RFC 8925 : IPv6-Only-Preferred Option for DHCPv4

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 octobre 2020

Date de publication du RFC : Octobre 2020

https://www.bortzmeyer.org/8925.html

Si une machine a IPv6 et est ravie de n'utiliser que ce protocole, pas la peine pour un serveur DHCP de lui envoyer une des rares adresses IPv4 restantes. Ce nouveau RFC décrit une option de DHCP-IPv4 qui permet au client de dire au serveur « je n'ai pas vraiment besoin d'IPv4 donc, s'il y a IPv6 sur ce réseau, tu peux garder les adresses IPv4 pour les nécessiteux ».

Idéalement, l'administrateur réseaux qui configure un nouveau réseau voudrait le faire en IPv6 seulement, ce qui simplifierait son travail. Mais, en pratique, c'est difficile (le RFC 6586[1] décrit une telle configuration). En effet, beaucoup de machines ne sont pas encore entrées dans le XXIe siècle, et ne gèrent qu'IPv4 ou, plus exactement, ont besoin d'IPv4 pour au moins certaines fonctions (comme des versions de Windows qui avaient IPv6 mais ne pouvaient parler à leur résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> qu'au-dessus d'IPv4). Il faut donc se résigner à gérer IPv4 pour ces machines anciennes. Mais, vu la pénurie d'adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, il est également souhaitable de ne pas allouer d'adresses IPv4 aux machines qui n'en ont pas besoin.

La solution la plus courante à l'heure actuelle est de mettre les machines antédiluviennes et les machines modernes dans des réseaux séparés (VLAN ou SSID différents, par exemple, comme c'est fait aux réunions IETF ou RIPE), le réseau pour les ancêtres étant le seul à avoir un serveur DHCPv4 (RFC 2131). Cela a plusieurs inconvénients :

— Cela complique le réseau et son administration,
— Le risque d'erreur est élevé (utilisateur sélectionnant le mauvais SSID dans le menu des réseaux Wi-Fi accessibles, par exemple).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6586.txt

L'idéal serait de n'avoir qu'un réseau, accueillant aussi bien des machines IPv6 que des machines IPv4, sans que les machines IPv6 n'obtiennent d'adresse IPv4, dont elles n'ont pas besoin. On ne peut pas demander aux utilisateurs de débrayer complètement IPv4, car les machines mobiles peuvent en avoir besoin sur des réseaux purement IPv4 (ce qui existe encore). La machine IPv6 ne sachant pas, a priori, si le réseau où elle se connecte est seulement IPv4, seulement IPv6 ou accepte les deux, elle va donc, logiquement, demander une adresse IPv4 en DHCP, et bloquer ainsi une précieuse adresse IPv4. Retarder cette demande pour voir si IPv6 ne suffirait pas se traduirait par un délai peu acceptable lorsque le réseau n'a pas IPv6.

Notre RFC résout ce problème en créant une nouvelle option pour les requêtes et réponses DHCP v4 : dans la requête, cette option indique que le client n'a pas absolument besoin d'une adresse IPv4, qu'il peut se passer de ce vieux protocole, si le réseau a de l'IPv6 bien configuré et, dans la réponse, cette option indique que le réseau fonctionne bien en « IPv6 seulement ». Et comment fait-on si on veut joindre un service IPv4 depuis un tel réseau ? Il existe des techniques pour cela, la plus répandue étant le NAT64 du RFC 6146, et la réponse du serveur DHCP indique également qu'une de ces techniques est présente.

La section 1.2 précise quelques termes importants pour comprendre les choix à effectuer pour le client et pour le serveur DHCP :

— Capable de faire de l'IPv6 seule ("*IPv6-only capable host*") : une machine terminale <https://www.bortzmeyer.org/terminal-host.html> qui peut se débrouiller sans problème sans adresse IPv4,
— Nécessite IPv4 ("*IPv4-requiring host*") : le contraire,
— IPv4 à la demande ("*IPv4-on-demand*") : le scénario, rendu possible par ce RFC, où le même réseau accueille des machines capables de faire de l'IPv6 seul, et des machines qui nécessitent IPv4 ; ce réseau se nomme « Essentiellement IPv6 » ("*IPv6-mostly network*"), et fournit NAT64 (RFC 6146) ou une technique équivalente,
— En mode seulement IPv6 ("*IPv6-only mode*") : état d'une machine capable de faire de l'IPv6 seule et qui n'a pas reçu d'adresse IPv4,
— Réseau seulement en IPv6 ("*IPv6-only network*") : un réseau qui ne fournit pas du tout d'IPv4 et ne peut donc pas accueillir les machines qui nécessitent IPv4 (c'est un tel réseau qui sert de base à l'expérience du RFC 6586),
— Notez que le cas d'un réseau qui non seulement serait seulement en IPv6 mais en outre ne fournirait pas de technique comme celle de NAT64 (RFC 6146) n'apparait pas dans le RFC. Un tel réseau ne permettrait pas aux machines terminales de joindre les services qui sont restées en IPv4 seulement comme MicrosoftHub ou l'Élysée <http://www.elysee.fr/>.

La section 2 du RFC résume ensuite les bonnes raisons qu'il y a pour signaler au réseau, via l'option DHCP, qu'on se débrouille très bien avec IPv6 seul :

— Il semble logique que la nouvelle option, qui veut dire « je n'ai pas réellement besoin d'IPv4 » soit envoyée via le protocole qui sert à demander les adresses IPv4,
— Tout le monde a déjà DHCP v4 et, surtout, utiliser le protocole existant n'introduit pas de nouvelles vulnérabilités (permettre à un nouveau protocole de couper IPv4 sur les machines terminales serait un risque de sécurité important),
— Comme il faut ajouter explicitement l'option aux requêtes et aux réponses, IPv4 ne sera coupé que si le client et le serveur DHCP sont tous les deux d'accord pour cela,
— Ce système n'ajoute aucun retard à la configuration via DHCP, le client qui envoie l'option alors que le réseau ne permet pas IPv6 seul, aura son adresse IPv4 aussi vite qu'avant (pas d'aller-retours de négociation),
— DHCP permet des résultats qui dépendent du client, donc, sur un même réseau, le serveur DHCP pourra économiser les adresses IPv4 en en n'envoyant pas aux machines qui peuvent s'en passer, tout en continuant à en distribuer aux autres.

La section 3 du RFC présente l'option elle-même. Elle contient le code 108 ("*IPv6-only Preferred*"), enregistré à l'IANA <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xml#options> (cf. section 5), la taille de l'option (toujours quatre, mais précisée car c'est l'encodage habituel des options DHCP, cf. RFC 2132) et la valeur, qui est, dans la réponse, le nombre de secondes que le client peut mémoriser cette information, avant de redemander au serveur DHCP.

Le logiciel client DHCP doit donc offrir un moyen à son administrateur pour activer « je me débrouille très bien en IPv6 », et cela doit être par interface réseau. Dans ce cas, le client DHCP doit envoyer l'option décrite dans notre RFC. La décision d'activer le mode « IPv6 seul » peut aussi être prise automatiquement par le système d'exploitation, par exemple parce qu'il détecte que 464XLAT (RFC 6877) fonctionne. De même, des objets connectés qui ne parlent qu'à des services accessibles en IPv6 pourraient être livrés avec l'option « IPv6 seul » déjà activée.

Outre le côté « je suis un bon citoyen, je ne gaspille pas des ressources rares » qu'il y a à ne pas demander d'adresse IPv4, cette option permet de couper un protocole réseau inutile, diminuant la surface d'attaque de la machine.

Côté serveur DHCP, il faut un moyen de configurer, pour chaque réseau, si on accepte l'option « IPv6 me suffit ». Si elle est activée, le serveur, lorsqu'il recevra cette option dans une requête (et uniquement dans ce cas), la mettra dans sa réponse, et n'attribuera pas d'adresse IPv4. On voit donc que les vieux clients DHCP, qui ne connaissent pas cette option et ne l'inclueront donc pas dans leurs requêtes, ne verront pas de changement, ils continueront à avoir des adresses IPv4 comme avant (s'il en reste…).

A priori (section 4 du RFC), l'administrateurice du serveur DHCP ne va pas activer cette option si son réseau ne fournit pas un mécanisme permettant aux machines purement IPv6 de joindre des services purement IPv4 (par exemple le mécanisme NAT64 du RFC 6146). En effet, on ne peut pas s'attendre, à court terme, à ce que tous les services Internet soient accessibles en IPv6. Activer l'option « IPv6 seul » sans avoir un mécanisme de traduction comme NAT64 n'est réaliste que sur des réseaux non-connectés à l'Internet public.

Un petit mot sur la sécurité, juste pour rappeler que DHCP n'est pas vraiment sécurisé et que l'option « v6 seul » a pu être mise, retirée ou modifiée suite aux actions d'un attaquant. Cela n'a rien de spécifique à cette option, c'est un problème général de DHCP, contre lequel il faut déployer des protections comme le "*DHCP snooping*".

Au moment de la sortie du RFC, je ne connaissais pas encore de mise en œuvre de cette option. Mais elle n'est pas trop dure à ajouter, elle n'a rien de très nouveau ou d'extraordinaire et, en 2022, Android et iOS l'envoyaient, comme le montre une étude faite pendant une réunion RIPE <https://labs.ripe.net/author/ondrej_caletka_1/deploying-ipv6-mostly-access-networks/>.

Un dernier mot : le RFC 2563 prévoyait une option pour couper l'auto-configuration des adresses IPv4. Elle peut être utilisée en même temps que l'option de notre RFC, qu'elle complète assez bien.