RFC 2181 : Clarifications to the DNS Specification

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 juillet 2008

Date de publication du RFC : Juillet 1997

http://www.bortzmeyer.org/2181.html

Le DNS est à la fois un des protocoles de base de l'Internet, dont presque toutes les transactions dépendent, et un des protocoles les plus mal spécifiés. Les RFC de référence, les RFC 1034[1] et RFC 1035, sont toujours en service mais, écrits il y a plus de vingt ans, ils accusent leur âge. Ils sont souvent ambigus et ont été mis à jour par de nombreux RFC ultérieurs. Ainsi, celui qui développe une nouvelle mise en œuvre du DNS doit lire plusieurs RFC successifs. L'un des plus importants est notre RFC 2181 qui avait clarifié plusieurs points particulièrement importants de la norme originelle.

On ne peut rien faire avec le DNS si on ne lit pas ce RFC 2181. Il est une sorte de FAQ des erreurs les plus souvent commises en lisant trop vite les RFC 1034 et RFC 1035. Mais il corrige aussi ces RFC, qui comportaient parfois de réelles erreurs (sections 1, 2 et 3).

Les consignes de notre RFC 2181 sont très variées.

Ainsi, la section 4 rappelle que le serveur DNS doit répondre depuis l'adresse IP à laquelle la question a été posée (pour un serveur qui a plusieurs adresses). La section 4.2 pose le même principe pour le numéro de port.

La section 5 introduit un concept nouveau, celui de "*RRSet*" ("*Resource Record Set*" ou « ensemble d'enregistrements de données »). Ce concept n'existait pas dans les RFC 1034 et RFC 1035. Un "*RRSet*" est un ensemble d'enregistrements DNS pour le **même nom de domaine**, et le même type. Ainsi, ce groupe forme un "*RRSet*" :

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

```
foobar.example.com.    IN    AAAA      2001:DB8:123:456::1
foobar.example.com.    IN    AAAA      2001:DB8:CAFE:645::1:2
```

mais pas celui-ci :

```
foobar.example.com.    IN    AAAA      2001:DB8:123:456::1
baz.example.com.       IN    AAAA      2001:DB8:CAFE:645::1:2
```

(car le nom est différent) ni celui-ci :

```
foobar.example.com.    IN    AAAA      2001:DB8:123:456::1
foobar.example.com.    IN    A         192.0.2.34
```

(car le type est différent).

Le RFC impose ensuite (section 5.1) que les enregistrements d'un "*RRSet*" soient tous envoyés dans une réponse (ou bien que le bit TC - indiquant la troncation - soit positionné, ce que détaille la section 9). Pas question de n'envoyer qu'une partie d'un "*RRSet*". Il impose également que les différents enregistrements d'un "*RRSet*" aient le même TTL (section 5.2). Il existe également des règles pour DNSSEC (section 5.3) mais elles concernent l'ancienne version de DNSSEC, qui a depuis été remplacée par DNSSEC-bis (RFC 4033 et suivants).

De même qu'un serveur ne peut pas n'envoyer qu'une partie des enregistrements d'un "*RRSet*", il ne doit pas fusionner un "*RRSet*" reçu en réponse avec des données du même "*RRSet*" qui seraient dans son cache (section 5.4). Le reste de la section 5.4 est d'ailleurs consacré à la nécessaire paranoïa d'un serveur de noms récursif. En effet, le RFC 2181 lui impose de ne pas accepter aveuglément n'importe quelle donnée mais de juger de la confiance qu'on peut lui accorder (section 5.4.1). Ainsi, les données présentes dans la section "*additional*" d'une réponse DNS sont moins fiables que celles de la section "*answer*". Le déploiement de notre RFC a ainsi résolu un gros problème de sécurité du DNS : les serveurs de noms récursifs avalaient tout le contenu de la réponse, sans juger de sa valeur, et étaient donc faciles à empoisonner avec de fausses données. Ainsi, avant le RFC 2181, un serveur qui demandait les enregistrements de type A pour `www.example.org` et qui recevait une réponse :

```
;; QUESTION SECTION:
;www.example.org.                        IN      A

;; ANSWER SECTION:
www.example.org.                    IN   A    192.0.2.1

;; ADDITIONAL SECTION:
www.google.example.                    IN   A   192.0.2.178
```

acceptait l'enregistrement A dans la section additionnelle, bien que cet enregistrement n'aie aucun rapport avec la question posée et ne fasse pas autorité.

La section 6 du RFC traite des frontières de zones DNS ("*zone cuts*"). L'arbre des noms de domaine est découpé en **zones** (RFC 1034, section 2.4 et 4.2), chaque zone étant traditionnellement décrite dans un fichier de zone spécifique. Pour connecter une zone parente à la fille, la parente ajoute des enregistrements de type NS. Il faut se rappeller que les frontières de zone ne se voient pas dans le nom de

domaine. Est-ce que `org.uk` est géré par la même organisation que `co.uk` ? Vous ne pouvez pas le savoir juste en regardant ces noms. D'autre part, les zones ne correspondent pas forcément à des frontières organisationnelles. Pendant longtemps, `nom.fr` était dans une zone différente de `fr` alors que les deux domaines étaient gérés par le même organisme, l'AFNIC. En sens inverse, le futur domaine `.tel` n'aura qu'une seule zone, tout en permettant aux utilisateurs de mettre leurs propres données.

Bref, la **zone** est une notion complexe. Notre RFC rappelle juste que les données de délégation (les enregistrements NS) ne font pas autorité dans la zone parente (section 6.1). En dehors des enregistrements indispensables à la délégation (NS et peut-être A et AAAA de colle), les serveurs ne doivent pas envoyer de données qui sont au delà d'une frontière de zone.

La section 8 corrige légèrement la définition du TTL qui se trouve section 3.6 du RFC 1034 en imposant que ce soit un entier non signé.

La section 10 s'attaque à des question plus délicates car plus visibles par l'utilisateur humain, les questions de **nommage**. Au contraire des règles des sections précédentes, qui ne seront guère vues que par les programmeurs qui écrivent des serveurs de noms, les règles des sections 10 et 11 concernent tous les gérants de zones DNS.

D'abord, un rappel en début de section 10 : dire que telle machine « a pour nom de domaine `gandalf.example.net` » est un net abus de langage. Une machine n'a pas **un** nom qui serait le « vrai » ou l'« authentique ». Il faut plutôt dire que des tas de noms dans le DNS peuvent pointer sur une machine donnée. Ainsi, il n'y a aucune obligation d'avoir un seul enregistrement de type PTR (section 10.2) pour une adresse IP donnée.

La section 10.1 clarifie les enregistrements de type CNAME. Leur noms peut être trompeur car il veut dire "*Canonical Name*" (« nom canonique ») alors que le CNAME sert plutôt à enregistrer des **alias** (section 10.1.1). Si le DNS contient :

```
www.example.org.    IN    CNAME    www.example.net.
```

il ne faut pas dire que `www.example.org` est le CNAME de `www.example.net` mais plutôt qu'il est l'alias de `www.example.net` ou, plus rigoureusement, qu'il existe un enregistrement de type CNAME dont le nom est `www.example.org`.

La section 10.2 rappelle qu'on peut avoir plusieurs enregistrements de type PTR et surtout qu'un PTR peut mener à un alias, et pas directement au nom de domaine désiré. Cette propriété est d'ailleurs à la base de la délégation sans classe de `in-addr.arpa` décrite dans le RFC 2317.

Par contre, les enregistrements NS et MX ne peuvent **pas** mener à un alias (section 10.3). Un logiciel comme Zonecheck <`http://www.zonecheck.fr/`> teste d'ailleurs cela.

Enfin, la section 11 est peut-être la plus ignorée de tout le RFC. Consacrée à la syntaxe des noms de domaines, elle rappelle (c'est juste un rappel, les RFC 1034 et RFC 1035 étaient déjà clairs à ce sujet) qu'un nom de domaine peut prendre n'importe quelle valeur binaire. Si vous entendez quelqu'un dire que « le DNS est limité aux caractères ASCII » ou bien « le DNS est limité aux lettres, chiffres et tiret », vous pouvez être sûr que la personne en question est profondément ignorante du DNS. Le DNS a toujours permis de stocker n'importe quels caractères, même non-ASCII et, s'il a fallu inventer les IDN du RFC 3490, c'est pour de tout autres raisons <`http://www.bortzmeyer.org/pourquoi-idn-et-pas-un-dns-unicode.html`>.

La section 11 souligne juste que les **applications** qui utilisent le DNS peuvent avoir des restrictions. Ainsi, avant les IRI du RFC 3987, les adresses du Web étaient en effet limitées à ASCII.