

①

DNS

distributed + replicated db
dynamic + scalable

Components:-

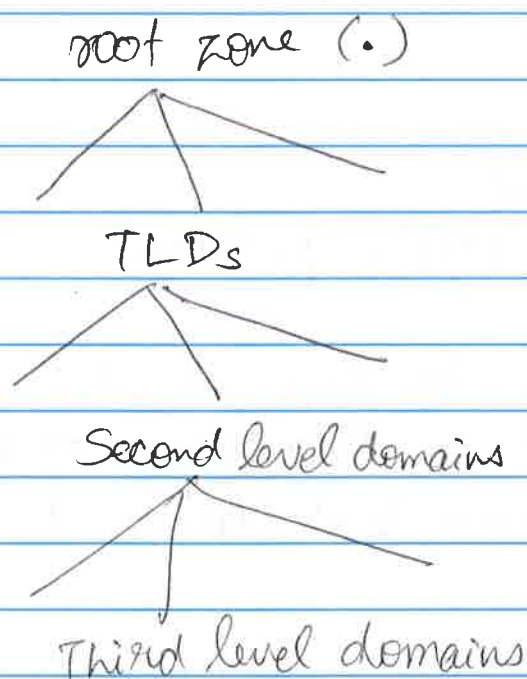
Name space

info stored \Rightarrow url \Rightarrow IP address

Resource records

Client - sends queries

Server - holds part of the namespace



Zone file = Plain text file containing Zone data
Exist on authoritative DNS servers,
not on caching resolvers

Record types

A - maps name to ip address

CNAME - Alias, maps name to another name

MX = Mail server of the domain

SOA = Start of Authority, must exist at least once
contains metadata of the domain itself

NS = IP addresses of authoritative (Name Servers)
of the domain

DNS uses Port 53

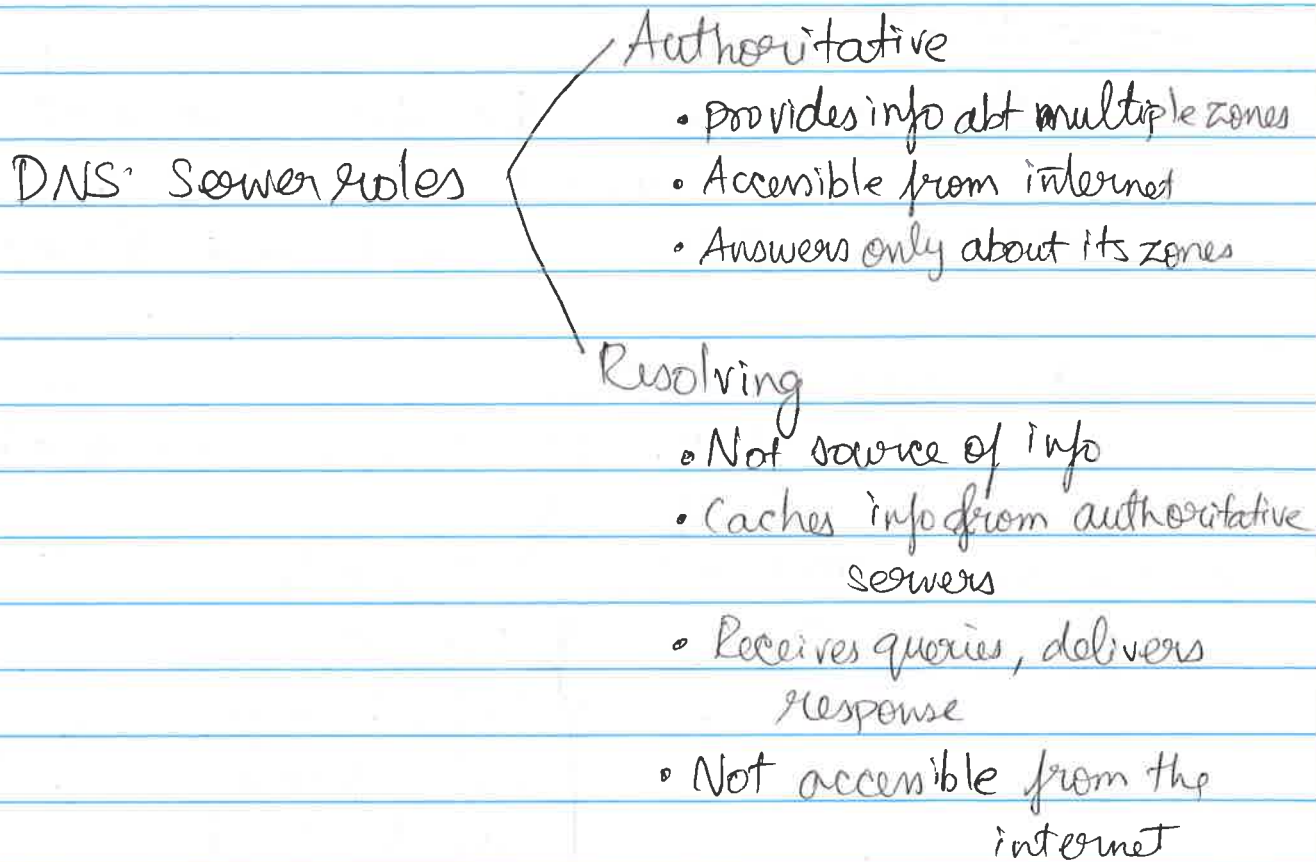
Client has no port requirement

Client only talks to local resolver

Local resolver only knows IP address of Root name server
- this info is called Root Stub - stored statically
on the resolver

Root name server has info on TLD servers -
referral response

(3)



Open DNS \Rightarrow resolving DNS server accessible from the internet

Tools

ping \Rightarrow A record

nslookup \Rightarrow Not on Unix, windows only

dig \Rightarrow

dig <host name>

just the answer \leftarrow dig <host name> <Record type> +short

To add a DNS server to resolve

dig <hostname> <Record type> @<DNS Server IP>

Zone file

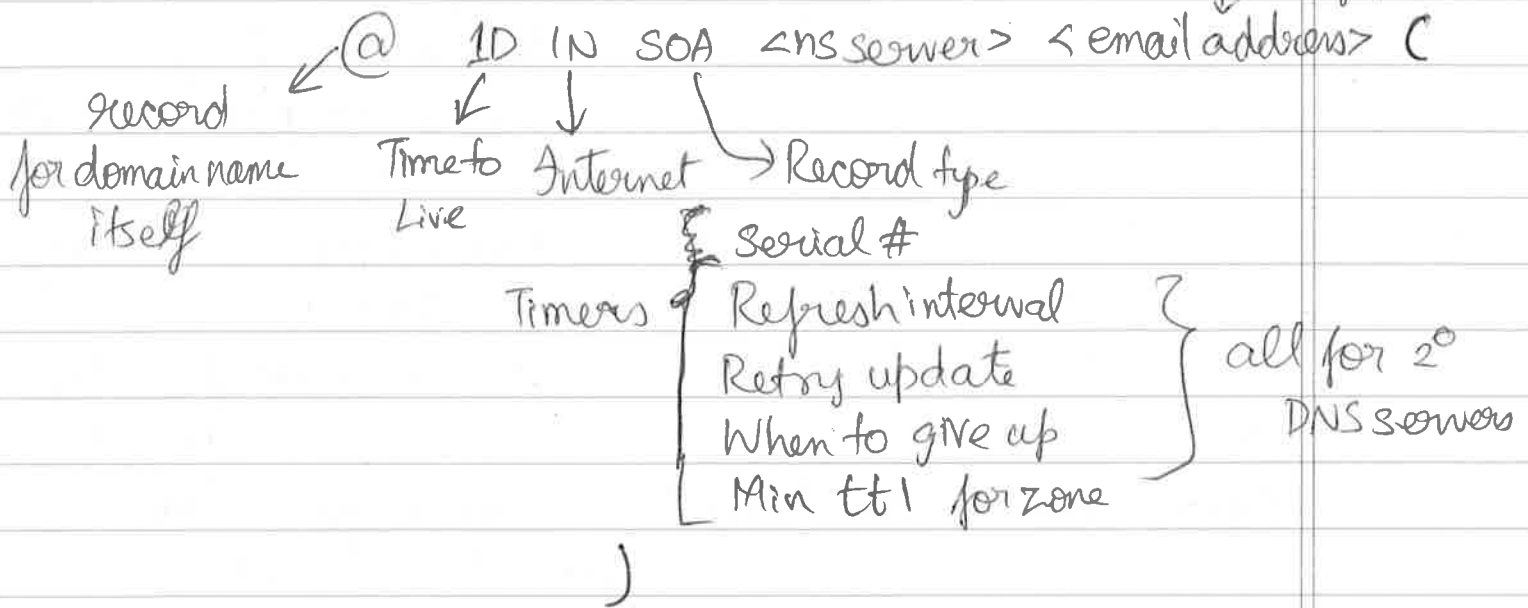
Absolutes to the root

* Origin statement \$ORIGIN <domain>!
which domain is this file about

* TTL \$TTL => time to cache @ most

* Server record

• instead of @



IN NS <ns server>

IN NS <ns server 2>

IN MX <mx server>

www IN A <a record> => webserver

@ IN A <a record> => domain itself =>
without www

(5)

BIND

Global config file /etc/bind/named.conf.local

Zone file /etc/bind/zones/<zone name>

service bind & reload \Rightarrow reloads the file.

Bind delegation

Subdomain records point to NS for that domain

A record in IPv6 is AAAA (quad A)

DNSKEY } DNSSEC
RRSIG }

DNS Spoofing - Attacker is blind, can attack only when window is open, need to guess Tx ID, Port #

Requirements:- * Spoof of Source IP
(Unicast RPF, Anti Spoof (Pakist) ^{Access List})

* Fast response

this is randomized \leftarrow * Guess Transaction ID

* Guess source port

