RIS Live, un flux de messages BGP en temps réel

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 février 2019

https://www.bortzmeyer.org/ris-live.html

Les annonces du protocole de routage BGP sont publiques, comme beaucoup de choses sur l'Internet. Mais si on ne gère pas soi-même un routeur connecté à la DFZ, comment récupère-t-on ces annonces ? Plusieurs systèmes vous donnent accès à ces annonces, mais pas en temps réel. Désormais, grâce à RIS Live <https://ris-live.ripe.net/>, tu peux, toi aussi, internaute ordinaire, accéder à cette information immédiatement.

Quel est l'intérêt de voir ces annonces ? Petit détour pour expliquer ce que fait BGP : l'Internet, et c'est sa principale caractéristique, est d'être un **réseau de réseaux**. Aucune organisation n'est en charge de l'Internet dans sa globalité. Chacun (entreprise, association, particulier) gère un des réseaux qui, connectés ensemble, constitue l'Internet. Comment, dans ces conditions, un réseau situé en France sait à qui envoyer les paquets lorsqu'un de ses utilisateurs veut écrire en Mongolie ? C'est tout simple (dans le principe) : chaque opérateur réseau prévient ses voisins (ceux à qui il est directement connecté) des adresses IP qu'il gère. Le voisin prévient ensuite son voisin, et ainsi de suite. Au bout d'un moment, l'opérateur français recevra l'information sur les adresses IP de son collègue mongol, et va donc savoir à qui transmettre les paquets, qui suivront un chemin à peu près réciproque (oui, je simplifie...) de celui suivi par les annonces. Ces annonces sont manuelles lorsqu'un petit acteur se connecte à un gros, mais les gros opérateurs utilisent entre eux le protocole BGP, normalisé dans le RFC 4271 [1]. En permanence, les opérateurs connectés à la DFZ (et quelques autres) s'échangent ces annonces : « j'ai désormais une route vers 2c0f:fe30::/32 », « je n'ai plus ma route vers 208.65.144.0/24 ». Ces annonces sont les battements de cœur de l'Internet. Notez que BGP n'informe que des nouveautés : il n'a pas d'envoi périodique, contrairement à ce que font certains protocoles de routage intérieurs. Néanmoins, comme il y a toujours quelque chose qui bouge ou qui change dans l'Internet, en pratique, l'activité BGP est importante.

Ces annonces sont traitées automatiquement par les routeurs qui ajoutent les nouvelles routes, retirent les anciennes et décident, au vu des routes disponibles, à quel voisin envoyer les paquets. Mais il y a aussi des humains qui regardent ces annonces. Il y a les opérationnels, les gens qui dans les

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4271.txt

NOC surveillent le réseau et interviennent en cas de problèmes. (Ils utilisent par exemple des systèmes d'alerte <https://www.bortzmeyer.org/alarmes-as.html> pour savoir si quelqu'un n'a pas annoncé leurs préfixes IP.) Il y a les chercheurs, qui publient d'intéressantes études sur les dynamiques à l'œuvre dans l'Internet. Il y a les étudiants qui veulent apprendre. Et il y a les curieux qui aiment regarder ce qui se passe. Comme exemple des travaux qui résultent de l'observation de BGP, notons par exemple le rapport sur la résilience de l'Internet français <https://www.ssi.gouv.fr/agence/rayonnement-scientifique/lobservatoire-de-la-resilience-de-linternet-francais/>, édité par l'ANSSI.

Passons maintenant au sujet principal de cet article, RIS Live <https://ris-live.ripe.net/>. Il s'agit d'un service du RIPE-NCC, s'appuyant sur un réseau de routeurs BGP, le RIS <https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris>. Les routeurs du RIS ont des sessions BGP avec un grand nombre d'opérateurs et voient donc une grande partie du trafic BGP. (Avec BGP, contrairement à des protocoles comme OSPF, les routeurs ne voient pas tous la même chose, et aucun routeur ne connait tout. Observer BGP nécessite donc plusieurs routeurs, placés à différents endroits de l'Internet et, même dans ce cas, on ne voit pas tout.) Les données récoltées par le RIS sont accessibles via divers moyens comme RIPE stat <https://stat.ripe.net/>, mais toujours avec un certain retard.

Au contraire, RIS Live est temps réel. Regardez la page Web <https://ris-live.ripe.net/>, on y voit le trafic actuel, rafraichi en permanence (tant que cette page reste ouverte, votre machine reçoit les informations de RIS Live).

Mais vous n'êtes pas obligé d'utiliser le Web, RIS Live est accessible via une API (la page Web utilise d'ailleurs cette API, via du code JavaScript chargé avec la page). Cette API repose sur WebSocket (RFC 6455) et est bien documentée <https://ris-live.ripe.net/manual/>.

J'ai écrit un petit programme Python d'exemple avec cette API, . Il utilise la bibliothèque websockets <https://websockets.readthedocs.io/> pour faire du WebSocket. Utilisons-le pour voir :

```
% ./ris-live.py
{"type":"ris_message","data":{"timestamp":1550561936.88,"peer":"198.32.176.14","peer_asn":"2914","id":"198.
{"type":"ris_message","data":{"timestamp":1550561936.88,"peer":"2001:504:d::6","peer_asn":"2914","id":"2001
{"type":"ris_message","data":{"timestamp":1550561936.88,"peer":"2001:504:d::6","peer_asn":"2914","id":"2001
{"type":"ris_message","data":{"timestamp":1550561936.91,"peer":"27.111.228.6","peer_asn":"18106","id":"27.11
```

Je vous avais prévenu qu'il y en avait du trafic BGP, à tout instant ! Les messages de RIS Live sont en JSON. Voyons une annonce complète :

```
{
  "timestamp": 1550562092.12,         (le moment de l'annonce, le 19
                                      février 2019 à 07:41:32 UTC,
      comme on peut le voir avec 'date -u --date=@1550562092.12')
  "peer": "2001:7f8:20:101::208:223", (le voisin BGP du routeur RIS)
  "peer_asn": "20764",                (le numéro de système autonome
                                      dudit voisin)
  "host": "rrc13",                    (l'identité du routeur RIS qui a
                                      vu l'annonce)
  "type": "UPDATE",
  "path": [                           (le chemin d'AS - Autonomous
                                      System, système autonome - : l'AS d'origine est le 33047)
    20764,
    8359,
```

```
    6327,
    16696,
    33047
  ],
  "community": [                        (les communautés BGP attachées
                                        à l'annonce)
    [
      6327,
      1405
    ],
    [
      6327,
      41030
    ]
  ],
  "origin": "igp",
  "announcements": [                    (l'annonce elle-même, pour le
                                         préfixe d'adresses IP 2a03:8160:14::/48)
    {
      "next_hop": "2001:7f8:20:101::208:223",
      "prefixes": [
        "2a03:8160:14::/48"
      ]
    }
  }
}
```

(La notion - cruciale - de système autonome ou AS est expliquée sur Wikipédia. Les communautés BGP sont normalisées dans le RFC 1997.)

RIS Live offre de nombreuses options pour ne pas être noyé sous l'afflux des annonces, et pour ne sélectionner que celles qui vous intéressent. Le programme `ris-live.py` permet d'en sélectionner certaines. Ici, par exemple, on ne demande que ce qui concerne l'AS 2484 (utilisé par l'AFNIC) :

```
% ./ris-live.py --path 2484 -v
Trying to connect, to send {"type": "ris_subscribe", "data": {"path": "2484"}}
Connected, {"type": "ris_subscribe", "data": {"path": "2484"}} sent
Trying to receive
Waking up, it is 2019-02-18T17:00:05Z
Waking up, it is 2019-02-18T17:01:05Z
{"type":"ris_message","data":{"timestamp":1550509323.73,"peer":"2001:7f8::514b:0:1","peer_asn":"20811","id":"200
Trying to receive
Waking up, it is 2019-02-18T17:02:05Z
...
Waking up, it is 2019-02-18T17:27:05Z
Waking up, it is 2019-02-18T17:28:05Z
{"type":"ris_message","data":{"timestamp":1550510896.29,"peer":"2001:7f8::514b:0:1","peer_asn":"20811","id":"200
```

On peut aussi ne demander que les informations d'un seul routeur RIS. Pour avoir la liste de ces routeurs :

```
 % ./ris-live.py -l
{"type":"ris_rrc_list","data":["rrc00","rrc01","rrc03","rrc04","rrc05","rrc06","rrc07","rrc10","rrc11","rrc12","
```

À ma connaissance, tous ne sont pas sur la DFZ et n'ont donc pas un flux complet, certains sont sur des points d'échange et ne voient que le trafic BGP au point d'échange.

Pour avoir un flux BGP en temps réel, je suppose qu'on peut utiliser l'alternative bgpstream <`https://bgpstream.caida.org/`> mais je n'ai pas encore testé.
