RFC 6304 : AS112 Nameserver Operations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 juillet 2011

Date de publication du RFC : Juillet 2011

http://www.bortzmeyer.org/6304.html

Le système AS112, autrefois décrit dans ce RFC, est à la fois un utile composant du DNS, améliorant les performances et reduisant la charge du réseau, un banc d'essai pour des nouvelles techniques comme l'"*anycast*", et une expérimentation sociale, celle d'un service 100 % acentré. Il est désormais documenté dans le RFC 7534 [1].

Comme beaucoup de bonnes choses sur l'Internet, la documentation arrive comme les carabiniers, longtemps après. Car l'AS112 tourne depuis des années. Pour comprendre son rôle, il faut d'abord se pencher sur le problème à résoudre.

Un certain nombre de sites connectés à l'Internet utilisent des adresses IP privées, tirées du RFC 1918. Bien des logiciels, lorsqu'ils voient passer un nouveau client, font une résolution DNS pour obtenir le nom du client en fonction de son adresse IP (résolution dite PTR). C'est par exemple le cas du serveur de courrier Postfix, chez qui ce comportement n'est pas débrayable. Lorsque l'adresse IP est privée, il ne sert à rien de poser la question au DNS public. Par définition, celui-ci ne peut pas savoir que MaPetiteEntreprise utilise `192.168.1.0/24` et a attribué `192.168.1.33` à `posteclientX.mapetiteentreprise.com`. La bonne pratique est donc que l'administrateur réseaux d'un site qui utilise ces adresses privées doit configurer des serveurs DNS pour répondre aux requêtes PTR (cf. RFC 6303). Pour voir cela, on peut utiliser l'option `-x` de dig, qui permet de faire automatiquement une résolution d'adresse en nom. Le domaine `in-addr.arpa` (RFC 5855) accueille la forme inversée des adresses (`192.168.1.33` devient `33.1.168.192.in-addr.arpa`). Testons ici une adresse publique :

```
% dig -x 192.134.4.20
...
;; ANSWER SECTION:
20.4.134.192.in-addr.arpa. 172800 IN    PTR     rigolo.nic.fr.
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7534.txt`

Mais beaucoup d'administrateurs réseaux sont négligents, surchargés de travail, incompétents ou les trois à la fois. Ils ne configurent pas ces serveurs DNS et, résultat, la requête PTR sort de leur réseau et va taper sur les serveurs DNS de la racine puis à ceux de `in-addr.arpa`. (Une bonne partie du trafic semble ainsi venir des réseaux 3G, où le "*smartphone*" ne reçoit qu'une adresse privée et où le résolveur DNS qui lui est indiqué ne connait pas les zones correspondantes.) Ceux-ci ont normalement autre chose à faire que de répondre à des requêtes qui sont, dès le départ, des erreurs. Ils délèguent donc à l'AS112, un ensemble de serveurs de noms qui est chargé de répondre « ce nom n'existe pas » à toutes ces requêtes parasites. L'AS112 est donc un **puits** où finissent les erreurs.

On peut voir la délégation de l'AS112 avec dig :

```
% dig NS 168.192.in-addr.arpa

; <<>> DiG 9.7.1 <<>> NS 168.192.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56273
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;168.192.in-addr.arpa.          IN      NS

;; ANSWER SECTION:
168.192.in-addr.arpa.   300     IN      NS      blackhole-2.iana.org.
168.192.in-addr.arpa.   300     IN      NS      blackhole-1.iana.org.

;; ADDITIONAL SECTION:
blackhole-1.iana.org.   3500    IN      A       192.175.48.6
blackhole-2.iana.org.   3500    IN      A       192.175.48.42

;; Query time: 29 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jul  6 12:34:19 2011
;; MSG SIZE  rcvd: 141
```

La délégation va être conservée dans les mémoires caches des résolveurs DNS et la racine ou `in-addr.arpa` ne seront donc plus embêtés, après la première requête.

Mais qui sont ces machines `192.175.48.6` et `192.175.48.42` ? Des très gros serveurs payés par un mécène et installées à un endroit bien connecté ? Pas du tout. C'est ici que rentre en jeu l'AS112. Ce dernier est composé d'un réseau informel de dizaines de machines un peu partout dans le monde et qui annoncent toutes être `192.175.48.6` et `192.175.48.42`. Chacune de ces machines encaisse une partie de la charge. L'AS112 n'a pas de chef, juste un site Web <`http://www.as112.net/`> et, depuis aujourd'hui, un RFC, ce RFC 6304.

L'AS112 doit son nom au numéro de système autonome qui lui a été attribué. Ses serveurs utilisent l'"*anycast*" (RFC 4786) pour distribuer la charge entre eux. Avant Global Anycast <`http://wiki.global-anycast.net/`>, c'était donc le premier projet d'"*anycast*" entre serveurs faiblement coordonnés.

Les détails pratiques, maintenant. La liste des zones servies figure en section 2.1. Elle comprend `10.in-addr.arpa` pour le réseau `10.0.0.0/8`, de `16.172.in-addr.arpa` à `31.172.in-addr.arpa` pour le `172.16.0.0/12`, et `168.192.in-addr.arpa` pour le `192.168.0.0/16`, les préfixes du RFC 1918. Elle inclus aussi `254.169.in-addr.arpa` pour le préfixe « local au lien » du RFC 5735. Pour aider à l'identification du nœud qui répond, les serveurs de l'AS112 servent également la zone `hostname.as112.net`, ici à Paris :

```
% dig +nsid TXT hostname.as112.net

; <<>> DiG 9.7.3 <<>> +nsid TXT hostname.as112.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1078
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hostname.as112.net.            IN      TXT

;; ANSWER SECTION:
hostname.as112.net.     267     IN      TXT     "Unicast IP: 193.17.192.194"
hostname.as112.net.     267     IN      TXT     "See http://as112.net/ for more information."
hostname.as112.net.     267     IN      TXT     "See http://noc.hivane.net/cgi-bin/dsc-grapher.pl for local info
hostname.as112.net.     267     IN      TXT     "Paris, FR"
hostname.as112.net.     267     IN      TXT     "Hivane Networks"

;; AUTHORITY SECTION:
hostname.as112.net.     267     IN      NS      blackhole-2.iana.org.
hostname.as112.net.     267     IN      NS      blackhole-1.iana.org.

;; ADDITIONAL SECTION:
blackhole-1.iana.org.   241     IN      A       192.175.48.6
blackhole-2.iana.org.   241     IN      A       192.175.48.42

;; Query time: 1 msec
;; SERVER: 217.70.184.225#53(217.70.184.225)
;; WHEN: Wed Jul  6 12:36:14 2011
;; MSG SIZE  rcvd: 348
```

On note que les préfixes IPv6 n'y figurent pas. Une des discussions les plus vives sur ce RFC, et qui explique le temps très long qu'il a mis à sortir, portait sur la délégation de préfixes d'`ip6.arpa` à l'AS112. Aucune décision n'a encore été prise et, pour l'instant, notre RFC 6304 décrit l'état actuel de l'AS112 (on peut avoir une liste à jour sur le site officiel <`http://www.as112.net/`>).

La section 2.2 décrit les serveurs de noms qui reçoivent la délégation, joliment (mais incorrectement, puisqu'ils répondent) nommés `blackhole-1.iana.org` et `blackhole-2.iana.org` (en dépit de leurs noms, les serveurs de l'AS112 ne sont pas gérés par l'IANA, cf. section 7). Dans le champ `MNAME` du SOA de la zone déléguée, on trouve également `prisoner.iana.org` dont la tâche principale est de répondre aux mises à jour dynamiques (RFC 2136) que certaines machines envoient audit `MNAME`.

Ce RFC 6304 n'est pas seulement la description d'une technique mais également un HOWTO sur la configuration d'un serveur de l'AS112. De tels textes, prévus pour les administrateurs système, sont rares dans les RFC. La section 3 décrit ainsi tout ce que doit savoir le volontaire qui va créer un nouveau nœud. Il doit connaître BGP (RFC 4271), nécessaire pour l'"*anycast*" (RFC 4786) et la gestion d'un serveur DNS faisant autorité. Les serveurs de l'AS112 peuvent être situés n'importe où mais ils sont surtout utiles dans les endroits bien connectés, notamment les points d'échange. Ils peuvent être locaux (annonçant les routes avec la communauté BGP `no-export`, 0xFFFFFF01, cf. RFC 1997), ou globaux (servant le monde entier). Et naturellement, ils doivent se coordonner (via une liste de diffusion) avec les autres serveurs de l'AS112.

L'AS112 n'impose pas de système d'exploitation particulier (section 3.3) mais tous les serveurs existants semblent utiliser Unix et tous (c'est difficile à dire, puisque l'AS112 ne contrôle pas tout ce qui se

passe sur les serveurs) se servent de BIND. Il est recommandé que la machine AS112 soit dédiée à cette tâche : ces serveurs reçoivent parfois un trafic intense qui pourrait perturber leurs autres activités.

Le serveur signale son existence et sa disponibilité en BGP. Il faut donc coupler le serveur de noms au serveur BGP, pour que l'arrêt du serveur DNS entraîne l'arrêt de l'annonce (le RFC ne fournit pas de script pour cela). Un exemple de comment cela peut se réaliser sur Linux, avec les adresses de l'AS112 attachées à une interface `dummy`, est (code utilisé sur un serveur "*anycast*" réel, quoique pas de l'AS112) :

```
# Load the variables (the machine is a RedHat)
. /etc/sysconfig/network-scripts/ifcfg-eth0

# Test if the name server actually works. Do not use ps: the server
may be there but unresponsive
TMP=(`dig +short +time=1 +tries=1 @${IPADDR} SOA example.`)
MASTER=${TMP[0]:=somethingwaswrong}

# Normal reply or not?
if test ${MASTER} != "nsmaster.nic.example."
then
    # Disable the interface: Quagga will stop announcing the route
    ifdown dummy0
    # Raise an alarm, send SMS, etc
fi
```

Le serveur BGP annonce le préfixe `192.175.48.0/24` qui couvre les adresses de tous les serveurs et l'origine est évidemment 112 <`http://whois.arin.net/rest/asn/AS112/`>.

Les exemples du RFC supposent que le serveur BGP est Quagga mais cela peut évidemment marcher avec d'autres. Dans l'exemple ci-dessous, tiré du RFC (section 3.4), le "*router ID*" est `203.0.113.1` et le serveur BGP a deux pairs, `192.0.2.1` et `192.0.2.2`. Voici un extrait du `bgpd.conf` (la version intégrale est dans le RFC) :

```
   hostname my-router
...
   router bgp 112
    bgp router-id 203.0.113.1
    network 192.175.48.0/24
    neighbor 192.0.2.1 remote-as 64496
    neighbor 192.0.2.1 next-hop-self
    neighbor 192.0.2.2 remote-as 64497
    neighbor 192.0.2.2 next-hop-self
```

En farfouillant sur le site officiel <`http://www.as112.net/`> (pas très bien organisé, je trouve), on peut trouver d'autres exemples.

Le serveur AS112 a ensuite besoin d'un serveur DNS faisant autorité (section 3.5), évidemment compatible avec toutes les règles du DNS (RFC 1034). Les exemples de configuration du RFC sont fondés sur BIND. Voici un extrait du `named.conf` (la version intégrale est dans le RFC) :

```
   options {
     listen-on {
        ...
        // the following addresses correspond to AS112 addresses, and
        // are the same for all AS112 nodes
        192.175.48.1;      // prisoner.iana.org (anycast)
```

```
        192.175.48.6;      // blackhole-1.iana.org (anycast)
        192.175.48.42;     // blackhole-2.iana.org (anycast)
      };
      recursion no;        // authoritative-only server
    };

    // RFC 1918
    zone "10.in-addr.arpa" { type master; file "db.empty"; };
    ...

    // RFC 5735
    zone "254.169.in-addr.arpa" { type master; file "db.empty"; };

    // also answer authoritatively for the HOSTNAME.AS112.NET zone,
    // which contains data of operational relevance
    zone "hostname.as112.net" {
      type master;
      file "db.hostname.as112.net";
    };
```

Un exemple équivalent pour NSD (utilisé sur le nœud AS112 de Paris) est disponible en (en ligne sur `http://www.bortzmeyer.org/files/as112-nsd.conf`). Pour simplifier son écriture, il a été produit à partir d'un source en M4, (en ligne sur `http://www.bortzmeyer.org/files/as112-nsd.conf.m4`).

Que contiennent les fichiers de zone `db.empty` et `db.hostname.as112.net` ? Conformes à la syntaxe de la section 5 du RFC 1035, ils sont communs à BIND et NSD. Le premier, comme son nom l'indique, est un fichier de zone vide, puisque le serveur AS112 ne connait évidemment rien : il ne peut que répondre `NXDOMAIN` (ce nom n'existe pas) à toutes les requêtes. Il ne contient donc que les informations obligatoires à toute zone (SOA, avec une adresse de contact appropriée) et NS. L'autre zone sert au déboguage de l'AS112, lorsqu'on veut obtenir des informations sur le serveur AS112 courant. Un contenu typique est juste composé d'enregistrements TXT :

```
        TXT     "Human AS112 server" "Minas Tirith, Gondor"
        TXT     "Forbidden to orcs and nazguls."
        TXT     "See http://www.as112.net/ for more information."
```

et parfois d'une localisation (cf. RFC 1876). Le résultat sur un site réel étant :

```
% dig ANY hostname.as112.net.

; <<>> DiG 9.7.3 <<>> ANY hostname.as112.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41528
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hostname.as112.net.            IN      ANY

;; ANSWER SECTION:
hostname.as112.net.     604796  IN      LOC     37 58 22.590 N 23 44 43.890 E 100.00m 100m 10m 10m
hostname.as112.net.     604796  IN      TXT     "See http://as112.net/ for more information."
hostname.as112.net.     604796  IN      TXT     "Unicast IP: as112.grnet.gr"
hostname.as112.net.     604796  IN      TXT     "Greek Research & Technology Network" "Athens, Greece"
hostname.as112.net.     604796  IN      SOA     flo.gigafed.net. dns.ryouko.imsb.nrc.ca. 1 604800 60 604800 6048
```

```
hostname.as112.net.     604796  IN      NS      blackhole-2.iana.org.
hostname.as112.net.     604796  IN      NS      blackhole-1.iana.org.

;; AUTHORITY SECTION:
hostname.as112.net.     604796  IN      NS      blackhole-1.iana.org.
hostname.as112.net.     604796  IN      NS      blackhole-2.iana.org.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jul  6 12:51:53 2011
;; MSG SIZE  rcvd: 391
```

(La version intégrale des deux fichiers de zone figure dans le RFC.)

Une fois le nœud installé, il faut évidemment le tester (avec dig, par exemple). Si les réponses aux requêtes PTR sont correctes, mais pas celles aux requêtes pour le nom `hostname.as112.net`, c'est sans doute un problème de routage (on est envoyés sur un autre nœud de l'AS112) et il faut alors sortir traceroute et les "*looking glasses*" (section 3.6). Des tests dignes de ce nom doivent être faits depuis plusieurs FAI, et doivent tester les trois adresses IP de l'AS112.

Le bon fonctionnement de l'AS112 ne dépend pas uniquement de sa configuration initiale mais aussi de sa gestion et surveillance quotidiennes. La section 4 est consacrée aux questions opérationnelles. Le nœud doit être surveillé automatiquement, pour s'assurer qu'il répond toujours. S'il doit être arrêté (par exemple pour une maintenance prévue), il faut s'assurer que l'annonce BGP stoppe (autrement, BGP annonce un trou noir, d'où aucune réponse ne reviendra). Autre point important de la gestion opérationnelle d'un serveur de l'AS112, des statistiques, obtenues à partir d'outils comme DSC <`http://dns.measurement-factory.com/tools/dsc/`> ou dnstop <`http://dns.measurement-factory.com/tools/dnstop/`>. Quelle est l'utilisation réelle de l'AS112 ? Ces statistiques n'étant pas consolidées globalement, c'est difficile à dire. Certains opérateurs publient leurs chiffres mais pas tous. Par exemple, le serveur d'Ottawa voit mille requêtes par seconde (cf. « "*AS112 Intro*" <`https://www.dns-oarc.net/files/workshop-2008/maton.pdf`> » par l'un des auteurs du RFC), celui géré par le RIPE-NCC dans les mille cinq cents <`http://www.ripe.net/data-tools/dns/as112`>, et celui à Paris deux fois plus (voir les graphiques <`http://noc.hivane.net/cgi-bin/dsc-grapher.pl?plot=bynode&server=as112`>), ce qui fait quand même quelques mégabits par seconde. La majorité des types demandés est évidemment du PTR mais il y a aussi un flux important de TXT, apparemment dus à la technologie SD ("*Service Discovery*") d'Apple (voir des statistiques plus détaillées à la fin).

Le nouveau serveur peut alors être annoncé sur les listes appropriées (par exemple, chaque point d'échange a en général la sienne). Enfin, bien que chaque serveur de l'AS112 puisse fonctionner indépendemment des autres, il est évidemment préférable de se coordonner avec les petits camarades (section 5) en écrivant à la liste officielle <`https://lists.dns-oarc.net/mailman/listinfo/as112-ops`>.

Et dans le futur ? La section 6 explore l'avenir possible de l'AS112. Idéalement, il devrait disparaître petit à petit au fur et à mesure que les administrateurs réseaux prennent soin de ne pas laisser fuir les requêtes PTR pour les réseaux privés, comme recommandé dans le RFC 6303. Le déploiement de logiciels respectant ce principe dès le début pourrait aider. Toutefois, aujourd'hui, les opérateurs de l'AS112 n'observent pas de tendance à la baisse du trafic. Même des années après le déploiement de serveurs mettant en œuvre le RFC 6303, il est probable que le trafic de l'AS112 ne tombera pas à zéro et que ce service restera donc nécessaire.

Il pourrait même s'étendre à IPv6 (cela a été fait début 2015) : les serveurs pourraient répondre en IPv6 (et pas seulement en IPv4 comme aujourd'hui). Un préfixe a déjà été alloué pour cela, `2620:4f:8000::0/48`

mais il n'est pas encore publié. Et les serveurs pourraient servir des données de `ip6.arpa`. Rien n'est encore décidé, gardez un œil sur <http://www.as112.net/> si vous voulez être au courant. Un bon exposé du problème est « "*AS112-bis.*" <http://www.ietf.org/proceedings/80/slides/dnsop-3.pdf> » et un plan de déploiement IPv6 est en <http://public.as112.net/node/26>. Quant aux nouveaux domaines délégués, la solution finalement adoptée a été décrite dans le RFC 7535.

Enfin, qu'en est-il de la sécurité ? Comme le rappelle la section 8, les requêtes DNS auxquelles répond l'AS112 ne devraient jamais y arriver, normalement. Elles auraient dû rester sur le réseau local. En sortant, elles exposent de l'information interne, qui était peut-être privée (qu'il y ait un serveur qui y réponde ou pas ne change guère ce risque).

Plus rigolo, comme ces requêtes sont en général involontaires (comme indiqué, elles auraient dû rester privées), les réponses sont inattendues. Plus d'un IDS a donc crié que l'AS112 essayait d'attaquer le réseau. Le RFC 6305 a été écrit pour fournir une réponse toute faite aux administrateurs incompétents qui accusaient l'IANA ou l'AS112.

Comme l'AS112 n'a pas de chef et que l'"*anycast*" ne permet pas de limiter le nombre de participants, il est tout à fait possible de fantasmer sur l'hypothèse d'un nœud AS112 voyou, qui donnerait exprès de mauvaise réponses. Ce problème (purement théorique) n'a pas vraiment de solution. Signer les zones avec DNSSEC semble franchement excessif.

L'annexe A du RFC expose la longue histoire de l'AS112, de ses débuts en 2002 (les adresses IP privées datent de 1996) à son état actuel, après la redélégation en 2011 de `in-addr.arpa`, autrefois sur les serveurs de la racine (RFC 5855). L'AS112 a été le premier déploiement massif de l'"*anycast*" et a donc joué un rôle primordial dans l'évaluation de cette technologie.

On voit que neuf ans ont donc été nécessaires pour documenter ce projet. Une des raisons du retard était la longue discussion pour savoir si le RFC devait documenter l'état actuel de l'AS112 (ce qui a finalement été fait) ou son état souhaité (avec, par exemple, les nouvelles zones IPv6).

À noter que, d'après la liste officielle des sites <http://public.as112.net/node/10>, il existe au moins un serveur AS112 en France, chez Hivane <http://www.hivane.net/>, désormais (novembre 2011) connecté au France-IX. Malgré cela, les requêtes françaises pour les serveurs de l'AS112 voyagent souvent loin. C'est un problème banal comme le montrait l'excellente présentation « "*Investigating AS112 Routing and New Server Discovery*" <https://www.dns-oarc.net/files/workshop-2008/wright.pdf> ».

Voici quelques analyses sur le trafic de ce serveur français, faites avec DNSmezzo <http://www.dnsmezzo.net/>. Le fichier pcap fait 6,8 Go. Il y a 43 701 087 paquets DNS dont 21 858 845 sont des requêtes. Les données ont été prises un vendredi, de 13h40 à 15h30 (heure locale). Regardons d'abord les types de données demandés :

```
dnsmezzo=> SELECT (CASE WHEN type IS NULL THEN qtype::TEXT ELSE type END),
       meaning,
       count(results.id)*100/(SELECT count(id) FROM DNS_packets WHERE query) AS requests_percent FROM
             (SELECT id, qtype FROM dns_packets
                 WHERE query)  AS Results
          LEFT OUTER JOIN DNS_types ON qtype = value
              GROUP BY qtype, type, meaning ORDER BY requests_percent desc;


 type  |                meaning                 | requests_percent
-------+----------------------------------------+------------------
```

```
 PTR   | a domain name pointer                  |              57
 TXT   | text strings                           |              35
 SOA   | marks the start of a zone of authority |               6
 CNAME | the canonical name for an alias        |               0
 MX    | mail exchange                          |               0
 AAAA  | IP6 Address                            |               0
 40    |                                        |               0
 DS    | Delegation Signer                      |               0
 ...
```

La première place des `PTR` est normale. Celle des `TXT` est plus surprenante. En regardant les noms utilisés (`cf._dns-sd._udp.Y.X.243.10.in-addr.arpa`...), on voit qu'ils sont dus à la technique "*Service Discovery*" d'Apple, un système normalement confiné au réseau local mais qui bave beaucoup à l'extérieur.

Et quels sont les domaines les plus populaires ?

```
dnsmezzo=> SELECT substr(registered_domain,1,46) AS domain,
         count(id)*100/(SELECT count(id) FROM DNS_packets WHERE query) AS requests_percent
       FROM dns_packets WHERE query GROUP BY registered_domain ORDER BY requests_percent DESC LIMIT 30;
      domain      | requests_percent
------------------+------------------
 10.in-addr.arpa  |               78
 192.in-addr.arpa |               12
 172.in-addr.arpa |                7
 169.in-addr.arpa |                1
 151.in-addr.arpa |                0
 i~-addr.arpa     |                0
 83.in-addr.arpa  |                0
                  |                0
 gfi.private      |                0
 local.de         |                0
 grupofdez.com    |                0
....
```

On voit que le réseau `10.0.0.0/8` est nettement le plus populaire. On notera les trois derniers, sans doute des erreurs de configuration.

Et quels sont les résolveurs les plus actifs ? En agrégeant les préfixes IPv4 en `/28` :

```
dnsmezzo=>  SELECT set_masklen(src_address::cidr, 28) AS client, count(id)*100/(SELECT count(id) FROM DNS_pa
     FROM dns_packets WHERE query GROUP BY set_masklen(src_address::cidr, 28)
          ORDER by requests_percent DESC LIMIT 30;
       client       | requests_percent
--------------------+------------------
 CENSURE.160/28     |               29
 CENSURE.0/28       |               10
 CENSURE.16/28      |                8
 CENSURE.96/28      |                6
...
```

Oui, j'ai préféré ne pas donner les adresses. Je dirai simplement que ces quatre plus gros sont des opérateurs de téléphonie mobile, deux français et deux extrême-orientaux (les mystères du routage...).

Merci à Clément Cavadore pour les données et pour sa relecture.
