Influence of Root & TLD Servers on DNS System Performance

RIPE 2003-05-12
Rickard Dahlstrand
rd@tilde.se
Goal of these tests

To investigate how the DNS service behaves and what the consequences are for the end-users when servers at .se or root level is subjected to stress and inconsistencies.
"From the user's point of view, the domain system is accessed through a simple procedure or OS call to a local resolver. The domain space consists of a single tree and the user can request information from any section of the tree.” - (RFC 1034)
DNS query

Client
Request: "IP-address for www.pts.se"

Forwarding server

Response: www.pts.se has IP-address xx

Internet

Name server for the root zone
Response – List of name servers for the .se zone:
SE-DNS.GBG.NETNOD.SE
SUNIC.SUNET.SE
....

Name server for the .se zone
Response – "IP-address for www.pts.se"

Name server for the pts.se zone
Response – List of name servers for the pts.se zone:
....

Name server for the pts.se zone
Response – "IP-address for www.pts.se"

Response – www.pts.se has IP-address xx
Cache Timeouts

Forwarding server

Cache

sunic.sunet.se  ttl= countdown
nic.lth.se  ttl= countdown
ns.uu.net  ttl= countdown
...

Name server for the root-zone

Server startup

request – z110.se?

TTL=2d

request – z111.se?

TTL<2d

request – z112.se?

response – Name servers for .se are:
- sunic.sunet.se  ttl= 2d
- nic.lth.se  ttl= 2d
- ns.uu.net  ttl= 2d
- se-dns.sth.netnod.se  ttl= 2d
- se-dns.gbg.netnod.se  ttl= 2d
- se-dns.mmo.netnod.se  ttl= 2d
- se-dns.svl.netnod.se  ttl= 2d

...
Some TTL values (November 2002)

<table>
<thead>
<tr>
<th>Zon</th>
<th>TTL for NS</th>
<th>TTL for A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>6 days</td>
<td>41 days, 16 hours</td>
</tr>
<tr>
<td>Root about TLD</td>
<td>2 days</td>
<td>2 days</td>
</tr>
<tr>
<td>.se about domains below .se</td>
<td>1 day</td>
<td></td>
</tr>
<tr>
<td>Verisign about domains below .com, .net och .org</td>
<td>2 days</td>
<td></td>
</tr>
<tr>
<td>.NU Domain about domains below .nu</td>
<td>1 day</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.sverigedirekt.riksdagen.se">www.sverigedirekt.riksdagen.se</a></td>
<td>1 day</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.regeringen.se">www.regeringen.se</a></td>
<td>1 day</td>
<td></td>
</tr>
<tr>
<td>www pts.se</td>
<td>1 day</td>
<td></td>
</tr>
<tr>
<td>www tt.se</td>
<td>1 day</td>
<td></td>
</tr>
</tbody>
</table>
Resolver Software

• Bind 9
  - Bind 9.2.0

• Bind 8
  - Bind 8.3.3

• Microsoft
  - DNS service running on Windows 2000 5.00.2195

• Cisco
  - Cisco Registrar DNS 5.5.1
The test environment
The traffic generator
Test 1 - Behavior of resolver at start-up

- **Forwarding server**
  - **Server start**
  - **Config file (root hints)**
  - **Name servers for root**

**request** – Name servers for root?

**response** – Name servers for root are:
- H.ROOT-SERVERS.NET TTL= 6 days
- B.ROOT-SERVERS.NET TTL= 6 days
- ...

- **tid**
  - Always the first server (A-root)
  - Random

---

**Local file with "root hints" used?**

- **Bind 8**: YES
- **Bind 9**: YES
- **MS DNS**: YES
- **CNR**: YES

**When did the update of root servers occur?**

- **Bind 8**: At start-up
- **Bind 9**: After the first request from the client
- **MS DNS**: After the first request from the client
- **CNR**: At start-up

**How did the resolver choose which server to use from the "root hints"?**

- **Bind 8**: Random
- **Bind 9**: Random
- **MS DNS**: Random
- **CNR**: Always the first server (A-root)
Test 2 - Method for choosing root server

**Method:** Approx 200 requests to different servers. The first 20 request were discarded.

**Note:** I-root had the best response time from the test network.
Test 3 - Method for choosing tld server

<table>
<thead>
<tr>
<th></th>
<th>nic.lth.se</th>
<th>ns.eu.net</th>
<th>ns.uu.net</th>
<th>se-dns.gbg.netnod.se</th>
<th>se-dns.sth.netnod.se</th>
<th>sunic.sunet.se</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIND 8</td>
<td>2%</td>
<td>7%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>88%</td>
</tr>
<tr>
<td>BIND 9</td>
<td></td>
<td></td>
<td></td>
<td>1%</td>
<td>10%</td>
<td>89%</td>
</tr>
<tr>
<td>MS DNS</td>
<td></td>
<td></td>
<td></td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco CNR</td>
<td>20%</td>
<td>12%</td>
<td>10%</td>
<td>12%</td>
<td>12%</td>
<td>34%</td>
</tr>
</tbody>
</table>

Method: Approx 100 requests to different servers. The first 20 request where discarded.

Note: sunic.sunet.se had the best response time from the test network.
Test 4 - Absence of all root-servers but one

<table>
<thead>
<tr>
<th>Got response?</th>
<th>Bind 8</th>
<th>Bind 9</th>
<th>MS DNS</th>
<th>CNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Did if search thru the root list until a server was found?</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Time out between requests?</td>
<td>4 sec</td>
<td>2 sec</td>
<td>3 sec</td>
<td>4 sec</td>
</tr>
</tbody>
</table>
Test 5- Absence of all root-servers at start-up

<table>
<thead>
<tr>
<th>Method of selecting which root-server to try next</th>
<th>Bind 8</th>
<th>Bind 9</th>
<th>MS DNS</th>
<th>CNR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Random</td>
<td>Random</td>
<td>Random</td>
<td>In order (a-m)</td>
</tr>
<tr>
<td>Time-out between request</td>
<td>4-8 sec ...</td>
<td>2 sec, 8 sec after 52 sec...</td>
<td>3 sec, ..</td>
<td>4 sec, ..</td>
</tr>
</tbody>
</table>
Test 6 - Absence of all root-servers but one while running

If the following are true does the resolver answer queries:
- One root server is reachable
- All TTL have expired for cached information about the TLD name server

<table>
<thead>
<tr>
<th></th>
<th>Bind 8</th>
<th>Bind 9</th>
<th>MS DNS</th>
<th>CNR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
Test 7 - Absence of all root-servers while running

If the following are thru does the resolver answer queries:

- Root servers are not reachable
- All TTL have expired for cached information about the TLD name server

<table>
<thead>
<tr>
<th></th>
<th>Bind 8</th>
<th>Bind 9</th>
<th>MS DNS</th>
<th>CNR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
Test 8 - Packet-loss

Client

DNS-testtool

Forwarding server

Name servers

Time out = 60 sec

request – z110.se?

response – z110.se?
Distribution of response times at 0% packet-loss

Antal anrop

Svarstid (s)

Antal anrop

Bind 8  Bind 9  Microsoft  Cisco
Distribution of response times at 2% packet-loss

Antal anrop

Svarstid (s)

Bind 8
Bind 9
Microsoft
Cisco
Distribution of response times at 10% packet-loss
Distribution of response times at 20% packet-loss

Antal anrop

Svarstid (s)

Antal anrop

Bind 8

Bind 9

Microsoft

Cisco
Distribution of response times at 50% packet-loss

Time out = 60 s

Antalet anrop

Svarstid (s)

Bind 8
Bind 9
Test 9 - 5 seconds packet delays

Svarstid (s) vs Antal anrop

- Bind 8
- Bind 9
- Microsoft
- Cisco
Test 10 - Absence of all root-servers while running when a the TLD name server is cached.

If the following are thru does the resolver answer queries:

- Root servers are not reachable
- All TTL have expired for cached information about the root name server
- All TTL have expired for cached information about the target
- TTL has not expired for cached information about the TLD name server

<table>
<thead>
<tr>
<th>Bind 8</th>
<th>Bind 9</th>
<th>MS DNS</th>
<th>CNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
What if all tld servers are unavailable?

Percentage of resolvers that are down.

- prerequisites
  - No re-starts of the resolvers.
  - This implies that the TLD is up to date and cached. TLD that are not in the cache are not available at all.
  - The TTL for the TLD name server are 48 hours
  - etc...
The "expire"-value

<table>
<thead>
<tr>
<th>Zon</th>
<th>Expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>rot</td>
<td>7 days</td>
</tr>
<tr>
<td>.se</td>
<td>28 days</td>
</tr>
<tr>
<td>.com</td>
<td>7 days</td>
</tr>
<tr>
<td>.nu</td>
<td>30 days</td>
</tr>
</tbody>
</table>
Client applications - Email

1. SMTP

2. smtp

3. POP/IMAP

MAIL.E1.SE

adam@E1.SE

MAIL.E2.SE

bertil@E2.SE
Client applications - Web

”Förbjud barn att ha mobiltelefoner”

”17-åringen skyldig till minst ett av morden”

’Washington: Nu riktar misstankarna mot kryptkyttens styvson
Aklagaren: 17-åringen holl i vapnet vid minst ett av morden.

Akzo Nobel säljer ut - 180 fär gå

’180 anställda i Malmö förlorar sina jobb Akzo Nobel säljer delar av sin verksamhet.”
Client applications - Web

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings. If you would like Windows to try and discover them, click Detect Network Settings.
- Some sites require 128-bit connection security. Click the Help menu and then click About Internet Explorer to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the Tools menu, and then click Internet Options. On the Advanced tab, scroll to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.
- Click the back button to try another link.
Client applications - Web
Conclusions

The DNS system is well designed and works very well in practice.

DNS handles network disturbances very well.

All tested resolvers did what they where expected to do and did if well.

Most applications are dependent on DNS and does not work very well without it.

There is no easy way to replace DNS if it fails.
More information about the tests

This presentation and the full test specification (in Swedish) are provided at:

http://www.iis.se/meta/english.shtml

http://www.learnswedish.nu

For questions contact me:
r@tilde.se