RFC 8273 : Unique IPv6 Prefix Per Host

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 décembre 2017

Date de publication du RFC : Décembre 2017

https://www.bortzmeyer.org/8273.html

Ce court RFC explique comment (et pourquoi) attribuer un préfixe IPv6 unique à chaque machine, même quand le média réseau où elle est connectée est partagé avec d'autres machines.

Ce RFC s'adresse aux gens qui gèrent un grand réseau de couche 2, partagé par de nombreux abonnés. Un exemple est celui d'un serveur dédié connecté à un Ethernet partagé avec les serveurs d'autres clients. Un autre exemple est celui d'une connexion WiFi dans un congrès ou un café. Dans les deux cas, la pratique sans doute la plus courante aujourd'hui est de donner une seule adresse IPv6 à la machine (ou, ce qui revient au même, un préfixe de 128 bits). C'est cette pratique que veut changer ce RFC. Le but est de mieux isoler les clients les uns des autres, et de bien pouvoir gérer les abonnements et leur utilisation. (Justement le problème de Comcast, dont un des auteurs du RFC est un employé, cf. section 1.) Les clients ne se connaissent en effet pas les autres et il est important que les actions d'un client ne puissent pas trop affecter les autres (et qu'on puisse attribuer les actions à un client précis, pour le cas où ces actions soient illégales). En outre, certaines options d'abonnement sont « par client » (section 3, qui cite par exemple le contrôle parental, ou la qualité de service, qui peut être plus faible pour ceux qui ne paient pas le tarif « gold ».)

Si chaque client a un préfixe IPv6 à lui (au lieu d'une seule adresse IP), toute communication entre clients passera forcément par le routeur géré par l'opérateur, qui pourra ainsi mieux savoir ce qui se passe, et le contrôler. (Les lecteurs férus de routage ont noté que le client, s'il est administrateur de sa machine, peut toujours changer les tables de routage, mais cela n'affectera que le trafic aller, le retour passera toujours par le routeur. De toute façon, je soupçonne que la technique décrite dans ce RFC ne marche que si le réseau donne un coup de main, pour isoler les participants.)

Le RFC affirme que cela protègera contre des attaques <https://www.bortzmeyer.org/hacking-ipv6.html> comme l'épuisement de cache "*Neighbor Discovery*", les redirections malveillantes faites avec

ICMP ou les RAcailles (RFC 6104 [1]). Cela éviterait de devoir déployer des contre-mesures comme le "*RA Guard*" (RFC 6105). Là aussi, il me semble personnellement que ça n'est complètement vrai que si l'attaquant n'est pas administrateur sur sa machine. Ou alors, il faut que le réseau ne soit pas complètement partagé, qu'il y ait un mécanisme de compartimentage.

Les mécanismes décrits ici supposent que la machine du client utilise SLAAC (RFC 4862) pour obtenir une adresse IP. Cette obtention peut aussi passer par DHCP (RFC 8415) mais c'est plus rare, relativement peu de clients étant capable de demander une adresse en DHCP (RFC 7934).

La section 4 du RFC décrit comment le client obtient ce préfixe. Il va envoyer un message RS ("*Router Solicitation*", voir le RFC 4861, section 3) et écouter les réponses, qui lui diront son adresse IP mais aussi d'autres informations comme les résolveurs DNS à utiliser (voir RFC 8106). Pas de changement côté client, donc (ce qui aurait rendu ce mécanisme difficile à déployer). Par contre, côté « serveur », il y a de légers changements. Le routeur qui reçoit les RS et génère des RA ("*Router Advertisement*"), qu'ils aient été sollicités ou pas, va devoir les envoyer uniquement à une machine (puisque chaque client a un préfixe différent : il ne faut donc pas diffuser bêtement). Comme le RFC 4861 (sections 6.2.4 et 6.2.6) impose que l'adresse IP de destination soit `ff02::1` (« tous les nœuds IPv6 »), l'astuce est d'utiliser comme adresse MAC, non pas l'adresse "*multicast*" habituelle, mais une adresse "*unicast*" (RFC 6085). Ainsi, chaque client ne recevra que son préfixe.

Ce RA contient le préfixe que l'opérateur alloue à ce client particulier. Les options du RA (RFC 4861, section 4.2) sont :

— Bit M à zéro (ce qui veut dire « pas d'adresse via DHCP »),
— Bit O à un (ce qui veut dire « d'autres informations sont disponibles par DHCP, par exemple le serveur NTP à utiliser »),
— Bit A du préfixe (RFC 4861, section 4.6.2) mis à un (ce qui veut dire « tu es autorisé à te configurer une adresse dans ce préfixe »),
— Bit L du préfixe (RFC 4861, section 4.6.2) mis à zéro (ce qui veut dire « ce préfixe n'est pas forcément sur le lien où tu te trouves, ne suppose rien, sois gentil, passe par le routeur »).

Le bit A étant mis à un, la machine qui a obtenu le préfixe peut s'attribuer une adresse IP à l'intérieur de ce préfixe, , avec SLAAC, comme indiqué dans le RFC 4862. Elle doit suivre la procédure DAD ("*Duplicate Address Detection*", RFC 4862, section 5.4) pour vérifier que l'adresse IP en question n'est pas déjà utilisée.

Voilà, l'essentiel de ce RFC était là. La section 5 concerne quelques détails pratiques, par exemple ce que peut faire la machine client si elle héberge plusieurs machines virtuelles ou containers (en gros, elle alloue leurs adresses en utilisant le préfixe reçu).

Ce mécanisme de préfixe IP spécifique à chaque client de l'opérateur n'est pas sans poser des questions liées à la vie privée, comme l'explique la section 7 du RFC. (Rappelez-vous la section 1, qui disait qu'un des buts de cette technique était de satisfaire aux « obligations légales », autrement dit de pouvoir suivre à la trace ses utilisateurs.) Bien sûr, la machine cliente peut utiliser le système du RFC 8981, mais, ici, il aurait peu d'impact. Même avec un identificateur d'interface temporaire et imprévisible, le préfixe resterait, et identifierait parfaitement le client. Le RFC mentionne (mais sans l'exiger) qu'on peut limiter les dégâts en changeant le préfixe de temps en temps.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6104.txt`