

DNS

David Malone

19th October 2004

Names vs. Addresses

- Computers like addresses eg. 134.226.81.11.
- People prefer names salmon.maths.tcd.ie.
- Need a way to translate.
- walton.maths.tcd.ie close to salmon.maths.tcd.ie.
- 134.226.81.11 close to 134.226.81.12.

hosts file

Originally hosts file listed names and addresses:

```
127.0.0.1    localhost
128.4.1.1    rackety.udel.edu
129.132.2.21  swisstime.ethz.ch
134.226.32.57  burke.cs.tcd.ie
134.226.81.9   bell.maths.tcd.ie bell
134.226.81.10  walton.maths.tcd.ie walton
134.226.81.11  salmon.maths.tcd.ie salmon
```

(actually without dotted bits). Downloaded from NIC.

DNS

Domain Name System is hierarchical distributed database.

- Hierarchy: `www.google.com` under `google.com` under `com` under ‘.’
- Distributed: responsibility delegated to ‘owners’.
- Database: allows requesting types of information about domains.

Based on the notion of root servers.

Example query

Who is `www.google.com`? \Rightarrow root server

\Leftarrow com servers are ...

Who is `www.google.com`? \Rightarrow com server

\Leftarrow google.com servers are ...

Who is `www.google.com`? \Rightarrow google server

\Leftarrow `www.google.com` is ...

Query types

For each domain can ask for:

A Addresses.

TXT Addresses.

NS Name of name server.

MX Name of mail server.

CNAME For aliases.

PTR Name corresponding to address.

Reverse query

Want to translate 134.226.81.11 to name?

Look up 11.81.226.134.in-addr.arpa.

PTR for 11.81.226.134.in-addr.arpa? \Rightarrow root server

\Leftarrow 134.in-addr.arpa servers

PTR for 11.81.226.134.in-addr.arpa? \Rightarrow 134.in-addr.arpa server

\Leftarrow 226.134.in-addr.arpa servers

PTR for 11.81.226.134.in-addr.arpa? \Rightarrow 226.134.in-addr.arpa server

\Leftarrow 81.226.134.in-addr.arpa server

PTR for 11.81.226.134.in-addr.arpa? \Rightarrow 81.226.134.in-addr.arpa server

\Leftarrow salmon.maths.tcd.ie

Players in DNS game

Clients Make simple queries like 'MX for hotmail.com'.

Recursive Servers Answer simple queries by querying root and following delegation.

Authoritative Servers Know the answers (and delegations) for particular collection of names.

Two types of authoritative: masters (primary) and slaves (secondary). Slaves copy data from masters using zone transfer.

DNS Tricks

- DNS allows caching.
- Forward and reverse need not match. Some people do double lookups.
- Zone transfers some times restricted.
- Answers relatively easy to fake. *DNS spoofing*.
- DNS TSIG and DNS SEC (coming soon) are supposed to address this.
- Some people use DNS for load balancing, where answer depends on business of servers, address of person making query, ...

DNS Politics

- Control ultimately rests in root zone (ICANN, IANA, US Gov).
- Contracts to run .com, .net, ...
- Most countries delegated pre-Internet-boom.
- Some actions have annoyed constituency.
- Continual discussions of future of gTLDs and ccTLDs.
- Infrastructure becoming more robust.
- Other databases exist, such as whois.

```
;; QUESTION SECTION:
;11.81.226.134.in-addr.arpa. IN PTR
;; AUTHORITY SECTION:
arpa. 518400 IN NS A.ROOT-SERVERS.NET.
arpa. 518400 IN NS H.ROOT-SERVERS.NET.
arpa. 518400 IN NS C.ROOT-SERVERS.NET.
arpa. 518400 IN NS G.ROOT-SERVERS.NET.
arpa. 518400 IN NS F.ROOT-SERVERS.NET.
arpa. 518400 IN NS B.ROOT-SERVERS.NET.
arpa. 518400 IN NS K.ROOT-SERVERS.NET.
arpa. 518400 IN NS L.ROOT-SERVERS.NET.
arpa. 518400 IN NS M.ROOT-SERVERS.NET.
arpa. 518400 IN NS I.ROOT-SERVERS.NET.
arpa. 518400 IN NS E.ROOT-SERVERS.NET.
arpa. 518400 IN NS D.ROOT-SERVERS.NET.
;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.4
H.ROOT-SERVERS.NET. 3600000 IN A 128.63.2.53
C.ROOT-SERVERS.NET. 3600000 IN A 192.33.4.12
G.ROOT-SERVERS.NET. 3600000 IN A 192.112.36.4
F.ROOT-SERVERS.NET. 3600000 IN A 192.5.5.241
B.ROOT-SERVERS.NET. 3600000 IN A 192.228.79.201
K.ROOT-SERVERS.NET. 3600000 IN A 193.0.14.129
L.ROOT-SERVERS.NET. 3600000 IN A 198.32.64.12
M.ROOT-SERVERS.NET. 3600000 IN A 202.12.27.33
I.ROOT-SERVERS.NET. 3600000 IN A 192.36.148.17
E.ROOT-SERVERS.NET. 3600000 IN A 192.203.230.10
D.ROOT-SERVERS.NET. 3600000 IN A 128.8.10.90
```

```
;; QUESTION SECTION:  
;11.81.226.134.in-addr.arpa. IN PTR
```

```
;; AUTHORITY SECTION:
```

```
134.in-addr.arpa. 86400 IN NS chia.ARIN.NET.  
134.in-addr.arpa. 86400 IN NS dill.ARIN.NET.  
134.in-addr.arpa. 86400 IN NS BASIL.ARIN.NET.  
134.in-addr.arpa. 86400 IN NS henna.ARIN.NET.  
134.in-addr.arpa. 86400 IN NS indigo.ARIN.NET.  
134.in-addr.arpa. 86400 IN NS epazote.ARIN.NET.  
134.in-addr.arpa. 86400 IN NS figwort.ARIN.NET.
```

```
;; QUESTION SECTION:  
;1. 81.226.134.in-addr.arpa. IN PTR
```

```
;; AUTHORITY SECTION:  
226.134.in-addr.arpa. 86400 IN NS ns.maths.tcd.ie.  
226.134.in-addr.arpa. 86400 IN NS ns1.ucd.ie.  
226.134.in-addr.arpa. 86400 IN NS ns2.tcd.ie.  
226.134.in-addr.arpa. 86400 IN NS ns.eu.net.  
226.134.in-addr.arpa. 86400 IN NS ns.tcd.ie.
```

```
;; QUESTION SECTION:
;11.81.226.134.in-addr.arpa. IN PTR

;; ANSWER SECTION:
11.81.226.134.in-addr.arpa. 86400 IN PTR salmon.maths.tcd.ie.

;; AUTHORITY SECTION:
81.226.134.in-addr.arpa. 86400 IN NS ns.maths.tcd.ie.
81.226.134.in-addr.arpa. 86400 IN NS ns1.tcd.ie.
81.226.134.in-addr.arpa. 86400 IN NS sec02.ns.esat.net.

;; ADDITIONAL SECTION:
ns.maths.tcd.ie. 86400 IN A 134.226.81.11
ns.maths.tcd.ie. 86400 IN AAAA 2001:770:10:300::86e2:510b
ns1.tcd.ie. 86400 IN A 134.226.1.114
```