The Domain Name System

DOMAIN NAME SYSTEM (DEFINITION)

- The DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. Source
- We do so because it is easy to remember names than to remember long decimal numbers. For example www.uta.edu maps to 129.107.56.31

The Domain Name System

- The **Domain Name System (DNS)** is a helper system for IP.
- DNS is:
  - A **naming hierarchy** for the Internet
  - A **directory service** to translate (resolve) these names to IP addresses
  - A **protocol** to perform name resolution
- You can think of DNS as a **phone book** for the Internet, helping you look up IP addresses for a specific name.

Why DNS Exists

- Domain names provide flexibility and human readability to the Internet Protocol.
- Domain names used in URLs and email addresses (e.g. www.google.com) are **easier for humans to remember** than IP addresses.
- In addition, network operators may want to **switch IP addresses** without having to change the domain name.
- And network operators may want to have **multiple IP addresses** assigned to a specific domain name to, for example, serve content from multiple locations.

WORKING

STEP 1: REQUESTING INFORMATION

- When we enter the URL in the web browser, the first place our computer looks is its local DNS cache, which stores information that our computer has recently retrieved.
- If our computer doesn’t already have it, it needs to perform a DNS query to find out.

STEP 2: ASKING RECURSIVE DNS SERVERS

- If our computer does not have the domain name in its local cache, then it requests the DNS server of our ISP.
- If it has the information, the process ends here and the reply is sent back to our computer.

STEP 3: ASKING ROOT NAME SERVER

- If DNS server does not have the information, then it asks Root Name servers.
- A name server is a computer that answers questions about domain names, such as IP addresses. They can direct our query to someone that knows where to find it.

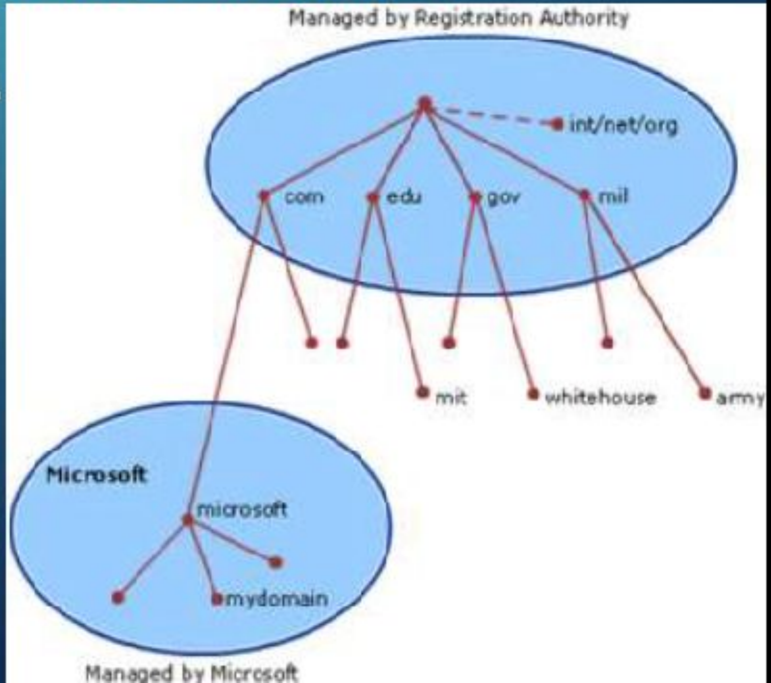
STEP 4: ASKING TOP-LEVEL DOMAIN (TLD) NAME SERVERS

The root name servers will look at the first part of our request, reading from right to left – www.abc.com – and direct our query to the Top-Level Domain (TLD) name servers for .com. Each TLD, such as .com, .org, and .us, have their own set of name servers, which act like a receptionist for each TLD

Managed by Registration Authority

STEP 5: ASKING AUTHORITATIVE DNS SERVER

- The TLD name servers review the next part of our request — www.abc.com — and direct our query to the name servers responsible for this specific domain. These authoritative name servers are responsible for knowing all the information about a specific domain, which are stored in DNS records.



PICTURE SOURCE: WWW.MICROSOFT.COM

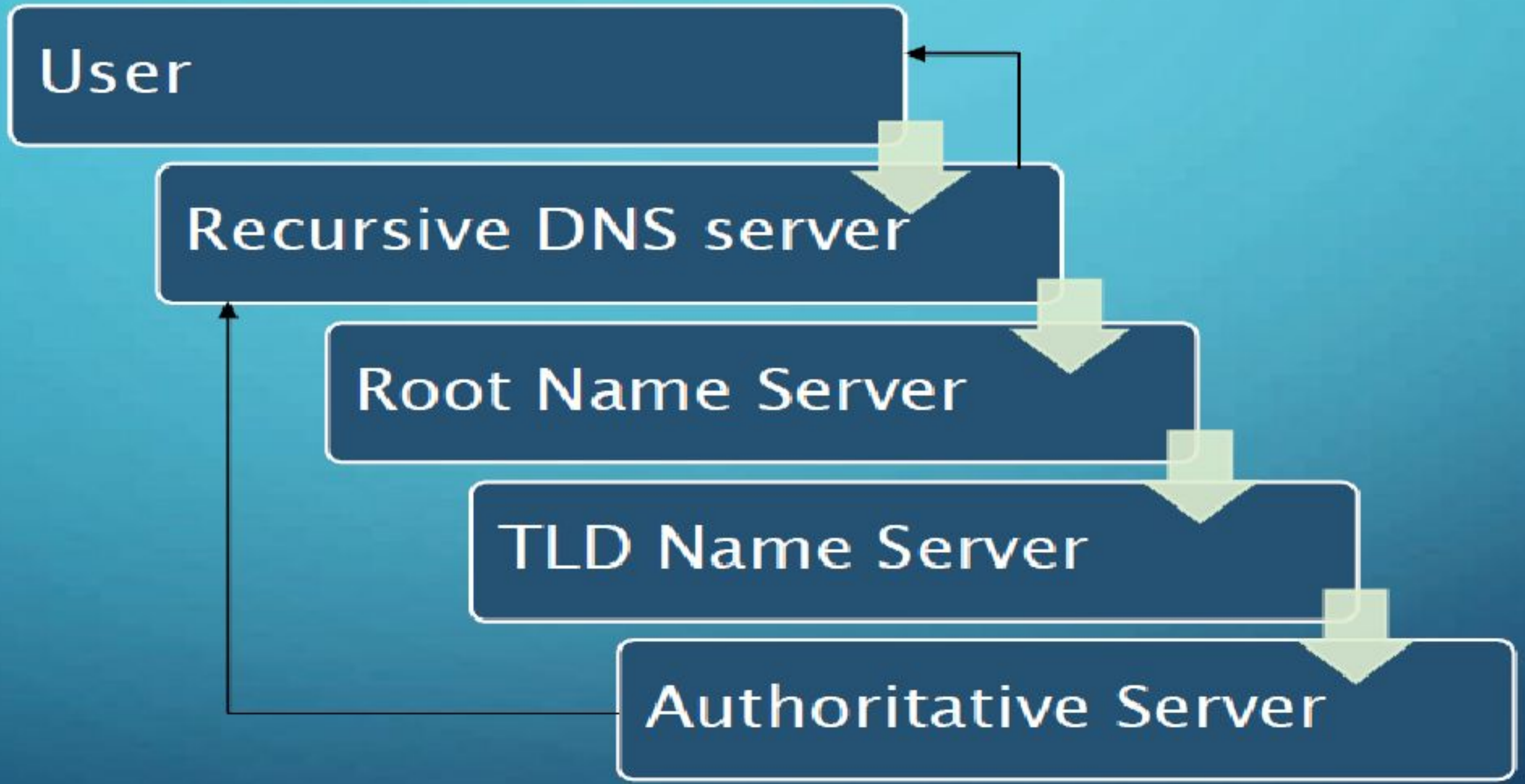
STEP 6: RETRIEVING THE RECORD

- The recursive server retrieves the record for abc.com from the authoritative name servers and stores the record in its local cache. If anyone else requests the host record for abc.com, the recursive servers will already have the answer and will not need to go through the lookup process again. All records have a time-to-live(TTL) value, which is like an expiration date.

STEP 7: RECEIVING THE REPLY

- Recursive server returns the record back to your computer. Our computer stores the record in its cache, reads the IP address from the record, then passes this information to the browser. The browser then opens a connection to the webserver and receives the website.

FLOW DIAGRAM



User

Recursive DNS server

Root Name Server

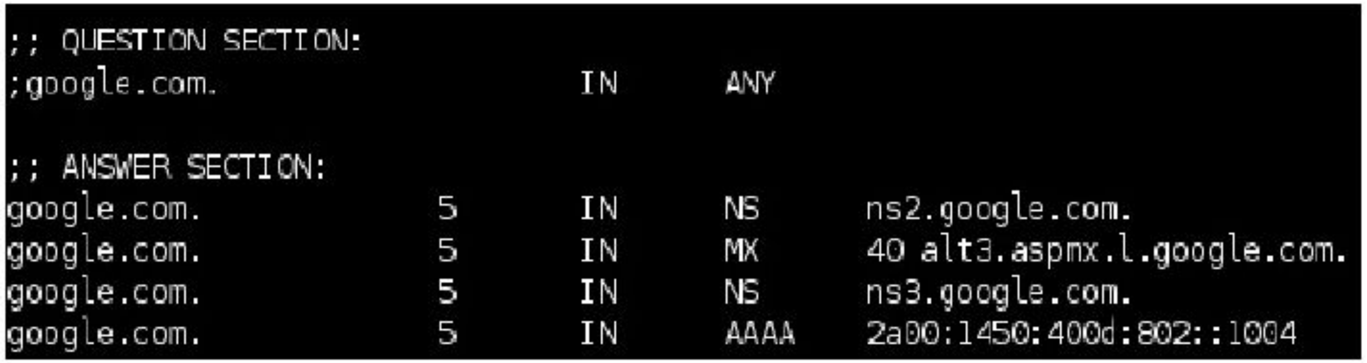
TLD Name Server

Authoritative Server

DNS Resources and Records

There are many **DNS record types** that store domain name data. Here are 5 commonly used record types:

- **A** - IPv4 address
- **AAAA** - IPv6 address
- **MX** - Email server
- **NS** - Name server
- **CNAME** – Alias to another domain name



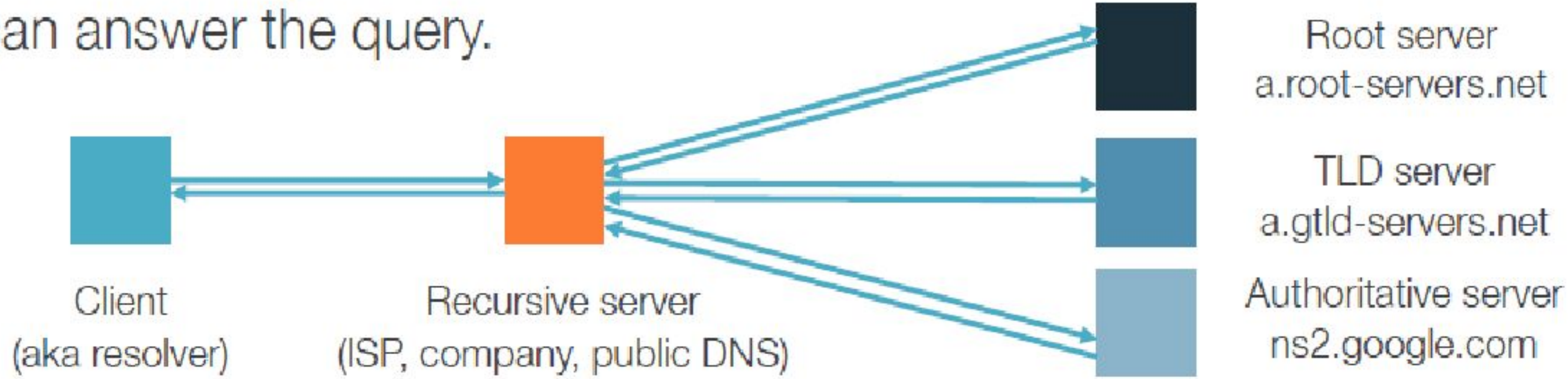
```
;; QUESTION SECTION:
;google.com.                     IN      ANY

;; ANSWER SECTION:
google.com.             5        IN      NS      ns2.google.com.
google.com.             5        IN      MX      40 alt3.aspmx.l.google.com.
google.com.             5        IN      NS      ns3.google.com.
google.com.             5        IN      AAAA    2a00:1450:400d:802::1004
```

A DNS record has a **Time-to-Live (TTL)** that specifies, in seconds, how long it can be **cached** by a name server. Once it expires, the name server must query for an updated record.

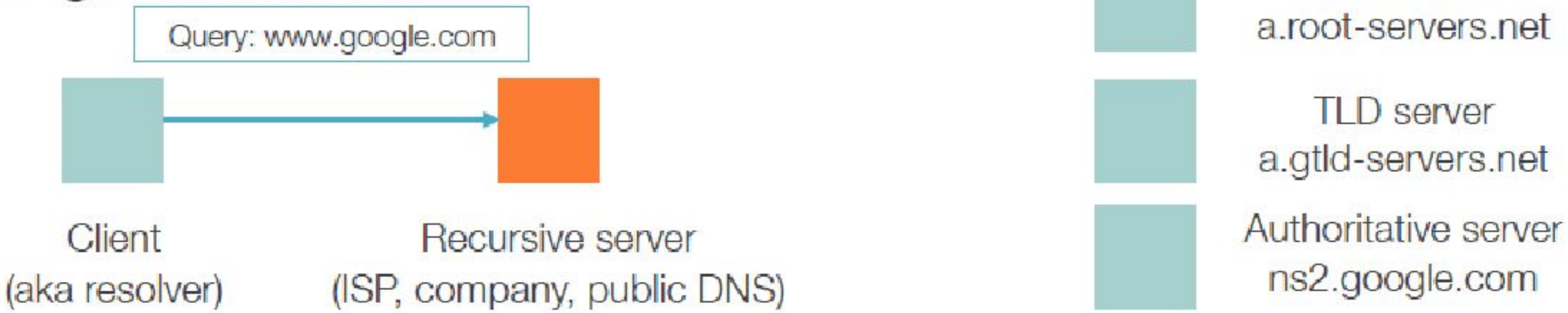
Name Resolution

- Clients use DNS to resolve a domain name to an IP address. Name servers store DNS records and respond to domain name queries.
- Many clients **use a recursive name server** located in their network to do work on their behalf. If this domain is unknown to the recursive server, it can **start at the root**. Each name server will provide the most specific answer it can. The recursive server will **iterate** through the DNS hierarchy of zones to find an **authoritative name server** that can answer the query.



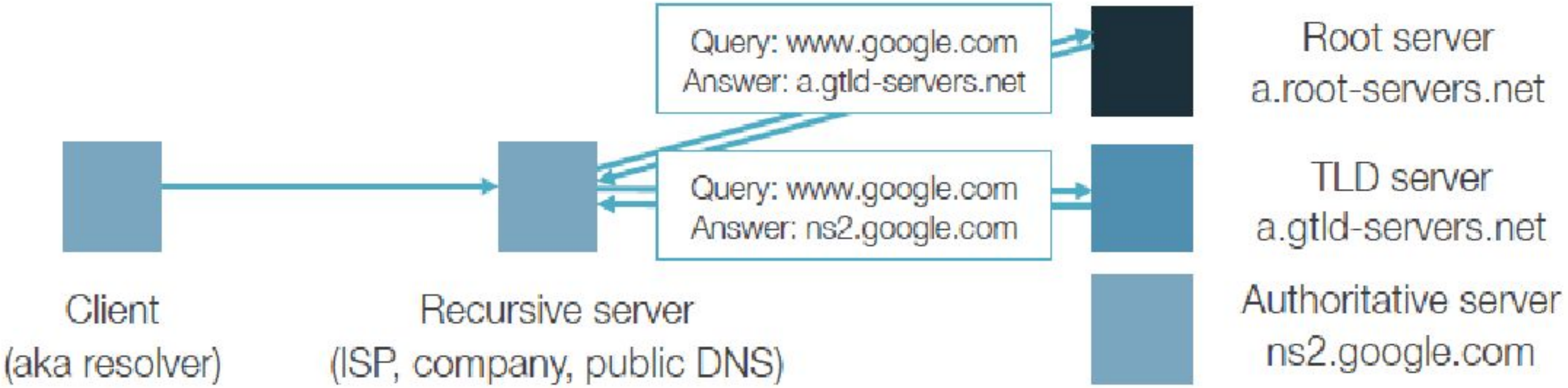
Recursive Name Servers

- Recursive name servers make **recursive queries** on behalf of DNS clients. They typically exist within ISPs, enterprise networks and public DNS servers (e.g. Google public DNS 8.8.8.8).
- Many recursive servers only respond to queries from within their own network. Some, called **open resolvers**, will respond to queries from any source.
- Most recursive servers also **cache** DNS records, which are valid for the length of the TTL.



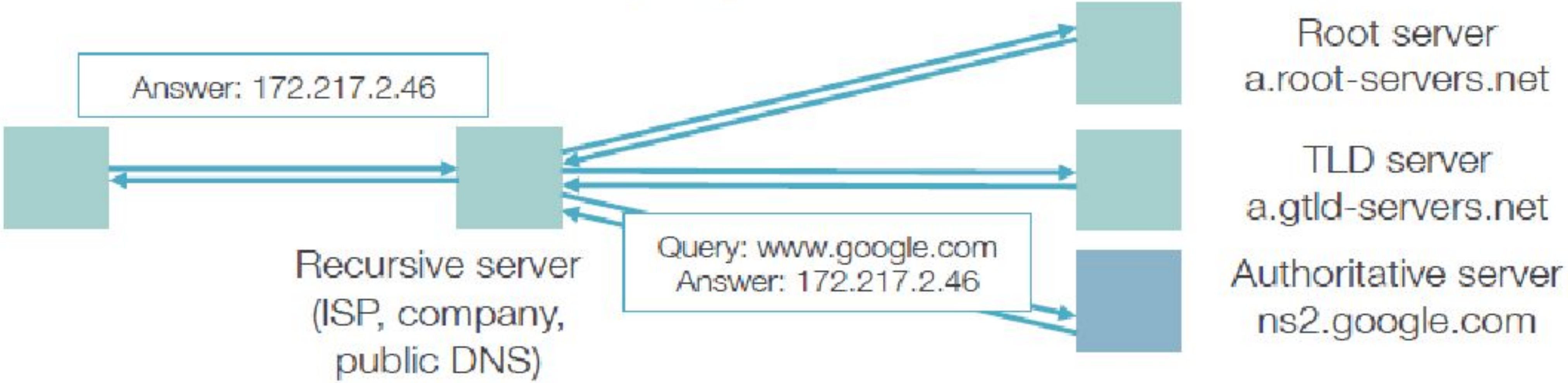
Root and TLD Name Servers

- There are 13 **root name servers** that sit atop the DNS hierarchy and are hard coded into any application that uses DNS. These root name servers maintain a list of the **top-level domain servers** (.com, .uk, .net, etc.).
- The answers provided by root and TLD name servers contain the name servers for the next known subdomain.



Authoritative Name Servers

- Authoritative name servers have **authority** to answer queries from other name servers or from DNS clients. The DNS records in an authoritative name server are maintained by domain administrator.
- A set of authoritative name servers are assigned for each zone. These may be maintained by the organization itself, or by an external company (UltraDNS, Akamai, Dyn, etc). Many organizations will split name servers between multiple providers for redundancy.


Answer: 172.217.2.46
Root server
a.root-servers.net
TLD server
a.gtld-servers.net
Recursive server
(ISP, company,
public DNS)
Query: www.google.com
Answer: 172.217.2.46
Authoritative server
ns2.google.com