RFC 6879 : IPv6 Enterprise Network Renumbering Scenarios, Considerations and Methods

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 février 2013

Date de publication du RFC : Février 2013

https://www.bortzmeyer.org/6879.html

Ce RFC ne normalise pas un protocole mais a pour ambition de servir de guide lors de la **rénumérotation** d'un réseau IPv6. Pourquoi renuméroter ? Et comment ? Les administrateurs réseaux ont tout intérêt à le lire, et de préférence **avant** la renumérotation et même avant la mise en production du réseau, pour ne pas mettre dans l'architecture de celui-ci des éléments qui gêneront les renumérotations futures.

C'est le deuxième RFC du groupe de travail 6renum <http://tools.ietf.org/wg/6renum> qui planche sur les scénarios de renumérotation de réseaux IPv6, ainsi que sur les moyens de rendre ces renumérotations plus faciles. Ce RFC particulier se focalise sur le cas d'une organisation de taille significative : ni un SOHO, ni un opérateur réseau, un client de taille moyenne qui a IPv6 sur son réseau local, une ou plusieurs connexions à l'Internet et au moins un employé chargé d'administrer le réseau (cf. RFC 4057 [1]).

La seule façon d'être sûr de ne jamais renuméroter serait de n'utiliser que des adresses PI. Mais, comme le note le RFC 4116, cela aurait des conséquences quantitatives néfastes pour BGP. Donc, on part du principe que l'organisation aura à renuméroter un jour. Lisons les prérequis (RFC 4192 et RFC 5887) et allons-y.

Les machines reçoivent des adresses IP dynamiques (si elles ont des adresses statiques, le problème est plus compliqué, et c'est le domaine du RFC 6866). Pour cela, on utilise DHCP ou les annonces des routeurs (SLAAC).

Mais pourquoi renumérote-t-on ? Pourquoi s'embêter dans cette opération au lieu de se contenter de garder ses adresses actuelles ? La section 3 décrit plusieurs scénarios déclencheurs. Certains peuvent être externes, d'autres internes. Parmi les externes :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4057.txt

— Passage à un nouveau FAI qui a d'autres adresses pour ses clients. Idéalement, il y aura une période de recouvrement pendant laquelle l'organisation sera connectée par les deux FAI. Si ce n'est pas possible, il y aura un "*flag day*" où il faudra tout basculer d'un coup.
— Renumérotation chez le FAI, soit parce que lui-même a changé de fournisseur, soit parce qu'il a réorganisé son réseau.
— Ajout d'un deuxième FAI, pour une organisation qui n'en avait qu'un et qui souhaite davantage de redondance. Les anciennes adresses ne changent pas mais de nouvelles s'y ajoutent.

Et les causes internes ?

— Réorganisation de l'organisation : fusion, acquisition, ou autre événement "*business*" qui a des conséquences sur le réseau.
— Réorganisation technique du réseau.

La section 4 décrit ensuite les méthodes existantes pour faire ces renumérotations avec le moins de douleur possible. Parmi les mécanismes qui peuvent aider, il ne faut pas oublier la délégation de préfixe IP (RFC 8415 et RFC 6603), qui permet à un routeur d'informer d'autres routeurs sur les préfixes qu'ils vont devoir gérer (annoncer avec des RA, router, etc). Ainsi, on n'aura pas à reconfigurer tous les routeurs. Autre mécanisme important, l'utilisation de noms de domaine le plus souvent possible, car ils sont plus stables <https://www.bortzmeyer.org/pourquoi-le-dns.html> que les adresses IP. Par exemple, pour IPsec, nul besoin de configurer en utilisant des adresses, des noms peuvent être utilisés (RFC 5996), simplifiant ainsi beaucoup les futures renumérotations. (Pour les réseaux sans serveur DNS, le RFC rappelle l'existence de "*Multicast DNS*", RFC 6762.) De même, les applications devraient aussi utiliser des noms et pas des adresses. Configurer une application avec une adresse IP, c'est placer une bombe qui explosera lors de la prochaine renumérotation du réseau.

Mais les adresses IP peuvent se cacher en d'autres endroits, comme dans les ACL des pare-feux. Au minimum, ces configurations devraient être **paramétrisées** : on n'utilise l'adresse IP qu'une fois, pour lui donner un identificateur, puis on se sert de cet identificateur partout (des outils comme m4 ou cpp peuvent être utilisés pour cela). C'est le B A BA de l'administration réseaux, mais ce n'est pas toujours fait.

Pendant qu'on parle d'adresses IP qui traînent, il ne faut évidemment pas mettre dans ses configurations des adresses IP d'autres sites. Sinon, lorsqu'ils renuméroteront, ils ne penseront sans doute pas à vous prévenir...

Un truc plus exotique est l'utilisation d'ULA, des adresses IP locales (RFC 4193). L'idée est de tout numéroter avec les ULA et d'effectuer une traduction d'adresses ou un relayage dans les routeurs de sortie. Ainsi, la renumérotation n'impacte que ces routeurs. Les ULA sont donc une sorte de substitut aux adresses PI.

Continuons avec les techniques utilisées sur le réseau local : comment les adresses IP arrivent-elles aux machines terminales ? En IPv6, il y a deux solutions, SLAAC (RFC 4862) et DHCP (RFC 8415). Ce RFC ne tranche pas entre les deux : du point de vue de la renumérotation, ils ont à peu près les mêmes possibilités. (DHCP a une option, `RECONFIGURE` qui permet, si le client DHCP la gère, de faire des renumérotations imprévues.)

Et le DNS ? Un petit site ne gère pas forcément ses propres serveurs DNS. Leur reconfiguration pourra nécessiter une coordination avec l'hébergeur DNS. Ce que le RFC recommande, c'est de ne pas le faire manuellement. Le fichier de zone édité avec vi et contenant les adresses IP de toutes les machines de l'organisation, c'est un mécanisme archaïque, et, en 2013, on doit normalement mieux faire : soit les données DNS sont dérivées automatiquement d'une base de données de machines (cela n'a pas besoin d'être une usine à gaz, cela peut être un simple script Perl/Python/Ruby), soit les machines (ou les serveurs DHCP) mettent à jour le DNS automatiquement avec les mises à jour dynamiques (RFC 3007).

Une fois qu'on a fait le tour de son réseau et des techniques utilisées, il faut se préparer, et **planifier soigneusement**. D'abord, diminuer la durée de vie des annonces d'adresses pour que la transition soit la plus courte possible et que les vieilles adresses ne trainent pas dans les caches. Avec l'autoconfiguration sans état (SLAAC), on ne peut pas réduire la durée de vie des annonces à moins de deux heures, il faudra faire avec. D'autre part, cette diminution va évidemment augmenter le trafic et il ne faut donc pas la faire des semaines à l'avance. Une telle durée de vie est stockée dans les enregistrements DNS (qu'il faut donc ajuster <https://www.bortzmeyer.org/changement-adresse-et-dns.html>), mais aussi dans les annonces indiquant le résolveur DNS à utiliser (RFC 8106 pour SLAAC et RFC 3646 pour DHCP, où il faut réduire la durée du bail, on ne peut pas réduire seulement la durée de vie de l'option DNS). À noter que les applications qui maintiennent des connexions sur de longues périodes (SSH, par exemple), n'ont pas de mécanisme propre pour gérer la renumérotation. Il faudra faire une déconnexion/reconnexion.

Bref, anticiper et planifier sont des nécessités.