RFC 8880 : Special Use Domain Name 'ipv4only.arpa'

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 septembre 2020

Date de publication du RFC : Août 2020

https://www.bortzmeyer.org/8880.html

La technique NAT64 pour permettre à des machines d'un réseau purement IPv6 d'accéder à des services toujours uniquement en IPv4 repose sur un préfixe IPv6 spécial, utilisé pour donner l'impression aux machines IPv6 que le service archaïque a de l'IPv6. Dans certains cas, il est pratique que toutes les machines du réseau connaissent ce préfixe. Une technique possible a été proposée dans le RFC 7050[1], utilisant un nom de domaine prévu à cet effet, ipv4only.arpa. Mais ce nom de domaine n'avait pas été documenté rigoureusement comme nom de domaine spécial <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml#special-use-domain> C'est désormais fait, avec ce nouveau RFC.

Le NAT64 est normalisé dans le RFC 6146, et la découverte, par une machine, du préfixe IPv6 utilisé, est dans le RFC 7050. Ce dernier RFC avait créé le nom de domaine ipv4only.arpa, mais sans préciser clairement son statut, et notamment sans demander son insertion dans le registre des noms de domaine spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>. (Cette bavure bureaucratique est d'ailleurs mentionnée dans le RFC 8244.) Le but de notre nouveau RFC 8880 est de réparer cet oubli et de documenter proprement le nom de domaine spécial ipv4only.arpa.

Un petit rappel si vous n'avez pas le courage de lire le RFC 7050 : le problème qu'on cherche à résoudre est celui d'une machine qui voudrait bénéficier de NAT64 mais sans utiliser systématiquement le résolveur DNS64 (RFC 6147). Pour cela, elle émet une requête DNS de type AAAA (adresse IPv6) pour le nom ipv4only.arpa. Comme son nom l'indique, ce nom n'a que des données de type A (adresses IPv4). Si on récupère des adresses IPv6, c'est que le résolveur DNS faisait du DNS64, et on peut déduire le préfixe IPv6 utilisé de la réponse. Sans DNS64, on aura une réponse normale, rien sur IPv6, et deux adresses stables en IPv4 :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7050.txt

```
% dig AAAA ipv4only.arpa
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18633
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
...
;; AUTHORITY SECTION:
ipv4only.arpa. 3600 IN SOA sns.dns.icann.org. noc.dns.icann.org. (
2020040300 ; serial
7200       ; refresh (2 hours)
3600       ; retry (1 hour)
604800     ; expire (1 week)
3600       ; minimum (1 hour)
)

;; Query time: 95 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 07 15:22:20 CEST 2020
;; MSG SIZE  rcvd: 127

% dig A ipv4only.arpa
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2328
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 14, ADDITIONAL: 27
...
;; ANSWER SECTION:
ipv4only.arpa. 86400 IN A 192.0.0.170
ipv4only.arpa. 86400 IN A 192.0.0.171
...
;; Query time: 238 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 07 14:24:19 CEST 2020
;; MSG SIZE  rcvd: 1171
```

En quoi est-ce que ce nom `ipv4only.arpa` est « spécial » (section 2 du RFC) ? D'abord, il n'y a aucune raison de le visiter en temps normal, il n'a aucune ressource utile, et ses deux adresses IP sont stables et bien connues. Paradoxalement, si on l'interroge, c'est qu'on espère un mensonge, l'apparition d'adresses IPv6 qui ne sont pas dans la zone originale. Ce nom de domaine permet en fait une communication de la machine terminale vers un intermédiaire (le résolveur DNS), pour savoir ce qu'il fait. C'est en cela que `ipv4only.arpa` est spécial.

Mais, rappelez-vous, le RFC 7050 avait oublié de déclarer `ipv4only.arpa` comme étant spécial. Résultat, les différents logiciels qui traitent des noms de domaine le traitent de la manière normale et, comme le note la section 3 de notre RFC, cela a quelques conséquences ennuyeuses :

— Si la machine NAT64 utilise un résolveur DNS <`https://www.bortzmeyer.org/resolveur-dns.html`> différent de celui du réseau local, par exemple un résolveur public, `ipv4only.arpa` peut ne pas donner le résultat attendu,
— Les résolveurs DNS64 doivent faire une résolution normale `ipv4only.arpa` alors qu'ils devraient avoir le droit de tout gérer localement et de fabriquer des réponses directement.

Bref, il fallait compléter le RFC 7050, en suivant le cadre du RFC 6761. Ce RFC 6761 impose de lister, pour chaque catégorie de logiciel, en quoi le nom de domaine est spécial. C'est fait dans la section 7 de notre RFC, qui indique que :

— Pour les utilisateurs finaux, pour les applications, pour les serveurs faisant autorité, et pour les résolveurs qui ne font que faire suivre à un résolveur plus gros (ce qui est typiquement le cas de celui des "*boxes*"), rien de particulier, ils et elles peuvent traiter `ipv4only.arpa` comme un domaine normal. Si elles le désirent, les applications peuvent résoudre ce nom `ipv4only.arpa` et apprendre ainsi si un résolveur DNS64 est sur le trajet, mais ce n'est pas obligatoire.

— Les bibliothèques qui gèrent la résolution de noms (comme la libc sur Unix) doivent par contre considérer `ipv4only.arpa` comme spécial. Notamment, elles doivent utiliser le résolveur configuré par le réseau (par exemple via DHCP) pour résoudre ce nom. Le demander à un résolveur public n'aurait en effet pas de sens.
— Les résolveurs qui ne font pas de DNS64 traitent `ipv4only.arpa` comme normal, et leurs clients apprendront donc ainsi que leur résolveur ne fait pas de DNS64.
— Les résolveurs DNS64 vont synthétiser des adresses IPv6 en réponse aux requêtes de type AAAA pour `ipv4only.arpa`, et leurs clients apprendront donc ainsi que leur résolveur fait du DNS64, et sauront quel préfixe IPv6 est utilisé. Ils n'ont pas besoin de consulter les serveurs faisant autorité, qui ne pourraient rien leur apprendre qui n'est pas déjà dans le RFC. L'annexe A du RFC donne un exemple de configuration pour BIND pour attendre cet objectif.

À noter qu'outre `ipv4only.arpa`, notre RFC réserve deux autres noms spéciaux, `170.0.0.192.in-addr.arpa` et `171.0.0.192.in-addr.arpa`, pour permettre la « résolution inverse ». Contrairement à `ipv4only.arpa`, ils ne sont pas actuellement délégués, et un résolveur normal, qui ne connait pas DNS64, répondra donc NXDOMAIN (ce nom n'existe pas).

Sinon, la section 5 de notre RFC est dédiée à la sécurité et note notamment que les noms synthétisés ne peuvent évidemment pas être validés avec DNSSEC. C'est pour cela que la délégation de `ipv4only.arpa` n'est même pas signée. (C'est un changement depuis le RFC 7050, qui demandait au contraire une zone signée, ce que `ipv4only.arpa` avait été au début.)

Vu par les sondes RIPE Atlas <`https://atlas.ripe.net/`>, voici les réponses de résolveurs à ce domaine spécial :

```
% blaeu-resolve -r 1000 -q AAAA ipv4only.arpa
[] : 986 occurrences
[64:ff9b::c000:aa 64:ff9b::c000:ab] : 4 occurrences
[2a01:9820:0:1:0:1:c000:aa 2a01:9820:0:1:0:1:c000:ab] : 1 occurrences
[2a0a:e5c0:0:1::c000:aa 2a0a:e5c0:0:1::c000:ab] : 1 occurrences
Test #24069173 done at 2020-02-24T14:49:43Z
```

Sur mille sondes Atlas, la grande majorité ne trouve pas d'adresse IPv6 pour `ipv4only.arpa` ce qui, comme le nom de domaine l'indique, est le comportement par défaut. Quelques sondes sont derrière un résolveur DNS64, utilisant en général le préfixe bien connu du RFC 7050 (les réponses `64:ff9b::...`), mais parfois d'autres préfixes (NSP - "*Network-Specific Prefix*" - dans la terminologie du RFC 7050).