Domain Name System (or Service) (DNS)
DNS Outline

- DNS Hierarchial Structure
- Root Name Servers
- Top-Level Domain Servers
- Authoritative Name Servers
- Local Name Server
- Caching and Updating DNS Records
- DNS Protocols and Messages
People: many identifiers:
- SSN, name, passport #

Internet hosts, routers:
- IP address (32 bit) - used for addressing datagrams
- “name”, e.g., www.yahoo.com - used by humans

Q: map between IP addresses and name?

Domain Name System:
- distributed database implemented in hierarchy of many name servers
- application-layer protocol host, routers, name servers to communicate to resolve names (address/name translation)
  - note: core Internet function, implemented as application-layer protocol
  - complexity at network’s “edge”
DNS

- DNS servers often run on Unix machines running BIND (Berkeley Internet Name Domain)
- Runs over UDP
- Uses port 53
DNS services

- hostname to IP address translation
- host aliasing
  - Aliases, where canonical name is “real” name
- mail server aliasing
- load distribution
  - replicated Web servers: set of IP addresses for one name

Why not centralize DNS?

- single point of failure
- traffic volume
- distant centralized database
- maintenance

→ doesn’t scale!

- Distributed by design
Three classes of servers (approximation):
- Root DNS servers
- Top-level domain (TLD) servers
- Authoritative name servers

Additionally:
- Local name server
Root DNS Servers

- com DNS servers
  - yahoo.com DNS servers
  - amazon.com DNS servers
- org DNS servers
  - pbs.org DNS servers
- edu DNS servers
  - poly.edu DNS servers
  - umass.edu DNS servers

Example: Client wants IP for www.amazon.com {1st approx:}

- client queries a root server to find .com DNS server
- client queries .com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com
DNS: Root Name Servers

- Contacted by local name server that can not resolve name
- Root name server:
  - Contacts authoritative name server if name mapping not known
  - Gets mapping
  - Returns mapping to local name server

13 root name servers worldwide (a-m)
Top-Level Domain (TLD)

- Top-level domain (TLD) servers:
  - Responsible for com, org, net, edu, etc, and all top-level country domains such as uk, fr, ca and jp.
  - Network Solutions maintains servers for com TLD.
  - Educause for edu TLD.
  - VeriSign for net TLD.
Authoritative Servers

Authoritative DNS servers:

- Organization’s DNS servers, providing authoritative hostname to IP mappings for organization’s servers (e.g., Web, mail).
- Can be maintained by organization or service provider.
Local Name Server

- Does not strictly belong to hierarchy.
- Each ISP (residential ISP, company, university) has one
  - Also called “default name server”
  - You can run one in your home/dorm!
- When a host makes a DNS query, the query is sent to its local DNS server.
  - ISP provides IP address of local DNS server using DHCP.
  - Acts as proxy, forwards query into the name server hierarchy.
Host at cis.poly.edu wants IP address for gaia.cs.umass.edu

Iterated query
• contacted server replies with name of server to contact.
• “I don’t know this name, but ask this server.”
Recursive query

- Puts burden of name resolution on contacted name server.
- Heavy load?

Computer Networks  DNS
Once (any) name server learns mapping, it caches mapping.

- Cache entries timeout (disappear) after some time (e.g. two days) \{specified as TTL == Time-To-Live\}.
- IP addresses of TLD servers are typically cached in local name servers.
  - Thus root name servers are not visited frequently.

Originally thought DNS names quite static, but increasingly not so → update/notify mechanisms under design by IETF
DNS: distributed database storing resource records (RR)

RR format: (name, value, type, ttl)

- **Type=A**
  - name is hostname
  - value is IP address

- **Type=NS**
  - name is domain (e.g. foo.com)
  - value is hostname of authoritative name server for this domain

- **Type=CNAME**
  - name is alias name for some “canonical” (the real) name
  - value is canonical name
    - www.ibm.com is really servereast.backup2.ibm.com

- **Type=MX**
  - value is name of mailserver associated with name
DNS protocol: query and reply messages, both with the same message format.

msg header
- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative

<table>
<thead>
<tr>
<th>identification</th>
<th>flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of questions</td>
<td>number of answer RRs</td>
</tr>
<tr>
<td>number of authority RRs</td>
<td>number of additional RRs</td>
</tr>
</tbody>
</table>

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)
### DNS Protocol and Messages

**Resources records in response to query**

- Name, type fields for a query
- Records for authoritative servers
- Additional "helpful" info that may be used

<table>
<thead>
<tr>
<th>Field</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>identification</td>
<td>12 bytes</td>
</tr>
<tr>
<td>flags</td>
<td></td>
</tr>
<tr>
<td>number of questions</td>
<td></td>
</tr>
<tr>
<td>number of answer RRs</td>
<td></td>
</tr>
<tr>
<td>number of authority RRs</td>
<td></td>
</tr>
<tr>
<td>number of additional RRs</td>
<td></td>
</tr>
<tr>
<td>questions</td>
<td>(variable number of questions)</td>
</tr>
<tr>
<td>answers</td>
<td>(variable number of resource records)</td>
</tr>
<tr>
<td>authority</td>
<td>(variable number of resource records)</td>
</tr>
<tr>
<td>additional information</td>
<td>(variable number of resource records)</td>
</tr>
</tbody>
</table>
Example: new startup “Network Utopia”
- How do people get IP address of your Web site?
- How do they send you email?

Register name networkuptopia.com at DNS registrar (e.g., Network Solutions)
- provide names, IP addresses of authoritative name server (primary and secondary).
- registrar inserts two RRs into .com TLD server:

(networkuptopia.com, dns1.networkuptopia.com, NS)
(dns1.networkuptopia.com, 212.212.212.1, A)

Create authoritative server Type A record for www.networkuptopia.com; Type MX record for networkuptopia.com for mail.
DNS Summary

- DNS Hierarchical Structure
- Root Name Servers
- Top-Level Domain Servers
- Authoritative Name Servers
- Local Name Server
- Caching and Updating DNS Records
- DNS Protocols and Messages