RFC 7720 : DNS Root Name Service Protocol and Deployment Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 décembre 2015

Date de publication du RFC : Décembre 2015

https://www.bortzmeyer.org/7720.html

L'Internet repose en grande partie sur le DNS (si ce dernier est en panne, presque plus rien ne fonctionne) et le DNS doit à sa nature arborescente de dépendre de sa racine ou plus exactement de ses serveurs racine. La gestion de ces derniers est donc une question cruciale, même si les débats sur la gouvernance de l'Internet se focalisent plutôt sur des sujets moins concrets comme la création (ou non) du TLD `.vin`. Ce très court RFC précise les obligations des serveurs racine en terme de protocoles réseau à suivre. D'autres documents décrivent les exigences opérationnelles. (Voir notamment le "*RSSAC 001 : Service Expectation of Root Servers*" <https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf>.)

Avant, ces obligations étaient dans un seul RFC, le RFC 2870[1]. Il contenait des recommandations concernant les protocoles, donc plutôt du ressort de l'IETF, et d'autres concernant les règles quotidiennes des opérations d'un serveur racine, considérées aujourd'hui comme relevant plutôt du RSSAC <https://www.icann.org/resources/pages/rssac-4c-2012-02-25-en> ("*Root Server System Advisory Committee*", qui publie ses propres recommandations dans le document nommé RSSAC-001 <https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-
pdf>). Ce RFC est donc encore plus court que son prédécesseur, désormais document historique.

À noter que les serveurs racine ne servent pas que la racine, mais aussi `root-servers.net`, domaine dans lequel ils sont nommés. Certains d'entre eux servent également `.arpa`.

Le cœur de notre RFC est la section 2 qui exige que les serveurs racine :
— Suivent le protocole DNS (encore heureux...),

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2870.txt`

— Soient capables de répondre en IPv4 et IPv6 (en octobre 2015, deux serveurs, E et G, n'avaient toujours pas d'IPv6),
— Soient capables de répondre en UDP **et** en TCP,
— Doivent gérer les sommes de contrôle UDP,
— Doivent évidemment gérer DNSSEC, pour pouvoir servir la racine, qui est signée,
— Doivent gérer EDNS (RFC 6891).

La plupart de ces règles vont de soi mais, en 2015, on rencontre hélas encore des serveurs DNS qui n'ont pas EDNS ou bien qui n'ont pas TCP (sans même parler d'IPv6...)

Moins liées aux protocoles, il y a deux autres exigences dans la section 3 :

— Répondre à tous les clients (c'est un principe de neutralité du réseau <https://www.bortzmeyer.org/neutralite.html>, qui a d'amusantes conséquences de gouvernance, par exemple les serveurs gérés par l'armée US doivent répondre aux requêtes venant d'Iran...),
— Servir l'unique racine « officielle », cf. RFC 2826 et pas une éventuelle racine alternative. Évidemment, cela implique de ne pas la modifier : les serveurs racine sont des imprimeurs, pas des éditeurs.

Merci à Lancelot et Atlal (et Opale), qui savent pourquoi...