La panne de la RATP et le DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 mai 2013

https://www.bortzmeyer.org/ratp-dns.html

Aujourd'hui, le site Web de la RATP, a été en panne de 11h à 16h environ (la reprise a été cahotique, avec de nombreuses rechutes jusqu'en soirée). Que s'est-il passé ? Comme pour chaque panne d'un service Internet, c'est l'occasion d'en tirer des leçons pour améliorer la **résilience**.

Sur les réseaux sociaux, les utilisateurs mécontents ont signalé le problème en disant que « le site Web ne marche pas » ou que « l'appli (pour mobile) ne marche pas ». Mais la vraie cause n'étant pas là. Regardons pendant la panne avec wget :

```
% wget http://www.ratp.fr/
--2013-05-16 11:52:21--  http://www.ratp.fr/
Resolving www.ratp.fr... failed: Name or service not known.
wget: unable to resolve host address 'www.ratp.fr'
```

Le message d'erreur est clair : le client HTTP wget n'a pas réussi à charger le site car il n'a pas pu résoudre le nom en adresse IP. C'était donc un problème DNS, apparemment. Regardons le DNS pendant la panne avec dig. Quels sont les serveurs de noms de `ratp.fr` ?

```
% dig NS ratp.fr
...
;; ANSWER SECTION:
ratp.fr.                3600    IN      NS      indom10.indomco.com.
ratp.fr.                3600    IN      NS      ns1.ratp.fr.
ratp.fr.                3600    IN      NS      indom30.indomco.fr.
ratp.fr.                3600    IN      NS      ns0.ratp.fr.
...
```

Et demandons à l'un d'eux l'adresse de `www.ratp.fr` :

```
% dig @ns0.ratp.fr. A www.ratp.fr
...
;; AUTHORITY SECTION:
www.ratp.fr.            3600    IN      NS      altns1.ratp.fr.
www.ratp.fr.            3600    IN      NS      altns2.ratp.fr.

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

;; Query time: 4 msec
;; SERVER: 193.104.162.15#53(193.104.162.15)
;; WHEN: Thu May 16 11:53:02 2013
;; MSG SIZE  rcvd: 114
```

Ah, on n'a pas directement l'adresse mais une **délégation**. Le DNS repose sur un système arborescent de délégations depuis la racine jusqu'à la machine qui connait la réponse. Dans `.fr`, il n'y a en général pas de délégation entre le deuxième et le troisième **composant** du nom de domaine mais, ici, c'est le cas : `www.ratp.fr` n'est pas dans la même **zone** que `ratp.fr`.

Avant de revenir sur les raisons de cette délégation inhabituelle (mais parfaitement légale), continuons la recherche de l'adresse IP de `www.ratp.fr` :

```
% dig @altns1.ratp.fr. A www.ratp.fr
; <<>> DiG 9.7.3 <<>> @altns1.ratp.fr. A www.ratp.fr
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Et c'est pareil pour `altns2.ratp.fr`. La zone n'a que deux serveurs de noms, ce qui est peu, et les deux sont en panne en même temps. Pas étonnant que le nom ne puisse pas être résolu.

Pourquoi ces deux serveurs sont en panne simultanément ? La proximité de leurs adresses IP fait penser qu'ils sont sans doute au même endroit, et qu'ils ont été victimes de la même panne de courant ou de réseau ou de la même attaque par déni de service. La RATP n'a pas suivi un principe de base de la résilience : éloigner les serveurs de noms, pour que la même panne ne les coupe pas tous en même temps. On note que la zone `ratp.fr` suit les bons principes (quatre serveurs, bien éloignés). Mais `www.ratp.fr` ne le fait hélas pas.

Mais pourquoi cette délégation relativement inhabituelle du nom `www` ? Le plus probable est que le site Web se trouve derrière un équipement de répartition de charge et que cet équipement prend également en charge le DNS, changeant les réponses suivant la demande. Une fois le service réparé, on peut d'ailleurs constater que ces engins envoient des réponses avec une durée de vie très courte (300 secondes). Ces équipements conçus pour les gens du Web (qui ne connaissent pas forcément le DNS) sont souvent bogués jusqu'au trognon. Ainsi, un des serveurs répond parfois `FORMERR` ("*Format Error*") et renvoie une réponse syntaxiquement incorrecte (le "*Messages has 11 extra bytes at end*") :

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

...
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 12599
```

```
;; 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: 37 msec
;; SERVER: 195.200.228.2#53(195.200.228.2)
;; WHEN: Thu May 16 22:17:06 2013
;; MSG SIZE  rcvd: 40
```

Ce comportement disparait si on coupe EDNS.

Merci à Jean-Baptiste Favre pour le premier signalement.