Répartition des serveurs de noms d'une zone dans plusieurs AS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 mars 2014

https://www.bortzmeyer.org/dns-et-asn.html

L'accès aux services sur l'Internet commence presque toujours par une requête DNS. Si ce dernier est en panne, il n'y a quasiment pas d'usage de l'Internet possible (sauf si vous vous contentez de `traceroute -n`...) D'où l'importance de la notion de **résilience** du DNS. Contrairement à ce qu'on lit parfois, le DNS n'est pas juste une application parmi d'autres : c'est une **infrastructure** de l'Internet, presque aussi vitale que BGP. La résilience est un phénomène complexe, pas trivial à mesurer. Dans ce très court article, je me concentre sur un seul aspect, la variété des AS parmi les serveurs de noms d'une zone DNS.

Pourquoi est-ce que cette variété des AS est un critère pertinent pour l'évaluation de la résilience ? Parce que certains pannes affectent un site physique (c'est le cas des incendies, par exemple), certaines affectent telle ou telle marque de serveurs de noms ou de routeurs (pensez à cisco-sa-20140326-ipv6 <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ip mais d'autres frappent un AS entier. Ce fut le cas de la panne CloudFlare de février 2013 <http://seenthis.net/messages/118644> ou de celle d'OVH en juillet 2013, à cause d'OSPF <http://travaux.ovh.net/?do=details&id=9003>. C'est pour cette raison que ce critère (diversité des AS) figure parmi les métriques de l'Observatoire sur la résilience de l[Caractère Unicode non montré [1]]Internet français <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/7114/show/l-observatoire-sur-la-resilience-de-l-internet-francais-publie-son-rapport-2012.html>. Vous trouverez tous les détails dans ce rapport, mon but est différent, il s'agit d'explorer des zones individuelles.

Bon, OK, toutes choses égales par ailleurs, c'est mieux de répartir les serveurs de noms faisant autorité pour une zone vers plusieurs AS. Mais comment le vérifier ? Si vous avez un flux BGP complet et les outils pour l'analyser, vous pouvez partir de là (regarder les annonces BGP et noter l'AS d'origine). Et si ce n'est pas le cas ? Eh bien, l'excellent service RouteViews <http://www.routeviews.org/> exporte, à partir de flux BGP reçus, cette information sur l'AS d'origine d'une route, et la publie notamment dans le DNS, via la zone `asn.routeviews.org`, qui met en correspondance une adresse IP (IPv4 seulement, hélas, je suis preneur d'informations sur une service équivalent pour IPv6) et le numéro d'AS d'origine :

1. Car trop difficile à faire afficher par LaTeX

```
% dig +short TXT 1.9.0.194.asn.routeviews.org
"2484" "194.0.9.0" "24"
```

La commande ci-dessus a permis de voir que l'adresse IP `194.0.9.1` était annoncée (sous forme du préfixe `194.0.9.0/24`) par l'AS 2484.

On peut alors construire un petit script shell qui va prendre un nom de zone DNS et afficher les AS d'origine de tous les serveurs. Bien sûr, cela ne donnera qu'un aspect de la résilience (notion bien plus riche que juste la variété des AS) et les résultats de ce script doivent être interprétés avec raison. Mais écrire un shell script est un remède souverain lorsqu'on est déprimé ou énervé donc je l'ai fait et il est disponible (en ligne sur `https://www.bortzmeyer.org/files/asns.sh`), fin des avertissements.

Voici un exemple sur le domaine de ce blog. L'outil affiche, pour chaque adresse IPv4 d'un serveur de la zone, l'AS d'origine :

```
% asns.sh bortzmeyer.org
93.19.226.142: "15557"
79.143.243.129: "29608"
204.62.14.153: "46636"
178.20.71.2: "29608"
106.186.29.14: "2516"
217.174.201.33: "16128"
217.70.190.232: "29169"
83.169.77.115: "8784"
95.130.11.7: "196689"
```

On voit une grande variété d'AS (y compris un sur 32 bits, cf. RFC 6793 [2]). De ce strict point de vue, la zone a des chances d'être robuste.

Essayons avec une autre zone :

```
% asns.sh  icann.org
199.43.132.53: "42"
199.43.133.53: "1280"
199.43.134.53: "12041"
199.4.138.53: "26710"
```

Également une bonne variété, on y trouve aussi le fameux AS 42. Et sur un grand site de e-commerce ?

```
% asns.sh amazon.com
204.74.114.1: "12008"
208.78.70.31: "33517"
204.74.115.1: "12008"
208.78.71.31: "33517"
204.13.250.31: "33517"
204.13.251.31: "33517"
204.74.108.1: "12008"
204.74.109.1: "12008"
199.7.68.1: "12008"
199.7.69.1: "12008"
```

2. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6793.txt`

Celui-ci n'a que deux hébergeurs DNS en tout, donc deux AS seulement.

Un cas plus délicat est fourni par `.com` :

```
% asns.sh com
192.54.112.30: "36623"
192.55.83.30: "36618"
192.35.51.30: "36620"
192.33.14.30: "26415"
192.43.172.30: "36632"
192.31.80.30: "36617"
192.5.6.30: "36621"
192.48.79.30: "36626"
192.12.94.30: "36627"
192.42.93.30: "36624"
192.26.92.30: "36619"
192.52.178.30: "36622"
192.41.162.30: "36628"
```

Il y a beaucoup d'AS mais c'est en fait le même fournisseur, Verisign, qui met un AS par serveur, suivant le RFC 6382.

Et des gens qui ont choisi de mettre tous leurs œufs dans le même panier ? On en trouve :

```
% asns.sh  leboncoin.fr
213.186.33.102: "16276"
213.251.128.136: "16276"
```

```
% asns.sh  laposte.net
195.234.36.4: "35676"
178.213.67.14: "35676"
195.234.36.5: "35676"
178.213.66.14: "35676"
```