RFC 7078 : Distributing Address Selection Policy using DHCPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 janvier 2014

Date de publication du RFC : Janvier 2014

https://www.bortzmeyer.org/7078.html

Lorqu'une machine IPv6 a plusieurs adresses IP, laquelle choisir pour une connexion sortante ? Le RFC 6724 [1] définit une politique par défaut, consistant en règles du genre « préférer les adresses temporaires du RFC 8981, pour des raisons de préservation de la vie privée ». Comme ce sont seulement des règles par défaut, on peut les changer. Un des mécanismes est que le serveur DHCP indique à ses clients d'autres règles et ce RFC décrit une nouvelle option DHCP permettant en effet de changer de politique de sélection d'adresse IP source. L'administrateur qui gère le serveur DHCP pourra alors fixer d'autres règles.

En effet, il y a peu de chances que la politique par défaut définie dans le RFC 6724 convienne à **tout** le monde. Le RFC 5221 demandait donc qu'on puisse changer de politique et ne pas être tenu éternellement par celle du RFC 6724. À noter que l'obéissance au serveur DHCP, quoique recommandée, n'est pas obligatoire : au bout du compte, l'administrateur de la machine contrôle la politique de sélection d'adresses IP source.

La syntaxe de la nouvelle option DHCP figure en section 2. L'option a le numéro 84 (dans le registre DHCP <https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xml#dhcpv6-parameters-2>), et comprend deux booléens, A et P, suivis par une suite d'options de numéro 85 (rappelez-vous que DHCPv6 permet de mettre des options dans d'autres options). Chaque option de cette suite vaut pour une ligne dans la table des politiques (une ligne dans le fichier `/etc/gai.conf` si vous êtes sur Linux), donc une règle, et comprend :

— Une étiquette (cf. RFC 6724, section 2.1),
— Une précédence,
— La longueur du préfixe,

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6724.txt`

— Le préfixe des adresses IP.
Des exemples figurent en annexe A, en utilisant les scénarios du RFC 5220.

Le booléen A signifie « "*Automatic row addition flag*" » et veut dire, lorsqu'il est mis à 0, que la règle en question peut poser des problèmes et ne devrait pas être ajoutée automatiquement à la politique. Normalement, il est à 1. Le booléen P signifie « "*Privacy preference flag*" » et exprime la préférence donnée aux adresses temporaires (RFC 8981) pour préserver la vie privée. Il est normalement à 1, le choix le plus sûr (on sélectionne de préférence les adresses temporaires comme adresses sources).

En recevant ces options, le client DHCP met à jour sa propre table. C'est le comportement par défaut recommandé, avec une option pour débrayer cette mise à jour, et garder sa propre table originale.

Cette politique de sélection de l'adresse IP source est globale à la machine. Même si elle a plusieurs interfaces réseau, la table est commune à toutes. Une des raisons de ce choix est que l'interface de sortie est souvent choisie **après** l'adresse IP source et en fonction de celle-ci.

Quelques détails utiles pour le programmeur figurent en section 4 : l'étiquette est représentée dans le protocole par un entier non signé mais, en fait, la seule opération sur les étiquettes est la comparaison, et l'ordre n'a aucune signification. Le client peut donc la convertir dans n'importe quel type.

Il n'y a pas de limite de taille dans ce RFC et on pourrait donc en théorie envisager des tables énormes. En pratique, la taille maximale d'un datagramme UDP met une limite aux alentours de 3 000 règles et, de toute façon, la plupart des implémentations auront des problèmes bien avant (par exemple, parce qu'elles n'accepteront pas le datagramme UDP fragmenté).

Enfin, un peu de sécurité (section 5) : DHCP n'offrant aucune protection, un méchant peut facilement se faire passer pour le serveur DHCP officiel et envoyer des tables délirantes, menant à sélectionner une mauvaise adresse. Notez quand même qu'un tel serveur DHCP méchant peut faire bien d'autre chose que de d'envoyer de mauvaises tables. Les protections posisbles sont l'utilisation de techniques cryptographiques comme IPsec (ce que quasiment personne ne fait) ou bien le contrôle des messages DHCP par le commutateur ("*DHCP snooping*").