Exemple d'analyse d'un problème DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 décembre 2012

https://www.bortzmeyer.org/dns-probleme-analyse.html

Ce matin, pour regarder de près l'amusant problème de la disparation du RER C (les sites Web de recherche d'itinéraire en Île-de-France ne connaissent plus cette ligne et ne la proposent plus), je me suis promené sur <http://www.ratp.fr/>. Cela a fortement déplu à mon Firefox : plus de rafraîchissement des pages, réactions très lentes, voire nulles, etc. À l'origine, un problème DNS avec une zone très mal configurée.

Je sais en effet que Firefox réagit de manière pathologique aux problèmes DNS (contrairement à Chromium) : il se bloque à attendre des réponses qui ne viennent pas, même les autres onglets sont paralysés. Donc, il était logique de suspecter un problème DNS. Mais quel problème ? C'est d'autant plus difficile de le savoir que dig donne parfois des réponses correctes et parfois SERVFAIL ("*Server Failure*"). Il faut regarder de plus près.

Le journal du serveur de noms, un Unbound, explique pourquoi on a des problèmes :

```
Dec 11 11:30:05 batilda unbound: [2631:0] info: iterator operate: query www.ratp.fr. A IN
Dec 11 11:30:05 batilda unbound: [2631:0] info: processQueryTargets: www.ratp.fr. A IN
Dec 11 11:30:05 batilda unbound: [2631:0] debug: out of query targets -- returning SERVFAIL
Dec 11 11:30:05 batilda unbound: [2631:0] debug: return error response SERVFAIL
```

"*out of query targets*" veut dire que le résolveur n'a trouvé aucun serveur faisant autorité qui soit disponible. Pourtant, parfois, il y arrive :

```
Dec 11 11:30:09 batilda unbound: [2631:0] info: iterator operate: query www.ratp.fr. AAAA IN
Dec 11 11:30:09 batilda unbound: [2631:0] info: processQueryTargets: www.ratp.fr. AAAA IN
Dec 11 11:30:09 batilda unbound: [2631:0] info: sending query: www.ratp.fr. AAAA IN
Dec 11 11:30:09 batilda unbound: [2631:0] debug: sending to target: <www.ratp.fr.> 195.200.228.2#53
```

Pour comprendre cette incohérence (problème de réseau ? bogue subtile ?), il faut regarder la configuration de `www.ratp.fr`. Si on interroge un des serveurs faisant autorité pour `ratp.fr`, on trouve une délégation :

```
% dig @ns0.ratp.fr A www.ratp.fr

...
;; AUTHORITY SECTION:
www.ratp.fr. 3600 IN NS altns2.ratp.fr.
www.ratp.fr. 3600 IN NS altns1.ratp.fr.

;; ADDITIONAL SECTION:
altns1.ratp.fr. 3600 IN A 195.200.228.2
altns2.ratp.fr. 3600 IN A 195.200.228.130
...
```

OK, `www.ratp.fr` n'est pas dans la même zone que `ratp.fr`. On note aussi qu'il n'y a que deux serveurs de noms et que leurs adresses IP, proches (dans le même /24) laissent supposer qu'il n'y a guère de redondance dans cette configuration. Mais passons et interrogeons les serveurs :

```
% dig @altns1.ratp.fr A www.ratp.fr

; <<>> DiG 9.9.2-P1 <<>> @altns1.ratp.fr A www.ratp.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 1960
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available
;; WARNING: Messages has 11 extra bytes at end

;; QUESTION SECTION:
;www.ratp.fr. IN A

;; Query time: 35 msec
;; SERVER: 195.200.228.2#53(195.200.228.2)
;; WHEN: Tue Dec 11 12:47:34 2012
;; MSG SIZE  rcvd: 40
```

Aïe, déjà un problème. Le `FORMERR` veut dire "*Format error*" et signifie que le serveur n'a pas compris la requête. Depuis peu, dig utilise EDNS par défaut, comme la plupart des résolveurs, et c'est peut-être cela qui a suscité l'incompréhension de `altns1.ratp.fr`. Essayons sans EDNS :

```
% dig +noedns @altns1.ratp.fr A www.ratp.fr

; <<>> DiG 9.9.2-P1 <<>> +noedns @altns1.ratp.fr A www.ratp.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10283
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.ratp.fr. IN A
```

```
;; ANSWER SECTION:
www.ratp.fr. 300 IN A 195.200.228.150
www.ratp.fr. 300 IN A 195.200.228.50

;; Query time: 38 msec
;; SERVER: 195.200.228.2#53(195.200.228.2)
;; WHEN: Tue Dec 11 12:49:37 2012
;; MSG SIZE  rcvd: 83
```

Cette fois, cela marche. Le RFC 2671 [1], qui normalisait EDNS, date de 1999 mais, apparemment, c'est encore une technologie nouvelle pour certains.

Alors, suffit-il de se rabattre sur du vieux DNS sans EDNS ? Sauf qu'il y a d'autres problèmes. Par exemple, alors que `www.ratp.fr` est censé être une zone, les serveurs ne répondent pas aux requêtes SOA :

```
% dig +noedns @altns1.ratp.fr SOA www.ratp.fr

; <<>> DiG 9.9.2-P1 <<>> +noedns @altns1.ratp.fr SOA www.ratp.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 60719
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.ratp.fr. IN SOA

;; Query time: 35 msec
;; SERVER: 195.200.228.2#53(195.200.228.2)
;; WHEN: Tue Dec 11 13:55:35 2012
;; MSG SIZE  rcvd: 29
```

Refusé... Charmant. C'est pareil pour d'autres types de données (comme TXT). Et pour tous les noms situés en dessous de `www.ratp.fr` ? Le serveur répond correctement `NXDOMAIN` (*"No such domain"*) **mais** n'inclut pas le SOA obligatoire dans la réponse :

```
dig +noedns @altns1.ratp.fr A test.www.ratp.fr

; <<>> DiG 9.9.2-P1 <<>> +noedns @altns1.ratp.fr A test.www.ratp.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16785
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;test.www.ratp.fr. IN A
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2671.txt`

```
;; Query time: 36 msec
;; SERVER: 195.200.228.2#53(195.200.228.2)
;; WHEN: Tue Dec 11 14:02:32 2012
;; MSG SIZE  rcvd: 34
```

Cela empêche le résolveur de déterminer le "*zone cut*", la limite de la zone.

Maintenant, pourquoi est-ce que `www.ratp.fr` a des serveurs de noms aussi bogués ? Le plus probable est que `ratp.fr` utilise des logiciels assez classiques mais que `www.ratp.fr` a été délégué, pour les besoins du serveur Web, a une "*appliance*" programmée avec les pieds. De tels boîtiers sont courants, pour assurer des fonctions comme la répartition de charge et, écrits par des gens qui ne connaissent pas le DNS et exploités par des gens du Web qui ne le connaissent pas non plus, ils sont fréquemment horriblement bogués.

Mais revenons à mon problème initial. Puisque Unbound se rabat automatiquement en « sans EDNS » lorsqu'il reçoit la réponse `FORMERR`, pourquoi est-ce que cela marchait irrégulièrement ? L'examen du journal d'Unbound le montre : on voit des requêtes pour `_443._tcp.www.ratp.fr`. Il s'agit là de requêtes DANE (RFC 6698), lancées par une extension Firefox installée sur ma machine. Le nom n'existe pas, OK. Mais la réponse erronée, ne comprenant pas le SOA, perturbe Unbound, l'amenant à conclure que le serveur a un problème. Il ne l'interrogera pas ensuite, pour un moment, renvoyant `SERVFAIL`. En pratique, tout dépendra de l'ordre des requêtes (la requête habituelle en premier ou bien la requête DANE d'abord).

Un tel phénomène (réponse erronée amenant le résolveur à conclure que le serveur est défaillant) avait déjà été observé avec le déploiement du type AAAA (pour les adresses IPv6). Le problème avait été documenté dans le RFC 4074 en 2005. Mais les auteurs d'"*appliances*" ne lisent jamais les RFC...

Si vous voulez voir la curieuse disparition du RER C, voici l'itinéraire proposé ce matin, pour aller de la station Champ de Mars à la station Pont de l'Alma (stations consécutives sur le RER C, options de recherche "Réseau ferré" et "Le moins de correspondance"). `<http://www.ratp.fr/>` suggère tout simplement de traverser la Seine pour aller prendre la ligne 9 ! Si vous trouvez que les trains rampent trop bas et que vous préférez vous envoler, la zone `www.airfrance.com` a la même architecture, et pas mal de problèmes identiques.