RFC 6604 : xNAME RCODE and Status Bits Clarification

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 avril 2012

Date de publication du RFC : Avril 2012

https://www.bortzmeyer.org/6604.html

Ce RFC est très court car il avait juste à répondre à une question simple : le DNS a des mécanismes (le plus connu est l'enregistrement CNAME) permettant à un nom de domaine de pointer vers un autre. Si, en suivant cette chaîne de noms, on rencontre une erreur, que doit indiquer le code de retour dans la réponse DNS ? Le résultat de la première requête de la chaîne ou bien celui de la dernière ? Le RFC tranche dans le sens de la grande majorité des résolveurs DNS actuels : le "*rcode*" doit être celui de la **dernière** requête de la chaîne.

C'est tout bête, mais ce cas n'était pas clairement spécifié dans les précédents RFC sur le DNS. Si on a par exemple, dans le DNS :

```
www.foobar.example. IN CNAME www.nothere.example.
```

Alors une requête `AAAA www.foobar.example` rencontrera l'alias et le résolveur continuera en demandant `www.nothere.example`. Si `www.nothere.example` n'existe pas, alors qu'on a demandé de l'information sur `www.foobar.example`, le code de retour doit-il être `NXDOMAIN` (ce nom n'existe pas) ou bien `NOERROR` (on a bien trouvé un enregistrement, ici le CNAME et `www.foobar.example` existe) ? Même chose avec d'autres types d'enregistrement « alias » comme DNAME. (CNAME redirige un nom, DNAME redirige les noms situés en dessous de lui.) On parle alors de xNAME pour désigner globalement tous les types « alias ». Notez bien que, quoique cela soit déconseillé, il peut y avoir une chaine de plus de deux xNAME.

Avant de voir le cas du code de retour (rcode dans la terminologie DNS, pour "*return code*"), la section 2 règle celui des bits de statut. Le bit AA ("*Authoritative Answer*") est décrit dans le RFC 1035 [1], section

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1035.txt`

4.1.1. Il indique que la réponse vient d'un serveur faisant autorité (pas d'un cache). Dans le cas d'une chaîne de xNAME, les AA peuvent être différents à chaque étape. Mais le RFC 1035 disait clairement que le bit dans la réponse était pour le premier nom mentionné dans la section Réponse du paquet. Rien ne change ici, la spécification était claire dès le début.

Le bit AD ("*Authentic Data*") est plus récent. Normalisé dans le RFC 4035, section 3.2.3, il indique que la réponse est correctement signée avec DNSSEC. Là encore, la règle était claire dès le début : ce bit n'est mis que si **toutes** les réponses dans la section Réponse (et la section Autorité) sont authentiques.

Mais le vrai problème concerne le rcode (RFC 1035, section 4.1.1) car, là, le RFC original (voir aussi RFC 1034, section 4.3.2 et bon courage pour le comprendre) n'était pas clair. Le RFC 2308, dans sa section 2.1, dit qu'il faut fixer le code de retour en fonction de la **dernière** étape de la chaîne, tout en notant que tous les serveurs ne le font pas. La section 3 fixe donc des règles précises : lorsqu'on suit une chaîne, les étapes intermédiaires n'ont pas d'erreur. Il ne sert donc à rien d'indiquer le résultat de la **première** étape. Le code de retour doit donc être mis en fonction de la **dernière** étape uniquement. Dans l'exemple plus haut, le résultat de la requête `AAAA www.foobar.example` doit donc être NXDOMAIN (domaine inexistant).

Voilà, vous pouvez arrêter la lecture ici, l'essentiel du RFC est le paragraphe précédent. Mais la section 4 apporte quelques détails sur la sécurité. Par exemple, elle rappelle que des bits comme AA ou AD ne sont **pas** protégés par DNSSEC. Un attaquant a donc pu les changer sans être détecté. Si on veut être sûr de leur intégrité, il faut protéger la communication avec le serveur, par exemple avec le TSIG du RFC 8945 (ou bien que le client ignore le bit AD et valide lui-même avec DNSSEC).

Si vous voulez tester vous-même que votre résolveur obéit bien aux règles de ce RFC, vous pouvez tester avec `dangling-alias.bortzmeyer.fr` qui existe mais pointe vers un nom qui n'existe pas. Vous devez donc obtenir un NXDOMAIN, ce qui est le cas avec la plupart des résolveurs actuels (la question de l'implémentation de ce RFC ne se pose pas, le RFC a pris acte du comportement très majoritaire des logiciels).

Voici un exemple avec un résolveur correct (un Unbound) :

```
% dig AAAA dangling-alias.bortzmeyer.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 45331
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1
```