RFC 7136 : Significance of IPv6 Interface Identifiers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 février 2014

Date de publication du RFC : Février 2014

https://www.bortzmeyer.org/7136.html

Les adresses IPv6 sont souvent composées en utilisant un truc nommé « "*interface identifiers*" » (identifiant d'interface réseau). Ces identifiants peuvent être formés, par exemple, en utilisant les adresses MAC, en utilisant des bits ayant un sens particulier dans les normes IEEE. Résultat, dans le passé, certains ont attribué à des bits de l'identifiant d'interface une signification qu'ils n'avaient pas. Ce nouveau RFC clarifie la question : les identifiants d'interface doivent être considérés comme **opaques** et il ne faut pas tirer de conclusion du fait que tel ou tel bit est mis.

Un exemple typique de construction d'adresse IPv6 est donné dans la section 2.5 du RFC 4291[1]. L'adresse IPv6 de 128 bits est formée en concaténant un préfixe avec un "*interface identifier*". Ce dernier est censé être unique sur le lien où la machine est connectée. Cet objectif peut être atteint en prenant l'adresse MAC de la machine et en la transformant en utilisant le format "*Modified EUI-64*". Dans ce format, le bit U (pour "*universal*") est inversé, 1 signifiant que l'identifiant EUI-64 est unique mondialement, 0 qu'il ne l'est pas (ainsi, les adresses fabriquées manuellement comme `2001:db8:33::1` ont un identifiant d'interface où le bit U est à zéro). Un autre bit est spécial, le G, qui indique s'il s'agit d'une adresse de groupe ou de machine individuelle. Ces deux bits **perdent** leur signification dès qu'ils sont mis dans une adresse IPv6, c'est le point important de ce RFC.

Un exemple ? Si la machine a l'adresse MAC `b8:27:eb:ba:90:94`, son identifiant d'interface va être `ba27:ebff:feba:9094` (suivant le tutoriel sur le format EUI-48 <http://standards.ieee.org/develop/regauth/tut/eui48.pdf>, on ajoute `ff:fe` au milieu, l'adresse Ethernet ne faisant que 48 bits, et on inverse le bit U, transformant le `b8` en `ba`).

Comme indiqué, il y a bien d'autres façons de fabriquer un identifiant d'interface (notre nouveau RFC 7136 utilise le sigle « IID » qui n'apparait pas dans le RFC 4291 original). Si celle utilisant une

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4291.txt`

adresse MAC est la plus souvent présentée dans les tutoriels IPv6, elle n'est pas la seule et on a des identifiants d'interface formés à partir d'un processus cryptographique (RFC 3972 ou RFC 5535), générés aléatoirement et utilisés temporairement, pour protéger la vie privée (RFC 8981), ou fabriqués à partir des adresses IPv4 (RFC 5214). Sans compter la méthode manuelle de choisir l'identifiant d'interface à volonté, en en faisant un nombre significatif (`::53` pour un serveur DNS) ou rigolo (`::dead:beef`). Et de nouvelles méthodes apparaissent de temps en temps. Pour chacune de ces méthodes, la norme stipule la valeur que doivent prendre les bits U et G. Par exemple, le RFC 3972 les met à zéro tous les deux et le RFC 8981 (section 3.3) met U à zéro et ne dit rien pour G. Les identifiants formés à partir de ces méthodes ont donc des valeurs très variables pour ces deux bits. En fait, l'identifiant d'interface ne fait même pas forcément 64 bits, comme illustré par le RFC 6164, qui le réduit à un seul bit pour les liaisons point à point entre deux routeurs !

Bref, l'affirmation du RFC 4291 (section 2.5.1) comme quoi le bit U signifie réellement que l'adresse est unique ou pas n'est **plus** vraie. Et, même si on n'avait gardé qu'une seule méthode de création des identifiants d'interface, celle fondée sur l'adresse MAC, les exemples n'ont pas manqué de constructeurs livrant plusieurs cartes Ethernet avec la même adresse (et c'est encore plus vrai sur les machines virtuelles). Simon Castaing m'a fourni une bonne liste :

— Chez Asus <http://support-org.asus.com/faq/asus-faq.aspx?type=6&no=03E7011E-0ACD-A
SLanguage=en-us>,
— Chez Homeseer <http://board.homeseer.com/showthread.php?p=987050>,
— Chez Archos <http://forum.archosfans.com/viewtopic.php?f=47&t=32132>,
— Chez D-link <http://community.spiceworks.com/topic/278156-d-link-dap-2553-aps-with-
— Chez Cisco <http://www.cisco.com/en/US/ts/fn/misc/7.html>,
— Et chez d'autres... <http://www.dslreports.com/faq/11873>

On ne peut donc pas espérer que les identifiants d'interface soient mondialement uniques. **On ne peut pas compter sur le bit U.**

Même des protocoles qui, au début, voulaient pouvoir compter sur l'unicité de l'identifiant d'interface ont fait marche arrière. Par exemple ILNP (RFC 6741) prévoit que les 64 derniers bits de l'adresse soient uniques pour un localisateur donné. Mais il a quand même un système de détection de duplication, car utiliser EUI-64 pour ces 64 derniers bits ne suffit pas, comme on l'a vu.

Ah, et puis on a beaucoup parlé du bit U et nettement moins du bit G. Les adresses IPv6 formées à partir de l'adresse Ethernet ne devraient pas avoir le bit G à 1 (on n'utilise pas les adresses de groupe) mais cela ne veut pas dire que ce bit ait une signification particulière, dans une adresse IPv6. Comme pour le bit U, une fois l'adresse fabriquée, on ne peut plus l'analyser. Si on sait, par un moyen ou un autre, qu'une adresse IPv6 a été formée à partir d'une adresse MAC, on peut recalculer l'adresse MAC, ce qui peut avoir des avantages opérationnels, lors du débogage d'un réseau. Mais, si on ne le sait pas, il vaut mieux s'abstenir : ce n'est pas parce que l'identifiant d'interface a le bit U à 1 et le bit G à 0 qu'il a forcément été engendré à partir d'une adresse MAC.

Parfois, le mécanisme de génération d'identifiants d'interface par une adresse MAC est présenté comme garantissant l'unicité, sans autre effort. Comme on l'a vu, ce n'est pas le cas, même si tout le monde utilisait ce mécanisme. C'est pour cela qu'IPv6 a un système de détection des duplications d'adresses, le DAD ("*Duplicate Address Detection*", RFC 4862). Comme ce système est obligatoire, on n'a pas besoin de trouver des méthodes de génération d'adresse qui assurent l'unicité : il suffit de laisser le DAD trouver les collisions et, dans ce cas, de réessayer. Par exemple, la section 3.4 du RFC 8981 dit qu'en cas de collision, on refait tourner l'algorithme (de génération aléatoire de l'identifiant) et on obtient donc un nouvel identifiant aléatoire.

Les sections 3 et 5 du RFC sont la partie normative de ce document : les bits U et G peuvent être utilisés librement par les méthodes de génération des identifiants d'interface (et donc des adresses IPv6)

et, lorsqu'on lit une adresse IPv6 sans connaître le mécanisme de génération, il ne faut pas croire qu'on peut déduire quelque chose de la valeur de ces deux bits. Dans certains cas (identifiants temporaires aléatoires du RFC 8981), c'est même un facteur de sécurité (donner le moins d'information possible, cf. section 6).

Cela nécessite de modifier le RFC 4291 : la régle comme quoi les identifiants d'interface (à part ceux commençant par trois bits mis à zéro) doivent être formés à partir d'une adresse MAC est officiellement retirée, et l'allusion aux bénéfices du bit U pour détecter un identifiant d'interface mondialement unique également. Comme le note notre RFC, cela ne devrait gêner aucune implémentation, cette réforme alignant simplement la norme sur la pratique constatée.