Reconfiguration des serveurs de noms du domaine haïtien

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 janvier 2010. Dernière mise à jour le 20 janvier 2010

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

Le tremblement de terre qui a frappé Haïti le 12 janvier 2010 a déjà fait l'objet de beaucoup d'articles, notamment sur les mesures d'aide qui ont été prises. Je voudrais ici détailler un aspect tout à fait secondaire, mais qui illustre bien le fonctionnement actuel de l'Internet : la reconfiguration du domaine de premier niveau `.HT`, pour lui garantir un fonctionnement prolongé. (Cet article est conçu pour tous, des détails techniques sur le DNS figurent à la fin.)

Comme tous les pays, Haïti a un nom de domaine dit « de tête » ou « de premier niveau », qui identifie le pays. En l'occurrence, c'est `.HT`. On peut donc avoir des ressources Internet avec des noms comme `www.fds.edu.ht` ou `rddh.org.ht`. Les liaisons Internet ont toutes été détruites lors du tremblement de terre mais les ressources (par exemple les sites Web) accessibles via un nom en `.HT` étaient parfois hebérgés à l'extérieur du pays et pouvaient donc continuer à être accessibles... si les noms en `.HT` marchaient toujours. Malheureusement, beaucoup de domaines (y compris des domaines de tête) sont publiés par un nombre de serveurs très limités, tous situés en un seul endroit. En cas de panne électrique ou de coupure de la liaison Internet, le service de noms ne fonctionne plus et, même si le serveur Web est toujours là, les clients ne peuvent plus trouver son adresse et donc le joindre.

Au contraire, `.HT` est bien géré (et bravo à ce sujet à Stéphane Bruno et Max Larson Henry) : il a six serveurs de noms, deux en Haïti, un en France, un au Canada, un aux États-Unis et un autre, géré depuis les États-Unis mais physiquement distribué sur toute la planète. `.HT` n'a donc jamais cessé de fonctionner.

Par contre, cela ne pouvait pas durer éternellement : pour des bonnes raisons techniques, les serveurs **secondaires**, situés à l'étranger, arrêtent tout service s'ils ne peuvent pas joindre le **primaire** pendant un certain temps. Et, de toute façon, toute modification des noms en `.HT` est gelée tant que le primaire n'est pas joignable.

S'il n'y avait pas d'urgence immédiate, il fallait néanmoins agir. En l'absence de toute communication avec les gérants du `.HT`, dans la nuit du 14 au 15 janvier, les responsables des serveurs secondaires, sous l'impulsion de Bill Woodcock <http://www.merit.edu/mail.archives/nanog/

msg04355.html>, de PCH, ont commencé à reconfigurer .HT pour un fonctionnement plus durable. Une copie de la base de données du registre se trouvait en Australie, chez Cocca. Un de leurs techniciens, Garth Miller, a configuré une machine comme primaire, les gérants des secondaires ont changé à leur tour la configuration de leurs machines (merci à Jean-Philippe Pick pour avoir réagi particulièrement vite) et, le 16 janvier au soir, après quelques problèmes techniques, .HT retrouvait un fonctionnement normal, qui pourra durer jusqu'à ce que les liaisons Internet avec les gérants de .HT et leurs ordinateurs soient rétablies. (Nous avons appris depuis que l'immeuble où se trouvait les serveurs a été réduit en poussière. Des organismes comme l'AFNIC travaillent à remplacer ces machines dès que les secours d'extrême urgence pourront laisser la place à l'envoi de matériel informatique. Une partie de l'infrastructure Internet sur place fonctionne encore, notamment le point d'échange sur la colline de Boutilliers <http://www.nsrc.org/CENTRAM/HT/haiti-ixp/002-boutilliers.JPG.html>, grâce à Reynold Guerrier <http://www.nsrc.org/CENTRAM/HT/haiti-ixp/>.)

Le point important à noter est qu'aucun autorité n'a ordonné ou même approuvé ce changement. Aucun comité ne s'est réuni. Aucune signature n'a été donnée. Les seules personnes pouvant décider, à Port-au-Prince, étant injoignables, le travail de reconfiguration a été fait entièrement entre administrateurs système des serveurs secondaires. La sécurité de l'Internet n'est en effet pas celle de murs de béton défendus par des règlements et des procédures. C'est celle d'un organisme vivant <http://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html>, dont les leucocytes sont intelligents et capables d'initiative. (Bien sûr, les administrateurs de .HT ont été informés.)

Les leçons à en tirer ? La première est d'assurer la redondance des serveurs de noms. Ils doivent être plusieurs, et répartis en des endroits très différents, pour faire face aux différents types de panne. On peut noter par exemple que .BD n'a que deux serveurs (un troisième est annoncé mais ne répond jamais), tous les deux à Dhâkâ. En cas de problème frappant cette ville, comme une inondation, tous les noms se terminant par .BD disparaissent. De même, .PF n'a que deux serveurs, tous les deux à Papeete. N'importe quelle carastrophe naturelle rendrait donc ce domaine inutilisable.

La redondance des serveurs est une chose, celle des données en est une autre. (Dans le cas d'un registre de noms de domaines, la base de données contient la liste des noms délégués.) S'il n'y avait pas eu une copie de la base de données à l'extérieur du pays, elle était peut-être perdue. Il faut donc aussi s'assurer que les données sont réparties.

Bien sûr par rapport au drame que viennent de vivre les habitants d'Haïti, c'est tout petit. Mais j'espère que les petites gouttes d'eau feront les grandes rivières : chaque problème réparé est un outil en plus pour les autres réparations. Au fait, depuis ce travail, Stéphane Bruno a pu être joint, il va bien et il a approuvé le changement. Même chose pour Max Larson Henry.

D'autres utilisations intelligentes de l'Internet ont été faites comme le moteur de recherche des disparus <http://haiticrisis.appspot.com/> de Google (disponible en anglais, français et créole) ou comme le flux d'informations Twitter de Carel Perdre <http://twitter.com/carelpedre>.

Comme promis, quelques détails techniques, pour ceux qui connaissent le DNS. Ce protocole est très résistant aux pannes et, si les serveurs sont bien répartis comme ils doivent l'être, un domaine peut résister à n'importe quelle catastrophe. Mais que se passe t-il ensuite ? Les serveurs secondaires (le terme correct aujourd'hui est d'ailleurs « serveur esclave » pour de bonnes raisons mais, dans le contexte d'Haïti, j'ai préféré l'éviter) continuent à servir la zone pendant une période qui est gouvernée par le champ Expire de l'enregistrement SOA (cf. RFC 1035[1], section 3.1.3). Ce champ vaut actuellement

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1035.txt

pour .HT 1296000 secondes soient deux semaines et, si rien n'avait été fait, le domaine .HT aurait donc disparu dans quinze jours (le but de ce champ est d'éviter qu'un ancien esclave oublié continue à servir des données dépassées éternellement). Il y a une seconde raison pour le travail de reconfiguration qui a été fait : il permet de modifier la zone et donc, si nécessaire, d'ajouter des nouveaux domaines ou bien de changer les adresses IP des serveurs de noms des domaines existants, pour assurer leur continuité (un serveur esclave, comme son nom l'indique, ne peut pas modifier les données). Aujourd'hui, on voit que les quatre serveurs extérieurs (dont le serveur "*anycast*" de PCH) sont bien à jour (ils ont tous le même numéro de série, qui est postérieur au séisme) :

```
% check_soa ht
There was no response from ns2.nic.ht
There was no response from ns1.nic.ht
dns.princeton.edu has serial number 2010011820
charles.cdec.polymtl.ca has serial number 2010011820
ht-ns.anycast.pch.net has serial number 2010011820
ns3.nic.fr has serial number 2010011820
```

À noter également que l'actuel serveur maître, chez Cocca, n'apparait pas dans les enregistrements NS : c'est un maître caché (en anglais, on dit un "*stealth*").

Le domaine nic.ht a été à son tour reconfiguré sur le même principe, avec l'idée de faire revivre le NIC à distance.

D'autres articles sur les technologies de l'information et Internet, dans le tremblement de terre :

— Un bon exposé de la situation <http://www.circleid.com/posts/20100126_haitis_telecommunications_sector_in_the_aftermath/> du réseau à Haïti
— Un autre article, contenant peu de détails, sur la reconfiguration de .HT : « "*Situation in Haiti and the DNS*" <http://blog.icann.org/2010/01/haiti/> »
— Un effort beaucoup plus considérable, pour actualiser les cartes d'OpenStreetMap <http://www.ecrans.fr/Haiti-Mobilisation-autour-d-une,8961.html>
— Autre utilisation des technologies pendant le tremblement de terre : signaler qu'on est sous les décombres <http://nuvohaiti.blogspot.com/2010/02/tale-of-android-phone-in-earthquake-i
html> (Stéphane Bruno est le responsable du .ht).
— Quelques semaines plus tard, le Chili était frappé et le NIC chilien a publié un rapport <http://www.nic.cl/anuncios/2010-03-01.html> (en espagnol) et gère un excellent site bourré d'informations détaillées <http://www.niclabs.cl/terremoto/>. En gros, le DNS n'a pas eu grand'chose. Un rapport en anglais a été fait à la réunion OARC de Prague <https://www.dns-oarc.net/files/workshop-201005/20100501-OARC-Earthquake_CL-mvergara.pdf>.