TCP grading meetings this week (Wed-Fri): Look for email today

Final project out
- Fill out group assignment form by tonight (11/29) by 11:59pm
- You can keep your current group, or switch

Return to PLQs

Grades on projects sent out soon
How it works

Hierarchical namespace broken into zones

cslab1a.cs.brown.edu
GLOBAL RECURSIVE RESOLUTION (NO CACHING)

Host → Local Resolver

Q: CSLABIA.CS.BROWN.EDU?

① Host asks Local Resolver

② Resolver starts recursive query from Root

③ Intermediate NameServers don't have answer, but respond to next server that knows more

④ Found server with authoritative answer!
DNS Architecture

• Hierarchy of DNS servers
  – Root servers
  – Top-level domain (TLD) servers
  – Authoritative DNS servers

• Two “types” of DNS servers (may overlap)
  – Authoritative servers: “owners” of certain DNS records
  – Resolvers: process lookups, caches authoritative records
Resolver operation

- Apps make **recursive** queries to local DNS server (1)
  - Ask server to get answer for you
- Server makes **iterative** queries to remote servers (2,4,6)
  - Ask servers who to ask next
  - Cache results aggressively
Where is the root server?

- Located in New York
- How do we make the root scale?

Verisign, New York, NY
DNS Root Servers

- 13 Root Servers (www.root-servers.org)
  - Labeled A through M (e.g., A.ROOT-SERVERS.NET)
- Does this scale?
DNS Root Servers

- 13 Root Servers (www.root-servers.org)
  - Labeled A through M (e.g., A.ROOT-SERVERS.NET)
- Remember anycast?

A Verisign, New York, NY (also Frankfurt, HK, London, LA)
B USC-ISI Marina del Rey, CA (plus 157 other locations)
C Cogent, Herndon, VA (also Los Angeles, NY, Chicago, Frankfurt and 3+)
D U Maryland College Park, MD (also in 106 other locations)
E NASA Mt View, CA (+70)
F Internet Software Consortium, Palo Alto, CA (and 57 other locations)
G US DoD Columbus, OH (+5)
H ARL Aberdeen, MD (also San Diego)
J Verisign (118 locations)
K RIPE London (plus 41 other locations)
M WIDE Tokyo, plus Seoul, Paris, San Francisco, Osaka

**Remember anycast?**

Advertise IP from multiple locations via BGP

E = "Closest" wins
DNS Root Servers

- 13 Root Servers (www.root-servers.org)
  - Labeled A through M (e.g., A.ROOT-SERVERS.NET)
- Remember anycast?
“Types” of DNS servers

• Top Level Domain (TLD) servers
  – Generic domains (e.g., com, org, edu)
  – Country domains (e.g., uk, br, tv, in, ly)
  – Special domains (e.g., arpa)
  – Corporate domains (…)
“Types” of DNS servers

- Top Level Domain (TLD) servers
  - Generic domains (e.g., com, org, edu)
  - Country domains (e.g., uk, br, tv, in, ly)
  - Special domains (e.g., arpa)
  - Corporate domains (…)

- Authoritative DNS servers
  - Provides public records for hosts at an organization
  - Can be maintained locally or by a service provider
“Types” of DNS servers

- Top Level Domain (TLD) servers
  - Generic domains (e.g., com, org, edu)
  - Country domains (e.g., uk, br, tv, in, ly)
  - Special domains (e.g., arpa)
  - Corporate domains (...)

- Authoritative DNS servers
  - Provides public records for hosts at an organization
  - Can be maintained locally or by a service provider

- Recursive resolvers
  - Big public servers, or local to a network
  - Lots of caching
DNS Caching

- Recursive queries are expensive
- Caching greatly reduces overhead
  - Top level servers very rarely change
  - Popular sites visited often
  - Local DNS server caches information from many users
- How long do you store a cached response?
  - Original server tells you: TTL entry
  - Server deletes entry after TTL expires
Reverse DNS

How do we get the other direction, IP address to name?

128.148.121.17 \rightarrow Cs.Brown\_EDU
Reverse DNS

How do we get the other direction, IP address to name?

• Addresses have a natural hierarchy:
  – 128.148.32.12

• Idea: reverse the numbers: 12.32.148.128 …
  – and look that up in DNS

• Under what TLD?
  – Convention: in-addr.arpa
  – Lookup 12.32.148.128.in-addr.arpa
  – in6.arpa for IPv6

Controlled by same authority that allocates IP addresses.
DNS Protocol

- TCP/UDP port 53
- Most traffic uses UDP
  - Lightweight protocol has 512 byte message limit
  - Retry using TCP if UDP fails (e.g., reply truncated)
- Bit in query determines if query is recursive
$ dig cs.brown.edu @10.1.1.10
; <<>> Dig 9.10.6 <<>> cs.brown.edu @10.1.1.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8536
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;cs.brown.edu.  IN  A

;; ANSWER SECTION:
| cs.brown.edu. 1800 IN A 128.148.32.12 |

;; Query time: 69 msec
;; SERVER: 10.1.1.10#53(10.1.1.10)
;; WHEN: Tue Apr 19 09:03:39 EDT 2022
;; MSG SIZE  rcvd: 57
Example

dig . ns

dig +norec www.cs.brown.edu @a.root-servers.net

dig +norec www.cs.brown.edu @a.edu-servers.net

dig +norec www.cs.brown.edu @bru-ns1.brown.edu

www.cs.brown.edu. 86400 IN A 128.148.32.110
Resource Records

All DNS info represented as resource records (RR)

name [ttl] [class] type rdata

- name: domain name
- TTL: time to live in seconds
- class: for extensibility, normally IN (1) “Internet”
- type: type of the record
- rdata: resource data dependent on the type

• Example RRss

  www.cs.brown.edu.     86400 IN A   128.148.32.110
  cs.brown.edu.         86400 IN NS  dns.cs.brown.edu.
  cs.brown.edu.         86400 IN NS  ns1.ucsb.edu.
# DNS record types

<table>
<thead>
<tr>
<th>RR Type</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>IPv4 Address</td>
<td>128.148.56.2</td>
</tr>
<tr>
<td>AAAA</td>
<td>IPv6 Address</td>
<td>2001:470:8956:20::1</td>
</tr>
<tr>
<td>CNAME</td>
<td>Specifies an alias (&quot;Canonical name&quot;)</td>
<td>systems.cs.brown.edu. 86400 IN</td>
</tr>
<tr>
<td></td>
<td>(CNAME)</td>
<td>systems-v3.cs.brown.edu. 86400 IN A 128.148.36.51</td>
</tr>
<tr>
<td>MX</td>
<td>Mail servers</td>
<td>MX &lt;priority&gt; &lt;ip&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eg. MX 10 1.2.3.4</td>
</tr>
<tr>
<td>SOA</td>
<td>Start of authority</td>
<td>Information about who owns a zone</td>
</tr>
<tr>
<td>PTR</td>
<td>Reverse IP lookup</td>
<td>7.34.148.128.in-addr.arpa. 86400 IN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PTR quanto.cs.brown.edu.</td>
</tr>
<tr>
<td>SRV</td>
<td>How to reach specific services (eg. host, port)</td>
<td>_minecraft._tcp.example.net 3600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SRV &lt;priority&gt; &lt;weight&gt; &lt;port&gt; &lt;server IP&gt;</td>
</tr>
</tbody>
</table>

Some important details

• How do local servers find root servers?
  – DNS lookup on a.root-servers.net?
  – Servers configured with root cache file
  – Contains root name servers and their addresses

  .        3600000 IN NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.  3600000 A     198.41.0.4

• How do you get addresses of other name servers?
  – To obtain the address of www.cs.brown.edu, ask a.edu-servers.net, says a.root-servers.net
  – How do you find a.edu-servers.net?
  – Glue records: A records in parent zone
Other uses of DNS

• Local multicast DNS
  – Used for service discovery
  – Made popular by Apple
  – This is how you learn of different Apple TVs in the building

• Load balancing

• CDNs (more on this later)
Reliability

- Answers may contain several alternate servers
- Try alternate servers on timeout
  - Exponential backoff when retrying same server
- Use same identifier for all queries
  - Don’t care which server responds, take first answer
Inserting a Record in DNS

Your new startup helpme.com

- BUY DOMAIN FROM REGISTRAR
- NEED TO PROVIDE ADDRS OF YOUR NAMESERVERS
- REGISTRAR ADDS DOMAIN TO .COM NAMESERVERS ⇒ POINTS TO YOUR DNS SERVERS

⇒ ALTERNATIVELY, MANY HOSTING COMPANIES THAT WILL MANAGE THIS FOR YOU.
Inserting a Record in DNS

• Your new startup helpme.com
• Get a block of addresses from ISP
  – Say 212.44.9.0/24
• Register helpme.com at namecheap.com (for ex.)
  – Provide name and address of your authoritative name server (primary and secondary)
  – Registrar inserts RR pair into the .com TLD server:
    • helpme.com NS dns1.helpme.com
    • dns1.helpme.com A 212.44.9.120
• Configure your authoritative server (dns1.helpme.com)
  – Type A record for www.helpme.com
  – Type MX record for helpme.com
Inserting a Record in DNS, cont

- Need to provide reverse PTR bindings
  - E.g., 212.44.9.120 -> dns1.helpme.com

- Configure your dns server to serve the 9.44.212.in-addr.arpa zone
  - Need to add a record of this NS into the parent zone (44.212.in-addr.arpa)

- Insert the bindings into the 9.44.212.in-addr.arpa zone
DNS Security

• You go to Starbucks, how does your browser find www.google.com?
  – Ask local name server, obtained from DHCP

• Can you trust this DNS server?

  By default, no authentication or verification of RSP.
DNS SNEAKY GAME

IF YOU ARE... WHAT CAN YOU DO?

[Diagram]

ISP

LOCAL DNS

AUTHORITATIVE SERVER

[Red lines]

CACHE POISONING, MALICIOUS ROUTING OR PATH CAN FORGE RESPONSE

[Blue lines]

Google.com

BAD IP
Great Firewall of CIT

If attacker is on the path (say, it is the ISP, or a malicious version of TStaff), what could they do?

– Can sniff all DNS queries
– Send fake responses back first
– Could do this selectively, to direct facebook.com to cs.brown.edu, for example…
Public DNS

Public DNS resolvers provided by cloud companies and ISPs

• 8.8.8.8 (Google)
• 1.1.1.1 (Cloudflare)
• ... and others

Why do this?
DNS: 8.8.8.8 kusun olsun!
Alternatif: 8.8.4.4
“Helpful” ISPs

• Many ISPs hijack NXDOMAIN responses to “help” by offering search and advertisement related to the domain
  
  • E.g., [www.bicycleisntadomain.com](http://www.bicycleisntadomain.com) doesn’t (currently) exist
    – Could return a page with search and ads on bicycles (or domain registrations?)
What can be done?

Some defenses against DNS spoofing/hijacking
What can be done?

Some defenses against DNS spoofing/hijacking

• DNSSEC: protocol to sign/verify hierarchy of DNS lookups
  – Expensive to deploy, hierarchy must support at all levels
  – APNIC DNSSEC monitor: https://stats.labs.apnic.net/dnssec

• Tunneling DNS: client uses DNS via more secure protocol
  – DNS over HTTPS
  – DNS over TLS
More on DNS
Structure of a DNS Message

- Same format for queries and replies
  - Query has 0 RRs in Answer/Authority/Additional
  - Reply includes question, plus has RRs
- Authority allows for delegation
- Additional for glue, other RRs client might want

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

- **Id**: match response to query; **QR**: 0 query/1 response
- **RCODE**: error code.
- **AA**: authoritative answer, **TC**: truncated,
- **RD**: recursion desired, **RA**: recursion available
Other RR Types

- **CNAME (canonical name):** specifies an alias
  
  www.l.google.com. 300 IN A 72.14.204.147

- **MX record:** specifies servers to handle mail for a domain (the part after the @ in email addr)
  
  – Different for historical reasons

- **SOA (start of authority)**
  
  – Information about a DNS zone and the server responsible for the zone

- **PTR (reverse lookup)**
  
  7.34.148.128.in-addr.arpa. 86400 IN PTR quanto.cs.brown.edu.