Les paquets IP passent-ils vraiment là où on leur dit ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 juillet 2022

https://www.bortzmeyer.org/control-plane-data-plane.html

La lecture d'une excellente étude faite à l'université de Twente m'a motivé pour faire un court article sur une question qu'on se pose trop rarement : sur un réseau comme l'Internet, les paquets IP passent-il vraiment là où le protocole de routage, typiquement BGP, leur a dit de passer ?

Je vous divulgâche tout de suite la fin : non. Comme répètent souvent les administrateurs réseau anglophones, « "*The data plane does not always follow the control plane*" ». Qu'est-ce que cela veut dire ?

Expliquons un peu le routage, dans un réseau comme l'Internet : les routeurs se parlent entre eux et échangent des informations (du genre « Tu sais quoi ? Je sais comment joindre 2001:db8:fa9:aa3::/64. ») et ces informations échangées leur servent à construire leur **table de routage**, une structure de données qui associe aux préfixes IP (comme ce 2001:db8:fa9:aa3::/64), l'adresse du routeur suivant, celui qui rapprochera le paquet du but. Ensuite, lorsqu'un routeur reçoit un paquet, il consulte sa table de routage et envoie le paquet au routeur suivant, via la bonne interface. Deux choses sont à noter :

— Il y a deux processus distincts, le **routage** ("*routing*" en anglosaxonien, construire la table avec les informations reçues par des protocoles de routage comme Babel - RFC 8966 [1]), et la **transmission** ("*forwarding*" dans la langue de Perlman, envoyer le paquet). Ces deux processus utilisent des protocoles très différents, n'ont pas les mêmes contraintes (par exemple, la transmission est temps-réel, avec des contraintes très serrées) et, dans un routeur haut de gamme, ces deux processus sont accomplis par des composants du routeur qui sont très différents.
— La responsabilité du routeur s'arrête une fois qu'il a transmis le paquet. Il ne peut pas indiquer au routeur suivant ce qu'il doit faire, et ne peut même pas connaitre la décision de celui-ci. C'est ce qu'on nomme le routage par étapes indépendantes ("*hop by hop*").

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8966.txt

Sur l'Internet, le protocole de routage standard est BGP (RFC 4271). Les annonces BGP ont la forme « je sais joindre `2001:db8:fa9::/48` et je le sais parce que l'AS 64500 me l'a dit et il le tenait de l'AS 65539 ». Mais, du fait du routage par étapes indépendantes, rien ne dit qu'un paquet envoyé au routeur qui a fait cette annonce ira bien à l'AS 64500 puis à l'AS 65539. Chaque AS (en pratique, un AS = un opérateur) est indépendant et a sa propre politique de routage. Par exemple, l'administratrice du routeur suivant a parfaitement pu configurer des routes statiques prioritaires, qui seront utilisées avant celles apprises via BGP. C'est le sens de la phrase « "*The data plane does not always follow the control plane*" ». « "*The data plane*" », c'est IP, c'est la transmission. « "*The control plane*" », c'est le protocole de routage, par exemple BGP.

L'étude de Koen van Hove <`https://labs.ripe.net/author/koen-van-hove/where-did-my-packet-`> citée plus haut est une illustration pratique de ce point (je vous en recommande vraiment la lecture). L'auteur travaille sur la validation de l'origine des routes (ROV, pour "*Route Origin Validation*"), via la RPKI <`https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html`> ("*Resource Public Key Infrastructure*"). Les titulaires de préfixes IP publient (et signent) des ROA ("*Route Origin Authorization*") qui indiquent quel AS peut être à l'origine d'une route (dans l'exemple plus haut, 65539 était l'origine). Les routeurs connectés à l'Internet peuvent utiliser ces ROA pour valider les annonces. Si on trouve un ROA correctement signé qui dit « `2001:db8:fa9::/48` doit avoir comme AS d'origine 65539 » et qu'une annonce « `2001:db8:fa9::/48` passe par moi et ça vient de l'AS 65500, qui en est l'origine », une telle annonce, invalide, peut être rejetée.

Est-ce que cela suffit à garantir la sécurité du routage ? Non, car, montre l'étude, même si on rejette cette annonce invalide, les paquets qu'on émet sont transmis à des AS différents et ceux-ci peuvent avoir d'autres règles et, par exemple, ne pas valider. Donc, le malheureux paquet destiné à `2001:db8:fa9:b3:551::12:a` sera peut-être finalement transmis au méchant AS 65500. C'est ennuyeux, mais c'est logique, chaque AS étant maitre de sa politique de routage.

Mais est-ce qu'on ne pourrait pas changer cela et « forcer » les AS à respecter des décisions prises par l'émetteur du paquet ? (Ce qu'on nomme le routage par la source.) Non, on ne peut pas, et le problème n'est pas technique (il existe plusieurs mécanismes pour représenter de telles décisions dans les paquets), mais d'ordre commercial et politique. En termes simples, les autres opérateurs font ce qu'ils veulent, et ils n'ont pas de raison de vous obéir. (Il faut se rappeler que l'Internet est une fédération de réseaux, pas un réseau unique.) Ils ont d'autant moins de raisons d'obéir à d'éventuelles consignes de l'émetteur que celles-ci permettraient des attaques contre la sécurité, par exemple en forçant le passage par un chemin qu'un attaquant sait moins contrôlé.

`https://www.bortzmeyer.org/control-plane-data-plane.html`