Practical DNS: Protocol, Operation and Security

This material comes from one recent private and one recent public talk

John Kristoff

jtk@depaul.edu

IT 263
BGP and DNS are, by far, the two most fundamentally critical components of the Internet infrastructure. One big difference is that almost all Internet systems participate in the DNS directly, either as a client, a server or both. In other words, DNS has to be, by definition, one of the most unencumbered protocols in use throughout the Internet.
The DNS Lookup Process

Step 1
I need an IPv4 address for www.example.com boss!! Show me some love. k thx!

Step 2
Hmm... I just came online. Nothing in my cache. All I have is this list or root (.) server IP addresses. Let me see if they can help.

Step 3
Yo! root server dude! You know anything about an IPv4 address for www.example.com?

Step 4
Sorry little bro, all I have is this NS RRset for the .com zone, maybe that helps?

Step 5
Hook me up with an A RRset for www.example.com??

Step 6
No can do, but how about this NS RRset for example.com?

Step 7
Hey dog, A IN RRset for www.example.com??!

Step 8
Just one A RR of 192.0.2.1 with TTL 86400, Respect my au-thor-i-TAY!

Step 9
192.0.2.1. with TTL 86400 word.

End User (stub resolver)

Root Servers
A.root-servers.net
M.root-servers.net

.com TLD servers
A.gtld-servers.net
M.gtld-servers.net

.example.com servers
Zone Delegation

Diagram showing the delegation process:
- Root (ICANN)
  - com. (Verisign)
  - edu. (EDUCAUSE)
  - org. (PIR)
  - us. (Neustar)
- depaul.edu. (DePaul)
- cti.depaul.edu. (computer science)
Delegation and Glue Records

- Parent contains non-authoritative NS RRs for the child zone
- Say you want to resolve www.educause.edu, walk the tree
- Eventually you end up here: dig @A3.NSTLD.COM educause.edu ns
- How do you contact NS1.educause.edu?
- Use the hint (address) in the additional section
- Out-of-balliwick versus in-balliwick glue
Resource Record (RR) format

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| |
| / |
| / |
| / NAME |
| |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| TYPE |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| CLASS |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| TTL |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| RDLENGTH |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| RDATA |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```
DNS Message Format

+---------------------+
| Header              |
+---------------------+
| Question            | the question for the name server
+---------------------+
| Answer              | RRs answering the question
+---------------------+
| Authority           | RRs pointing toward an authority
+---------------------+
| Additional          | RRs holding additional information
+---------------------+
DNS Message Header Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| ID |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR| Opcode |AA|TC|RD|RA| Z | RCODE |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| QDCOUNT |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| ANCOUNT |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| NSCOUNT |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| ARCOUNT |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
Sources of Authoritative Data

- Where does authority come from? Zone delegation from a parent.
- However, the child is *authoritative* for the NS RRset.
- Primary/Master name server - zone data from a local source
- Secondary/Slave name server - zone data obtained from another slave/master
Things that make DNS interesting

- General lack of agreement on what DNS is and how to run it
- Implementations differ, particularly in handling corner cases
- Admins have great control over configuration and policy
Administrative Services

- Registry - organization responsible for maintaining TLD (usually) zone data
- Registrar - the interface between registry and domain name holders
- whois - a TCP-based Internet directory service, run by various DNS and address registries, there is no central whois
Resolvers

- Caching (Recursive) name server - what is typically in your resolv.conf
- Forwarding name server - think proxy DNS
- Stub resolver - what end systems use, simple message passer
ORSN Candidate Data Sets

- 51,196 reflector attack, Feb. 2006
- 191,966 ORSN from Duane Wessels, March 2006
- 2,660,229 somethings querying us, March 2006
Netblocks - Attack Set
Netblocks - Duane’s Set

![Graph of Netblocks from Duane Wessels Set](image-url)
Netblocks - Our Flows

![Diagram of Netblocks from Flows Set](image)

**Netblocks from Flows Set**

- Count: 0, 50, 100, 150, 200, 250
- /8: 0, 50, 100, 150, 200, 250

[jtk (jtk@depaul.edu)](mailto:jtk@depaul.edu)

DNS Overview

January 31, 2007

16 / 27
ORSN Netblocks - Our Flows (~14%)
Referrer Netblocks - Our flows (~2%)
Filtering in the Presence of Hidden ORNSs

- How many ORNSs are out there lurking?
- The CPE ORNSs do not reveal themself until an attack
- Only two of the attack addresses seen in flows set
- Generic port 53 filtering/limiting and whitelisting?
- Do we do a continual all netblocks ORNS scan?
Multifaceted ORNS Probing

- Query for whoareyou.ultradns.net
- Query for whoami.ultradns.net
- Query again for whoami.ultradns.net
- Query for unique, but bogus TLD
- Fingerprint with fpdns
- Query for unique name for a zone I control
Remote Probing Challenges

• Recursion available (ra) bit is an unreliable indicator
• Non-existent TLD query doesn’t always result in NXDOMAIN
• Low or zero TTL adherence is not guaranteed
• High-speed querying and timeouts
• Unexpected answer due to configuration or implementation
$ dig @61.46.219.237 whoareyou.ultradns.net +noall +answer

; <<< DiG 9.2.2 <<< @61.46.219.237 whoareyou.ultradns.net +noall +answer
;; global options: printcmd
whoareyou.ultradns.net. 0 IN A 204.74.96.5

$ dig @61.46.219.237 whoareyou.ultradns.net +noall +answer

; <<< DiG 9.2.2 <<< @61.46.219.237 whoareyou.ultradns.net +noall +answer
;; global options: printcmd
whoareyou.ultradns.net. 4294967292 IN A 204.74.96.5
$ dig @211.220.209.3 bogus-tld +noall +answer +authority

; <<>> DiG 9.2.2 <<>> @211.220.209.3 bogus-tld +noall +answer +authority
;; global options:  printcmd
realname. 86400 IN A 211.106.67.200
realname. 86400 IN NS update-psi.netpia.com.
$ dig @213.30.189.132 nanug.org +noall +answer

; <<>> DiG 9.2.2 <<>> @213.30.189.132 nanug.org +noall +answer
;; global options:  printcmd
nanug.org. 10000 IN A 62.210.183.75
nanug.org. 10000 IN TXT "toto"
Flags and Inconsistency

$ dig @213.215.76.84 +noall +comments +answer www.nanog.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52909
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

$ dig @213.215.76.84 +noall +comments +answer www.nanog.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43523
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
www.nanog.org. 86392 IN A 198.108.1.5
Query Amplification and Aggression?

Auth Server #1
client 209.63.146.65#37695: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
Auth Server #2
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
Bad Defaults

$ dig @202.146.225.194 bogus-tld +noall +comments +answer

;; DiG 9.2.2 ;; @202.146.225.194 bogus-tld +noall +comments +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30140
;; flags: qr QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
bogus-tld. 3600 IN A 10.61.32.1