A Survey of the .EDU DNS Name Space

TEAM CYMRU™

John Kristoff
jtk@cymru.com

Editorial Note

This is not a rigorous, peer-reviewed, research quality survey. The numbers aren't perfect, but should be generally representative. Many of the examples were probably correct at the time they were observed.

For those that forgot or were MIA

- Open resolvers
- edu.edu OH NOES!
- miskatonic.edu – in the town of Arkham?
- REN-ISAC tech bursts (e.g. DNS .. for R&E part 2)
  - Almost all problems identified are gone
  - Sorry Purdue, your's got a little worse :-(

Fundamental DNS Components

end users
stub resolvers

caching servers
full resolvers
forwarders

DNS name space
authoritative servers

Parents and Children

- Question: I need to ask Johnnie a question
- Parent: He's over there [*__points__*]
- Question: Hey Johnnie, can you tell me …?
- Johnnie: [Yes I can / No I can't]
- Unfortunately there are a lot of wayward parents
- And some children disown their family
- Parent pointers, if a direct descendant, may give glue
    - Specific address (aka hint) to where the child is

Auxiliary information: WHOIS

- Text-based information store about domains
- May include:
  - NS RRs (may or may not match what is in DNS)
  - Contact information
  - Record filing, update and expiry dates
- Note, WHOIS != DNS
- WHOIS maintains registration info (resource of record)
- DNS is a distributed naming protocol and system

Reverse Engineered .EDU

- I've long given up hope on bulk zone / WHOIS access
- Thankfully “You may use "%" as a wildcard in your search”, but this is limited to 100 records at a time
- So we can brute force WHOIS % our way to .edu's
- As of 2015-04-29 there were 7483 names including:
  - um.edu and lamedelgation.edu

Does size matter?

- Longest domain: medicalcareerandtechnicalcollege
- Many two-character domains
  - BTW, any chance someone from Finlandia can alias jtk@fu.edu for me? Drinks on me all week.
- Domain length popularity:
  - 1304 – 4 characters
  - 1218 – 3 characters
  - 698 – 5 characters
- 15 character names more popular than 2 character

WHOIS contacts

- There are two types of contacts, almost has both:
  - Administrative
  - Technical
- Should there be an abuse-specific contact option?
- There is no Administrative contact for erickson.edu
- There is no contact detail for nlpbc.edu
  - How is this getting renewed?

WHOIS activations

- Year with most activations: 2002 (663)
- Year with the fewest is also the earliest: 1985 (20)
- Busiest month for activiations: January (919)
- Slowest month: November (471)
- Most recent activation: np.edu (2015-04-29)
- Tied for earliest: berkeley, cmu, purdue, rice, ucla

WHOIS updates

- 795 domains updated in 2015
- 2391 domains updated in 2014
- 1523 domains last updated in 2013
- ...
- 3 domains last updated in 2000 (most distant year)
  - covenantseminary, opsu, um (placeholder domain)
- July most popular (by ~2:1) month for updates (1523)

WHOIS expiry

- Majority synchronized to expire July 31, 2015
- um.edu (placeholder) expired in 2006
- muohio.edu expired in 2012
- Ten expired in 2014

WHOIS name servers

- There are 20,135 name server names set
- There are 4505 associated IP addresses
  - Sometimes because out-of-balliwick, but not always
  - EDU glue defined elsewhere
- 4757 domains have just two name servers listed
- 1208->3, 901->4, 383-5, 178->6, 30->7, 25->8
- Many name servers names have multiple A/AAAA RRs

.EDU zone NS RRs and Glue

- 20,133 NS RRs in .edu
- 7,939 A RRs (glue)
- 465 AAAA RRs (glue)

VeriSign and .edu glue

- Since VeriSign is contracted to run .edu with Atlas
- And the [acdfgl].edu-servers.net are like .com/.net
- .edu gets the glue from .com and .net free

DoD Where Art Thou?

- A RRs of cvcs.edu name servers are:
  - 23.23.250.157 and 22,23.253.254
- Look for route announcements covering these
- Now try to query those DNS servers for cvcs.edu
- Now WHOIS the IP addresses... Hmmm
- Others not (clearly) affiliated with DoD exhibit this
- But why and how?

Covering IPv4 prefix size of glue

- 5807 → /24
- 3936 → /16
- 1974 → /23
- 1378 → /20
- 1341 → /19
- Over 1000 have covering prefix less than /16
- 30 of which are most specifically covered by a /8
  - All in 38/8 (Cogent)

EDU NS RR Lame Delegations

- 18603 NOERROR
- 447 REFUSED
- 176 SERVFAIL
- 3 NXDOMAIN
- Anything but NOERROR suggests minimal number of lame delegations
- 841 'aa' bits set to zero
- Oh... and 904 completely unresponsive delegations

TCP responsiveness

- 2070 NS RRs totally unresponsive to a TCP query
- 199 REFUSED
- 100 SERVFAIL

TCP source port packet filters

- NS RRs unresponsive when source port = X
- 3305 can't respond to 1900
- 1828 → 1434
- 1237 → 5060
- 1214 → 1433
- 1153 → 6667
- 1003 → 6000
- 993 → 49152
- 931 → 1024

DNSSEC

- I found 1001 DNSKEY RRs
- 138 using RSA/SHA-512
- 232 using RSA/SHA-256
- 233 using RSASHA1-NSEC3-SHA1
- 398 using RSA/SHA-1

Common names

- Over 2000 unique vpn. [domain] .edu answers
- Over 600 unique wpad. [domain] .edu answers

localhost isn't always local

- It was over 7000 times
- But over 1100 times it was an Amazon cloud node
  - Ala SiteFinder, yay :-(

I see NAT people

```
$ dig 1.1.168.192.in-addr.arpa \
  @accuvax.northwestern.edu ptr +norecurse
  +short
lev-1-po255.ittns.private.

$ dig 1.0.0.10.in-addr.arpa \
  @uic-dns2.uic.edu ptr +norecurse +short
10-0-0-1.nat.uipd.uic.edu.

$ dig @NS1.NYU.EDU 0.16.172.in-addr.arpa \
  ns +norecurse +short
NS1.NYU.EDU.
...
```

IPv6 inconsistency (and TTL?)

(hello r-i crew, andrew)

```
$ dig @dns1.iu.edu iu.edu ns +norecurse

;; ANSWER SECTION:
iu.edu.                 3600    IN      NS      dns1.illinois.edu.
iu.edu.                 3600    IN      NS      dns1.iu.edu.
iu.edu.                 3600    IN      NS      dns2.iu.edu.

;; ADDITIONAL SECTION:
dns1.iu.edu.            600     IN      A       134.68.220.8
dns1.iu.edu.            3600    IN      AAAA    2001:18e8:3:220::10
dns2.iu.edu.            600     IN      A       129.79.1.8
dns2.iu.edu.            3600    IN      AAAA    2001:18e8:2:8::10

$ dig @a.edu-servers.net iu.edu ns +norecurse | grep ^dns1.iu
dns1.iu.edu.            172800  IN      A       134.68.220.8
```

Lame Delegation

(hi keith)

```
$ dig @halley.cc.gettysburg.edu ns baylor.edu +norecurse \
  +noall +answer

baylor.edu.         3600   IN   NS      ns1.baylor.edu.
baylor.edu.         3600   IN   NS      halley.cc.gettysburg.edu.
baylor.edu.         3600   IN   NS      ns2.baylor.edu.
baylor.edu.         3600   IN   NS      ncs.net.utulsa.edu.
```

```
$ dig @ncs.net.utulsa.edu ns baylor.edu +norecurse
;; connection timed out; no servers could be reached
```

The Wrong Combination of Bits

(hi ken)

```
$ dig -b0.0.0.0#1434 @dns.uni.edu uni.edu ns +norecurse
;; connection timed out; no servers could be reached
```

I could do this all day, but I won't

- Some of this you can do yourself with something like:
  - http://www.zonecheck.fr
- The good news is:
  - DNS works reasonably well even when we're sloppy
  - Most DNS problems are reasonably easy to fix

The End