DNS Looking Glass: motivations and explanations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

First publication of this article on 20 January 2013. Last update on of 1 March 2013

http://www.bortzmeyer.org/dns-lg.html

There was a time where getting information about the content stored in the DNS was easy : just fire dig from any machine in the Internet and ask your question. It has never been a perfect solution (because of caching and because of different network connectivity) but it worked most of the time : the DNS was supposed to give the same data to anyone. Now, several recent changes make this solution too limited. We need **DNS Looking Glasses**.

What are these changes ?

— Answers can be different depending on the source IP address of the query, for instance to direct users to a closer server.
— Cache poisoning may have the effect that the users of some resolvers/caches will see a different set of data.
— DNSSEC can have an effect. Today, some resolvers validate and some do not. If a DNS zone administrator makes a mistake, validating resolvers will experience a problem but not the users of non-validating resolvers.
— Lying resolvers can rewrite answers for their users.
— Legal requirments on DNS censorship (both in dictatorships and in democracies) may make some data unavailable (or modified) from some places.

It means we need **DNS Looking Glasses**, points of observation to look at the DNS data from a different viewpoint. Such looking glasses are already very common to observe BGP but not for the DNS. People typically use open resolvers, DNS resolvers open for everyone, for that purpose (for instance, scientific papers analyzing the DNS are often based on surveys with open resolvers). But they create various security problems and that's why the RFC 5358 [1] recommends their closing.

Therefore, I present here three things :

— A proposal for the format of requests and responses of these DNS looking glasses.
— A free program implementing this format.
— An actual service with this software that you can query.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5358.txt

The service is available using the REST paradigm, at `https://dns.bortzmeyer.org/$DOMAIN[/$TYPE]` where DOMAIN is the domain name and TYPE a DNS record type (such as AAAA or MX). For instance, <https://dns.bortzmeyer.org/example.com/AAAA> will get you the AAAA record for the name `example.com`. There is no Web form, you have to construct the URL and send it with a HTTP client (which can be a Web browser or a program like curl ; you do not need a DNS client like dig or drill). Of course, people are welcome to write such a form. The complete documentation of this service is available online <http://www.bortzmeyer.org/dns-lg-usage.html> (for instance, you can change the output format, it does not have to be HTML).

Since the DNS looking glass uses a structured output format, it is quit easy to develop a program which will query the existing looking glasses instances and ask them a question. Such programs are available in the subdirectory usages/ of the distribution <https://github.com/bortzmeyer/dns-lg/tree/master/usages>. For instance, the program `get-ip` asks for the IP addresses of its argument :

```
% ./get-ip www.ietf.org
http://dns-lg.tetaneutral.net/: [64.170.98.30 2001:1890:126c::1:1e]
http://dns.bortzmeyer.org/: [64.170.98.30 2001:1890:126c::1:1e]
http://dns-lg.dk-hostmaster.dk/: [64.170.98.30 2001:1890:126c::1:1e]
http://dnslg.generic-nic.net/: [64.170.98.30 2001:1890:126c::1:1e]
http://dns-lg.vs.uni-due.de/: [64.170.98.30 2001:1890:126c::1:1e]
```

Here, you see the same results from all the instances ?. If you don't, it does not always mean there is someone with nefarious aims in the middle. Some services do send different DNS replies, depending where you ask, in order for instance to balance the load geographically :

```
% ./get-ip pool.ntp.org
http://dns-lg.tetaneutral.net/: [193.52.136.2 213.251.172.92 88.190.219.242 91.121.92.90]
http://dns-lg.dk-hostmaster.dk/: [217.198.219.102 80.196.238.30 94.126.0.23 80.71.132.103]
http://dns.bortzmeyer.org/: [199.7.177.206 204.235.61.9 64.16.214.60 72.8.140.240]
http://dns-lg.vs.uni-due.de/: [176.9.47.150 188.174.232.178 89.238.66.126 89.238.75.57]
http://dnslg.generic-nic.net/: [193.52.136.2 213.251.172.92 88.190.219.242 188.165.211.5]
```

The program is freely available (under a free software license) at the GitHub hosting service <https://github.com/bortzmeyer/dns-lg>. You can install it on your own machines (it requires Python and a few non-standard packages, as well as a WSGI-able server such as Apache or Nginx). This way, we will have many looking glasses around the planet (remember they will not all see the same thing, which is the reason we need several).

By the way, GitHub provides an issue tracker and the recommended way to report bugs, send patches or give advices is to use this tracker. (It apparently requires a GitHub account but it is easier for me to rely on an existing, and nice, tool.) Do not forget to read the existing issues <https://github.com/bortzmeyer/dns-lg/issues> to be sure yours is not a duplicate.

The proposal for the request and response format is in the sources of the above program (specially the "Format-specific things" section of the README). It may be implemented by other programs, free or not. Do note that, at this time (june 2012), it is not yet stable and certainly not "standard" in any way. The output XML format follows partially the format of Internet-Drafts draft-mohan-dns-query-xml <http://tools.ietf.org/id/draft-mohan-dns-query-xml> for the outer elements (plus some extensions) and of draft-daley-dns-schema <http://tools.ietf.org/id/draft-daley-dns-schema> for the resource data. (Other output formats are available, see the documentation <http://www.bortzmeyer.org/dns-lg-usage.html>.)

Here are some existing DNS looking glasses : most are Web-only, with no API to automatize them or to provide an alternative interface, and no structured output :

`http://www.bortzmeyer.org/dns-lg.html`

— <http://www.dns-lg.com/>, structured output, source code available,
— <http://dns-lg.wullink.nl/dns-lg/>, structured output, written in Java,
— <http://www.statdns.com/api/> (REST URLs and a structured output, in JSON)
— <http://114.114.114.114/> (also reachable with the DNS protocol ; managed in China) Example : <http://114.114.114.114/d?dn=www.afnic.fr&type=aaaa>
— <http://dns.comcast.net/dig-tool.php>
— <http://live.icmynet.com/icmynet-dns/>
— <http://www.zonecut.net/dns/index.cgi>
— <http://www.whatsmydns.net/> (this one has REST URLs)
— <http://www.kloth.net/services/dig.php>
— <http://www.hscripts.com/tools/HDNT/dns-record.php>
— <http://www.digwebinterface.com/> (this one has REST URLs)
— <http://networking.ringofsaturn.com/Tools/dig.php> (requires knowing the raw syntax of dig)
— <http://www.a-record.de/> (only A records)