DNS Roles and Responsibilities

Country Code Managers and Generic Name Relationships with Governments

Bruce Tonkin
.au Domain Administration Limited (auDA)
18 September 2022, Kuala Lumpur
## DNS Roles – Authoritative Name Servers

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Example</th>
<th>ICANN Role</th>
<th>Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root zone manager</td>
<td>ICANN</td>
<td>Yes</td>
<td>Manages the list of top level domains including gTLDs and ccTLDs</td>
</tr>
<tr>
<td>Root server operator</td>
<td>RIPE NCC</td>
<td>Cooperation</td>
<td>Globally Distributed set of DNS nameservers that operate a directory of gTLD and ccTLD DNS name servers</td>
</tr>
<tr>
<td>gTLD registry</td>
<td>.com, .net, .org, .London, .afl, .digital</td>
<td>Yes – by contract</td>
<td>Globally Distributed set of DNS nameservers that operate a directory of nameservers for each name in the gTLD zone (e.g. ns.example.com)</td>
</tr>
<tr>
<td>ccTLD registry</td>
<td>auDA (.au), SIDN (.nl)</td>
<td>Cooperation</td>
<td>Distributed set of DNS nameservers that operate a directory of authoritative nameservers for each name in the ccTLD zone (e.g. ns.example.nl)</td>
</tr>
<tr>
<td>Authoritative DNS name server</td>
<td>Registrars, ISPs, web hosting companies, DNS service providers</td>
<td>No</td>
<td>Distributed set of DNS nameservers that typically contain A records (with IP addresses for web servers) and MX records (with IP addresses for email servers)</td>
</tr>
</tbody>
</table>
DNS Roles – Content

• The DNS does not contain any content (other than in the domain name itself – e.g. haveaniceday.au)

• The DNS is a hierarchical set of directories that progressively direct users to a DNS authoritative name server that has information on where to find a website server or mail server

• The website server and mail servers are generally not operated by domain name registries

• Removing a domain name doesn’t remove content from the Internet just an entry in a directory. Content could be reached by many domains across multiple gTLDs and ccTLD registry operators, or by the IP address directly.
DNS Roles – DNS Resolvers

• DNS Resolver sends a query to the authoritative DNS nameservers on behalf of the end user, and keeps a copy of the result
• Generally operated by Internet Service Providers (ISPs)
• Some large scale public DNS resolvers – e.g. Google, Cloudflare, Quad9
• Generally operate by keeping a copy of a DNS result for a period of time (DNS caching) to provide the IP addresses of websites and email servers quickly
• Don’t contain any content
• DNS Resolvers operators can implement security measures including blocking the DNS resolution of some names, or even redirecting users to information pages
• Not managed via ICANN contracts, but some Government laws are implemented by ISPs at the DNS resolver layer
ccTLD relation with ICANN

• Policy discussions generally about how ccTLDs are added or subtracted from the top level zone
• New ccTLDs added include internationalized versions of domain names that reflect the national languages in each country
• Removal of ccTLDs generally when a country ceases to exist
• The operation of each ccTLD is managed through the local community
ccTLD relationship with Government

Bruce Tonkin
.au Domain Administration Limited
ccTLD relations with national government

- Starting to split between the requirements around the operational infrastructure, and requirements about naming rules

- Operational infrastructure
  - in many countries including Australia the registry database and DNS nameservers are treated as critical infrastructure like water, electricity, gas, telecommunications
  - Focus on security - confidentiality, availability, data integrity issues

- Naming policy
  - Eligibility – who gets a name
  - Allocation – what name a registrant can have
  - Accountability – how is a registrant held to account to ensure that use of the name is compliant with local laws
  - Transparency – public information on who is responsible for each name – WHOIS
  - Naming policy – generally developed through multi-stakeholder mechanisms – Government, industry, not-for-profits, academic, and civil society

- ccTLD managers are subject to local laws that may relate to critical infrastructure or privacy