Le port source 53 du DNS, et les vieux fichiers de configuration

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 juillet 2011

https://www.bortzmeyer.org/port-source-53.html

L'informatique est à la fois un domaine de changements permanents (et souvent futiles) et d'extrême conservatisme. Sur bien des points, lorsque quelque chose marche, ou semble marcher, on n'y touche surtout pas. On voit ainsi parfois des survivances du passé bien vivantes, comme la persistance de résolveurs DNS qui utilisent le port **source** 53.

Les chiffres, d'abord. En regardant (avec DNSmezzo <http://www.dnsmezzo.net/>) un sous-ensemble des serveurs DNS faisant autorité pour .fr, on observe que 1,8 % des clients (les **résolveurs**) envoient toutes leurs requêtes depuis un seul port source, le 53. Ces clients représentent environ 1 % des requêtes (ce sont donc des petits résolveurs, en moyenne). Ce n'est pas beaucoup, c'est moins que le pourcentage de requêtes envoyées via IPv6, mais, en 2011, c'est surprenant.

En effet, utiliser toujours le même port source a un gros inconvénient : cela rend plus facile d'injecter une réponse DNS mensongère, permettant ainsi un empoisonnement du cache du résolveur (par exemple, avec la méthode Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kamins
html>). Normalement, le port source doit être aléatoire (RFC 5452 [1], pensez à tester le vôtre <https:
//www.dns-oarc.net/oarc/services/porttest>). En outre, utiliser le port source 53 peut poser des problèmes avec certains pare-feux, qui demandent que le port source des clients soit supérieur à 1023 (les ports plus bas étant réservés aux serveurs).

Alors, pourquoi est-ce que certains (le plus gros résolveur de la liste est le principal FAI d'un pays d'Afrique) utilisent quand même le port source 53 ? Parce que c'était la méthode recommandée, à une époque très lointaine. Au début des années 1990, on recommandait d'utiliser un port source inférieur ou égal à 1023 pour les services critiques, car, sur une machine Unix, seul un logiciel lancé par root pouvait utiliser ce port source (rlogin avait une méthode de « sécurisation » équivalente). Aujourd'hui,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5452.txt

évidemment comme chacun est root sur son PC Linux, sa tablette et son téléphone, cela semble ridicule mais cela a longtemps été une recommandation souvent donnée et très suivie. Lorsque les premiers pare-feux sont apparus, vers la même époque, il était courant de filtrer sur le port source (ce qui est bien plus contestable, puisque ce port est complètement contrôlé par l'assaillant présumé).

Cette recommandation se retrouvait dans le comportement du résolveur DNS le plus utilisé, BIND, qui, jusqu'à la version 8.1 (sortie en 1997), utilisait le port source 53 par défaut. Le script de conversion des anciens fichiers de configuration rajoutait ceci en commentaire :

```
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below.  Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
```

Ce message s'est donc retrouvé dans un grand nombre de fichiers de configuration, `named.conf` (y compris dans ceux distribués par défaut dans des paquetages comme celui de Debian), fichiers dont la syntaxe n'a pas changé depuis. Apparemment, un certain nombre d'administrateurs systèmes avaient décommenté la ligne `query-source`. Et, depuis désormais quatorze ans, ils recopient fidèlement leur `named.conf` de machine en machine, sans avoir jamais mis en cause ce réglage, et sans s'être renseigné sur les évolutions de l'Internet. Bel exemple du poids du passé.