L'Internet, ça ne marche pas de partout

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 août 2020. Dernière mise à jour le 16 août 2020

https://www.bortzmeyer.org/routage-divers.html

Lorsqu'une panne survient et empêche l'accès à une ressource sur l'Internet, il y a parfois discussion car certaines personnes disent « mais non, pour moi, ça marche », alors que la victime originelle insiste « je te dis que c'est cassé ». Les deux peuvent avoir simultanément raison. Les pannes peuvent dépendre d'où vous vous trouvez, mais elles dépendent surtout de votre réseau d'accès à l'Internet. Voyons un exemple concret avec une panne affectant Algérie Télécom et qui empêche, par exemple, les abonnés d'Orange en France d'accéder à .

Avant de tester depuis plusieurs endroits, il faut s'assurer qu'on dispose d'un moyen fiable de tester. Beaucoup de gens font une confiance aveugle à la commande ping mais ils ont tort : les paquets ICMP de type Écho qu'elle utilise peuvent être bloqués par un pare-feu hargneux, sans que les autres services soient affectés. Dans le cas de `cetic.dz`, le signalement initial portait sur un problème DNS et on aurait donc pu tester avec des requêtes DNS mais, ici, ce n'est pas la peine : les machines en cause, `193.251.169.83` et `193.251.169.84` répondent en ICMP Echo :

```
% ping -c 3 193.251.169.83

PING 193.251.169.83 (193.251.169.83) 56(84) bytes of data.
64 bytes from 193.251.169.83: icmp_seq=1 ttl=50 time=81.2 ms
64 bytes from 193.251.169.83: icmp_seq=2 ttl=50 time=79.2 ms
64 bytes from 193.251.169.83: icmp_seq=3 ttl=50 time=79.3 ms

--- 193.251.169.83 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 79.184/79.875/81.183/0.953 ms
```

Depuis un réseau où ça ne marche pas :

```
% ping -c 3 193.251.169.83
PING 193.251.169.83 (193.251.169.83) 56(84) bytes of data.

--- 193.251.169.83 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2052ms
```

Bon, nous avons un problème variable : à certains endroits, ça marche, à d'autres pas. Dans des cas comme cela, lorsque les gens discutent sur un forum quelconque du problème, ceux et celles qui ont compris que le problème dépendait du point de mesure précisent souvent leur expérience en indiquant leur ville (« depuis Marseille, ça marche »). C'est une erreur car ce n'est en général pas la localisation géographique qui compte mais plus souvent le réseau d'accès, donc le FAI ou plus exactement l'AS. Il est curieux que même sur une liste de diffusion de professionnels du réseau comme NANOG, les gens qui signalent une panne indiquent plus souvent leur ville que leur AS…Pour M. Toutlemonde, comme il ne connait pas en général son AS, indiquer le FAI est plus utile.

Donc, ici, on a une panne qui dépend de l'endroit. Comment la tester ? J'ai utilisé des comptes sur deux machines différentes, connectées à des opérateurs différents. Mais si on n'a pas des comptes partout, on fait comment ? Eh bien le plus simple est d'utiliser les sondes RIPE Atlas <https://atlas.ripe.net/>, ces petits boitiers installés par des volontaires un peu partout et qui peuvent effectuer des mesures actives, créés par exemple via le logiciel Blaeu <https://framagit.org/bortzmeyer/blaeu>. Demandons à cent sondes Atlas de pinguer 193.251.169.84 :

```
% blaeu-reach --requested 100 193.251.169.84
98 probes reported
Test #26682471 done at 2020-08-13T12:10:32Z
Tests: 245 successful tests (83.6 %), 0 errors (0.0 %), 48 timeouts (16.4 %), average RTT: 111 ms
```

On aurait dû avoir à peu près 100 % de succès mais on n'a que 84 %. Et, surtout, cela dépend du réseau. Si on essaie depuis Orange (AS 3215) :

```
% blaeu-reach --requested 100 --as 3215 193.251.169.84
96 probes reported
Test #26682501 done at 2020-08-13T12:12:04Z
Tests: 3 successful tests (1.0 %), 0 errors (0.0 %), 285 timeouts (99.0 %), average RTT: 139 ms
```

On a cette fois quasiment uniquement des échecs. Depuis un autre opérateur (ici, Free), tout marche :

```
% blaeu-reach --requested 100 --as 12322 193.251.169.84
98 probes reported
Test #26683832 done at 2020-08-13T14:08:11Z
Tests: 293 successful tests (99.7 %), 0 errors (0.0 %), 1 timeouts (0.3 %), average RTT: 52 ms
```

Mais pourquoi est-ce que ça marche depuis Free et pas depuis Orange ? La première tentation est de suspecter un problème BGP, le protocole qui distribue les routes sur l'Internet. Le service RIPE Stat <https://stat.ripe.net/> nous permet de voir le routage du préfixe concerné <https://stat.ripe.net/193.251.169.84#tabId=routing> et, pour citer RIPE Stat, « "*At 2020-08-13 00 :00 :00 UTC, 193.251.169.0/24 was 100% visible (by 321 of 321 RIS full peers).*" ». Bref, le préfixe 193.251.169.0/24 est visible partout, et ne semble pas massivement filtré.

Mais attention, le RIS <https://ris.ripe.net/>, réseau de routeurs sur lequel se base RIPE Stat n'est pas présent partout. Et, notamment, il ne semble pas présent chez OpenTransit, transitaire d'Orange et membre du même groupe. On notera en effet qu'un préfixe IP plus général, 193.251.160.0/20, est annoncé par la société OpenTransit. Et, en regardant le "*looking glass*" d'OpenTransit on ne voit que ce préfixe plus général, pas le /24 <https://looking-glass.opentransit.net/>.

Il semble donc bien qu'OpenTransit n'accepte pas l'annonce BGP d'Algérie Télécom pour 193.251.169.0/24 et n'ait pas de route pour ce préfixe.

La faute à qui dans cette embrouille ? C'est évidemment difficile à dire. Le préfixe 193.251.160.0/20 est bien à Orange, comme on le voit avec whois :

```
% whois 193.251.160.0/20
...
inetnum:        193.248.0.0 - 193.253.255.255
netname:        FR-TELECOM-248-253
org:            ORG-FT2-RIPE
...
organisation:   ORG-FT2-RIPE
org-name:       Orange S.A.
```

Mais le préfixe plus spécifique `193.251.169.0/24` a bien été délégué proprement à Algérie Télécom :

```
% whois 193.251.169.0/24
...
inetnum:        193.251.169.0 - 193.251.169.255
netname:        Djaweb-Algerie-Telecom
descr:          Internet Service Provider of Algerie Telecom
country:        DZ
```

Il n'y a par contre pas d'objet « route » dans les IRR pour `193.251.169.0/24`, on ne voit que la route du plus général /20 :

```
% whois -T route 193.251.169.0/24
...
route:          193.251.160.0/20
descr:          France Telecom
descr:          OPENTRANSIT
origin:         AS5511
```

Mais le préfixe `193.251.169.0/24` a un ROA ("*Route Origin Authorizations*", une signature des ressources Internet pour garantir leur authenticité, cf. RFC 6482 [1] :

```
% whois -h whois.bgpmon.net 193.251.169.0/24
...
Prefix:             193.251.169.0/24
Origin AS:          36947
Origin AS Name:     ALGTEL-AS, DZ
RPKI status:        ROA validation successful
...
```

Il n'aurait pas pu avoir ce ROA sans l'autorisation du titulaire du préfixe plus général (Orange). Donc, il se pourrait qu'il s'agisse d'un problème interne à Orange, une délégation d'un préfixe incomplètement faite.

Ah, et pour revenir au problème original, on m'avait signalé l'injoignabilité de `cetic.dz` en suspectant un problème DNS. En effet, le domaine `cetic.dz` ne fonctionne pas du tout depuis Orange. Mais

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6482.txt`

c'est parce que ce domaine n'a que deux adresses IP pour ses serveurs de noms, les 193.251.169.83 et 193.251.169.84 cités plus haut, et que ces deux adresses sont injoignables depuis Orange. Le problème n'était donc pas de la faute des résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> d'Orange mais du routage.

J'en profite pour rappeler les bonnes pratiques de robustesse DNS : attention aux SPOF, ne faites pas comme cetic.dz, ne mettez pas tous vos serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> dans le même /29...Voici les serveurs de cetic.dz vus par check-soa <https://www.bortzmeyer.org/check-soa-go.html>. On pourrait croire qu'ils sont trois mais il n'y a en fait que deux adresses IP :

```
% check-soa cetic.dz
dns.cetic.dz.
193.251.169.83: OK: 2020070604
193.251.169.83: OK: 2020070604
ftp.cetic.dz.
193.251.169.84: OK: 2020070604
raqdns.cetic.dz.
193.251.169.83: OK: 2020070604
```

Sur ces bonnes pratiques de gestion de serveurs DNS, on fera bien de consulter le guide de l'AFNIC <https://www.afnic.fr/medias/documents/afnic-dossier-dns-attaques-securite-2009-06.pdf> et celui de l'ANSSI <https://www.ssi.gouv.fr/guide/bonnes-pratiques-pour-lacquisition-et>.

Voilà, j'espère vous avoir convaincu que le déboguage de problèmes Internet n'est pas toujours simple et que, quand on signale un problème, il faut donner le maximum de détails <https://www.bortzmeyer.org/donner-des-details.html>. Merci au signaleur du problème, ce fut une recherche intéressante. Et merci à Pierre Emeriaud, Pavel Polyakov et Radu-Adrian Feurdean pour leurs observations pertinentes.