

RFC 9619 : In the DNS, QDCOUNT is (usually) One

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 juillet 2024

Date de publication du RFC : Juillet 2024

<https://www.bortzmeyer.org/9619.html>

Dans un message DNS, il y a quatre sections qui peuvent prendre un nombre variable d'enregistrements ("*resource records*"). Chaque section est précédée d'un chiffre qui indique ce nombre d'enregistrements. L'une de ces sections indique la question posée. Est-ce que cela a un sens de mettre plusieurs questions dans un message? Non, répond, ce très court RFC, qui clarifie le RFC 1035¹ sur ce point.

Regardons une requête DNS avec tshark :

```
% tshark -V -r dns.pcap
...
Domain Name System (query)
  Transaction ID: 0x0dfd
  Flags: 0x0120 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
...
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    wylag.de: type A, class IN
      Name: wylag.de
      [Name Length: 8]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Additional records
```

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

```
<Root>: type OPT
  Name: <Root>
  Type: OPT (41)
  UDP payload size: 4096
  Higher bits in extended RCODE: 0x00
  EDNS0 version: 0
  Z: 0x8000
    1... .... = DO bit: Accepts DNSSEC security RRs
    .000 0000 0000 0000 = Reserved: 0x0000
  Data length: 12
  Option: COOKIE
    Option Code: COOKIE (10)
    Option Length: 8
    Option Data: 93c545f2aaf3f12c
    Client Cookie: 93c545f2aaf3f12c
    Server Cookie: <MISSING>
```

Il s'agit d'une requête, pas d'une réponse, donc il est normal que les sections Answer et Authority soient vides (taille à zéro). La section Additional n'est pas vide car elle contient l'enregistrement EDNS. Et la section Question contient un seul enregistrement, la question (« quelle est l'adresse IPv4 de wylag.de? »).

Tout le problème traité par ce RFC est : que se passe-t-il si la section Question d'une requête contient plus d'un enregistrement? Je divulgue tout de suite : c'est interdit, il ne faut pas. (Pour le cas des requêtes/réponses ordinaires, avec l'"opcode" 0; d'autres messages DNS peuvent avoir des règles différentes.) La principale raison pour cette interdiction est que, dans la réponse, certains champs sont globaux à toute la réponse (comme le code de réponse, le "rcode") et on ne peut donc pas se permettre d'accepter des questions qui risqueraient de nécessiter des réponses différentes. Désormais, un serveur DNS qui voit passer une requête avec un nombre de questions supérieur à 1 doit répondre avec le code de retour FORMERR ("format error").

Le RFC 1035, la norme originelle, traitait ce point mais restait flou.

Il y avait une autre façon de régler le problème, en imposant que, s'il y a plusieurs questions, toutes portent sur le même nom de domaine. Cela aurait réglé le doute sur le code de retour et aurait pu être pratique pour des cas comme la demande simultanée de l'adresse IPv4 et IPv6. Mais cette solution a été écartée au profit de la solution plus simple qui était d'interdire les questions multiples. (Et, de toute façon, on ne peut pas garantir que le code de retour sera le même pour tous les types, même si le nom est le même. Pensez aux serveurs DNS générant dynamiquement les données.)