Qui contrôle les serveurs racine du DNS ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 mai 2008

https://www.bortzmeyer.org/qui-controle-les-serveurs-racine.html

---

Un récent petit incident, sans conséquence pratique, la réutilisation de l'ancienne adresse IP d'un serveur racine du DNS, le serveur L.root-servers.net, a mis en évidence la question de la gestion des serveurs racine. Onze organisations <https://www.bortzmeyer.org/combien-serveurs-racines.html> gèrent un de ces treize serveurs. Qui les a désignées ? Qui les contrôle et les surveille ? Que se passe t-il s'il l'une d'elles ne rend plus un service correct ? Que se passe t-il si une organisation se porte volontaire pour remplacer l'une d'elles ?

Revenons d'abord sur ce minuscule incident. Le serveur racine L.root-servers.net, géré par l'ICANN, a changé d'adresse IP <http://l.root-servers.org/ip-change-28oct07.htm> le 1 novembre 2007, passant de 198.32.64.12 à 199.7.83.42. Compte-tenu de la nature particulière des serveurs racine (toutes les résolutions DNS commencent par eux, jusqu'à ce que les caches soient peuplés), de tels changements sont difficiles à propager. Il faut mettre à jour d'innombrables fichiers de configuration un peu partout dans le monde (avec BIND, c'est typiquement dans le fichier root.hints ou db.root). Il n'est donc pas étonnant que, des mois plus tard, l'ancienne adresse reçoive encore des requêtes. (Plus bizarre est le fait qu'elle reçoive des requêtes autre que la requête initiale, dite de « "*priming*" », après laquelle le résolveur DNS, aurait dû se rendre compte de son erreur. Mais c'est une autre histoire.)

L'ancienne adresse de L venait de l'espace d'adresses allouées à ep.net. Et c'est là que commence le problème. ep.net a commencé à annoncer en BGP les adresses incluant l'ancienne adresse du serveur racine et, plus fort, un serveur DNS répondait bien à cette ancienne adresse. Ses réponses étaient apparemment correctes (identiques à celles des « vrais » serveurs racine) donc l'incident n'a eu aucune conséquence pratique. Mais pourquoi ep.net avait-il fait cela ? Avaient-ils le droit ?

Je passe sur les débats parfois assez puérils sur ce point. Bill Manning, le responsable d'ep.net, étant une personnalité controversée, il n'est pas étonnant que certaines accusations soient allées assez loin (voir par exemple le règlement de comptes de David Conrad <http://blog.icann.org/?p=309> et la réponse de CommunityDNS <http://www.communitydns.eu/Old-L.html>, qui travaillait avec Manning).

Mais la discussion a soulevé un point d'habitude pudiquement laissé dans l'ombre. Qui est responsable des serveurs racine ? Si un opérateur de serveur racine ne fait pas son travail comme attendu (Bill Manning opère un autre serveur racine, le `B.root-servers.net`), peut-on le virer ? À partir de quel niveau de non-service ? Et, sans citer de cas aussi dramatiques (après tout, les opérateurs actuels font plutôt bien leur travail), est-ce qu'une nouvelle organisation peut candidater et proposer de remplacer un des serveurs existants (certains, sans être clairement en panne, ne sont pas très performants) ?

La réponse à toutes ces questions est la même et elle représente un des secrets les mieux gardés de la gouvernance Internet : personne ne sait. Aucune règle, aucun contrat, n'encadre le travail des opérateurs de serveurs racine. (Une seule petite exception à cette absence de contrat, le "*Mutual Responsibilities Agreement*" <`https://www.icann.org/froot/ICANN-ISC-MRA-26dec07.pdf`> entre l'ISC et l'ICANN.) Tout dépend uniquement de leur bonne volonté. Certes, elle n'a pas manqué jusqu'à présent, avec des félicitations particulières pour les opérateurs du `F.root-servers.net`, de loin les plus dynamiques et ceux qui se soucient le plus d'informer la communauté des utilisateurs. Mais cette bonne volonté se maintiendra t-elle dans le futur ? Est-ce acceptable qu'une ressource aussi critique pour l'Internet dépende juste de cela ?

Les onze organisations ont été désignées il y a très longtemps, parce que Jon Postel les connaissait et personne aujourd'hui n'ose remettre en cause cette désignation. Aucune organisation, et surtout pas l'ICANN, n'a de légitimité suffisante pour « virer » un serveur racine. La liste est donc, "*de facto*", fermée et non modifiable.

Quelques autres articles sur ce sujet : plein de détails techniques sur le blog de Renesys <`http://www.renesys.com/blog/2008/05/identity_theft_hits_the_root_n_1.shtml`> (gâchés par un titre racoleur, voir aussi la suite <`http://www.renesys.com/blog/2008/06/securing_the_root.shtml`> et leur exposé à NANOG <`http://public.oarci.net/files/dnsops-2008/Brown-Lroot.pdf`>) et un bon résumé <`http://www.circleid.com/posts/852211_uprooting_the_dns_root/`> de Danny McPherson, qui plaide pour un contrôle accru par l'ICANN.