Un résolveur DNS public en Inde

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 avril 2024

https://www.bortzmeyer.org/resolveur-inde.html

J'avais raté l'information : il y a désormais un résolveur DNS public en Inde, dns.nic.in.

Il ne semble pas y avoir eu beaucoup de communication publique sur ce service mais il fonctionne. Un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> **public** est un résolveur qui est ouvert à toustes et accepte donc des requêtes DNS de n'importe quelle adresse IP. (Un résolveur ouvert fait pareil mais c'est une erreur de configuration ; un résolveur public résulte d'une action volontaire.) Les plus connus sont ceux de grosses entreprises étatsuniennes comme Google (avec son 8.8.8.8) ou Cloudflare (avec son 1.1.1.1). Si on ne veut pas, et avec raison, contribuer à nourrir ces entreprises d'encore plus de données personnelles, sans compter les risques de centralisation de la résolution DNS, on a le choix : on peut avoir son propre résolveur <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>, ou bien utiliser d'autres résolveurs publics comme celui de Yandex <https://dns.yandex.com/> (si on veut envoyer ses données personnelles au FSB plutôt qu'à la NSA), celui d'une entreprise allemande <https://www.bortzmeyer.org/dns-sb.html> ou d'une association française <https://www.bortzmeyer.org/fdn-dot-doh.html>. (Il y en a même un que je gère <https://doh.bortzmeyer.fr/policy>.)

Cette offre importante et variée s'est enrichie (mais je ne sais pas trop quand) d'un résolveur indien. Il est accessible en UDP et TCP avec plusieurs adresses IP <https://dns.bortzmeyer.org/dns.nic.in>. Prenons l'une des plus jolies, 2409::.

```
%  dig @2409:: mastodon.gougere.fr AAAA

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @2409:: mastodon.gougere.fr AAAA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33859
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: d5d69e4575277422010000000661296ca11b1e6683393ded2 (good)
```

```
;; QUESTION SECTION:
;mastodon.gougere.fr. IN AAAA

;; ANSWER SECTION:
mastodon.gougere.fr. 900 IN AAAA 2001:bc8:1202:ce00::1
mastodon.gougere.fr. 900 IN RRSIG AAAA 13 3 900 (
20240522050147 20240323042710 18689 gougere.fr.
YUzJqyzLVFbndBhaFPtxcQZPoFgVynD9BpxukCuYKJzP
PtSzNK/lY3xFvHi44Txda+/KrZiRIr7LvuU46s0RhQ== )

;; Query time: 304 msec
;; SERVER: 2409::#53(2409::) (UDP)
;; WHEN: Sun Apr 07 14:51:22 CEST 2024
;; MSG SIZE  rcvd: 210
```

OK, tout fonctionne, et on peut voir (*"flag"* AD, pour *"Authentic Data"*) que ce résolveur valide avec DNSSEC. Le temps de réponse n'est pas extraordinaire depuis ma machine en France mais il est probable que les gérants de ce serveur ont privilégié leur présence en Inde.

Testons cette hypothèe avec les sondes RIPE Atlas <https://atlas.ripe.net/> :

```
% blaeu-resolve --nameserver 2409:: --displayvalidation --displayrtt --requested 100 \
                    --country IN --old_measurement 69708749   --type AAAA geoponum.com
...
[ (Authentic Data flag)  2001:41d0:301::28] : 33 occurrences Average RTT 27 ms
[TIMEOUT] : 11 occurrences
Test #69708785 done at 2024-04-07T13:01:15Z

% blaeu-resolve --nameserver 2409:: --displayvalidation --displayrtt --requested 100 \
                    --country JP --old_measurement 69708763     --type AAAA geoponum.com
...
[ (Authentic Data flag)  2001:41d0:301::28] : 98 occurrences Average RTT 134 ms
[2001:41d0:301::28] : 1 occurrences Average RTT 897 ms
[TIMEOUT] : 1 occurrences
Test #69708813 done at 2024-04-07T13:03:37Z
```

(On réutilise les sondes d'une mesure précédente, pour augmenter la probabilité que tout soit dans la mémoire du résolveur.) On voit que la latence moyenne est plus basse en Inde qu'au Japon, ce qui est logique. Ce résolveur n'est donc peut-être pas la solution idéale si vous vivez en dehors de l'Inde.

Je l'ai dit, l'offre en matière de résolveurs publics est très diverse et donc les arguments des contempteurs de DoH <https://www.bortzmeyer.org/doh-et-ses-adversaires.html> comme quoi DoH pousserait à la centralisation sont bien à côté de la plaque. Notez aussi que, bien qu'il existe de nombreux résolveurs publics de qualité opérationnels, celui annoncé en fanfare par la Commission Européenne il y a déjà plusieurs années, DNS4EU <https://www.joindns4.eu/>, ne fonctionne toujours pas (Thierry Breton est plus doué pour les annonces que pour l'opérationnel, ce qui était déjà le cas <https://www.liberation.fr/politique/fiasco-datos-au-senat-thierry-breton-fait-sa-det
TU42K7LBTJDFJLKPJ5FWJ3RVFQ/> lorsqu'il dirigeait Atos).

Ah, mais j'ai dit que le résolveur était accessible en UDP et en TCP. Et avec des protocoles chiffrés comme DoT (RFC 7858 [1]) ou DoH (RFC 8484) ?

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7858.txt

```
% kdig +tls @2409:: geoponum.com
;; WARNING: can't connect to 2409::@853(TCP)
;; ERROR: failed to query server 2409::@853(TCP)
```

Ah, zut, pas encore de chiffrement. Mais, en fait, c'est plus compliqué que cela. Il semble que certaines instances du nuage "*anycast*" (cf. plus loin) aient du chiffrement, mais pas les autres. Donc, selon l'adresse IP de service qu'on utilise et l'endroit où on est, on verra du chiffrement ou pas :

```
% kdig +nsid +https=/dns-query @1.10.10.10 geoponum.com
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(RSA-PSS-RSAE-SHA256)-(AES-256-GCM)
;; HTTP session (HTTP/2-POST)-(1.10.10.10/dns-query)-(status: 200)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 0
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1232 B; ext-rcode: NOERROR
;; NSID: 696E2D626F6D2D7331 "in-bom-s1"

;; QUESTION SECTION:
;; geoponum.com.        IN A

;; ANSWER SECTION:
geoponum.com.        3600 IN A 51.91.236.193

;; Received 70 B
;; Time 2024-04-07 16:49:26 CEST
;; From 1.10.10.10@443(TCP) in 613.4 ms
```

Ici, l'instance de Bombay a bien répondu en DoH (son certificat, sans surprise, est un Let's Encrypt).

En demandant le NSID (RFC 5001, on voit que le résolveur est manifestement "*anycasté*" :

```
% blaeu-resolve --nameserver 2409::  --nsid --requested 200 --type AAAA geoponum.com
Nameserver 2409::
[TIMEOUT] : 12 occurrences
[2001:41d0:301::28 NSID: in-amd-s1;] : 134 occurrences
[2001:41d0:301::28 NSID: in-blr-s1;] : 32 occurrences
[2001:41d0:301::28 NSID: in-maa-s1;] : 6 occurrences
[2001:41d0:301::28 NSID: in-maa-s2;] : 3 occurrences
[2001:41d0:301::28 NSID: in-bom-s1;] : 1 occurrences
[2001:41d0:301::28 NSID: in-gau-s1;] : 6 occurrences
[2001:41d0:301::28 NSID: None;] : 3 occurrences
[2001:41d0:301::28 NSID: in-bom-s2;] : 3 occurrences
Test #69708899 done at 2024-04-07T13:10:50Z
```

On voit au moins sept instances différentes. Le schéma de nommage semble être le classique code IATA des aéroports (AMD = Ahmedabad, BLR = Bangalore, etc).

Si on essaie d'obtenir le nom du serveur à partir de son adresse IP, on voit que la zone `0.0.0.9.0.4.2.ip6.arpa` est bien cassée (regardez l'EDE - RFC 8914) :

```
% dig -x 2409::
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 9388
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; EDE: 7 (Signature Expired): (6GJV)
;; QUESTION SECTION:
;0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.0.4.2.ip6.arpa. IN PTR

;; Query time: 4296 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (UDP)
;; WHEN: Sun Apr 07 10:40:34 CEST 2024
;; MSG SIZE  rcvd: 111
```

Outre les signatures DNSSEC expirées, cette zone a plein d'autres problèmes DNS <https://dnsviz.net/d/0.0.0.9.0.4.2.ip6.arpa/ZhJdfg/dnssec/>.

Et les adresses IP sortantes, à partir desquelles le résolveur indien pose des questions aux serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> ? Testons avec le service `ip.dyn.bortzmeyer.fr`, qui renvoie l'adresse IP de son client (du résolveur, donc) :

```
% blaeu-resolve --nameserver 2409::  --nsid --requested 200 --type TXT ip.dyn.bortzmeyer.fr
Nameserver 2409::
["160.202.194.2" NSID: in-amd-s1;] : 140 occurrences
[TIMEOUT] : 10 occurrences
["160.202.198.2" NSID: in-blr-s1;] : 5 occurrences
["2409:e:e7::3" NSID: in-maa-s2;] : 4 occurrences
["240a:eff6::2" NSID: in-blr-s1;] : 23 occurrences
["160.202.200.2" NSID: in-gau-s1;] : 1 occurrences
["180.250.245.54" NSID: None;] : 1 occurrences
["2409:e:e7::2" NSID: in-maa-s1;] : 2 occurrences
["45.249.124.2" NSID: in-maa-s1;] : 1 occurrences
["240a:eff8::2" NSID: in-gau-s1;] : 7 occurrences
["2409:e:e4::2" NSID: in-bom-s1;] : 2 occurrences
["2409:e:e4::3" NSID: in-bom-s2;] : 2 occurrences
["99.212.0.7" NSID: None;] : 1 occurrences
["121.46.96.2" NSID: in-bom-s1;] : 1 occurrences
Test #69709105 done at 2024-04-07T13:26:34Z
```

On voit une grande variété de préfixes, tous enregistrés en Inde, à divers organismes publics.