D-mystifying the D-Root Address Change

Matthew Lentz, Dave Levin, Jason Castonguay, Neil Spring, Bobby Bhattacharjee

University of Maryland
Domain Name System (DNS)

Top-Level Domains

- arpa
- edu
- com
- gov

Root

...
Domain Name System (DNS)

Top-Level Domains

Root

Resolver

Q: www.umd.edu.
Domain Name System (DNS)

Resolver

Q: www.umd.edu.
Domain Name System (DNS)

Root Zone

A B C D E F G H I J K L M
Root Server Anycasting

Root Zone

A B C D E F G H I J K L M
Anycasting enables global server replication
Root Server Anycasting

Root Zone

Anycasting enables global server replication
Root Server Anycasting

Anycasting enables global server replication
Root Server Anycasting

Anycasting enables global server replication

D-Root required IP address change
Root Server Anycasting
Updating Resolvers: Out-of-Band
# Updating Resolvers: Out-of-Band

1. Obtain the root hints file

<table>
<thead>
<tr>
<th>Domain</th>
<th>TTL</th>
<th>Type</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>3600000</td>
<td>NS</td>
<td>D.ROOT-SERVERS.NET.</td>
</tr>
<tr>
<td>D.ROOT-SERVERS.NET.</td>
<td>3600000</td>
<td>A</td>
<td>199.7.91.13</td>
</tr>
<tr>
<td>D.ROOT-SERVERS.NET.</td>
<td>3600000</td>
<td>AAAA</td>
<td>2001:500:2D::D</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Diagram showing resolver process](chart.png)
Updating Resolvers: In-Band

2. Issue priming query to known root server

```
;; ANSWER SECTION:
.      518400 IN NS d.root-servers.net.

;; ADDITIONAL SECTION:
d.root-servers.net. 3600000 IN A 199.7.91.13
... 
```

![Diagram showing resolver, A, D-Root, and M connections with query Q: . IN NS](Image)
Updating Resolvers: In-Band

New

A ... D-Root ... M
D-Root Address Change

New

A \quad \cdots \quad \text{D-Root} \quad \cdots \quad M
D-Root Address Change

Serves queries on both addresses
Experimental Setup

New     Old

D-Root
Experimental Setup

Internet \rightarrow Queries/Responses

- Detect Resolver Update
- Capture Traffic Samples

D-Root

New \rightarrow Old
The Changeover

![Graph showing queries per second over days since address change. The graph indicates a significant drop in queries shortly after the address change.]
Expected Behavior

- Overall
- Old Address
- New Address

Queries per Second

Days Since Address Change

Friday, October 25, 13
Expected Behavior

- Overall
- Old Address
- New Address

Queries per Second

Days Since Address Change
Reality

Days Since Address Change

Queries per Second

Overall
Old Address
New Address
Reality

![Graph showing queries per second over days since address change. The graph has three lines representing Overall, Old Address, and New Address. The y-axis represents queries per second ranging from 5k to 40k, and the x-axis represents days since the address change ranging from 0 to 6.](image)
Reality

Overall query volume increases

Queries per Second

Days Since Address Change
Reality

Overall query volume increases
Resolvers still query old address
Reality

Overall query volume increases

Resolvers still query old address
Reality

Overall query volume increases

Resolvers still query old address
Reality

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often
Why ... ?

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often
Why ...?

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often
Why does query volume increase?

New Resolvers and/or More Queries
Why does query volume increase?

New Resolvers

and/or

More Queries

Actually, unique resolvers decreased
QPS - 24 Hours Before/After

![Graph showing the relationship between QPS on Day Before and QPS on Day After. The graph is on a log-log scale, with QPS on Day After on the y-axis and QPS on Day Before on the x-axis. The graph shows a straight line indicating a direct proportionality.]
QPS - 24 Hours Before/After

The diagram shows a scatter plot with a logarithmic scale on both axes. The x-axis represents QPS on Day Before, ranging from $10^{-4}$ to $10^2$. The y-axis represents QPS on Day After, also ranging from $10^{-4}$ to $10^2$. The plot includes several lines indicating growth factors, such as 1x, 2x, 10x, and 100x, which show how QPS values change between the two days.
Excitables

Accounts for the increase in query volume
Excitables Explained by ... ?
Excitables Explained by ... ?

Couldn’t
Fingerprint
Excitables Explained by ... ?

Couldn’t Fingerprint

Popular in Europe
Excitables Explained by ... ?

“Spike” Query Distribution

Couldn’t Fingerprint

Popular in Europe
Excitables Explained by ... ?

“Spike” Query Distribution

Couldn’t Fingerprint

Frequently Re-Primes

Popular in Europe
Why ... ?

Overall query volume increases

Resolvers still query old address

Queries to old address fail less often
Why ...?

Overall query volume increases
Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often
Why ... ?

Overall query volume increases
Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often
Who’s still using the old address?

Expect most resolvers to update correctly
Who’s still using the old address?

Expect most resolvers to update correctly
Who’s still using the old address?

Expect most resolvers to update correctly

- 63% Old
- 9% Both
- 28% New
Who’s still using the old address?

Expect most resolvers to update correctly.
Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxsnue
...

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...

Friday, October 25, 13
Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxsnue
...

Random

Always Fail

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...

Friday, October 25, 13
### Barnacles: Feature Selection

<table>
<thead>
<tr>
<th>Random</th>
<th>Always Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>kp8goqfsz2skj.sukaxdmziq</td>
<td></td>
</tr>
<tr>
<td>gfpb4fimbreso.qlbkgxsnuе</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNSBLs</th>
<th>Always Succeed</th>
</tr>
</thead>
<tbody>
<tr>
<td>210.33.31.50.bl.spamcop.net</td>
<td></td>
</tr>
<tr>
<td>85.180.105.46.zen.spamhaus.org</td>
<td></td>
</tr>
</tbody>
</table>

...
Barnacles: Feature Selection

kp8goqfsz2skj.sukaxdmziq
gfpb4fimbreso.qlbkgxs nue
...  

210.33.31.50.bl.spamcop.net
85.180.105.46.zen.spamhaus.org
...  

Random                Always Fail

DNSBLs                Always Succeed

Query Diversity  Failure Rate
What should root servers expect?

Expected area if correctly caching
Classifying “Normals”

Query Domain Name Diversity vs. Fraction of Failed Queries

0 0.2 0.4 0.6 0.8 1
0 0.2 0.4 0.6 0.8 1

Friday, October 25, 13
Classifying “Normals”

![Graph showing query domain name diversity against the fraction of failed queries.](image-url)
Classifying “Barnacles”
Classifying “Barnacles”

Majority have <10% failures
Classifying “Barnacles”

Majority have <10% failures

Like “Normals”, but do not prime
Classifying “Barnacles”

Majority have <10% failures

Like “Normals”, but do not prime

Queries from a small set

Query Domain Name Diversity vs. Fraction of Failed Queries
Why ... ?

Overall query volume increases

Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often
Why ... ?

Overall query volume increases

Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often

Barnacles due to misconfigurations, bugs, scanners, etc
Summary

Overall query volume increases
Excitables pointed to bug in PowerDNS

Resolvers still query old address

Queries to old address fail less often
Barnacles due to misconfigurations, bugs, scanners, etc

http://www.cs.umd.edu/projects/droot
Resolver Query Ratio

Graph showing the query ratio of old versus new queries with respect to the fraction of sources. The graph has two curves: one for all sources and another for the top 10% by volume.
Classifying "Swappers"