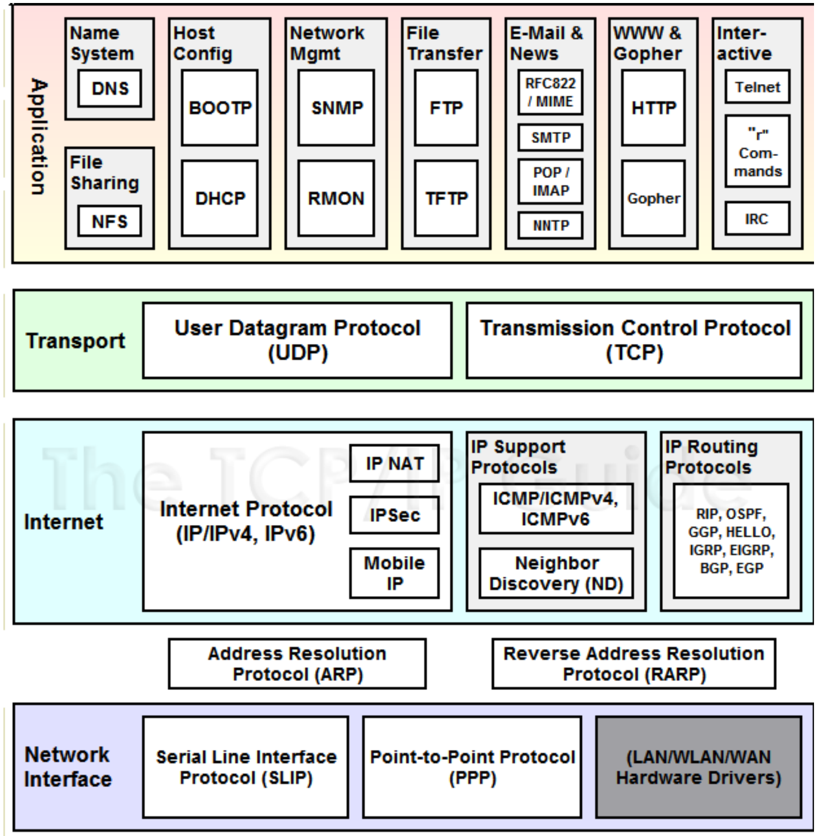
Attacks on DNS

(some slides based on SEED LAB)

- Do you remember the IP address of google.com from the first tutorial?



Application

Name System: DNS

File Sharing: NFS

Host Config: BOOTP, DHCP

Network Mgmt: SNMP, RMON

File Transfer: FTP, TFTP

E-Mail & News: RFC822 / MIME, SMTP, POP / IMAP, NNTP

WWW & Gopher: HTTP, Gopher

Inter-active: Telnet, "r" Com-mands, IRC

Transport: User Datagram Protocol (UDP), Transmission Control Protocol (TCP)

Internet: Internet Protocol (IP/IPv4, IPv6), IP NAT, IPSec, Mobile IP

IP Support Protocols: ICMP/ICMPv4, ICMPv6, Neighbor Discovery (ND)

IP Routing Protocols: RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP

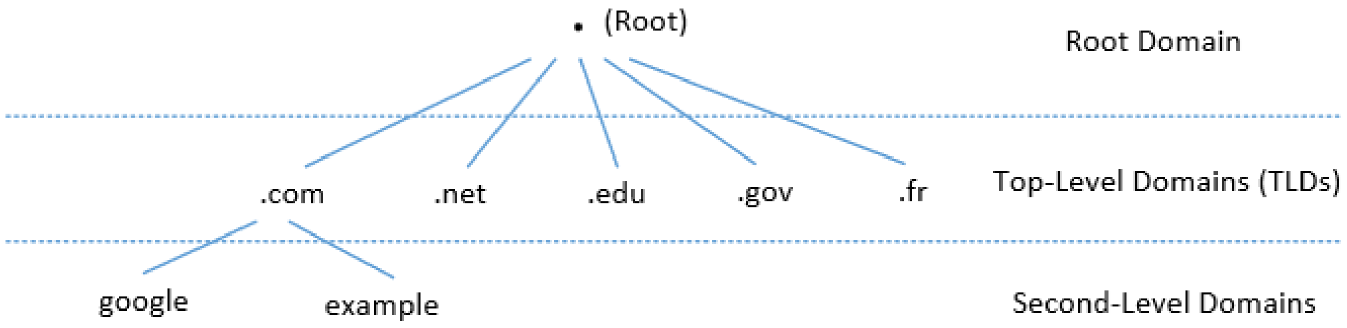
Address Resolution Protocol (ARP)

Reverse Address Resolution Protocol (RARP)

Network Interface: Serial Line Interface Protocol (SLIP), Point-to-Point Protocol (PPP), (LAN/WLAN/WAN Hardware Drivers)

The TCP/IP Guide

DNS Domain Hierarchy

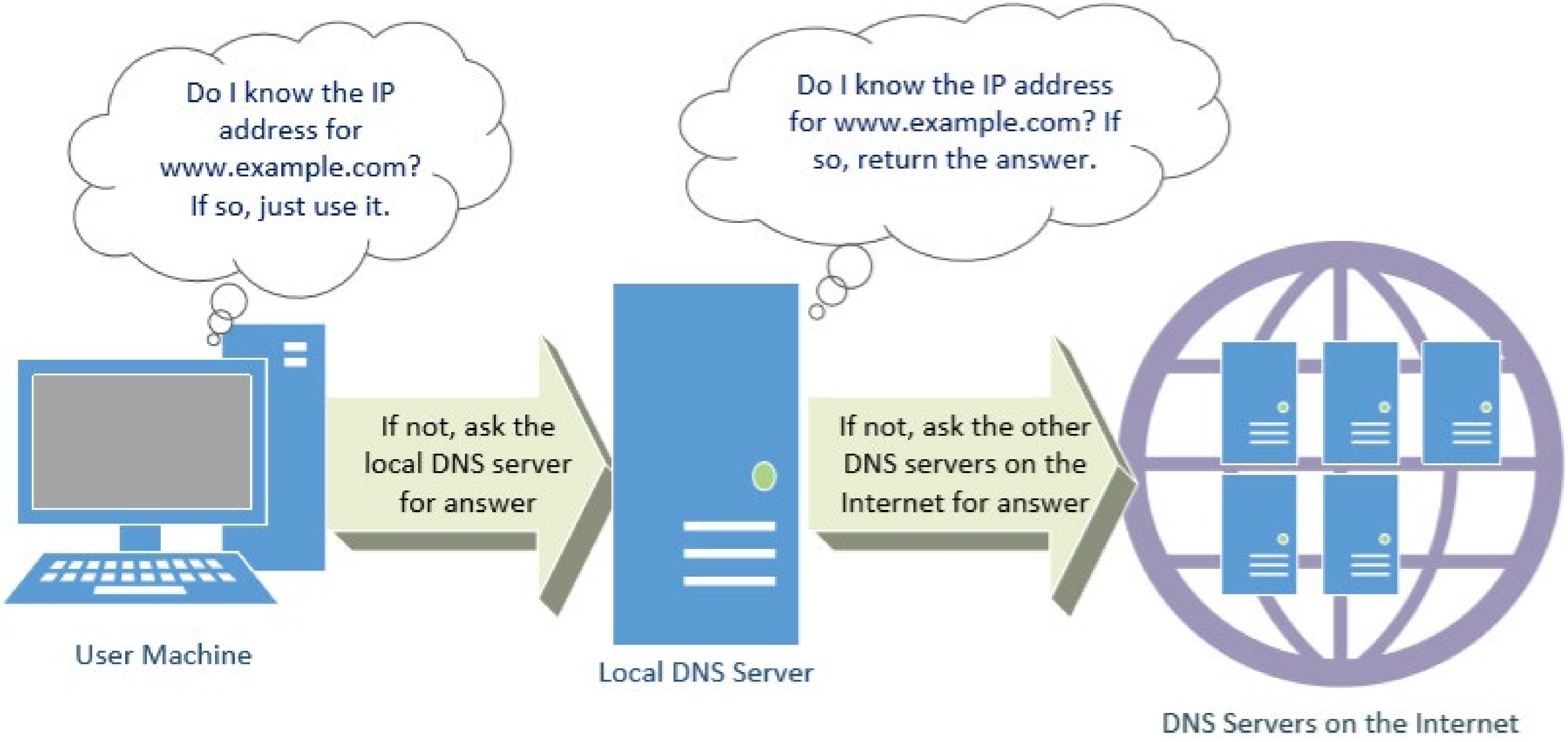


- Below ROOT, we have Top-Level Domain (TLD). Ex: In www.example.com, the TLD is .com.

- The next level of domain hierarchy is second-level domain which are usually assigned to specific entities such as companies, schools etc

- Domain namespace is organized in a hierarchical tree-like structure.
- Each node is called a domain, or subdomain.
- The root of the domain is called ROOT, denoted as ‘ . ‘.

DNS Query Process



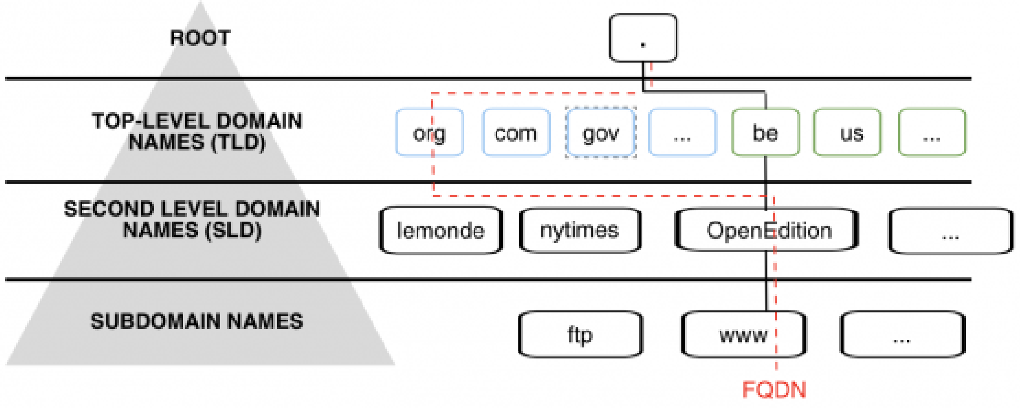
Do I know the IP address for www.example.com? If so, just use it.

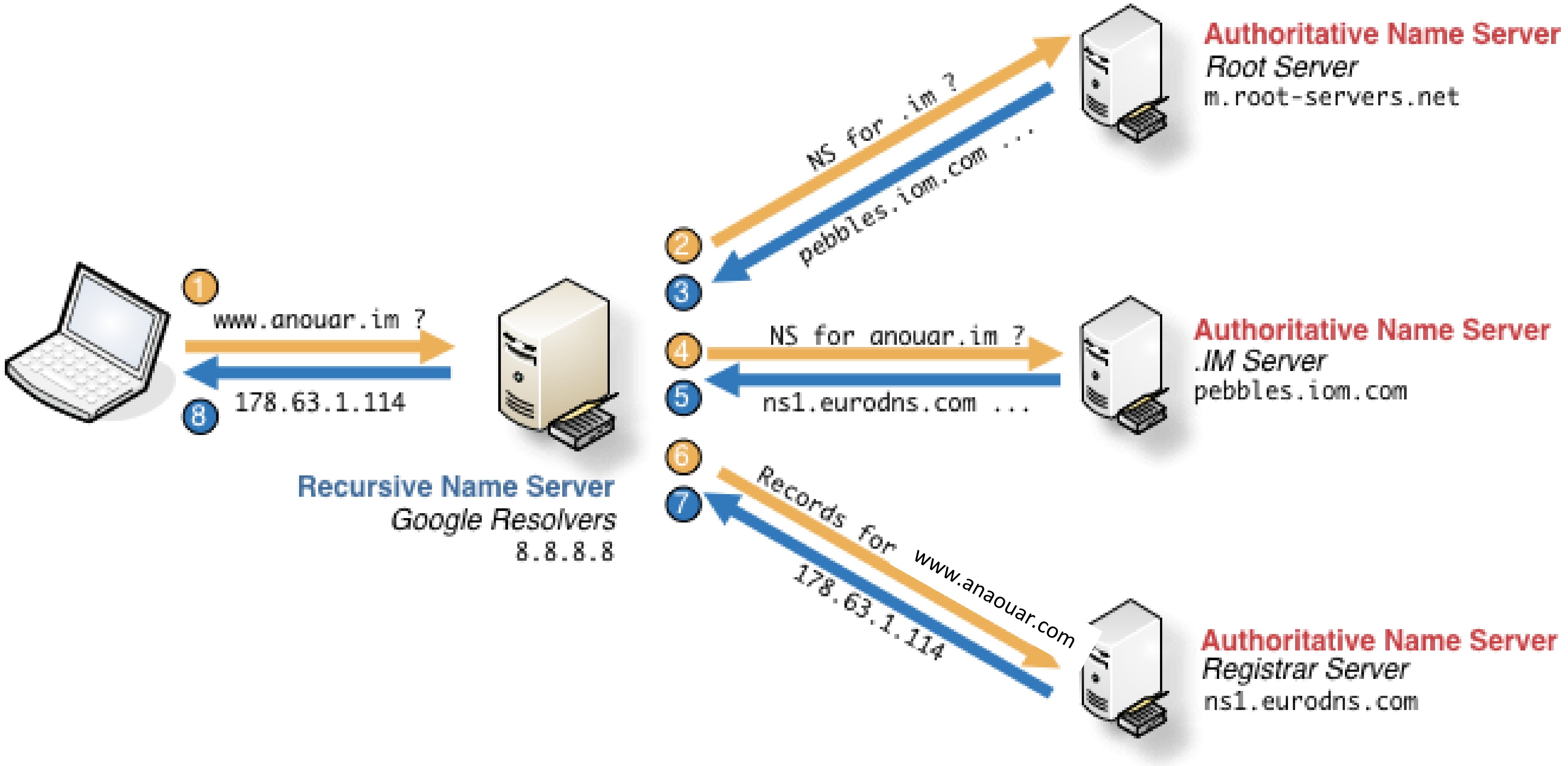
If not, ask the local DNS server for answer

Do I know the IP address for www.example.com? If so, return the answer.

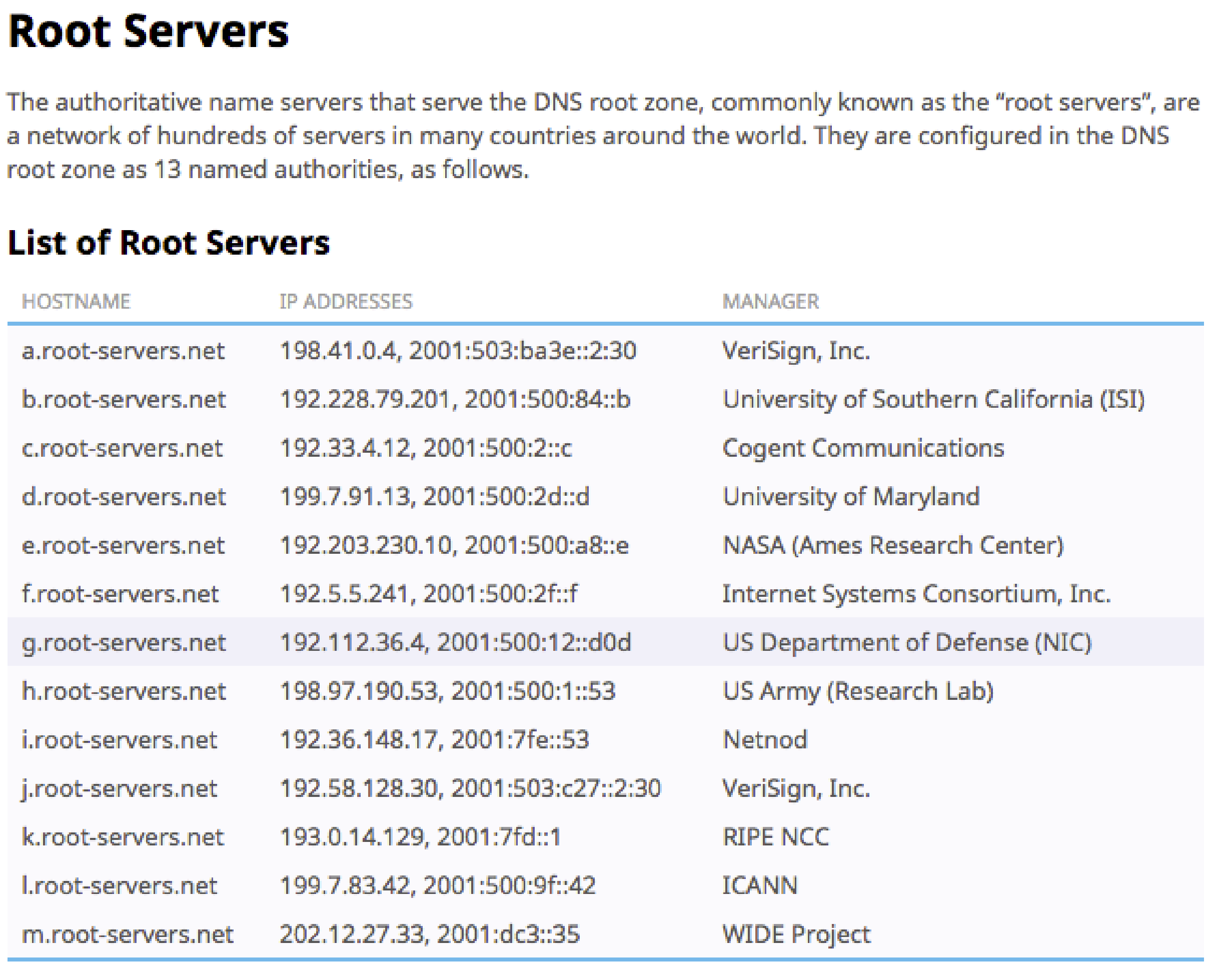
If not, ask the other DNS servers on the Internet for answer

DNS Hierarchy





DEMO on retrieving IP of www.example.net



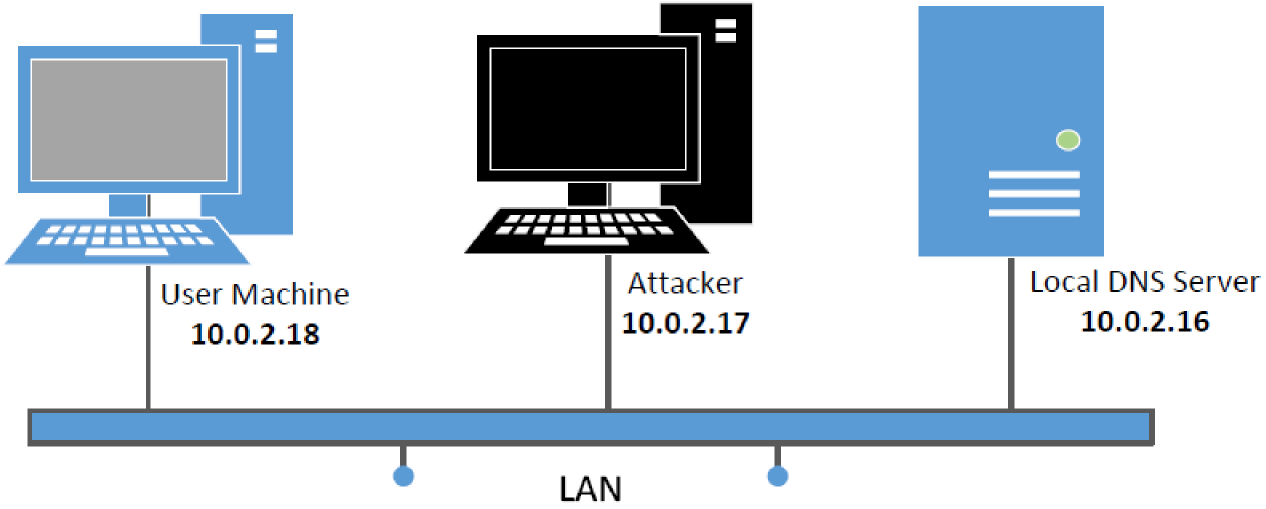
Root Servers

The authoritative name servers that serve the DNS root zone, commonly known as the “root servers”, are a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities, as follows.

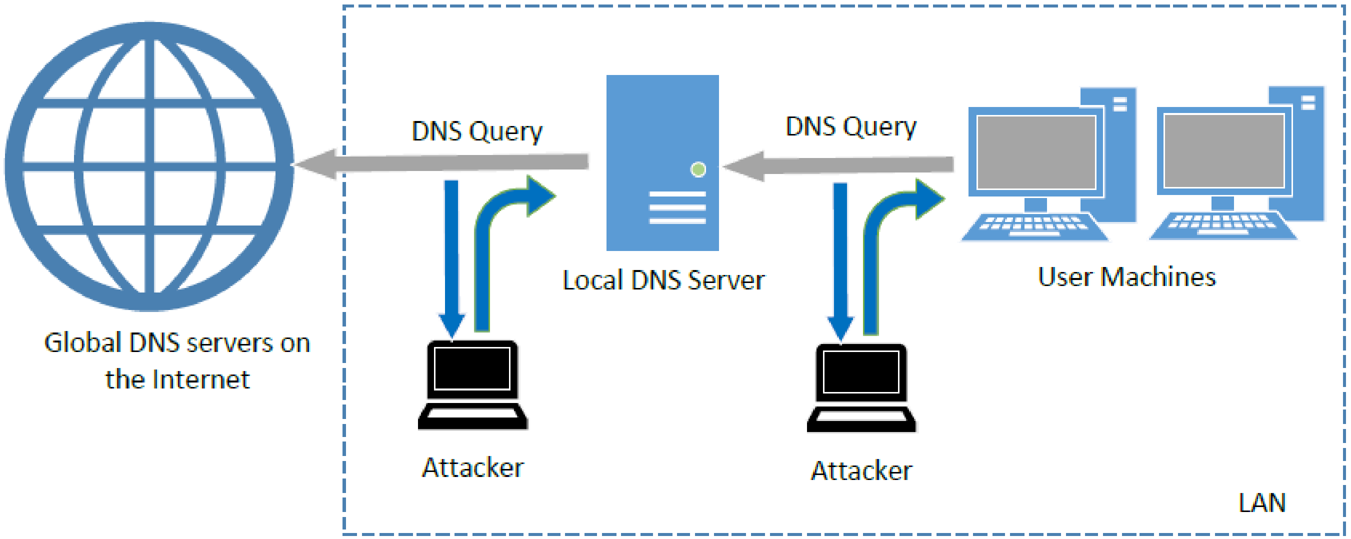
List of Root Servers

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, 2001:500:84::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

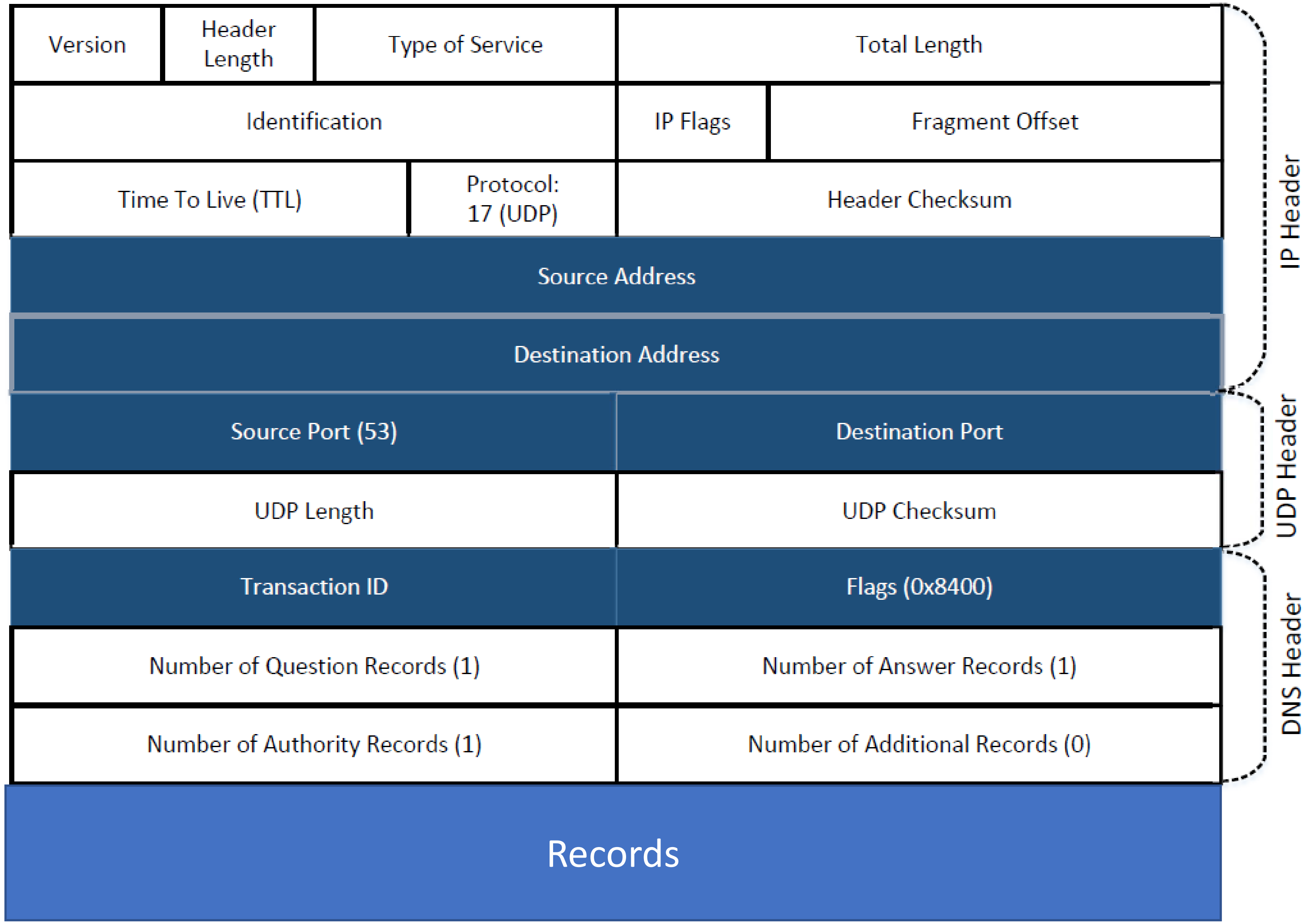
Set Up DNS Server and Experiment Environment



Attack Surfaces



DNS Packet



Version | Header Length | Type of Service | Total Length

Identification | IP Flags | Fragment Offset

Time To Live (TTL) | Protocol: 17 (UDP) | Header Checksum

Source Address

Destination Address

Source Port (53) | Destination Port

UDP Length | UDP Checksum

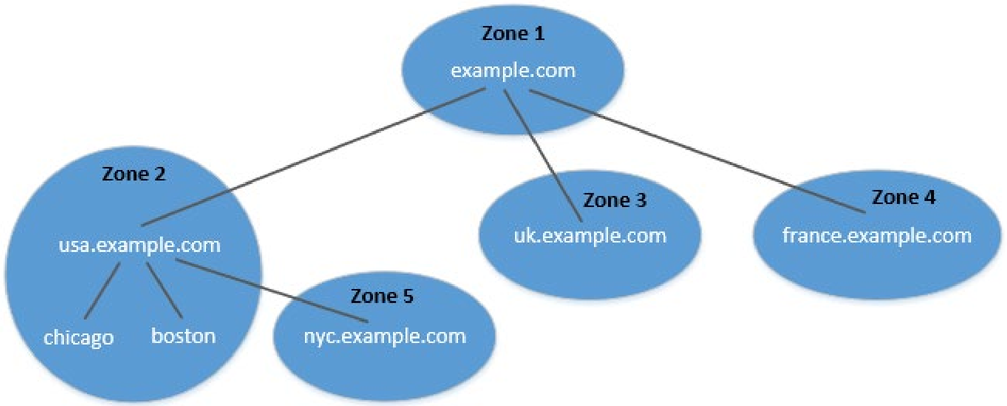
Transaction ID | Flags (0x8400)

Number of Question Records (1) | Number of Answer Records (1)

Number of Authority Records (1) | Number of Additional Records (0)

Records

DNS Zone



- DNS is organized according to zones.
- A zone groups contiguous domains and subdomains on the domain tree and assign management authority to an entity.

- The tree structure depicts subdomains within example.com domain.
- In this case, there are multiple DNS zones one for each country. The zone keeps records of who the authority is for each of its subdomains.
- The zone for example.com contains only the DNS records for the hostnames that do not belong to any subdomain like mail.example.com