RFC 7934 : Host address availability recommendations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 juillet 2016

Date de publication du RFC : Juillet 2016

https://www.bortzmeyer.org/7934.html

Combien d'adresses IPv6 faut-il permettre à une machine qui se connecte ? « Une » est évidemment le minimum mais est-ce suffisant ? Non, explique ce RFC qui recommande aux opérateurs et FAI de permettre aux machines de s'allouer autant d'adresses IPv6 qu'elles en ont besoin.

IPv6 est juste une nouvelle version d'IP. Ce n'est pas un nouveau protocole. Néanmoins, la taille bien plus importante de son espace d'adressage a des conséquences qui sont souvent oubliées par les administrateurs de réseaux. Ainsi, il est fréquent que la gestion des réseaux soit faite en limitant chaque machine à une seule adresse IPv6. En IPv4, il n'y a évidemment pas d'autre choix possible, en raison de la pénurie d'adresses publiques <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>. Mais en IPv6, il n'y a aucune raison de se limiter, et beaucoup de raisons de permettre davantage d'adresses. Bref, bien qu'IPv6 ne soit pas complètement nouveau, cela ne veut pas dire que les bonnes pratiques IPv4 s'appliquent directement à IPv6.

Il est banal de faire remarquer que les adresses IPv6 sont, en pratique, illimitées. Un simple lien réseau (numéroté avec un préfixe de 64 bits) offre quatre milliards de fois plus d'adresses que tout l'Internet IPv4 ! Il n'est donc pas du tout obligatoire de rationner. IPv6 est conçu depuis le début (section 2 de notre RFC) avec l'idée que chaque machine (et même chaque interface réseau de chaque machine) aura plusieurs adresses IP (par exemple, une adresse locale au lien, une adresse publique stable, et au moins une adresse temporaire du RFC 8981 [1]). Et toutes les mises en œuvre d'IPv6 existantes gèrent cela correctement.

Mais quel est l'intérêt de permettre plusieurs adresses ? La section 3 de ce RFC répond à la question :

— Cela permet d'utiliser les adresses temporaires citées plus haut, pour améliorer la protection de la vie privée (RFC 8981).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8981.txt

— Cela simplifie l'adressage si la machine a plusieurs processeurs séparés (par exemple, dans les mobiles, le processeur « normal » et celui de bande de base), surtout s'ils partagent une connexion (cas du I-WLAN).
— Cela facilite le partage de connexion ("*tethering*"), la machine partageuse ayant alors plusieurs adresses à prêter. (Voir les RFC 6459 et RFC 7278 pour le cas de 3GPP.)
— Cela facilite l'hébergement de machines virtuelles (ou de containers) sur chaque machine, chacune pouvant avoir sa propre adresse publique.
— Cela simplifie le déploiement de mécanismes de co-existence IPv4¡-¿IPv6 comme 464XLAT (RFC 6877).
— Cela permet des solutions fondées sur la séparation de l'identificateur et du localisateur <https://www.bortzmeyer.org/separation-identificateur-localisateur.html> comme l'ILA (décrite dans le document draft-herbert-nvo3-ila).
— Cela permettra des nouveaux concepts d'adressage, inimaginables en IPv4, comme le fait de donner une adresse IP à chaque application (cf. TARP, « "*Transient Addressing for Related Processes : Improved Firewalling by Using IPv6 and Multiple Addresses per Host* " <https://www.usenix.org/legacy/publications/library/proceedings/sec01/gleitz.html>» par Gleitz et Bellovin).

Et quels sont les problèmes si on ne fait **pas** ce que recommande ce RFC ? La section 4 les liste. Évidemment, si ajouter des adresses IP est complètement impossible, on est fichus. Et si la connexion au réseau permet d'ajouter des adresses IPv6 mais que cela nécessite une action explicite (par exemple via l'interface Web de l'hébergeur) ? Cela entraine :

— Délai supplémentaire avant de déployer un nouveau service sur la machine,
— Risque qu'un problème survienne au cours de l'opération (tiens, c'était juste le jour où l'interface Web a un problème),
— Complexité car il faut gérer une action en plus (pour laquelle il n'y a pas de mécanisme normalisé.)

Pourquoi les opérateurs restreindraient-ils ainsi l'obtention d'adresses IPv6 supplémentaires ? Par pur sadisme ? Non, il peut y avoir des raisons objectives :

— Limites du matériel (TCAM limité en taille),
— Souhait de garder une cohérence avec le style IPv4 (une adresse IP par machine, qui peut servir d'identificateur simple),
— Volonté de faire payer par tous les moyens possibles, y compris par adresse IPv6 supplémentaire.

Avec le temps, il faut espérer que les limites matérielles reculent et que la raison "*business*" (faire payer) soit rejetée par les utilisateurs (ils peuvent la contourner, par exemple en faisant du NAT, ce qui serait un comble pour IPv6).

À propos de NAT, est-ce que c'est une bonne stratégie pour résoudre le problème d'un opérateur qui ne laisserait pas assez d'adresses IPv6 à ses clients (section 5 du RFC) ? Les problèmes et limites du NAT sont bien connus (RFC 2993). Les applications sont plus complexes (car leurs programmeurs doivent déployer des trésors d'ingéniosité pour contourner le NAT), la gestion de la durée de vie des correspondances entre adresses dans le routeur NAT est pénible (quel intervalle entre les paquets d'entretien de la connexion <http://www.ietf.org/proceedings/88/slides/slides-88-tsvarea-10.pdf> ?), etc. C'est pour cela que le NAT sur IPv6 est très déconseillé (RFC 5902).

Ce n'est pas faute de mises en œuvre (le NAT66 est dans Linux depuis 2012...), un vendeur de virtualisation l'a aussi développé, précisement pour contourner ce manque d'adresses IPv6 allouées, mais il n'est pas souhaitable que cela continue. Le but d'IPv6 est d'avoir une vraie connectivité de bout en bout, qui ne soit limitée que par des choix délibérés (Alice ne veut plus parler à Bob), pas par des limites techniques inutiles.

Et si l'opérateur du réseau où se connecte la machine a été convaincu par ce RFC, et veut permettre à ses clients d'allouer les multiples adresses IPv6 dont ils ont besoin, quels sont les mécanismes techniques dont il dispose pour cela ? La section 6 les couvre :

— Naturellement, le moyen le plus simple est d'utiliser SLAAC (RFC 4862) : les routeurs annoncent les préfixes IP publics et chaque machine forme des adresses à volonté en utilisant ces préfixes. Comme SLAAC impose de détecter les éventuelles collisions, avant d'utiliser une adresse (RFC 4862, section 5.4), le risque que deux machines se retrouvent avec la même adresse est nul. C'est évidemment encore mieux si chaque machine a son propre préfixe /64, elle n'a même plus à tester les collisions.
— On peut utiliser DHCP (RFC 8415). Le protocole permet de continuer à réclamer des adresses.
— Et il y a aussi la délégation de préfixes IPv6 via DHCP (RFC 8415). Cela permet d'envoyer un /64 à chaque client, dont il fera ce qu'il voudra.

Un tableau à la fin de la section 6 résume les forces et faiblesses de chaque solution.

Au fait, combien d'adresses exactement peut-on s'attendre à voir sur une seule machine ? La section 7 se lance dans la spéculation. Les adresses « vie privée » du RFC 8981 peuvent consommer jusqu'à huit adresses en même temps. Avec une demi-douzaine de services réseau, et une demi-douzaine de machines virtuelles (ou de containers) hébergés, avoir vingt adresses sur une seule machine peut donc être raisonnable. Mais, bien sûr, il est difficile de prévoir les usages futurs et, en pratique, ce sera peut-être bien plus.

Allez, c'est presque fini, la section 8 du RFC synthétise les recommendations officielles :

— Il est recommandé que les hébergeurs et FAI qui déploient IPv6 permettent aux client d'avoir plusieurs adresses IP par machine.
— Il est également recommandé qu'il n'y ait pas de limite stricte au nombre d'adresses utilisables.
— Il est recommandé que cette allocation d'adresses supplémentaires puisse se faire sans requête explicite à l'hébergeur ou FAI.

Ces recommandations, si elles sont suivies, auront quelques conséquences pratiques (section 9). Par exemple, elles ne permettent pas de garder trace de quelles adresses sont utilisées par quelle machine. (Alors qu'avec une demande d'allocation explicite, par exemple par le biais d'une nouvelle interface virtuelle, comme c'est le cas actuellement chez Gandi, ce suivi est possible.) C'est ennuyeux si on veut remonter d'une adresse IP qui pose un problème (par exemple parce qu'il a téléchargé Les tortues Ninja) à son propriétaire. Une solution de remplacement est de superviser le réseau et de relever les réponses NDP, permettant ainsi de se constituer une base de la relation entre les adresses IP et les adresses MAC. Le logiciel NDPMon permet de faire cela. (On peut aussi interroger les commutateurs en SNMP, pour avoir un résultat analogue.) Les auteurs du RFC notent que tous leurs employeurs ont déjà un tel système en place, et ils citent plusieurs gros campus universitaires qui font de même, ce qui montre le caractère réaliste de la proposition.

Puisqu'on parle de sécurité, il faut noter que de ne pas permettre officiellement aux machines de s'attribuer des adresses IP supplémentaires ne signifiera pas qu'elles ne le feront pas. Si on n'a pas de sécurité dans la couche 2 (cf. RFC 7039), les machines peuvent toujours se configurer ce qu'elles veulent. En outre, si le mode d'allocation est DHCP, les efforts actuels pour améliorer la vie privée des utilisateurs de DHCP (RFC 7844) vont de toute façon diminuer l'intérêt de DHCP pour la sécurité.

Autre problème pratique pour les administrateurs réseau, les limites du matériel. Si un commutateur connecte mille machines, sa table de correspondance adresses IP ¡-¿ adresses MAC aura mille entrées. Si chaque machine s'alloue dix adresses, cette table devra stocker dix mille entrées. Le commutateur a-t-il cette capacité ? S'il ne l'a pas, on risque des pertes de connectivité. Certes, le matériel va évoluer. Mais il existe une autre solution, suggérée par notre RFC : utiliser un préfixe IP par machine. Ainsi, le commutateur n'aura à gérer qu'une seule entrée par machine, quel que soit son nombre d'adresses. Évidemment, cela consommera davantage d'adresses IPv6, et cela compliquera un peu la gestion des adresses. Cette proposition est donc légèrement plus sujette à controverse que la principale (permettre plusieurs adresses par machine) qui, elle, est largement reconnue comme justifiée.