On-line tools to test your DNS setup

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

First publication of this article on 20 September 2010. Last update on of 21 September 2010

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

Even without DNSSEC (which will perhaps become "*de facto*" mandatory in the next years), the setup of DNS is far from obvious for the typical system administrator and many errors are found in the wild. The DNS being very robust, these errors have typically no visible consequences (they may have serious invisible consequences, such as longer than necessary delays in name resolution). But the growing demand for a more reliable Internet makes these errors less and less acceptable. And, with DNSSEC, they will probably have actual and visible consequences for the end users. So, testing the DNS zone that you have just configured is the least you can do, if quality control matters to you. There are many software tools to help the system administrator here but this small article focuses on **online** tools, that you can use from a Web browser.

Testing with dig is far from enough : there are many things that can go wrong and using only dig would require typing dozens of complicated commands. Many tools automate these tests and some of the local tools are very good. My choice to focus on Web services results from two important properties of online tools :

— You do not need to install any software or any library, you just need a browser.
— You have a view of your DNS zone from the outside (many things may work from the inside and break from the outside because, for instance, of BIND's views or badly configured firewalls).

So, let's explore the online, Web-based, solutions. Let me tell you immediately that I'm going to express opinions : not all tools are created equal and some have really significant issues, which make it difficult to recommend them to sysadmins. Either their authors do not know enough about the DNS (which is indeed a complicated beast) or they failed to follow the changes of the Internet in the last ten years. If you disagree with my choices, you can send technical explanations of your opinions to stephane+blog@bortzmeyer.org. (Or discuss it publicly on the dns-operations mailing list <https://lists.dns-oarc.net/mailman/listinfo/dns-operations>.)

OK, now, let's start with the good tools. First, the generic ones, which exercice all the parts of DNS.

DNScheck <http://dnscheck.iis.se/> is a nice tool, with a beautiful interface. (This tool is also available as a local program but I did not test this version.) It indicates clearly whether the error is serious or not and gives good explanations. It supports DNSSEC but, in September 2010, it still does not

support the recent algorithms of type 8 (SHA-256) or 10 (SHA-512) and it claims that `.org`, for instance, is not properly signed (”At least one DNSKEY should be of type RSA/SHA1”, which is wrong). The same software is also used at Pingdom <http://dnscheck.pingdom.com/>.

Zonecheck <http://www.zonecheck.fr/demo> has a plainer interface (in English or in French). It performs many tests and typically catches more errors than most of the other tools (for instance network errors when a packet cannot travel over links with small MTU because a broken firewall blocks ICMP packets). Sometimes, its enthusiasm leads to false positives (for instance when the zone changes rapidly, it complains about the different serial numbers in the authoritative name servers). It also experiences too often network timeouts, if the remote server is not blazingly fast. Among its other possibilities, you can use it to test a zone which is not yet delegated (by specifying the name servers explicitly). But it stays on the one zone you indicate, it does not follow the tree from the parent zones so it cannot be used to debug complicated hierarchy-related issues. Zonecheck supports DNSSEC. (Disclaimer : I work for AFNIC, where most of the Zonecheck development is done.)

There are also tools which are specific and test only a part of the DNS setup, typically DNSSEC.

DNSSEC debugger <http://dnssec-debugger.verisignlabs.com> makes very comprehensive DNSSEC tests and produces good explanations.

A tool even more specific is DNSviz <http://dnsviz.net/>. It visualizes the DNSSEC keys of the zone and its parents, and produces a very good and readable graph of their relationships. Very few tools analyze the entire chain from the root, something which is very important for DNSSEC.

Speaking of specific tools, squish.net DNS checker <http://www.squish.net/dnscheck/> is not really a DNS tester but rather a DNS analyzer, giving to experts (the documentation emphasizes that it is intended only for them) a lot of information about the domain, as seen from the root. Speaking of experts, the Mother of All DNS Checking Web Sites, <http://www.dnscheck.se/>, is still on line but is not for the faint of heart.

Now, there are tools which I cannot recommend.

Cricket Liu, author of the very good O’Reilly book ”DNS and BIND” <http://oreilly.com/catalog/9780596100575/>, is a well-known figure in the world of the DNS so it is not a surprise if Infoblox emphasizes his name on the DNS advisor <http://ww2.infoblox.com/services/dns_advisor_tool.cfm>. Unlike the two previous tools, it requires you to provide a working email address to use it. It fails on IPv6 name servers (claiming ”returned : no nameservers” or ”No A RRs”) which is, in my opinion, not acceptable in 2010, less than a year before the end of the IPv4 address pool <http://www.potaroo.net/tools/ipv4/index.html>.

DNSqueries <http://www.dnsqueries.com/> does many things besides testing the DNS. Like the previous tool, it fails on IPv6 name servers. It also gives a strange advice : ”I found that you have only one MX record. If this mail server goes down this can cause mail delivery delays or even mail loss. This acceptable [sic] but consider increasing the number of your MXs.” But having more than one MX record (and keep them in synch, specially for the anti-spam struggle) is certainly a bad idea for most small and medium organizations. (I wrote a paper in French about it <http://www.bortzmeyer.org/mx-secondaire.html>.) Speaking of spam, this tool still mentions RFC 821 [1] as the authoritative source for SMTP... (The current RFC is RFC 5321.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc821.txt

intoDNS <http://www.intodns.com/> has also the same problems (fails on IPv6 name servers and warns when there is only one MX). More funny, It sends errors when there is no www name in the zone which is quite stupid. And it can not test TLD (it says "Invalid request").

DNSsniffer <http://www.dnssniffer.com/> has exactly the same problems ("Fail. You have 1 mx record listed, this can be a single point of failure.") and some more (for instance, it flags stealth name servers as an error, or it reports as a warning the fact that the name servers of .org do not send glue records for a name server in .net!).

DNSsy <http://dnssy.com/report.php> also fails badly when there are IPv6 name servers. It makes it spit several spurious errors (because each test involving these name servers fails).

What about SolveDNS <http://www.solvedns.com/>? I find it has many spurious answers such as "No name server found that can respond to A Record queries." which I find quite baffling.

Like many of the others, How is my DNS? <http://www.howismydns.com/>, LeafDNS <http://leafdns.com/> or MyDNScheck <http://mydnscheck.com/> produce spurious errors, regarding every IPv6 name server as a broken server. The problem is not that these services do not have IPv6 support (which would be understandable).The problem is that they **fail** when they encounter an IPv6 name server (marking the server as invalid) instead of simply ignoring it (as an IPv4-only DNS resolver would do). For instance, an option "Transport layer" of Zonecheck allows you to disable IPv6 and, in that case, IPv6 name servers are simply ignored.

None of these last tools support DNSSEC.

DNScog <http://dnscog.com/> also has no IPv6 support (which could be understood) but does not know it has no such support and therefore fail badly when a nameserver has an IPv6 address : "Some of the nameservers did not answer any of our queries for your domain.".

DNSreport at DNSstuff <http://www.dnsstuff.com/> is apparently no longer (September 2010) available gratis online. The Domain Health Report <http://www.ultratools.com/> of UltraDNS displays its results only to registered people, so I was not able to test it.

In the category of DNSSEC-specific tools, there are also services I cannot recommend.

DNSSEC monitor <http://www.dnssecmonitor.org/index.php> produces warnings such as "server is using nsec instead of nsec3" as if there were something fundamentally wrong with NSEC. Maybe this is because this tool is made for a local community which decided to promote NSEC3? Also, the "errors" it reports are repeated for every authoritative name server, despite the fact they all serve the same content, which is distracting.

So, my advice is, for generic DNS testing, use DNScheck <http://dnscheck.iis.se/> or Zonecheck <http://www.zonecheck.fr/>. If you are interested only in thorough DNSSEC testing, use DNSSEC debugger <http://dnssec-debugger.verisignlabs.com>.

Thanks to Gilles Massen and Niall O'Reilly for their clever comments.