Domain Name System (DNS)

Root DNS Server:

- The Root DNS servers are a crucial part of the Domain Name System (DNS) hierarchy. There are 13 sets of root DNS servers labeled A through M, managed by various organizations worldwide. These servers are the top-level authority in the DNS hierarchy.
- The main purpose of the Root DNS servers is to answer requests for domain names that they know nothing about. In other words, they don't hold information about specific domain names like "google.com" or "example.org." Instead, they store information about the authoritative name servers for top-level domains (TLDs) such as .com, .net, .org, .uk, .de, and country-code TLDs like .us, .jp, .cn, etc.
- When a DNS resolver receives a request for a domain name, and it doesn't have the IP address associated with that domain name in its cache, it starts the resolution process by querying one of the Root DNS servers. The Root DNS server responds with the IP addresses of the authoritative name servers for the appropriate TLD. This allows the resolver to continue the resolution process by querying the TLD DNS servers and then the authoritative DNS servers for the specific domain name.

Top-Level Domain (TLD) DNS Server:

- Top-level domains are first-tier domains available for the use of the general public. They are installed in the Root DNS Server; all other domains are part of TLDs. For example, google.com is a top-level domain, while google.co.in is a secondary-level domain.
- Top-level domains are divided into two categories:
- Generic top-level domains (gTLD) – These domains are not associated with any country. Example – .com, .org, .net, .int, .mil, .edu, .gov
- Country-code top-level domains(ccTLD) – These are two letter domains established for countries or territories. Examples – .in, .uk, .to, .ca, .co, .us etc.

Authoritative DNS server:

- It is the last step for a DNS query and returns. It is a nameserver with original DNS records such as (A record, MX record, etc.). The request to them reaches from resolving name servers, which are the endpoint of any request. Note they don’t respond to recursive queries.

DNS (Domain Name System) request and response messages contain specific information necessary for the resolution of domain names to IP addresses and vice versa. These messages are used in DNS queries and responses during the process of translating human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) and vice versa. Here's what these messages typically contain:

DNS Request Message:

Query Type (QTYPE): This field specifies the type of DNS record being requested. Common query types include:

A (IPv4 address) record: Used to resolve a domain name to an IPv4 address.

AAAA (IPv6 address) record: Used to resolve a domain name to an IPv6 address.

MX (Mail Exchange) record: Used to find mail servers responsible for a domain.

CNAME (Canonical Name) record: Used for aliasing one domain name to another.

PTR (Pointer) record: Used for reverse DNS lookups (IP address to domain name).

NS (Name Server) record: Used to find authoritative name servers for a domain, among others.

Query Class (QCLASS): This field specifies the class of the query. The most common class is IN (Internet).

Question Section: This section includes the domain name being queried (e.g., www.example.com), the query type, and the query class.

Additional Sections: These sections may be included in some cases and can provide additional information, such as the EDNS (Extension Mechanisms for DNS) options.

DNS Response Message:

Response Code (RCODE): This field indicates the result of the DNS query and whether it was successful or encountered an error. Common response codes include:

0: No error (successful response).

3: Name Error (domain name does not exist).

5: Refused (the DNS server refused to process the query).

12: Name exists when it should not (for some query types).

Answer Section: This section contains the actual DNS resource records (RRs) that provide the answer to the query. For example, if the query was for an A record, this section would contain the IP address associated with the domain name.

Authority Section: If the DNS server responding to the query is authoritative for the requested domain, this section provides information about the authoritative name servers for that domain.

Additional Section: This section can include additional information that may be relevant to the query, such as the IP addresses of name servers or any additional resource records.

Query Identifier (ID): This field helps match the response to the corresponding query, as DNS queries and responses may be asynchronous and arrive out of order.

Flags: Various flags in the DNS response message provide information about the query and response, such as the QR (Query/Response) flag indicating whether it's a query or response, the AA (Authoritative Answer) flag indicating whether the DNS server is authoritative for the domain, and the RD (Recursion Desired) flag indicating whether the client requests recursive resolution.

These are the core components of DNS request and response messages. The specific content and format of these messages adhere to the DNS protocol standards, which are documented in RFCs (Request for Comments).