RFC 6059 : Simple procedures for Detecting Network Attachment in IPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 décembre 2010

Date de publication du RFC : Novembre 2010

https://www.bortzmeyer.org/6059.html

Un engin mobile connecté à l'Internet change souvent de réseau. Il se déplace, s'attache à un autre réseau, perd le contact avec la borne WiFi, retrouve du 3G un peu plus loin et, chaque fois, il peut se retrouver sur un réseau différent, avec des paramètres différents mais aussi parfois sur un réseau déjà visité, auquel cas il peut peut-être réutiliser tout de suite des paramètres mémorisés. Il est donc nécessaire de pouvoir déterminer rapidement à quel réseau on est attaché, et si les paramètres précédents sont toujours valables. C'est le but de la méthode exposée dans ce RFC, équivalent IPv6 du RFC 4436 [1].

Le but, comme exposé par la section 2.1, est donc de rendre la mobilité plus agréable, sans avoir à changer les routeurs, sans dégrader le service existant (par exemple, le temps de réponse ne doit jamais être pire qu'avec les méthodes actuelles), en acceptant des faux négatifs (un réseau déjà visité n'est pas reconnu) mais jamais les faux positifs (un réseau nouveau est pris à tort pour un réseau connu).

A-t-on besoin d'un nouveau protocole pour cela ? Après tout (section 2.2), il existe déjà la procédure standard de "*Neighbor Discovery*" du RFC 4861. Le nouveau "*Simple DNA*" ne sera pas une amélioration de ND dans tous les cas mais il aidera dans certains, notamment ceux où l'engin se déplace régulièrement parmi un ensemble de quelques réseaux. Si le réseau est complètement nouveau, "*Simple DNA*" n'apportera rien (mais n'aura pas d'inconvénients). De même, "*Simple DNA*" n'aidera pas pour le cas où le réseau est statiquement configuré, il ne marche qu'avec les adresses allouées par "*Router Advertisement*" (RFC 4862) ou DHCP (RFC 8415).

"*Simple DNA*" va fonctionner en interrogeant les routeurs connus pour voir s'ils sont toujours là. Une autre approche aurait été possible, en interrogeant les couches basses (section 2.3) pour voir si

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4436.txt

l'attachement au réseau n'avait pas changé (par exemple, même si le RFC ne le mentionne pas, en WiFi, on peut regarder le SSID et l'adresse MAC de la borne). Mais cette méthode aurait été moins générale.

Donc, comment fonctionne ce "*Simple DNA*" (section 2.4) ? Le fait d'être connecté à un réseau est signalé par les couches basses ("*Link Up*" en Ethernet ou WiFi). Reste à trouver à quel réseau on est connecté. "*Simple DNA*" utilise à la fois des paquets "*unicast*" "*Neighbor Solicitation*" (RFC 4861, section 7.2.2) et des paquets "*multicast*" "*Router Solicitation*" (RFC 4861, section 6.3.7) pour tester les routeurs dont il se souvient. Si aucun ne répond, "*Simple DNA*" passe aux procédures normales, "*Stateless address autoconfiguration*" ou bien DHCP. Le fait de se servir de "*Neighbor Solicitation*" permettra d'obtenir une réponse plus rapide (les routeurs ne répondent pas instantanément aux "*Router Solicitation*").

Bien sûr, dans la réalité, tout ne se passe pas aussi bien. "*Simple DNA*" dépend de plusieurs choses, résumées par la section 2.5 : le fait que le couple {adresse MAC du routeur, adresse IP du routeur locale au lien} soit unique et le fait que les machines sont prévenues lorsque le lien physique devient fonctionnel (RFC 4957 et section 5.4 de notre RFC).

La section 4 note ensuite que la mise en œuvre complète de l'algorithme nécessite une nouvelle structure de données, la SDAT ("*Simple DNA Address Table*"). Elle va contenir la liste des routeurs déjà vus et est donc composée d'entrées indexées par le couple {adresse MAC du routeur, adresse IP du routeur locale au lien}. Elle contiendra les informations suivantes : l'information a-t-elle été obtenue par DHCP ou bien autoconfiguration sans état, adresse IP de la machine, durée de vie, préfixe utilisé, l'information a-t-elle été sécurisée par SEND, ainsi que des informations spécifiques à DHCP. Ainsi, si "*Simple DNA*" trouve qu'un réseau a déjà été visité, il a toutes les informations sous la main pour configurer immédiatement l'interface réseau.

La marche exacte à suivre de la part de la machine qui se trouve connectée est détaillée en section 5 (avec une représentation en pseudo-code en section 6). La section 5.5 décrit ainsi l'envoi des paquets de sondage (un "*Router Solicitation*" pour voir si un routeur répond, des "*Neighbor Solicitations*" pour tester les routeurs dont on se souvient, six au maximum à la fois, pour ne pas surcharger le réseau). C'est là qu'est précisé le fait que ces paquets de sondage devraient être envoyés en parallèle, pour diminuer le temps total de l'opération (et garantir ainsi que "*Simple DNA*" ne prendra jamais plus de temps qu'une méthode classique).

Le traitement des réponses est en section 5.7 : il est important que la machine vérifie que les adresses MAC correspondent bien à ce dont elle se souvient. Sinon, cela signifie que le réseau est en fait différent et qu'il faut abandonner "*Simple DNA*" pour revenir à la méthode habituelle. Naturellement, si on reçoit un "*Router Advertisement*" normal, il faut l'utiliser, quelles que soient les informations stockées dans la table SDAT.

Bien plus embêtant est le cas où les informations recueillies sont incohérentes (section 5.7.3). Par exemple, si le test d'un routeur avec le "*Neighbor Solicitation*" ne coïncide pas avec les "*Router Advertisement*" reçus. Dans ce cas, le RFC décide qu'il faut croire le "*Router Advertisement*" (sauf si SEND est utilisé). Si le conflit est entre des tests par "*Neighbor Solicitation*" et DHCP, il faut faire confiance à DHCP.

Autres recommandations, ne pas effectuer de tests de duplication d'adresses (RFC 4862, section 5.4) si on retourne à un réseau connu et ne pas insister éternellement si les "*Neighbor Solicitations*" ne ramènent pas de réponses du tout : ce cas veut sans doute dire simplement que le réseau ne marche pas.

Ah, et si on tient à faire de l'IPv4 ? La section 8 rappelle que IPv4 a aussi un système équivalent (RFC 4436) mais qui suit un algorithme très différent (IPv4 n'a pas de "*Router Advertisement*", par exemple).

Enfin, comme avec toutes les techniques de configuration automatiques ou semi-automatiques, il y a un sérieux problème de sécurité (section 10). Les messages reçus peuvent être des faux. À part utiliser SEND (RFC 3971), il n'y a pas de solution miracle, et la seule recommandation de notre RFC est de veiller à ce que des informations non sécurisées par SEND ne remplacent pas des informations sécurisées. Autrement dit, si on avait visité un réseau qui avait un routeur SEND et, qu'en revenant sur un réseau qui semble le même, on reçoit des "*Router Advertisement*" non-SEND, il ne faut pas les utiliser. (J'ai d'ailleurs bien l'impression que, si on suit strictement les règles du RFC, on ne pourra jamais se connecter à un réseau qui **avait** SEND mais a choisi ensuite de l'abandonner, sauf à vider la SDAT à la main.)

Reléguée en annexe A, une dernière recommandation. Bien que le DNA de IPv4 puisse se combiner avec des adresses manuellement configurées, les problèmes que cela a soulevé (notamment pour les réseaux qui utilisaient à la fois des adresses manuelles et des automatiques) font que DNA IPv6 déconseille formellement son utilisation dans les cas où l'adresse a été fixée à la main par l'administrateur système.