DNS Root NameServers

An Overview
Dr. Farid Farahmand
Updated: 9/24/12
Who-is-Who!

- Over half million networks are connected to the Internet – 5 billion users by 2015!
- Network numbers are managed by ICANN (Internet Corporation for Assigned Names and Numbers) – [http://www.icann.org/](http://www.icann.org/)
  - Delegates part of address assignments to regional authorities called registrars
    - Registrars are authorized by ICANN to assign blocks of addresses
    - IP address blocks are given to ISPs and companies
    - ISPs distribute individual addresses to users and organizations
ICANN Organization

• The Internet Corporation for Assigned Names and Numbers (ICANN)
  – ICANN is a non-profit organization
  – It is under a contract with DoC (U.S. department of commerce)
    • The United States Department of Commerce who must approve all changes requested to addressing (Zone files) by ICANN.
  – Responsible for coordinating the Internet's systems of unique identifiers, including the systems of domain names and numeric addresses that are used to reach computers on the Internet
• ICANN assigns address blocks to regional Internet registries (RIR)
  – There are five RIR (e.g., Africa or US-Canada)
  – In U.S. RIR is called The American Registry for Internet Numbers (ARIN)
IANA Function

• The ICANN is under contract (since 1998) with the United States Department of Commerce to perform the IANA function
  – Internet Assigned Numbers Authority – IANA
• The IANA functions includes
  – Internet Protocol (IP) address space allocation,
  – protocol identifier assignment
  – generic (gTLD) and country code (ccTLD) Top-Level Domain name system management
  – root server system management functions
ARIN & AS

- In U.S. Regional Internet Registries is called **The American Registry for Internet Numbers** (ARIN)
- ARIN manages the distribution of Internet number resources, including IPv4 and IPv6 address space and AS numbers
  - **Autonomous System** (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators
  - Example: AT&T has AS# 7018
  - Border Gateway Protocol (BGP) uses the AS# for routing purposes
Nameserver

• The entire Internet is managed through special **hierarchical addressing** system
• In order to reach a destination, each request must find out about the IP address of the domain (destination’s physical location) it is trying to reach
• Thus, before sending a request, the source must perform a query to learn about the IP address of the destination node
  – The queries (questions) are sent to authoritative **nameservers**
• An **authoritative nameserver** is a name server that gives answers in response to questions asked about names in a zones
  – Authoritative only
    • Only answer to queries about a zone
  – Caching name server
    • They are configured to give authoritative answers to queries for some zones and act as a caching name server for all other zones.
• **DNS zones** may consist of only one domain, or may comprise many domains and sub-domains
  – Each Zone is defined by a Zone File
• A **Zone File** contains specification for host addressing, name aliasing, electronic mail routing, backup server systems, geographic location, administrative contacts, and many other pieces of information
  – Each entry has a DNS record types (e.g., A=address record; MX=Mail exchange record)
• The **Root Zone** is controlled by the United States Department of Commerce who must approve all changes to the root zone file requested by ICANN.
A fully qualified domain name (FQDN)

- A fully qualified domain name (FQDN) is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS)
  - It is an authoritative name server
  - It specifies all domain levels
  - For example, given a device with a local hostname myhost and a parent domain name example.com, the fully qualified domain name is myhost.example.com
  - The FQDN therefore uniquely identifies the device —while there may be many hosts in the world called myhost, there can only be one myhost.example.com.
  - In DNS zone files, a fully qualified domain name is specified with a trailing dot. For example, myhost.example.com.
The obvious question is how does DNS operation actually take place?
  – Using DNS software

Berkeley Internet Name Domain (BIND) is the de facto standard for running DNS on Unix-like OS
  – Developed by four graduate students at the Computer Systems Research Group at Berkeley

A new version of BIND (BIND 9) was written by the ISC (Internet Systems Consortium, Inc.,) from scratch
  – Included new features: IPv6, remote name daemon control, etc.

All Zone-files, thus follow BIND-style
NSD Software

- Another notable software is NSD for *name server daemon*
  - Daemon is a background process that handles requests for service
- NSD is an open-source server program for the Domain Name System
  - Developed by NLnet Labs of Amsterdam
  - Uses the standard TCP/UDP port 53
  - Latest version is 3
  - Main advantage is *more efficient memory usage*: e.g., for serving domains, NSD can save significant RAM space (PROJECT IDEA)
  - Remember: It is all about cache!
- Three root nameservers have switched from BIND to NSD
  - k.root-servers.net
  - h.root-servers.net (there are three H1, H2, H3)
  - l.root-servers.net

http://www.nlnetlabs.nl/projects/nsd/index.html
Finding the IP Address for a Domain
(Name Resolution)

1. User types www.technowidgets.com in browser
2. Browser queries DNS server to get IP address
3. DNS server queries root server to find IP address of COM server
4. DNS server queries COM server to find IP address of technowidgets.com server
5. DNS queries technowidgets.com server to find IP address of www
6. IP address for www.technowidgets.com is sent back to browser

Root nameserver
E.g., a-root-server.com

TLD; e.g.,
a-gTLD-server.net

E.g., ns1-tnwgt.net
Example of Hierarchical Naming

DNS Root nameserver
e.g., DNS server: 192.5.5.241 (f.root-servers.net.)

DNS TLD:
e.g., a.gtld-servers.net
with two IP address
IPv4: 192.5.6.30,
IPv6: 2001:503:a83e::2:30

A second-level domain (SLD) – it refers to the organization that registered the domain name
e.g.,

A third-level domain

ru.wikipedia.org.
Example of Hierarchical Naming

DNS Root nameserver
e.g., DNS server: 192.5.5.241 (f.root-servers.net.)

DNS TLD:
e.g., a.gtld-servers.net
with two IP address
IPv4: 192.5.6.30,
IPv6: 2001:503:a83e::2:30
There are currently 13 root name servers specified, with names in the form `letter.root-servers.net`, where `letter` ranges from A to M.
There are currently **13** root name servers specified, with names in the form `letter.root.servers.net`, where *letter* ranges from A to M.

<table>
<thead>
<tr>
<th>Letter</th>
<th>IPv4 address</th>
<th>IPv6 address</th>
<th>AS number</th>
<th>Old name</th>
<th>Operator</th>
<th>Location</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>198.41.0.4</td>
<td>2001:503:ba3e:2:30</td>
<td>AS10836</td>
<td>ns.intonic.net</td>
<td>Verisign</td>
<td>Distributed using anycast 5/0</td>
<td>BIND</td>
</tr>
<tr>
<td>B</td>
<td>192.228.70.201 (since January 2004; originally was 128.0.0.107)[3]</td>
<td>2001:478.55:53 (not in root zone yet)</td>
<td>none</td>
<td>ns1.list.edu</td>
<td>USIC-KSI</td>
<td>Marina Del Ray, California, U.S. 0/1</td>
<td>BIND</td>
</tr>
<tr>
<td>C.P</td>
<td>192.33.4.12</td>
<td>2001:500:2:c (not in root zone yet)</td>
<td>AS2146</td>
<td>cpsi.net</td>
<td>Cogent Communications</td>
<td>Distributed using anycast 5/0</td>
<td>BIND</td>
</tr>
<tr>
<td>D.P</td>
<td>128.8.10.90</td>
<td>2001:500:2:d:d</td>
<td>AS27</td>
<td>term.unm.edu</td>
<td>University of Maryland</td>
<td>College Park, Maryland, U.S. 1/0</td>
<td>BIND</td>
</tr>
<tr>
<td>E</td>
<td>192.203.230.10</td>
<td>N/A</td>
<td>AS247</td>
<td>ns.nasa.gov</td>
<td>NASA</td>
<td>Mountain View, California, U.S. 1/0</td>
<td>BIND</td>
</tr>
<tr>
<td>G.P</td>
<td>192.112.36.4</td>
<td>N/A</td>
<td>AS5927</td>
<td>ns.nic.ddn.mil</td>
<td>Defense Information Systems Agency</td>
<td>Distributed using anycast 6/0</td>
<td>BIND</td>
</tr>
<tr>
<td>J</td>
<td>192.58.128.30 (since November 2002; originally was 198.41.0.10)</td>
<td>2001:500:27:2:30</td>
<td>AS26415</td>
<td>Verisign</td>
<td>Distributed using anycast 63/7</td>
<td>BIND</td>
<td></td>
</tr>
<tr>
<td>L.P</td>
<td>199.7.83.42 (since November 2007; originally was 198.33.64.12)[9]</td>
<td>2001:500:3:42</td>
<td>AS20144</td>
<td>ICANN</td>
<td>Distributed using anycast 37/1</td>
<td>NSD[9]</td>
<td></td>
</tr>
<tr>
<td>M.P</td>
<td>202.12.27.33</td>
<td>2001:dc3:35</td>
<td>AS7500</td>
<td>WIDE Project</td>
<td></td>
<td>Distributed using anycast 5/1</td>
<td>BIND</td>
</tr>
</tbody>
</table>

IN_MY_MAC:~ farid11$ dig
There are currently **13 root name servers** specified, with names in the form `letter.root-servers.net`, where `letter` ranges from A to M.

![Root Server Table]

Who Controls the Nameserver

- As an example, Internet Systems Consortium (ISC) operates one of the 13 global authoritative DNS root servers, **F-root**
- This server uses BIND software
- It has two addresses (IPv4 and IPv6)
Who is ISC
Internet Systems Consortium

• ISC, is a non-profit corporation (in Delaware) supporting the infrastructure of the Internet

• It develops and maintains software, protocols, and operations
  – For example they developed BIND 9.0 and Dynamic Host Configuration Protocol (DHCP)
How many gTLD (generic Top-Level Domain)?

280 delegated

11 testing

20 “g”s

13 sponsored

4 unrestricted

3 generic restricted

248 country codes

1 .arpa

242 in ISO 3166-1

6

3 former countries

3 exceptional current countries

246 in 3166-1

4 not deleg.
## gTLD

**http://en.wikipedia.org/wiki/Generic_top-level_domain**

<table>
<thead>
<tr>
<th>Name</th>
<th>Entity</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>aero</td>
<td>air-transport industry</td>
<td>Must verify eligibility for registration; only those in various categories of air-related entities may register.</td>
</tr>
<tr>
<td>asia</td>
<td>Asia-Pacific region business</td>
<td>This is a TLD for companies, organizations, and individuals based in the region of Asia, Australia, and the Pacific.</td>
</tr>
<tr>
<td>biz</td>
<td></td>
<td>This is an open TLD; any person or entity is permitted to register; however, registrations may be challenged later if they are not held by commercial entities in accordance with the domain's charter. This TLD was created to provide relief for the widely popular .com TLD.</td>
</tr>
<tr>
<td>.cwl</td>
<td>Catalan</td>
<td>This is a TLD for Web sites in the Catalan language or related to Catalan culture.</td>
</tr>
<tr>
<td>.com</td>
<td>commercial</td>
<td>This is an open TLD; any person or entity is permitted to register. Though originally intended for profit business entities, for a number of reasons it became the &quot;main&quot; TLD for domain names and is currently used by all types of entities including nonprofits, schools and private individuals. Domain name registrations may be challenged if the holder cannot prove an outside relation justifying reservation of the name, to prevent &quot;squatting&quot;.</td>
</tr>
<tr>
<td>coop</td>
<td>cooperatives</td>
<td>The .coop TLD is limited to cooperatives as defined by the Rochdale Principles.</td>
</tr>
<tr>
<td>edu</td>
<td>educational</td>
<td>The .edu TLD is limited to specific educational institutions such as, but not limited to, primary schools, middle schools, secondary schools, colleges, and universities. In the US, its usability was limited in 2001 to post-secondary institutions accredited by an agency on the list of nationally recognized accrediting agencies maintained by the United States Department of Education. This domain is therefore almost exclusively used by U.S. colleges and universities. Some institutions that do not meet the current registration criteria have &quot;grandfathered&quot; domain names.</td>
</tr>
<tr>
<td>gov</td>
<td>governmental</td>
<td>The .gov TLD is limited to U.S. governmental entities and agencies.</td>
</tr>
<tr>
<td>info</td>
<td>information</td>
<td>This is an open TLD; any person or entity is permitted to register.</td>
</tr>
<tr>
<td>int</td>
<td>international organizations</td>
<td>The .int TLD is strictly limited to organizations, offices, and programs which are endorsed by a treaty between two or more nations.</td>
</tr>
<tr>
<td>jobs</td>
<td>companies</td>
<td>The .jobs TLD is designed to be added after the names of established companies with jobs to advertise. At this time, owners of a &quot;company.jobs&quot; domain are not permitted to post jobs of third-party employers.</td>
</tr>
<tr>
<td>mil</td>
<td>U.S. military</td>
<td>The .mil TLD is limited to use by the U.S. military.</td>
</tr>
<tr>
<td>mobi</td>
<td>mobile devices</td>
<td>Must be used for mobile-compatible sites in accordance with standards.</td>
</tr>
<tr>
<td>museum</td>
<td>museums</td>
<td>Must be verified as a legitimate museum.</td>
</tr>
<tr>
<td>name</td>
<td>individuals, by name</td>
<td>This is an open TLD; any person or entity is permitted to register; however, registrations may be challenged later if they are not held by individuals (or the owners of fictional characters) in accordance with the domain's charter.</td>
</tr>
<tr>
<td>net</td>
<td>network</td>
<td>This is an open TLD; any person or entity is permitted to register. Originally intended for use by domains pointing to a distributed network of computers, or &quot;umbrella&quot; sites that act as the portal to a set of smaller websites.</td>
</tr>
<tr>
<td>org</td>
<td>organization</td>
<td>This is an open TLD; any person or entity is permitted to register. Originally intended for use by non-profit organizations, and still primarily used by same.</td>
</tr>
<tr>
<td>pro</td>
<td>professions</td>
<td>Currently .pro is reserved for licensed or certified lawyers, accountants, physicians and engineers in France, Canada, NL, UK and the U.S. A professional seeking to register a .pro domain must provide their registrar with appropriate credentials.</td>
</tr>
<tr>
<td>tai</td>
<td>Internet communication services</td>
<td>A contact directory housing all types of contact information directly in the Domain Name System.</td>
</tr>
<tr>
<td>travel</td>
<td>travel and tourism industry related sites</td>
<td>Must be verified as a legitimate travel-related entity.</td>
</tr>
<tr>
<td>.xxx</td>
<td>adult entertainment</td>
<td>For sites providing sexually-explicit content, such as pornography.</td>
</tr>
</tbody>
</table>
What authority does gTLD have?
Testing the Public Root Servers

• Go to http://public-root.com
• Do Root-Server-Check and examine which Root Servers are up
• Do Root-Server-Location and see where they are located at
• Get information about E.Root.Server – Where is it?
A Practical Example!

• When you visit a Web site, you need the DNS server to resolve your requested domain name.

• The DNS server of your workstation queries for name resolution and it is typically run by your ISP

• If you find out that the DNS server is too slow, you can change your DNS!!
A Practical Example! – cont.

• Using my MacBook Pro I did:
  – cat /etc/resolv.conf

```
# Mac OS X Notice
#
# This file is not used by the host name and address resolution
# or the DNS query routing mechanisms used by most processes on
# this Mac OS X system.
#
# This file is automatically generated.
#
# domain sbx02888.rohneca.wayport.net
# nameserver 192.168.5.1
```

Let’s say the DNS ended up being very slow. So, I want to change it to another machine which is faster so I can brows quicker!

I decided to use Google Public DNS, instead (8.8.8.8)

http://www.itistimed.com/?DATA=8.8.8.8&ACTION_TYPE=Resolve

Go to http://www.plus.net/support/software/dns/changing_dns_mac.shtml
To learn how to change your DNS in your MAC.
A Practical Example! – cont.

Using my MacBook Pro I did:

```
  cat /etc/resolv.conf
```

I am connected to Wayport.net machines
The dynamic DNS that I have received is 192.168.5.1 – This is where my machine goes and make query

Let’s say the DNS ended up being very slow. So, I want to change it to another machine which is faster so I can brows quicker!

I decided to use Google Public DNS, instead (8.8.8.8)

```
  http://www.itistimed.com/?DATA=8.8.8.8&ACTION_TYPE=Resolve
```

Go to

```
  http://www.plus.net/support/software/dns/changing_dns_mac.shtml
```

To learn how to change your DNS in your MAC.

This is using the default DNS!
Commands

Here are a series of command I used on my MAC to measure the Address Resolution using different DNS servers:

- `dscacheutil -flushcache` // flush the cache
- `time nslookup www.google.com 125.22.47.125`
- `time nslookup www.google.com 208.67.222.222`

I used these to compare the performance of the two DNS servers.

Thus, for DNS server 125.22.47.125, it took 15 millisecond to resolve my Google query!!

Here is the information about the DNS server: http://www.itistimed.com/?DATA=125.22.27.125&ACTION_TYPE=Resolve
DNS Cache Poisoning

• DNS cache poisoning is a data integrity compromise in the Domain Name System (DNS)
• Read: http://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf
• Short Video: http://www.youtube.com/watch?v=1d1tUefYn4U
• This is a nice demo if you can follow it: http://www.videosurf.com/video/dns-cache-poisoning-demo-1240529251
References

• Learn about Google DNS
  http://code.google.com/speed/public-dns/

• Free DNS servers

• http://theos.in/windows-xp/free-fast-public-dns-server-list/