DNS Security

Dr. Balaji Rajendran
Joint Director

Centre of Excellence in DNS Security
Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore 560 100

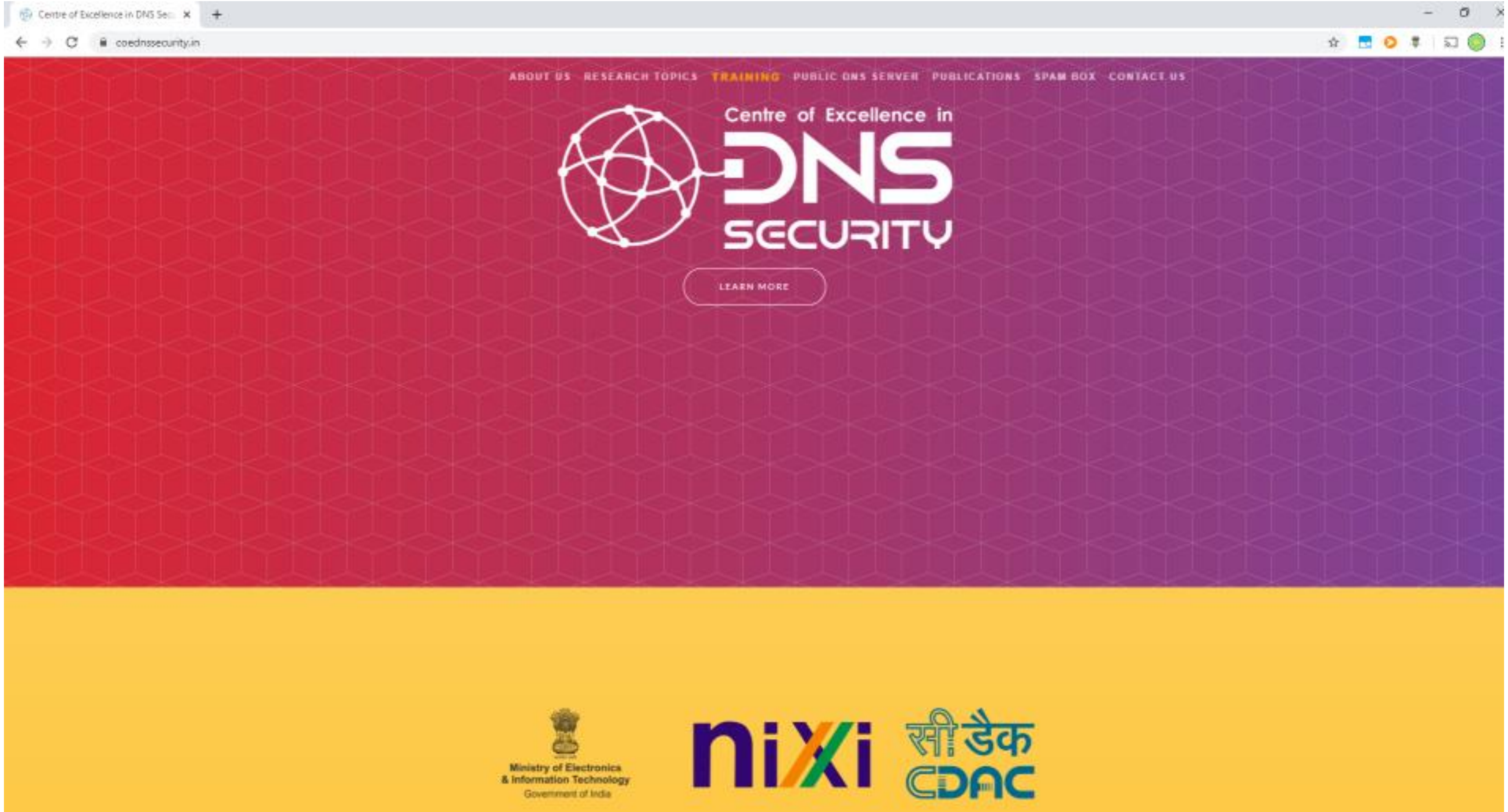
2-Day Webinar on DNS Security
21st May 2020

/iiref coednssecurity.in @IIRnEF

Agenda

- DNS Basics
- Architecture
- Forward and Backward Resolution

Need for DNS



Application Layer

- HTTP/HTTPS
- www.coednssecurity.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 does DNS do?

- Translates 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.
  - 5.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.2.0.6.0.0.a.8.5.0.4.2.ip6.arpa. → www.cdac.in.

DNS Fundamentals

- Application Layer protocol
- Runs over **UDP** and user port 53 (for queries and responses)
- Uses TCP for zone data transfers (between master and slave)
- Used by other Application Layer Protocols such as HTTP, FTP, SMTP for name resolution
- No single server in the World has all of the mappings for all of the hosts in the Internet

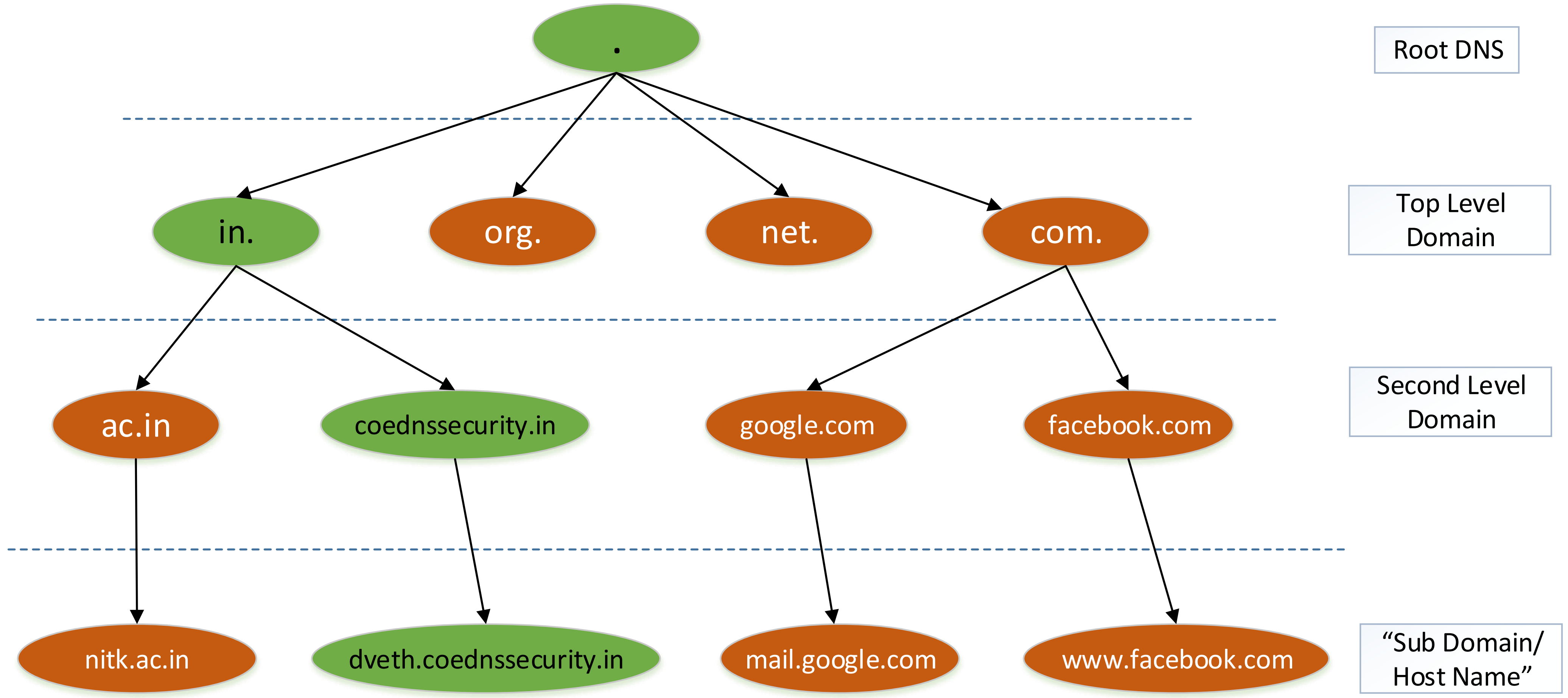
DNS Fundamentals

- Consistent hierarchical name space for referring to resources
  - Nodes at same level cannot have same names
  - Tree Structure
- A critical component of the Internet Infrastructure
- Globally Distributed, Scalable, and Reliable Database

Structure of DNS

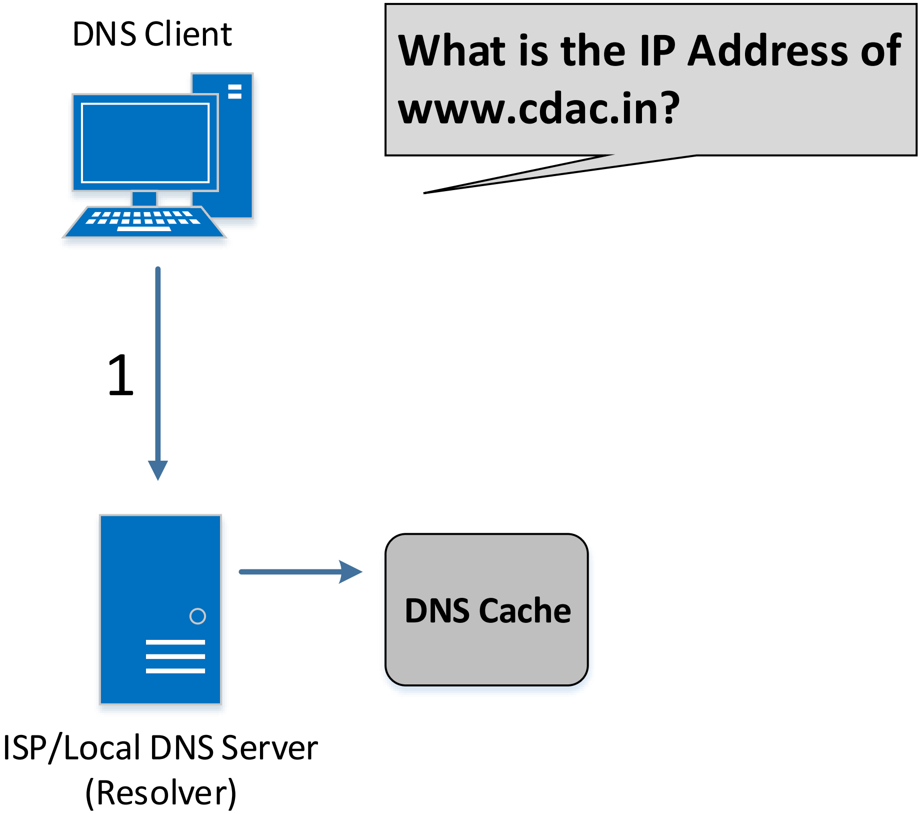
- Decentralized *naming* system
- DNS *administration* is shared – no single central entity administrates all DNS data
- This distribution of the administration is called *delegation*

Structure of DNS



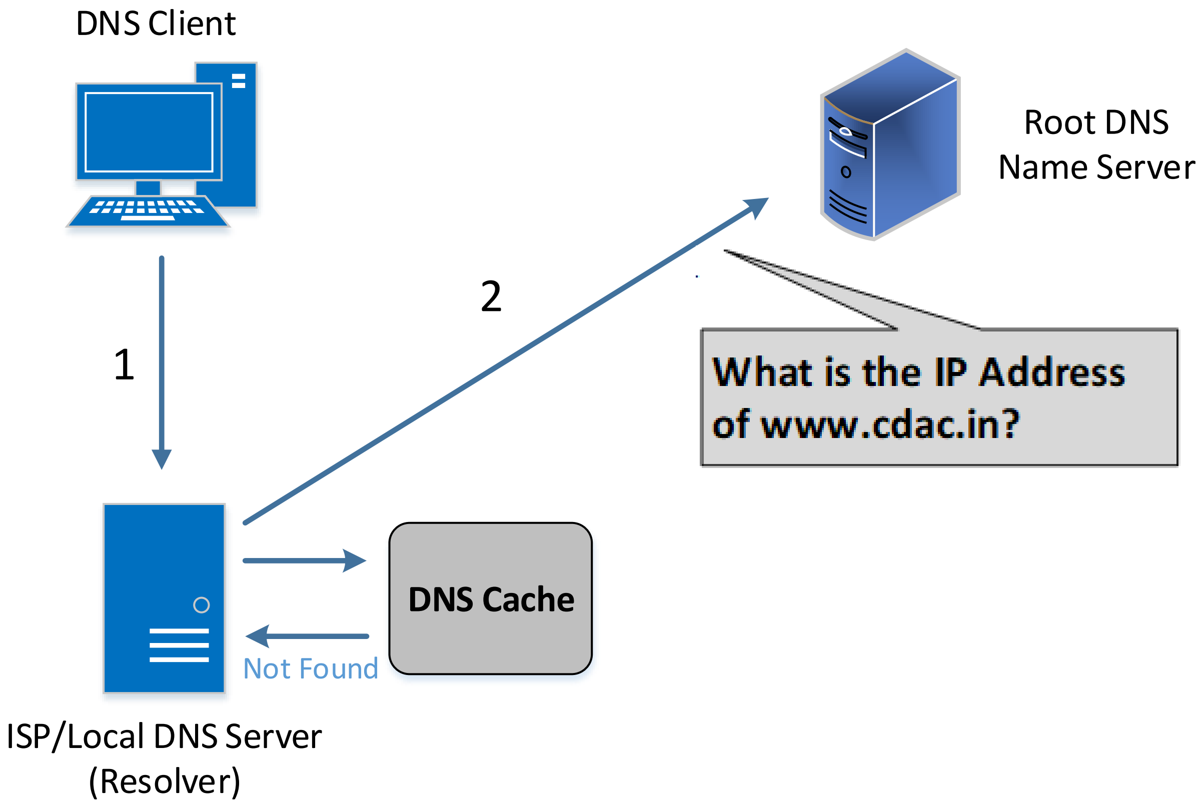
How DNS Works?

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


DNS Client
What is the IP Address of www.cdac.in?
1
DNS Cache
ISP/Local DNS Server (Resolver)

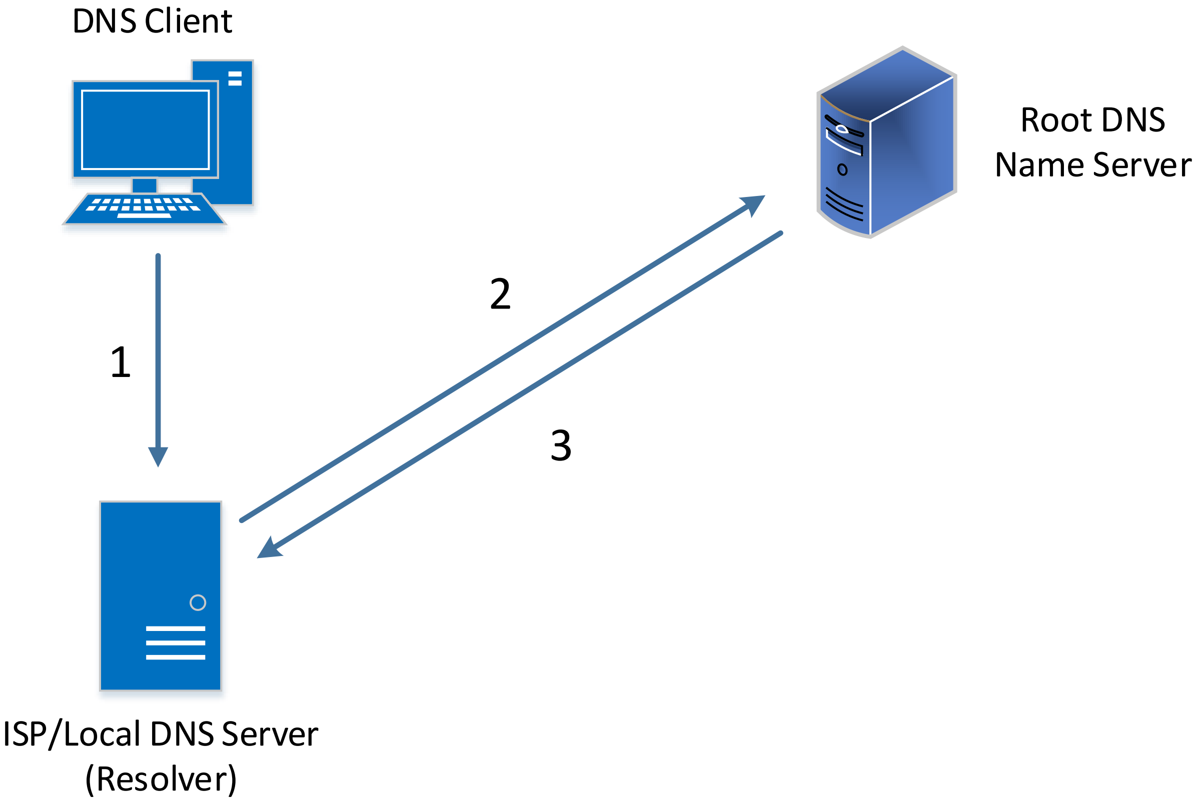
How DNS Works?

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



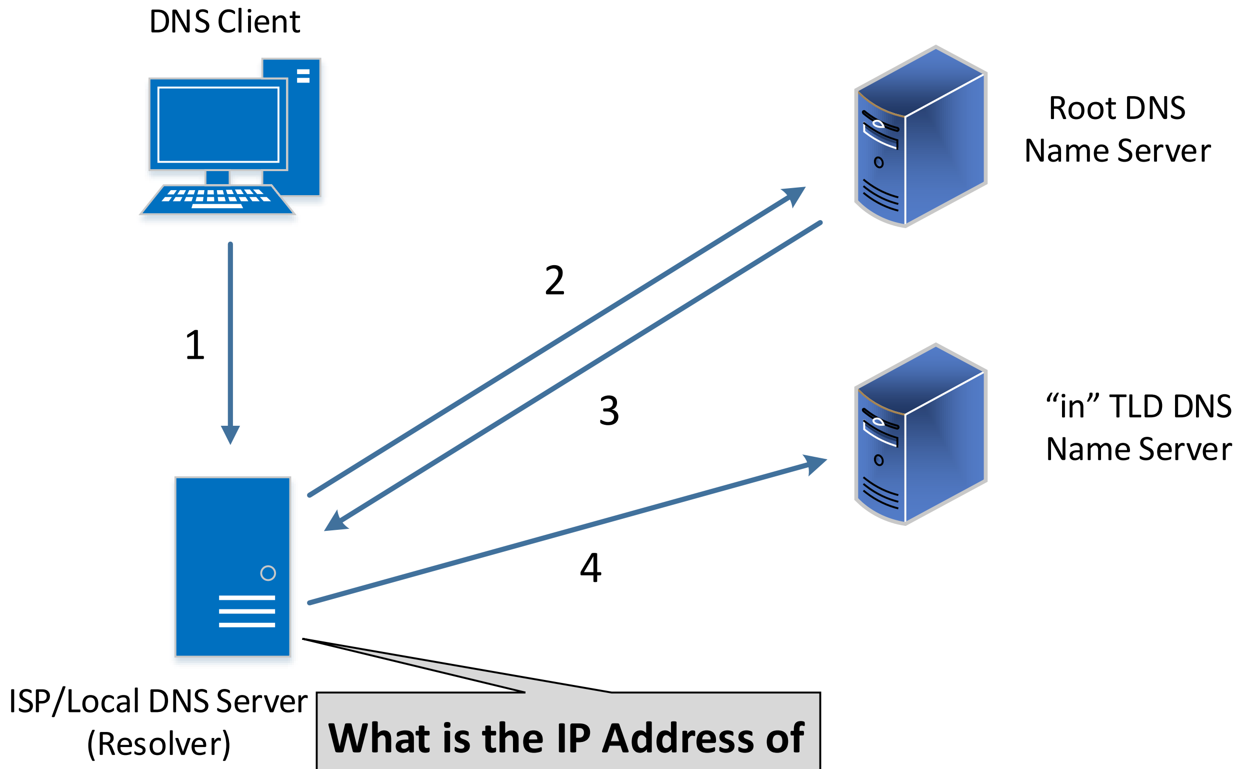
How DNS Works?

3.Root DNS server reply with referral to TLD DNS “in”.



How DNS Works?

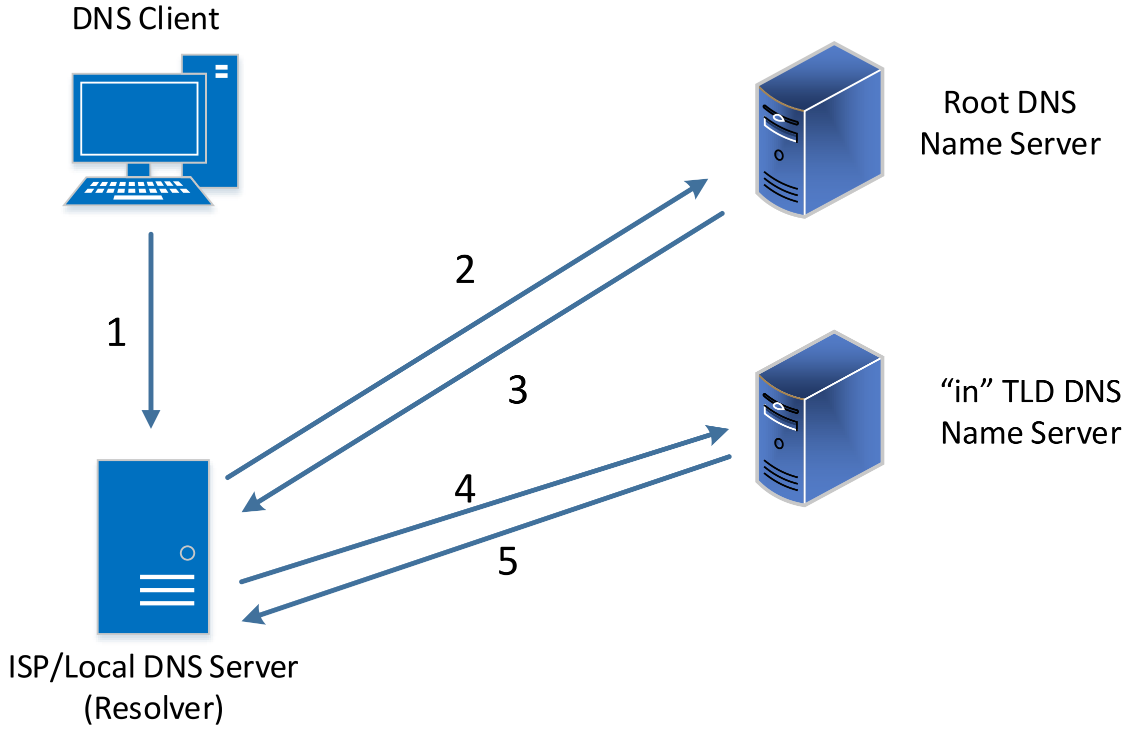
4.ISP/Local DNS Server queries TLD DNS.



What is the IP Address of www.cdac.in?

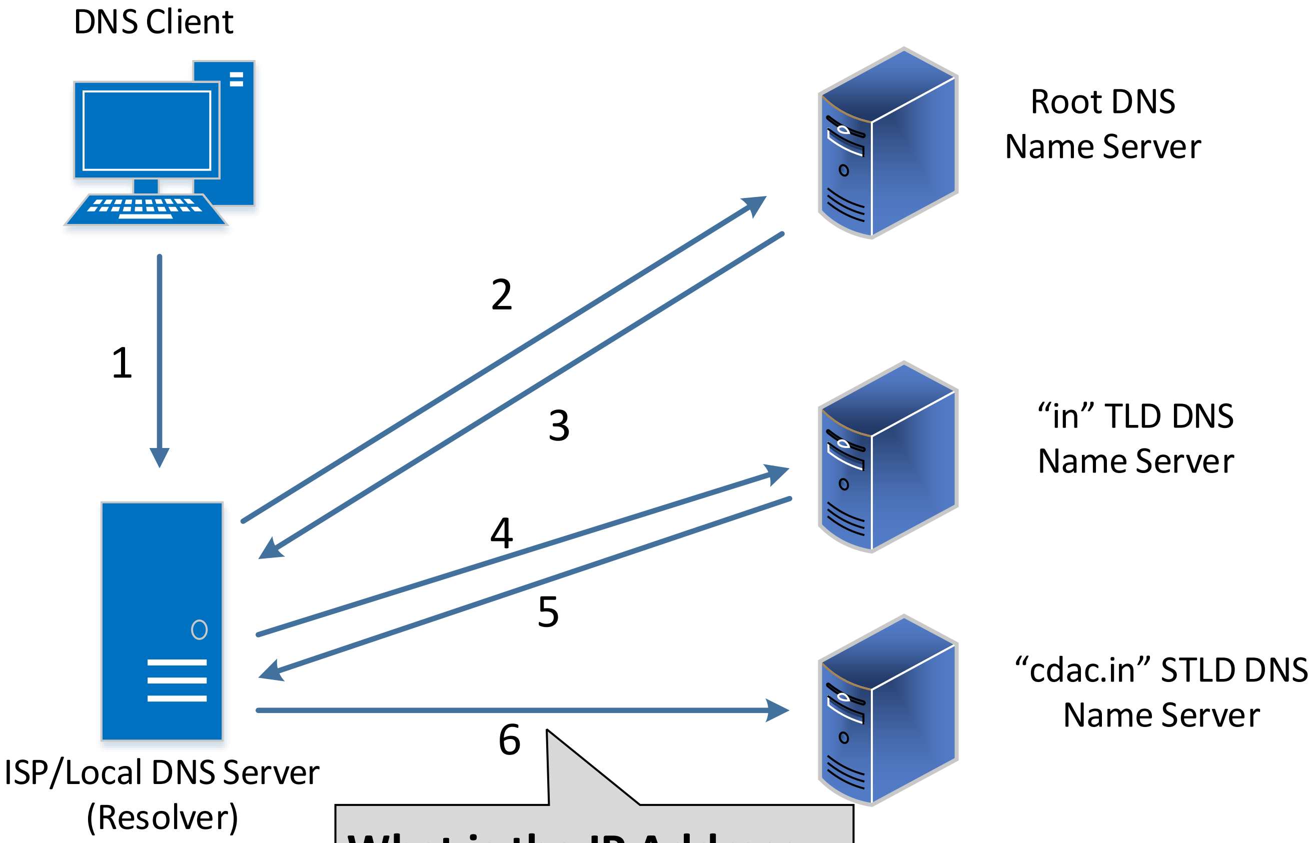
How DNS Works?

5.TLD DNS reply with referral to STLD DNS “cdac.in”.



How DNS Works?

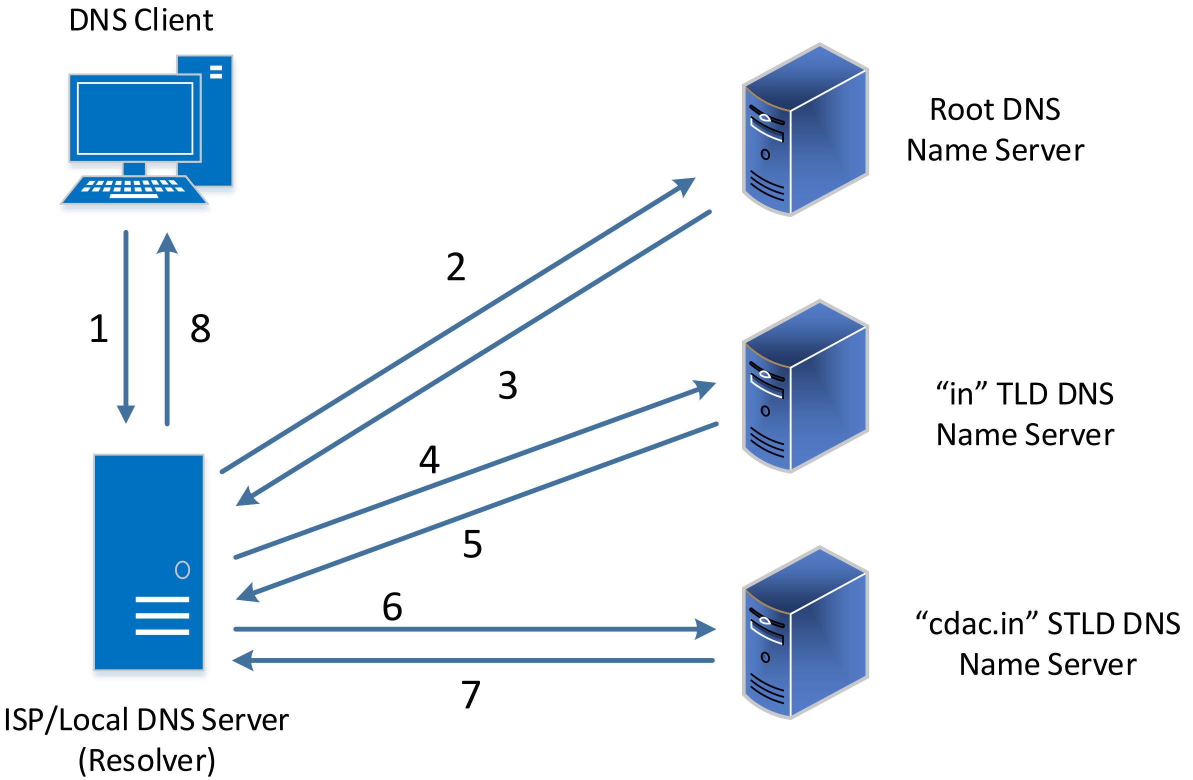
6.ISP/Local DNS Server queries STLD DNS.


DNS Client
Root DNS Name Server
"in" TLD DNS Name Server
"cdac.in" STLD DNS Name Server
1
2
3
4
5
6
ISP/Local DNS Server (Resolver)

What is the IP Address of www.cdac.in?

How DNS Works?

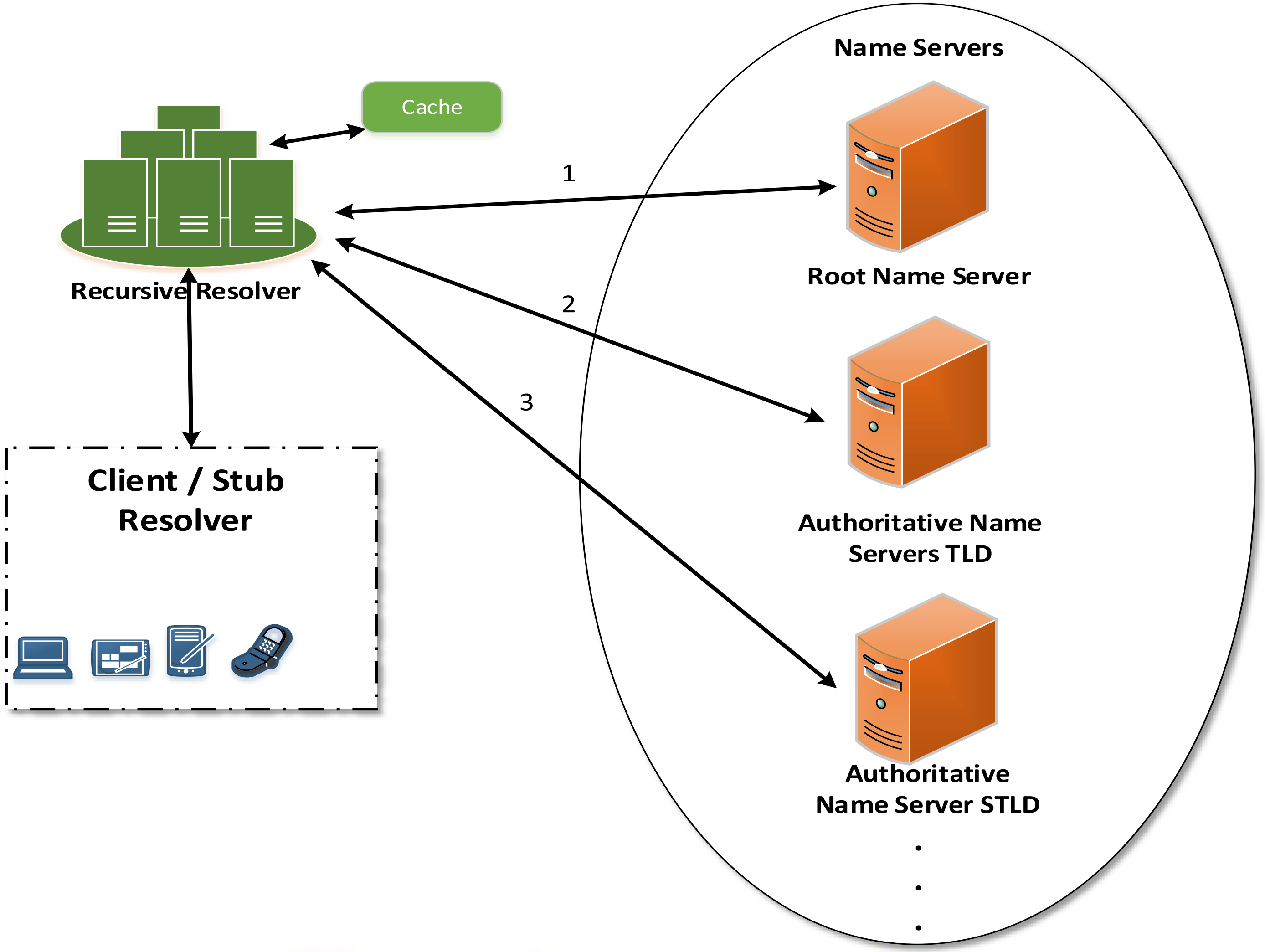
7. ”cdac.in” STLD DNS Server gives the reply - i.e IP address of “www.cdac.in”



Elements of DNS

- Domain Name Space and Resource Records
  - A tree structure name space and data associated with the names
- Name Servers
  - Programs that hold information about the domain’s tree structure
- Resolvers
  - Programs that extract information from name servers to respond to client’s requests.

DNS Ecosystem



Stub Resolver

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

Authoritative Name Server

- They 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 Configurations are maintained to increase availability

Recursive Resolver

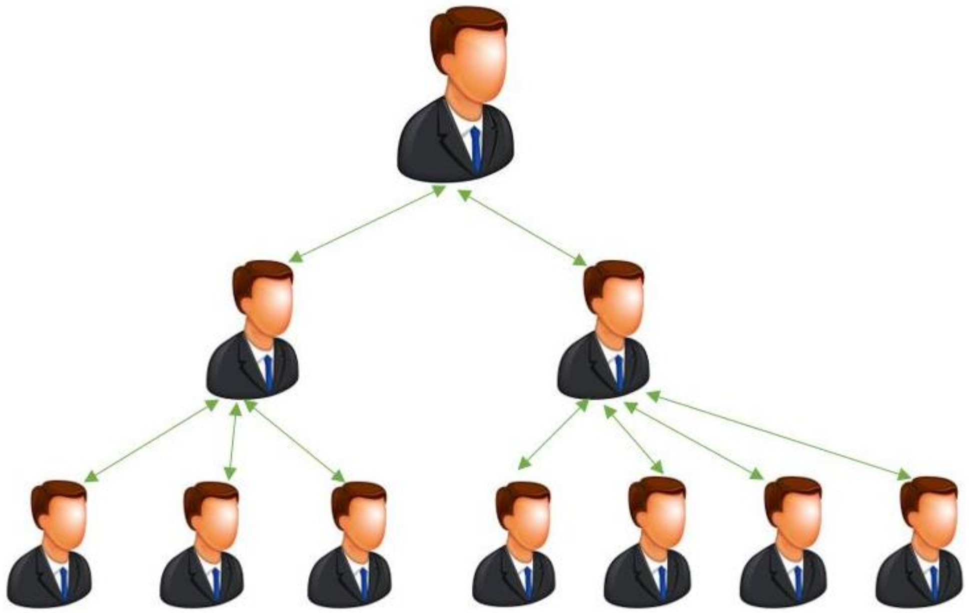
- Also called as recursive DNS Server.
- The user queries to RR for domain lookup.
- RR queries the entire DNS Hierarchy for the final result.
- RR can also be Authoritative for some domains

DNS Server Types

- Root DNS Server
    - Root Servers(A to M)
    - Instances
- Authoritative DNS Server
    - Master
    - Slave
- Recursive DNS Server
- Stub Resolver

DNS Centralized or Decentralized ?

- Centralized or Decentralized ??



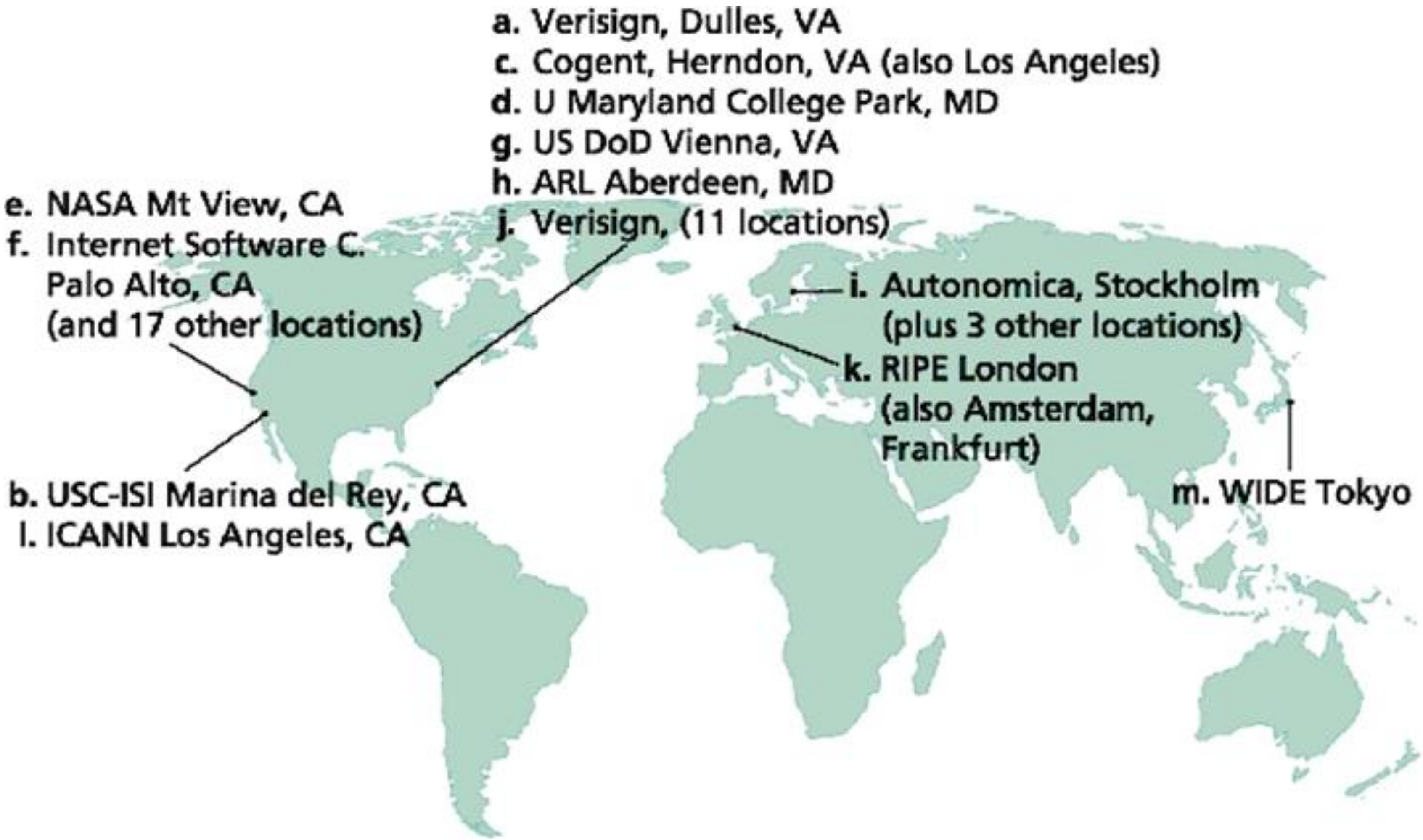
DNS Root Server

- 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, named A to M, maintained by 12 independent organisations.
    - Each root server is a copy and none of them are special.
    - There are several **instances** (997 as of Jul 2019) 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

Why 13 root servers?

- Historic Reasons
  - In IPv4, routers tend to fragment packets if the next receiver cannot receive a packet beyond a certain size
    - All IP protocol implementations should minimally support packet size of 576 bytes (including 20 byte header)
    - So if a packet is of <= 576 bytes, it can be transmitted without fragmentation
    - Even if it were part of a large packet, and fragmented, it can always be reassembled, as the size of the DNS packet is fixed at 512 bytes (in the first RFC of DNS).
    - Initially all the root servers did not have commonality in their names, varying from 15 bytes to 31 bytes; - 'NS' record;
    - 'A' record – the address record includes the root server operator also, and can be represented by 16 bytes;
    - 14 name servers could have fit in; However it was decided to stick with 13, to allow room for future expansions and to add 'options'

Root Name Servers



Root Name Server Operators

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Root Server instances in India (15)

Delhi (3)
J, K , F

Mumbai (7)
D, E, F, I, J, K, L

Kolkata (2)
J, L

Bengaluru (1)
J

Chennai (2)
E, F

Maintainer: NIXI – 3 (I-MUM, K-DEL, F- CHN), Verisign – J

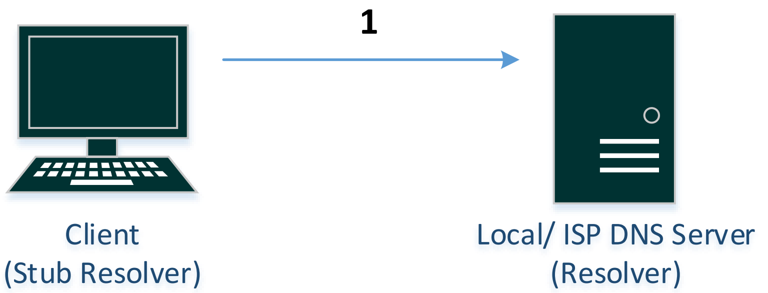
DNS Record Types

- A Record
  - Maps a FQDN to an IP address; Most often used record type
- NS Record
  - Indicate which name servers are authoritative for the Zone / domain
- TXT Record
  - Type of Resource Record;
  - Associates arbitrary text with a host
  - Typically used for verification and email validation
- MX Record
  - Used by Mailservers to determine where to deliver email
  - Used in conjunction with 'A' record;
  - Should point to the mail server, (should point to the 'A' record, which will give the IP address; and should not directly give the IP address);
- PTR Record
  - Resolves an IP address to a domain or host name
  - Should be separately configured and hosted

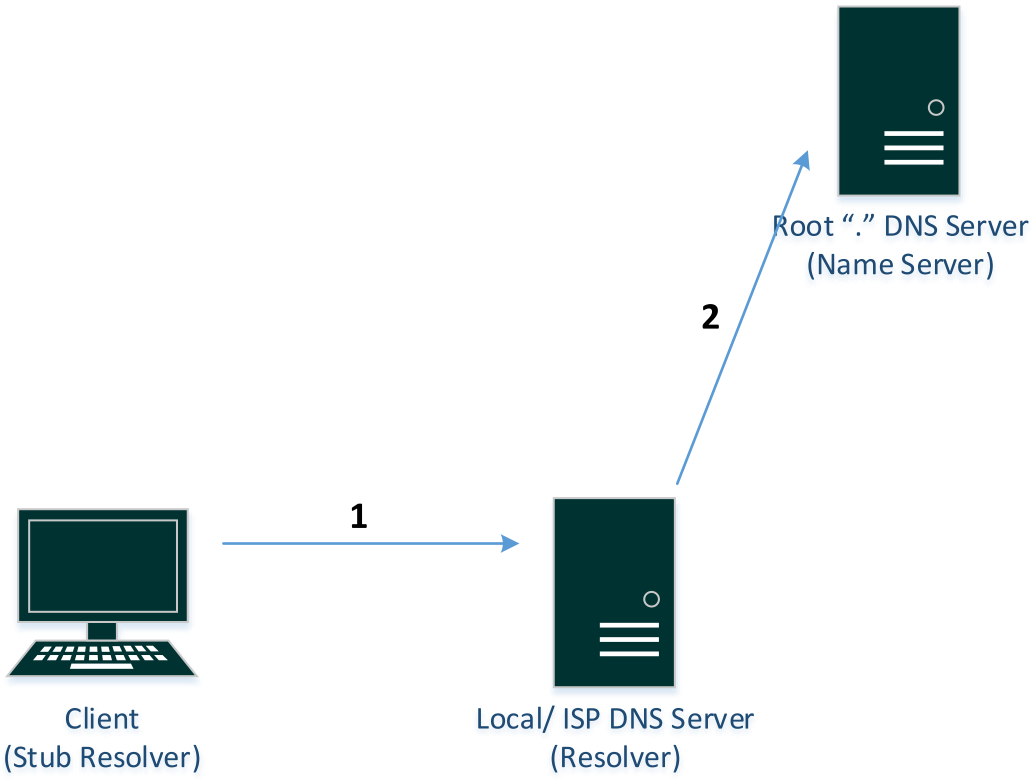
DNS Query Types

- Recursive Query
- Iterative Query
- Inverse (Reverse) Query

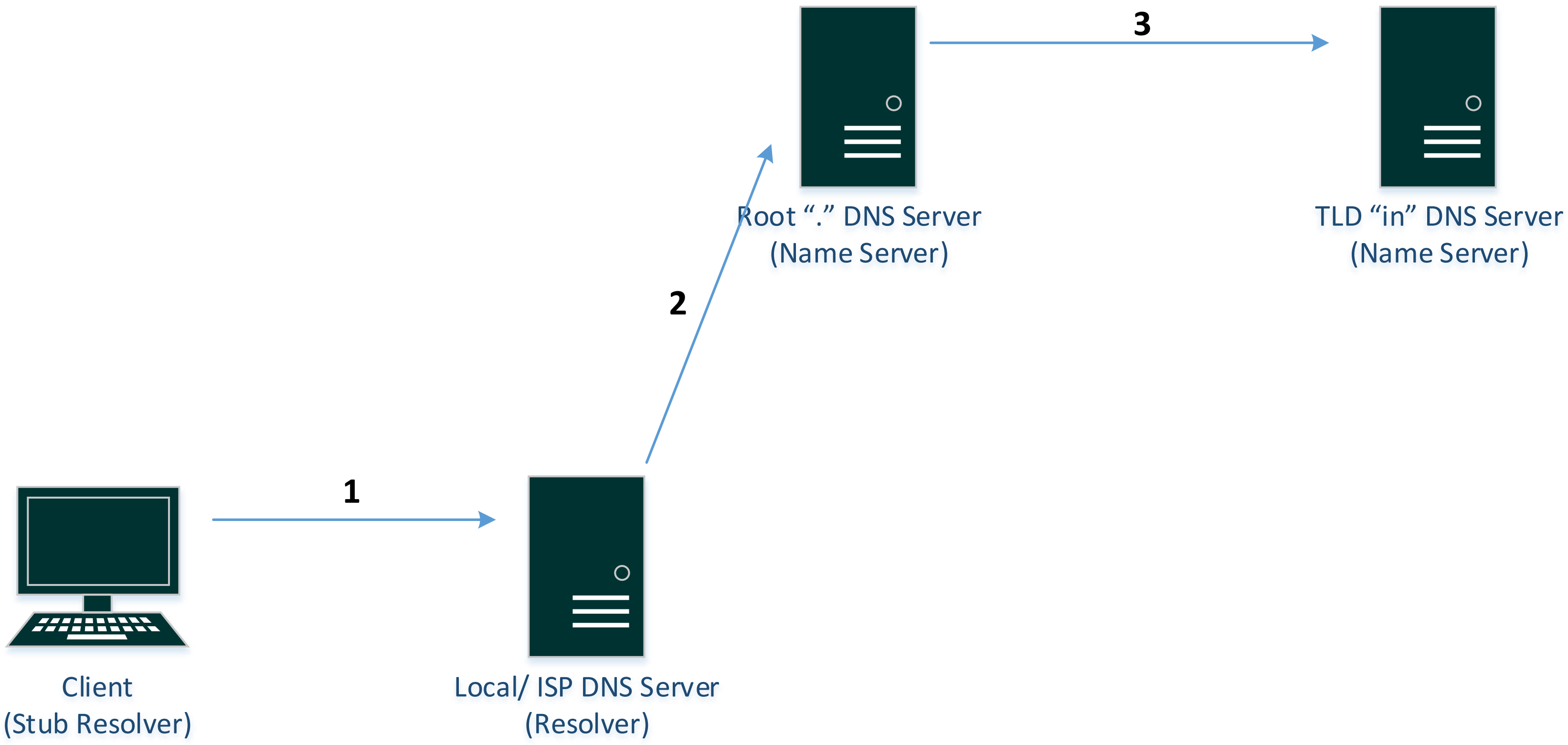
Recursive Query - Illustration



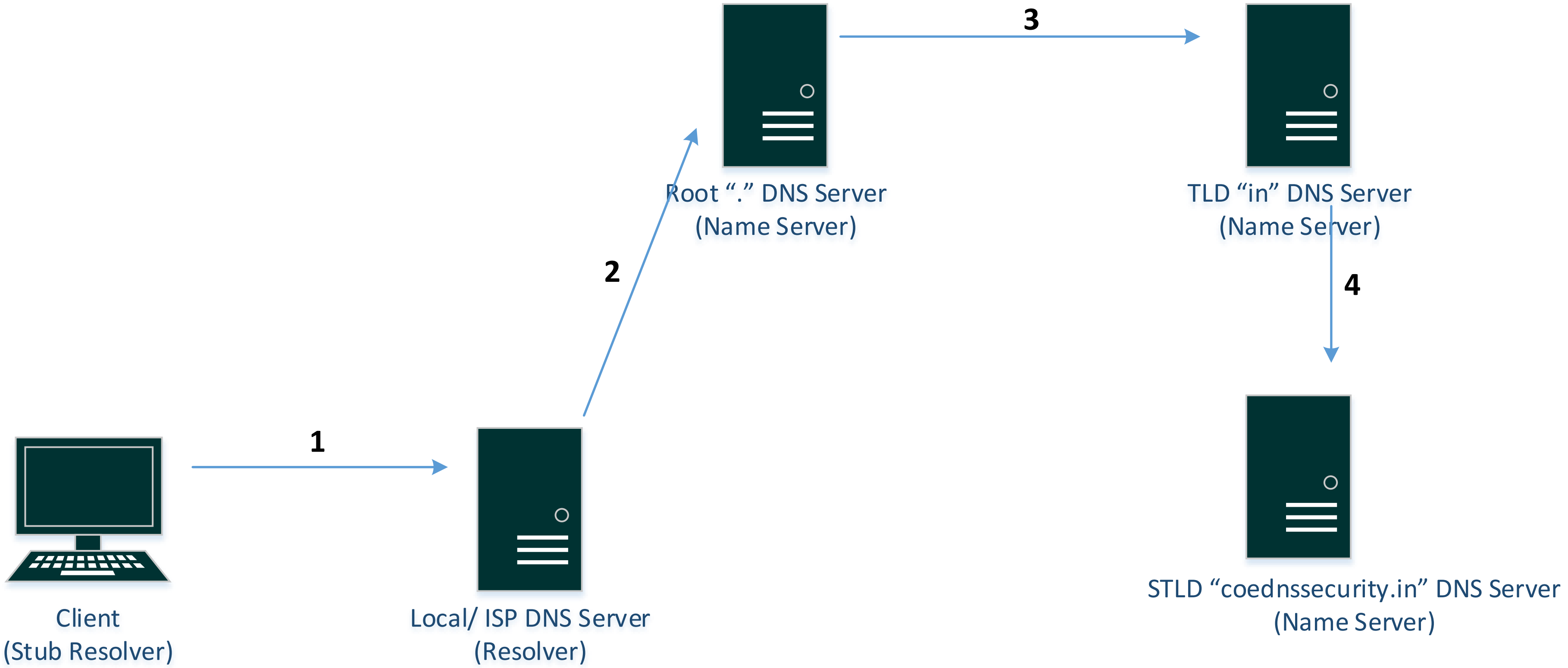
Recursive Query



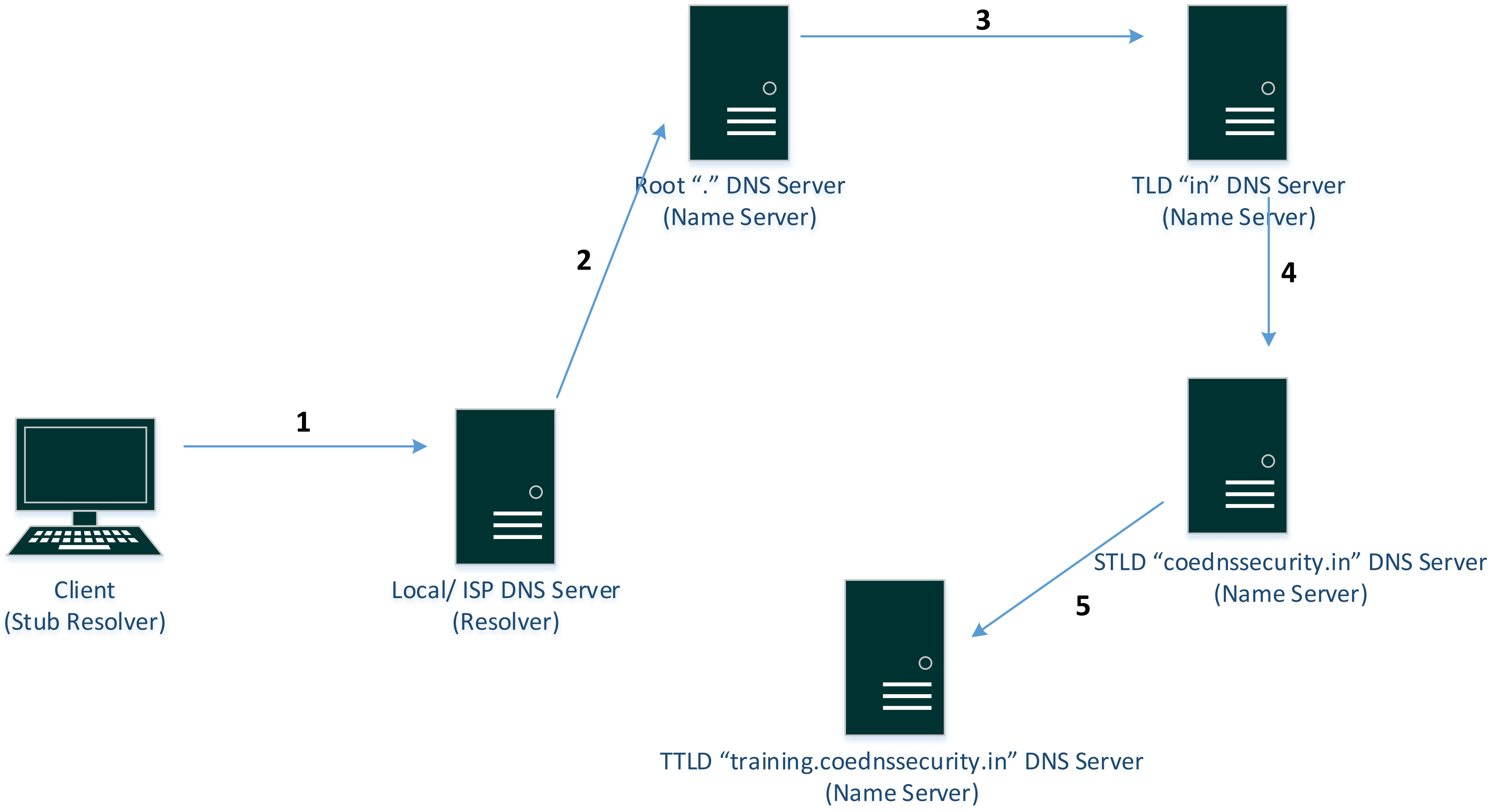
Recursive Query



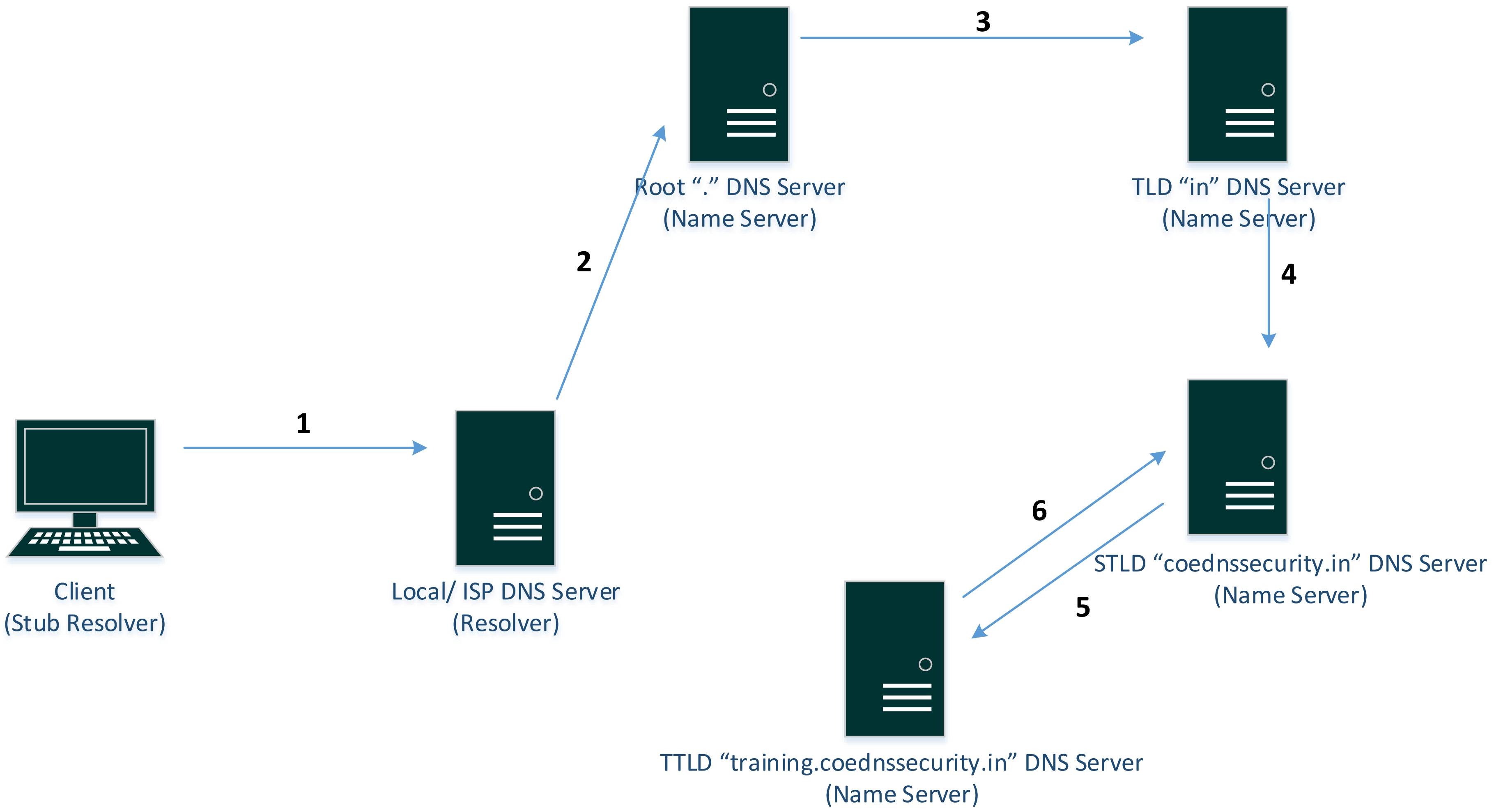
Recursive Query



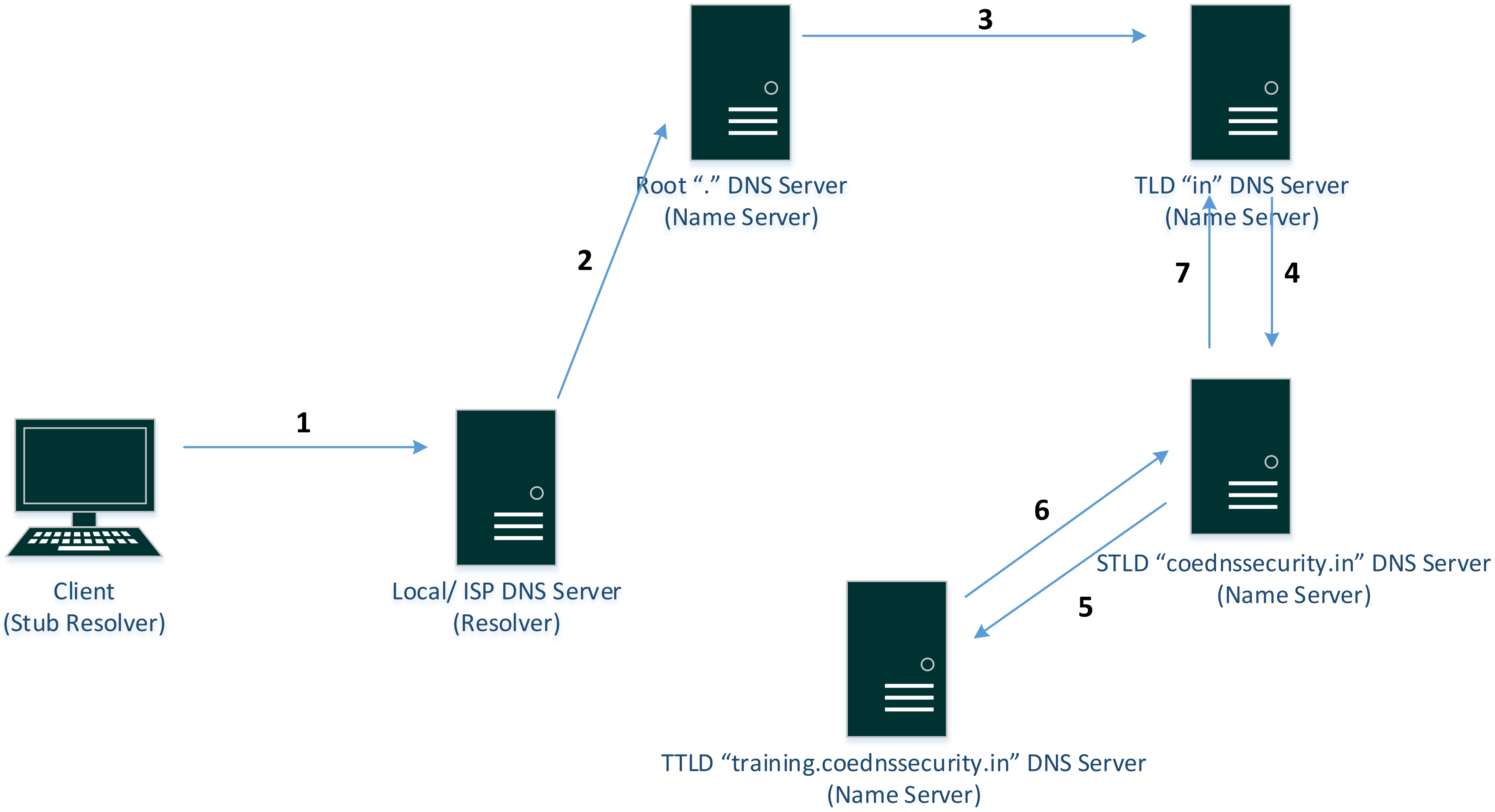
Recursive Query



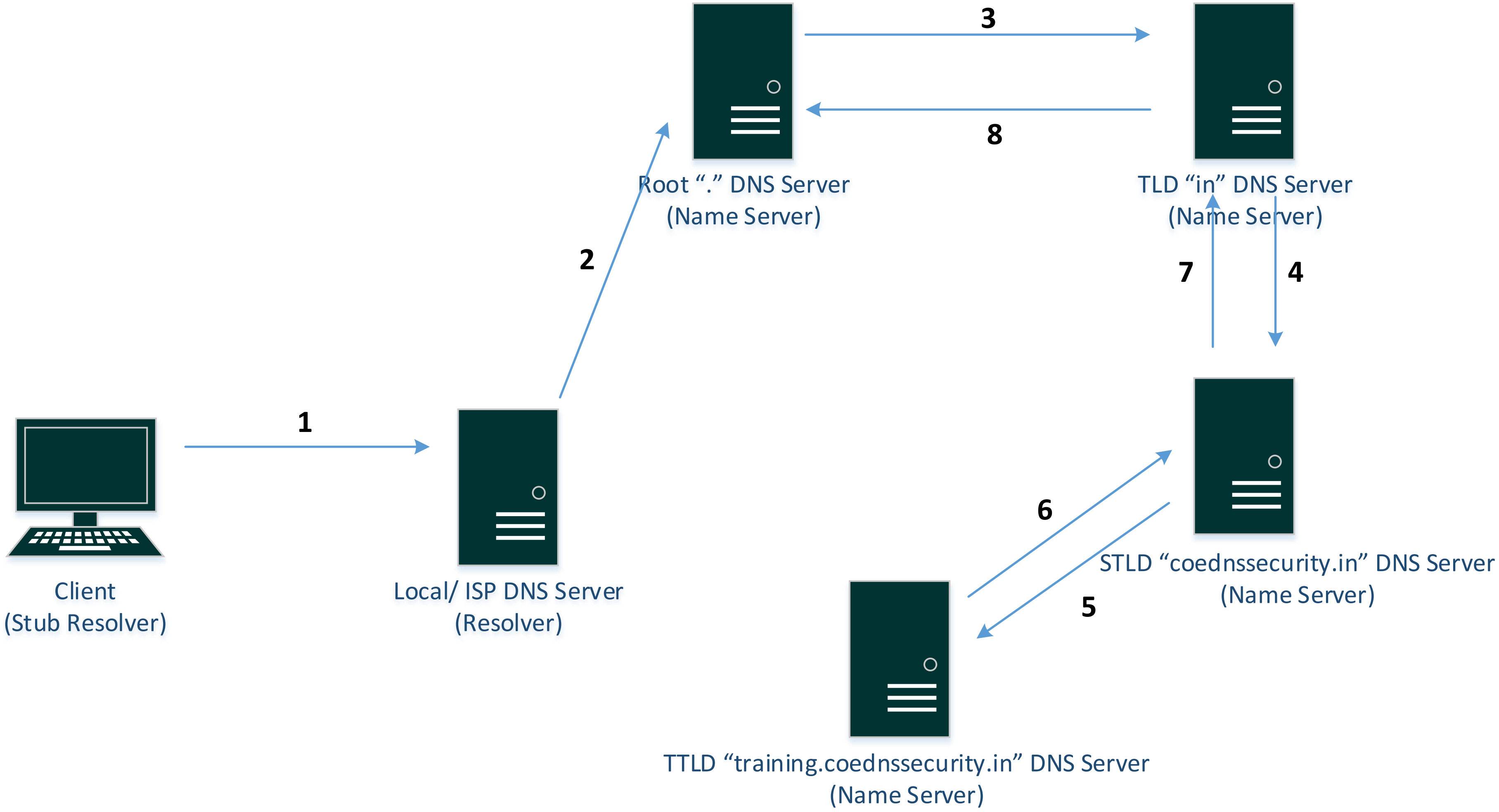
Recursive Query



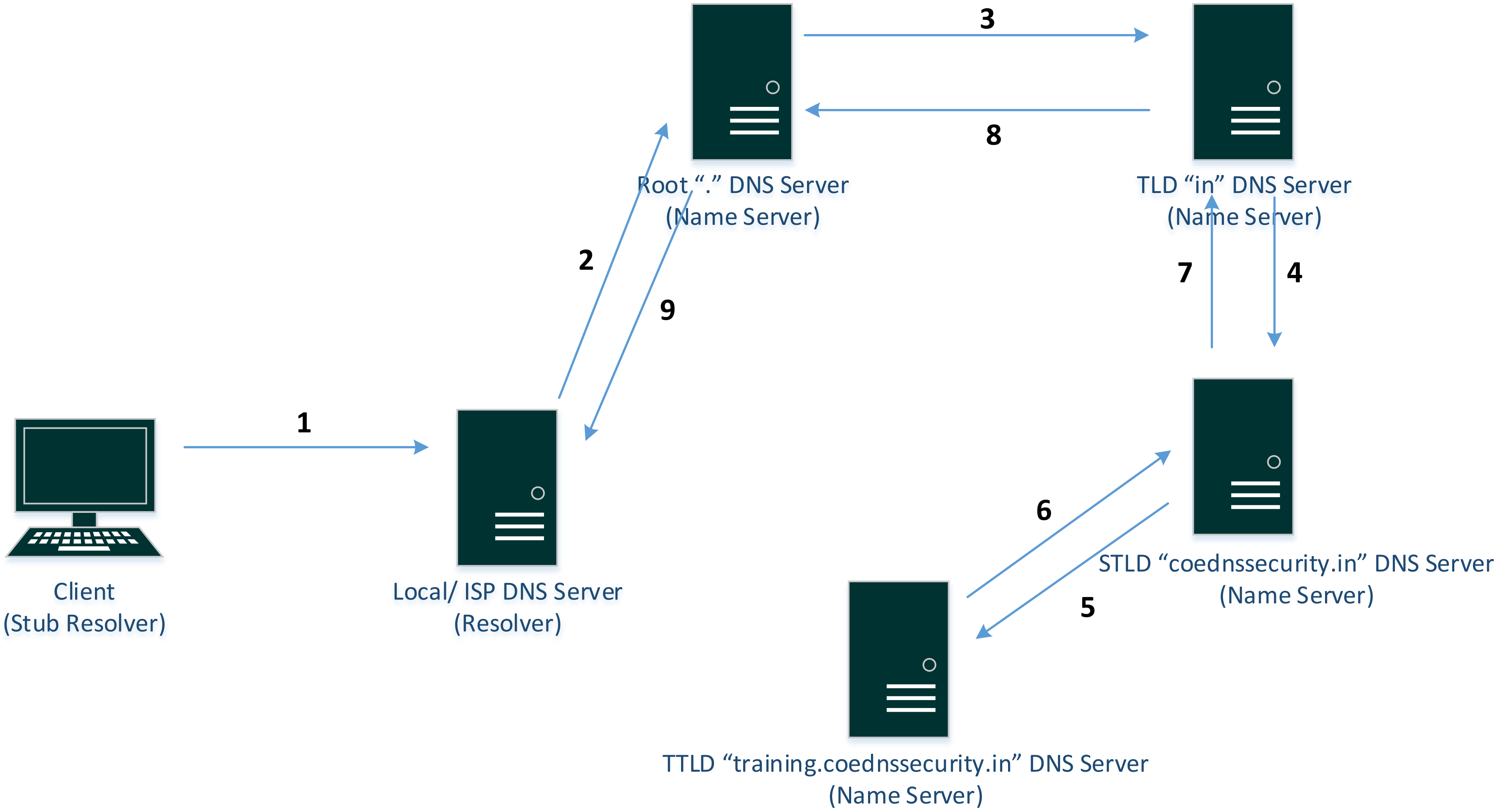
Recursive Query



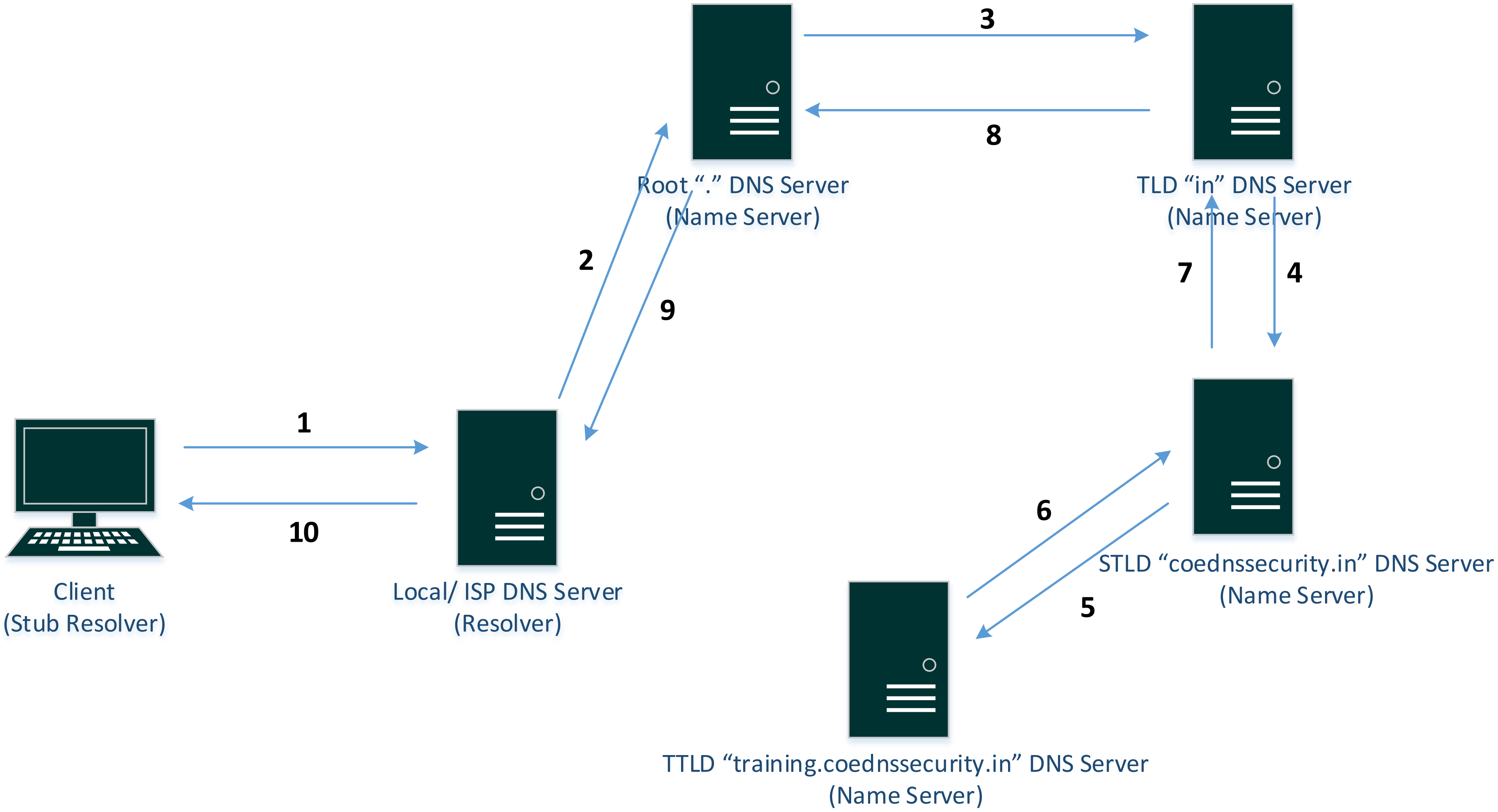
Recursive Query



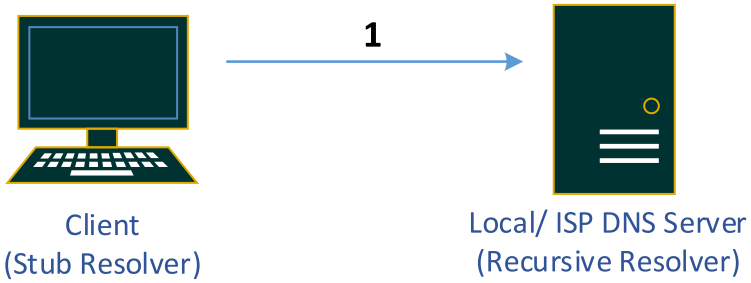
Recursive Query



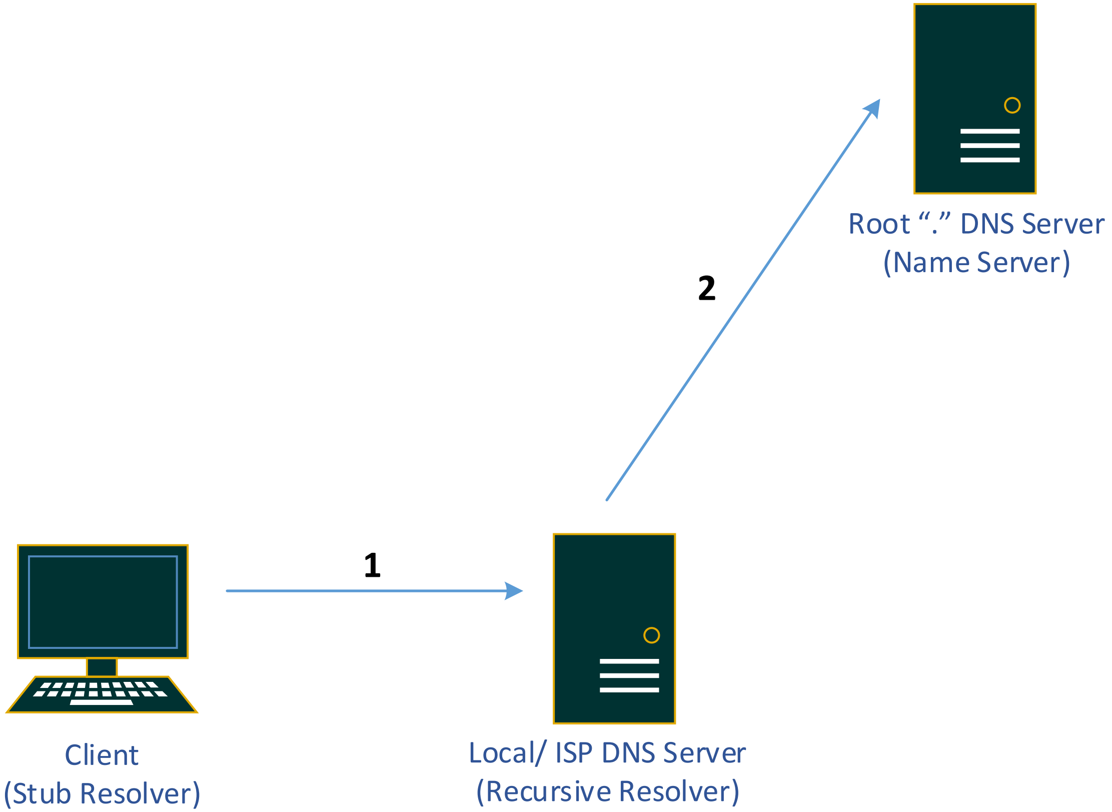
Recursive Query



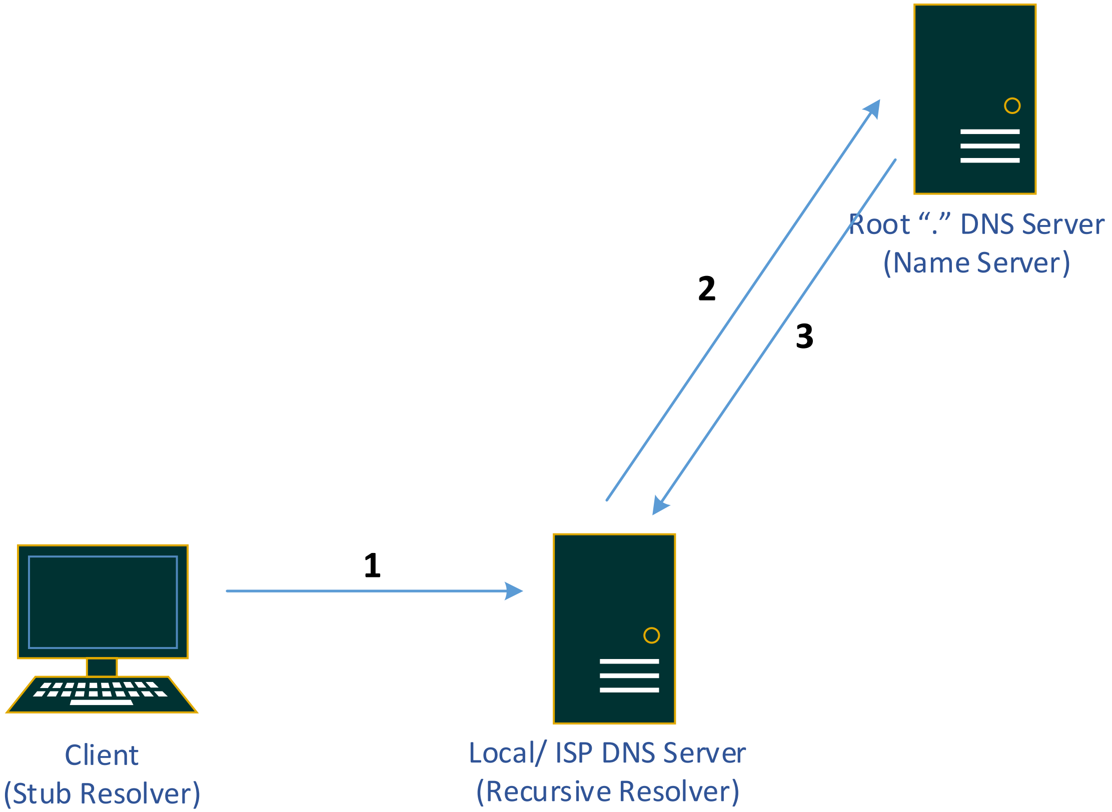
Iterative Query



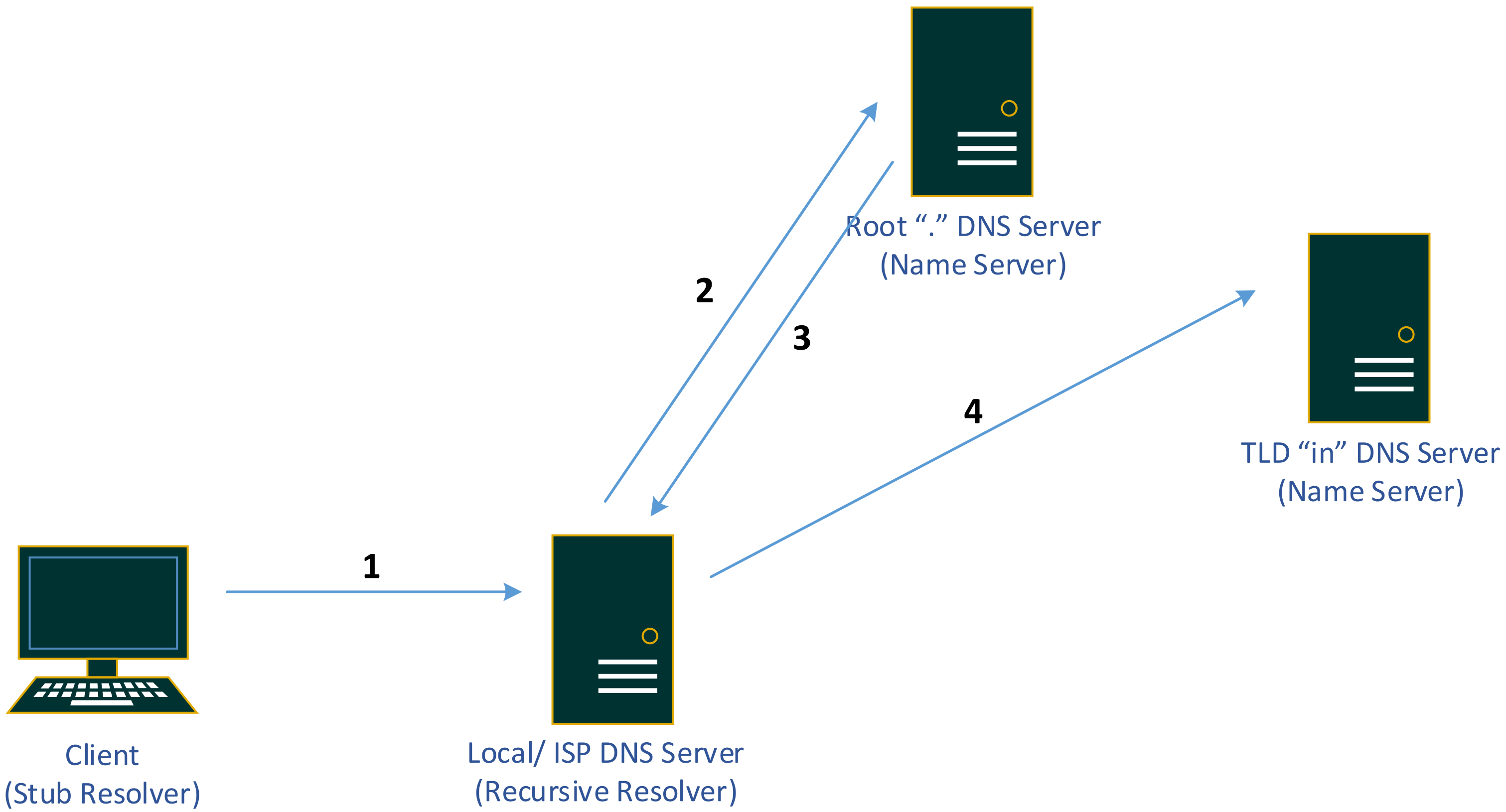
Iterative Query



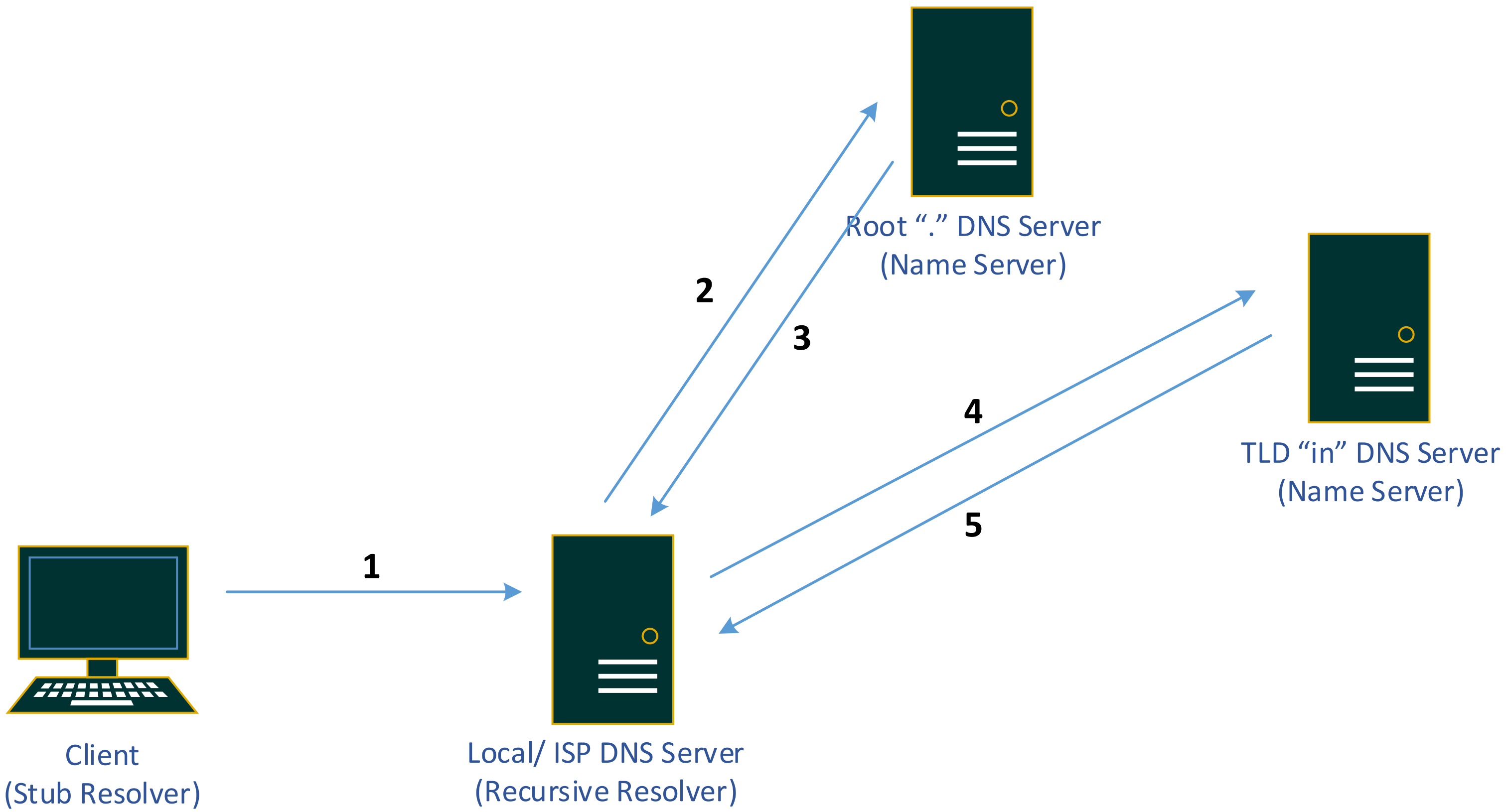
Iterative Query



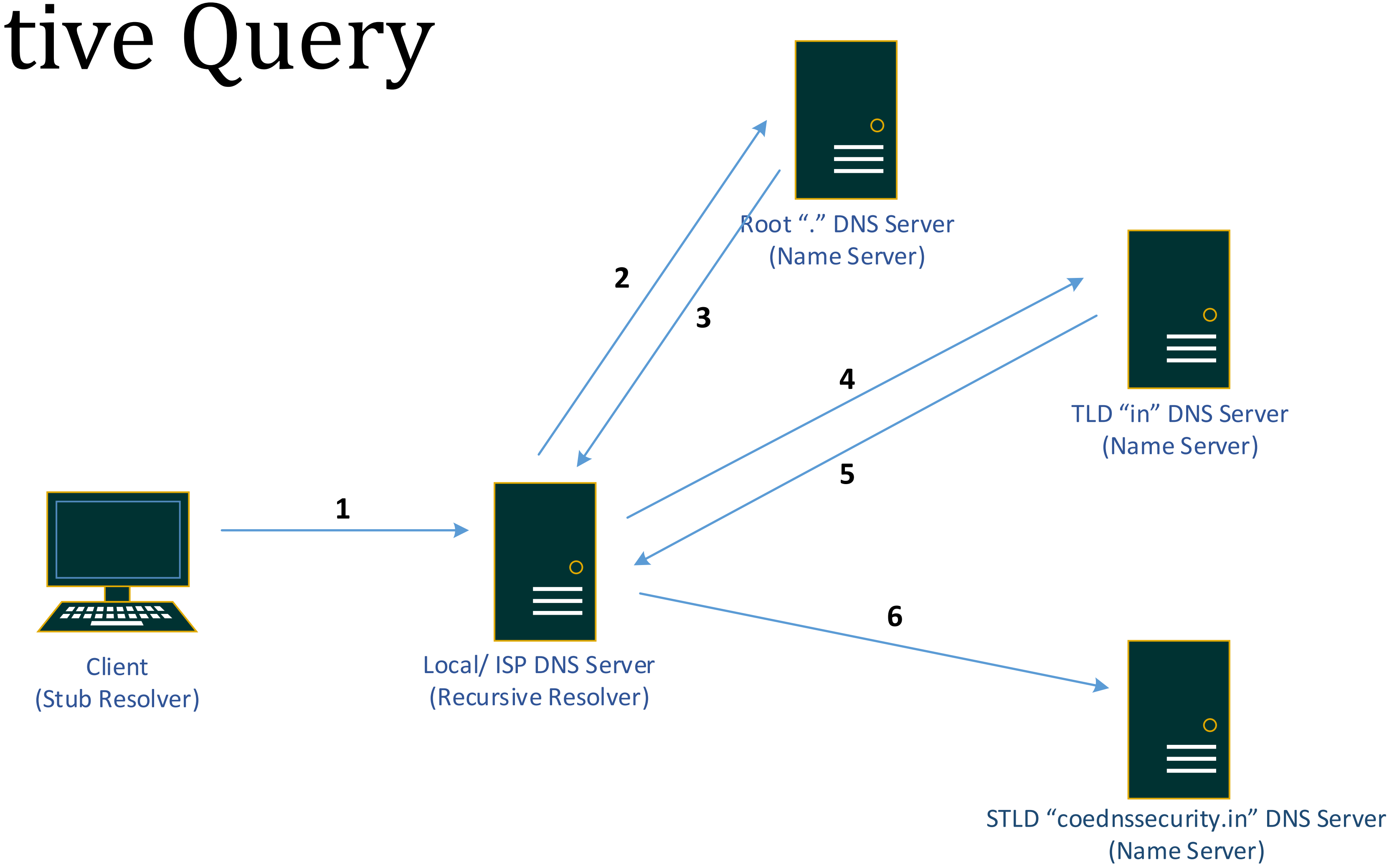
Iterative Query



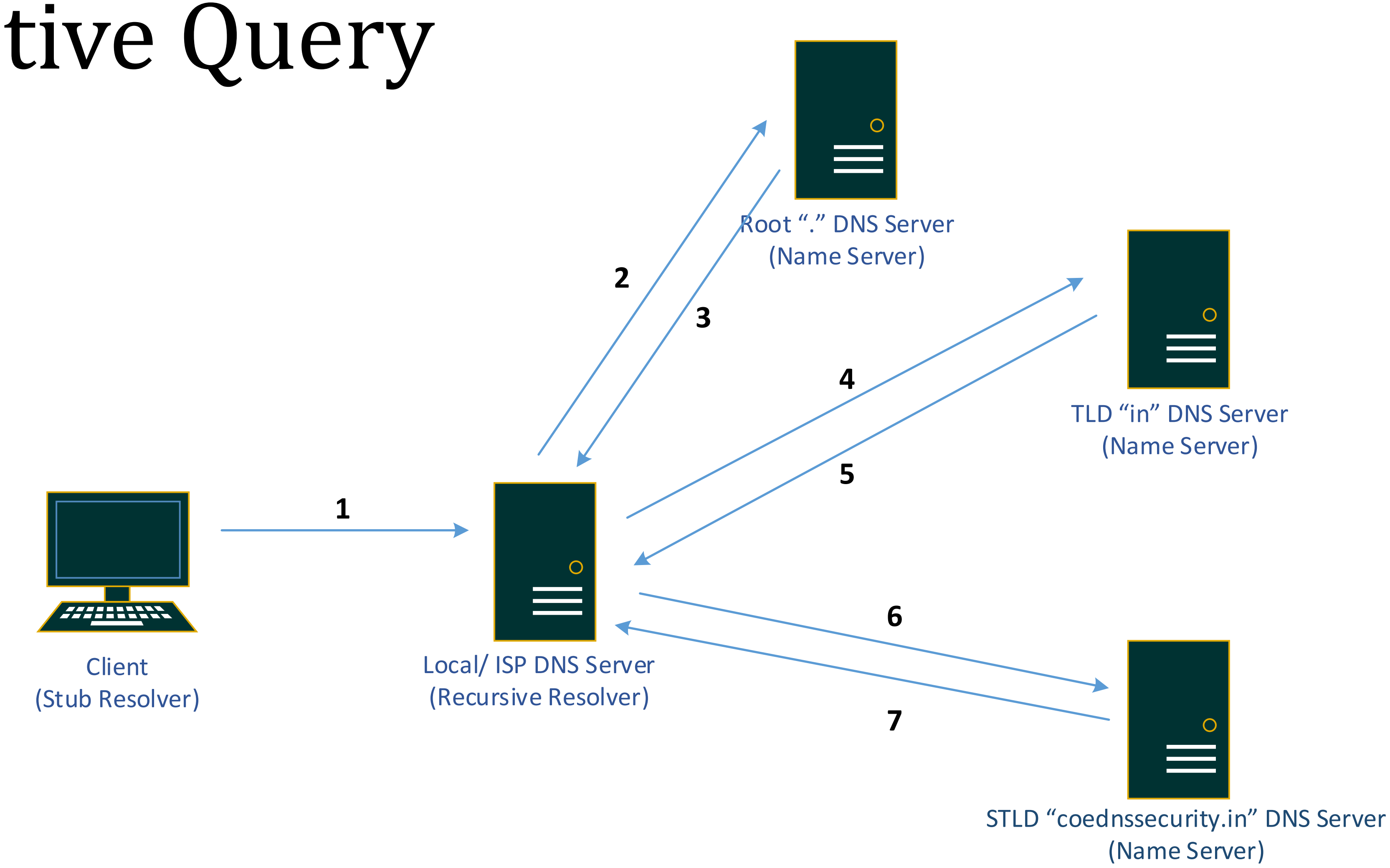
Iterative Query



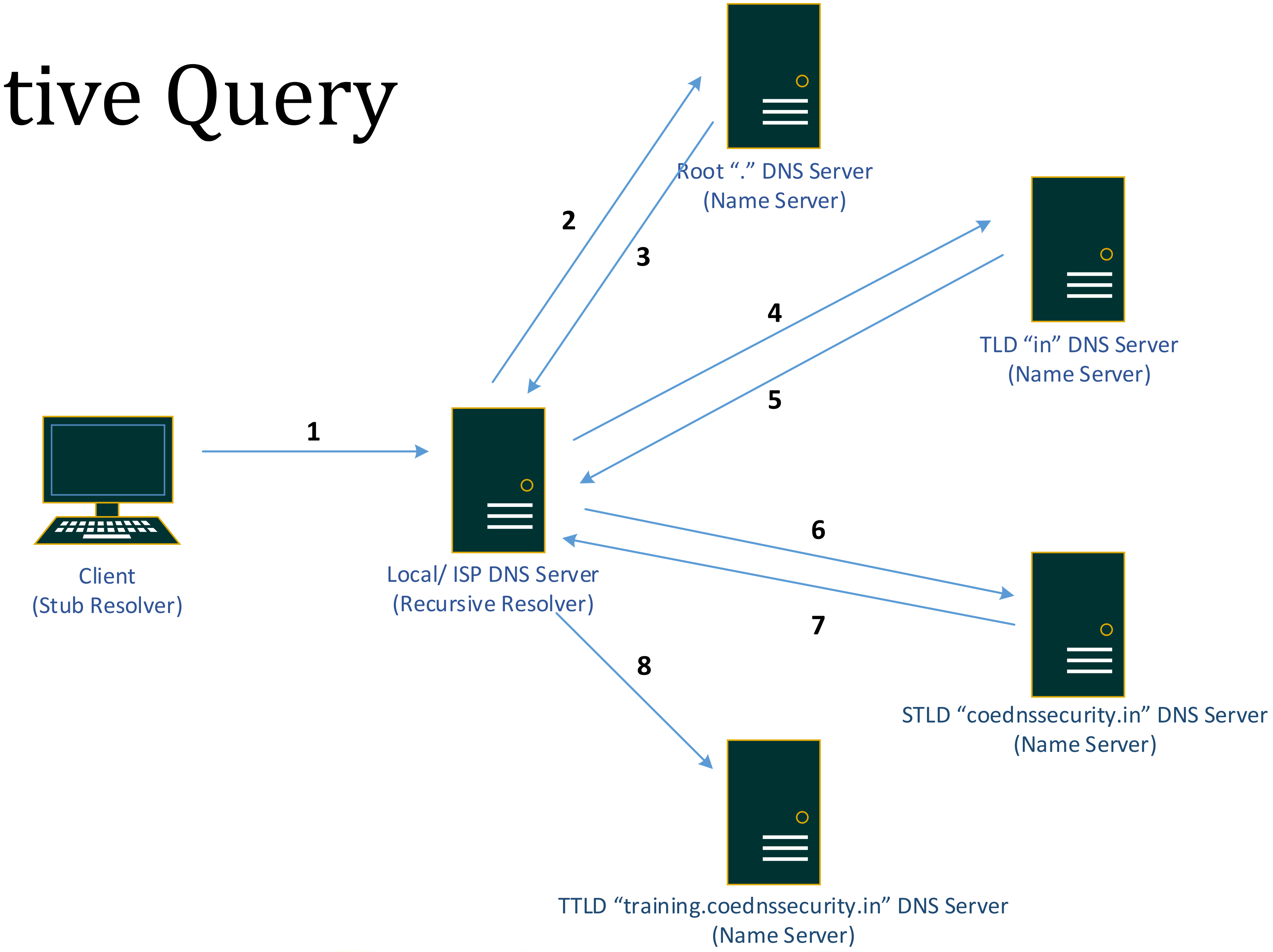
Iterative Query



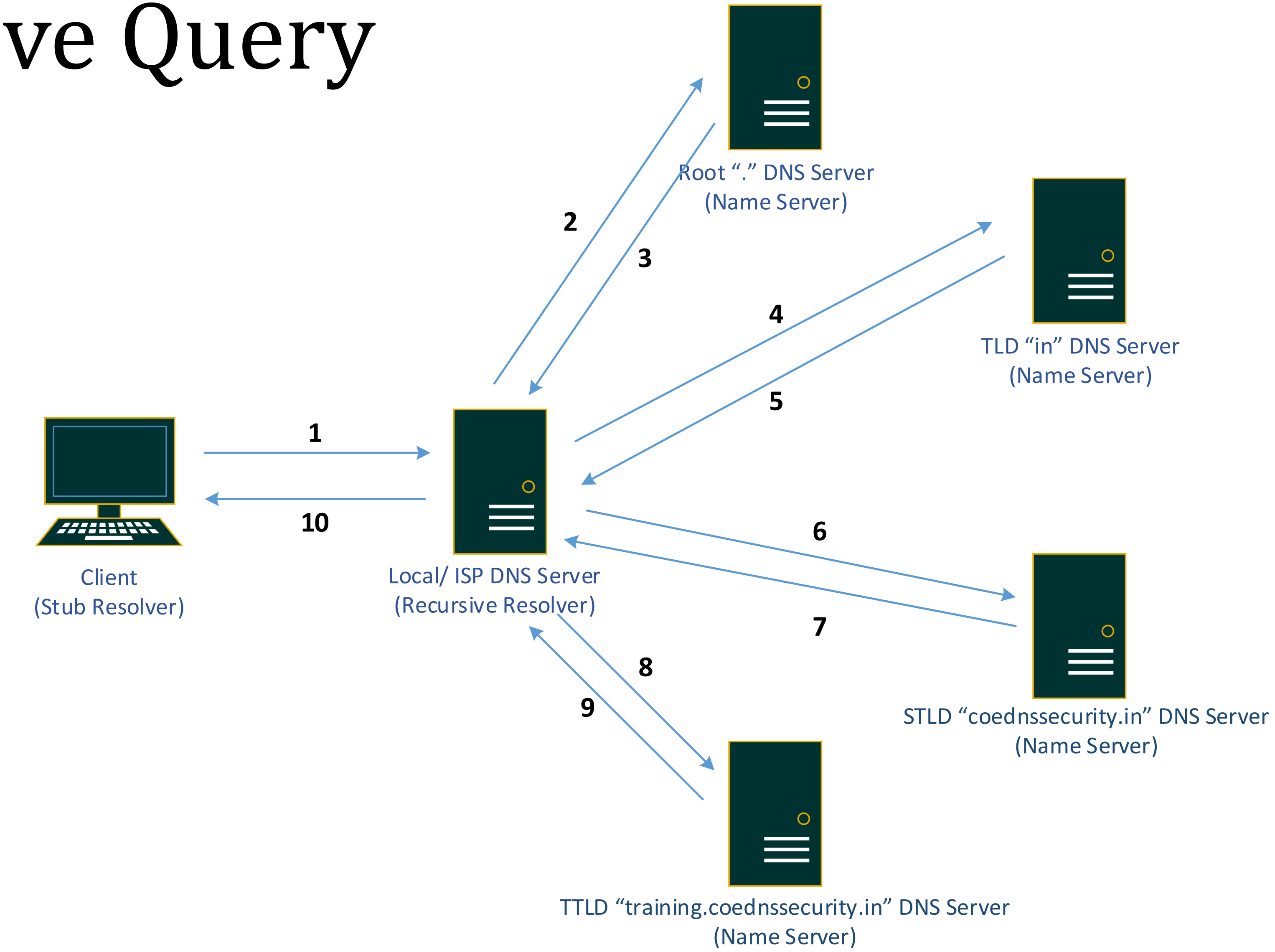
Iterative Query



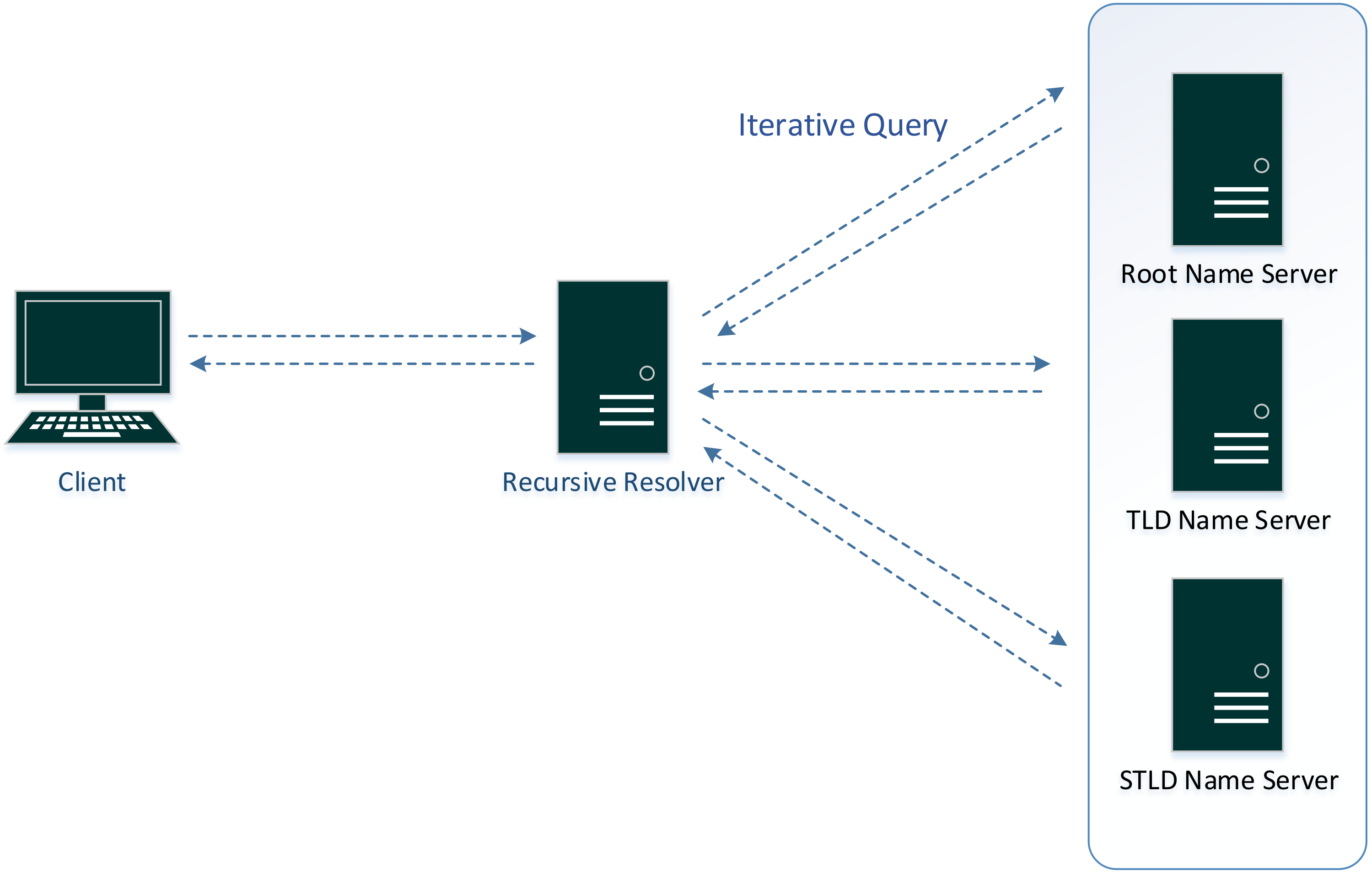
Iterative Query



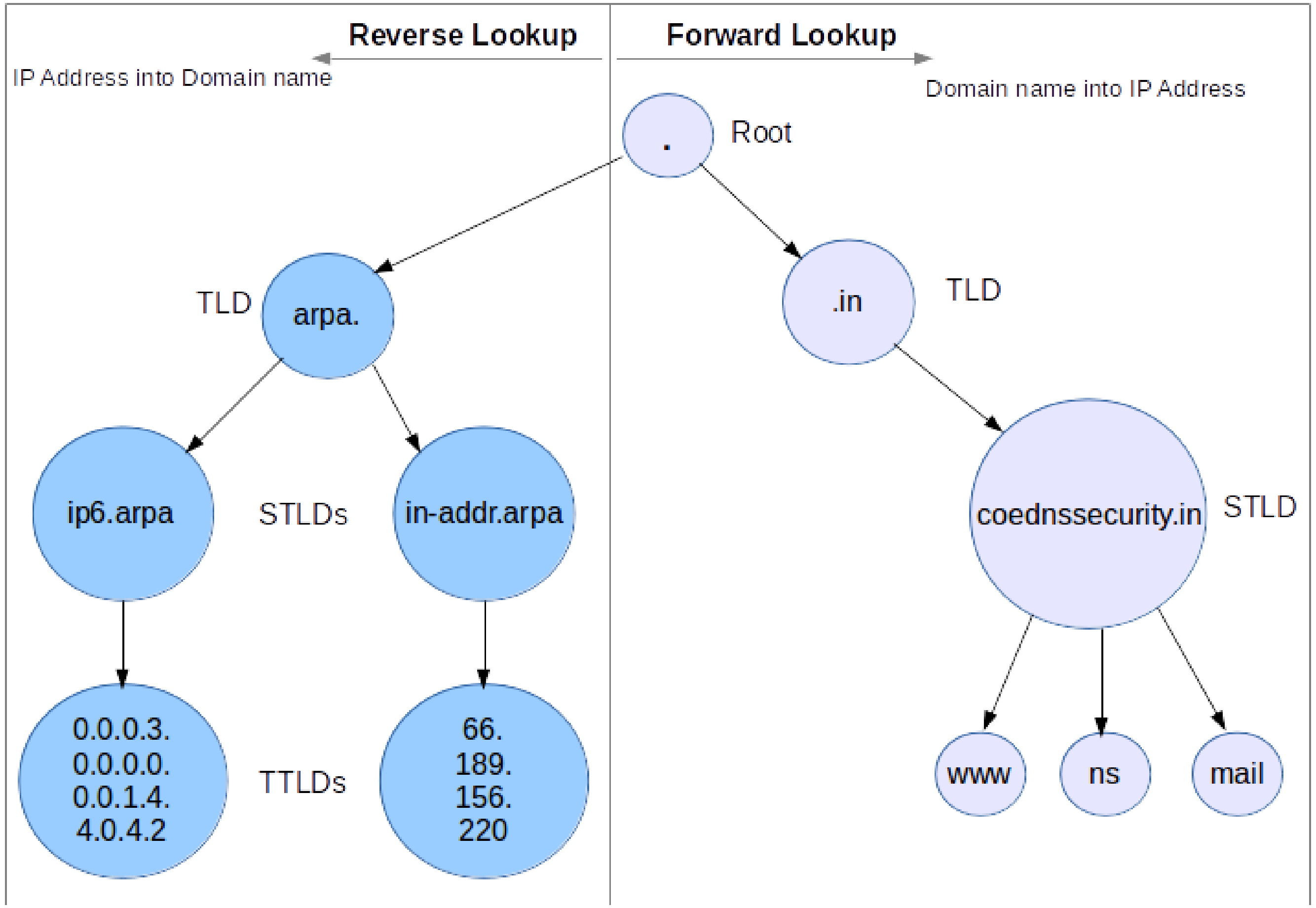
Iterative Query



In Reality ...


Iterative Query
Client
Recursive Resolver
Root Name Server
TLD Name Server
STLD Name Server

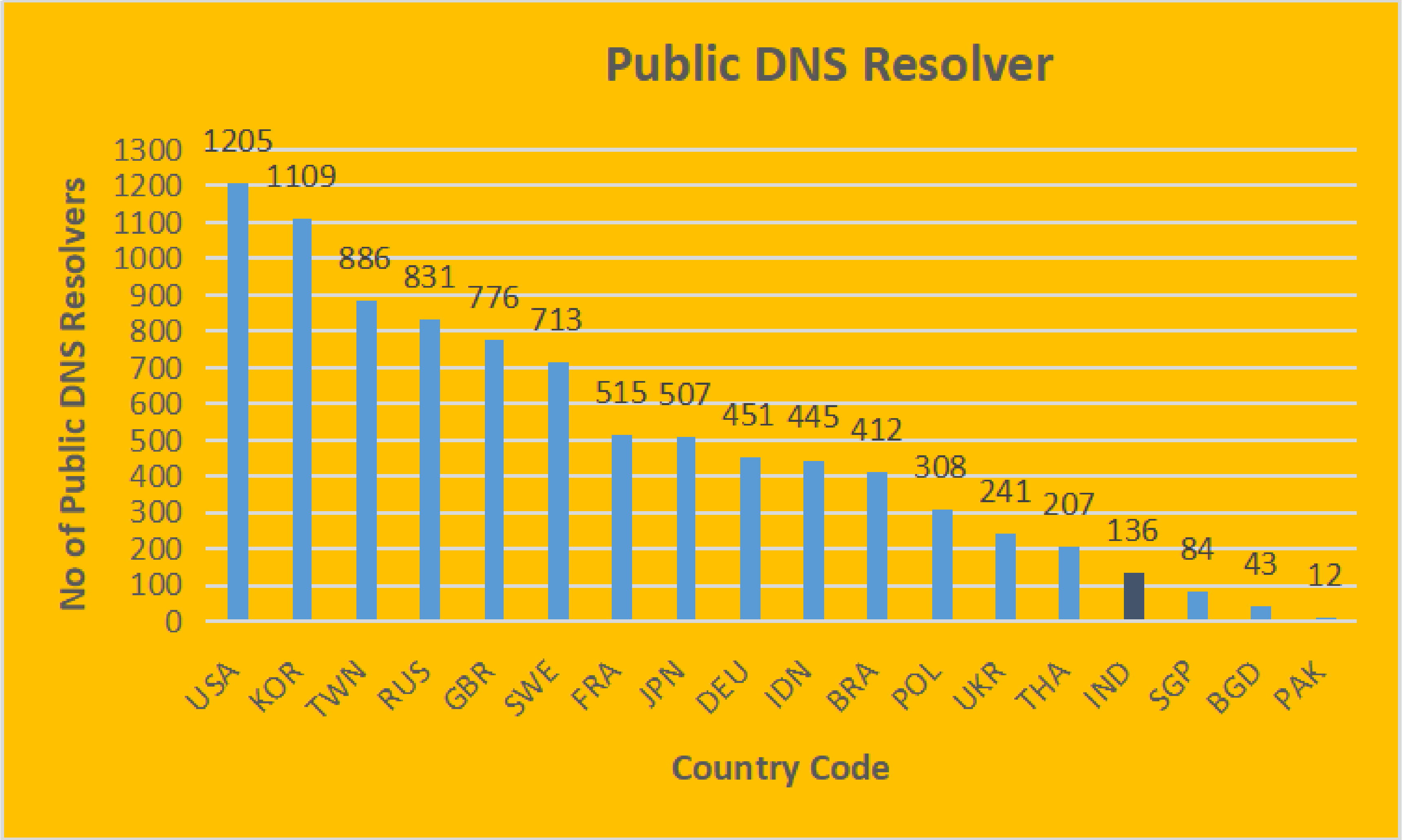
Forward and Reverse Lookup



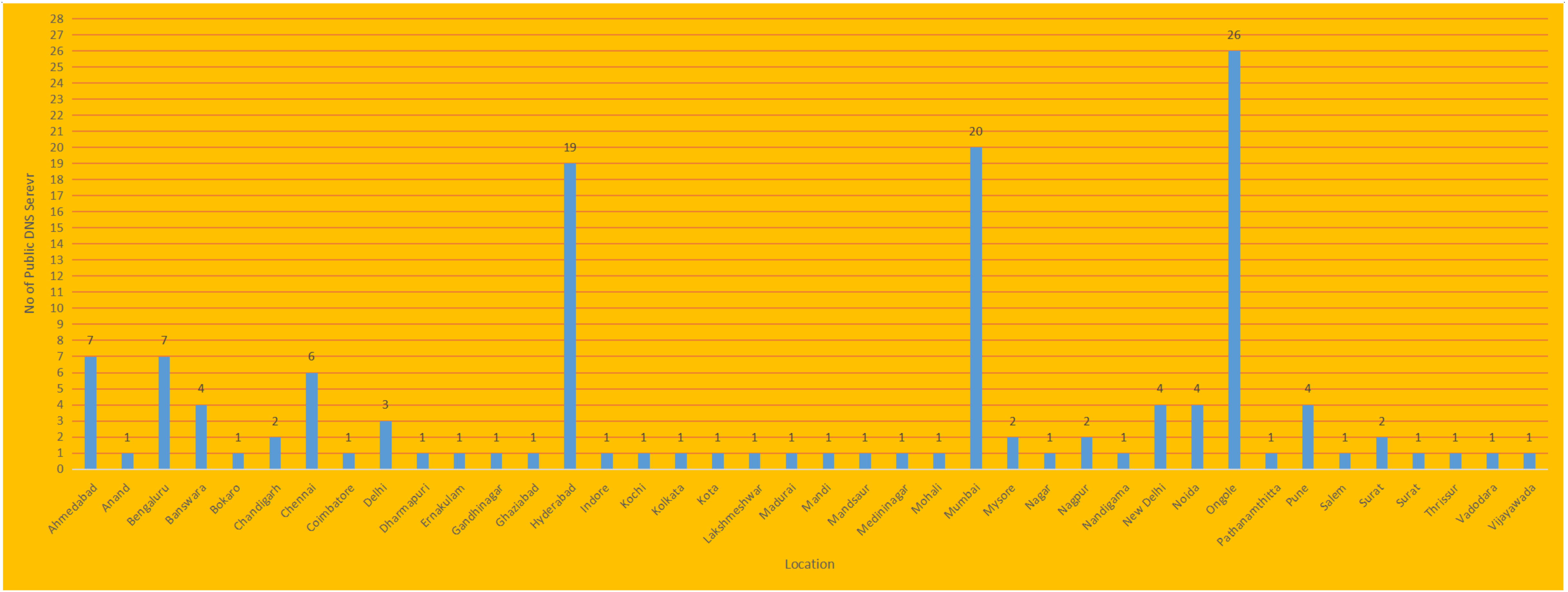
Public DNS Recursive Resolver

- DNS Resolvers are the critical components within the DNS Ecosystem
- Our Public DNS resolver for IPv4 and IPv6 is available at:
  - **IPv4: 223.31.121.171**
  - **IPv6: 2405:8a00:8001::20**
- Optimized Configuration
  - Compliance with RFC 7706

Public DNS Resolvers

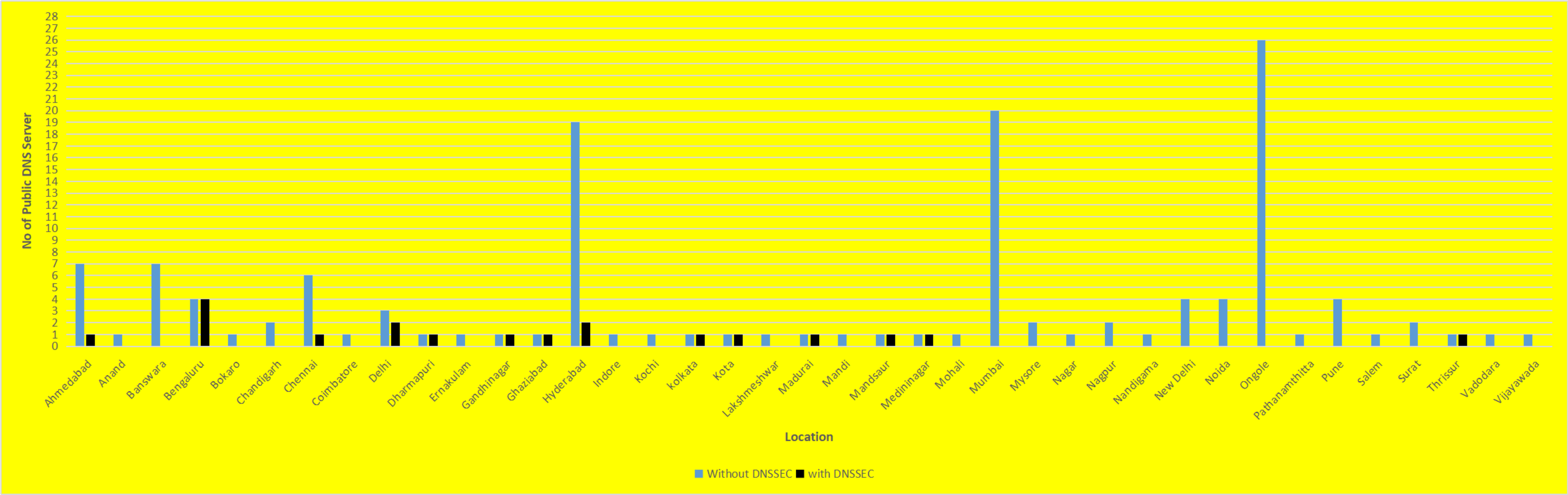


Public DNS Resolvers in India



/iiref coednssecurity.in @IIRnEF

Indian Public DNS Resolvers – DNSSEC Stats



Thank You