RFC 10001 : Operational Guidelines for DNS Transport in Mixed IPv4/IPv6 Environments

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 août 2026

Date de publication du RFC : Août 2026

https://www.bortzmeyer.org/10001.html

Vous gérez des serveurs DNS (qu'ils soient des résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> ou des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant.html>) dans un environnement où il y a à la fois IPv4 et IPv6 ? Alors, ce RFC va vous aider. Il remplace le RFC 3901 [1], qui avait été écrit pour un monde très différent, où IPv6 était marginal. Désormais, la recommandation est que tout serveur DNS doit pouvoir servir les requêtes avec les deux versions d'IP.

Alors que le plan de transition initial pariait sur une migration de quelques années suite à laquelle IPv4 ne serait plus qu'un souvenir, la réalité est celle d'une co-existence de longue durée des deux versions (cf. RFC 9386). Le retard avec lequel certains acteurs de l'Internet ont migré fait que le paysage d'aujourd'hui est très complexe, avec des réseaux purement IPv4, des réseaux purement IPv6 et des réseaux mixtes. Si une zone DNS n'est servie que par des serveurs <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> en IPv6, un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> n'ayant qu'IPv4 ne pourra pas la résoudre, et c'est pareil en sens inverse. On aurait une **fragmentation** de l'espace des noms de domaine, et c'est ce qu'il faut éviter. (Du fait du caractère arborescent du DNS, la fragmentation pourrait aussi se produire si un domaine parent, quelque part entre la racine et le domaine que vous voulez résoudre, n'avait qu'IPv4 ou qu'IPv6. Le RFC cite un cas encore plus amusant où, dans la chaine des noms, certains domaines ne sont accessibles qu'en IPv4 et d'autres qu'en IPv6 ; seul un résolveur à double pile - IPv4 **et** IPv6 - pourrait résoudre les noms situés au bout de cette chaine.) La lecture de « *"How Ready is DNS for an IPv6-Only World ?"* <https://link.springer.com/chapter/10.1007/978-3-031-28486-1_22> est recommandée.

Lorsque le RFC 3901, premier RFC à parler de la version d'IP utilisée pour transporter les requêtes et les réponses DNS, a été écrit, le paysage était nettement dominé par IPv4. Ce RFC 3901 se préoccupait

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3901.txt

surtout de maintenir la résolution de noms avec les zones existantes, dont l'écrasante majorité n'était servie qu'en IPv4. Aujourd'hui (voyez le rapport ARCEP <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv> html>), IPv6 est dans une position très différente, dans certains pays, la grande majorité des réseaux d'accès fournit IPv6, et les gros services Web populaires ont souvent IPv6. Bien des réseaux sont purement IPv6 à la base, IPv4 étant désormais un service fourni au-dessus d'IPv6. Le RFC 6540 considère à juste titre que IP, aujourd'hui, implique IPv6. Notre RFC remplace donc le RFC 3901 pour demander de l'IPv6 sur tous les serveurs faisant autorité et tous les résolveurs.

Un petit rappel au passage : ce RFC parle du transport des données dans les requêtes et les réponses DNS, **pas** des données elles-mêmes. Une requête/réponse pour des données de type A (adresses IPv4) peut se faire sur des messages échangés sur IPv6 et une requête/réponse pour des données de type AAAA (adresses IPv6) peut se faire sur des messages échangés sur IPv4.

Donc, il faut IPv4 et IPv6 sur les serveurs. Mais il ne suffit pas de croire qu'on a activé les deux. Des erreurs de configuration peuvent faire qu'on pense avoir IPv4 et IPv6 mais qu'un des deux ne marche pas. Cela peut être dû à un pare-feu qu'on a mis devant le serveur DNS (une mauvaise idée, en général, mais c'est une autre histoire) et qui n'autorise qu'une des deux versions. Mais il peut aussi y avoir des erreurs spécifiquement DNS :

— Les serveurs faisant autorité ont IPv4 mais pas d'enregistrements de type A (ou bien ils ont IPv6 mais on a oublié de publier un AAAA),
— les serveurs ont bien les enregistrements A et AAAA dans leur zone mais on a oublié la colle <https://www.afnic.fr/observatoire-ressources/papier-expert/le-dns-ca-colle-ou-ca > (RFC 9471),
— il y a la colle mais pas d'enregistrements dans la zone, ce qui empêcherait les résolveurs qui revalident (cf. draft-ietf-dnsop-ns-revalidation) de résoudre le nom,
— le nom du serveur de noms est dans une autre zone, qui n'est pas elle-même résolvable en IPv4 et IPv6,
— une des zones situées au dessus, dans l'arbre du DNS, n'est pas résolvable avec les deux versions d'IP (la résolution DNS <https://www.afnic.fr/wp-media/uploads/2024/09/DNS-resolution-we jpg> part de la racine et suit un chemin descendant dans l'arbre des noms de domaine).

Toutes ces erreurs possibles imposent à l'administrateurice DNS de **vérifier** sa zone. On ne doit pas se contenter de se dire « c'est bon, j'ai tout configuré, on doit **tester**, par exemple avec Zonemaster <https://zonemaster.fr/> (ou, en plus léger et moins riche, check-soa <https://framagit.org/bortzmeyer/check-soa>). Et re-tester régulièrement car des erreurs peuvent survenir par la suite.

```
% check-soa bortzmeyer.org
ns-global.kjsl.com.
 23.128.97.53: OK: 2026083000
 2607:7c80:53::53: OK: 2026083000
ns.eu.org.
 78.194.169.74: OK: 2026083000
ns1.bortzmeyer.org.
 80.77.95.49: OK: 2026083000
 2602:fbb1:1:245b::42: OK: 2026083000
ns1.shaftinc.fr.
 2001:41d0:404:200::49e1: OK: 2026083000
 51.178.53.118: OK: 2026083000
ns2.bortzmeyer.org.
 2400:8902::f03c:91ff:fe69:60d3: OK: 2026083000
 172.104.125.43: OK: 2026083000
ns2.shaftinc.fr.
 2a05:f480:1c00:28a:5400:2ff:fee7:316f: OK: 2026083000
 136.244.112.196: OK: 2026083000
ns4.bortzmeyer.org.
 2001:4b98:dc0:41:216:3eff:fe27:3d3f: OK: 2026083000
 92.243.4.211: OK: 2026083000
```

Il peut aussi y avoir des problèmes dûs au réseau. L'un des plus courants est un problème de MTU. Si la réponse, notamment en raison des signatures DNSSEC, dépasse la MTU du chemin, elle devra être fragmentée et, dans l'Internet tel qu'il est, cela se passera souvent mal (cf. RFC 8900 et RFC 9715). Il vaut mieux, pour un serveur DNS, éviter d'envoyer des réponses trop grosses (le RFC suggère 1[Caractère Unicode non montré [2]]232 octets maximum), pour être sûr qu'il n'y ait pas de fragmentation. (Attention, le mot « fragmentation » ici n'a pas le même sens que plus haut, quand on parlait de fragmentation de l'espace de noms.) Notez que DNSSEC n'est pas nécessaire pour faire des grosses réponses. Essayez `oracle.com/TXT` pour voir.

Ça, c'était pour UDP. Et pour TCP ? Bien sûr, la découverte de la MTU du chemin existe (RFC 8201, RFC 8899) mais elle prend du temps alors que le DNS est censé avoir une très faible latence <`https://www.bortzmeyer.org/latence.html`>. Le RFC recommande donc de configurer la MSS à moins de 1[Caractère Unicode non montré]388 octets.

Mais il n'y a pas que la MTU. Par exemple, un résolveur peut avoir des problèmes de connectivité. Un cas où elle sera interrompue de manière intermittente (et donc difficile à déboguer) est celui où le résolveur est derrière un routeur CGNAT (RFC 6888) avec des délais d'expiration des « connexions » très court. Le trafic DNS, plutôt variable, ne sera pas suffisant pour maintenir la « connexion » ouverte. Et le RFC cite de nombreux autres exemples de problèmes réseau possibles.

Il est aussi possible qu'un serveur ne soit pas accessible avec une des deux versions d'IP suite à un choix délibéré. Si on regarde le domaine de la BNF, par exemple :

```
% check-soa bnf.fr
ariane.bnf.fr.
 193.50.133.237: OK: 2026081807
galatee.bnf.fr.
 193.50.133.202: OK: 2026081807
```

Pas d'IPv6 du tout. Comme le FAI de la BNF route l'IPv6, c'est certainement un choix délibéré. En 2023 (étude « "*How Ready is DNS for an IPv6-Only World ?*" <`https://link.springer.com/chapter/10.1007/978-3-031-28486-1_22`> »), presque aucun domaine n'avait que IPv6 alors que presque la moitié de ceux testés n'avait que IPv4 (comme `bnf.fr`).

Après ces observations et analyses, le RFC, dans sa section 4, en arrive aux recommandations. Pour les serveurs faisant autorité, il faut, notamment :

— La règle « au moins deux serveurs faisant autorité par zone » devrait désormais être entendue comme « au moins deux en IPv4 et deux en IPv6 ». (On notera que cela ne figure pas dans les recommandations IANA <`https://www.iana.org/help/nameserver-requirements`>, cf. section 6 du RFC.) Zonemaster <`https://zonemaster.fr/`> fait déjà ce test <`https://zonemaster.fr/fr/result/11e8b6128b27cdf2/`> (« Les serveurs de noms de la zone ne retournent pas assez de serveurs (1) faisant autorité ayant une adresse IPv6. La limite inférieure étant fixée à 2. »).
— Évidemment, ces (au moins) deux serveurs IPv6 ne doivent pas utiliser des adresses IPv6 spéciales, genre "*IPv4-embedded*" (RFC 6052), et la résolution de leurs noms ne doit pas nécessiter IPv4.
— Toujours aussi évidemment, les serveurs faisant autorité doivent servir les mêmes données en IPv4 et IPv6.

2. Car trop difficile à faire afficher par LaTeX

— Et pour être sûr de pouvoir passer des données de grande taille, sans compter sur la fragmentation, tous les serveurs doivent accepter TCP (RFC 9210).

Pour les résolveurs :

— Dans presque tous les cas, le résolveur devrait pouvoir parler IPv4 et IPv6.
— Si le résolveur n'a qu'IPv6 (ce qui sera de plus en plus fréquent), il faut qu'il puisse utiliser un mécanisme de coexistence qui lui permette de résoudre des zones purement IPv4 (par exemple RFC 6146, peut-être avec RFC 8781, ou bien en étant capable de faire suivre à un autre résolveur ayant tout ce qu'il faut).
— Pour les résolveurs simplifiés ("*stub resolvers*"), comme celui dans la libc, il faut s'assurer que les résolveurs complets à qui ils transmettent leurs requêtes savent faire IPv4 et IPv6 (en indiquer plusieurs, par exemple dans `/etc/resolv.conf` sur Unix, ne marche pas bien, en raison de la limite sur leur nombre mais aussi du retard que cela entraine).

Le RFC ne semble pas en parler mais je tiens à ajouter une de mes obsessions personnelles : il faut superviser automatiquement vos serveurs DNS, en IPv4 **et** IPv6. Voici par exemple la configuration que j'utilise avec Icinga :

```
apply Service "dns-auth4" {
  check_command = "dig"
  assign where host.address && host.vars.dns_auth
  vars.dig_server = host.address
  vars.dig_ipv4 = true
  ...
}

apply Service "dns-auth6" {
  check_command = "dig"
  assign where host.address6 && host.vars.dns_auth
  vars.dig_server = host.address6
  vars.dig_ipv6 = true
  ...
}

object Host "mononoke" {
  address = "mononoke.bortzmeyer.org"
  address6 = "mononoke.bortzmeyer.org"
  vars.dns_auth = 1
  ...
}
```

Et le serveur DNS sera alors testé avec les deux versions d'IP.

L'annexe A du RFC résume les changements depuis le RFC 3901 :

— Longue discussion sur la question de la fragmentation,
— Et surtout recommandation d'avoir les deux versions d'IP partout (et de le tester).