DNS a Required Review

Are you using DNS right?

Intro/Disclaimers

I CARE A LOT ABOUT DNS

I have worked on:

- ccTLDs/TLDs
- Global Anycast DNS
- CDN Services
- IXP/ISP/WebHosting to Millions of Users.
- I have little patience for mortals

Was not the best day

Beware, I might bite your head off.

Topics for Today

- Review
- Deeper Aspects
- Adoption
- The Client Side
- Misconceptions
- Resources
- Questions

Review

DNS is:

- A Service
- Vitally Important to the Internet
- Largely Misused or Poorly Implemented
- Simple to Use Correctly
- Prone to Attack - Security Exists
- Awesome

Basics

- Forward
  - sluug.org = 207.223.253.71
- Reverse
  - 207.223.253.71 = sluug.org, stllinux.org, etc...
- Authority Model
- Queries ANY, A, AAAA, PTR, NS, MX, SOA
- Transfers AXFR
- Information TXT, SPF, LOC

TTL

Time to Live is a limit of the lifespan of some data.

“The dishes are clean” TTL of your next snack.

SOA

Start of Authority is the header describing the authority to present the responses to queries.

“I am a mechanic, your car is low on oil”

Zones

Zones are areas of authority. A zone is easy to think of as a domain name like example.com and can become more complex.

Reverse zones can be very very confusing.

Adoption or Use

To use DNS there are a confusing number of options.

- HOSTS
- Directory
- DNS Resolver
- DNS Root

HOSTS

/etc/hosts

```
200.24.224.1    router.tecnoera.com   router
127.0.0.1       localhost.local       localhost
127.0.0.3       app.test              app
::1             localhost.local       localhost
```

NIS / YP

Really, we are not going to cover this.

DNS Resolver

A DNS Resolver is a middle man for queries used to speed up the Internet. Authority is passed in the response.

“Hey Bob, what time is it.”
“The clock says it is 4:19”

DNS Root

Root servers are the source of authority. 13 Servers* contracted via ICANN who must get approval from the United States Department of Commerce. The roots are designated as a.root-servers.net - m.root-servers.net.

* These are no longer just single servers.

Clients

Each operating system can handle queries to DNS differently. Some embedded systems do not understand all responses.

Resolv.conf

Resolv.conf

```
search sluug.org
nameserver 8.8.4.4
nameserver 8.8.8.8
nameserver 4.2.2.2
nameserver 4.2.2.3
```

Open Source DNS Server Software

- BIND - Berkeley Internet Name Daemon
- Knot
- DNSMASQ
- PowerDNS
- MaraDNS
- Unbound

What a zone might look like: Demo

Basic Resource Records

A = Address

AAAA = IPv6 Address

NS = Nameserver

MX = Mail Exchange

CNAME = Canonical Name or Alias

TXT = Textual Information

Misconceptions

Al Gore did not invent DNS

DNS was used as flat files in the 1970s

DNS was standardized in an RFC in Nov. 1983

DNS Can be secure - DNSSEC

You can have more than two resolvers!!!!

You can have more than two nameservers!!!!

Misconceptions Part 2

- DNS is NOT UDP only, size decides 512,4k
- DNS is can be both UDP or TCP
- TTLs snowball, 300 is reasonable today
- TTLs snowball, 86400 is crazy, 604800 means you should step away from the keyboard.
- DNS SOA Serial is 32 bit

Resources

- http://en.wikipedia.org/wiki/Domain_Name_System
- http://en.wikipedia.org/wiki/List_of_DNS_record_types
- http://en.wikipedia.org/wiki/Zone_file
- http://en.wikipedia.org/wiki/Root_name_server
- https://google.com

Would you like a detailed talk?

Help us chiefs pick talks by voicing your interest in topics like DNS on the mailing list.

Thanks

Andrew “lathama” Latham