Network Protocols

Domain Name System (DNS)
Routing (BGP) and naming (DNS) are by far the two most critical subsystems of the Internet infrastructure. And in the case of DNS, practically all Internet hosts participate directly in the DNS as a client, server or both. As a result, DNS is one of the most unencumbered protocols in use throughout the Internet. This can be good, bad or interesting depending on your perspective.
First a DNS resolution primer...
I need an IPv4 address for www.cdm.depaul.edu.

Please get it (recursion desired) for me?
Check cache.
If empty, ask a parent.
Follow delegation if necessary.

Local Caching Server
(full resolver)

parent zones: cdm.depaul.edu.
depaul.edu.
edu.
.
Let's assume cache is empty, and all it knows about is (.) root.*

A.root-servers.net

... 

M.root-servers.net

*Do you see why a reliable and trustworthy root is so important?
I need an IPv4 address for www.cdm.depaul.edu.

Can you tell me or refer me to someone?

Local Caching Server
(full resolver)

root (.) server
Don't know.
Try one of these .edu servers:

A.GTLD-SERVERS.NET
C.GTLD-SERVERS.NET
D.GTLD-SERVERS.NET
E.GTLD-SERVERS.NET
F.GTLD-SERVERS.NET
G.GTLD-SERVERS.NET
L.GTLD-SERVERS.NET

Local Caching Server  (full resolver)

root (.) server
Does the caching server have something in its cache now?

Raise your hand for yes.
Ultimately we should get here...
You've come to the right place.
The authoritative answer is:

140.192.32.142

and that answer is valid for 3600 seconds

Local Caching Server
(full resolver)

ns1.cti.depaul.edu.
or
ns2.cti.depaul.edu.
or
ns3.cti.depaul.edu.
Zones, delegations and hierarchy

- root (.) - ICANN and root-servers.org
- top-level domain (TLD)
  - country-code TLD (ccTLD)
  - generic TLD (gTLD)
  - special (e.g. .arpa)
  - sponsored (e.g. aero)
  - unsponsored (e.g. .com)
- second-level domain (SLD)
- third-level domain (3LD)
Whats in a name?

• Host name is a domain name used as a host name
• Some SLDs behave like TLDs (e.g. co.uk.)
• Label, up to 63 8-bit octets separated by dots
  • Maximum 255 octets
• What are valid name characters?
  • For a domain name, any 8-bit value is valid
  • For a host name, see IETF RFC 1123
    • [0-9a-zA-Z-] # case insensitive
    • Underscore disallowed, but often used :/
Domain name registration

- Registry
  - Keeper/maintainer of zone data
- Registrar
  - Agent through which registrant obtains name
- Registrant
  - Authorized user of name, customer of registrar
DNS message format

| +---------------------+ |
| | Header | (see next slide) |
| +---------------------+ |
| | Question | the question for the name server |
| +---------------------+ |
| | Answer | RRs answering the question |
| +---------------------+ |
| | Authority | RRs pointing toward an authority |
| +---------------------+ |
| | Additional | RRs holding additional information |
| +---------------------+ |
# DNS header format

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-------------------------------+</td>
<td>ID</td>
<td>+-------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------+</td>
<td>QR</td>
<td>Opcode</td>
<td>AA</td>
<td>TC</td>
<td>RD</td>
<td>RA</td>
<td>Z</td>
<td>RCODE</td>
<td>+-------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------+</td>
<td>QDCOUNT</td>
<td>+-------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------+</td>
<td>ANCOUNT</td>
<td>+-------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------+</td>
<td>NSCOUNT</td>
<td>+-------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------+</td>
<td>ARCOUNT</td>
<td>+-------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DNS RR format

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+----------------------------------------+
|                                        |
|                                        |
+----------------------------------------+
|                                        |
|                                        |
+----------------------------------------+
|                                        |
|                                        |
|                                        |
+----------------------------------------+
|                                        |
|                                        |
|                                        |
+----------------------------------------+
|                                        |
|                                        |
|                                        |
|                                        |
+----------------------------------------+
|                                        |
|                                        |
|                                        |
+----------------------------------------+
```

- NAME
- TYPE
- CLASS
- TTL
- RDLENGTH
- RDATA