

RFC 4592 : The Role of Wildcards in the Domain Name System

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 février 2007

Date de publication du RFC : Juillet 2006

<http://www.bortzmeyer.org/4592.html>

La norme DNS avait prévu le cas des **jokers** ("*wildcards*"), des enregistrements DNS qui répondaient à toutes les questions. Ces jokers ont été une telle source de confusion pour les versions successives des protocoles DNS qu'il a fallu faire un RFC de clarification.

L'idée parait simple a priori. Si une zone DNS `mondomaine.oi.example` contient des enregistrements comme :

```
*      IN      A      192.0.2.42
```

alors, toute requête pour l'adresse IP `absolumentnimportequoi.mondomaine.oi.example` renverra 192.0.2.42. Cette fonction a été surtout mise en cause pour des raisons politiques (son utilisation par Verisign dans l'affaire des jokers de `.com`) mais elle a aussi des lourdes conséquences techniques : tous les protocoles bâtis sur le DNS (et il y en a beaucoup, en raison du succès du DNS) doivent gérer le cas particulier des jokers.

Par exemple, notre RFC note un problème dans le RFC 2782¹ sur l'enregistrement SRV, qui laisse entendre (et c'est une erreur fréquente) qu'un joker, comme dans le shell Unix, est interprété même s'il se trouve au milieu d'un nom (ce n'est pas le cas).

Une des victimes de cette confusion a été DNSSEC et c'est dans le cadre du travail sur ces extensions de sécurité du DNS qu'est apparue la nécessité de clarifier la norme sur ce point.

Disons-le tout de suite, notre RFC de clarification n'est pas un travail pédagogique. Son rôle est normatif, il vise à rendre la spécification des jokers moins ambiguë, pas à la rendre plus claire. Le texte est donc très abstrait et nécessite une connaissance détaillées des RFC 1034 et RFC 1035 et de leur vocabulaire.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc2782.txt>