ITT565
Chapter 4
Domain Name System (DNS)

Domain Name System (DNS)

- When you open your web browser and type in hub.tutsplus.com to find something interesting to learn, your computer can find a server with the IP address **190.93.242.181**.
- Among other technologies, a protocol called DNS helps your computer in finding that server.

https://computers.tutsplus.com/tutorials/how-to-change-your-dns-for-safer-faster-browsing--mac-61232

apt-get install dnsutils

DNS: A Definition and Example

- DNS stands for *Domain Name System* and is a protocol, or language, that computers use when talking to each other.
- Every device on the public Internet has an IP address;
- DNS is like a phonebook that associates a domain name, hub.tutsplus.com for instance, with the server's IP address, 190.93.242.181.

https://computers.tutsplus.com/tutorials/how-to-change-your-dns-for-safer-faster-browsing--mac-61232

DNS concepts:

1. 3 types of DNS servers—DNS Resolver, DNS Root Server, and Authoritative Name Server
2. 3 types of DNS queries—recursive, iterative, and non-recursive
3. 10 types of common DNS records—including A (host address), AAAA (pronouns as Quad A is IPv6 host address), CNAME (Canonical name for an alias), MX (Mail eXchange), and NS (Name Server)

https://ns1.com/resources/dns-types-records-servers-and-queries

DNS Resolver

- A DNS resolver, also called a recursive resolver, is a server designed to receive DNS queries from web browsers and other applications.
- The resolver receives a hostname - for example, www.example.com - and is responsible for tracking down the IP address for that hostname.
- A component called a DNS Resolver is responsible for checking if the hostname is available in local cache, and if not, contacts a series of DNS Name Servers, until eventually it receives the IP of the service the user is trying to reach, and returns it to the browser or application.
- nslookup is a command-line tool that lets you test and troubleshoot Domain Name System (DNS) resolution.
- To start nslookup, open a command prompt and enter nslookup

***** Domain resolution is the process of converting domain names to IP addresses.***
The resolution of the domain name is done by the DNS server . Domain resolution is also called domain pointing, server settings, domain configuration, reverse IP registration, and so on.

DNS Root Server

- Root servers, or DNS root servers, are name servers that are responsible for the functionality of the DNS as well as the entire Internet.
- They're the first step in the name resolution of any domain name, meaning they translate domain names into IP addresses
- A root name server is a name server for the root zone of the Domain Name System of the Internet.
- It directly answers requests for records in the root zone and answers other requests by returning a list of the authoritative name servers for the appropriate top-level domain (TLD)

Authoritative Name Server

- An authoritative name server is a name server that gives answers in response to questions asked about names in a zone.
- An authoritative-only name server returns answers only to queries about domain names that have been specifically configured by the administrator.
- The authoritative nameserver is typically the DNS provider or the DNS registrar (like GoDaddy which offers both DNS registration and hosting).
- And here we can find the DNS record that maps example.com to the IP address 127.66

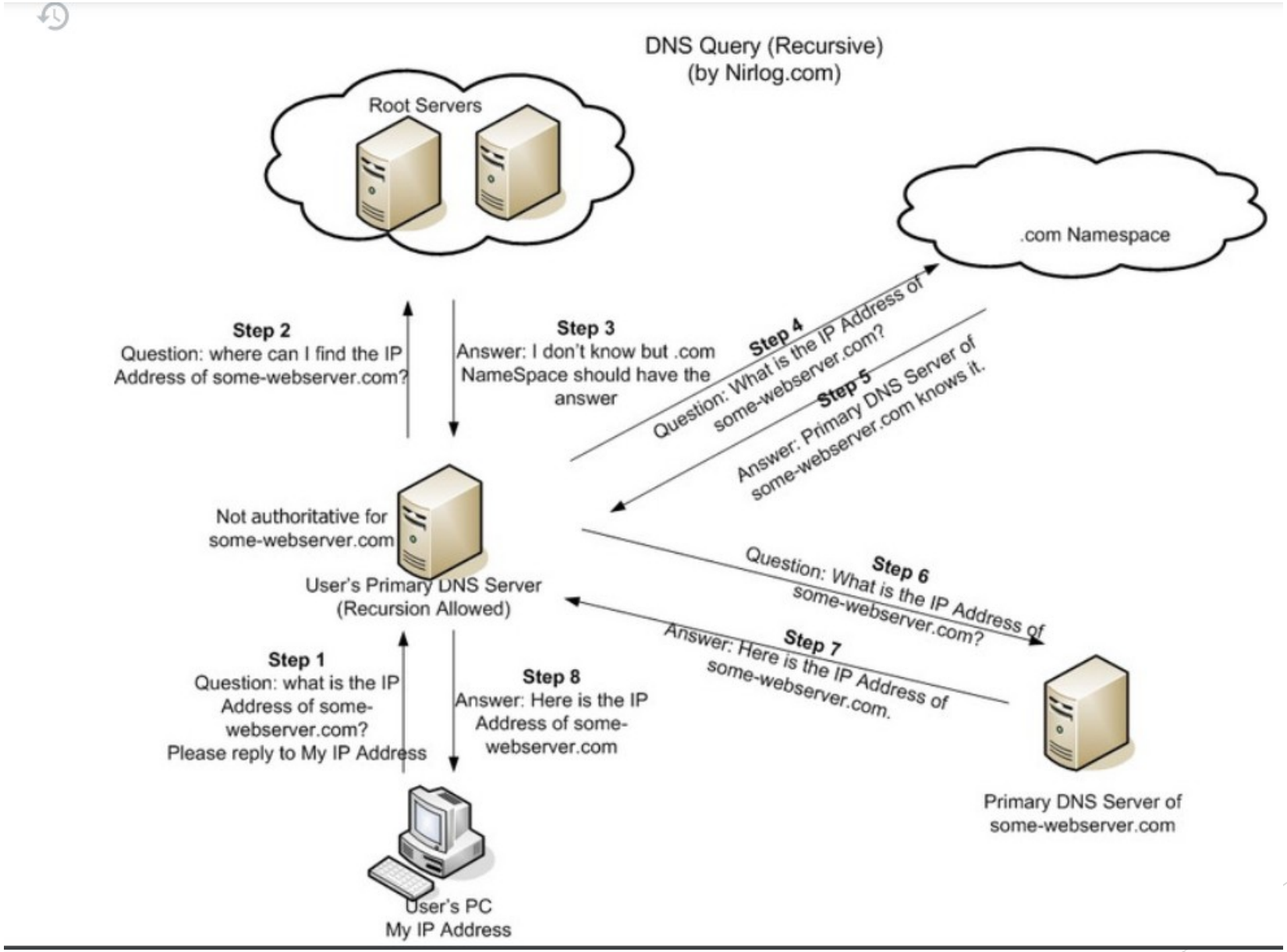
```
apt-get install dnsutils
```

- **How DNS works:**

1. **Connect to a wireless network; the router tells your computer what DNS server to use, usually the router itself.**
2. **Type hub.tutsplus.com into the web browser; the computer asks the router for the IP address for hub.tutsplus.com so it can connect to the server.**
3. **The router asks a DNS server for the IP address. If other devices have previously requested the Tuts+ Hub, the router may have the result cached already and may skip this step.**
4. **The router receives a reply from a public DNS server and sends that on to your computer; among other details, it includes an IP address such as 190.93.242.181.**
5. **The computer initiates a connection to that IP address and continues with loading the page. If the page needs resources from another domain, as many do, the computer will go through the whole process again for each domain or subdomain.**

- **Frankly, it's amazing that this whole process, called the *resolution*, takes less than a second. In fact, DNS requests can take as little as 40 milliseconds! YSlow, DNS lookups on average take between 20-120 milliseconds to complete.**

https://computers.tutsplus.com/tutorials/how-to-change-your-dns-for-safer-faster-browsing--mac-61232


DNS Query (Recursive)
(by Nirlog.com)
Root Servers
.com Namespace
Step 2
Question: where can I find the IP Address of some-webserver.com?
Step 3
Answer: I don't know but .com NameSpace should have the answer
Step 4
Question: What is the IP Address of some-webserver.com?
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.
Not authoritative for some-webserver.com
User's Primary DNS Server
(Recursion Allowed)
Step 6
Question: What is the IP Address of some-webserver.com?
Step 7
Answer: Here is the IP Address of some-webserver.com.
Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address
Step 8
Answer: Here is the IP Address of some-webserver.com
Primary DNS Server of some-webserver.com
User's PC
My IP Address

```
apt-get install dnsutils
```

- **Public DNS Servers**
  - **Your home router is likely set by default to use your ISP's DNS servers, which may or may not be very reliable.**
- **There are a number of third-party DNS servers available as well.**
  - **OpenDNS (208.67.220.220 and 208.67.222.222)**
    - **OpenDNS is an American company providing Domain Name System (DNS) resolution services—with features such as phishing protection, optional content filtering, and DNS lookup in its DNS servers—and a cloud computing security product suite, Umbrella, designed to protect enterprise customers from malware, botnets, phishing, and targeted online attacks.**
  - **Google Public DNS (8.8.8.8 and 8.8.4.4).**
    - **Google Public DNS is a Domain Name System service offered to Internet users worldwide by Google. It functions as a recursive name server. Google Public DNS was announced on 3 December 2009, in an effort described as "making the web faster and more secure". As of 2018, it is the largest public DNS service in the world, handling over a trillion queries per day.**
- **Every major DNS service has at least primary and secondary servers to ensure that requests will always be answered. When changing DNS server settings, you'll want to make sure that you specify at least two servers, although you**

More about DNS

- IP assigns 32-bit addresses to hosts (interfaces)
  - Binary addresses easy for computers to manage
  - All applications use IP addresses through the TCP/IP protocol software
  - Difficult for humans to remember:

    % telnet 134.82.11.70

- The Domain Name System (DNS) provides translation between symbolic names and IP addresses
- DNS runs over UDP and uses port 53 of messages less than 512 bytes; otherwise, it uses TCP port 53

Structure of DNS names

- Each name consists of a sequence of alphanumeric components separated by periods
- Examples:

  www.eg.bucknell.edu

  www.netbook.cs.purdue.edu

  charcoal.eg.bucknell.edu

- Names are hierarchical, with most-significant component on the right
- Left-most component is computer name

Structure of DNS names

- Top level domains (right-most components; also known as TLDs) defined by global authority

com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military organization

- Organizations apply for names in a top-level domain:
  - kfupm.edu
  - macdonalds.com
- Organizations determine own internal structure
  - ccse.kfupm.edu
  - cs.purdue.edu

*TDL – Top domain level

Geographic structure

- Top-level domains are US-centric
- Geographic TLDs used for organizations in other countries:

TLD	Country
.uk	United Kingdom
.fr	France
.ch	Switzerland
.in	India

- Countries define their own internal hierarchy: ac.uk and .edu.au are used for academic organizations in the United Kingdom and Australia. In SA, it is edu.sa.

Domain names within an organization

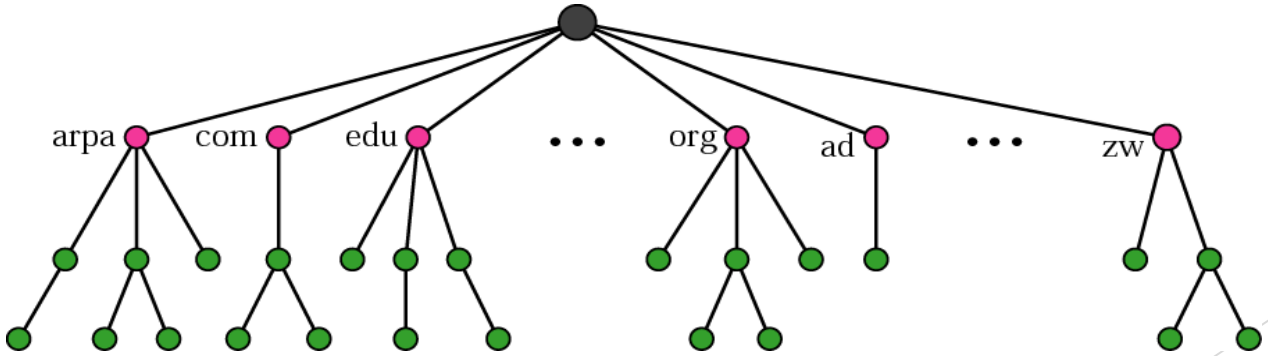
- Organizations can create any internal DNS hierarchy
- Uniqueness of TLD and organization name guarantee uniqueness of any internal name (much like file names in your directories)
- All but the left-most component of a domain name is called the domain for that name:

Name	Domain
www.netbook.cs.purdue.edu	netbook.cs.purdue.edu
regulus.eg.bucknell.edu	eg.bucknell.edu
coral.bucknell.edu	bucknell.edu

- Authority for creating new subdomains is delegated to each domain
  - Administrator of kfupm.edu has authority to create eg.kfupm.edu and need not contact any central naming authority
- DNS domains are logical concepts and need not correspond to physical location of organizations
  - DNS domain for an organization can span multiple networks

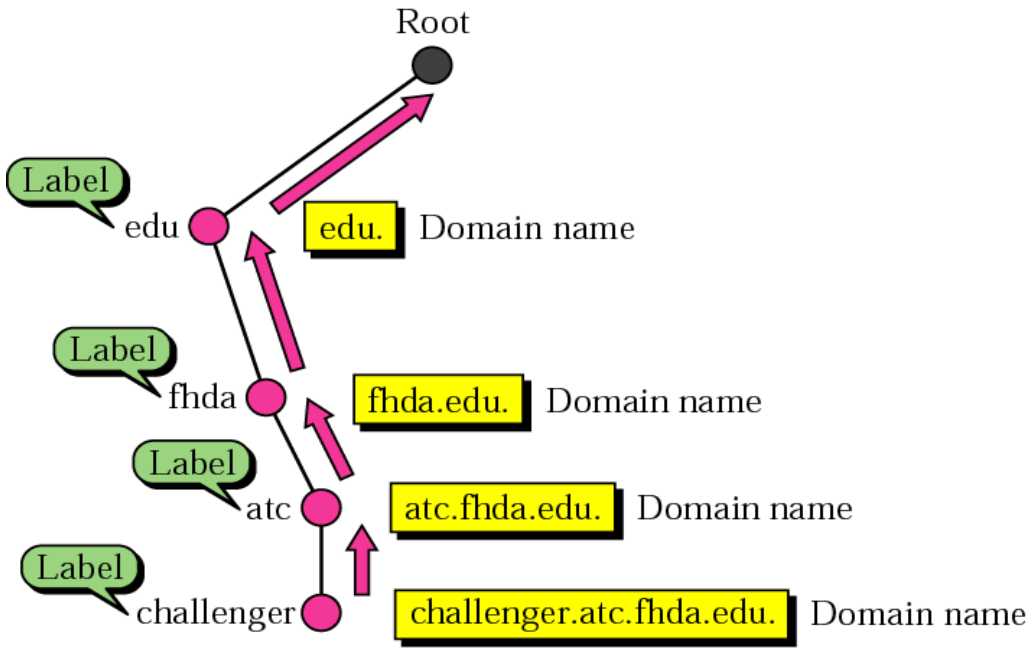
Domain name space

- Names are defined in an inverted-tree structure with the root at the top.
- Can have 128 levels: level 0 (root) to level 127.
- Label:
  - Each node in the tree has a level
  - Maximum of 63 characters.
  - Root label is a null string (empty string).
  - Children of a node have different labels.



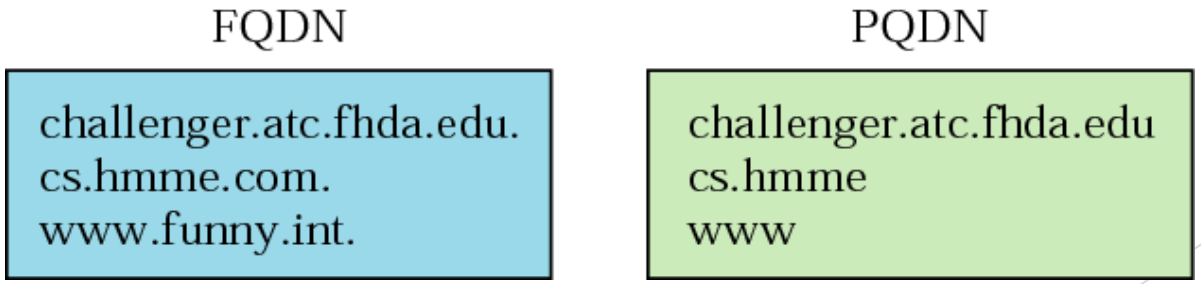
Domain names and labels

- Full domain name is a sequence of *labels* separated by dots.
- Domain names are always read from the node up to the root. Last label is the label of root (null). So, full domain name always ends in a null label [means dot].



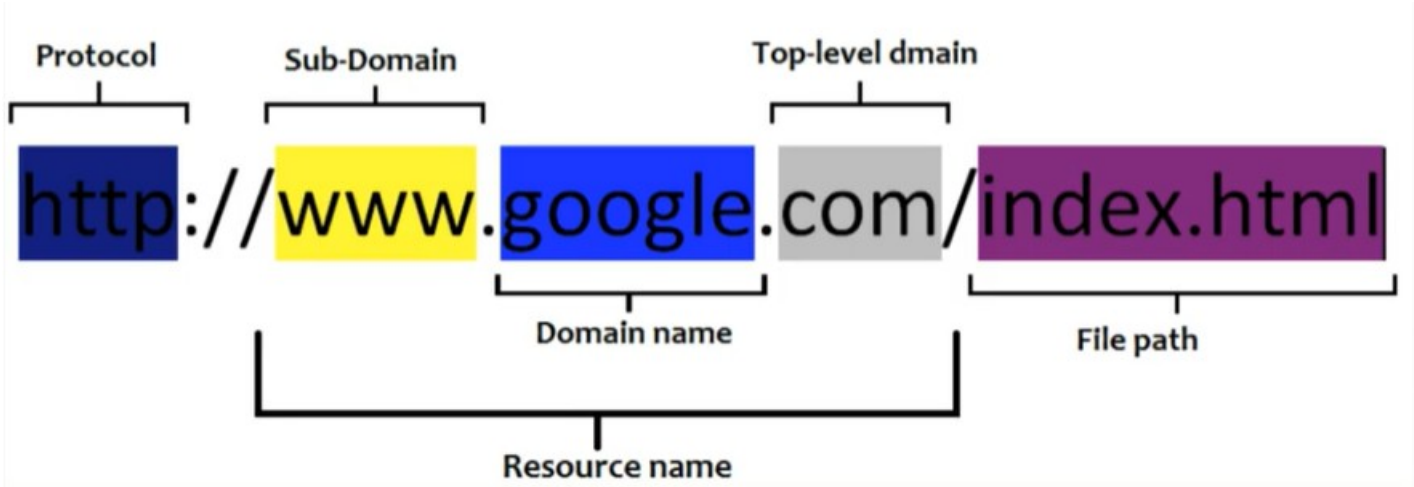
FQDN and PQDN

- Fully Qualified Domain Name (FQDN) or Absolute Domain Name
  - Label is terminated by a null string.
  - Contains the full name of a host.
- Partially Qualified Domain Name (PQDN) or Relative Domain Name
  - Not terminated by a null string.
  - Used when the name to be resolved belongs to the same site as the client.
  - Resolver supplies the missing part called a suffix.



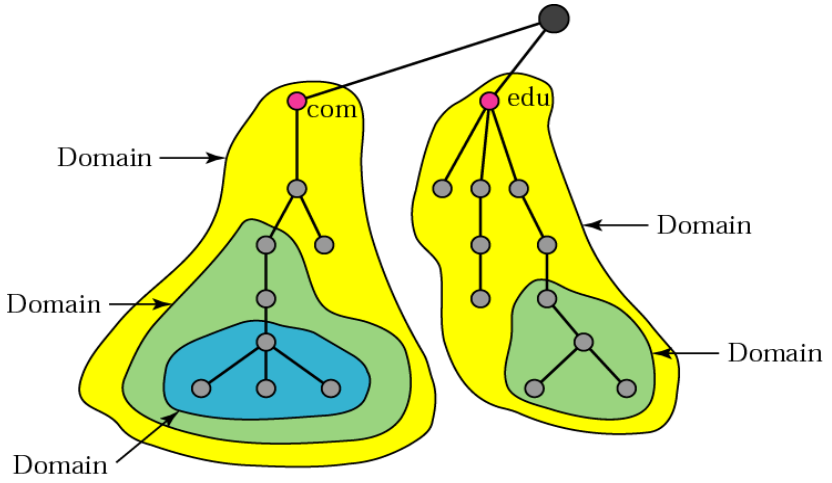
Fully Qualified Domain Name

- **Sometimes also referred to as an absolute domain name**
- **It is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System.**
- **It specifies all domain levels, including the top-level domain and the root zone.**



Domains

- Domain:
  - Subtree of the domain name space.
  - Name of the domain is the domain name of the node at the top of the subtree.
  - A domain can be divided into subdomains.



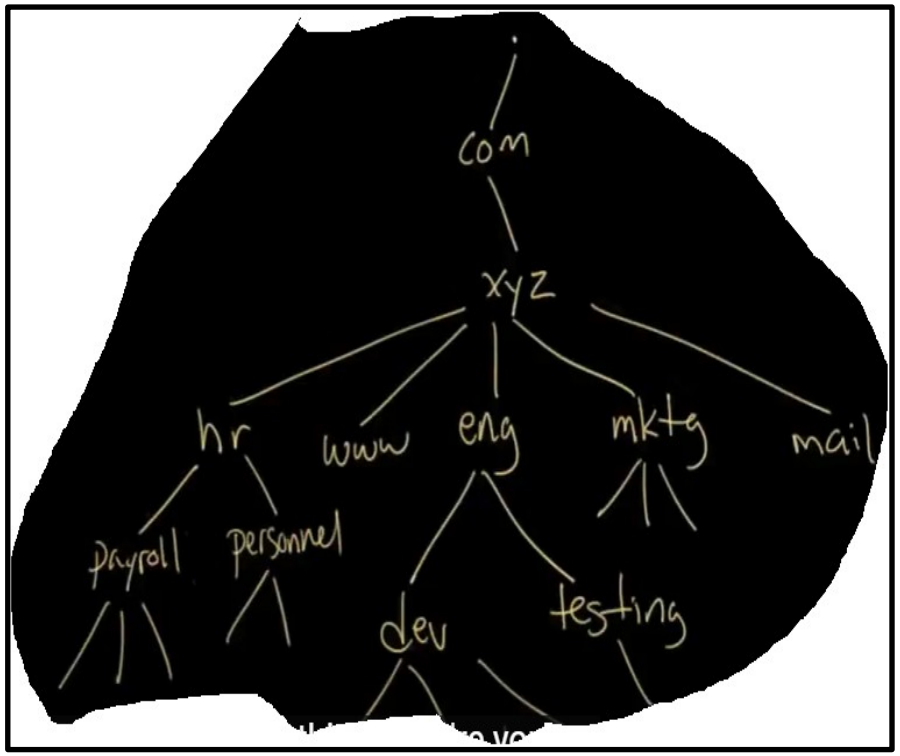
DNS and client-server computing

- DNS names are managed by a hierarchy of DNS servers
- Root server at top of tree knows about next level servers.
- Next level servers, in turn, know about lower level servers

- Some Jargon
  - Each DNS server is the authoritative server for the names it manages
  - What a server is responsible for or has authority over is called a *zone*. A *domain* can span multiple servers.
  - *Primary server* is also called authoritative server
  - *Second server* has a copy

- **What are DNS ZONES | DNS Zones explained | DNS Zones and Delegation | Tutorial on DNS Zones**
  https://www.youtube.com/watch?v=JIwi6ii-rzI

Explained

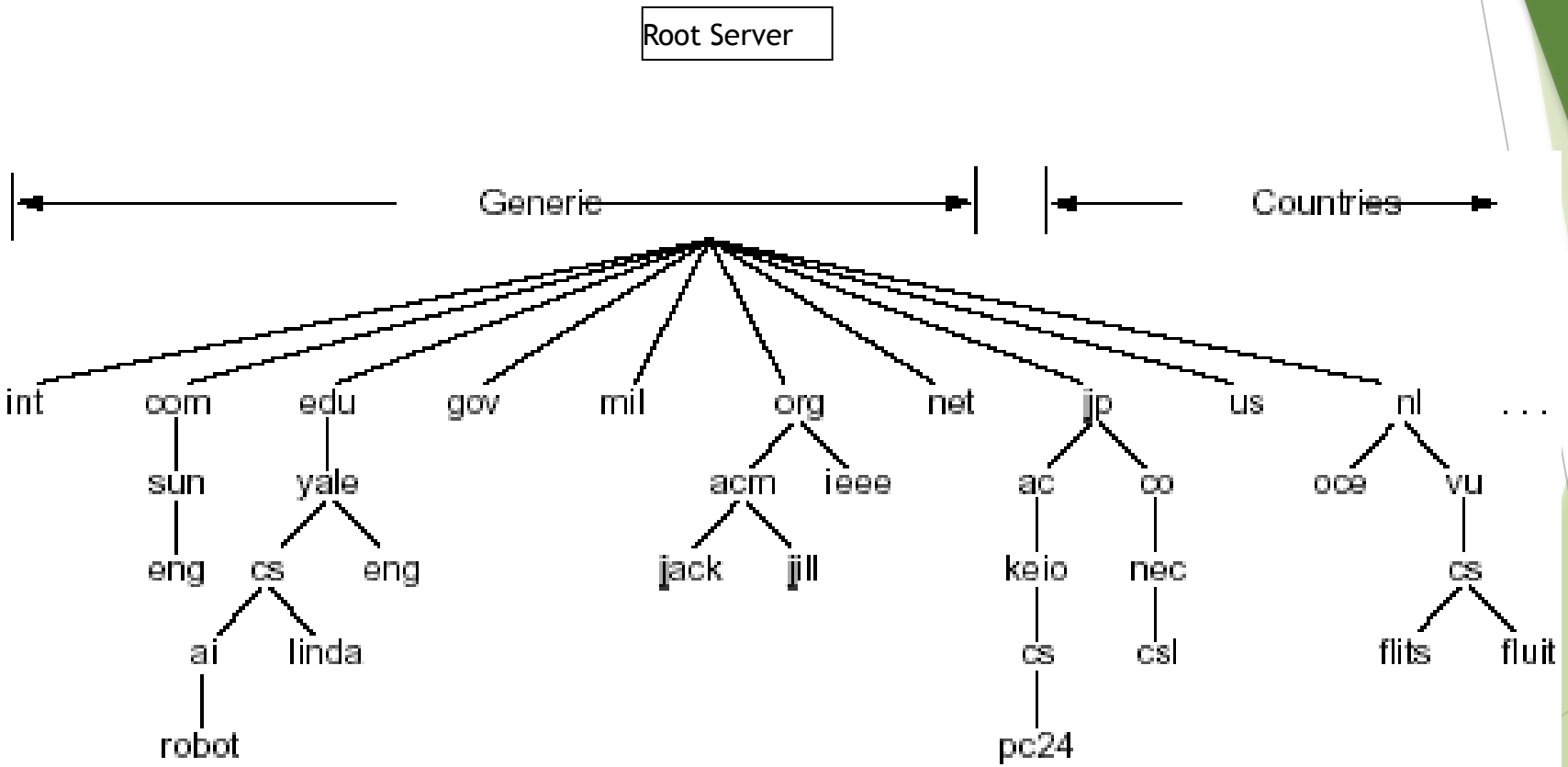


Quiz: Create your own structure

- Click to add Text

Root Name Servers:

A root name server is a name server for the root zone of the Domain Name System (DNS) of the Internet. It directly answers requests for records in the root zone and answers other requests by returning a list of the authoritative name servers for the appropriate top-level domain (TLD)



Choosing DNS server architecture

- Small organizations can use a single server
  - Easy to administer
  - Inexpensive
- Large organizations often use multiple servers
  - Reliability through redundancy
  - Improved response time through load-sharing
  - Delegation of naming authority
- Locality of reference applies - users will most often look up names of computers within same organization

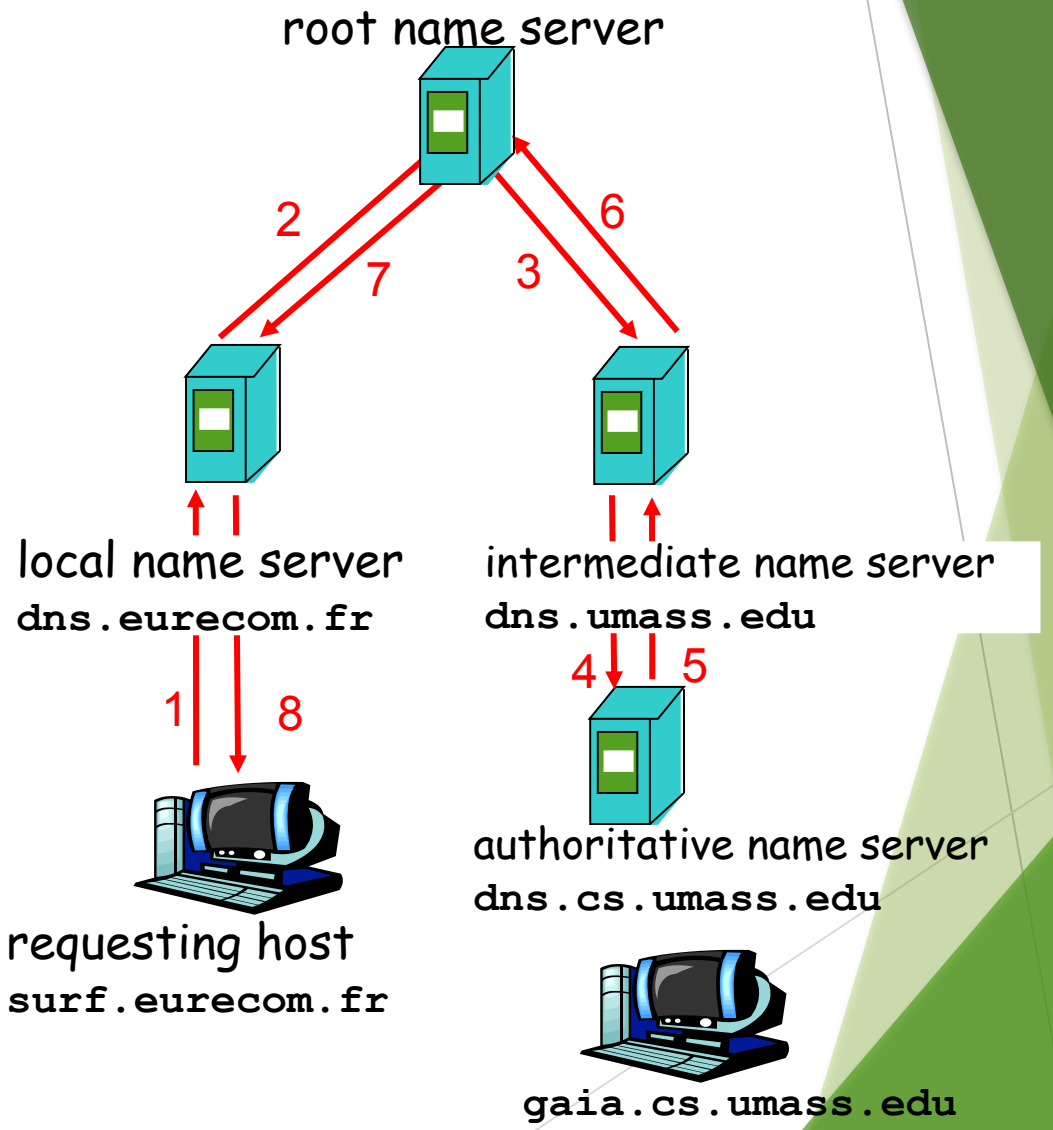
- ***All DNS servers are linked together to form a unified system. Each server knows how to reach a root server and how to reach servers that are authorities for names further down the hierarchy.***

Name Resolution

host **surf.eurecom.fr** wants IP address of **gaia.cs.umass.edu**

1. contacts its local DNS server, **dns.eurecom.fr**
2. **dns.eurecom.fr** contacts root name server, if necessary
3. root name server eventually contacts authoritative name server, **dns.cs.umass.edu**, if necessary

- This is called "Recursive Resolution"



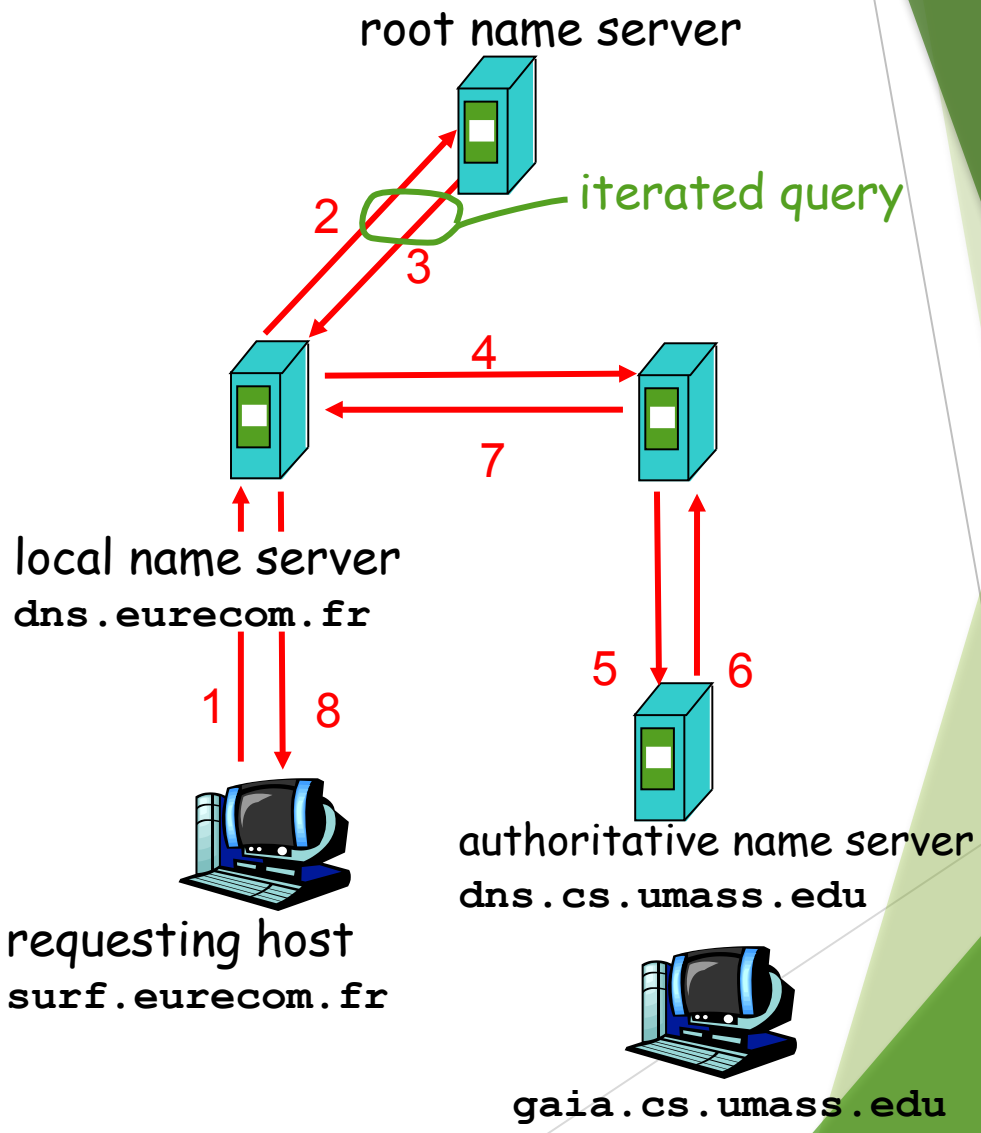
Types of Queries

recursive query:

- puts burden of name resolution on contacted name server
- heavy load?

iterated query:

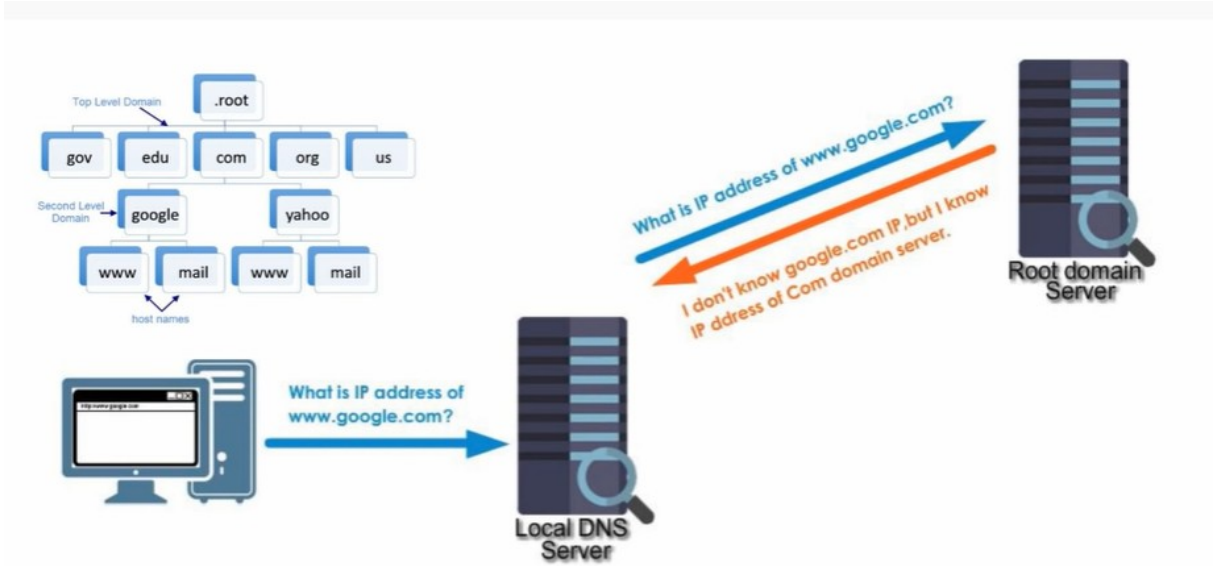
- contacted server replies with name of server to contact
- "I don't know this name, but ask the following server(s)"
- Gives more control to client



- **Non-Recursive Query**
  - **A non-recursive query is a query in which the DNS Resolver already knows the answer.**
  - **It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname.**
  - **In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.**

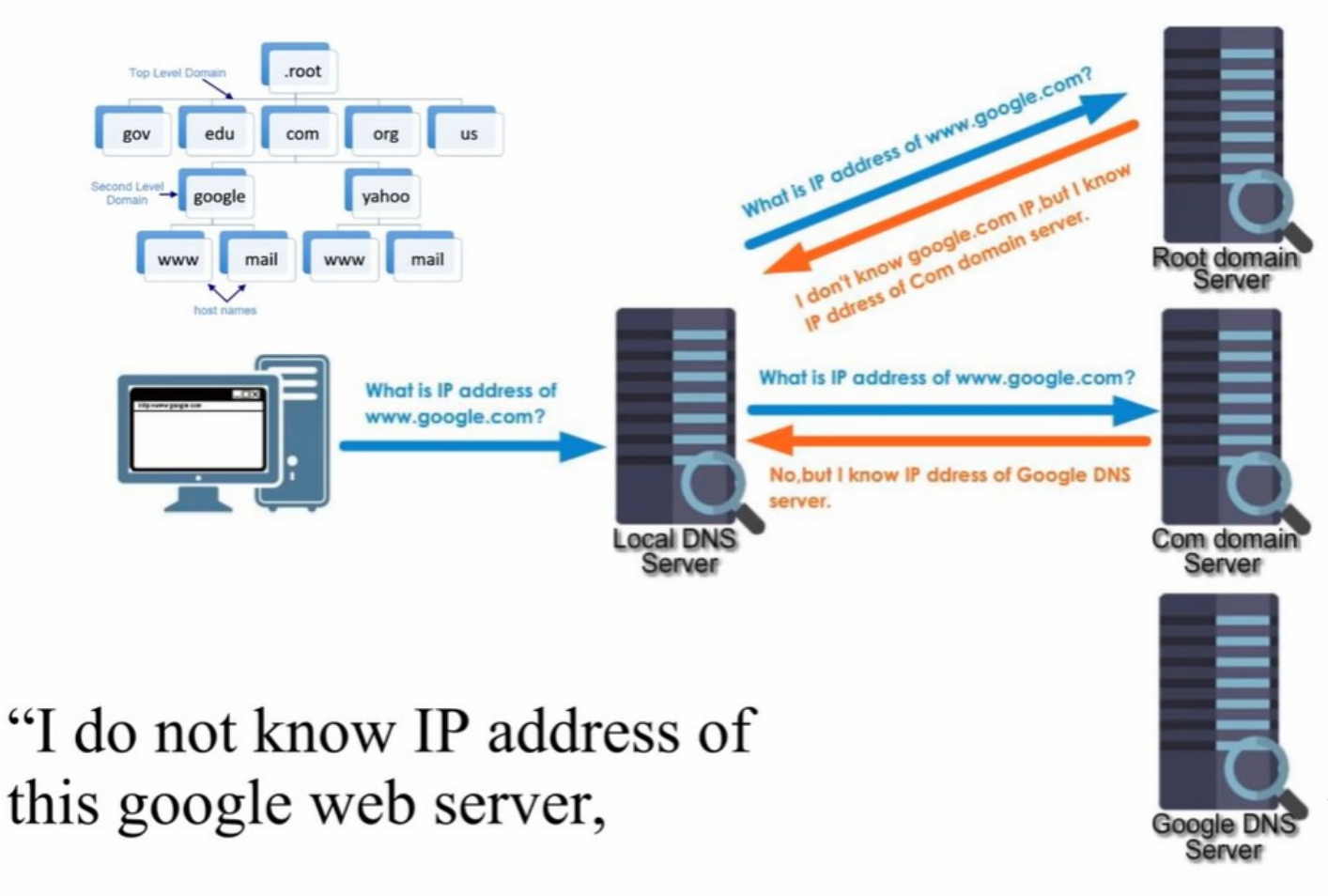
https://ns1.com/resources/dns-types-records-servers-and-queries

Searching for www.google.com



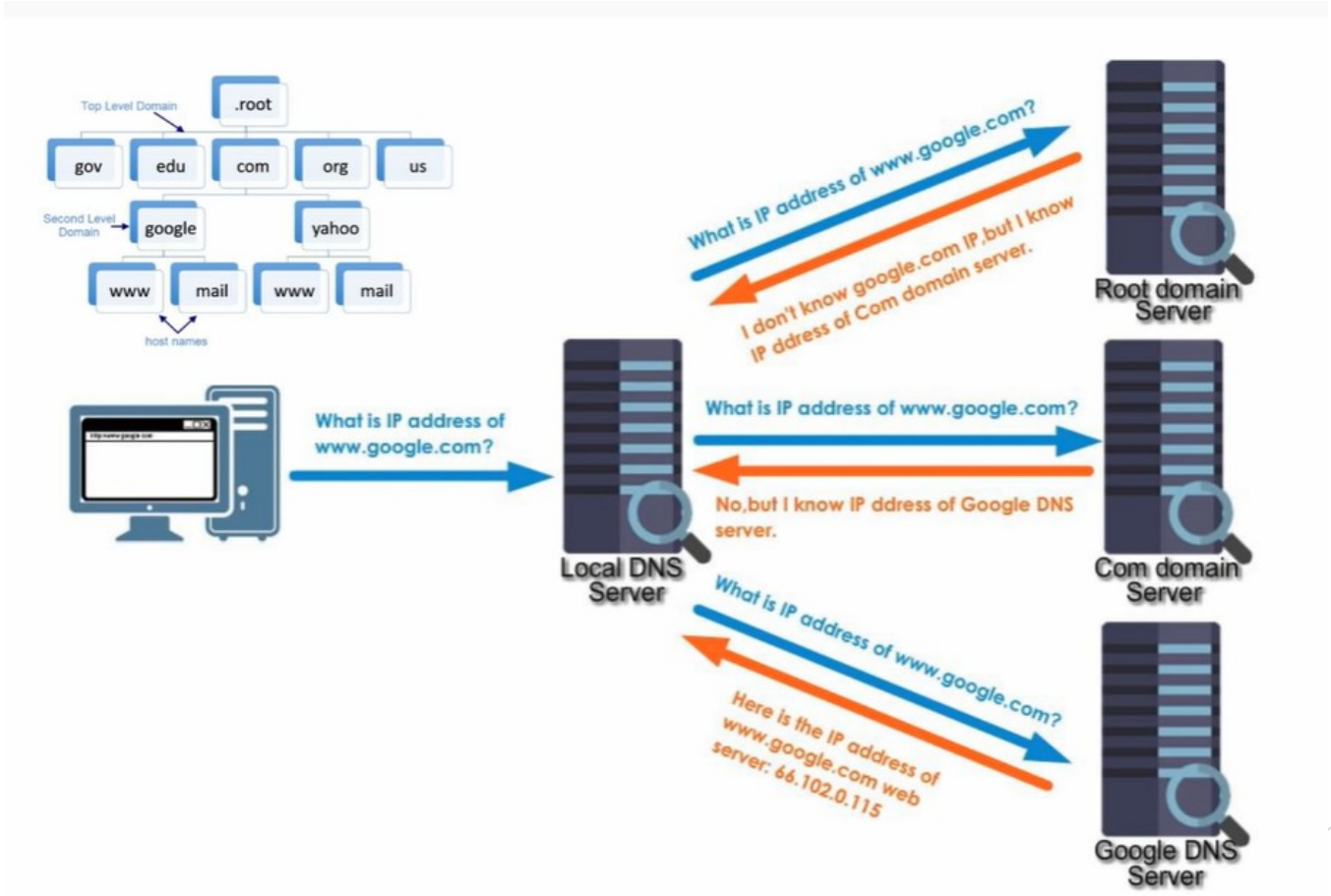
"I don't know the IP address of www.google.com, but I do know an IP address of a .COM server. "

Searching for www.google.com

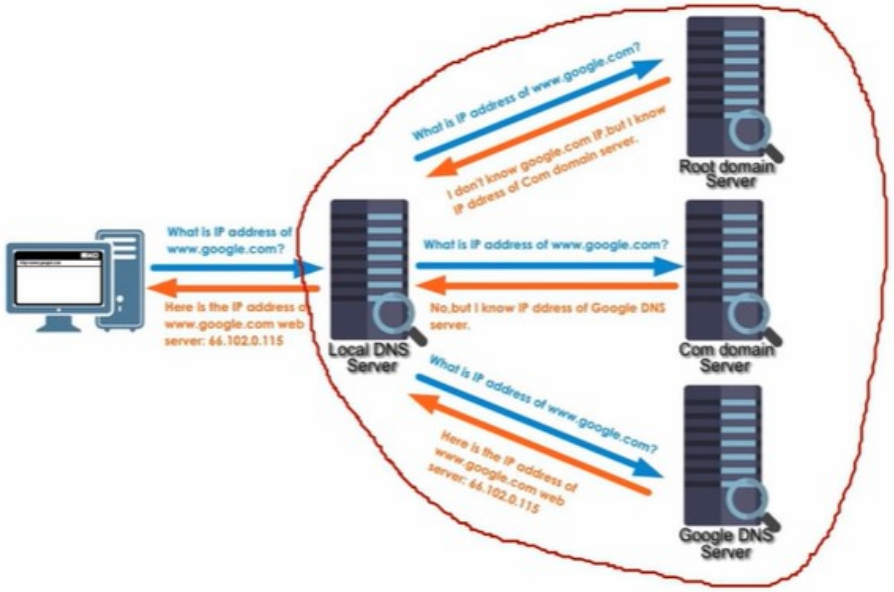


"I do not know IP address of this google web server,

Searching for www.google.com



Iterative Query



When this local DNS server could not resolve a new name from its own database, it would make an **iterative query** to other DNS servers.

- **DNS recursive query vs. Iterative query**
- https://www.youtube.com/watch?v=PS0UppB3-fg

- **How to check your current DNS**
- https://www.youtube.com/watch?v=ghWBAGZxd2s

SAMPLE FORWARD LOOKUP FILE

```
; This is the Start of Authority (SOA) record.  Contains contact & other information about the name serve
; must be changed whenever the file is updated (to inform secondary servers that zone information has chan
    @ IN SOA mydomain.name.  postmaster.mydomain.name. (
   19990811; Serial number
   3600     ; 1 hour refresh
   300      ; 5 minutes retry
   172800   ; 2 days expiry
   43200 )  ; 12 hours minimum

; This is the mail-exchanger.  You can list more than one (if applicable), with the integer field indicating priority (lowest
; being a higher priority)
   IN MX    mail.mydomain.name.

; Provides optional information on the machine type & operating system used for the server
   IN HINFOPentium/350   LINUX

; A list of machine names & addresses
    spock.mydomain.name.     IN A     123.12.41.40    ; OpenVMS Alpha
    mail.mydomain.name.      IN A     123.12.41.41    ; Linux (main server)
    kirk.mydomain.name.      IN A     123.12.41.42    ; Windows NT (blech!)

; Including any in our other class C's
    twixel.mydomain.name.    IN A     126.27.18.161   ; Linux test machine
    foxone.mydomain.name.    IN A     126.27.18.162   ; Linux devel. kernel

; Alias (canonical) names
    gopher IN CNAMEmail.mydomain.name.
    ftp    IN CNAMEmail.mydomain.name.
    www    IN CNAMEmail.mydomain.name.
```

Information about the lookup itself

Mail exchange record

Records that specify the name and IP

Aliases that allow different names to associate to a single fully qualified domain name: One physical server with multiple services.

DNS Types: 10 Top DNS Record Types

- DNS servers create a DNS record to provide important information about a domain or hostname, particularly its current IP address. The most common DNS record types are:

1. Address Mapping record (A Record)—also known as a DNS host record, stores a hostname and its corresponding IPv4 address.
2. IP Version 6 Address record (AAAA Record)—stores a hostname and its corresponding IPv6 address.
3. Canonical Name record (CNAME Record)—can be used to alias a hostname to another hostname. When a DNS client requests a record that contains a CNAME, which points to another hostname, the DNS resolution process is repeated with the new hostname.
4. Mail exchanger record (MX Record)—specifies an SMTP email server for the domain, used to route outgoing emails to an email server. Is an extremely important record that allows the third parties to be able to find the local mail servers.

Example MX Record:

```
; This is the mail-exchanger.  You can list more than one (if
; applicable), with the integer field indicating priority (lowest
; being a higher priority)
  IN MX   mail.mydomain.name.
```

```
; A list of machine names & addresses
   spock.mydomain.name.     IN A     123.12.41.40    ; OpenVMS Alpha
   mail.mydomain.name.      IN A     123.12.41.41    ; Linux (main server)
   kirk.mydomain.name.      IN A     123.12.41.42    ; Windows NT (blech!)
```

5. Name Server records (NS Record)—specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server.

DNS Types: 10 Top DNS Record Types

6. Reverse-lookup Pointer records (PTR Record)—allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup).
7. Certificate record (CERT Record)—stores encryption certificates—PKIX, SPKI, PGP, and so on.
8. Service Location (SRV Record)—Finding specific service: a service location record, like MX but for other communication protocols.

Example of SRV:

```
;Service records
; _service._proto.name.   TTL   class SRV priority weight port target.
 _ldap._tcp.domain.com.   300   IN    SRV 10       60     389  s1.domain.com.
```

Associate a particular service (_ldap._tcp.domain.com with a particular device (s1.domain.com)

https://ns1.com/resources/dns-types-records-servers-and-queries

DNS Types: 10 Top DNS Record Types

9. **Text Record (TXT Record)—typically carries machine-readable data such as opportunistic encryption, sender policy framework, DKIM, DMARC, etc.**
10. **Start of Authority (SOA Record)—this record appears at the beginning of a DNS zone file, and indicates the Authoritative Name Server for the current DNS zone, contact details for the domain administrator, domain serial number, and information on how frequently DNS information for this zone should be refreshed.**

- Sender **Policy Framework** (**SPF)**→ allows email senders to define which IP addresses are allowed to send mail for a particular domain.
- **Domain Keys** Identified Mail (**DKIM**)→ provides an encryption key and digital signature that verifies that an email message was not forged or altered.
- Domain-Based Message Authentication Reporting and Conformance (**DMARC**,) is an added authentication method that uses both SPF and **DKIM** to verify whether or not an email was actually sent by the owner of the “Friendly-From” domain that the user sees.

https://ns1.com/resources/dns-types-records-servers-and-queries

References

- https://www.slideserve.com/zavad/module-2-2-domain-name-system-powerpoint-ppt-presentation
- https://computers.tutsplus.com/tutorials/how-to-change-your-dns-for-safer-faster-browsing--mac-61232

The End