

Day-1

# DNS

Day-1

\_\_\_/\_\_\_/\_\_\_

**DN:** DNS translates domain names into ip address, which computers use to identify each other on network.

Public dns:

google (8.8.8.8, 8.8.4.4)

cisco dns:

umbrella

(IPv4)

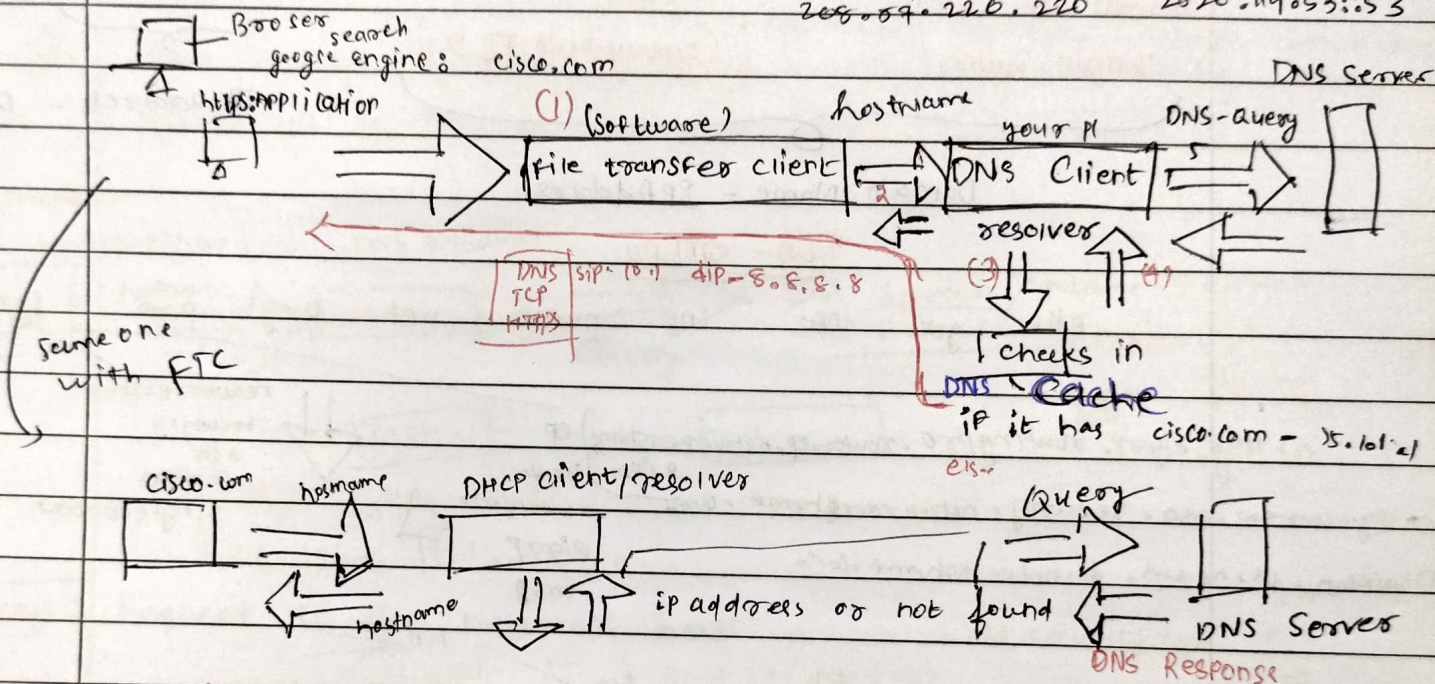
(IPv6)

208.67.222.222

208.67.220.220

2606:1192:35::35

2620:119:53::53



(DNS - Server DNS query PKT format size)  
DNS Reply

Name Space / Domain Name -

(0) Root (.)

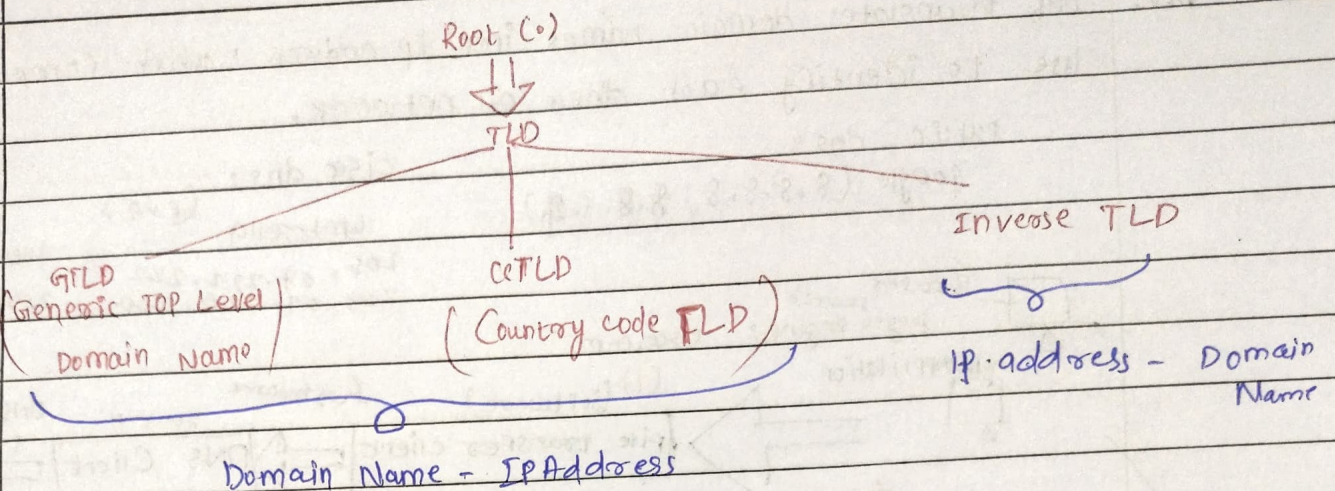
(1) TLD (Top Level Domain Name)

(2) Second Level Domain Name

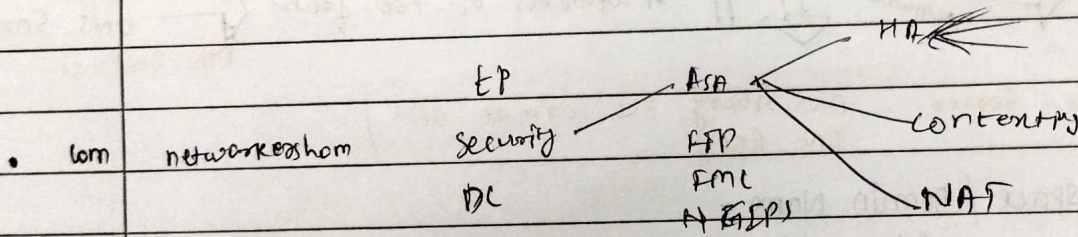
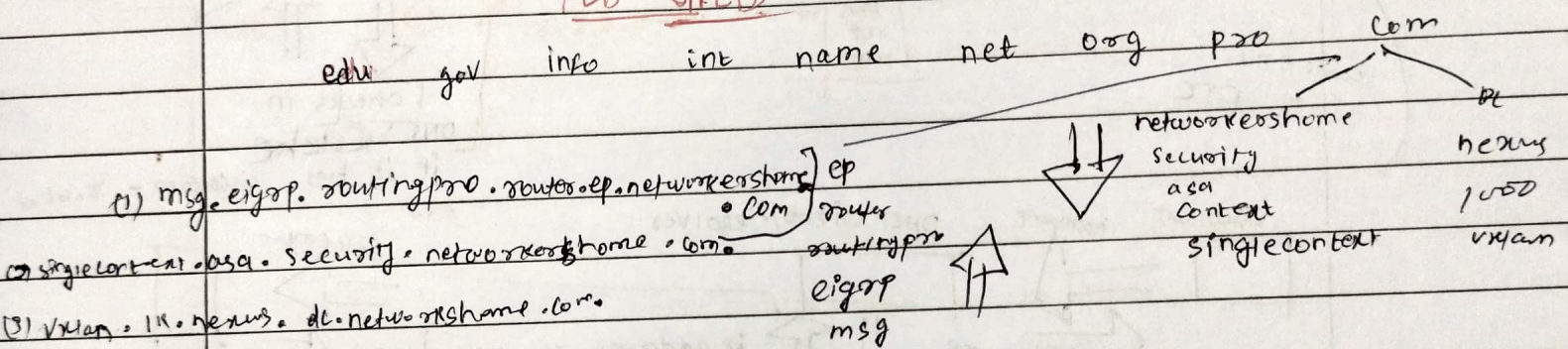
(255)

(0-255)

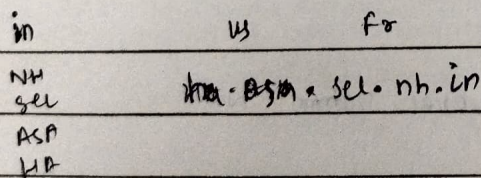




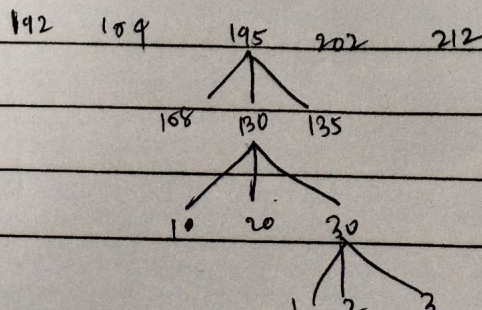
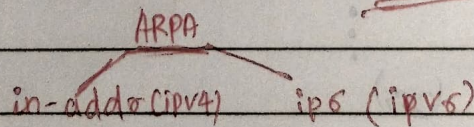
### TLD - GILD



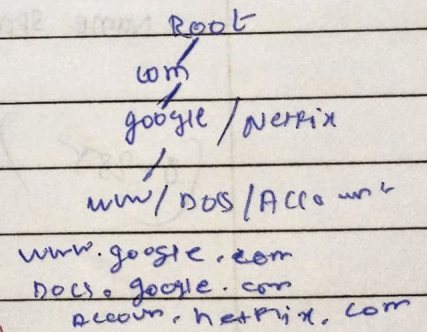
### ccTLD - Country Code TLD



(Inverse)

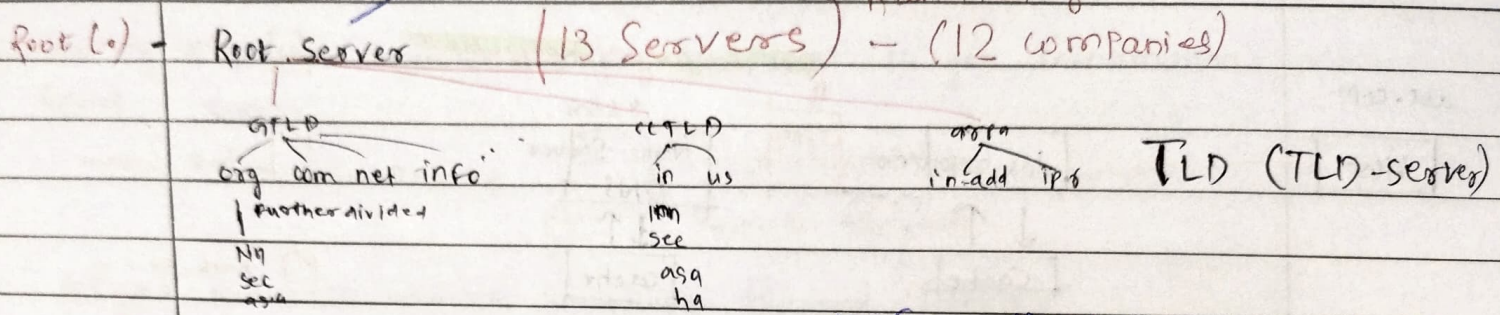


3.30.130.195.in-addr.arpa.



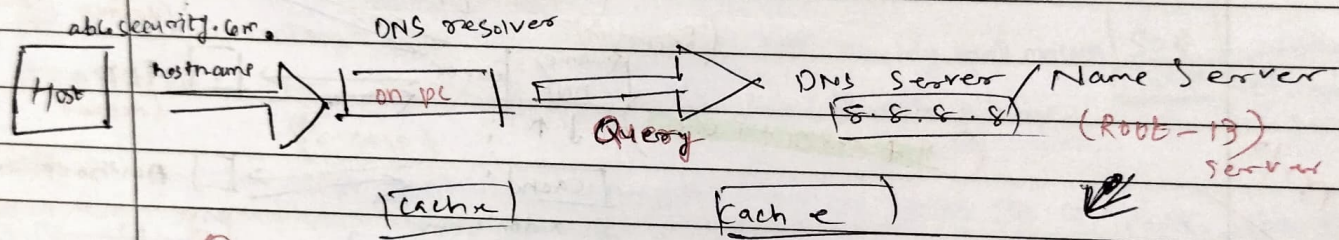


Imp The DNS system's starting point for resolving unknown domain names



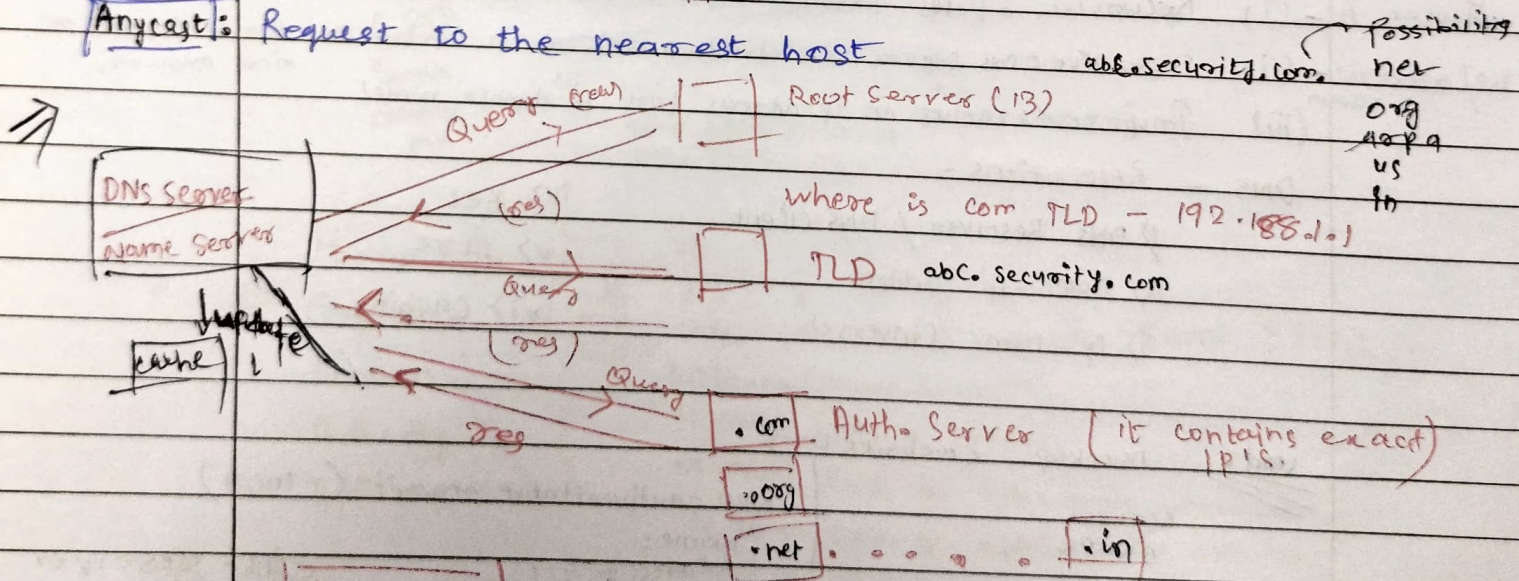
Q. Root Server Vs DNS Server - Any Server that helps resolve domain names including recursive, caching, and authoritative servers

Authoritative Name Server



Query Resolution  
Recursive Iterative

Anycast: Request to the nearest host



Homework

Record, Query msg format, Response pkt format

Q. when dns use TCP and UDP

A- Domain - IP  
mx  
COINAM



Day 2

DNS -

Resolution  
DNS Resolver / DNS Client

abc.com

Host

dns resolver

Cache

x

Rec. Query / Resolution

Query

8.8.8.8  
Name Servers  
DNS

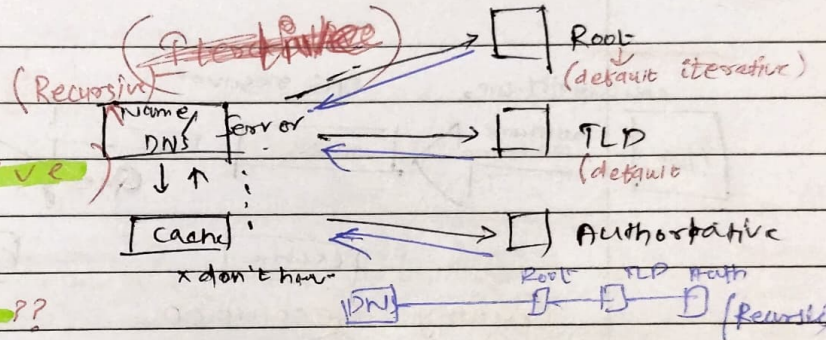
Cache

Root server

TLD Server

Auth. server

if it present it  
Sends back to dns resolver.  
It is called as (Recursive DNS Resolver),



Imp?

Q. Types of DNS Query??

- end-user A:- (i) Recursive: DNS resolver does all the work to resolve the full domain name
- isp/enterprise-resolve:- (ii) Iterative: DNS server replies with a referral to another DNS server instead of final answer.
- (iii) Inverse: resolves an ip address back to domain name

DNS - Resolutions -

- 1) DNS Resolver / DNS client
- 2) name - ip address
- 3) ip - name (inverse)
- iv) Rec
- v) Iter
- vi) Caching

cmd: nslookup <website url>

server:  
Address:

Non-authoritative answer: (local)

Name:  
Address:

If reply from Authoritative server

(1) Auth. Ser

If reply from dns-resolver

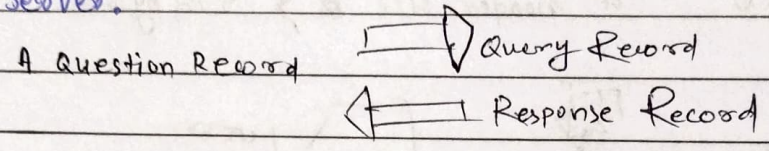
(0) No. Authoritative Server

Imp

Records - Question Record  
- RR (Resource Record)



Question Record : A question record is used by client to get information from server.



A Type: Name to address mapping Record (IPv4)

AAAA Type: Host to IPv6 address Record

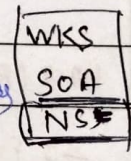
CNAME: (canonical Name) short form of a website known as canonical

facebook.com == fb.com

MX : mail Exchange - mail server responsible for receiving email messages

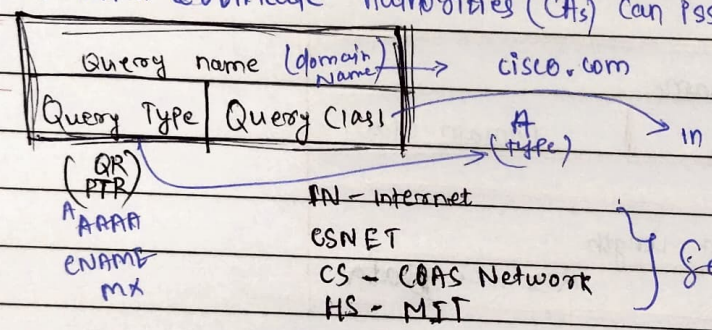
PTR \* Pointer : ip - domain name / Fully Qualified Domain Name (inverse)

CAA : Specifies which Certificate Authorities (CAs) can issue SSL certificates for the domain.



authoritative server  
Hosts records

Question Rec:

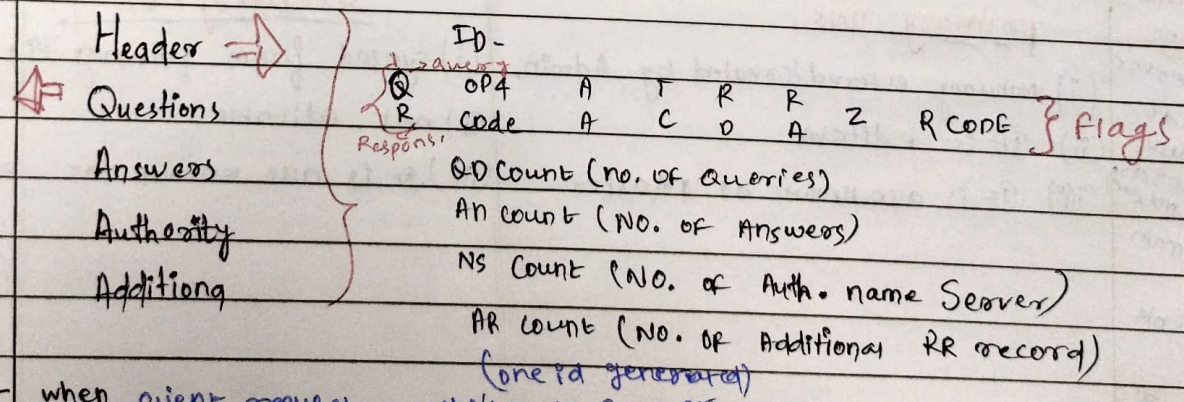


(QR)  
PTR  
AAAA  
CNAME  
MX

IN - Internet  
CSNET  
CS - COAS Network  
HS - MIT

Server

Query



ID - when client request a website to server, then the server will send to the client using same id number.

op code: 0 - standard Query, 1 - inverse Query, 2 - status Query, 4 - notify query, 5 - update query

1. 1-10-1944 2. 1-10-1944 3. 1-10-1944



1. 1-10-1944 2. 1-10-1944 3. 1-10-1944

- 1-10-1944

(1) 1-10-1944 2-10-1944 3-10-1944

(2) 1-10-1944 2-10-1944 3-10-1944

(3) 1-10-1944 2-10-1944 3-10-1944

1-10-1944

(1) 1-10-1944 2-10-1944 3-10-1944

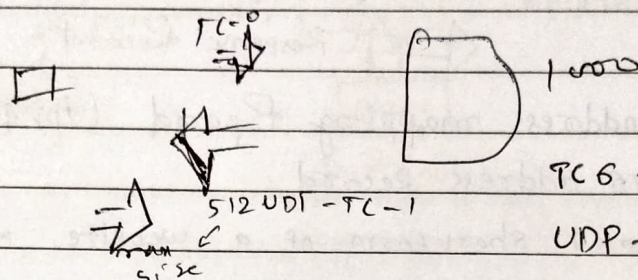
(2) 1-10-1944 2-10-1944 3-10-1944

(3) 1-10-1944 2-10-1944 3-10-1944



function Bit: (tc)

0 - query always 0 if header size is 512 bytes  
1 - resp



Post no  
TC 6-06 - 53  
UDP - 17 - 53

RA: (Recursive Server Availability)

2: Future use

Rcode: 0 - no error  
1 - error

Domain Name	
Domain Type	Domain Class
Resource data Length	
Resource Data	

**Authoritative DNS Server**  
DNS server that holds the actual DNS records (A, AAAA, MX, etc.) for a domain and is responsible for responding to queries about that domain with definitive answers.

### primary DNS

- (i) manually entered/created by Admin.
- (ii) It is editable
- (iii) It is also known as master

### Secondary DNS

- (i) synced from primary via zone
- (ii) not editable
- (iii) It is also known as slave