RFC 8354 : Use Cases for IPv6 Source Packet Routing in Networking (SPRING)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mars 2018

Date de publication du RFC : Mars 2018

http://www.bortzmeyer.org/8354.html

Le sigle SPRING signifie « "*Source Packet Routing In NetworkinG*" ». C'est quoi, le routage par la source ("*source routing*") ? Normalement, la transmission de paquets IP se fait uniquement en fonction de l'adresse de destination, chaque routeur sur le trajet prenant sa décision indépendemment des autres, et sans que l'émetteur original du paquet n'ait son mot à dire. L'idée du routage par la source est de permettre à cet émetteur d'indiquer par où il souhaite que son paquet passe. L'idée est ancienne, et resurgit de temps en temps sur l'Internet. Ce nouveau RFC décrit les cas où une solution de routage par la source serait utile.

L'idée date des débuts de l'Internet. Par exemple, la norme IPv4, le RFC 791 [1], spécifie, dans sa section 3.1, deux mécanismes de routage par la source, « "*Loose Source Routing*" » et « "*Strict Source Routing*" ». Mais ces mécanismes sont peu déployés et vous n'avez guère de chance, si vous mettez ces options dans un paquet IP, de voir un effet. En effet, le routage par la source est dangereux, il permet des attaques variées, et il complique beaucoup le travail des routeurs. Le but du projet SPRING, dont c'est le deuxième RFC, est de faire mieux. Le cahier des charges du projet est dans le RFC 7855.

L'architecture technique de SPRING est dans un document pas encore publié, draft-ietf-spring-segment-routi
Ce "*segment routing*" est déjà mis en œuvre dans le noyau Linux depuis la version 4.14 (cf. le site du projet <http://www.segment-routing.org/>). Notre nouveau RFC 8354 ne contient, lui, que les scénarios d'usage. (Certains étaient déjà dans la section 3 du RFC 7855.) Seul IPv6 est pris en compte.

D'abord, le cas du SOHO connecté à plusieurs fournisseurs d'accès. Comme chacun de ces fournisseurs n'acceptera que des paquets dont l'adresse IP source est dans un préfixe qu'il a alloué au client, il est essentiel de pouvoir router en fonction de la source, afin d'envoyer les paquets ayant une adresse source du FAI A vers le FAI A et seulement celui-ci. Voici par exemple comment faire sur Linux, quand on veut envoyer les paquets ayant l'adresse IP source 2001:db8:dc2:45:216:3eff:fe4b:8c5b vers un routeur différent de l'habituel (le RFC 3178 peut être une bonne lecture, quoique daté, notamment sa section 5) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc791.txt

```
#!/bin/sh

DEVICE=eth1
SERVICE=2001:db8:dc2:45:216:3eff:fe4b:8c5b
TABLE=CustomTable
ROUTER=2001:db8:dc2:45:1

echo 200 ${TABLE} >> /etc/iproute2/rt_tables
ip -6 rule add from ${SERVICE} table ${TABLE}
ip -6 route add default via ${ROUTER} dev ${DEVICE} table ${TABLE}
ip -6 route flush cache
```

Notez que la décision correcte peut être prise par la machine terminale <http://www.bortzmeyer.org/terminal-host.html>, comme dans l'exemple ci-dessus, ou bien par un routeur situé plus loin sur le trajet (dans le projet SPRING, la source n'est pas forcément la machine terminale initiale).

Outre le fait que le FAI B rejetterait probablement les paquets ayant une adresse source qui n'est pas à lui (RFC 3704), il peut y avoir d'autres raisons pour envoyer les paquets sur une interface de sortie particulière :

— Elle est plus rapide,
— Elle est moins chère (pensez à un réseau connecté en filaire mais également à un réseau mobile avec forfait « illimité » ce qui, en langage telco, veut dire ayant des limites),
— Dans le cas du télétravailleur, il peut être souhaitable de faire passer les paquets de la machine personnelle par un FAI payé par le télétravailleur et ceux de la machine de bureau par un FAI payé par l'employeur.

Autre cas où un routage par la source peut être utile, le FAI peut s'en servir pour servir certains utilisateurs ou certains usages dans des conditions différentes, par exemple avec des prix à la tête du client. Cela viole sans doute la neutralité du réseau <http://www.bortzmeyer.org/neutralite.html> mais c'est peut-être un scénario qui en tentera certains (sections 2.2 et 2.5 du RFC). Cela concerne le réseau d'accès (de M. Michu au FAI) et aussi le cœur de réseau ; « l'opérateur peut vouloir configurer un chemin spécial pour les applications sensibles à la latence <http://www.bortzmeyer.org/latence.html> ».

De plus haute technologie est le scénario présenté dans la section 2.3. Ici, il s'agit d'un centre de données entièrement IPv6. Cela simplifie considérablement la gestion du réseau, et cela permet d'avoir autant d'adresses qu'on veut, sans se soucier de la pénurie d'adresses IPv4 <http://www.bortzmeyer.org/epuisement-adresses-ipv4..html>. Certains opérateurs travaillent déjà à de telles configurations. Dans ce cas, le routage par la source serait un outil puissant pour, par exemple, isoler différents types de trafic et les acheminer sur des chemins spécifiques.

Si le routage par la source, une très vieille idée, n'a jamais vraiment pris, c'est en grande partie pour des raisons de sécurité. La section 4 rappelle les risques associés, qui avaient mené à l'abandon de la solution « "*Type 0 Routing Header*" » (cf. RFC 5095).