RFC 8212 : Default External BGP (EBGP) Route Propagation Behavior without Policies

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 juillet 2017

Date de publication du RFC : Juillet 2017

https://www.bortzmeyer.org/8212.html

Ce RFC est très court, mais concerne un problème fréquent sur l'Internet : les fuites de routes BGP. Traditionnellement, un routeur BGP acceptait par défaut toutes les routes, et annonçait par défaut à ses voisins toutes les routes qu'il connaissait. Il fallait une configuration explicite pour ne pas le faire. En cas d'erreur, ce comportement menait à des fuites (RFC 7908 [1]). Notre RFC normalise désormais le comportement inverse : un routeur BGP ne doit, par défaut, **rien** accepter et rien annoncer. Il faut qu'il soit configuré explicitement si on veut le faire.

Avec l'ancien comportement, la configuration de certains routeurs BGP, les plus imprudents, indiquait les pairs avec qui on échangeait de l'information, plus un certain nombre de routes qu'on n'envoyait **pas**. Si une erreur faisait qu'on recevait tout à coup des routes imprévues, on les acceptait, et on les renvoyait telles quelles, propageant la fuite (RFC 7908). Des cas fameux de fuites ne manquent pas (voir par exemple celle d'un opérateur malaisien <https://www.bortzmeyer.org/bgp-malaisie.html>). L'idée derrière ce comportement était d'assurer la connectivité du graphe de l'Internet. Aujourd'hui, on est plutôt plus sensibles aux risques de sécurité qu'à ceux de partitionnement du graphe, et les bonnes pratiques demandent depuis longtemps qu'on indique explicitement ce qu'on accepte et ce qu'on envoie. Voyez par exemple les recommandations de l'ANSSI <https://www.ssi.gouv.fr/guide/le-guide-des-bonnes-pratiques-de-configuration-de-bgp/>.

En pratique, ce très court RFC ajoute juste deux paragraphes à la norme BGP, le RFC 4271. Dans sa section 9.1, les paragraphe en question disent désormais qu'il ne doit pas y avoir du tout d'exportation ou d'importation de routes, par défaut. Notez donc que cela ne change pas le protocole BGP, juste le comportement local.

Du moment qu'on change le comportement par défaut, il va y avoir un problème de transition (et ce point a soulevé des discussions à l'IETF <https://www.ietf.org/mail-archive/web/idr/current/msg18093.html>). Si le logiciel du routeur s'adaptait au nouveau RFC, certains opérateurs seraient bien surpris que leurs routes ne soient tout coup plus annoncées. L'annexe A du RFC recommande une stratégie en deux temps :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7908.txt

— D'abord introduire une nouvelle option « BGP non sécurisé » qui serait à Vrai par défaut (mais que les opérateurs pourraient changer), ce qui garderait le comportement actuel mais avec un avertissement émis quelque part « attention, vous exportez des routes sans décision explicite »,
— Ensuite, dans la version suivante du logiciel, faire que cette option soit à Faux par défaut.

Les routeurs Cisco utilisant IOS-XR ont déjà ce comportement.

Et pour finir sur une note d'humour, à une réunion IETF (IETF 97 <https://www.ietf.org/meeting/97/index.html>), le projet qui a finalement mené à ce RFC était illustré…de photos de préservatifs. Pratiquez donc le BGP "*safe*", l'Internet vous remerciera.