Lessons from history relevant to the future of DNS – principles and examples

Paul V. Mockapetris

PVM@A21.com, PVM@ThreatSTOP.com, PVM@fsi.io,
pvm@coinweb.net, pmockapetris@gmail.com
Darwin on Evolution:

“In the long history of humankind (and animal kind, too) those who learned to collaborate and improvise most effectively have prevailed.”

Two Theories:

• Applies to the Internet as well

• Evolution is about prevailing, which may be cruel to sacred cows
Evolutionary Survival Imperatives

• Be Adaptable
• Be powered by an expanding resource
• Create a new desirable resource
**Examples**

| Moore’s Law on density + adjustments to process, voltage, etc. creates more, faster transistors |
| Intel creates faster processors |
| Microsoft, Apple et al discover we need more text, justified text, colored displays, music, AI… |
| (DNS servers run faster, more names) |

| Internet protocols prevail over OSI stack because of: |
| Genius of the fathers of the Internet? |
| First to harness the explosive growth in bandwidth and processing power |
All Distributed Systems have 3 Parts:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Software</th>
<th>Configuration (e.g. DNS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image of Hardware" /></td>
<td><img src="image2.png" alt="Image of Software" /></td>
<td><img src="image3.png" alt="Image of Configuration" /></td>
</tr>
</tbody>
</table>
Nobody thinks complexity is good for you

But unlike tobacco, software complexity will always be with us.

Further, a DNS that was too complex for the critics in 1983 wasn’t good enough in 1988.

Luckily we learn from experience and develop better tools, so the real issue is how much complexity you can handle.
Where did the Complexity come from?

Because we always build systems that balance:

- the competition
- the complexity we can handle
Security Economics:
Cost of Defense < Value of Target < Cost of Attack

• Cost of Defense < Value of Target - spending $100 to protect $5 will bankrupt you. This is also how you explain to your customers why you haven't put a bank vault door on a chicken coop.

• Value of Target < Cost of Attack - if your data is worth $1000 and it costs the other guy $999 to get it, then the other guy makes a buck on every attack.

• Cost of Defense < Cost of Attack - the arms race clause. If your spending $1000 and your attacker is spending $500, pretty soon you can't afford to play the game any more.
Maintenance Economics:
Effort of putting data in DNS<Value I get for putting the data in

• The “Obviously required” Internet directory that was endorsed by the Internet research community for decades died in various incarnations.

• Facebook discovered people would type all day to get dates, listen to themselves expound, etc, etc

• For the DNS, MX gets maintained so you get mail, WKS died since the maintainer saw no benefit
Shifting sands (100 queries/sec max?)

Development of the Domain Name System*

Paul V. Mockapetris
USC Information Sciences Institute, Marina del Rey, California

Kevin J. Dunlap
Digital Equipment Corp., DECwest Engineering, Washington

Abstract

The Domain Name System (DNS) provides name service for the DARPA Internet. It is one of the largest name services in operation today, serves a highly diverse community of hosts, users, and networks, and uses a unique combination of hierarchical, caching, and datagram access.

This paper examines the ideas behind the initial design of the DNS in 1983, discusses the evolution of these ideas into the current implementations and usage, notes conspicuous surprises, successes and shortcomings, and attempts to predict its future evolution.

I. Introduction

The genesis of the DNS was the observation, circa 1982, that the HOSTS.TXT system for publishing the mapping between host names and addresses was encountering or headed for problems. HOSTS.TXT is the name of a simple text file, which is centrally maintained on a host at the SRI Network Information Center (SRI-NIC) and distributed to all hosts in the Internet via direct and indirect file transfer.

The problems were that the file, and hence the costs of its distribution, were becoming too large, and that the centralized control of updating did not fit the trend toward more distributed management of the Internet.

Simple growth was one cause of these problems; another was the evolution of the community using HOSTS.TXT from the NCP-based original ARPANET to the IP/ICP-based Internet. The research ARPANET's role had changed from being a single network connecting large timesharing systems to being one of several long-haul backbone networks linking local networks which were in turn populated with workstations. The number of hosts changed from the number of timesharing systems (roughly organizations) to the number of workstations (roughly users). This increase was directly reflected in the size of HOSTS.TXT, the rate of change in HOSTS.TXT, and the number of transfers of the file, leading to a much larger than linear increase in total resource use for distributing the file. Since organizations were being forced into management of local network addresses, gateways, etc., by the technology anyway, it was quite logical to want to partition the database and allow local control of local and address spaces. A distributed naming system seemed to be in order.

Existing distributed naming systems included the DARPA Internet's IEN116 [IEN 116] and the XEROX Grapevine [Ewell 82] and Cheeringhous systems [Oppen 83]. The IEN116 services seemed excessively limited and host specific, and IEN116 did not provide much benefit to justify the costs of implementation. The XEROX system was then, and may still be, the most sophisticated name service in existence, but it was not clear that its heavy use of replication, light use of caching, and fixed number of hierarchy levels were appropriate for the heterogene-
At the SRI root server 2/12/87

Up for 3 days
114 queries/minute
48% A query type
74% normal responses

11 | ICANN DNS Montreal
Can we make DNS a more powerful database?

Then
- Separate Concepts and Implementation
  - Concepts
    - Tree structure
      - Delegation of ownership/control
      - Navigate top down guaranteed
      - Opportunistic caching
    - Sets of primitive data records
  - Two types of data transfer
    - Queries for RR sets
    - Transfers for zones

Now?
- Separate Concepts, Implementation, and Theories/Ideas
  - Name space as lattice
  - Bidirectional navigation
  - Bidirectional, Mutirooted security? (What did we learn from X.509 certificates?)
  - Use signed zones for security
The root servers

A Proposed Governance Model for the DNS Root Server System

THE MODEL

Governance
- ICANN Community
- IETF/IAB
- RSOs

Stakeholders

Strategy, Architecture, & Policy Function (SAPF)
- Financial Function (FF)
- Designation & Removal Function (DRF)
- Performance Monitoring & Measurements Function (PMMF)

Secretariat Function (SF)

RSOs

Performance Metrics

DNS Root Sources
- root zone
- root hosts file
- root-servers.net.zone

Onboarding & Offboarding
- Designate Operator

Remove Operator
We appreciate the efforts of the RSOs

• But its time to create a new redundant infrastructure to deliver signed copies of the root zone (including glue)

• One signature for the whole zone!

• Have all resolving servers check their authoritative zones first

• Do the same for all zones of the organization

• No hard target for DDOS anymore
Works in a lot of cases, not all, just like cloud
In Today’s DNS, can I outsource AND keep control

Increasing outsourcing:

- Authoritative service
- Authoritative tailoring (GSLB, etc)
- Recursive service (X.X.X.X)
- Recursive filtering (DNS firewall)

Questions:

- Is the increasing centralization a good idea?
- Is it good to let X.X.X.X look at my data, or set my filtering policy?
- Where do I get the best filtering threat intelligence?
OH NO – Internet Censorship

SOPA/PIPA: Internet Blacklist Legislation

The Stop Online Piracy Act (SOPA) (originally known as the E-PARASITE Act) and its Senate counterpart the PROTECT IP Act (PIPA) (originally the Combating Online Infringement and Copyright Act (COICA)) were a series of bills promoted by Hollywood in the US Congress that would have created a "blacklist" of censored websites. These bills were defeated by an enormous online campaign started by EFF and a handul of other organizations, which culminated in the Internet Blackout on the January 18, 2012.

Although the bills were ostensibly aimed at reaching foreign websites dedicated to providing illegal content, their provisions would allow for removal of enormous amounts of non-infringing content including political and other speech from the Web. The various bills defined different techniques for blocking "blacklisted" sites. Each would interfere with the Internet's domain name system (DNS), which translates names like "www.eff.org" or "www.nytimes.com" into the IP addresses that computers use to communicate. SOPA would also allow rightsholders to force payment processors to cut off payments and advertising networks to cut ties with a site simply by sending a notice.

These bills are targeted at "rogue" websites that allow indiscriminate piracy, but use vague definitions that could include hosting websites such as Dropbox, MediaFire, and RapidShare; sites that discuss piracy such as pirate-party.us, p2pnet, Torrent Freak, torproject.org, and ZeroPaid; as well as a broad range of sites for user-generated content, such as SoundCloud, Etsy, and Deviant Art. Had these bills been passed five or ten years ago, even YouTube might not exist today – in other words, the collateral damage from this legislation would be enormous.

There are already laws and procedures in place for taking down sites that violate the law. These sites would allow the Attorney General and even individuals to create a blacklist of suspect sites.
Harkens back to SOPA and PIPA debates where DNS policy enforces copyright

My bottom line:

It’s effective (like antispam, which everyone seems to accept)

It’s OK so long as the user controls policies
We’ll argue when policy is set by government, ISP, parents ...

While the user controls policies, the user’s ISP may be doing the work

Key issue: diversified structure of industry, i.e. user choice, including DNS provider
Internet history

“The rapid growth of the network made it impossible to maintain a centrally organized hostname registry and in 1983 the Domain Name System was introduced on the ARPANET and published by the Internet Engineering Task Force as RFC 882 and RFC 883.” - Wikipedia

“The first IETF meeting was attended by 21 U.S.-government-funded researchers on 16 January 1986.” - Wikipedia

“January 1, 1983, was an official 'flag day' for the ARPANET, which became what we know as the Internet.” – Internet Society
Raw materials for the DNS design

<table>
<thead>
<tr>
<th>Candidates:</th>
<th>PVM Background:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEN116</td>
<td>IBM Cambridge Scientific Center</td>
</tr>
<tr>
<td>Xerox Naming System</td>
<td>• Virtual machine technology ~1966</td>
</tr>
<tr>
<td>NSF name server</td>
<td>MIT Architecture Machine (now Media Lab)</td>
</tr>
<tr>
<td>X.500 –The anointed choice</td>
<td>• MAGIC distributed computing system ~1969</td>
</tr>
<tr>
<td></td>
<td>• Multiple minicomputers acting as one system</td>
</tr>
<tr>
<td></td>
<td>• Two-level hierarchies are enough</td>
</tr>
</tbody>
</table>

Charles Stark Draper Labs
• Highly reliable systems for space ~1971

UC Irvine Distributed Computer System
• Networking by name ~1973
We should think about stealing from several emerging technologies:

- Blockchain
- Database
- ...
Some predictions
Intermediate term predictions

The research community has dozens of projects, such as:
- Named Data Networking
- Information Centric Networking
- Mobility First, etc, etc

Common Theme
- Named, digitally signed objects accessed by name not address

Historians might claim that looks like X.509
- Challenge is reducing the cost of doing this for every piece of data
- It’s a problem of tailoring, simplifying and cost reducing security
- e.g. BII Yeti work, et al
Long term prediction

As an undergraduate at MIT, I learned a saying:

“Data is just the stupidest form of program”

In the ultimate, the DNS should hold programs as well as data.
Questions?

Perhaps of interest:

Regarding the death of the internet by new TLDs, name collisions, and why you shouldn’t trust all the experts

ICANN 2014 report of a study by experts (including me and several others here in Montreal) on the future of DNS