RFC 6672 : DNAME Redirection in the DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 juin 2012

Date de publication du RFC : Juin 2012

https://www.bortzmeyer.org/6672.html

Depuis sa normalisation dans le RFC 1034[1], le DNS a suscité le développement d'innombrables extensions, plus ou moins réalistes, plus ou moins utilisées. L'enregistrement **DNAME**, sujet de ce RFC, semble encore très peu utilisé : il permet de donner un synonyme à une **zone** entière, pas à un seul nom, comme le fait l'enregistrement CNAME. DNAME avait à l'origine été normalisé dans le RFC 2672, que notre RFC met à jour.

Les enregistrements DNAME permettent d'écrire des équivalences comme :

```
vivendi-environnement.fr. DNAME veolia.fr.
```

et un nom comme `www.vivendi-environnement.fr` sera transformé en `www.veolia.fr`. Le but étant ici de changer le nom de l'entreprise en Veolia sans avoir à s'inquiéter de toutes les occcurrences de l'ancien nom qui trainent dans des signets privés, dans la presse écrite, sur del.icio.us, etc. DNAME a aussi été envisagé (mais peu utilisé) pour les délégations des sous-arbres de traduction d'adresses IP en noms (`in-addr.arpa` et `ip6.arpa`), afin de permettre une rénumérotation d'un réseau relativement légère (section 6.3, qui fournit un exemple et note honnêtement que cela ne résout qu'une petite partie du problème de la renumérotation). Il a aussi été prévu de l'utiliser pour les variantes de domaines IDN (par exemple pour faire une équivalence entre le domaine en chinois traditionnel et le domaine en chinois simplifié). Enfin, il est utilisé dans l'ONS fédéré <http://www.caad.arch.ethz.ch/noolab/files/external/conferences/IoT2010_proceedings/pdf/Demo/D4.pdf>.

En fait, les enregistrements DNAME ne sont pas aussi simples que cela. Le DNAME ne s'applique pas réellement à la zone mais à tous les sous-domaines de l'apex. Il faut donc dupliquer tous les enregistrements de l'apex (typiquement, les MX et les NS). Le vrai fichier de zone pour `videndi-environnement.fr` ressemblerait plutôt à :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1034.txt`

```
@ IN SOA ... Dupliquer le SOA de veolia.fr
        IN   NS  ... Idem pour NS et MX
        IN   MX   ...

        IN   DNAME veolia.fr.

; Et ça suffit, les noms comme www.vivendi-environnement.fr seront
; gérés par le DNAME.
```

DNAME est donc complémentaire du CNAME : celui-ci « aliase » un nom, le DNAME aliase un sous-arbre. Si on veut aliaser les deux, il faut faire comme dans le fichier de zone ci-dessus. Sinon, il faudrait DNAME **et** CNAME (mais on ne peut pas se servir des deux en même temps) ou bien créer un nouveau type de données (un BNAME, qui aurait les propriétés des deux, a été discuté à l'IETF).

Le tableau 1 du RFC donne des exemples de cas simples et de cas plus tordus. Il prend trois entrées, le nom demandé (QNAME pour "*Query Name*"), le nom du DNAME ("*owner name*") et la cible de ce dernier. Par exemple, avec le DNAME ci-dessus ("*owner name*" `videndi-environnement.fr`, cible `veolia.fr`), un QNAME de `videndi-environnement.fr` ne donnera rien (le DNAME ne concerne que les domaines en dessous de l'apex), un QNAME de `www.videndi-environnement.fr` donnera `www.veolia.fr`, un QNAME de `www.research.videndi-environnement.fr` donnera `www.research.veol`
Attention, les chaînes (un DNAME pointant vers un DNAME) sont légales. Du point de vue sécurité, une chaîne est aussi forte que son maillon le plus faible et notre RFC, comme le RFC 6604 spécifie que DNSSEC ne doit valider une chaîne que si **tous** les alias sont valides (section 5.3.3).

Pour que la redirection vers la cible soit déterministe, le RFC impose (section 2.4) qu'un seul DNAME, au maximum, existe pour un nom. BIND refuserait de charger une telle zone et nous dirait (version 9.9.1) :

```
23-May-2012 22:39:35.847 dns_master_load: foobar.example:20: sub.foobar.example: multiple RRs of singleton t
23-May-2012 22:39:35.847 zone foobar.example/IN: loading from master file foobar.example failed: multiple RR
23-May-2012 22:39:35.847 zone foobar.example/IN: not loaded due to errors.
```

Si on préfère tester avec l'excellent validateur de zones validns <`https://github.com/tobez/validns/`>, il faut se rappeler que ce test est considéré comme de politique locale et n'est pas activé par défaut. Il faut donc penser à l'option `-p` :

```
% validns -z foobar.example -p all ./foobar.example
./foobar.example:19: multiple DNAMEs
```

Notre RFC prévoit le cas où le client DNS pourrait ignorer les DNAME. Le serveur synthétise des enregistrements CNAME équivalents (section 3.1) et les met dans la réponse. Le TTL de ses enregistrements doit être celui du DNAME (c'est un des gros changements par rapport au RFC 2672, où le TTL du CNAME généré était de zéro).

Notez qu'un DNAME peut être créé par mise à jour dynamique du contenu de la zone (section 5.2, une nouveauté par rapport au RFC 2672), masquant ainsi tous les noms qui pouvaient exister avant, sous son nom. Avec un serveur BIND 9.9.1, avant la mise à jour, on voit un nom ayant une adresse :

```
% dig @127.0.0.1 -p 9053 AAAA www.sub.foobar.example
...
;; ANSWER SECTION:
www.sub.foobar.example. 600     IN      AAAA    2001:db8::2
```

et, après une mise à jour dynamique où ce programme (en ligne sur `https://www.bortzmeyer.org/files/dns-dname-dynamic-update.py`) ajoute un DNAME pour `sub.foobar.example` et pointant vers `example.org`, on obtient :

```
% dig @127.0.0.1 -p 9053 AAAA www.sub.foobar.example
...
;; ANSWER SECTION:
sub.foobar.example.     300     IN      DNAME   example.org.
www.sub.foobar.example. 300     IN      CNAME   www.example.org.
```

(Si le serveur était récursif, on obtiendrait également l'adresse IPv6 de `www.example.org`.)

Les DNAME sont mis en œuvre dans BIND et nsd mais semblent peu déployés. Si vous voulez regarder ce que cela donne, testez `testonly.sources.org` qui est un DNAME de `example.org` donc, par exemple, `www.testonly.sources.org` existe :

```
% dig AAAA www.testonly.sources.org
...
;; ANSWER SECTION:
testonly.sources.org.   86400   IN      DNAME   example.org.
www.testonly.sources.org. 0     IN      CNAME   www.example.org.
www.example.org.        171590  IN      AAAA    2001:500:88:200::10
```

(Notez que le serveur utilisé n'a pas suivi la nouvelle règle de notre RFC 6672 et a mis un TTL de zéro.)

Selon moi, une des raisons pour le peu de déploiement de DNAME est que le problème peut se résoudre tout aussi simplement, sans changement dans le DNS, par l'utilisation d'une préprocesseur ou bien en créant un lien symbolique entre les deux fichiers de zone <`https://www.bortzmeyer.org/identical-domains-with-bind.html`> (si le fichier ne contient que des noms relatifs, ça marche très bien, que ce soit avec BIND ou avec nsd).

Les changements par rapport au RFC 2672 sont limités. C'est le même type d'enregistrement (numéro 39 <`https://www.iana.org/assignments/dns-parameters`>) et le même format sur le réseau. Parmi les principaux changements, le TTL du CNAME synthétisé (déjà décrit plus haut) et la disparition complète de l'utilisation d'EDNS pour signaler qu'un client connait les DNAME (cette option était normalisée dans le RFC 2672, section 4.1). L'annexe A donne la liste complète des changements.