Week-4 Network Services

- Why DNS?
  - MAC address - 48-bit binary numbers - written out in 6 grouping of 2 hexadecimal digits;
  - Remembering numbers is a tedious task than words.

- DNS - Domain Name System - A global and highly distributed network service that resolves strings of letters into IP addresses for you.

- Example for a weather website - IP address - 184.29.131.121 while the Domain name is - www.Weather.com - easier to remember the domain name.
- The IP address for a domain name can also change all the time - in case of administrative changes, movements of the data centers.
- The Domain name - The term we use for something that can be resolved by DNS;
- DNS provides geographical data utlilty by enabling clients to gather data from servers that are collated, New Delhi server -> New Delhi, New york -> New York clients; Cause of the global structure DNS lets organizations decide if youre in the region resolve the domain name to this IP.

Name Resolution

Name Resolution - The process of using a DNS system to convert Domain names into IP addresses;
- MAC address are hoardcoded to the hardware components;

4 Things that must be configured for a host to operate on a network in an expected way in standard modern networking are:
---
1. IP address
2. Subnet mask
3. Gateway for a host
4. DNS server

5 types of DNS servers:

1. Caching name servers - Purpose is to store known domain name lookups for a certain amount of time
2. Recursive name servers - Purpose is to store known domain name lookups for a certain amount of time; Perform full DNS resolution requests
3. Root name servers
4. TLD name servers
5. Authoritative name servers

- All domain names in the global DNS system have a TTL/ time to live;
- Time to Live - (TTL) - A value, in seconds, that can be configured by the owner of a domain name for how long a name server is allowed to cache an entry before it should discard it and perform a full resolution again;

Local Recursive server performs a full recursive resolution

1. Contact a root named server; There are 13 Root name servers/ 13 authorities that provide root name lookups as service - responsible for directing queries towards appropriate TLD name servers. They are distributed across the globe via anycast;
   * Anycast - A technique that is used to route traffic to different destination depending on factors like location, congestion, or ink health;

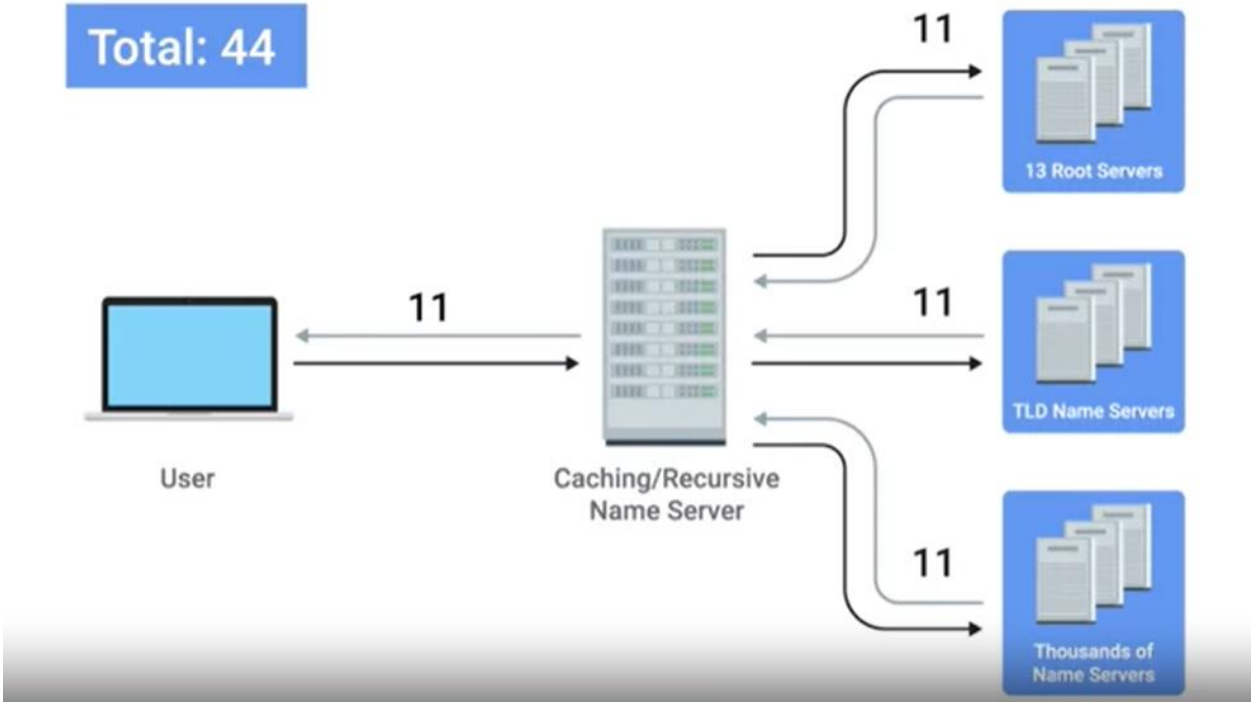
2. The root servers will respond to a DNS lookup with TLD(Top-level domain - Last part of any domain name - .com/.org/.edu, etc) name server that should be queried;
3. For each TLD there is a TLD name server / global distribution;
4. The TLD servers will respond again with a redirect, informing the computer performing the name lookup with what authoritative name server to contact;
5. The DNS lookup could be redirected at the authoriative server for the respective domain name;
6. The authoritative server would finally provide the actual IP of the server in question;

DNS and UDP

- DNS is an example of an application layer service that uses UDP for the transport layer instead of TCP;
- UDP is connectionless - there is no setup or teardown of a connection;

- A single DNS request and its response can fit inside a single UDP datagram - ideal for a connectionless protocol;
- DNS can generate a lot of traffic, caches of DNS entries are stored on local machines and caching name severs, for the full resolution to be processed all lot of traffic will exist;

Full DNS lookup to take place via TCP

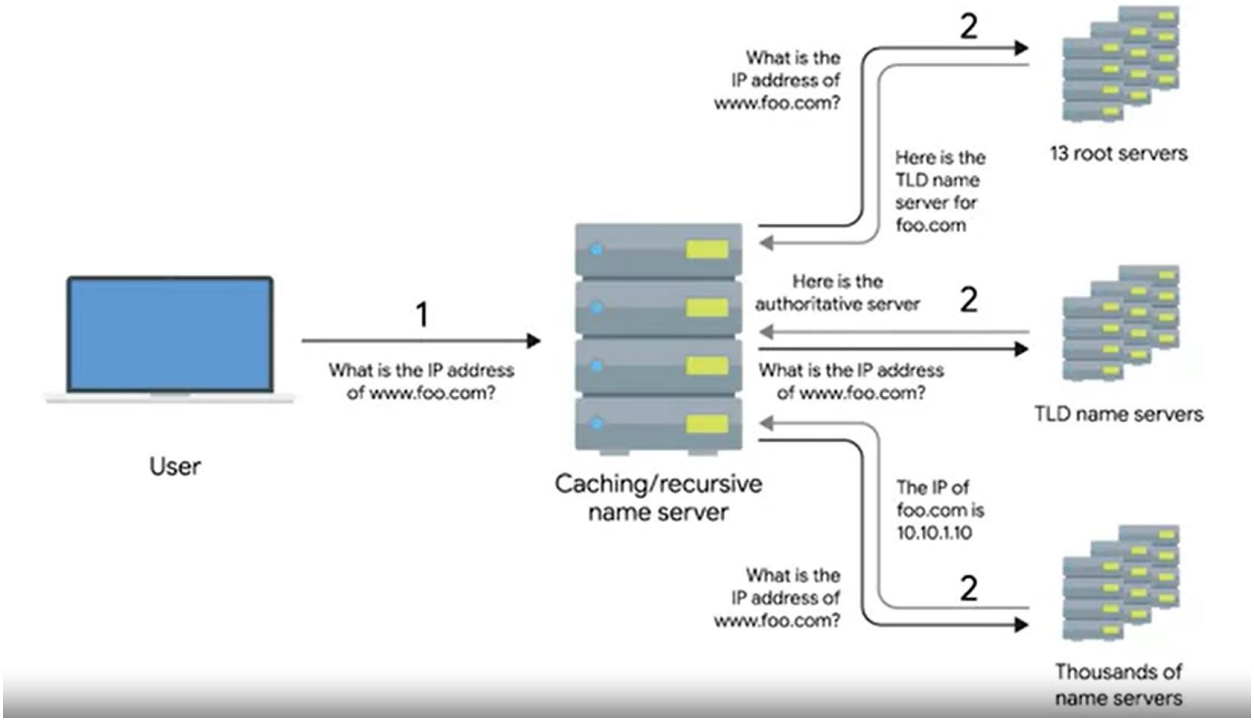


1. The host making the DNS resolution request would send a SYN packet to the local name server on port 53 (port DNS - Domain Name System - listens on);
2. The name servers responds with a SYN ACK packet;
3. The original host needs to respond with an ACK in order to complete the three-way handshake - connection has been established;
4. The original host has to send the actual request (IP address for a food accomplice);
5. The name server would respond with another ACK;
6. The caching server needs to talk to root name server to find who is responsible for the.com TLD; (3 way handshake) (opened) Four way handshake (closed connection) -- process requires 11 packets
- The recursive server has the correct TLD - top-level domain (.com, .edu. org, etc)name server;
7. The recursive server needs to repeat the entire process to discover proper authoritative name servers; -- requires 11 packets
8. The recursive server repeats the process inorder to get the ip of food.com (TLD); --- requires 11 packets;
9. The recursive/cachine name server responds to the original host; - 1 packet;

10. The host responds with an ACK confirmation; - 1 packet;
11. Finally the TCP connection needs to be closed - four-way handshake; - 4 packets;

Total packets : 44 packets; (minimum)

- Full DNS lookup to take place via UDP



1. The host sends a UDP packet to its local name server on port 53 asking for the IP address for food.com; - 1 packet
2. The local name server acts like a recursive server and sends up a UDP packet to root sever;
3. The root server sends a response containing the proper TLD name server;
4. The recursive name server sends a packet to the TLD server;
5. Receives back a response containing the correct authoritative server;
6. The recursive server sends its final request to the authoritative name server;
7. The Authoritative name server sends a response containing IP for food.com;
8. The recursive name server sends its final request to DNS resolver / host that made the request;

Total -> 8 packets;
(In case it doesn't get the packet, it request again);

Name Resolution in practice

Resource Record Types
DNS (Domain name system) - operates with a set of defined resource record types - this allow for different types of DNS resolutions to take place.

A record

- Most common resource record - A record - It is used to point a certain domain name at a certain IPv4 IP address;
- A single A record is configured for a single Domain name, but a single domain name can have multiple A records - Allows for a DNS Round Robin technique;
- DNS round robin - is used to balance traffic across multiple IPs - iterate over a list of items one by one in an orderly fashion – in order to equally balance each entry on the list thats selected;
    - Example - consider www.microsoft.com - domain name - likely sees a lot of traffic - to balance this traffic across multiple servers - four A records are configured at the authoritative server for microsoft.com domain;
- The IPs - 10.1.1.1, 10.1.1.2, 10.1.1.3, and 10.1.1.4 are used;
- When DNS resolver performs a look-up of www.microsoft.com - all four IPs will be returned in the order first configured - 10.1.1.1, 10.1.1.2, 10.1.1.3, and 10.1.1.4;
- The next computer to perform a look-up for www.microsoft.com - all four IPs will be returned in response but in different order - 10.1.1.2, 10.1.1.3, 10.1.1.4,and 10.1.1.1;
- This cyclic process keeps continuing;

AAAA - Quad A
- Similar to A record but instead of an IPv4 address it returns a IPv6 address;

CNAME (Canonical Name) record

- It redirects traffic from one domain to another;
- microft.com => resolve to www.microsoft.com => by configuring the CNAME record for microsoft.com that resolves to www.microsoft.com - the resolution client will perform another resolution attempt - www.microsoft.com;
- Then use the IP returned by the second attempt;
- They enable to change the canonical IP address of the server at one place;

Two domain names redirected to the same place - 2 ways

1. Identical A records can be setup for both microsoft.com and www.microsoft.com domain names - if the underlying IP address changes - then A records for both the domain names need to be changes;
2. By setting a CNAME that points microsoft.com at www.microsoft.com - then only A records for www.microsoft.com needs to be changed;
- Clients pointing at the new domain will get the IP address;

MX records - mail exchange

- Record server is used to deliver e-mails to the correct server
- Many companies run their web and mail servers on different machines with different IPs

SRV - service record
- Used to define the location of various specific services - CalDAV - Calendar and Scheduling service;

TXT record - text
- Intended for text , additional data intended for other computers to process, used to communicate configuration preferences about the network service that other organizations are entrusted to handle for your domain;

NS and SOA records - define authoritive information about DNS zones;

Anatomy of Domain name
- 3 parts
www.google.com

- .com - last part - TLD - Top-level domain name; - handled by ICANN - The Internet Corporation for Assigned Names and Numbers;
- google - Domains - Used to demarcate where control moves from TLD name server to an authoritative name server; - registered and chossen by any individuals/ companies;
- www - subdomain / hostname;

- All together - fully qualified domain name (FQDN) - 255 characters
- DNS can technically support 127 levels of domain i total for a single fully qualified domain name -each individual sections can be - 63 characters long;

DNS zones

- ✓ They are an hierarchical concept;
- ✓ The root name servers are responsible for the root zones;
- ✓ Each TLD name server is responsible for the zone covering its specific TLD;
- ✓ Authoritative name servers are responsible for even fine grained zones;
- ✓ The root and TLD name servers are authoritative name servers - zones are special case;
- ✓ Zones don't overlap;

- Allows for easier control over multiple levels of a domain;

- As the number of resource records in a single domain increase its difficult to manage, network administrators can ease their pain by splitting the configurations into multiple zones;
- Consider - largecompany.com - offices in Tokyo, Bangalore and London - with 200 members each - total of 600 Unique desktop number - 600 A records - configured in a single DNS zone;
- If it splits up each office into its own zone - ty.largecompany.com, bl.largecompany.com, ln.largecompany.com - as subdomains with their DNS zones and total of four authoritative name servers - largecompany, ty.largecompany.com, bl.largecompany.com, and ln.largecompany.com;

- Zones are configured through Zone files - Simple configuration files that declare all resource records for a particular zone;
- Contains an

SOA - Start of Authority resource record declaration - declares the zone and the name server name that is authoritative for it;
NS records - Indicates - other name servers responsible for the zone;
A
Quad A
CNAME
Configurations - Default TTL values;

- Reverse lookup zone files - These let DNS resolvers ask for an IP and get FQNS (fully qualified domain name) associated with it returned; - using a PTR;
  - PTR - Pointer resource record - Resolves an IP to a name;