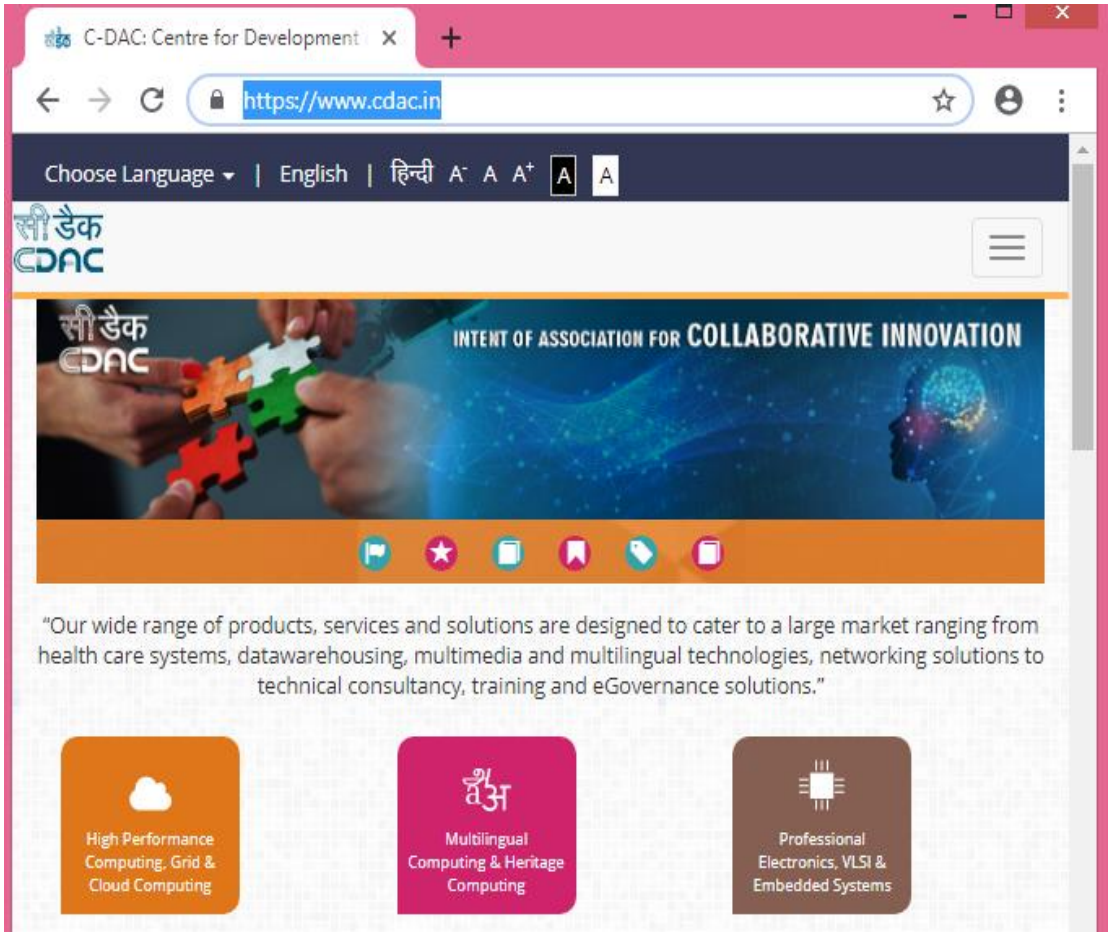
Safe and Healthy DNS Ecosystem

Sanjay Adiwal
Principal Technical Officer
C-DAC Electronics City
Bangalore

What is DNS?



Application Layer
- HTTP/HTTPS
- www.cdac.in

Transport Layer
- TCP
- Source Port:87878
- Destination Port:80/443

Network Layer
- Source IP: 202.141.136.152
- Destination IP: ?

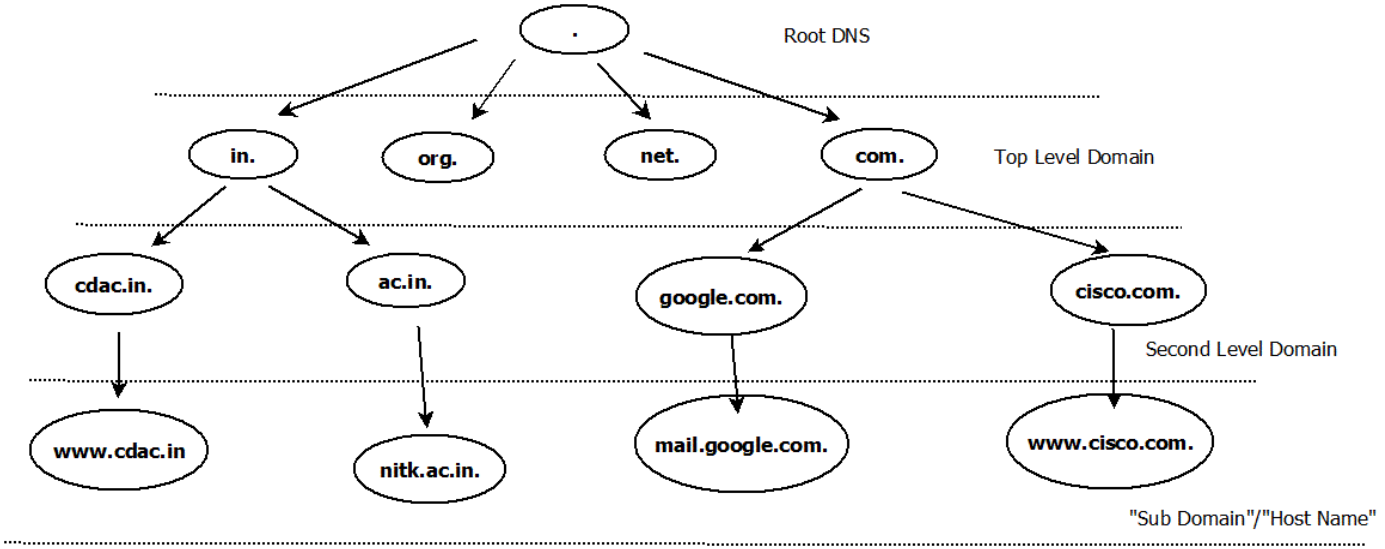
Data Link Layer
- Source Mac: aa:bb:cc:dd:ee:ff
- DMAC: MAC of Gateway

What is DNS?

- Service or Application that converts Domain names to IP Addresses:
  - www.cdac.in. → 196.1.113.45
  - www.cdac.in. → 2405:8a00:6029::45
- … and back:
  - 196.1.113.45 → www.cdac.in.
  - 2405:8a00:6029::45 → www.cdac.in.

How is DNS built ?

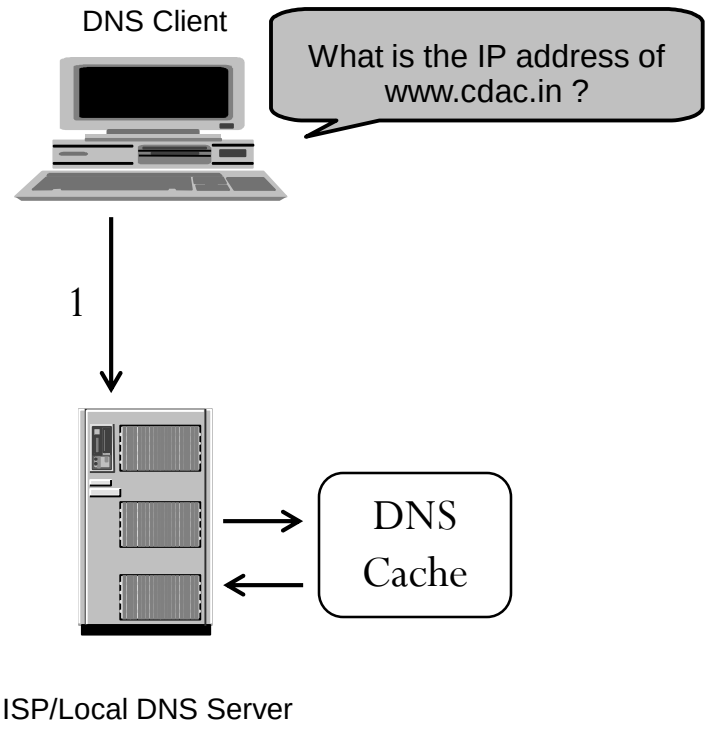
- DNS is hierarchical



- **www.cdac.in.**
- DNS administration is shared – no single central entity administrates all DNS data

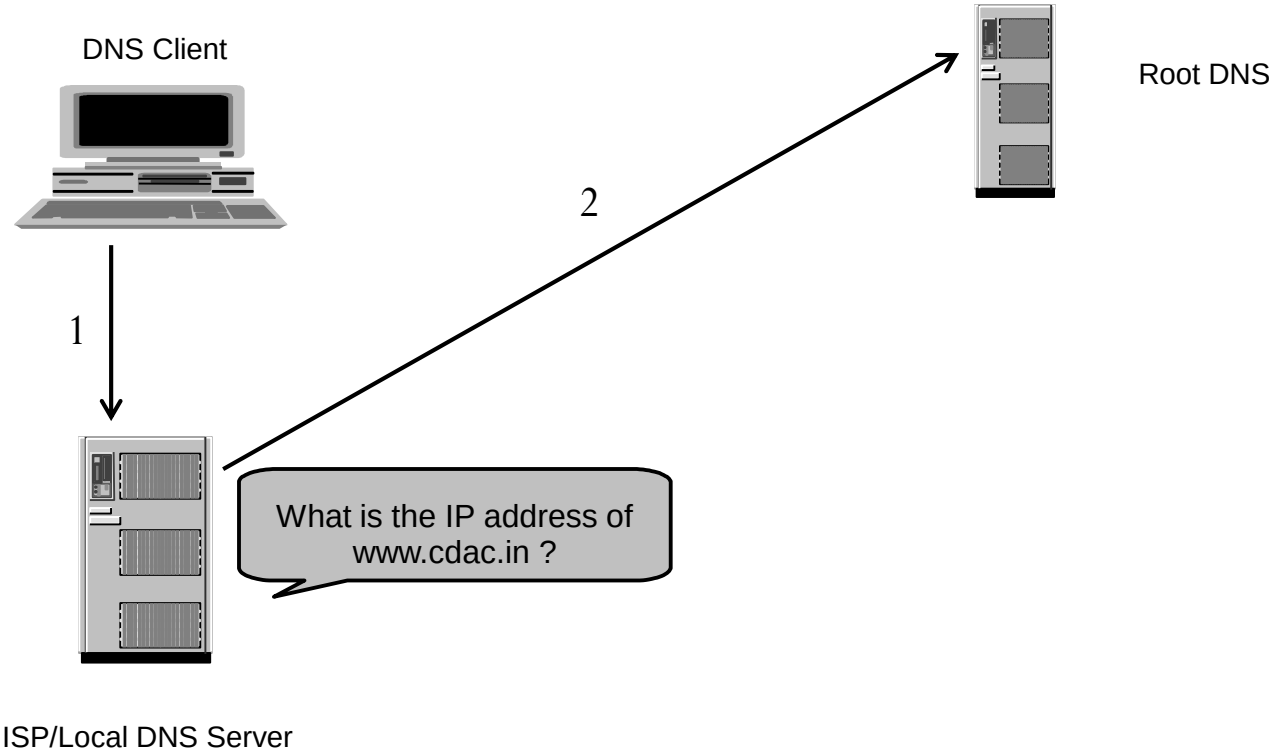
How DNS Works?

1. Client asks to Local/ISP DNS server for lookup.



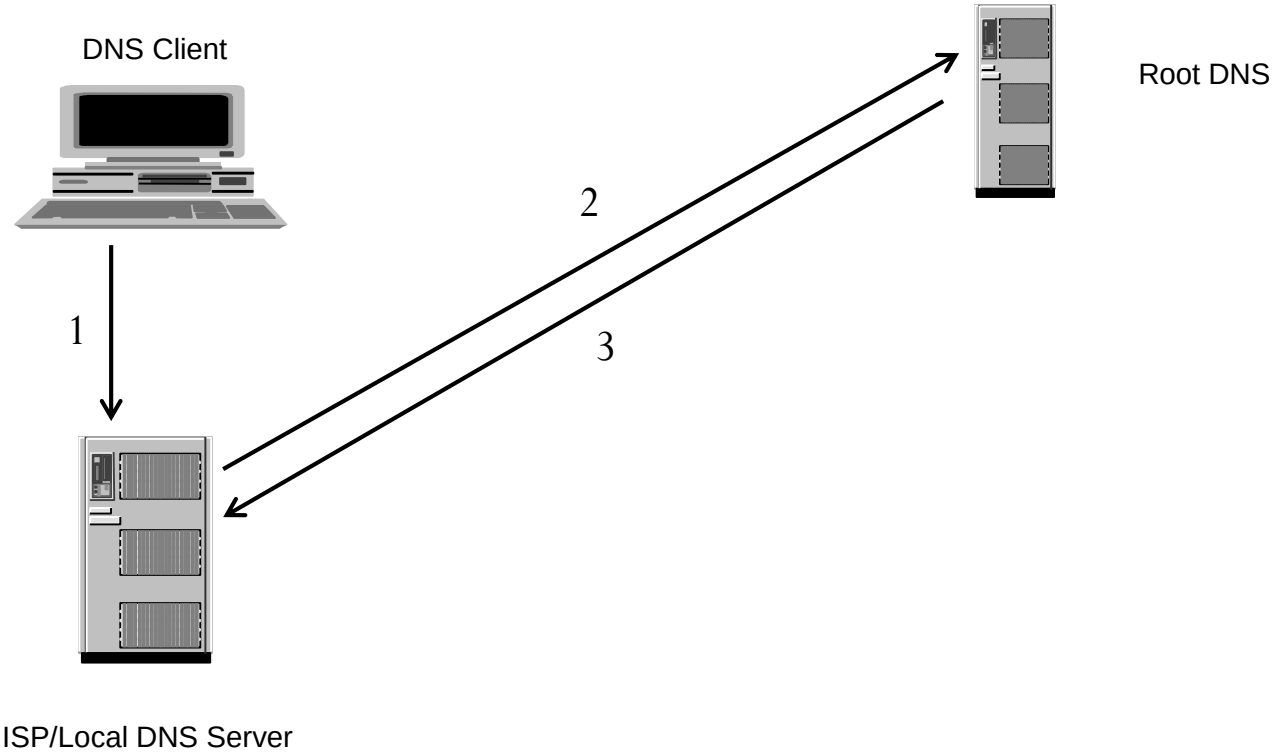
How DNS Works?

2. Local/ISP DNS Server asks Root DNS server.



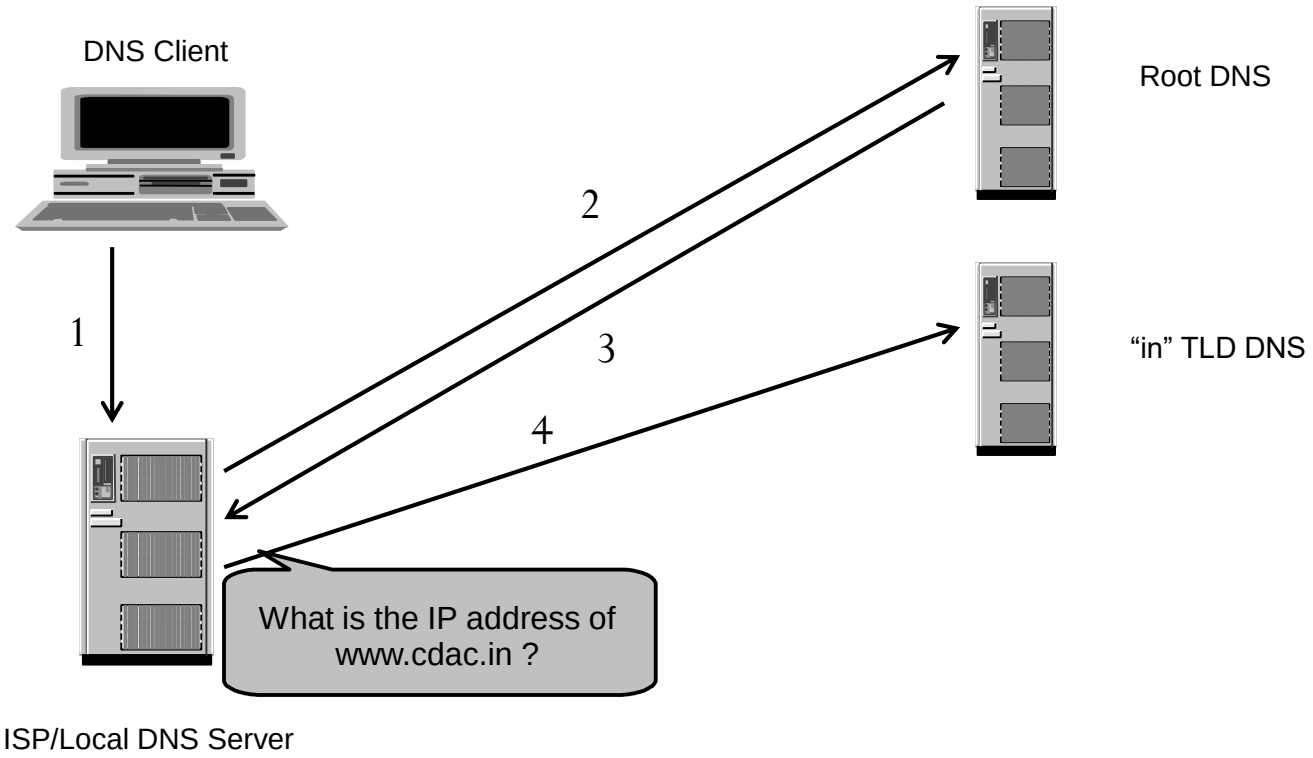
How DNS Works?

3. Root DNS server reply with referral to TLD DNS "in".



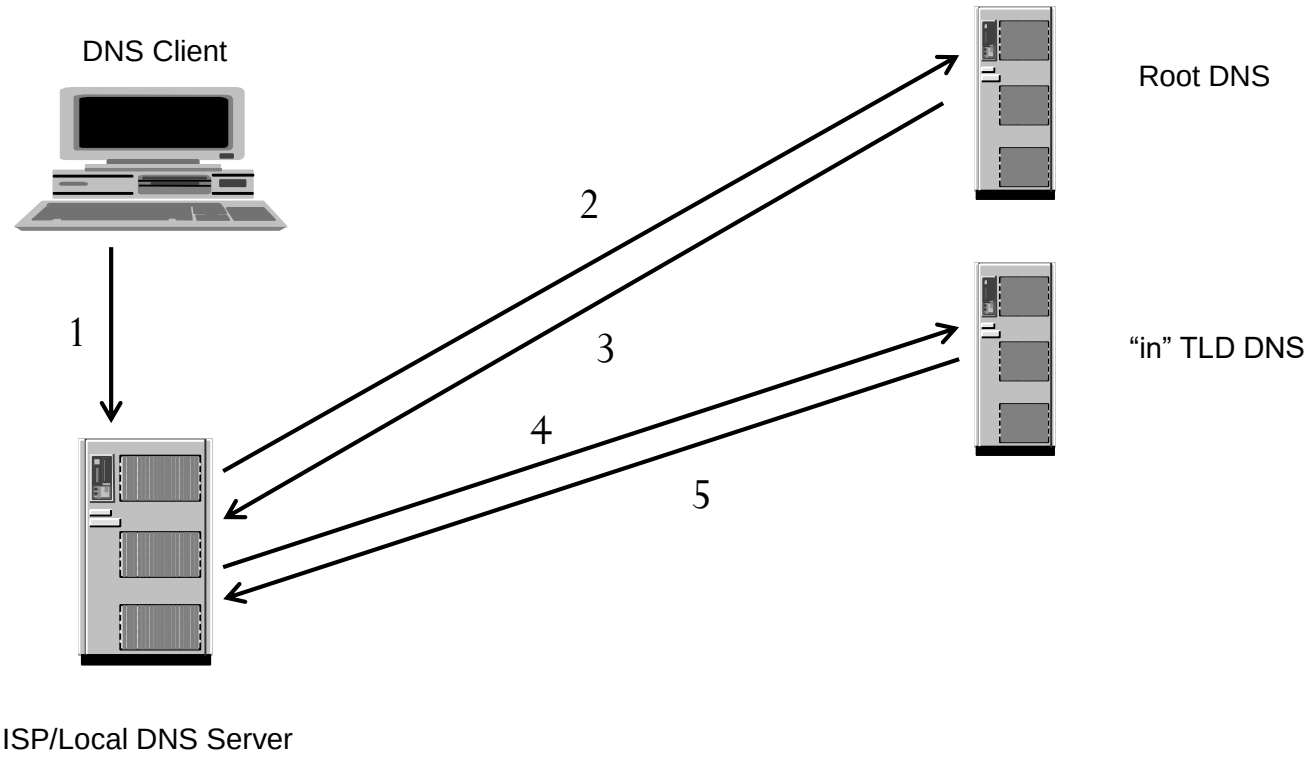
How DNS Works?

4.ISP/Local DNS Server queries TLD DNS.



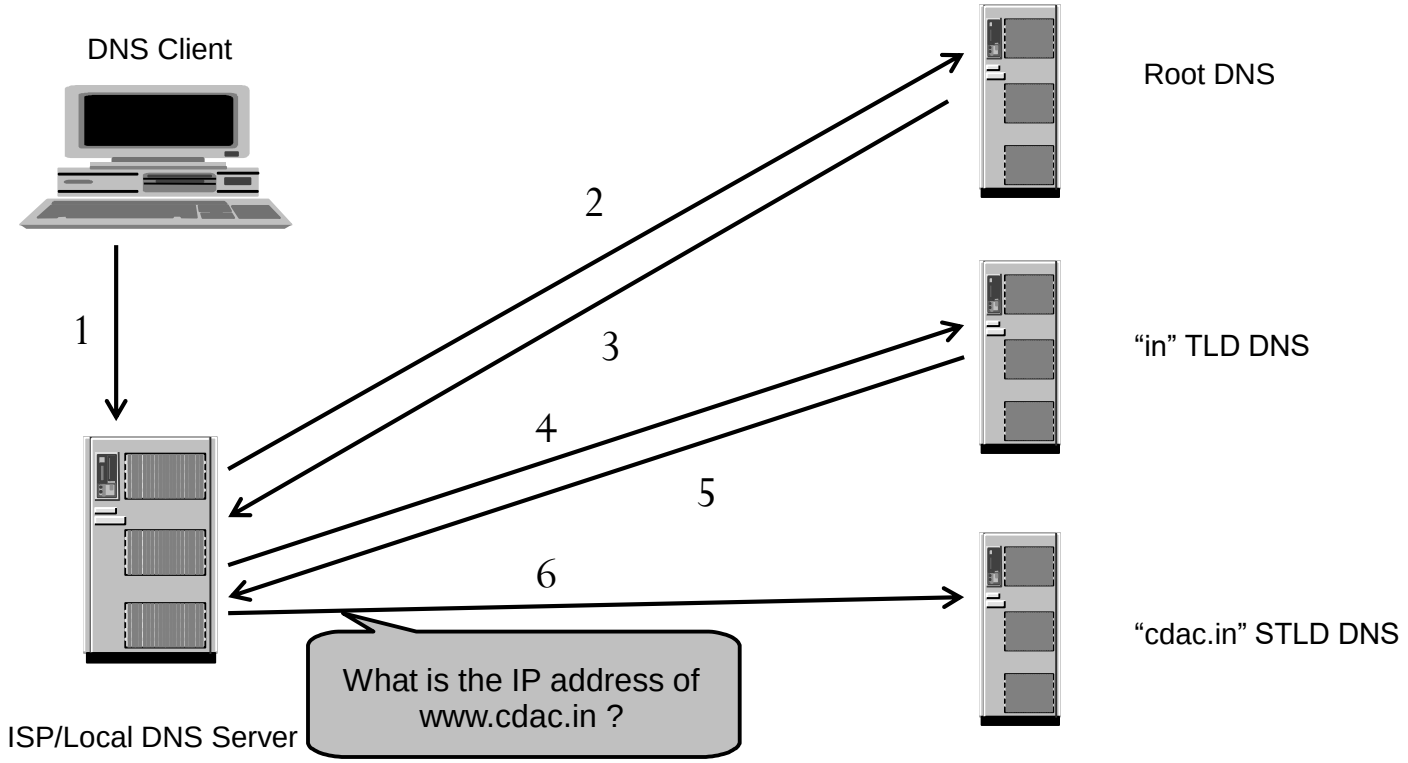
How DNS Works?

5. TLD DNS reply with referral to STLD DNS "cdac.in".



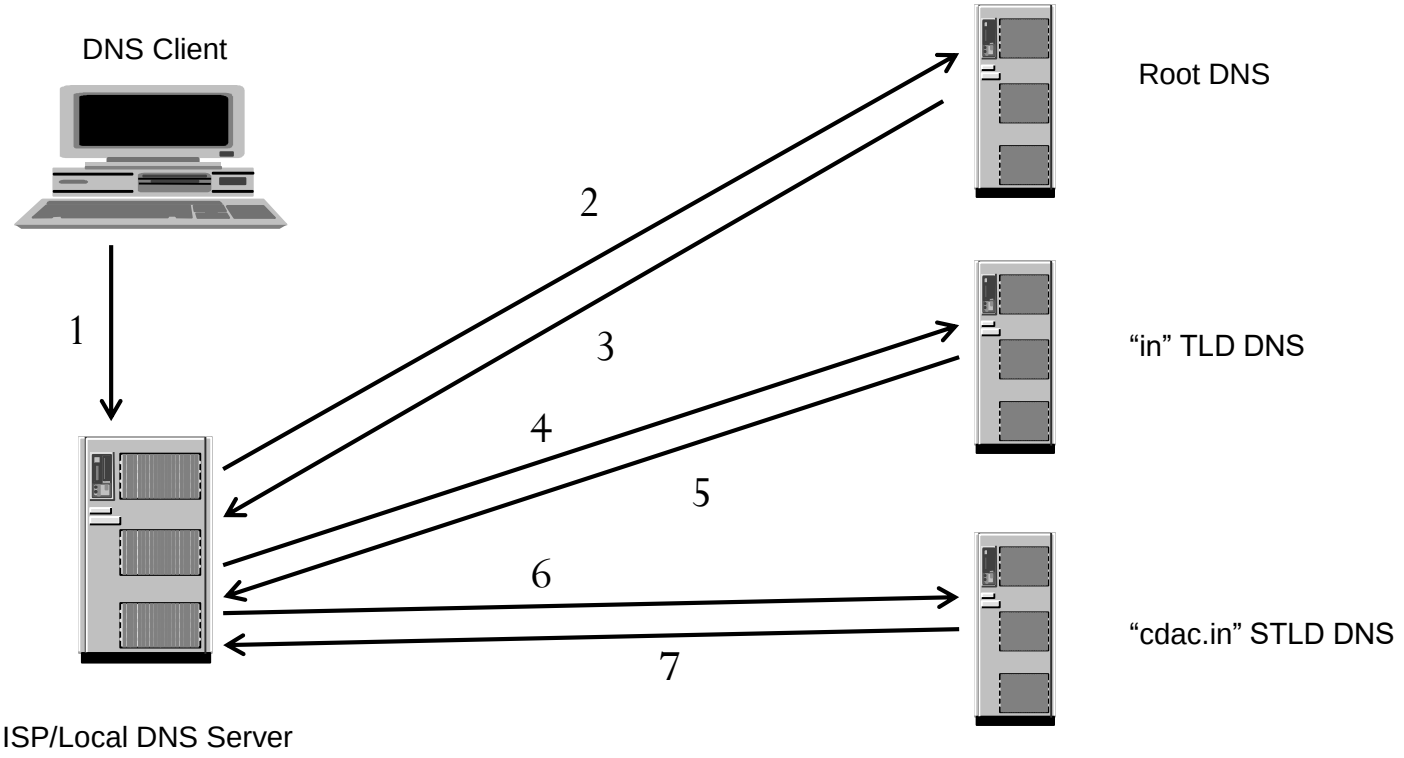
How DNS Works?

6.ISP/Local DNS Server queries STLD DNS.



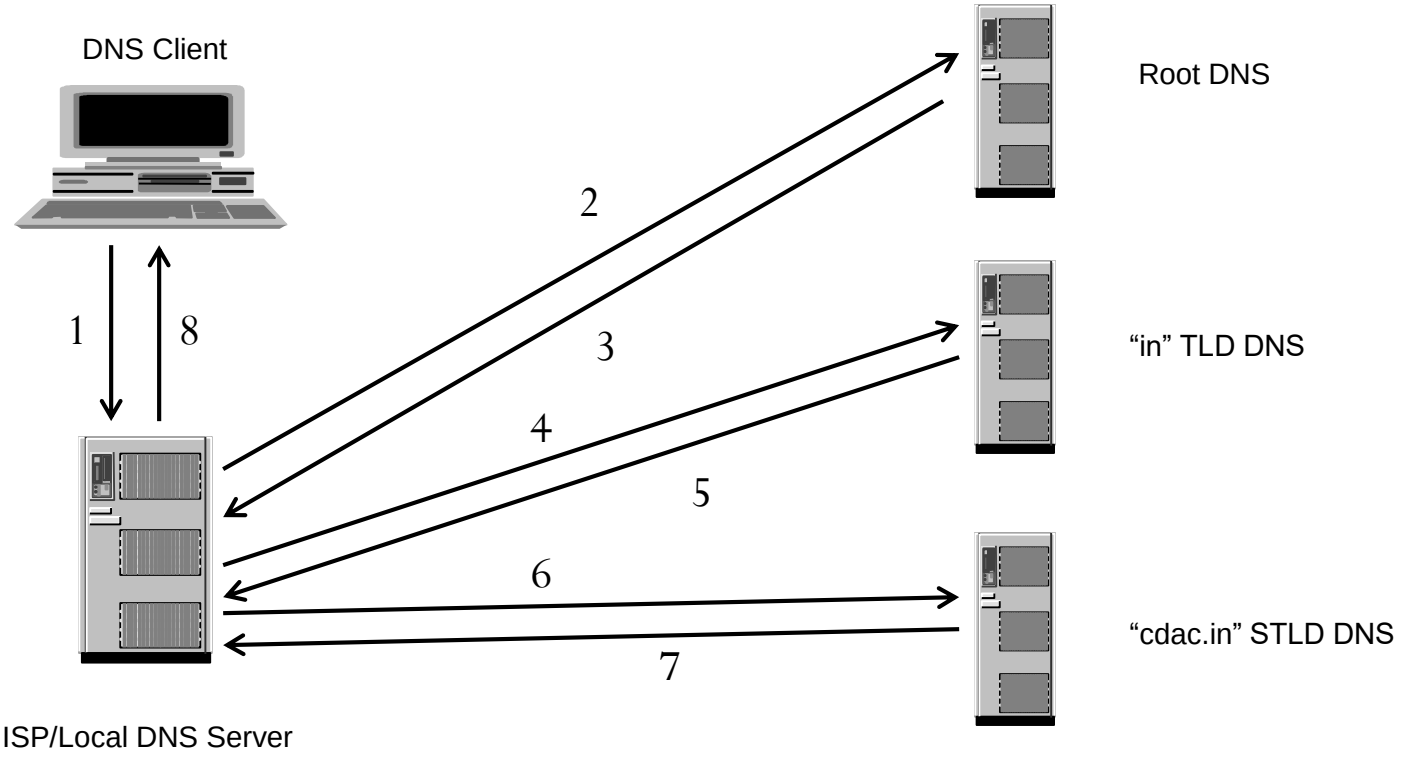
How DNS Works?

7."cdac.in" STLD DNS Server will gives the reply i.e IP address of "www.cdac.in".



How DNS Works?

7."cdac.in" STLD DNS Server will gives the reply i.e IP address of "www.cdac.in".



DNS Servers Classifications

- Root DNS Server
- Authoritative DNS Server
  - Master
  - Slave
- Recursive DNS Server
- Stub Resolver

Root DNS Server

- On the Top of the DNS Hierarchy.
- Contains the information(root zone) of all TLD (e.g. in, org, com, gov etc).
- There are 13 root Name Servers, maintained by 12 independent organisations.
  - There are several instances of all the Root Servers across the World.
  - In India we have instances of D,E,F,I,J,K,L Root Servers across the country.
- Root name server operations currently provided by volunteer efforts by a very diverse set of organizations

Root Name Server Operators

Nameserver	Operated by:
A	Verisign (US East Coast)
B	University of S. California –Information Sciences Institute (US West Coast)
C	Cogent Communications (US East Coast)
D	University of Maryland (US East Coast)
E	NASA (Ames) (US West Coast)
F	Internet Software Consortium (US West Coast)
G	U. S. Dept. of Defense (ARL) (US East Coast)
H	U. S. Dept. of Defense (DISA) (US East Coast)
I	Autonomica (SE)
J	Verisign (US East Coast)
K	RIPE-NCC (UK)
L	ICANN (US West Coast)
M	WIDE (JP)

Authoritative DNS Server

- Authoritative DNS servers serve the actual reply – i.e., the final translation of the FQDN to the IP address, as they are the authoritative source for the domain in question.
- DNS hosting companies typically manage the authoritative DNS servers for a domain name which, the users query through recursive resolvers.
- Master and Slave.

Recursive DNS Server

- Also called Recursive Resolver.
- The user queries to RR for domain lookup.
- RR queries the entire DNS Hierarchy for the final result.
- RR can also be Authoritative for some domain.

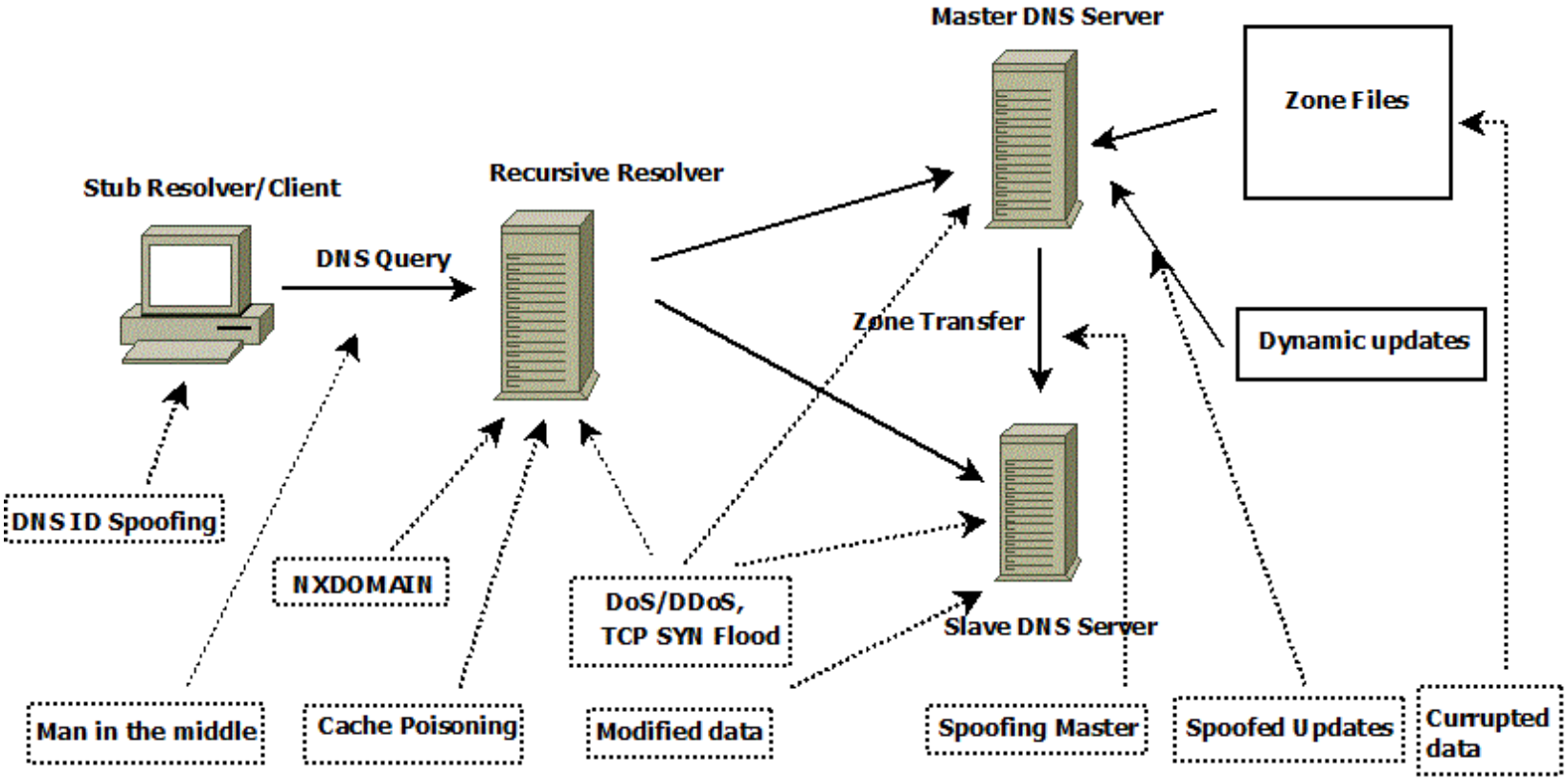
Stub Resolver

- DNS Client is called Stub Resolver.
- Always Queries RR.
- RR Replied back to Stub Resolver.

DNS Attacks

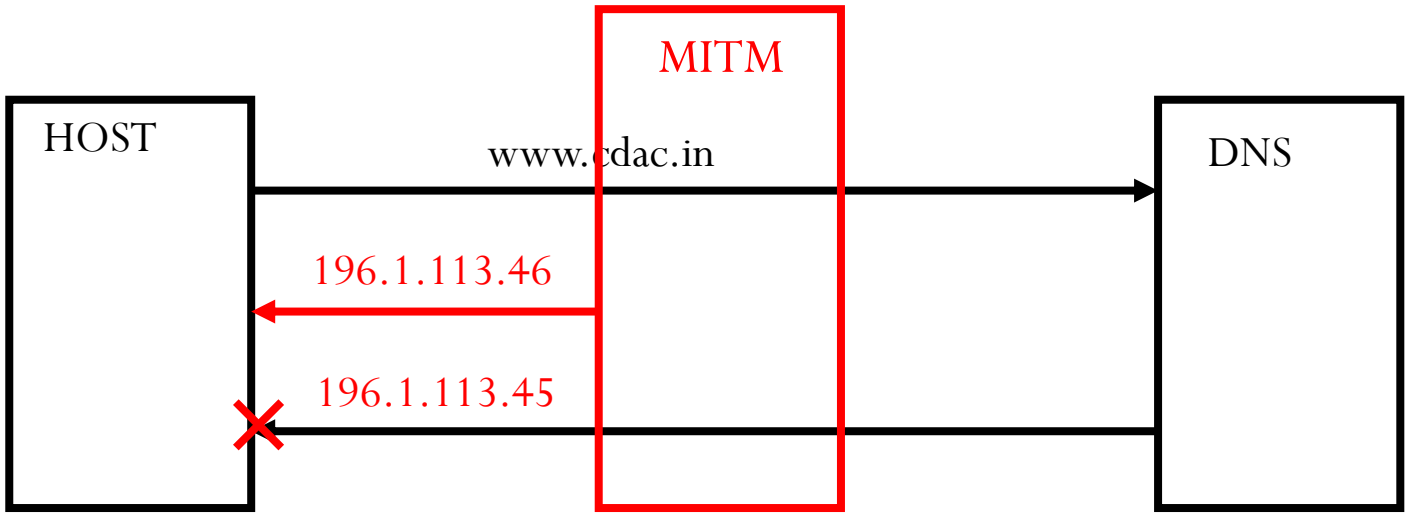
- Attacks on DNS Infrastructure
- Attacks exploiting the DNS Infrastructure

Attacks on DNS Infrastructure



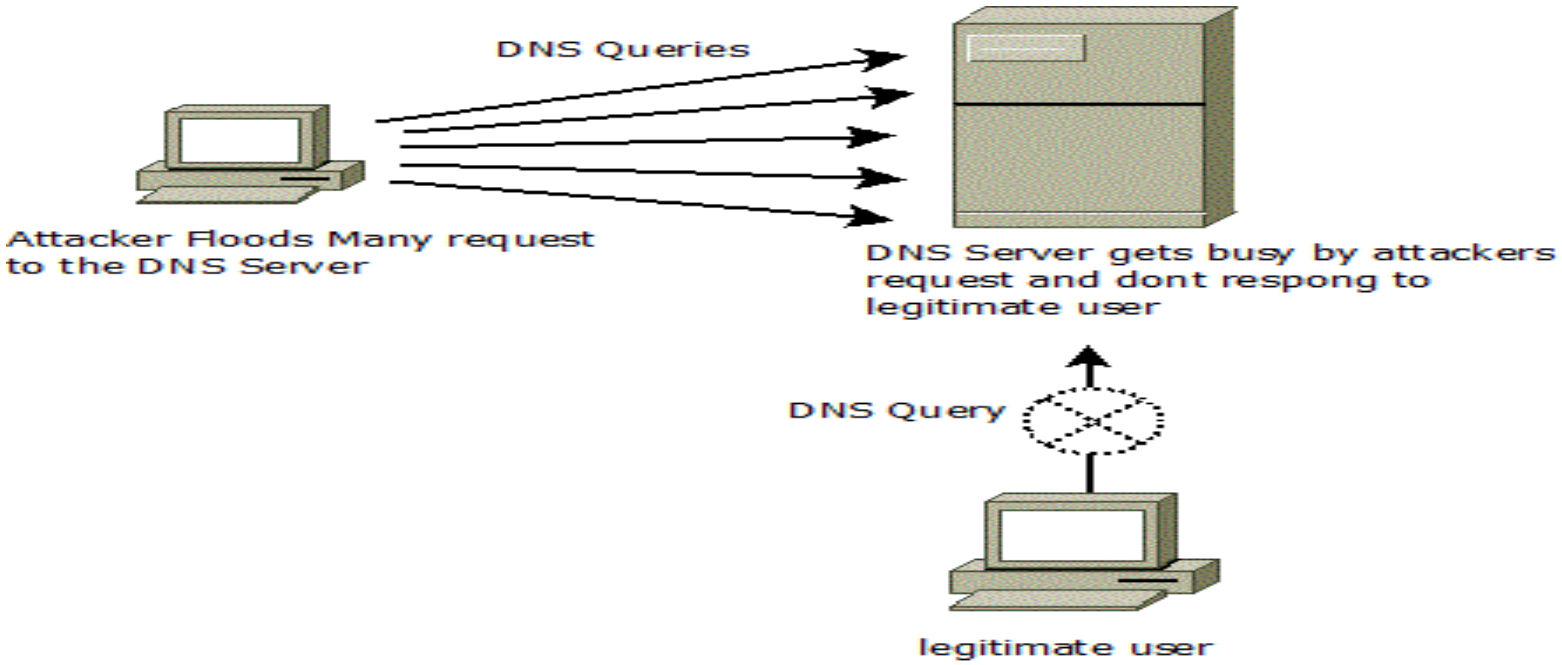
Man in The Middle Attack

- This is done by spoofing the source IP of the DNS servers and can become a bridge between the real DNS server and the client.



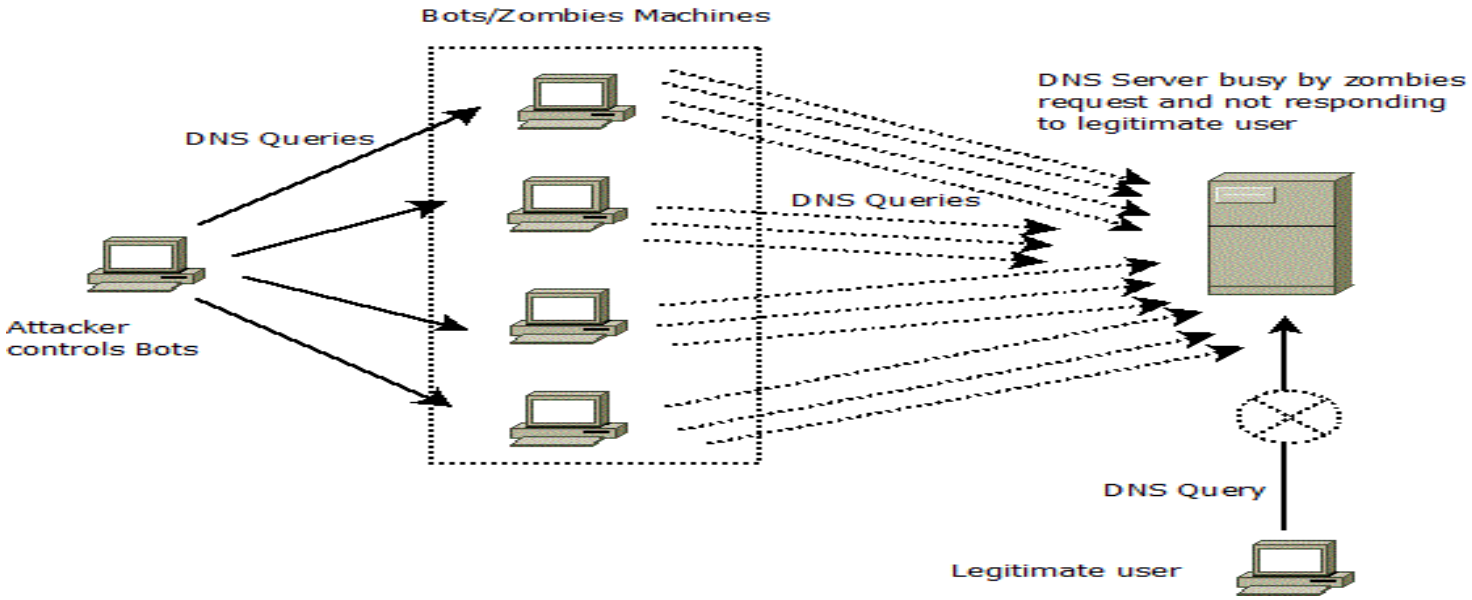
DoS

- Denial of Services(DoS) attack is a cyber-attack that is designed to bring down the network by creating unwanted traffic.



DDoS

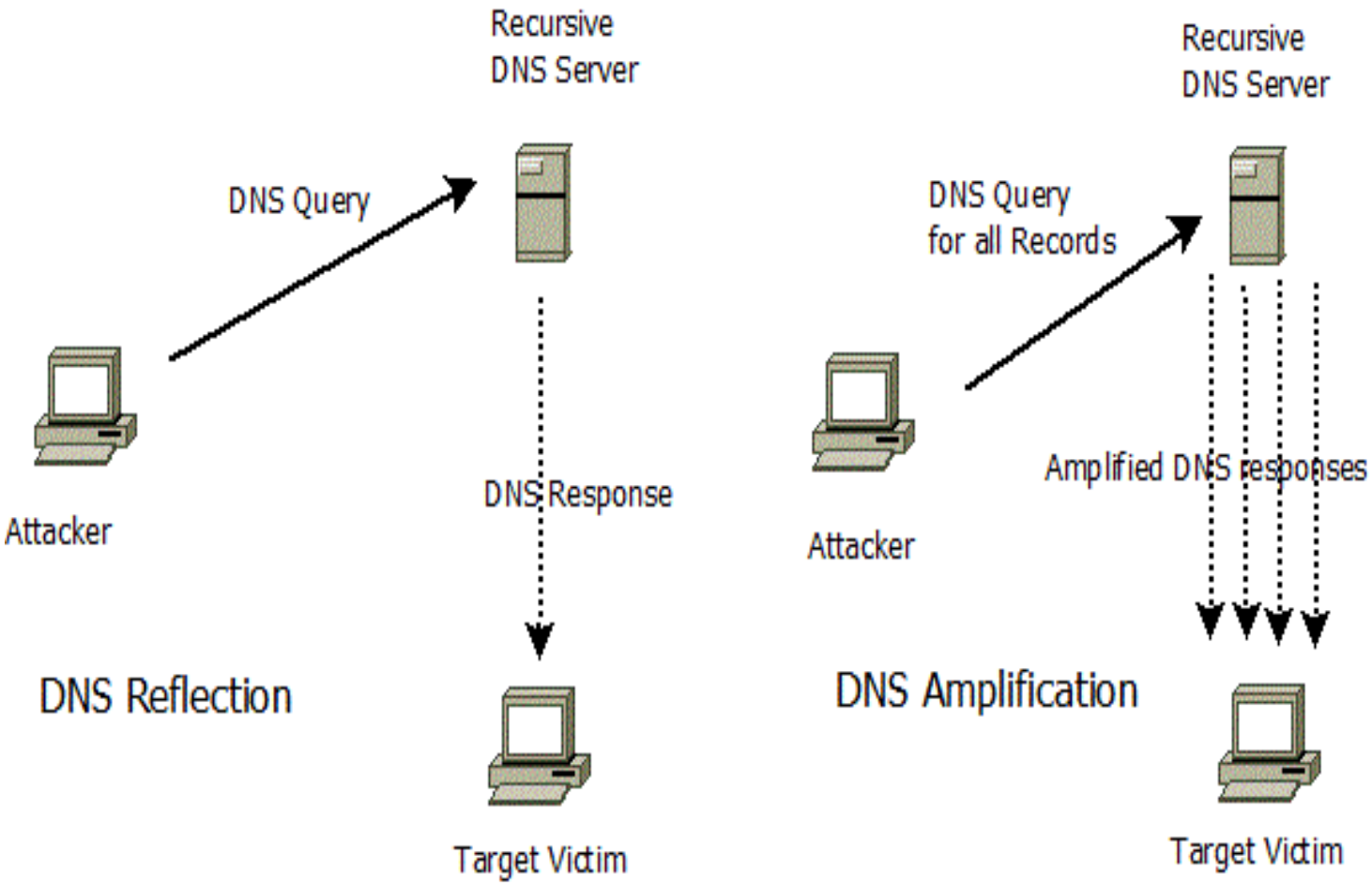
- Distributed Denial of Services(DDoS) attack, uses a Trojan horse in which it uses multiple systems to target a single system.



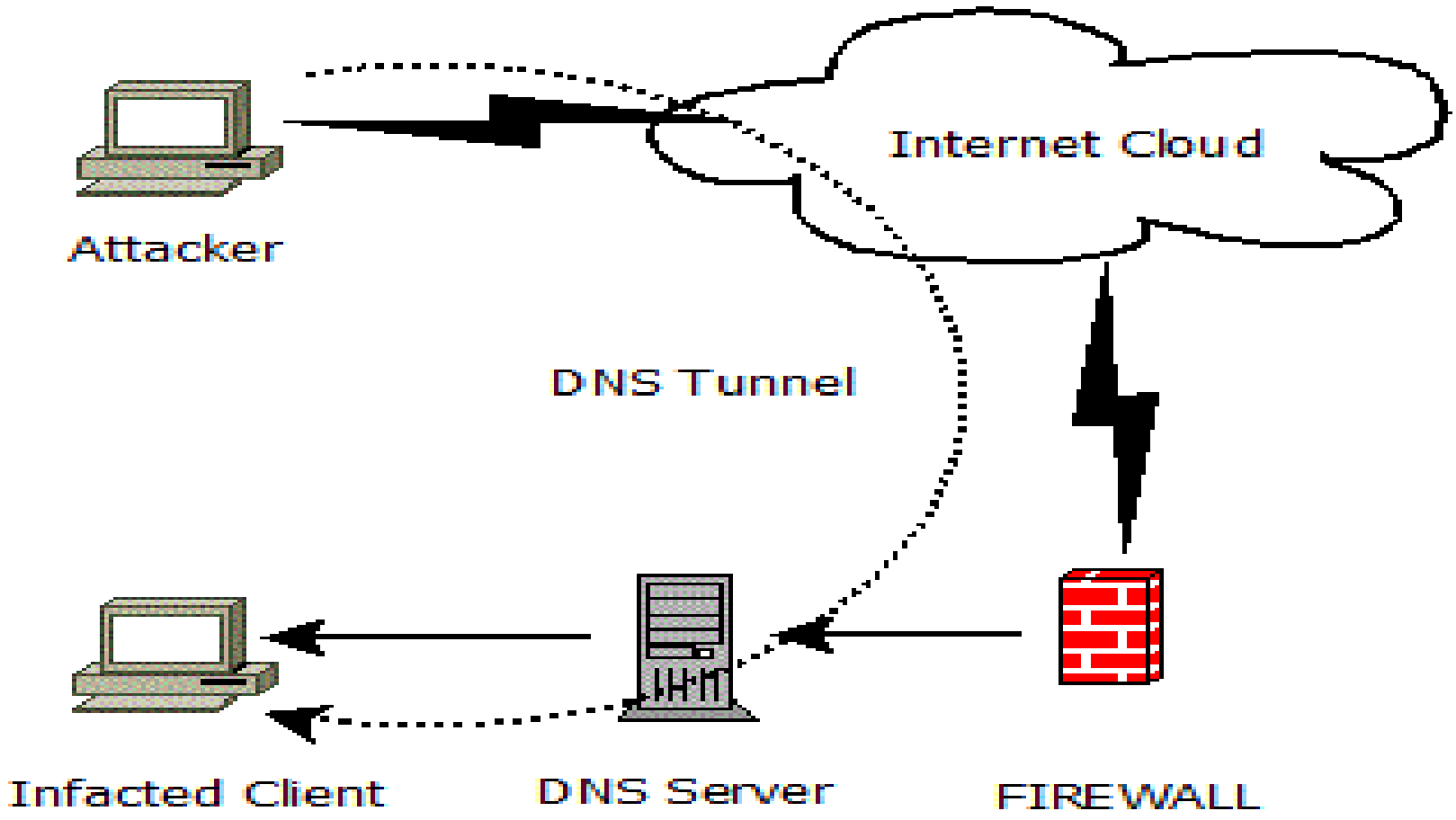
Attacks Exploiting DNS Infrastructure

- DNS Reflection
- DNS Amplification
- DNS Tunnelling
- DNS Hijacking

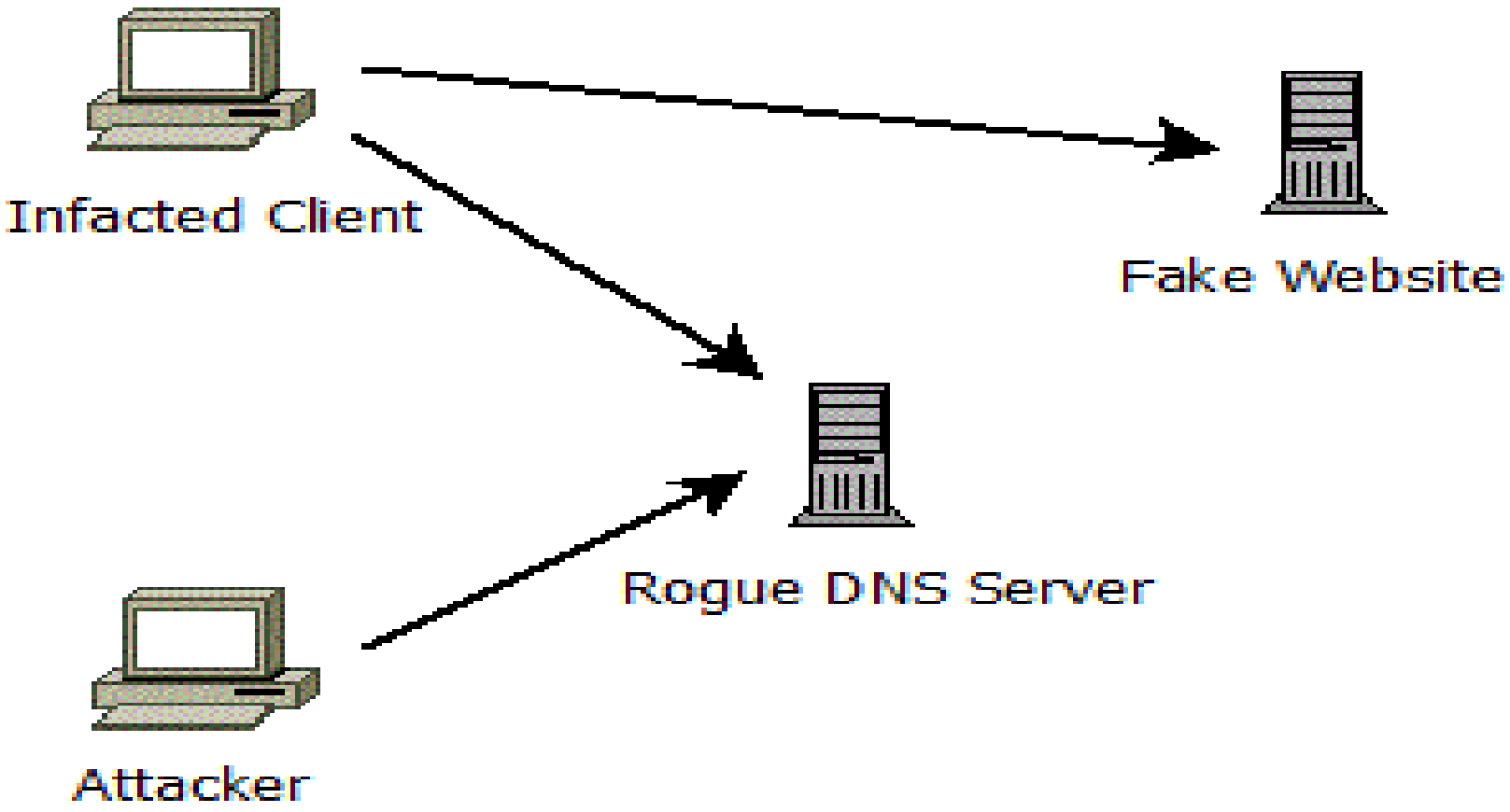
DNS Reflection and Amplification



DNS Tunnelling



DNS Hijacking



DNS Security Solution

- DNSSEC
- TSIG
- DNS Firewall
- DNS Health Measurement
- DNS Intrusion Detection

DNS Health Measurement

- DNS Vulnerabilities
  - DNS Version Check
  - SOA Check
  - Dual Stack
  - Recursion Check
  - DNSSEC Check
  - TSIG Check
- RTT Query Latency Check

DNS Intrusion Detection

- SNORT
- Signature for attacks
  - DOS/DDoS
  - Amplification
  - Tunneling
  - Hijacking

Thank You

- Queries?
- sanjayadiwal@cdac.in
- +91-9916938713