RFC 9120 : Nameservers for the Address and Routing Parameter Area (”arpa”) Domain

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 octobre 2021. Dernière mise à jour le 4 mai 2022

Date de publication du RFC : Octobre 2021

https://www.bortzmeyer.org/9120.html

Le TLD .arpa sert pour différentes fonctions techniques et est géré directement par l'IAB. Ce RFC décrit un changement dans ses serveurs de noms.

Ce TLD est décrit dans le RFC 3172[1]. Le nom de .arpa fait référence à l'ancien nom de la DARPA, l'agence qui avait financé le développement de l'Internet. Mais, aujourd'hui, il veut dire « *”Address and Routing Parameter Area”* » et le TLD sert à diverses fonctions techniques comme la résolution d'adresses IP en noms de domaine via des sous-domaines comme ip6.arpa. Par exemple, l'adresse IP du serveur Web de l'IAB a pour nom correspondant :

```
% dig -x 2001:1900:3001:11::2c
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53150
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
c.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.1.0.0.3.0.0.9.1.1.0.0.2.ip6.arpa. 3600 IN PTR mail.ietf.org.
```

Comme vous le voyez, dig a inversé l'adresse IP et ajouté ip6.arpa à la fin. .arpa sert également à d'autres fonctions comme le home.arpa du RFC 8375.

Traditionnellement, le domaine .arpa était hébergé sur une partie des serveurs de noms de la racine. Le 22 octobre 2021, voici quels étaient les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour .arpa :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3172.txt

```
% dig +nodnssec NS arpa
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43670
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
arpa.   15910 IN NS b.root-servers.net.
arpa.   15910 IN NS f.root-servers.net.
arpa.   15910 IN NS d.root-servers.net.
arpa.   15910 IN NS l.root-servers.net.
arpa.   15910 IN NS e.root-servers.net.
arpa.   15910 IN NS a.root-servers.net.
arpa.   15910 IN NS c.root-servers.net.
arpa.   15910 IN NS i.root-servers.net.
arpa.   15910 IN NS h.root-servers.net.
arpa.   15910 IN NS g.root-servers.net.
arpa.   15910 IN NS k.root-servers.net.
arpa.   15910 IN NS m.root-servers.net.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Oct 22 20:35:36 CEST 2021
;; MSG SIZE  rcvd: 241
```

Comme vous pouvez le voir, c'était presque tous les serveurs de la racine (si vous aimez les jeux : quel serveur de la racine n'hébergeait pas `.arpa` ?). La raison pour cela est que `.arpa` est critique et doit donc bénéficier d'un hébergement solide. Profiter des serveurs de la racine était donc intéressant. Mais le problème est que ça lie `.arpa` à la racine. On pourrait avoir envie de faire des changements dans les serveurs faisant autorité pour `.arpa` sans toucher aux serveurs de la racine, celle-ci étant encore plus critique (cf. RFC 7720). Le principe de base de notre nouveau RFC est donc : découpler les serveurs DNS de `.arpa` de ceux de la racine (ce qui avait été fait pour `ip6.arpa` il y a dix ans, voir le RFC 5855).

Le changement ne concerne que l'hébergement DNS, pas la gestion de `.arpa` (section 2 de notre RFC), qui reste un TLD critique, et soumis au RFC 3172. Le choix des sous-domaines et de leur administration est inchangé (par exemple, pour `ip6.arpa`, c'est décrit dans le RFC 5855).

La section 3 du RFC décrit le nouveau système. Le principe est de commencer par utiliser des noms différents pour les serveurs, mais qui pointeront vers les mêmes machines, au moins au début. Les nouveaux noms sont dans le sous-domaine `ns.arpa`, on a donc `a.ns.arpa`, `b.ns.arpa`, etc. Aucune modification dans les serveurs ne sera nécessaire pour cette première étape, qui n'affectera que la zone racine et la zone `.arpa`. Comme tous les noms seront dans la zone qu'ils servent, il faudra ajouter de la colle <https://www.afnic.fr/observatoire-ressources/papier-expert/le-dns-ca-colle-ou-ca-> aux réponses DNS (ne pas juste dire « le serveur est `c.ns.arpa` » mais également indiquer son adresse IP). Il n'y a désormais plus de nom de serveur commun à la racine et à `.arpa`, et il sera possible dans le futur de migrer vers d'autres serveurs. (Toujours en respectant le RFC 3172.) Voici l'état actuel :

```
% dig +nodnssec NS arpa

; <<>> DiG 9.16.1-Ubuntu <<>> +nodnssec NS arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15962
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
```

```
;; QUESTION SECTION:
;arpa.   IN NS

;; ANSWER SECTION:
arpa.   517877 IN NS h.ns.arpa.
arpa.   517877 IN NS i.ns.arpa.
arpa.   517877 IN NS k.ns.arpa.
arpa.   517877 IN NS l.ns.arpa.
arpa.   517877 IN NS m.ns.arpa.
arpa.   517877 IN NS a.ns.arpa.
arpa.   517877 IN NS b.ns.arpa.
arpa.   517877 IN NS c.ns.arpa.
arpa.   517877 IN NS d.ns.arpa.
arpa.   517877 IN NS e.ns.arpa.
arpa.   517877 IN NS f.ns.arpa.
arpa.   517877 IN NS g.ns.arpa.

;; Query time: 3 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)
;; WHEN: Wed May 04 08:57:47 CEST 2022
;; MSG SIZE  rcvd: 228
```

Vous pouvez également voir cet état actuel de `.arpa` à l'IANA <https://www.iana.org/domains/root/db/arpa.html> ou bien dans le DNS <https://dns.bortzmeyer.org/arpa/NS>.

Notez enfin que certains des serveurs de `.arpa` autorisent le transfert de zones. Voici une copie faite le 24 octobre 2021 (en ligne sur `https://www.bortzmeyer.org/files/arpa-octobre-2021.zone`).