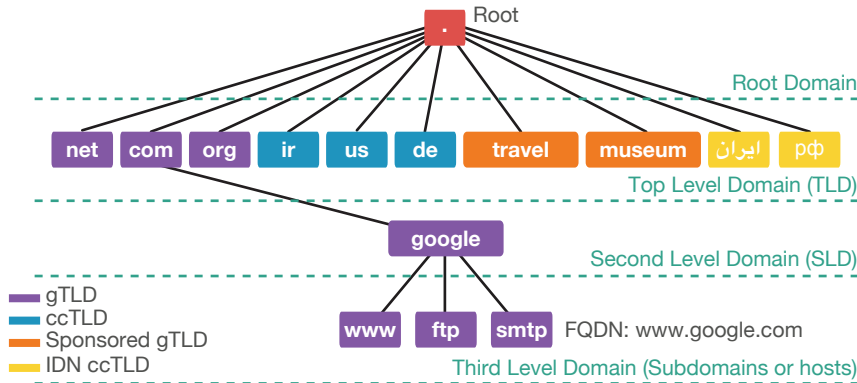


DNS Name Space Hierarchy



Terminology

Domain Name System (DNS) client-server application that maps host names into their corresponding IP addresses, uses Port 53 TCP/UDP

Registry an organization that manages and set rules/policy for domain name extensions (TLD) which has edit control of the database. I.e. Verisign

Registrar an organization that sells domain name to public and submit change requests to the registry on behalf of the registrant. I.e. Godaddy

Registrant a person or company who registers and use the domain name. Manage their domain name's settings through their registrar. I.e. Google

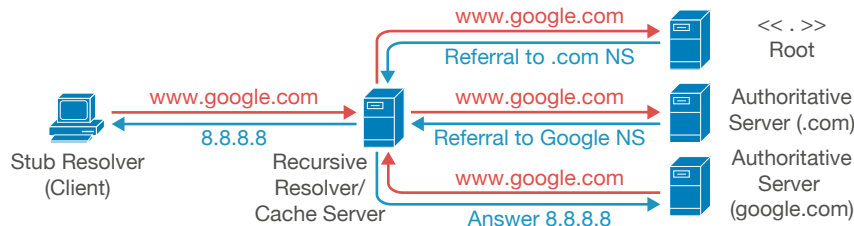
Resource Records (RR) are the dns data in DNS database and consist of {label, ttl, class, type, rdata (Resource Data)}.

[www.google.com. IN A 172.217.25.4]

Resource Record Sets (RRsets) a set of RRs with same name, class, TTL & type. I.e. RRSet would contain multiple NS records for a zone/domain

[google.com. IN NS ns1.google.com.
google.com. IN NS ns2.google.com.]

DNS Main Components



Authoritative Server contains records in its zone file & answer to queries for data under its authority. if can't answer, it points to another authority

Recursive Resolver queried by stub resolvers to resolve names and they query authoritative servers for the answer and cache the result base on TTL

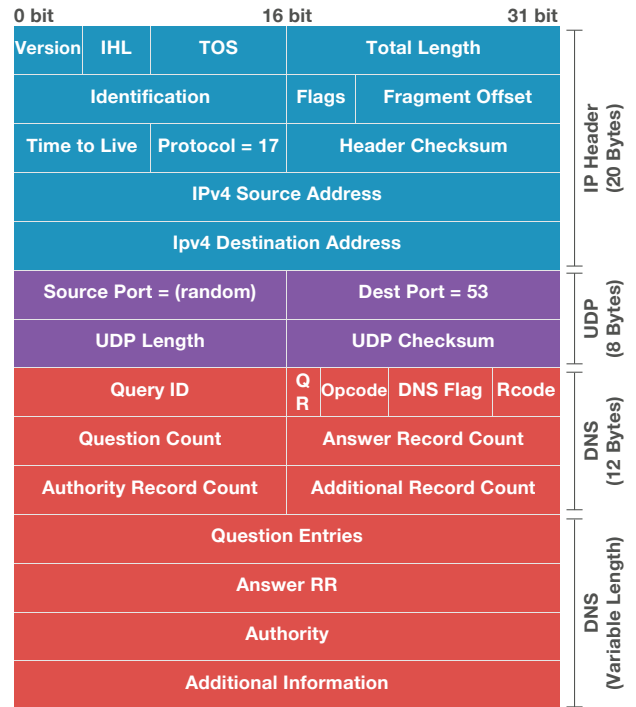
Stub Resolver / Resolver a DNS client that sends DNS messages to obtain information about the requested domain name space

Lookup Methods

Recursive Resolution DNS client requests information from the DNS server that is set to query subsequent authoritative server until the complete answer is returned to the client. The queries from recursive DNS server to authoritative servers are iterative queries

Iterative Queries when the name server of a host cannot resolve a query, it sends a "referral to another server message" to the resolver

DNS Packet Format



Resource Record Types

A address record for IPv4 (32-bit IPv4 address)
[www.apnic.net. IN A 203.176.189.99]

AAAA address record for IPv6 (128-bit IPv6 address)
[www.apnic.net. IN AAAA 2001:db8::1]

NS provides name of authoritative name server for zone
[apnic.net. IN NS ns1.apnic.net.]

CNAME maps one name to another (name aliasing)
[web.apnic.net. IN CNAME www.apnic.net.]

MX provides name of e-mail handling host for a domain
[apnic.net. IN MX 10 mail01.apnic.net.]

SOA authoritative information for the zone {name servers, contact, serial number, zone transfer timers}
[apnic.net. IN SOA ns1.apnic.net.
noc-notify.apnic.net. 110022 3600 1800 691200 10800]

DNS Transactions

DNS Query/Response query originates from a resolver to dns server and contain qname (domain name), qtype (A, AAAA, MX, AXFR, IXFR...), qclass (IN, CH, HS) and flag (QR, RD, EDNS, ...)

Zone Transfer (AXFR, IXFR) synchronization of new/updated domains between master and slave DNS servers by comparing their serial number

Dynamic Update a method for adding, replacing or deleting records in a master server (allow-update)

DNS Notify a method which master servers notify slave for change in zone file & slave will initiate zone transfer if their version of zone file is not current