ICIRE 2019 Tutorial on

DNS: Critical Infrastructure of the Internet and DNSSEC

Sanjay Adiwal
Principal Technical Officer
C-DAC Electronics City
Bangalore

ICIRE

04-03-2019

Contents

- DNS Basics and Fundamentals
- Configuration of Recursive and Authoritative DNS Server
  - DEMO
- Attacks on DNS Server
- DNSSEC
- DNSSEC implementation on Authoritative DNS Server
  - DEMO

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.
  - 4.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.2.0.6.0.0.a.8.5.4.2.4.ip6.arpa. → www.cdac.in.

DNS Fundamentals

- DNS is the most critical component of Internet Infrastructure.
- A service that Resolves Domain Name to IPV4/V6 address and vice-versa.
  - eg. www.nitk.ac.in has 14.139.155.216
- A globally distributed, scalable, reliable database.

DNS History (1)

- ARPANET utilized a central file HOSTS.TXT
  - Contains names to addresses mapping
  - Maintained by SRI's NIC (*Stanford-Research-Institute: Network-Information-Center*)

- Administrators email changes to NIC
  - NIC updates HOSTS.TXT periodically
- Administrators FTP (download) HOSTS.TXT

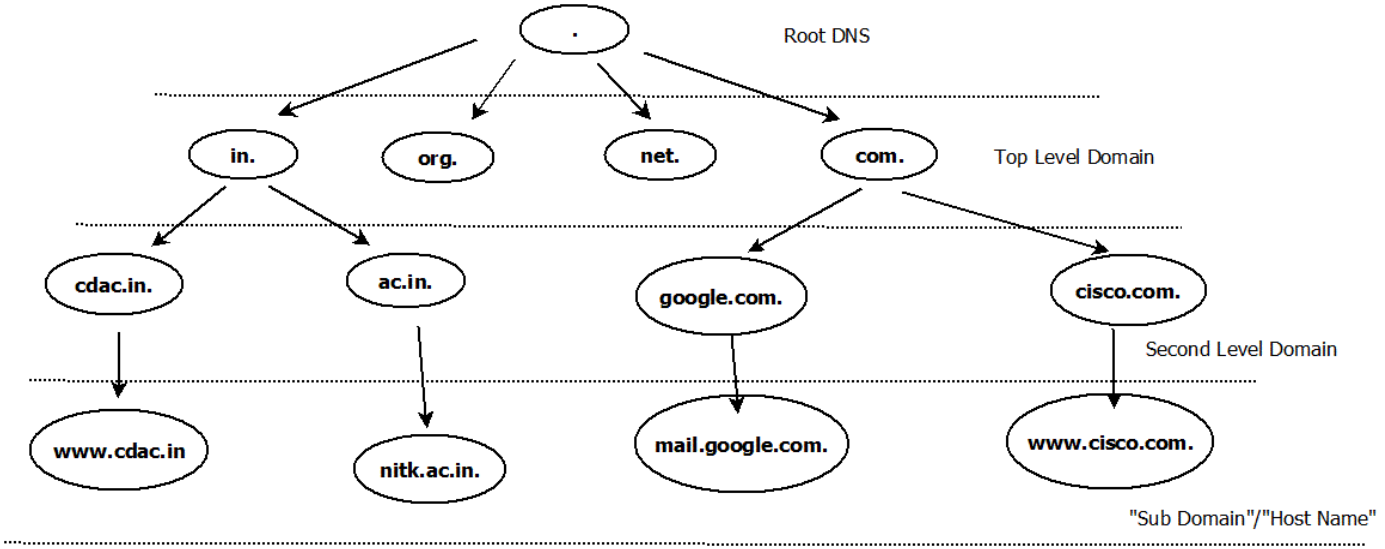
DNS History (2)

- As the system grew, HOSTS.TXT had problems with:
  - Scalability (traffic and load)
  - Name collisions
  - Consistency

- In 1984, Paul Mockapetris released the first version (RFCs 882 and 883, superseded by 1034 and 1035 …)

How is DNS built ?

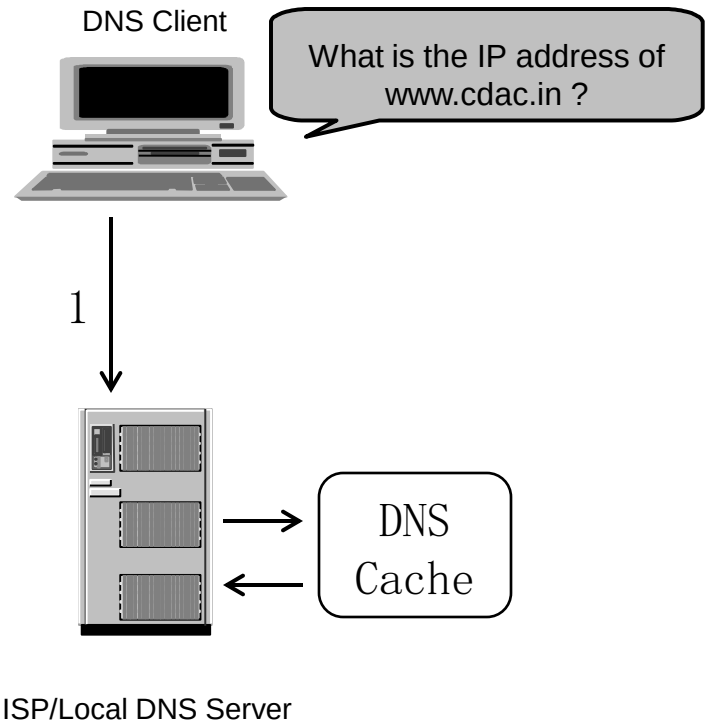
- DNS is hierarchical



- DNS administration is shared – no single central entity administrates all DNS data

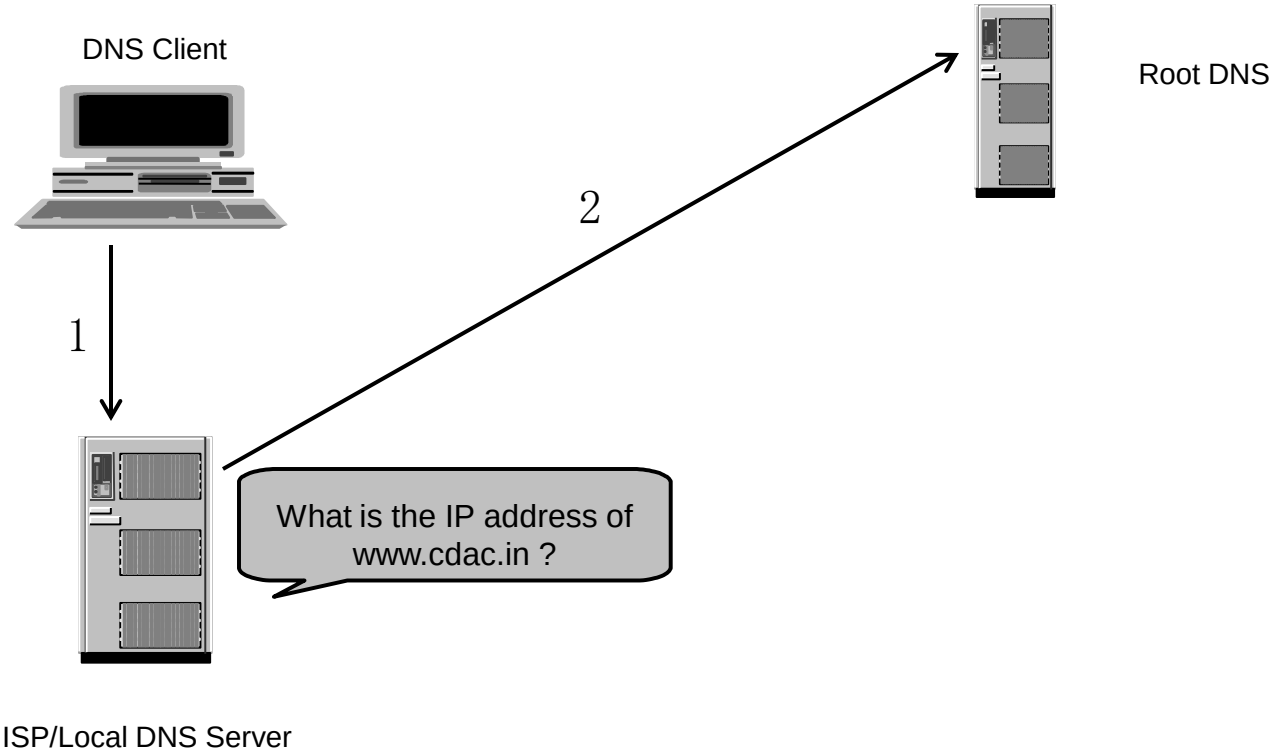
How DNS Works?

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



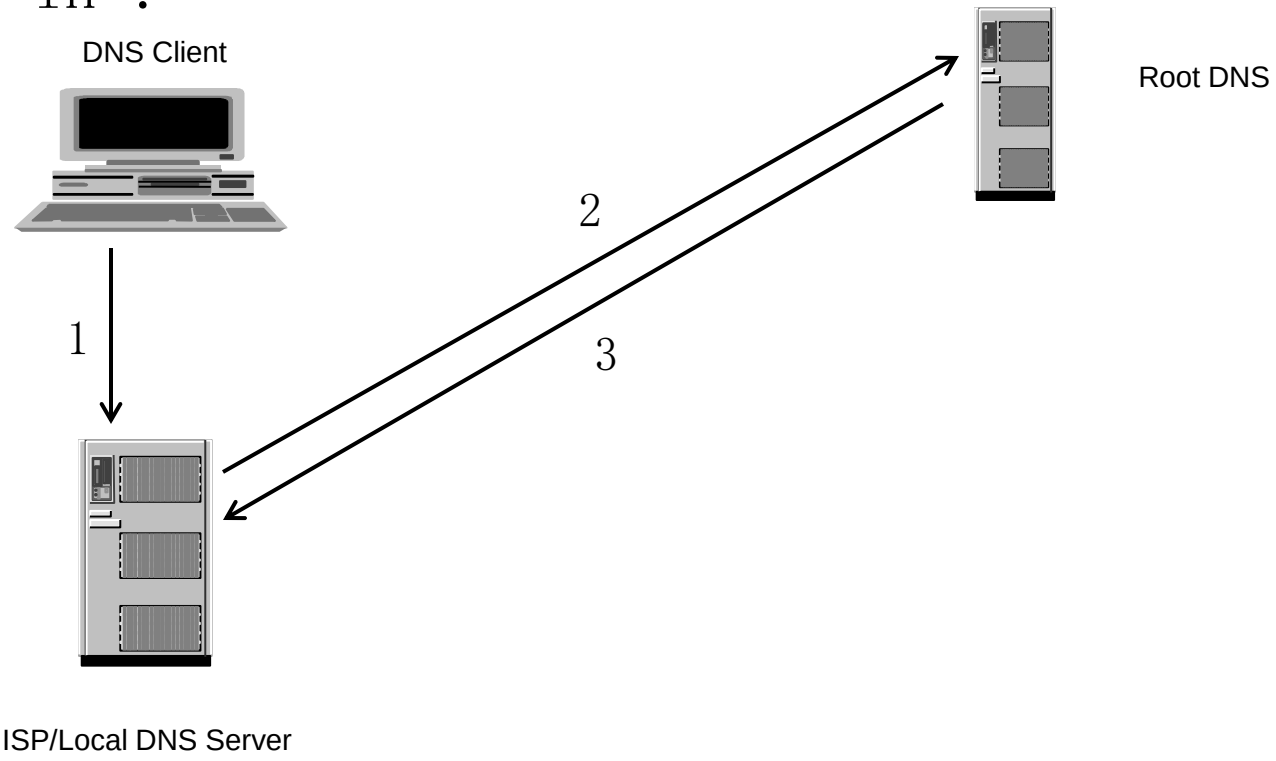
How DNS Works?

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



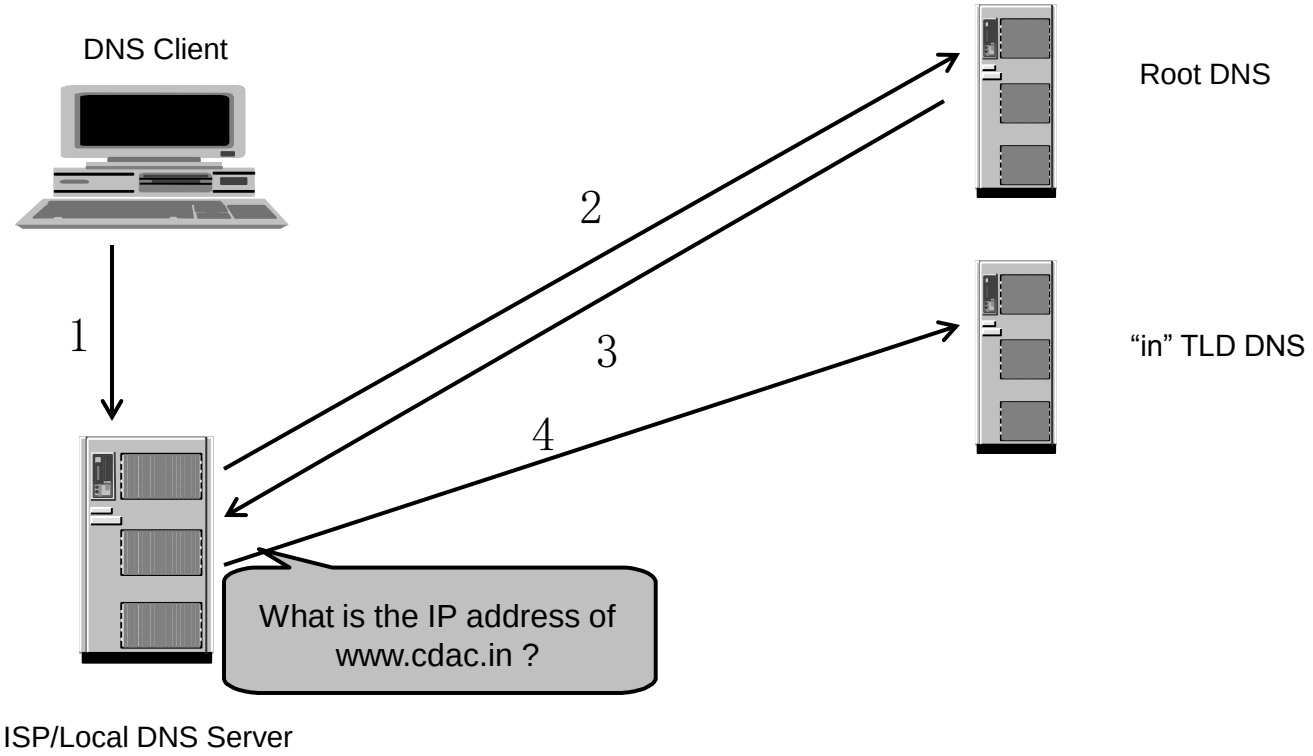
How DNS Works?

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



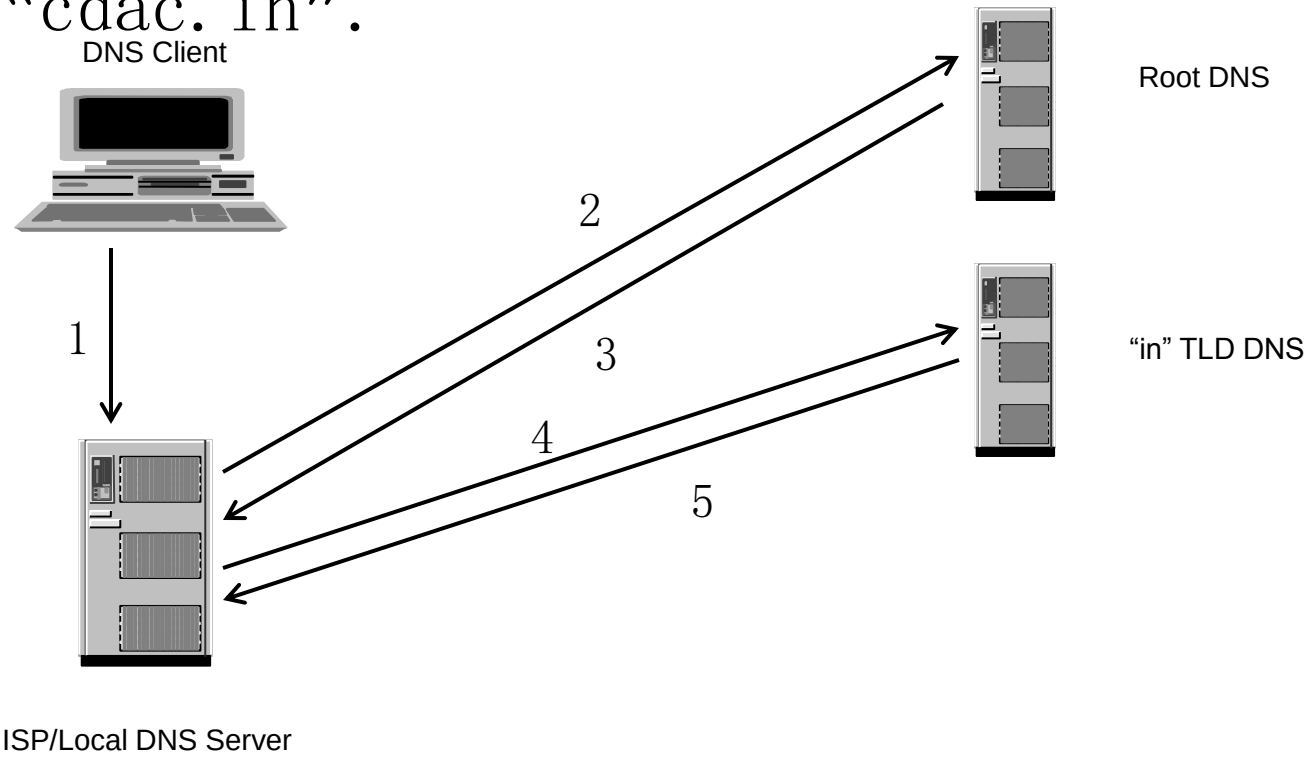
How DNS Works?

4. ISP/Local DNS Server queries TLD DNS.



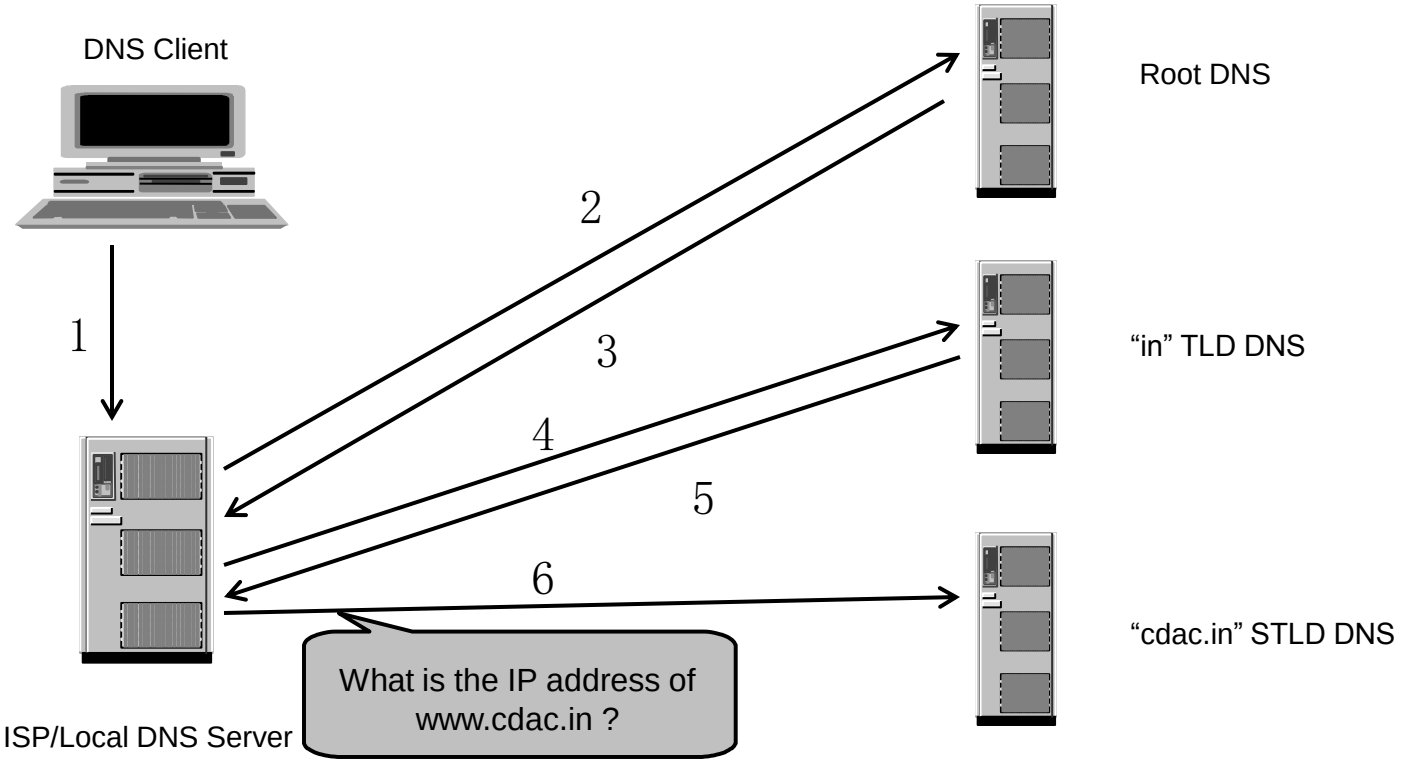
How DNS Works?

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



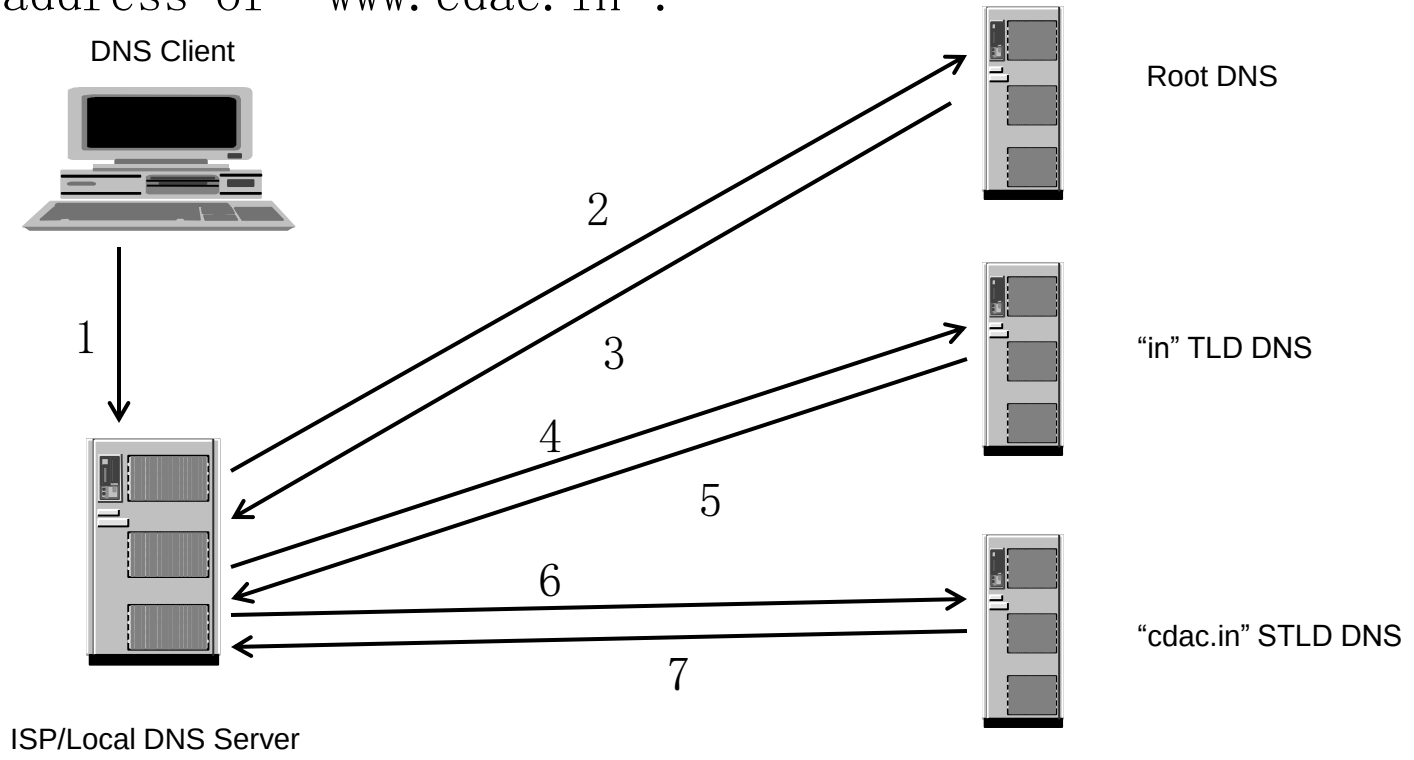
How DNS Works?

6. ISP/Local DNS Server queries STLD DNS.



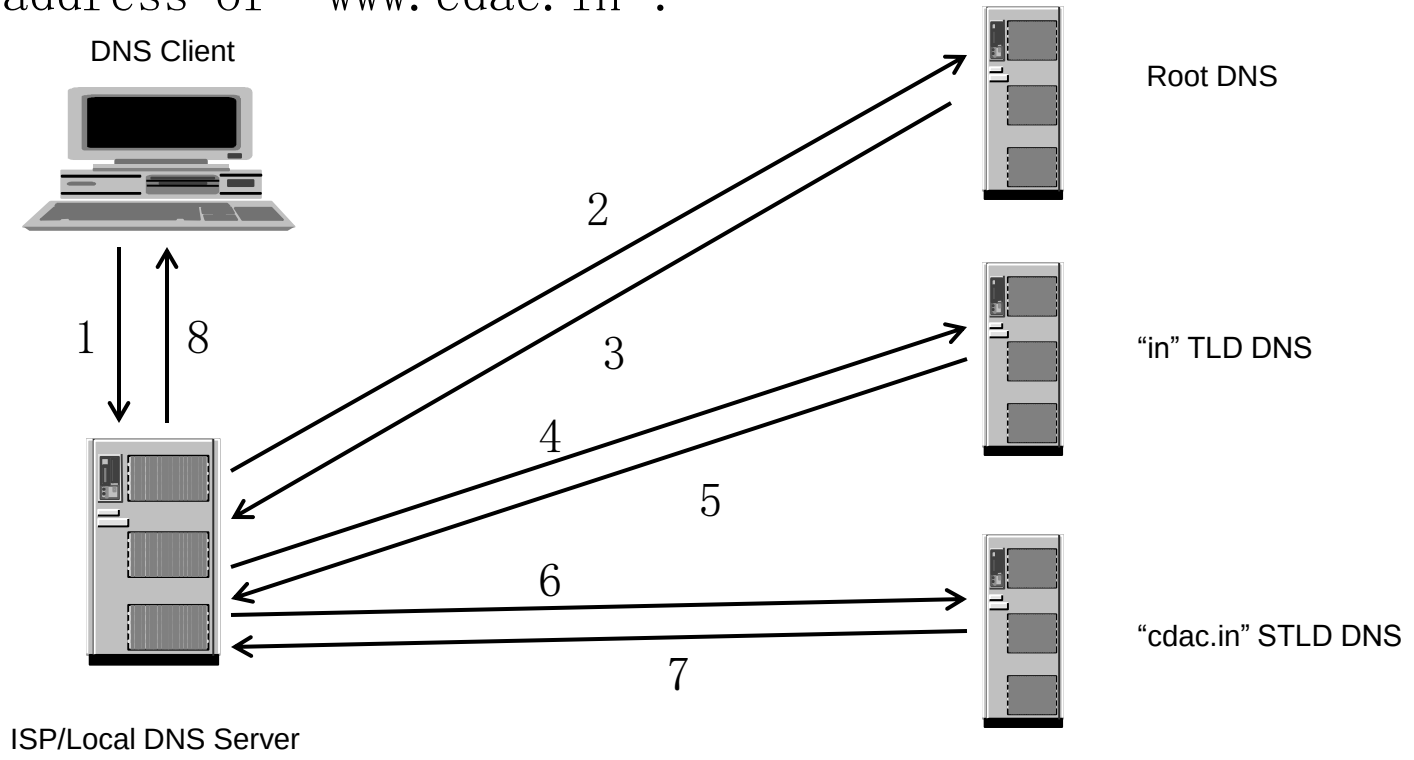
How DNS Works?

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.

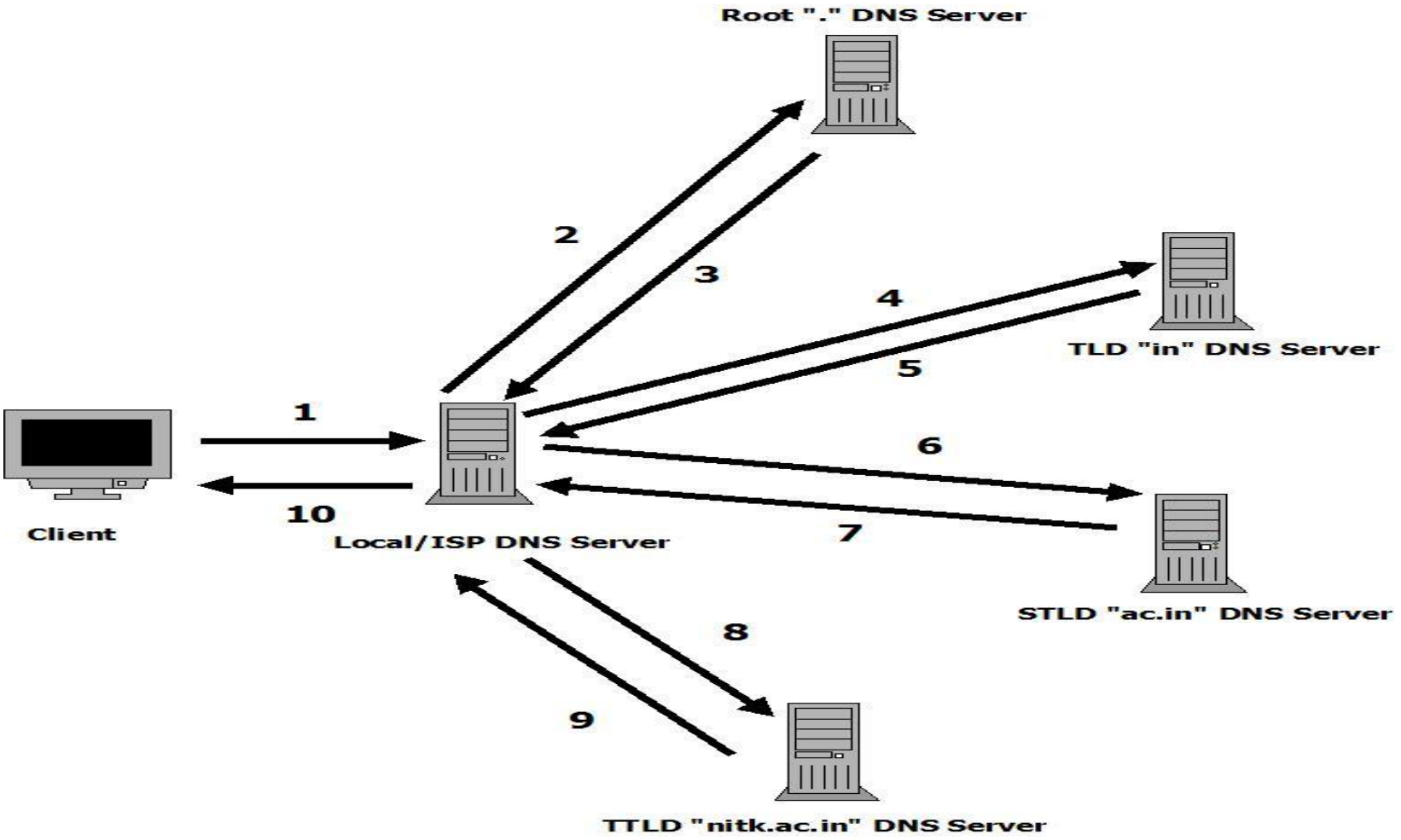
Stub Resolver

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

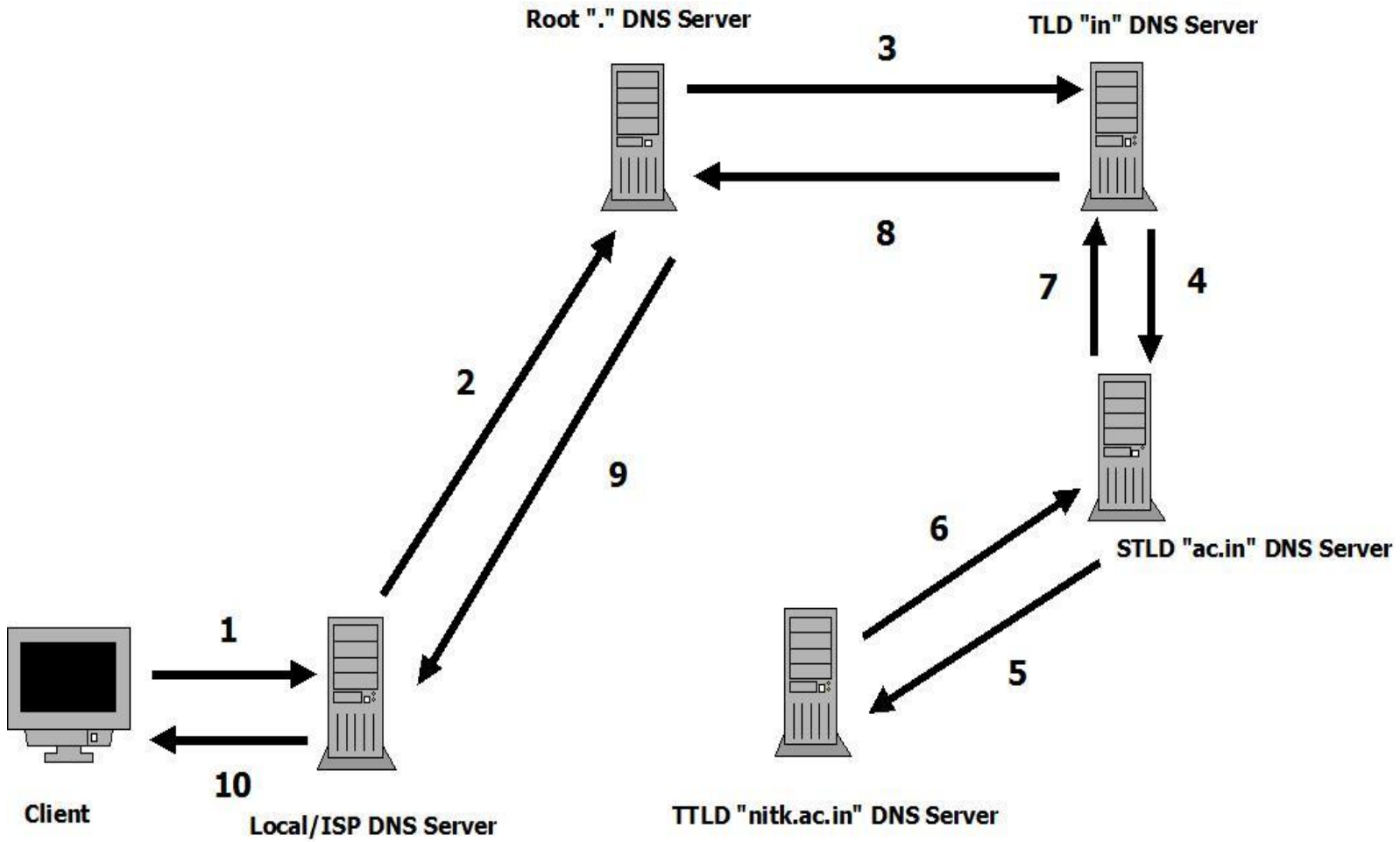
DNS Query Types

- Iterative Query
- Recursive Query
- Inverse Query

Iterative Query



Recursive Query



BIND

- Berkeley Internet Name Domain project, which is a group that maintains the DNS-related software suite that runs under Linux.
- The most well known program in BIND is named, the daemon that responds to DNS queries from remote machines.

DNS Resource Records(RR)

- Unit of data in the Domain Name System
- Define attributes for a domain name.

Label	TTL	Class	Type	RData
www	3600	IN	A	192.168.0.1

- Most Common RR
  - SOA
  - A
  - MX
  - NS

The SOA Record

- The first resource record is the Start of Authority (SOA) record, which contains general administrative and control information about the domain.

@ IN SOA	Start Of Authority. Identifies the zone followed by options enclosed in brackets.
serial	Is manually incremented when data is changed. Secondary servers query the master server's serial number. If it has changed, the entire zone file is downloaded
refresh	Time in seconds before the secondary server should query the SOA record of the primary domain. This should be at least a day.
retry	Time interval in seconds before attempting a new zone transfer if the previous download failed
expire	Time after which the secondary server discards all zone data if it contact the primary server. Should be a week at least
minimum	This is the ttl for the cached data. The default is one day (86400 seconds) but should be longer on stable LANs

The "A" Record

- The "Address" record
- One or more normally defines a host
- Contains an IPv4 Address (the address computers use to uniquely identify each other on the internet)
- Eg. The record:

  www A 202.141.136.157

  In the cdacbangalore.in domain, defines the host uniquely identifiable as "www.cdacbangalore.in" to be reachable at the IPv4 Address 202.141.136.157

The "CNAME" Record

- A CNAME defines an alias
- The alias will then be resolved, if another CNAME is encountered then the process continues until an A record is found
- Eg. The record:

  search CNAME www.google.com.

  In the cdacbangalore.in domain, defines the name uniquely identifiable as "search.cdacbangalore.in" to be and alias to "www.google.com"

The "MX" Record

- An MX record defines the mail servers for a particular domain
- Mail eXchange records hold the name of hosts, and their priorities, able to deliver mail for the domain.
- Eg. The record:

  cdac.in MX 10 trinetra.cdac.in

  In the cdac.in domain, defines the host trinetra to be the priority 10 mail server for the "cdac.in" domain

The "NS" Record

- An NS record defines the authoritative Name servers for the domain.
- The "Name Server" records also define the name servers of children domains
- Eg. The record:

  cdacbangalore.in NS md1.cdacmumbai.in

  In the cdacbangalore.in domain, defines the host "md1.cdacbangalore.in" to be a name sever for the "cdacbangalore.in" domain

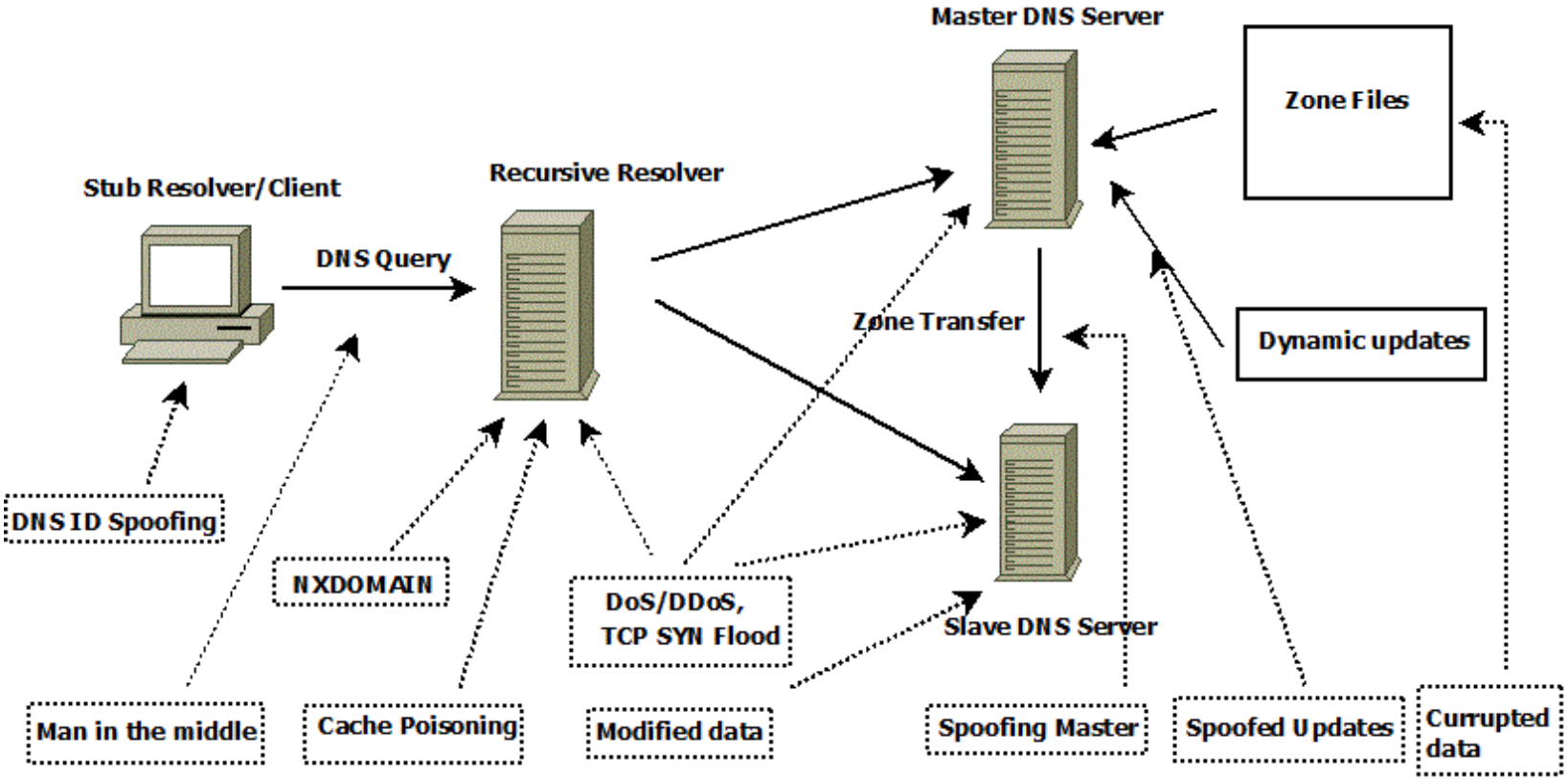
Configuring BIND

- OS CentOS
- Named is DNS Sever demon.
- DEMO
  - Configuration of Recursive Resolver
  - Configuration of Authoritative DNS Server

DNS Attacks

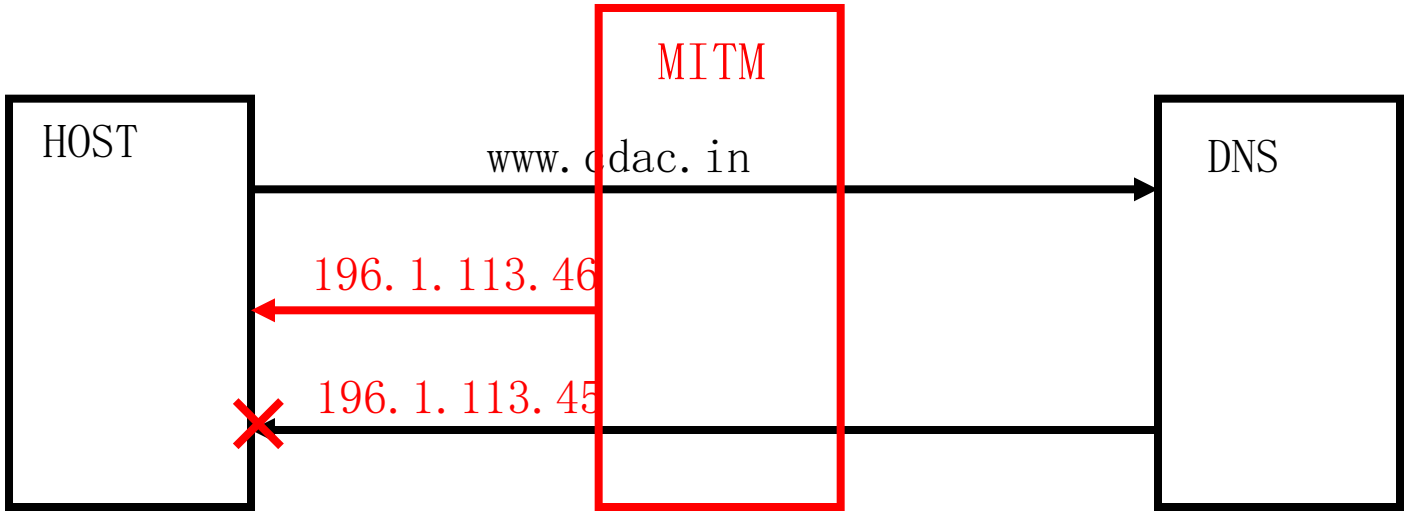
- Attacks on DNS Infrastructure
- Attacks exploiting the DNS Infrastructure

Attacks on DNS Infrastructure



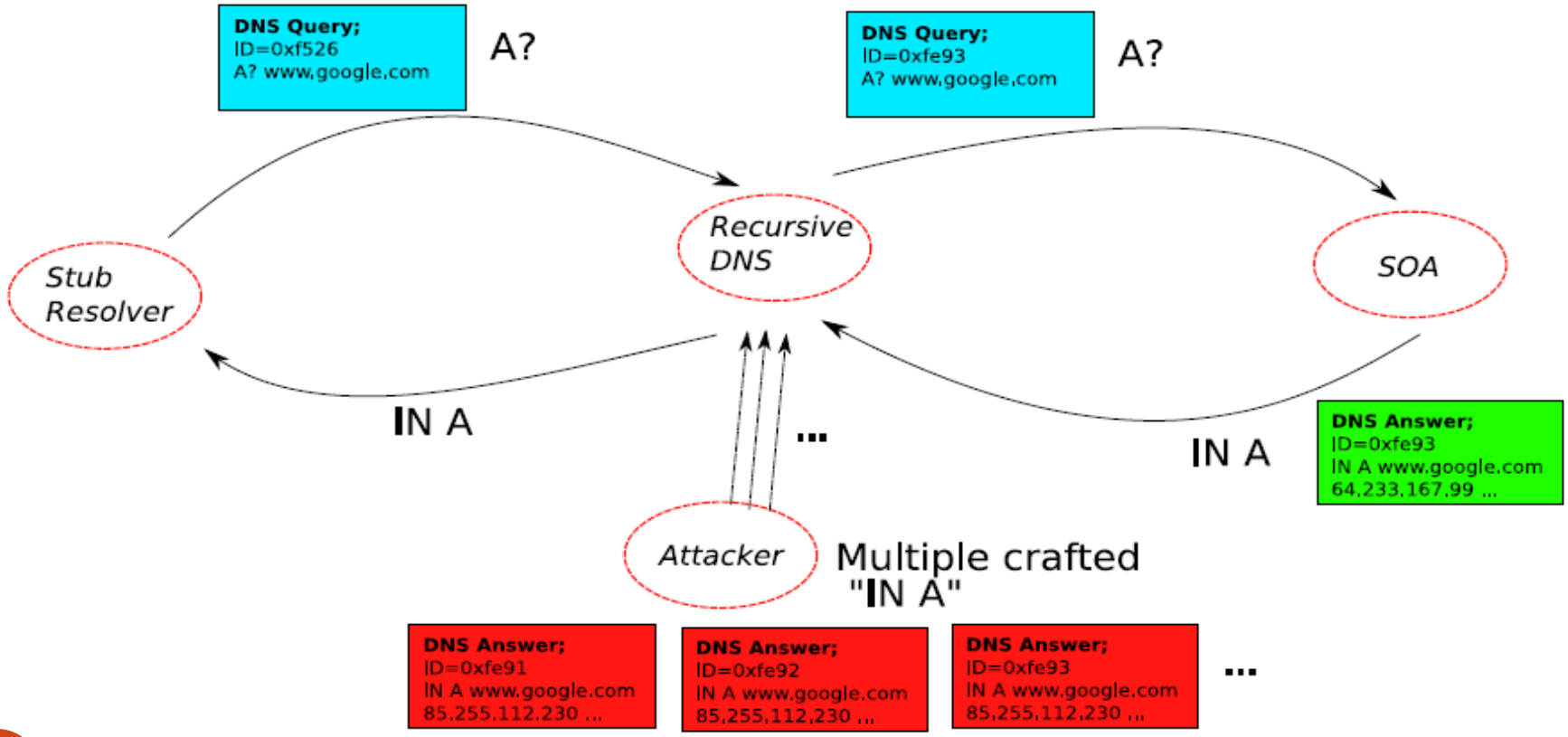
Man in The Middle Attack

- 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.



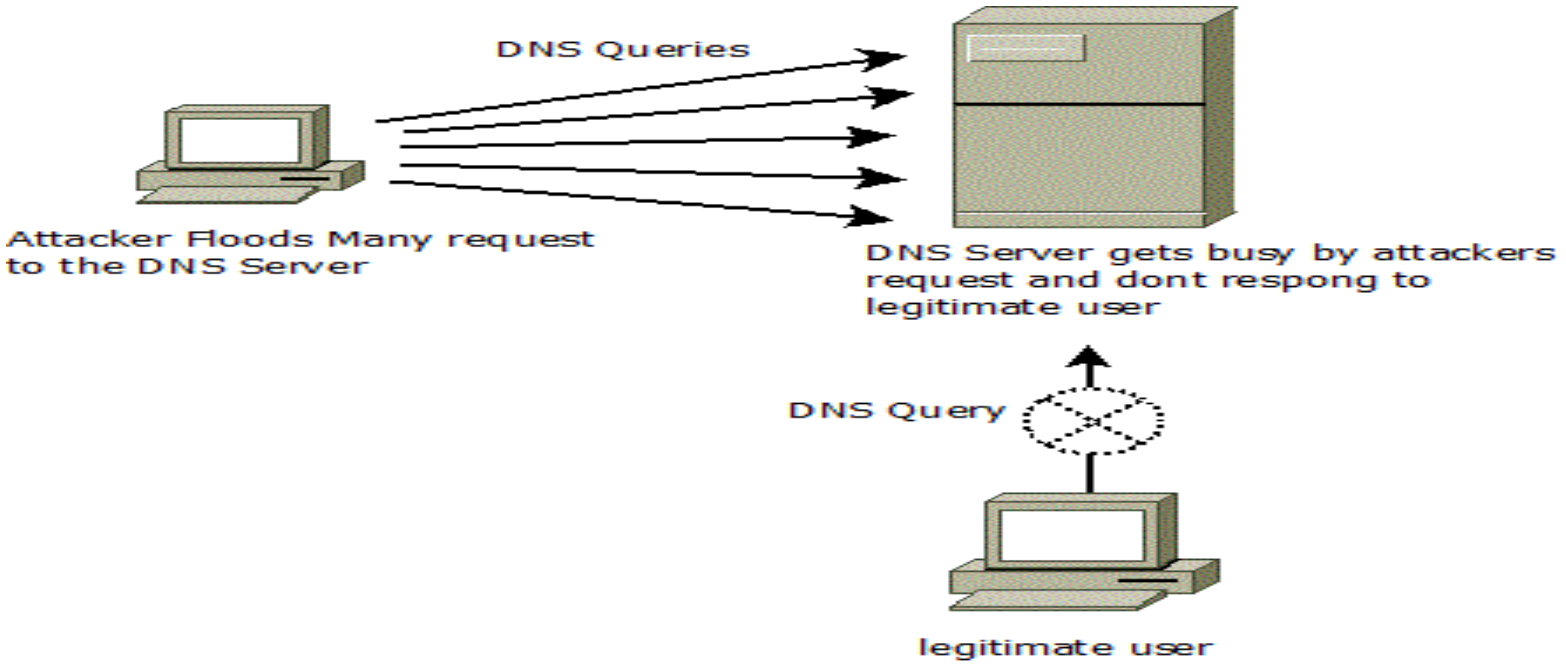
DNS Cache Poisoning

- Racing to Respond First



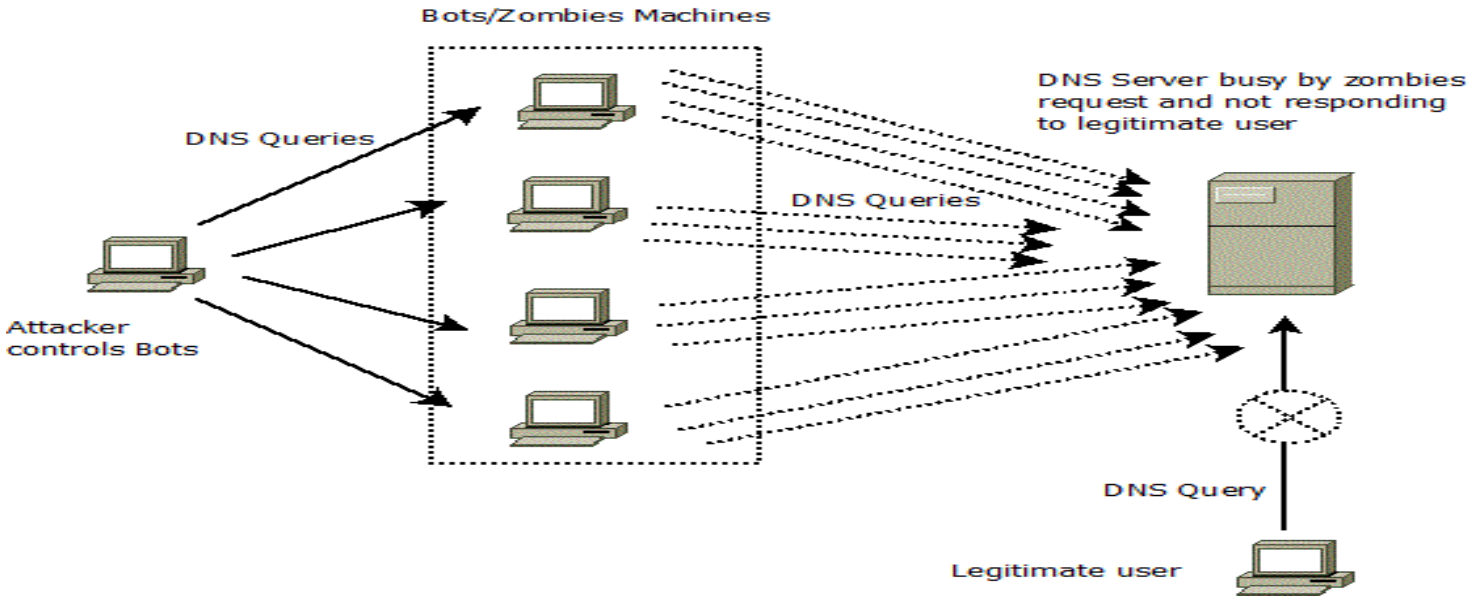
DoS

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



DDoS

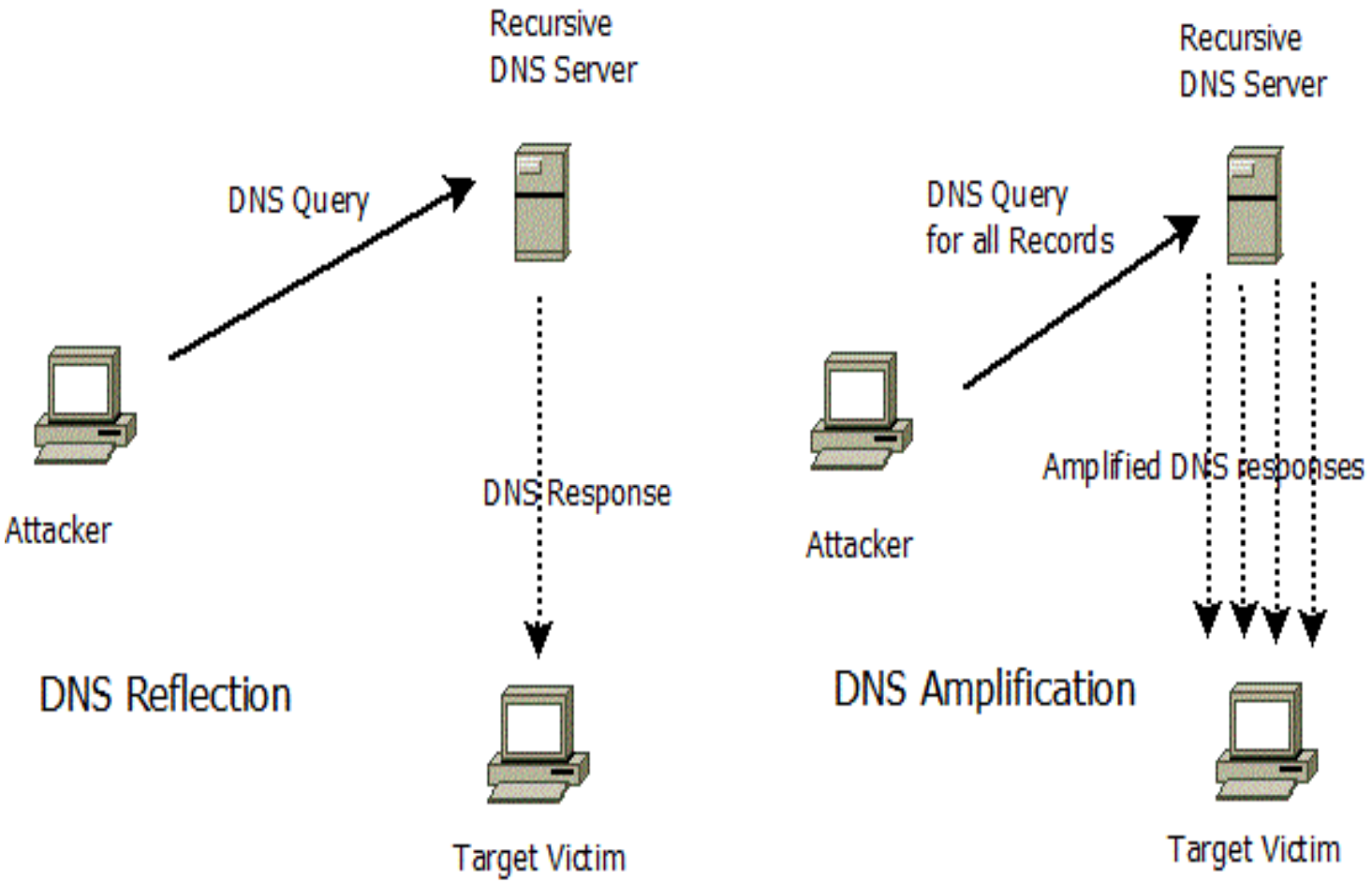
- Distributed Denial of Services(DDoS) attack, uses a Trojan horse in which it uses multiple systems to target a single system.



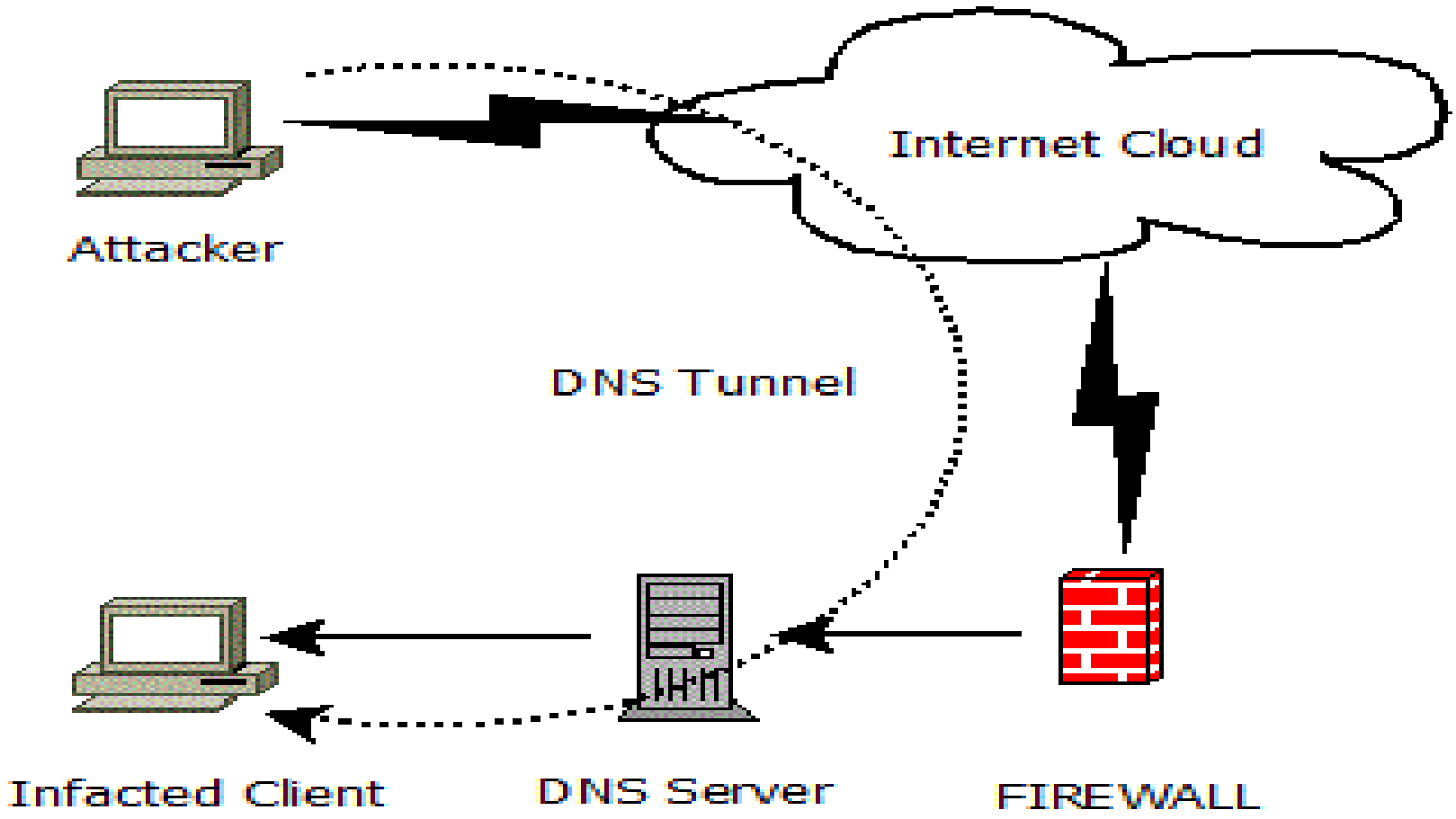
Attacks Exploiting DNS Infrastructure

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

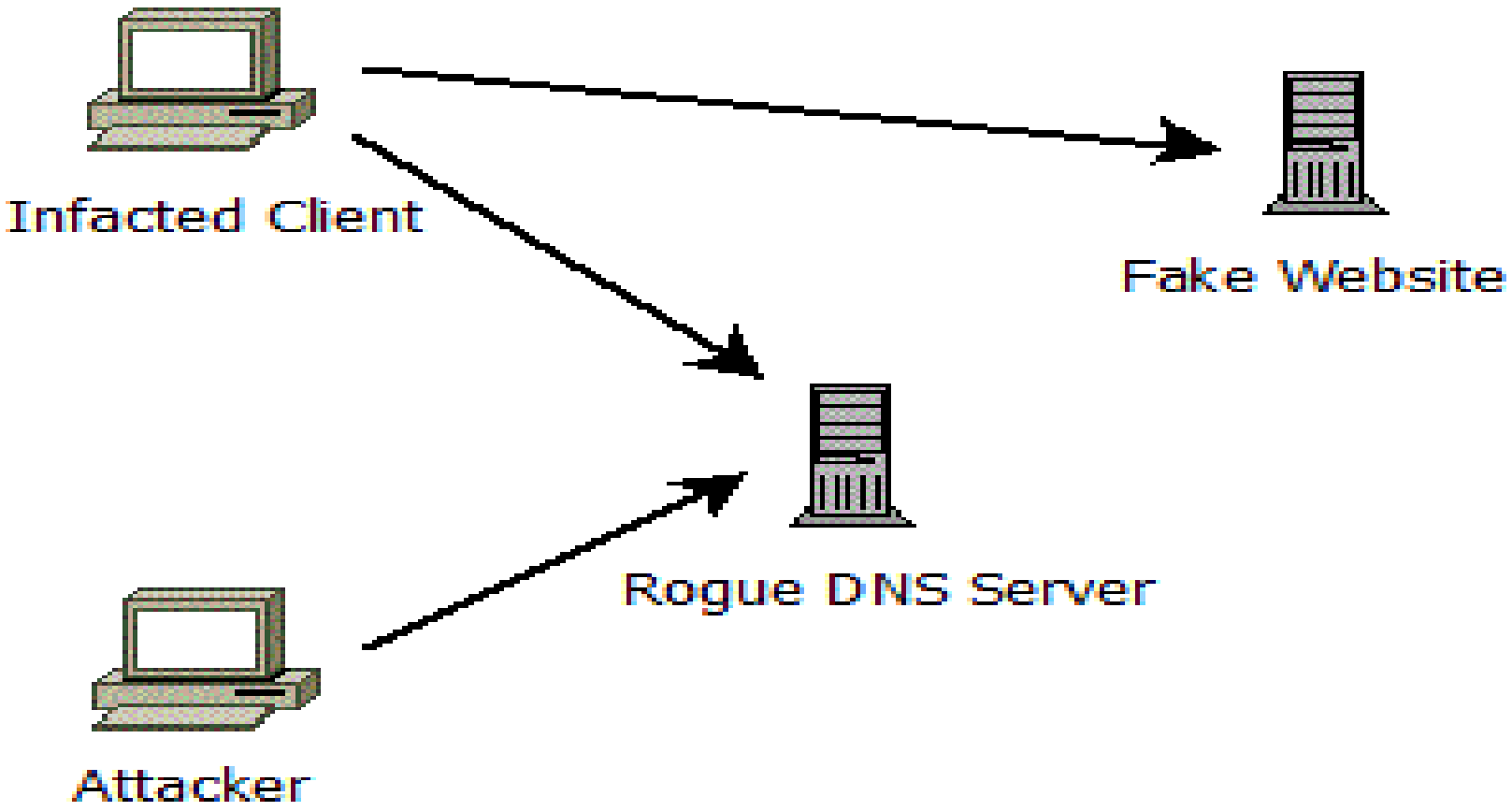
DNS Reflection and Amplification



DNS Tunnelling



DNS Hijacking



DNS Vulnerability

- Most DNS queries and responses are in plaintext
- No authentication is done for DNS response
  - You really has no good way to tell if the DNS response you get are trustable or not!
- DNS is mostly relying on UDP packets
  - IP address spoofing is very easy for UDP packets
    - No seq/ack numbers

DNS Security Solutions Available

- DNSSEC
- TSIG

DNSSEC

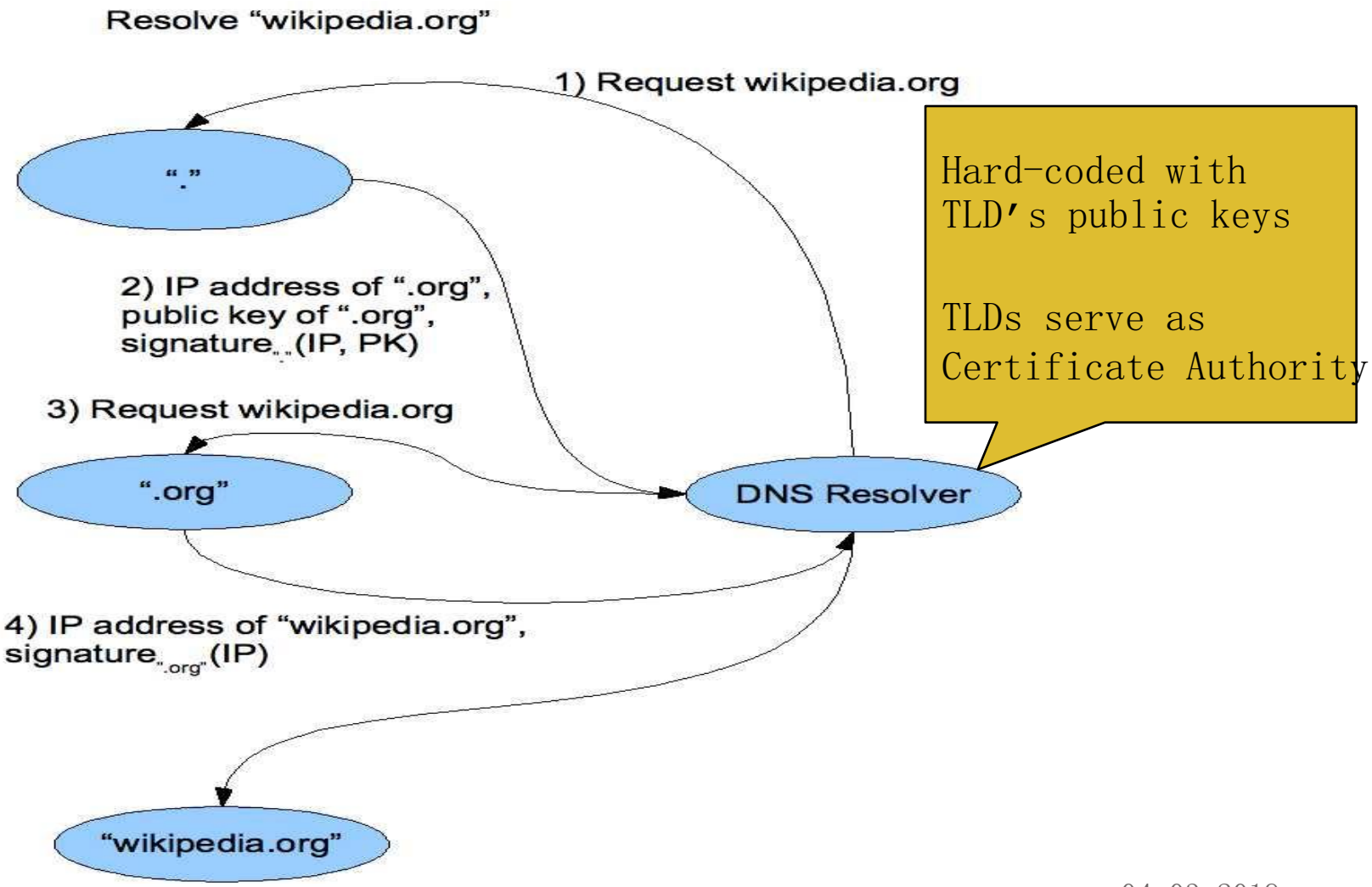
Guarantees:

- Authenticity of DNS answer origin
- Integrity of reply
- Authenticity of denial of existence

Accomplishes this by signing DNS replies at each step of the way

Uses public-key cryptography to sign responses

DNS Signing


Resolve "wikipedia.org"
1) Request wikipedia.org
"."
2) IP address of ".org",
public key of ".org",
signature"."(IP, PK)
3) Request wikipedia.org
".org"
DNS Resolver
4) IP address of "wikipedia.org",
signature".org"(IP)
"wikipedia.org"
Hard-coded with
TLD's public keys
TLDs serve as
Certificate Authority

DNSSEC Resource Record

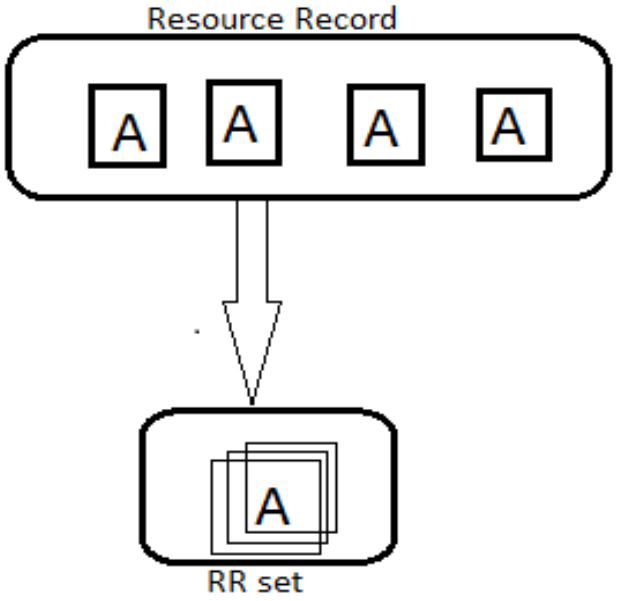
- **DNSKEY Resource Record**
- **RRset's (Resource Record Set)**
- **Zone Signing Key (ZSK)**
- **Key Signing Key (KSK)**
- **DS Record (Delegation Sign Record)**

DNSKEY Resource Record

- DNSKEY is use to store the public key of zone signing key and key signing key

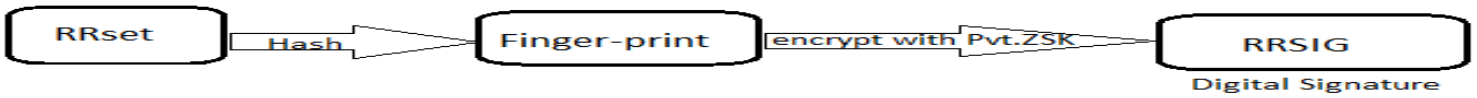
RRset's (Resource Record Set)

- A set of record which contain the same type and same record or zone.



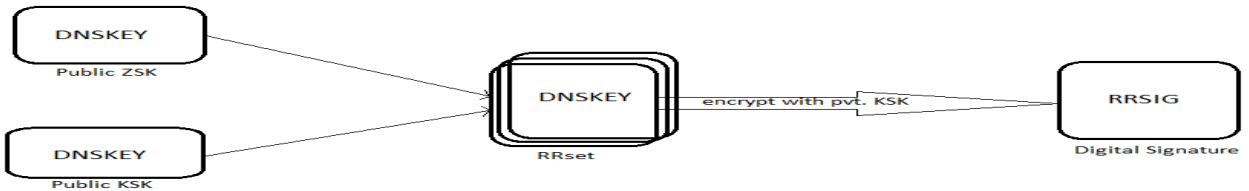
Zone Signing Key (ZSK)

- Each zone in DNSSEC has a zone-signing key pair (ZSK)
  - private portion of the key digitally signs each RRset in the zone, while the public portion verifies the signature.
- To enable DNSSEC, a zone operator creates digital signatures for each RRset using the private ZSK and stores them in their name



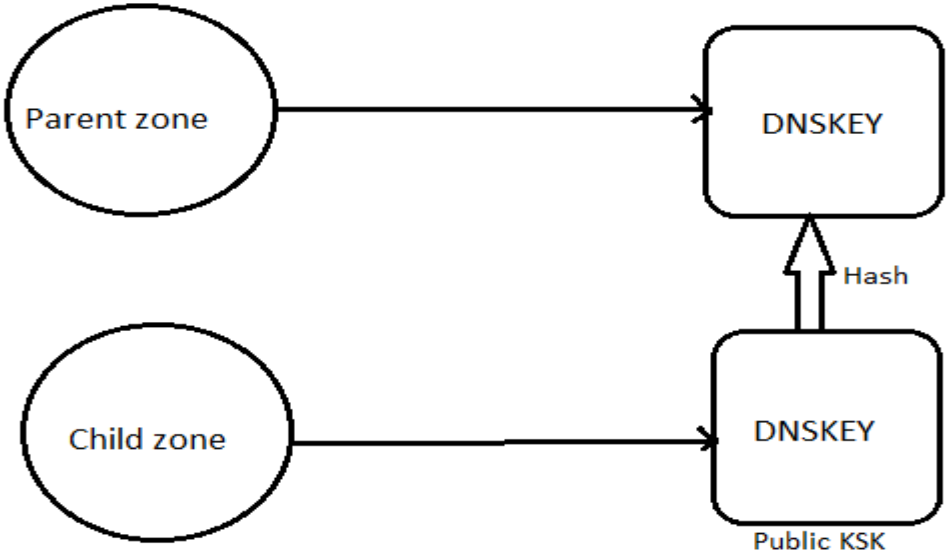
Key Signing Key (KSK)

- what if the zone-signing key was compromised? We need a way to validate the public ZSK.
- Both the public KSK and public ZSK are signed by the private KSK in DNSKEY Record.
- Resolvers can then use the public KSK to validate the public ZSK.



DS Record (Delegation Sign Record)

- DNSSEC introduces a delegation signer (DS) record to allow the transfer of trust from a parent zone to a child zone.
- DS Record is the hash of DNSKEY.



DNSSEC Configuration

- DEMO
  - DNSSEC on authoritative DNS Server

Thank You

- Queries?