

RFC 7043 : Resource Records for EUI-48 and EUI-64 Addresses in the DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2013

Date de publication du RFC : Octobre 2013

<https://www.bortzmeyer.org/7043.html>

Tout le monde connaît les identifiants EUI-48 et EUI-64 même si ce n'est pas sous ce nom là. Normalisés par l'IEEE, ils servent notamment d'adresses Ethernet. Désormais, on peut les mettre dans le DNS, en utilisant les nouveaux types créés par ce RFC. Attention : pour des raisons liées à la protection de la vie privée, il n'est pas prévu que ces enregistrements DNS EUI48 et EUI64 se retrouvent dans le DNS public, seulement dans des zones locales (un point qui a soulevé des controverses).

Donc, d'abord, le type EUI48 (section 3). Il a le numéro 108 dans le registre IANA <<https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>>. En binaire, c'est simplement un groupe de six octets. Sous la forme texte (par exemple dans un fichier de zone), c'est six groupes (séparés par des tirets) de chacun deux chiffres hexadécimaux, par exemple :

```
host.example. 86400 IN EUI48 00-00-5e-00-53-2a
```

(Notez que l'adresse MAC utilise le préfixe IANA et les valeurs réservées pour les exemples par le RFC 7042¹.)

C'est quasiment pareil pour le type EUI64. Numéro 109, huit octets à la suite en binaire, huit groupes de chiffres hexa en mode texte :

```
host.example. 86400 IN EUI64 00-00-5e-ef-10-00-00-2a
```

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc7042.txt>

Mais à quoi cela sert, ces adresses Ethernet dans le DNS? La section 5 répond à la question en décrivant le cas d'usage qui avait motivé ce RFC. Au Canada, les FAI utilisant le câble utilisent DHCP pour fournir des adresses IP aux abonnés. Souvent, cela passe par un revendeur qui ne contrôle pas tout le réseau. Le revendeur connaît l'adresse EUI-48 de son client mais pas l'adresse IP allouée. La correspondance entre l'adresse IP et l'adresse MAC, a décidé le régulateur, doit être publiée dans le DNS (document « *Implementation of IP Address Tracking in DOCSIS Networks (TIF18)* » du *"CRTC Interconnection Steering Committee Network Working Group"*, voir leurs documents <<http://www.crtc.gc.ca/cisc/eng/cisf3d0g.htm>>). Avant ce RFC, les méthodes utilisées étaient variables et pas forcément très jolies (des enregistrements TXT, par exemple).

Cela pose quelques problèmes de sécurité, notamment liés à la protection de la vie privée. Une adresse MAC est en effet (en théorie) unique au niveau mondial et peut donc permettre de suivre une machine. Elle change moins que l'adresse IP attribuée et fournit donc un meilleur moyen de traque, permettant de suivre un utilisateur donné. C'est pour cela que la section 8 du RFC dit clairement que les types EUI48 et EUI64 ne doivent apparaître que dans des zones privées, non accessibles au public. (Cela n'a pas suffi à certains participants à l'IETF qui réclamaient qu'on ne mette **jamais** ces adresses EUI48 et EUI64 dans le DNS, zones privées ou pas.)

Ces deux nouveaux types d'enregistrement DNS sont mis en œuvre dans NSD en expérimental (ticket #496 <https://www.nlnetlabs.nl/bugs-script/show_bug.cgi?id=496>, il faut compiler avec l'option `--enable-draft-rrtypes`) et dans Knot <<https://www.knot-dns.cz/>>, apparemment depuis la version 1.3.0.