

RFC 6895 : Domain Name System (DNS) IANA Considerations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 avril 2013

Date de publication du RFC : Avril 2013

<https://www.bortzmeyer.org/6895.html>

Un RFC un peu bureaucratique, pour détailler les mécanismes utilisés pour l'enregistrement dans les registres de l'IANA des paramètres liés au DNS. Il met très légèrement à jour son prédécesseur, le RFC 6195¹, libéralisant encore un peu plus l'enregistrement de nouveaux types de données dans le DNS.

Un certain nombre de paramètres (section 2, qui résume le format des paquets DNS), dans le DNS, sont enregistrés à l'IANA, afin de s'assurer d'une interprétation identique partout. C'est ainsi que l'IANA gère un registre des paramètres DNS <<https://www.iana.org/assignments/dns-parameters>> où on trouve, entre autres, les types d'enregistrement (A, codé 1, pour une adresse IPv4, AAAA, codé 28, pour une adresse IPv6, LOC, codé 29, pour les positions géographiques du RFC 1876, TLSA, codé 52, pour le RFC 6698, etc). Cet espace n'étant pas de taille infinie, il faut y enregistrer de nouveaux paramètres avec prudence.

L'affectation dans cet espace forme le point le plus important de ce RFC (section 3). Il faut comprendre qu'il y a trois types de numéros utilisés dans cet espace : ceux qui identifient un type de données (comme les quatre cités plus haut), ceux qui identifient une question et le cas particulier des méta-types. Une question, dans le DNS, peut être un type de données (on met 52 dans le champ QTYPE de la requête pour dire qu'on veut des enregistrements TLSA), mais il existe aussi des questions qui ne correspondent pas à un type unique comme 255 (noté ANY ou ALL ou *) qui veut dire « envoie-moi toutes les données que tu as, quelles que soit leur type ». Enfin, les méta-types sont des données temporaires, liées à une transaction, comme les TSIG (numéro 250) du RFC 8945, qui n'existent que le temps de la session DNS.

Pour les types de données, la politique d'allocation est simple et libérale : on remplit un formulaire (qui se trouve en annexe A du RFC), on l'envoie à l'IANA (via l'adresse dns-rrtype-applications@ietf.org)

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc6195.txt>

et un expert l'examinera (procédure "*Expert Review*" du RFC 5226) et rendra son jugement. (Il est recommandé de l'envoyer d'abord à la liste de groupe de travail dnsex <<http://tools.ietf.org/wg/dnsex>> pour un examen préalable.) Les formulaires approuvés sont ensuite publiquement archivés (mais je n'ai pas trouvé où).

Le RFC donne les critères que doit suivre l'expert pour sa décision :

- D'abord, être libéral et accepter la plupart des demandes, sauf raison impérieuse. Par défaut, la réponse est oui.
- Parmi les bonnes raisons de rejeter une demande, l'insuffisance de la documentation fournie, des erreurs DNS dans la spécification du nouveau type (par exemple des suppositions incorrectes sur le fonctionnement des jokers, un cas relativement fréquent) ou un trop grand nombre de types demandés alors que l'application pourrait s'en tirer avec un seul.
- Il y a une autre raison technique de rejeter une demande, ou en tout cas de l'examiner de plus près : l'enregistrement facile et libéral ne concerne que les types de données où les serveurs de noms n'ont pas besoin d'appliquer un traitement spécial (question I du formulaire à remplir). Autrement dit, ils peuvent traiter le nouveau type comme un type inconnu, selon le RFC 3597. S'il y a besoin d'un traitement spécial (par exemple CNAME, DS), on revient à la procédure, bien plus lourde, d'une norme en bonne et due forme. Notez que, pour certains types, un traitement spécial est possible mais pas obligatoire (cas de MX, où il est conseillé d'inclure les adresses IP des serveurs de courrier dans la réponse mais, si ce n'est pas fait, le service marche quand même). Dans ce cas, c'est la procédure libérale qui s'applique

Outre l'enregistrement de nouveaux types de ressources DNS, notre RFC mentionne également d'autres champs des messages DNS. Un changement ou une extension de leur sémantique continue à nécessiter une action plus lourde à l'IETF. C'est le cas des classes (comme la plus courante, IN pour Internet). C'est aussi le cas de bits comme RD ("*Recursion Desired*"), qui n'a de signification que dans une question DNS. Dans une réponse, il est indéfini et son éventuelle utilisation future nécessitera un RFC sur le chemin des normes. Même chose pour le dernier bit qui reste libre dans les options, le bit Z (section 2.1). Quant aux "*opcodes*" qui indiquent le type du message (requête / notification / mise à jour dynamique / etc), un ajout à leur liste nécessitera le même chemin (section 2.2). Ils ont leur propre registre <<https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-5>>.

Les codes de réponse ("*rcodes*"), comme NXDOMAIN (nom inexistant), FORMERR (erreur de format) ou BADTIME (signature trop ancienne ou trop récente, cf. RFC 8945) sont tirés d'un espace plus vaste (il n'y a pas que les quatre bits 12 à 15 dans l'en-tête classique, il y a aussi des extensions comme les pseudo-enregistrements OPT) et la procédure est donc un peu plus libérale ("*IETF Review*", c'est-à-dire un RFC non individuel mais pas forcément sur le chemin des normes, cf. section 2.3). Il y a également un registre de ces codes <<https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-6>>. À noter qu'une gestion trop légère des registres avait entraîné à une époque une double affectation du "*rcode*" 16, enregistré par le RFC 2671, puis ré-enregistré par le RFC 2845...

Notez aussi que notre RFC mentionne (section 3.3) l'allocation des noms, pour rappeler qu'il existe des noms réservés (RFC 2606) et qu'il existe un RFC (bien dépassé par les évolutions politiciennes ultérieures à l'ICANN), le RFC 1591, sur l'allocation et la gestion des TLD.

Les changements depuis le RFC 6195 sont décrits dans l'annexe B. Le seul vraiment important est une simplification du processus d'enregistrement des nouveaux types de données (par exemple, l'examen de la demande d'enregistrement d'un nouveau type de données par le groupe de travail dnsex n'est **plus** obligatoire). Cette simplification était largement consensuelle. Le reste des changements est un ensemble varié de clarifications et de précisions.