RFC 8064 : Recommendation on Stable IPv6 Interface Identifiers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 février 2017

Date de publication du RFC : Février 2017

https://www.bortzmeyer.org/8064.html

Ce RFC parle de vie privée mais il est très court, car il se contente de changer une règle, la nouvelle étant déjà largement acceptée. Désormais, si une machine IPv6 configure son adresse par le système SLAAC, et que cette adresse doit être stable dans le temps, désormais, donc, la méthode recommandée est celle du RFC 7217[1] et non plus celle, mauvaise pour la vie privée, d'utiliser l'adresse MAC. (Si l'adresse n'a pas besoin d'être stable, aucun changement, la méthode recommandée reste celle du RFC 8981, les adresses temporaires.)

Que veut dire SLAAC, au fait ? Ce mécanisme de configuration d'une adresse IPv6 est normalisé dans le RFC 4862. L'idée est que la machine écoute sur le réseau les annonces faites par les routeurs, apprenant ainsi le·s préfixe·s IP du réseau. Elle ajoute ensuite à ce préfixe un terme, l'identificateur d'interface (IID, cf. RFC 4291), formant ainsi une adresse IPv6 mondiale, et unique (si l'IID est bien choisi). La méthode originelle était de dériver l'IID de l'adresse MAC. Celle-ci est en effet unique et, en prime, son utilisation présente certains avantages (compression des en-têtes du RFC 6775, par exemple). Mais s'en servir soulève plein de problèmes de sécurité et notamment de vie privée : traçabilité des utilisateurs dans le temps, et dans l'espace (si la machine se déplace, elle change de préfixe mais garde le même identificateur d'interface), facilitation du balayage des adresses dans le réseau, etc (cf. RFC 7721). D'une manière générale, réutiliser des identificateurs d'un autre « monde » est une fausse bonne idée, souvent dangereuse en matière de vie privée. Voilà pourquoi ce RFC dit clairement que, désormais, il est fortement déconseillé d'utiliser les adresses MAC. (Plusieurs mises en œuvre d'IPv6, comme celles de Microsoft, avaient déjà cessé, avant même que ce RFC ne soit publié.)

Et ce RFC 7217 qu'il faut désormais suivre, il dit quoi ? Il propose de fabriquer l'identificateur d'interface en condensat une concaténation du préfixe et de diverses valeurs stables. Si on change de réseau,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7217.txt

on a une nouvelle adresse (on ne peut donc pas suivre à la trace une machine mobile). Mais, si on reste sur le même réseau, l'adresse est stable.

La section 1 de notre RFC rappelle aussi la différence entre les adresses stables et les autres. Toutes les adresses IP n'ont pas besoin d'être stables. La solution la meilleure pour la vie privée est certainement celle du RFC 8981, des adresses temporaires, non stables (pour de telles adresses, on peut aussi utiliser le système des adresses MAC si elles changent souvent par exemple avec macchanger <https://www.it-connect.fr/changer-dadresse-mac-sous-linux-avec-macchanger/>). Toutefois, dans certains cas, les adresses stables sont souhaitables : l'administration réseaux est plus simple, les journaux sont plus faciles à lire, on peut mettre des ACL, on peut avoir des connexions TCP de longue durée, etc. Et, bien sûr, si la machine est un serveur, ses adresses doivent être stables. Il y a donc une place pour une solution différente de celle du RFC 8981, afin de fournir des adresses stables. C'est seulement pour ces adresses stables que notre RFC recommande désormais la solution du RFC 7217.

La nouvelle règle figure donc en section 3 de notre RFC : lorsqu'une machine veut utiliser SLAAC **et** avoir des adresses stables, qui ne changent pas dans le temps, tant que la machine reste sur le même réseau, alors, dans ce cas et seulement dans ce cas, la méthode à utiliser est celle du RFC 7217. L'ancienne méthode (qu'on trouve par exemple dans le RFC 2464) d'ajouter le préfixe à l'adresse MAC ne doit plus être utilisée.

Notez donc bien que ce RFC ne s'adresse pas à toutes les machines IPv6. Ainsi, si vous configurez vos serveurs (qui ont clairement besoin d'une adresse stable) à la main, avec des adresses en "*leet*" comme `2001:db8::bad:dcaf`, ce RFC 8064 ne vous concerne **pas** (puisqu'il n'y a pas de SLAAC).

Les RFC comme le RFC 4944, RFC 6282, RFC 6775 ou RFC 7428 devront donc être remplacés par des documents tenant compte de la nouvelle règles. (Cf. RFC 8065.)

Aujourd'hui, il semble que les dernières versions de Windows, MacOS, iOS et Android mettent déjà en œuvre la nouvelle règle.