DOMAIN NAME SYSTEM (DNS)

Acknowledgement: some slides were prepared by Abhishek Tarapara (22CSM1R01), MTech student, NIT Warangal and Muneeswaran, PhD student at IIT Mandi.

Domain Name System

- The Domain Name System (DNS) is the system used to translate alphanumeric domain names into Internet Protocol numbers.
- As a human we can not remember ip address of all websites but we can remember names of websites.
- Even is we remember ip address of some website then it might possible that ip address of that website changes in future.
- Whenever we search anything on browser the DNS request will be sent to get ip of that website.
- The Domain Name System is a distributed database arranged hierarchically.
- DNS use UDP at transport layer.

Types of Domain

1. Generic Domain

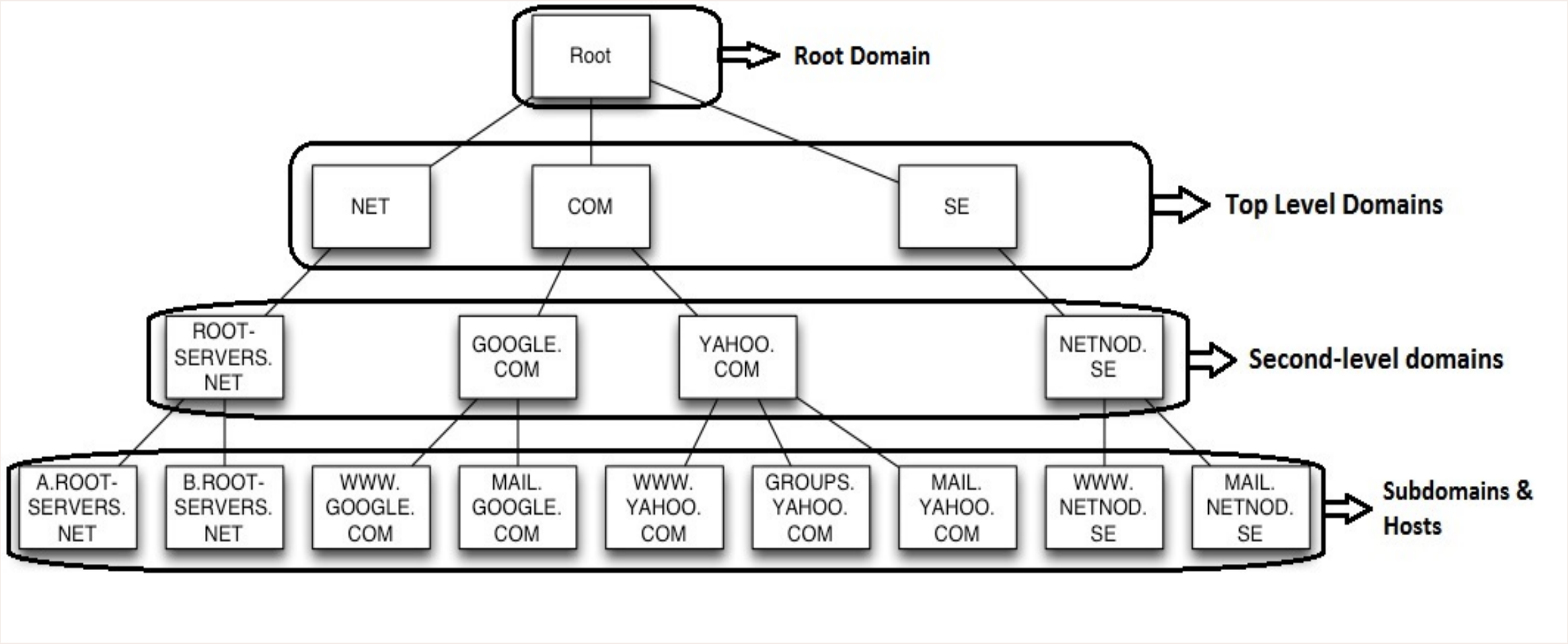
- .com - Open domain for commercial web offers.
- .net - Open address for ISPs.
- .org - Open TLD for non-profit organization.
- .gov - Domain for government institutions.
- .edu - Domain intended for trade schools and universities.
- .mil - TLD available only to departments, services, and agencies of the U.S. Department of Defenses.

2. Country Domain

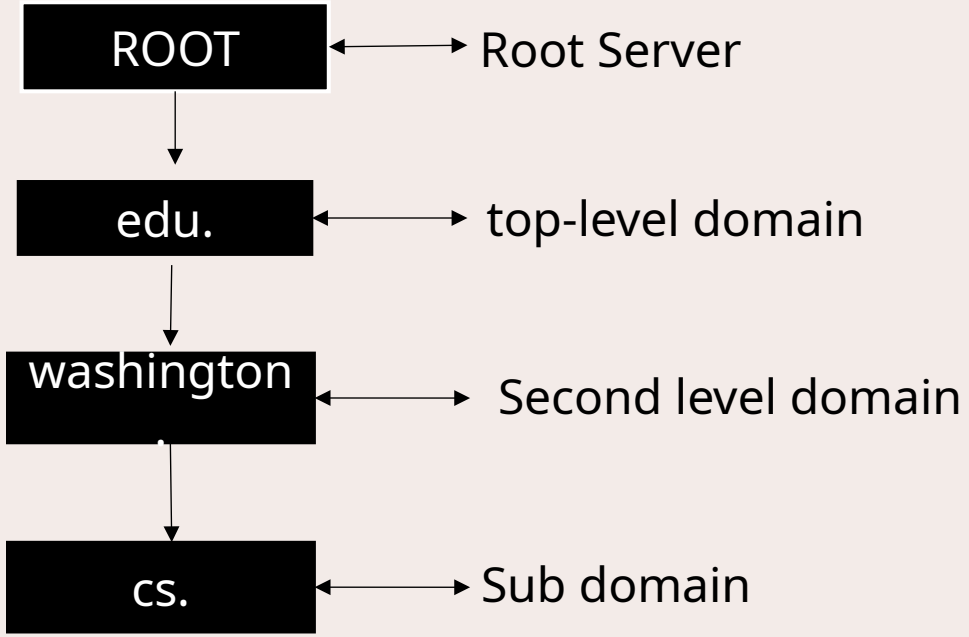
- .in - India
- .us - Unites state
- .uk - United Kingdom
- .de - Germany
- .ch - Switzerland
- .cn - China
- .ru - Russia

DNS Hierarchy

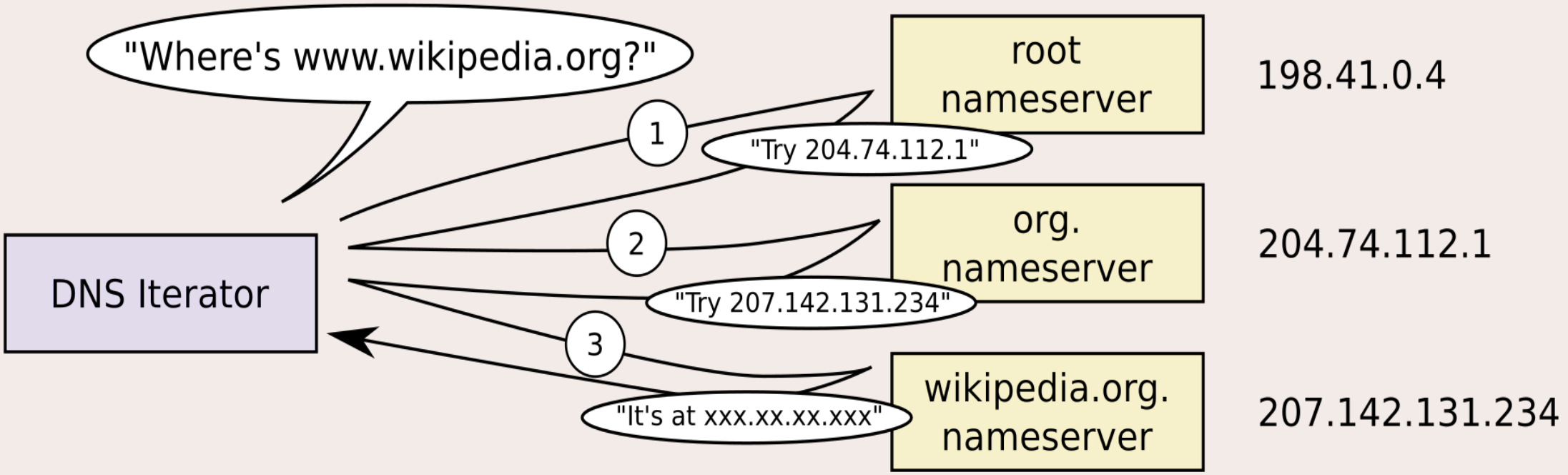
- 1) Root Level
- 2) Top Level Domains
- 3) Second Level Domains
- 4) Sub-Domain
- 5) Host


Root
Root Domain
NET
COM
SE
Top Level Domains
ROOT-SERVERS.NET
GOOGLE.COM
YAHOO.COM
NETNOD.SE
Second-level domains
A.ROOT-SERVERS.NET
B.ROOT-SERVERS.NET
WWW.GOOGLE.COM
MAIL.GOOGLE.COM
WWW.YAHOO.COM
GROUPS.YAHOO.COM
MAIL.YAHOO.COM
WWW.NETNOD.SE
MAIL.NETNOD.SE
Subdomains & Hosts

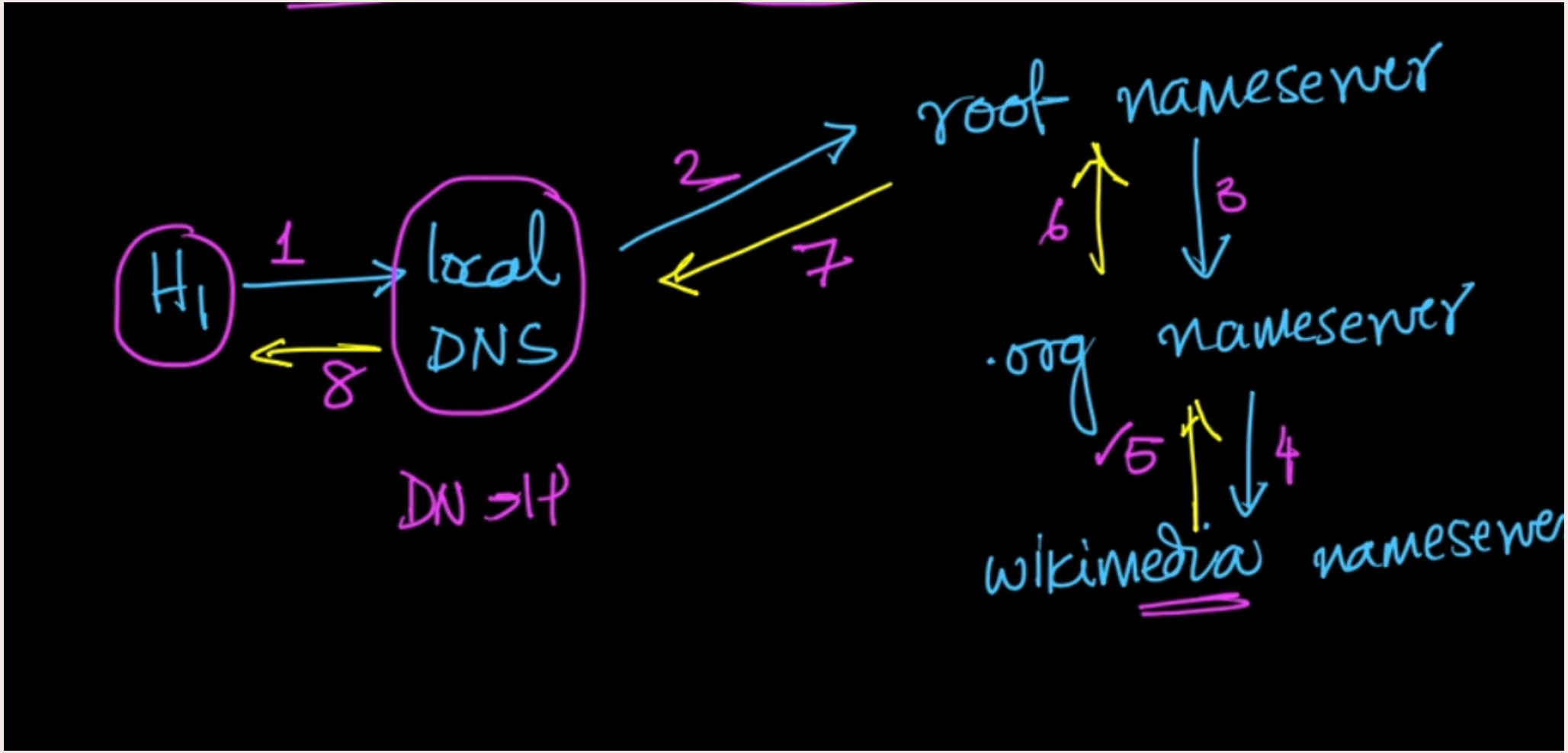
cs.washington.edu
(University of Washington, in the U.S.)



Iterative Query resolver



Recursive Query resolver

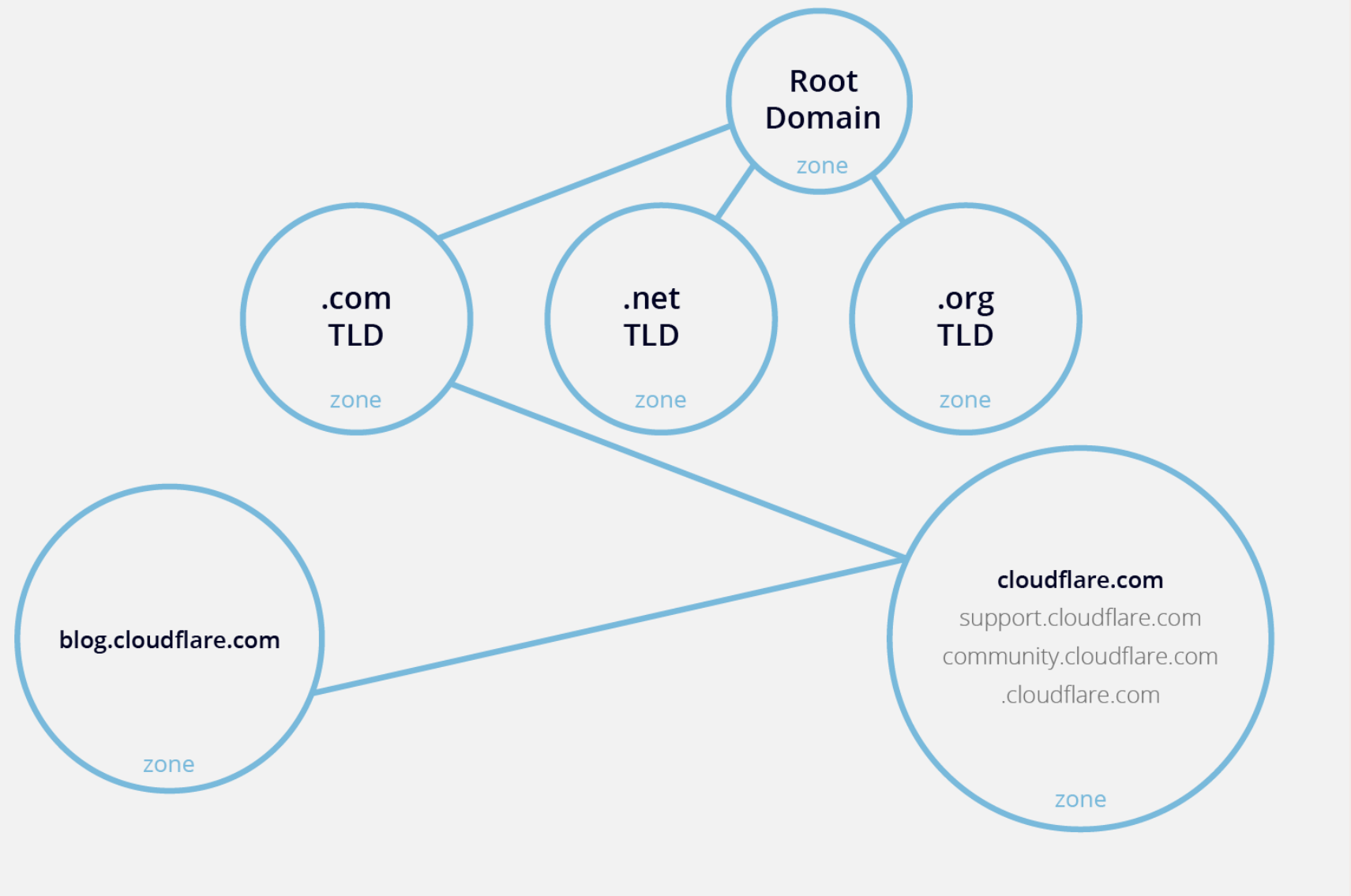


DNS zones

- DNS zone is a portion of DNS namespace that is managed by specific organization or administrator.
- DNS zones can contain multiple subdomains and they can exist on same server.
- All subdomains of zones are managed independently.
- Example : csa.iisc.ac.in

  ece.iisc.ac.in

  math.iisc.ac.in


Root
Domain
zone
.com
TLD
zone
.net
TLD
zone
.org
TLD
zone
blog.cloudflare.com
zone
cloudflare.com
support.cloudflare.com
community.cloudflare.com
.cloudflare.com
zone

DNS zone file

- Domain name(origin domain)
- Time to live
- Class
- Type
- Value

- The Domain name tells the domain to which this record applies. Normally, many records exist for each domain and each copy of the database holds information about multiple domains
- The Time to live field gives an indication of how stable the record is. Information that is highly stable is assigned a large value, such as 86400 (the number of seconds in 1 day). Information that is highly volatile is assigned a small value, such as 60 (1 minute).
- The third field of every resource record is the Class. For Internet information, it is always IN.
- The Type field tells what kind of record this is. The most important record type is the A (Address) record. It holds a 32-bit IPv4 address of an interface for some host. The corresponding AAAA, or ‘‘quad A,’’ record holds a 128-bit IPv6 address. For other record types: https://www.site24x7.com/learn/dns-record-types.html

Dig Command

- Dig (domain information groper) is a tool that is used for querying DNS servers for various DNS records
- It is very useful for troubleshooting DNS problems.
- Install Dig

  CentOS/RHEL/Fedora

  yum install bind-utils -y

  Debian/Ubuntu

  apt-get install dnsutils -y

Basic DNS Query

- Specify a domain name after the dig command and it will perform a DNS lookup, as shown below

  munees@Munees ~ $ **dig iitmandi.ac.in**

  ; <<>> DiG 9.10.3-P4-Ubuntu <<>> iitmandi.ac.in

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7553

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;iitmandi.ac.in. IN A

;; ANSWER SECTION:

iitmandi.ac.in. 14159 IN A 204.197.248.190

;; AUTHORITY SECTION:

iitmandi.ac.in. 6358IN NS ns2.iitmandi.net.in.

iitmandi.ac.in. 6358IN NS ns1.iitmandi.net.in.

;; ADDITIONAL SECTION:

ns1.iitmandi.net.in. 462 IN A 204.197.250.58

ns2.iitmandi.net.in. 14159 IN A 204.197.251.58

Output of Command

- Lines beginning with ; are comments not part of the information.
- The first line tell us the version of dig (9.10.3) command.
- Next, dig shows the header of the response it received from the DNS server.
- Next comes the question section, which simply tells us the query, which in this case is a query for the “A” record of **iitmandi.ac.in**. The IN means this is an Internet lookup (in the Internet class).
- The answer section tells us that **iitmandi.ac.in**. has the IP address 204.197.248.190.
- Lastly there are some stats about the query. You can turn off these stats using the +nostats option.

Trace DNS Path

- We can perform a trace on the DNS lookup path with the +trace option.
- First the root name servers for '.' are looked up, followed by the name servers for the .com domain, and then finally the name servers for google.com are returned, followed by the DNS records for it.

munees@Munees ~ $ **dig google.com +trace**

; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com +trace

;; global options: +cmd

. 170572 IN NS m.root-servers.net.

. 170572 IN NS b.root-servers.net.

. 170572 IN NS a.root-servers.net.

. 170572 IN NS j.root-servers.net.

. 170572 IN NS c.root-servers.net.

. 170572 IN NS l.root-servers.net.

. 170572 IN NS k.root-servers.net.

. 170572 IN NS g.root-servers.net.

. 170572 IN NS i.root-servers.net.

. 170572 IN NS f.root-servers.net.

. 170572 IN NS h.root-servers.net.

. 170572 IN NS d.root-servers.net.

. 170572 IN NS e.root-servers.net.

;; Received 811 bytes from 127.0.1.1#53(127.0.1.1) in 1 ms

com. 172800 IN NS j.gtld-servers.net.

com. 172800 IN NS g.gtld-servers.net.

com. 172800 IN NS e.gtld-servers.net.

com. 172800 IN NS k.gtld-servers.net.

Query All DNS Record Types

- We can use the 'ANY' option to query all DNS record types, this way we can quickly see all DNS records available for a domain.
- In the below example we can see the results for all types of different records, including A, AAAA, TXT, MX and NS.

```
;;ANSWER SECTION:
google.com.     129  IN    MX   10 aspmx.l.google.com.
google.com.     63   IN    AAAA      2404:6800:4007:801::200e
google.com.     209  IN    A    172.217.26.174
google.com.     2005IN    NS   ns3.google.com.
```

Reverse DNS Lookup

- we can query an IP address and find the domain name that it points to by querying the PTR record. PTR is a specific type of DNS record. This is done by using the -x option followed by the IP address to query.
- In the below example we perform a reverse lookup on one of the IP addresses that google.com resolved to in the first example.
- This IP address has one PTR record, pointing to del03s09-in-f14.1e100.net.

munees@Munees ~ $ **dig -x 172.217.160.238**

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 172.217.160.238

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48217

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;238.160.217.172.in-addr.arpa.	IN	PTR

;; ANSWER SECTION:

238.160.217.172.in-addr.arpa. 13924 IN PTR del03s09-in-f14.1e100.net.

;; AUTHORITY SECTION:

217.172.in-addr.arpa.	5086	IN	NS	ns3.google.com.

217.172.in-addr.arpa.	5086	IN	NS	ns2.google.com.

217.172.in-addr.arpa.	5086	IN	NS	ns1.google.com.

217.172.in-addr.arpa.	5086	IN	NS	ns4.google.com.

;; ADDITIONAL SECTION:

ns1.google.com.	292881	IN	A	216.239.32.10

ns1.google.com.	15005	IN	AAAA	2001:4860:4802:32::a

ns2.google.com.	306102	IN	A	216.239.34.10

ns2.google.com.	343201	IN	AAAA	2001:4860:4802:34::a

ns3.google.com.	343852	IN	A	216.239.36.10

ns3.google.com.	258267	IN	AAAA	2001:4860:4802:36::a

ns4.google.com.	181501	IN	A	216.239.38.10

ns4.google.com.	287786	IN	AAAA	2001:4860:4802:38::a