# RFC 6441 : Time to Remove Filters for Previously Unallocated IPv4 /8s

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 novembre 2011. Dernière mise à jour le 5 janvier 2012

Date de publication du RFC : Novembre 2011

https://www.bortzmeyer.org/6441.html

---

Pour limiter certains risques de sécurité, des opérateurs réseaux filtraient en entrée de leur réseau les adresses IP non encore allouées (dites "*bogons*"). Les adresses IPv4 étant désormais totalement épuisées <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, cette pratique n'a plus lieu d'être et ce RFC demande donc que ces filtres soient démantelés.

L'idée était d'empêcher l'usage de ces préfixes IP non alloués. Ils représentaient des cibles tentantes, par exemple pour un spammeur qui voulait des adresses jetables et non traçables : on trouve un bloc non alloué, on l'annonce en BGP (puisqu'il n'est pas alloué, il n'y a pas de risque de collision), on envoie son spam et on arrête l'annonce BGP (voir les articles cités à la fin). Pour éviter cela, et d'autres attaques analogues, l'habitude s'est prise de filtrer les "*bogons*", ces préfixes non alloués. Certains opérateurs rejetaient les annonces BGP pour ces "*bogons*", d'autres bloquaient sur le pare-feu les paquets ayant une adresse source dans ces préfixes non alloués. Ces pratiques étaient largement documentées par exemple sur le site de référence sur les bogons <http://www.cymru.com/Bogons/>.

Cette pratique a toujours posé des problèmes, notamment celui de la « débogonisation ». Lorsqu'un préfixe qui n'était **pas** alloué le devient, il faut toute une gymnastique pour le retirer des filtres existants, sachant que beaucoup de ces filtres ne sont que rarement mis à jour <https://www.bortzmeyer.org/pas-de-listes-noires-statiques.html>. On voit ainsi des messages sur les listes de diffusion d'opérateurs réseaux avertissant de l'arrivée prochaine d'un nouveau préfixe et demandant qu'il soit supprimé des filtres. Voici deux exemples de ces annonces en 2004 <http://seclists.org/nanog/2004/Aug/59> et en 2005 <http://archive.apnic.net/mailing-lists/apops/archive/

2005/03/msg00010.html>. Pour permettre aux opérateurs de tester que tout va bien après cette suppression, les RIR mettent souvent un "*beacon*", un amer, dans le préfixe, une adresse IP qu'on peut pinguer pour tester, comme le recommande le RFC 5943 [1]. Tout ce travail faisait donc que la chasse aux "*bogons*" était contestée depuis longtemps <http://www.nanog.org/mailinglist/mailarchives/old_archive/2008-08/msg00050.html>.

À noter (section 2) que le terme de "*bogon*" a été défini dans le RFC 3871, qui recommande leur blocage. Ce même RFC 3871 décrit en détail le problème que posent les "*bogons*" et la raison de leur éradication. Le terme de martien, plus flou (il vient du RFC 1208), est appliqué à toutes sortes de paquets dont l'adresse source est anormale (dans le DNS, il a un autre sens, celui de paquet de réponse à une question qui n'a pas été posée).

La section 3 représente le cœur du RFC : elle formule la nouvelle règle. Celle-ci, tenant compte de l'épuisement des adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> est simple : tous les préfixes IPv4 sont désormais alloués ou réservés. Il ne faut donc filtrer que les réservés. Les autres peuvent désormais tous être une source légitime de trafic IP. La chasse aux "*bogons*" et les difficultés de la débogonisation faisant partie du folklore de l'Internet depuis très longtemps, c'est donc une page d'histoire qui se tourne. (Les adresses IPv6 sont, elles, loin d'être toutes allouées et ne sont donc pas concernées.)

La section 4 rappelle que l'autorité pour cette liste de préfixes réservés est le RFC 6890. On y trouve par exemple les adresses privées du RFC 1918 ou bien les adresses réservées à la documentation du RFC 5737. Les listes de "*bogons*" qu'on trouve sur le réseau, comme celle de TeamCymru <http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt> sont désormais réduites à ce groupe.

À noter que l'assertion « Tous les préfixes sont désormais alloués » ne vaut que pour les préfixes de longueur 8 (les « /8 ») distribués aux RIR. Certains peuvent filtrer à un niveau plus fin, en distinguant dans ces /8 les adresses que les RIR ont affectés de celles qui ne le sont pas encore. Comme le rappelle la section 3.2, cette pratique est risquée, les affectations par les RIR changeant vite. Le RFC demande donc que, si on a de tels filtres, ils soient changés au moins une fois par jour.

Pour en apprendre plus sur les "*bogons*", on peut regarder la bonne analyse faite par BGPmon <http://bgpmon.net/showbogons.php?inet=4>. On voit finalement peu d'annonces BGP de "*bogons*" (6 seulement en 2011), la plupart pour le préfixe 198.18.0.0/15 des mesures de performance (RFC 5735). Un bon résumé des "*bogons*" et de la débogonisation avait été fait par Dave Deitrich en 2005 <http://www.nanog.org/meetings/nanog33/presentations/deitrich.pdf>.

Quelques articles sur les trucs utilisés par des méchants (spammeurs, par exemple), en connexion avec les "*bogons*" :

- « "*Understanding the network-level behavior of spammers*" <http://www.cc.gatech.edu/~avr/publications/p396-ramachandran-sigcomm06.pdf> » par Anirudh Ramachandran (Georgia Tech) et Nick Feamster (Georgia Tech). Très bonne analyse technique des trucs réseaux utilisés par les spammeurs. C'était le première article à mettre en évidence le truc d'annoncer en BGP des préfixes "*bogons*", d'envoyer le spam, puis d'arrêter l'annonce BGP.
- « "*Practical BGP Security : Architecture, Techniques and Tools*" <http://www.renesys.com/tech/notes/WP_BGP_rev6.pdf> » (page 3)
- Le premier témoignage <http://www.merit.edu/mail.archives/nanog/2002-07/msg00257.html>, en 2002.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5943.txt