Blame (and) DNS

Who, where, and how broke your DNS

Petr Špaček • petr.spacek@nic.cz • 2018-02-04
Focus

• Who broke your DNS?
• Not fixing issues, just detecting them
Who is to blame?

Unable to connect

Firefox can’t establish a connection to the server at test.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again
DNS resolution theory

- Resolver → authoritative
DNS resolution with user

- App → OS → resolver → auth
DNS resolution in practice ... almost

- App → OS → forwarder → resolver → auth
DNS resolution reality

- App → OS → "something"
Where to start?

- Use own judgment
- Authoritative end – web app, expected values
- Local end
Authoritative end:

- **http://dnsviz.net** – a DNS "looking glass"
- Enter a DNS name
- "Updated" time → Update now
- Notices
  - ok → look somewhere else
  - errors → bad, call domain owner
  - warnings → likely bad → call domain owner
- Record data – compare with local answer
DNSViz is a tool for visualizing the status of a DNS zone. It was designed as a resource for understanding and troubleshooting deployment of the DNS Security Extensions (DNSSEC). It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool. Your feedback is appreciated.

Enter a domain name

www.example.com  Go »

e.g., www.example.com
Authoritative end:

<table>
<thead>
<tr>
<th>Name</th>
<th><a href="http://www.example.com">www.example.com</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>86400</td>
</tr>
<tr>
<td>Type</td>
<td>A</td>
</tr>
<tr>
<td>Record data</td>
<td>93.184.216.34</td>
</tr>
<tr>
<td>Servers</td>
<td>199.43.133.53, 199.43.135.53, 2001:500:8d::53, 2001:500:8f::53</td>
</tr>
<tr>
<td>Query options</td>
<td>UDP_0_EDNS0_32768_4096</td>
</tr>
<tr>
<td>Status</td>
<td>SECURE</td>
</tr>
</tbody>
</table>
Local machine: Is it a DNS issue?

- Compare
  - $ ping <name>
    - or $ getent hosts <name>
  - $ dig <name>

- ping wrong, dig same as DNSViz
  → not a DNS problem, e.g. broken /etc/hosts

- ping & dig same but different than DNSViz
  → problem beyond OS DNS API
  → next step /etc/resolv.conf
What is next hop?

- `$ cat /etc/resolv.conf`
  - dig's default, override with `@`
  - → localhost → see logs, flush cache
  - weird stuff → ISP/tranzit mocking with DNS → time to change ISP now!
- `$ dig @authority <name>` – compare with DNSViz
- `$ dig @192.0.2.1 <name>` – works?!
- → anything else → CPE/local net/ISP → check config on it/call
Avoid first hop (local thing)

- Ask ISP's resolver directly
- `$ dig @<IP from CPE config> <name>`
- Works
  → CPE/local problem, flush, restart, call ISP
- Doesn't work
  → ISP DNS down? call ISP
Summary

- DNS is Wild West
- Expect unexpected, do not panic
- Use looking glass (DNSViz, SSH, ...)
- Use DNSViz, dig, and common sense

Complain loudly
- the domain owner might not know about the problem
- change ISP if needed

https://github.com/dns-violations/dns-violations/