Panne Internet à Saint-Pierre-et-Miquelon

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 janvier 2014. Dernière mise à jour le 5 janvier 2014

https://www.bortzmeyer.org/panne-saint-pierre-miquelon.html

Aujourd'hui, vers 19 :30 UTC, une coupure complète de la connexion Internet de Saint-Pierre-et-Miquelon a eu lieu. C'est l'occasion de regarder ce que fait le protocole de routage de l'Internet, BGP, dans ce cas, puisque toutes les données sont publiques.

La panne a été signalée par BGPmon <https://bgpmon.net> sur Twitter <https://twitter.com/bgpmon/status/419577842200899584>. Il y a normalement quatre préfixes d'adresses IP, qui sont émis depuis l'île, 70.36.4.0/22, 70.36.12.0/22, 70.36.8.0/22 et 70.36.0.0/22. Tous pourraient s'agréger en un 70.36.0.0/20 mais ce n'est pas le cas. Il y a apparemment un seul opérateur à Saint-Pierre-et-Miquelon, SPM Télécom (qui gère le portail <http://www.cheznoo.net> à l'adresse 70.36.0.23). Tous ces services étaient inaccessibles (cela remarche désormais <http://www.cheznoo.net/saint-pierre-et-miquelon/assistance/reseau.php>). On notera que le domaine cheznoo.net n'a que deux serveurs DNS, ce qui est insuffisant, et que les deux sont dans les préfixes affectés (manque de redondance) rendant donc le domaine complètement inaccessible. Cela permet, pendant la panne, de regarder des sites comme un blog parlant de la vie à Saint-Pierre-et-Miquelon <http://ma-vie-st-pierre-et-miquelon.over-blog.com/> et des problèmes de réseau <http://ma-vie-st-pierre-et-miquelon.over-blog.com/article-28118644.html>.

Pour analyser les données BGP, nous allons utiliser les données de RouteViews <http://www.routeviews.org/>. Elles sont en binaire, au format MRT (RFC 6396 [1]), il faut les transformer en texte avec bgpdump <https://bitbucket.org/ripencc/bgpdump/>. On sait d'après BGPmon l'heure approximative de la panne, on va donc récupérer le fichier, le transformer en texte et le fouiller. RouteViews offre deux types de fichier, "RIBS" qui contient l'état courant des tables de routage, et "UPDATES" qui contient les mises à jour. Vérifions d'abord l'état avant la panne, en prenant le fichier de 18 :00 :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6396.txt

```
% wget ftp://archive.routeviews.org/route-views.linx/bgpdata/2014.01/RIBS/rib.20140104.1800.bz2
% bgpdump rib.20140104.1800.bz2 > rib.20140104.1800.txt
% fgrep -B3 -A5 70.36.0. rib.20140104.1800.txt
...
TIME: 01/04/14 18:00:02
TYPE: TABLE_DUMP_V2/IPV4_UNICAST
PREFIX: 70.36.0.0/22
SEQUENCE: 95877
FROM: 195.66.225.111 AS5580
ORIGINATED: 12/29/13 19:25:03
ORIGIN: IGP
ASPATH: 5580 1299 3356 11260 3695
...
```

Et on voit que le préfixe `70.36.0.0/22` existait bien à 18 :00. L'AS 3695, à l'origine de cette annonce, est SPM Télécom. Et à 20 :00 ?

```
% wget ftp://archive.routeviews.org/route-views.linx/bgpdata/2014.01/RIBS/rib.20140104.2000.bz2
% bgpdump rib.20140104.2000.bz2 > rib.20140104.2000.txt
% fgrep -B3 -A5 70.36.0. rib.20140104.2000.txt
%
```

Le préfixe a disparu. Quand exactement et que lui est-il arrivé ? Regardons cette fois les "UPDATES" :

```
% wget ftp://archive.routeviews.org/route-views.linx/bgpdata/2014.01/UPDATES/updates.20140104.1930.bz2
% bgpdump updates.20140104.1930.bz2 > updates.20140104.1930.txt
```

Et explorons ce fichier, bien plus petit que les "RIBS", avec un éditeur ordinaire. On voit le premier retrait du préfixe à 19 :33 :57 :

```
TIME: 01/04/14 19:33:57
TYPE: BGP4MP/MESSAGE/Update
FROM: 195.66.236.32 AS3257
TO: 195.66.237.222 AS6447
WITHDRAW
  70.36.12.0/22
  70.36.8.0/22
  70.36.4.0/22
  70.36.0.0/22
```

Ce retrait est suivi de plusieurs annonces. En effet, tous les routeurs BGP ne sont pas synchrones. Certains croient que la route qu'ils connaissent est toujours valable et l'annoncent à nouveau, avant de la retirer quelques secondes plus tard. Le dernier retrait, définitif, n'aura lieu que deux minutes après, ce qui donne une bonne idée du temps typique de propagation des annonces BGP :

```
TIME: 01/04/14 19:35:42
TYPE: BGP4MP/MESSAGE/Update
FROM: 195.66.224.215 AS31500
TO: 195.66.225.222 AS6447
WITHDRAW
  70.36.0.0/22
  70.36.4.0/22
  70.36.8.0/22
  70.36.12.0/22
```

Et la cause de cette panne ? Apparemment une importante coupure de courant à Terre-Neuve <http://www.cbc.ca/news/canada/newfoundland-labrador/newfoundland-power-may-be-out-until-monday-2484031>. La connectivité a été rétablie le lendemain vers 00 :30 UTC. Le fichier ftp://archive.routeviews.org/ro contient les nouvelles annonces :

```
TIME: 01/05/14 00:34:35
TYPE: BGP4MP/MESSAGE/Update
FROM: 195.66.224.32 AS3257
TO: 195.66.225.222 AS6447
ORIGIN: IGP
ASPATH: 3257 11260 3695
NEXT_HOP: 195.66.224.32
MULTI_EXIT_DISC: 751
COMMUNITY: 3257:4000 3257:8138 3257:50002 3257:50120 3257:51100 3257:51105
ANNOUNCE
  70.36.8.0/22
  70.36.0.0/22
  70.36.12.0/22
```

Notez que Saint-Pierre-et-Miquelon a son propre TLD, .pm mais que les serveurs DNS de celui-ci sont en dehors de l'île et n'ont donc pas été affectés. De même, des sites Web comme <http://www.tourisme-saint-pierre-et-miquelon.com/> sont manifestement hébergés en France métropolitaine et ont continué à fonctionner. Des sites Web comme celui de la compagnie aérienne <http://www.airsaintpierre.com/>, hébergés localement, ont par contre été mis hors d'usage.

La connexion actuelle de Saint-Pierre-et-Miquelon ne se fait que par un faisceau hertzien vers Terre-Neuve (cette grande île étant ensuite connectée par un câble sous-marin, sans doute Greenland Connect). Elle utilise l'opérateur canadien Eastlink. Ce n'est pas la première panne de cette liaison (voir le blog du président du conseil territorial <http://www.stephaneartano.net/article-nouvelle-panne-internet-vive html>). Un projet est en cours <http://www.avicca.org/IMG/pdf/130523_StPierreMiquelon_DossierCRIP_FSN.pdf> pour remplacer l'hertzien par un câble sous-marin. Si vous voulez candidater pour la pose du futur câble, l'appel d'offres est ici <http://www.marchesonline.com/mol/front/visualisation/run.do?idsim=6010841&versionsim=1&typeinfo=typeao>.

Merci à Andree Tonk pour BGPmon, et à Marc Albert Cormier <https://twitter.com/marccormier> pour ses informations.