». Une définition forte serait « Si A.example et B.example sont synchronisés, l'utilisateur doit voir exactement la même chose s'il utilise un nom ou l'autre ». Avec une telle définition, il n'y a pas de solution DNS au problème puisque, par exemple, si l'utilisateur se sert d'un navigateur Web, le résultat dépendra aussi de la configuration du serveur HTTP (directives `ServerName` et `ServerAlias` sur Apache). (Merci à John Levine pour ses bonnes explications sur ce point. On les trouve aussi dans les commentaires d'EURID au plan ICANN <<http://forum.icann.org/lists/sync-idn-cctlds/msg00007.html>>, dont je parle plus loin.)

Avec une définition plus limitée, « Si A.example et B.example sont synchronisés, nimportequoi.A.example et nimportequoi.B.example doivent avoir les mêmes enregistrements DNS », on s'approche d'un problème soluble. Comment atteindre ce résultat dans le DNS aujourd'hui?

La première solution est la plus simple : ne pas compter sur le DNS mais simplement résoudre le problème au niveau de l'avitaillement : si on délègue les deux domaines à la même organisation, celle-ci peut s'assurer que les deux domaines restent « synchronisés ». C'est d'ailleurs ce qui est fait pour les deux TLD IDN de Taïwan cités plus haut, tous les deux délégués à TWNIC <<http://www.twnic.net.tw/>>. La principale limite de cette méthode est qu'elle ne **garantit** pas la synchronisation : tout dépend en effet de la politique du titulaire des deux domaines.

La seconde idée est d'utiliser les enregistrements CNAME par exemple dans un fichier de zone de .example :

```
B.example. IN CNAME A.example.
```

mais cela ne gère que le domaine A.example, pas ses sous-domaines. Et avec les plus récents DNAME du RFC 6672? Essayons :

```
B.example. IN DNAME A.example.
```

Cette fois, c'est le problème inverse, seuls les sous-domaines sont « *aliasés* ». Le problème a été bien illustré par Ond[Caractère Unicode non montré] Sur[Caractère Unicode non montré] dans son excellent exposé de synthèse à la réunion CENTR/OARC <<https://www.centri.org/main/5582-CTR/version/default/part/AttachmentData/data/Tech22%20-%20Sury%20-%20DNS-20100502-Tech.pdf>> de Prague le 2 mai 2010 : il n'existe pas de solution idéale, sauf à combiner CNAME et DNAME, ou bien à créer un nouveau type qui combine leurs deux rôles, tel le BNAME proposé par J. Yao ou encore un système de réplication comme le SHADOW proposé par Paul Vixie.

2. Car trop difficile à faire afficher par L^AT_EX

Bon, mais, finalement, puisque tout cela est bien compliqué, fallait-il vraiment faire quelque chose? Mais il faut savoir qu'il y a un contexte politique. Le 22 mars, l'ICANN avait annoncé son plan pour les TLD synchronisés <<http://icann.org/en/annoncements/annonce-22mar10-en.htm>> et, bien que ce plan n'imposait pas forcément une solution technique, il a suscité beaucoup de discussions à l'IETF. (Les commentaires de ce plan sont en ligne <<http://forum.icann.org/lists/sync-idn-cctlds/index.html>>, notez celui de l'IETF <<http://forum.icann.org/lists/sync-idn-cctlds/msg00012.html>>.) L'ICANN a annoncé des positions contradictoires (en faveur d'une solution technique <<http://ops.ietf.org/lists/namedroppers/namedroppers.2010/msg00883.html>> ou bien contre cette idée <<http://ops.ietf.org/lists/namedroppers/namedroppers.2010/msg00994.html>>).

Sur la partie politique, voir aussi la FAQ de l'ICANN <<http://icann.org/en/topics/idn/fast-track/synchronized-idn-cctlds-faq-en.htm>>. Sur la partie technique, les "*Internet-Drafts*" à lire sont :

- La proposition SHADOW <<http://tools.ietf.org/id/draft-vixie-dnsex-dnshadow>>,
- La proposition BNAME <<http://tools.ietf.org/id/draft-yao-dnsex-bname>>,
- La proposition CNAME+DNAME <<http://tools.ietf.org/id/draft-sury-dnsex-cname-dname>>.

Voici la situation après la réunion de Maastricht : <<http://ops.ietf.org/lists/namedroppers/namedroppers.2010/msg02117.html>>.