RFC 6106 : IPv6 Router Advertisement Options for DNS Configuration

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 novembre 2010. Dernière mise à jour le 22 décembre 2010

Date de publication du RFC : Novembre 2010

https://www.bortzmeyer.org/6106.html

Il existe deux méthodes pour configurer une machine IPv6 automatiquement, DHCP (RFC 8415[1]) et RA ("*Router Advertisement*", RFC 4862). Pendant longtemps, l'avantage de la première était de pouvoir indiquer d'autres informations que l'adresse IP, comme par exemple les adresses des serveurs DNS. Le RFC 5006 avait apporté cette possibilité à la configuration par RA. Mais son statut n'était qu'expérimental. Désormais, voici la même option mais sous la forme d'une vraie norme. (Ce RFC a depuis été à son tour remplacé par le RFC 8106.)

Si on gère un gros réseau, avec de nombreuses machines dont certaines, portables, vont et viennent, s'assurer que toutes ces machines ont les adresses IP des serveurs de noms à utiliser n'est pas trivial (section 1 du RFC). On ne peut évidemment pas utiliser le DNS, cela serait tenter de voler en tirant sur les lacets de ses chaussures. Et configurer à la main les adresses sur chaque machine (par exemple, sur Unix, en les écrivant dans le fichier `/etc/hosts`) est bien trop difficile à maintenir. Se passer du DNS est hors de question. Pour les machines bi-protocoles (IPv4 et IPv6), une solution possible était d'utiliser un serveur de noms en v4. Mais pour une solution purement v6 ?

La solution la plus populaire actuellement est DHCP (RFC 8415 et RFC 3646). Son principal inconvénient est qu'elle est **à état** : le serveur DHCP doit se souvenir des **baux** qu'il a attribué. Sur un gros réseau local, le nombre de requêtes à traiter, chacune nécessitant une écriture dans une base de données, peut devenir très lourd.

Une autre solution est **sans état** et repose sur une nouveauté d'IPv6, les RA ("*Router Advertisements*", cette méthode est aussi appelée ND, pour "*Neighbor Discovery*", les RA en étant un cas particulier),

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8415.txt`

décrits dans le RFC 4862. Ce sont des messages envoyés à intervalles réguliers par les routeurs et qui informent les machines non-routeuses des caractéristiques essentielles du réseau, comme le préfixe utilisé (par exemple `2001:DB8:BEEF:42::/64`). Le routeur diffuse ses messages et n'a pas besoin d'écrire quoi que ce soit sur son disque, ni de faire des traitements compliqués lors d'une sollicitation, il répond toujours par le même message RA.

Ces RA peuvent diffuser diverses informations, par le biais d'un système d'options. Le principe de notre RFC est donc d'utiliser ces RA pour transporter l'information sur les serveurs de noms récursifs utilisables sur le réseau local, via des nouvelles options notamment celle nommée RDNSS (le numéro 25 lui a été affecté par l'IANA).

La section 1.1 du RFC rappelle qu'il existe plusieurs choix, notre RFC 6106 n'étant qu'une possibilité parmi d'autres. Le RFC 4339 contient une discussion plus détaillée de ce problème du choix d'une méthode de configuration des serveurs de noms (notons qu'il existe d'autres méthodes comme l'"*anycast*" avec une adresse « bien connue »). La section 1.2 décrit ce qui se passe lorsque plusieurs méthodes (par exemple DHCP et RA) sont utilisées en même temps.

La méthode RA décrite dans notre RFC repose sur deux nouvelles options, RDNSS, déjà citée, et DNSSL, qui n'existait pas dans le RFC précédent (section 4). La première permet de publier les adresses des serveurs de noms, la seconde une liste de domaine à utiliser pour compléter les noms courts (formés d'un seul composant).

La première option, RDNSS, de numéro 25, est décrite en section 5.1. Elle indique une liste d'adresse IPv6 que le client RA mettra dans sa liste locale de serveurs de noms interrogeables.

La seconde option, DNSSL, de numéro 31, est en section 5.2 (les deux options sont enregistrées dans le registre IANA `<https://www.iana.org/assignments/icmpv6-parameters>`, cf. section 8). Elle publie une liste de domaines, typiquement ceux qui, sur une machine Unix, se retrouveront dans l'option `search` de `/etc/resolv.conf`.

Sur Linux, le démon rdnssd `<http://rdnssd.linkfanel.net/>` permet de recevoir ces RA et de modifier la configuration DNS. Pour FreeBSD, on peut consulter une discussion sur leur liste `<http://lists.freebsd.org/pipermail/freebsd-net/2009-June/022248.html>`. Les CPE de Free, les Freebox, émettent de telles options dans leurs RA (apparemment, à la date de publication de notre RFC 6106, uniquement des RDNSS). Voici ce qu'affiche Wireshark :

```
...
Ethernet II, Src: FreeboxS_c3:83:23 (00:07:cb:c3:83:23),
              Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
...
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
...
    ICMPv6 Option (Recursive DNS Server)
        Type: Recursive DNS Server (25)
        Length: 40
        Reserved
        Lifetime: 600
        Recursive DNS Servers: 2a01:e00::2 (2a01:e00::2)
        Recursive DNS Servers: 2a01:e00::1 (2a01:e00::1)
```

et les serveurs DNS annoncés répondent correctement. (Vous pouvez récupérer le paquet entier sur pcapr.net <http://www.pcapr.net/view/bortzmeyer+pcapr/2009/10/6/9/v6-fb.pcap.html>.)

Autre mises en œuvre de ces options, dans radvd, qui a déjà l'option RDNSS et bientôt (en décembre 2010) la nouvelle DNSSL <http://lists.litech.org/pipermail/radvd-devel-l/2010-December/000507.html> (ainsi que pour les logiciels auxiliaires <http://lists.litech.org/pipermail/radvd-devel-l/2010-December/000528.html>). Quant à Wireshark, le code a déjà été écrit <https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5476> mais n'est pas encore intégré.

La section 6 de notre RFC donne des conseils aux programmeurs qui voudraient mettre en œuvre ce document. Par exemple, sur un système d'exploitation où le client RA tourne dans le noyau (pour configurer les adresses IP) et où la configuration DNS est dans l'espace utilisateur, il faut prévoir un mécanisme de communication, par exemple un démon qui interroge le noyau régulièrement pour savoir s'il doit mettre à jour la configuration DNS.

RA pose divers problèmes de sécurité, tout comme DHCP, d'ailleurs. Le problème de ces techniques est qu'elles sont conçues pour faciliter la vue de l'utilisateur et de l'administrateur réseau et que « faciliter la vie » implique en général de ne pas avoir de fonctions de sécurité difficiles à configurer. La section 7 traite de ce problème, par exemple du risque de se retrouver avec l'adresse d'un serveur DNS méchant qui vous redirigerait n'importe Dieu sait où (les RA ne sont pas authentifiés). Ce risque n'a rien de spécifique aux options DNS, toute la technique RA est vulnérable (par exemple, avec un faux "*Neighbor Advertisement*"). Donc, notre RFC n'apporte pas de risque nouveau. Si on considère cette faiblesse de sécurité comme insupportable, la section 7.2 recommande d'utiliser SEND (RFC 3971).

À noter que l'annexe A résume les changements depuis le RFC 5006. Passage sur le chemin des normes, ajout de la nouvelle option DNSSL ("*DNS Search List*") plus diverses précisions sur le protocole. Depuis, le RFC 8106 a été publié et c'est lui qui est désormais la norme pour cette option.

Merci à Alexis La Goutte pour ses informations.