

RFC 7216 : Location Information Server (LIS) Discovery using IP address and Reverse DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 avril 2014

Date de publication du RFC : Avril 2014

<https://www.bortzmeyer.org/7216.html>

Normalement, pour trouver le serveur de localisation (LIS) qui lui permettra d'en connaître plus sur sa position physique, et donc d'accéder à des services fondés sur cette position, une machine utilise les techniques du RFC 5986¹. Mais celles-ci nécessitent une coopération de la part de la "box", coopération qui a l'air difficile à obtenir. Ce nouveau RFC propose donc une autre solution, fondée entièrement sur le DNS.

Un LIS est normalement un service du système d'accès à l'Internet (et on en change donc quand on change de réseau). Il connaît la topologie du réseau et pourra donc répondre aux requêtes des machines clients lorsqu'elles voudront connaître leur place dans le monde (en utilisant le protocole du RFC 5985). Cette localisation est utilisée, par exemple, dans les services d'urgence (imaginez un appel VoIP au 112 où l'appelant n'a pas le temps de donner sa position : il faut que son logiciel le fasse pour lui.) Reste à trouver ce LIS. Le RFC 5986 proposait une méthode simple, une option DHCP (comme il en existe pour trouver les serveurs DNS ou NTP). Mais cela suppose que le serveur DHCP soit mis à jour pour suivre le RFC 5986 et, apparemment, peu le sont. Déployer une nouvelle option DHCP sur toutes les "boxes" du monde prend un temps fou (convaincre les développeurs, modifier le code, mettre à jour les millions de "boxes" existantes ou bien attendre leur remplacement...)

Donc, il vaut mieux une méthode qui ne dépende pas de la "box". C'est ce que propose notre RFC. Le principe est de partir de l'adresse IP de la machine, de la transformer en un nom de domaine et d'utiliser ensuite ce nom pour des requêtes DDDS, comme c'était le cas avec le RFC 5986, qui partait d'un nom de domaine reçu en DHCP puis le soumettait à DDDS.

Bon, mais le lecteur attentif a dû noter un piège : la machine typique du réseau local typique du M. Michu typique a une adresse IPv4 privée. Ce n'est pas très utile pour faire des requêtes dans le DNS public. Il va donc falloir que la machine commence par utiliser un protocole comme STUN pour trouver son adresse IP publique. Donc, le principe de notre RFC 7216 est :

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc5986.txt>

- D'abord, on essaie la requête DHCP du RFC 5986. Si elle réussit, c'est bon, sinon, on continue avec la nouvelle méthode,
- On cherche la ou les adresses IP publiques de la machine,
- On les convertit en noms de domaine dans les zones comme `in-addr.arpa`. Par exemple, `192.0.2.143` devient `143.2.0.192.in-addr.arpa`.
- On passe alors à la découverte DDDS de la section 4 du RFC 5986. En gros, on fait une requête pour le type NAPTR, service `LIS:HELD`, sur le nom de domaine obtenu à l'étape précédente.
- Si ça ne donne rien, on raccourcit le nom de domaine (on retire le composant le plus à gauche) et on réessaie la requête NAPTR.

Pour l'étape « trouver l'adresse IP publique de la machine », on a vu que la méthode suggérée est STUN (RFC 8489), avec un message de type *"Binding Request"* et une réponse dans le paramètre `XOR-MAPPED-ADDRESS`. Mais une machine a aussi le droit de se servir de PCP (RFC 6887, sections 10.1 et 11.4, la réponse à un *"MAP request"* va contenir l'adresse publique) ou UPnP pour cela. Notez que, parfois, l'adresse ainsi obtenue peut être à son tour une adresse privée (RFC 1918) et que cela n'empêche pas la procédure de découverte du LIS de fonctionner (à condition que le résolveur DNS utilisé sache rediriger les requêtes vers un serveur local qui fait autorité pour les `in-addr.arpa` correspondants).

Quant au raccourcissement du nom de domaine, il est prévu pour tenir compte du fait qu'il n'y aura pas forcément un enregistrement NAPTR pour tous les noms de domaine correspondant à une adresse publique. Parfois, le LIS servira une population plus large (en IPv4, un /24, voire même un /16) et on n'aura de NAPTR que pour le nom raccourci. Ainsi, avec l'adresse IP publique citée plus haut, si on ne trouve pas de NAPTR pour `143.2.0.192.in-addr.arpa`, on essaiera avec `2.0.192.in-addr.arpa` puis `0.192.in-addr.arpa`. Pour IPv6, notre RFC recommande de raccourcir le nom de domaine pour correspondre successivement à un /64, un /56, un /48 ou un /32.

Comme toujours avec la géolocalisation, il y a des questions de vie privée délicates (section 5, et voir aussi le RFC 6280). Ce RFC décrit un mécanisme pour permettre à une machine de trouver son LIS, et donc finalement sa localisation. Ceci n'est pas un risque pour la vie privée. Par contre, une fois cette information obtenue, il faudra faire attention à qui on l'envoie.

Il y a apparemment plusieurs mises en œuvre de ce mécanisme alternatif de découverte du LIS mais je n'ai pas de liste sous la main.