

# Amusant problème DNS Orange/Oléane/Google

Stéphane Bortzmeyer  
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 janvier 2022

<https://www.bortzmeyer.org/oleane-dns-google.html>

---

Les résolveurs DNS <<https://www.bortzmeyer.org/resolveur-dns.html>> utilisés entre autres par Orange Business Services renvoient l'adresse locale localhost (127.0.0.1) pour des noms chez Google.

Cela ne concerne apparemment que les résolveurs 194.2.0.20 et 194.2.0.50, qui ne semblent pas utilisés par tout le monde chez Orange (comme l'indique leur nom, ce sont des anciennes machines d'Oléane, société rachetée par Orange). Vu avec les sondes RIPE Atlas :

```
% blaueu-resolve -r 100 --as 3215 --nameserver 194.2.0.20 --type A www.google.com
Nameserver 194.2.0.20
[142.250.179.68] : 20 occurrences
[216.58.213.164] : 14 occurrences
[127.0.0.1] : 13 occurrences
[216.58.214.164] : 6 occurrences
[216.58.206.228] : 11 occurrences
[216.58.213.68] : 11 occurrences
[142.250.179.100] : 11 occurrences
[216.58.213.132] : 5 occurrences
[172.217.18.196] : 8 occurrences
Test #34858799 done at 2022-01-19T14:07:44Z
```

La ligne importante est celle avec 127.0.0.1. Notez donc que ce résolveur ne répond pas toujours avec cette adresse. Un problème analogue existe en IPv6 :

```
% blaueu-resolve -r 100 --as 3215 --nameserver 194.2.0.20 --type AAAA www.google.com
Nameserver 194.2.0.20
[2a00:1450:4007:80e::2004] : 12 occurrences
[2a00:1450:4007:813::2004] : 29 occurrences
[2a00:1450:4007:811::2004] : 11 occurrences
[2a00:1450:4007:810::2004] : 11 occurrences
[2a00:1450:4007:806::2004] : 14 occurrences
[::1] : 11 occurrences
[2a00:1450:4007:817::2004] : 11 occurrences
Test #34858911 done at 2022-01-19T14:35:32Z
```

Pourquoi est-ce que la même adresse IP, 194.2.0.20, donne des résultats différents aux sondes, le tout dans un intervalle de temps très court? Probablement parce que derrière cette adresse, il y a plusieurs machines physiques, avec des configurations différentes.

Plusieurs personnes ont signalé ce problème par exemple sur Twitter (ici <https://twitter.com/GmNico/status/1483802992986009606> ou là <https://twitter.com/montreuillois/status/1483745661807910919>), sans réponse d'Orange. Le problème est bien du côté de ces résolveurs, pas des serveurs faisant autorité (<https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>) pour google.com. (Notez qu'aucun autre domaine ne semble avoir été touché, par exemple google.fr n'a pas eu de problème.) En dehors de ces résolveurs, on ne voit pas de problème :

```
% blaeu-resolve -c FR -r 100 - -type A alt2.gmail-smtp-in.l.google.com.
[142.250.150.27] : 53 occurrences
[74.125.200.27] : 1 occurrences
[142.250.150.26] : 43 occurrences
[74.125.200.26] : 2 occurrences
[173.194.202.27] : 1 occurrences
Test #34858791 done at 2022-01-19T14:05:34Z
```

Les signalements à DownDetector <https://downdetector.fr/> sont réels mais trompeurs, Google n'y étant apparemment pour rien :

Quelques heures plus tard, le problème était apparemment réparé :

```
% blaeu-resolve -r 100 --as 3215 --nameserver 194.2.0.20 --type A www.google.com
Nameserver 194.2.0.20
[216.58.206.228] : 17 occurrences
[216.58.213.164] : 30 occurrences
[142.250.179.68] : 24 occurrences
[142.250.74.228] : 12 occurrences
[142.250.186.36] : 1 occurrences
[216.58.214.164] : 16 occurrences
Test #34861409 done at 2022-01-19T20:08:59Z
```

La réponse d'Orange à ses clients : « ORANGE INFO INCIDENT xxxxxx Il y avait un problème de résolution sur le service Cache DNS. Nous avons fait un changement au niveau de nos serveurs. Le service est rétabli depuis hier soir 18H . Nous passons à la cloture du ticket. »

Quelle est la cause de la panne? On l'ignore et il est certain qu'Orange ne communiquera rien. Rappelons juste que le DNS est un service critique de l'Internet et qu'il est donc essentiel de ne pas vouloir le bricoler à des fins, par exemple, de censure. (La panne est peut-être due à une erreur dans la configuration d'un résolveur menteur. Tout bricolage augmente les risques de panne, comme on l'a déjà vu chez Orange <https://www.bortzmeyer.org/google-detourne-par-orange.html> et comme le rapport du Conseil Scientifique de l'Afnic <https://www.afnic.fr/observatoire-ressources/actualites/le-conseil-scientifique-de-lafnic-partage-sur-le-filtrage-internet-par-dns> > avait déjà alerté à ce sujet.)