RFC 6319 : Issues Associated with Designating Additional Private IPv4 Address Space

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 juillet 2011

Date de publication du RFC : Juillet 2011

https://www.bortzmeyer.org/6319.html

Il y a bien longtemps que la pénurie d'adresses IPv4 est une réalité. Longtemps avant leur épuisement complet, ces adresses étaient très difficiles à obtenir, nécessitant un long processus bureaucratique (et le remplissage de nombreux documents), ou tout simplement l'abonnement à une offre qualifiée de « professionnelle » ou « "*gold*" » dont le seul intérêt était d'avoir quelques adresses de plus. Résultat, beaucoup d'organisations ont choisi des adresses IP privées et des systèmes de relais ou de traduction d'adresses pour se connecter à l'Internet. Si l'organisation ne grossit pas par la suite, tout va bien. Mais si elle devient plus importante et dépasse la taille permise par les plages d'adresses privées existantes, que se passe-t-il ?

La section 3 du RFC détaille les mécanismes utilisés pour se connecter à l'Internet malgré l'absence d'adresses IP publiques. La principale est sans doute le NAT (RFC 2993 [1] et RFC 3022). Le NAT a de multiples inconvénients, notamment pour les applications pair-à-pair, même si certaines techniques (comme ICE, RFC 8445) permettent de contourner partiellement le problème.

On peut emboîter plusieurs niveaux de NAT, mettant par exemple un traducteur dans la maison ou le bureau et un autre sur le réseau du FAI (on nomme souvent ce double-NAT **NAT444**). Si le FAI contrôle le CPE et donc les adresses IP qu'il alloue (cas de la Freebox par défaut, par exemple), cela peut marcher. C'est bien plus délicat si le CPE alloue les adresses qu'il veut car, alors, rien ne garantit qu'elles ne seront pas en conflit avec celles utilisées dans le réseau interne du FAI. Bref, le NAT444 ajoute de la complexité et des problèmes. Enfin, toute traduction d'adresses effectuée hors du réseau local de l'abonné soulève les problèmes liés au partage d'adresses que le RFC 6269 documente.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2993.txt

Le plus large bloc privé est le 10.0.0.0/8 (cf. RFC 1918). Il a parfois été suggéré d'allouer de nouveaux blocs pour agrandir l'espace privé mais ce projet a très peu de chances de se matérialiser désormais, vu l'épuisement des adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>. Ce bloc 10.0.0.0/8 comprend 16 777 216 adresses IP. Qui peut en consommer autant ? Comme le résume la section 2 de notre RFC, les gros opérateurs, par exemple un câblo-opérateur national (comme Comcast, non cité mais qui est effectivement dans ce cas), un opérateur de téléphonie mobile 3G, un gros fournisseur VPN, l'intranet d'une grosse entreprise, peuvent tous se trouver à l'étroit dans ce /8.

Quelles sont les possibilités une fois les adresses du RFC 1918 épuisées ? La section 4 les passe en revue. La première (section 4.1) est évidemment de passer enfin à IPv6, ce qui aurait dû être fait depuis longtemps. Le RFC note à juste titre que déployer IPv6 sur un réseau dont la taille est telle qu'il arrive à épuiser un /8 entier n'est pas une opération triviale. Elle va prendre du temps et c'est pour cela que ces opérateurs auraient dû commencer il y a des années. Si cela n'a pas été fait, l'opérateur peut se trouver dans le cas où les adresses du RFC 1918 sont épuisées et où il n'a matériellement pas le temps de déployer IPv6.

Notons que les adresses IPv6 utilisées ne sont pas forcément globales, on peut aussi déployer IPv6 avec des ULA (RFC 4193). Toutefois, celles-ci ne sont que pseudo-uniques donc, dans des cas comme celui du fournisseur de VPN, le risque de collision existe.

Bon, et pour les administrateurs réseaux qui, en 2011, n'ont toujours pas déployé IPv6, quelles solutions ? La section 4.2 liste les solutions purement v4. Obtenir de nouvelles adresses était la solution classique. Mais ajourd'hui, où les RIR qui ont encore des adresses IPv4 les épuisent vite et passent à la politique d'allocation finale <http://www.nro.net/rir-comparative-policy-overview/rir-comparative-policy-overview-2011-01#2-6>, cela ne parait pas très réaliste.

La seconde solution est d'acquérir des adresses IP d'autres organisations, comme l'avait fait Microsoft dans une opération fameuse <http://blog.internetgovernance.org/blog/_archives/2011/3/23/4778509.html>. Cette opération peut désormais être légale vis-à-vis des RIR comme le montre l'étude comparée de leurs politiques de transfert <http://www.nro.net/rir-comparative-policy-overview/rir-comparative-policy-overview-2011-01#1-3-2>. Les possibilités pratiques d'un tel transfert sont très incertaines. Y aura-t-il assez d'adresses sur ce « marché » ? Et à quel coût ? Personne ne le sait trop. Mais le RFC est pessimiste : on ne trouvera probablement pas de larges blocs d'adresses continus ainsi, il est plus probable qu'il n'y aura qu'une poussière de /24 et /23. (Le RFC discute aussi la possibilité de **locations** de tels blocs, encore pire car sans garantie sur ce qui arrivera au terme de la location.)

Il y a bien sûr une autre possibilité. Après tout, qui a dit qu'il fallait être honnête et respecter les règles de vie en société ? Comme le montre l'exemple d'innombrables hommes d'affaires, on réussit bien mieux en violant ces règles et en écrasant les autres. La section 4.2.2 du RFC est donc consacrée à la solution libérale : prendre ce qui vous intéresse sans se poser de questions, ici, utiliser des adresses IP non encore allouées, ou bien allouées à quelqu'un mais pas annoncées dans la table de routage mondiale. L'article de Duane Wessels <https://www.dns-oarc.net/files/dnsops-2008/Wessels-Unused-space.pdf> montre bien que l'espace non alloué est déjà utilisé. C'est évidemment très mal de faire cela : les rares blocs non encore alloués vont l'être bientôt (et cela fera une collision avec ceux du voleur, avec des conséquences imprévisibles), et ceux qui ne sont pas annoncés dans la table de routage publique le seront peut-être demain. Même si ce n'est pas le cas, la collision est toujours possible (cela dépend de la façon dont est configuré le réseau qui utilisait ces adresses mais, par exemple, les adresses internes fuient souvent, par exemple dans les en-têtes de courrier). La section 2.3 du RFC 3879 discute plus en détail ce

problème. Il y a aussi bien sûr des risques juridiques à jouer avec les adresses des autres. Cela peut expliquer pourquoi les voleurs d'adresses préfèrent utiliser des préfixes alloués à des opérateurs peu dangereux juridiquement, par exemple en Afrique <http://www.afnog.org/archives/2006-May/002117.html>.

Quelle solution pourrait-on développer ? La section 5 examine plusieurs possibilités : la première est d'agrandir le RFC 1918 en y ajoutant des préfixes actuellement marqués comme publics. Cela réduirait encore plus le stock d'adresses IPv4 disponibles. Plusieurs propositions avaient été faites de réserver, par exemple un /8 supplémentaire. Par exemple, le réseau 1.0.0.0/8 était tentant car son utilisation publique soulevait des problèmes <https://www.bortzmeyer.org/le-reseau-1.html>. Comme indiqué plus haut, il est clair <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/103_awkward.html> que cela se fait déjà, de manière officieuse. Aucune de ces propositions n'a été adoptée officiellement et leurs chances semblent désormais nulles. (Voir la discussion à NANOG <http://mailman.nanog.org/pipermail/nanog/2010-January/017451.html>.)

Il y a en effet pas mal de systèmes qui traitent les adresses du RFC 1918 de manière spéciale, et où ces adresses sont codées en dur. Il y a peu de chances de pouvoir mettre à jour tous ces systèmes. Déjà, "*dé-bogoniser*" <http://www.ripe.net/ripe/docs/ripe-351.html> les plages allouées est très difficile.

Dernière possibilité, réaffecter une plage réservée, 240.0.0.0/4, qui avait été mise de côté pour des usages futurs qui ne se sont jamais concrétisés. Le problème est que beaucoup de systèmes déployés traitent de manière spécifique ces adresses et qu'il y a peu de chance de pouvoir les changer tous. En pratique, elles seront donc largement inutilisables. Par exemple, sur Linux :

```
% sudo ifconfig eth1 240.0.0.1/24
SIOCSIFADDR: Invalid argument
```

(Mais ça marche sur FreeBSD et NetBSD). L'"*Internet-Draft*" draft-fuller-240space documente ce problème pour quelques systèmes.)

Bref, même si le RFC ne le rappelle pas, il n'y a pas vraiment d'autre solution que de migrer vers IPv6.