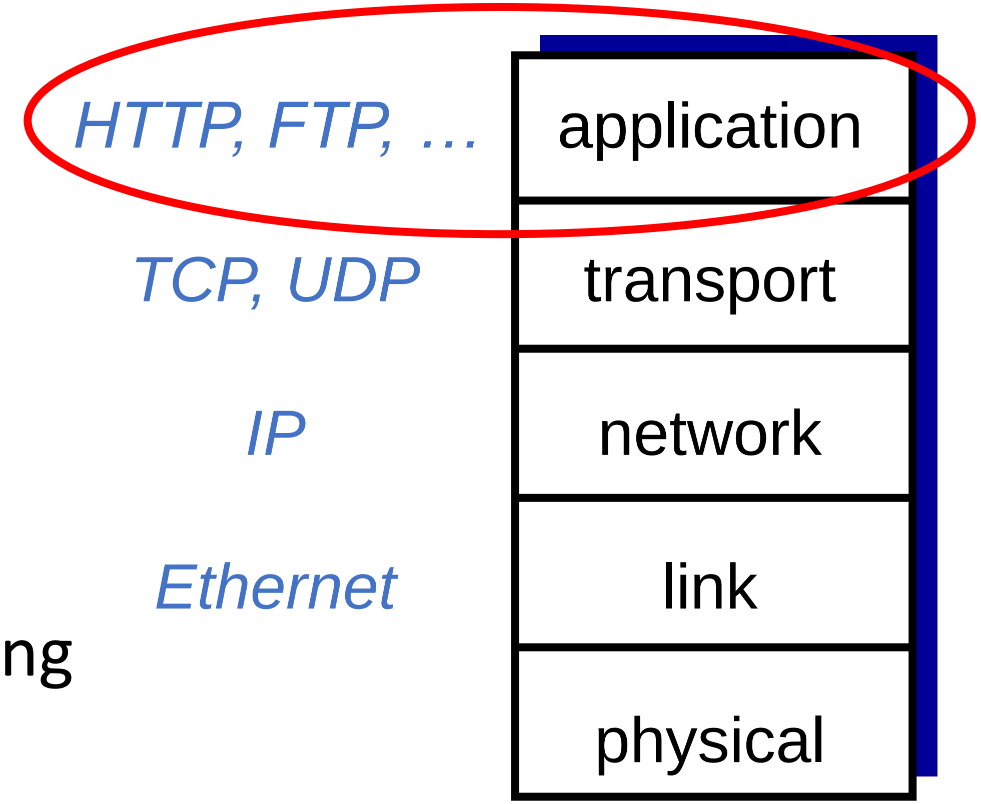
DNS Attacks

Instructor: Khaled Diab

Recall: TCP/IP Protocol Suite

- *application:* supporting network applications
  - FTP, SMTP, HTTP
- *transport:* process-to-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits “on the wire”

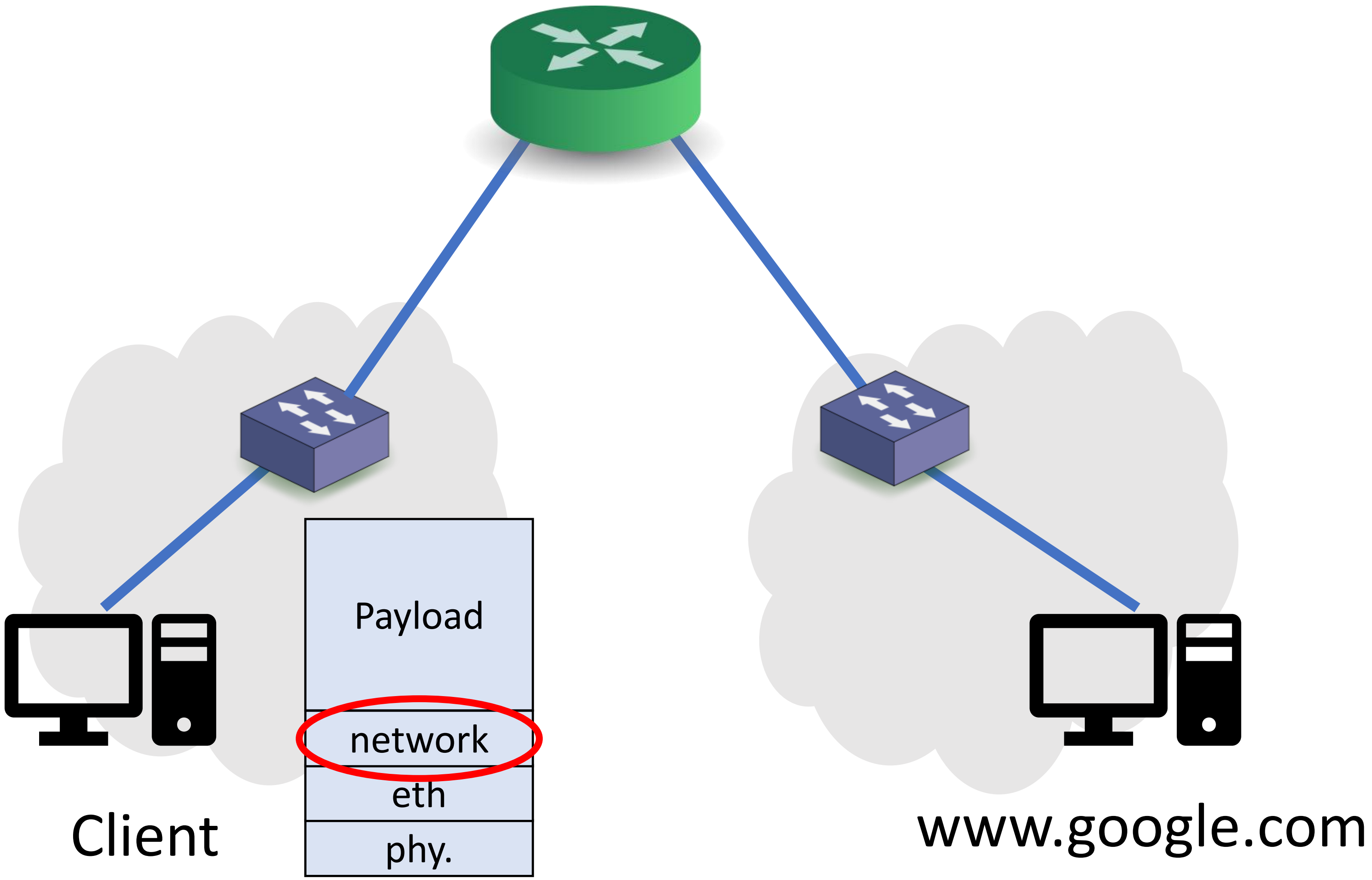


Outline

- DNS
    - Hierarchy, Zones and Servers
    - DNS Query Process
- DNS Attacks Overview

Domain Name System (DNS)

Internet Naming



Rationale

- Hosts need to map a domain name to and IP address
  - Needed for Layer 3

- What are our options?

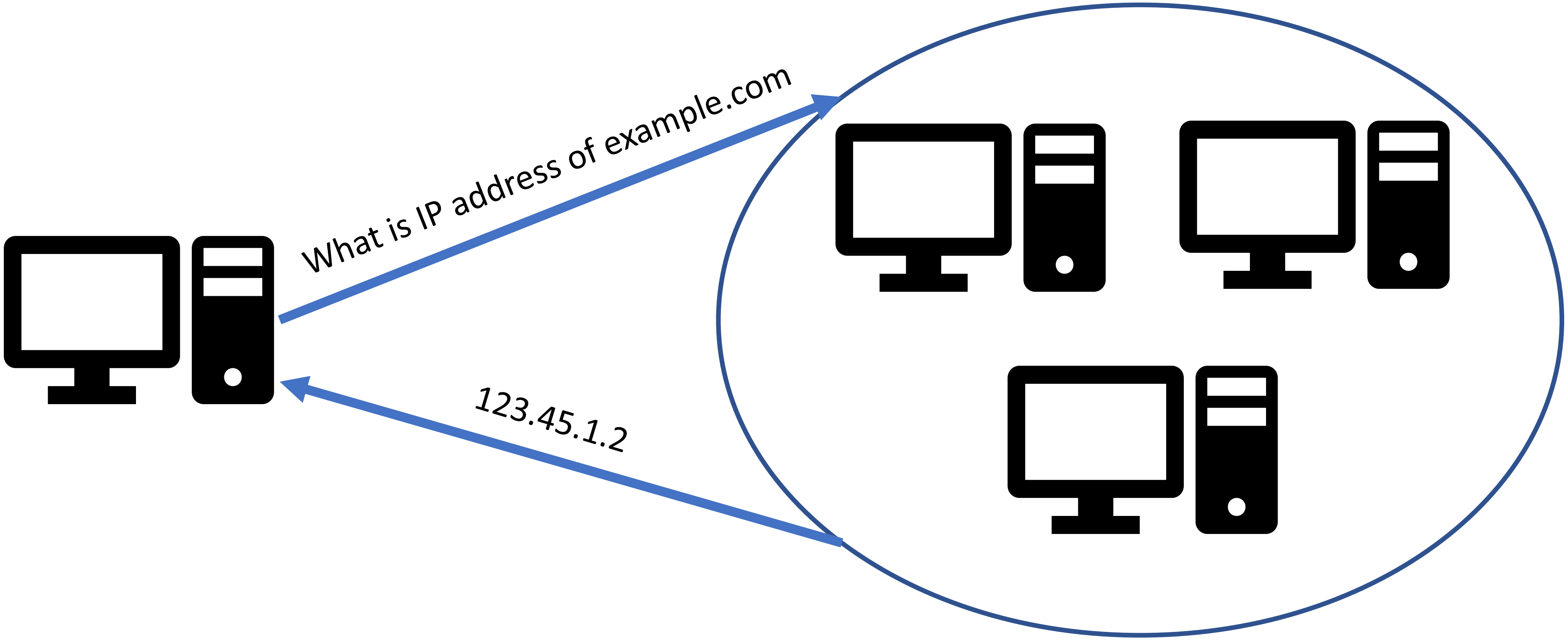
Rationale

- Option #1: Store all IP-name mappings
  - Issues?

Name	IP
Example.com	123.45.1.2
Example.net	67.12.8.10
…	…

Rationale

- Option #2: Hosts ask another system about this mapping

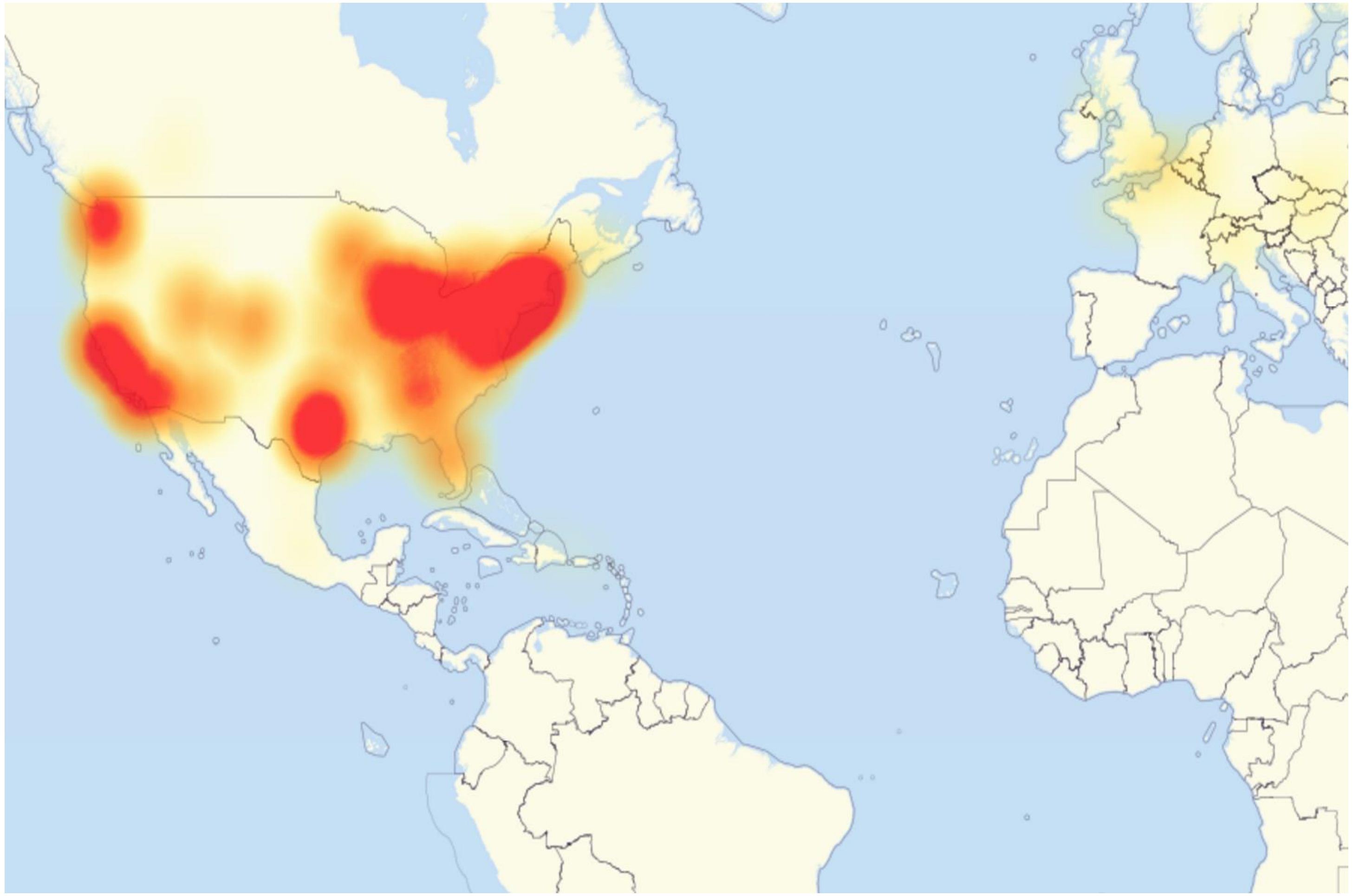


Domain Name System (DNS)

- The Internet phone book
- A distributed system that maintains the mapping between domain name and IP address
    - Why is DNS distributed?
- A core component in the Internet
- Attacks on DNS may result in:
    - massive Internet shutdown
    - traffic directed to attacker's servers

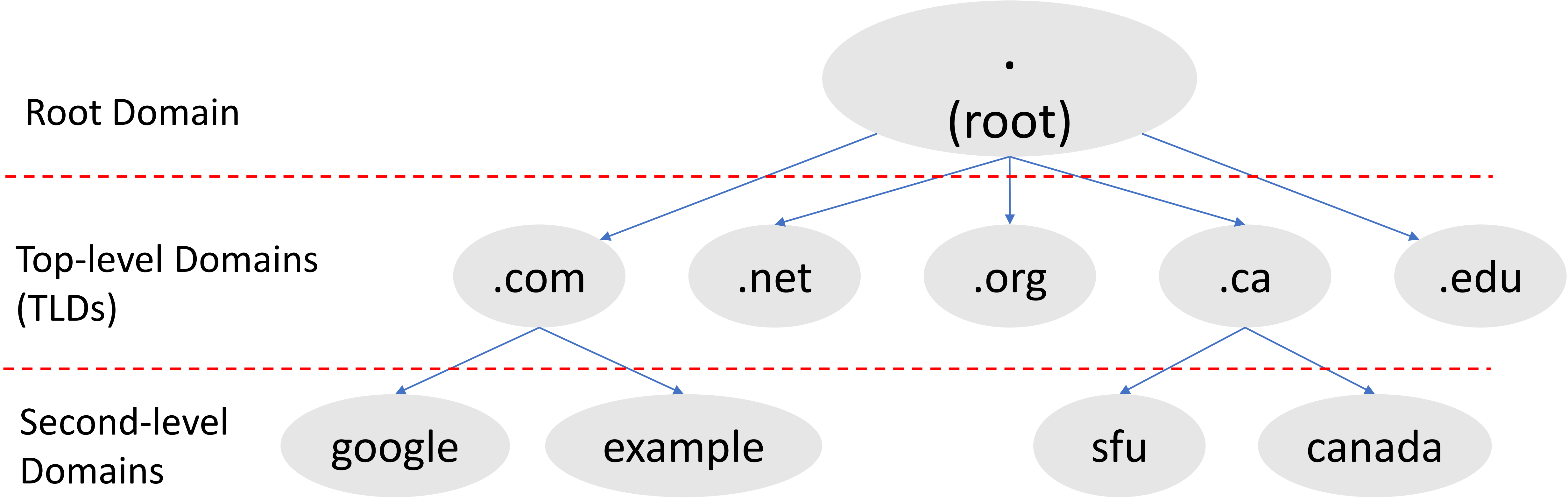
Recent Incident: DDoS on Dyn Servers

- Massive Internet disruption in 2016
- Many affected clients and businesses
- DDoS on Dyn’s DNS servers
  - Attackers use infected IoT devices with Mirai botnet
- Three charges announced later in 2017



DNS Domain Hierarchy

- Domain *namespace* are organized in a hierarchy



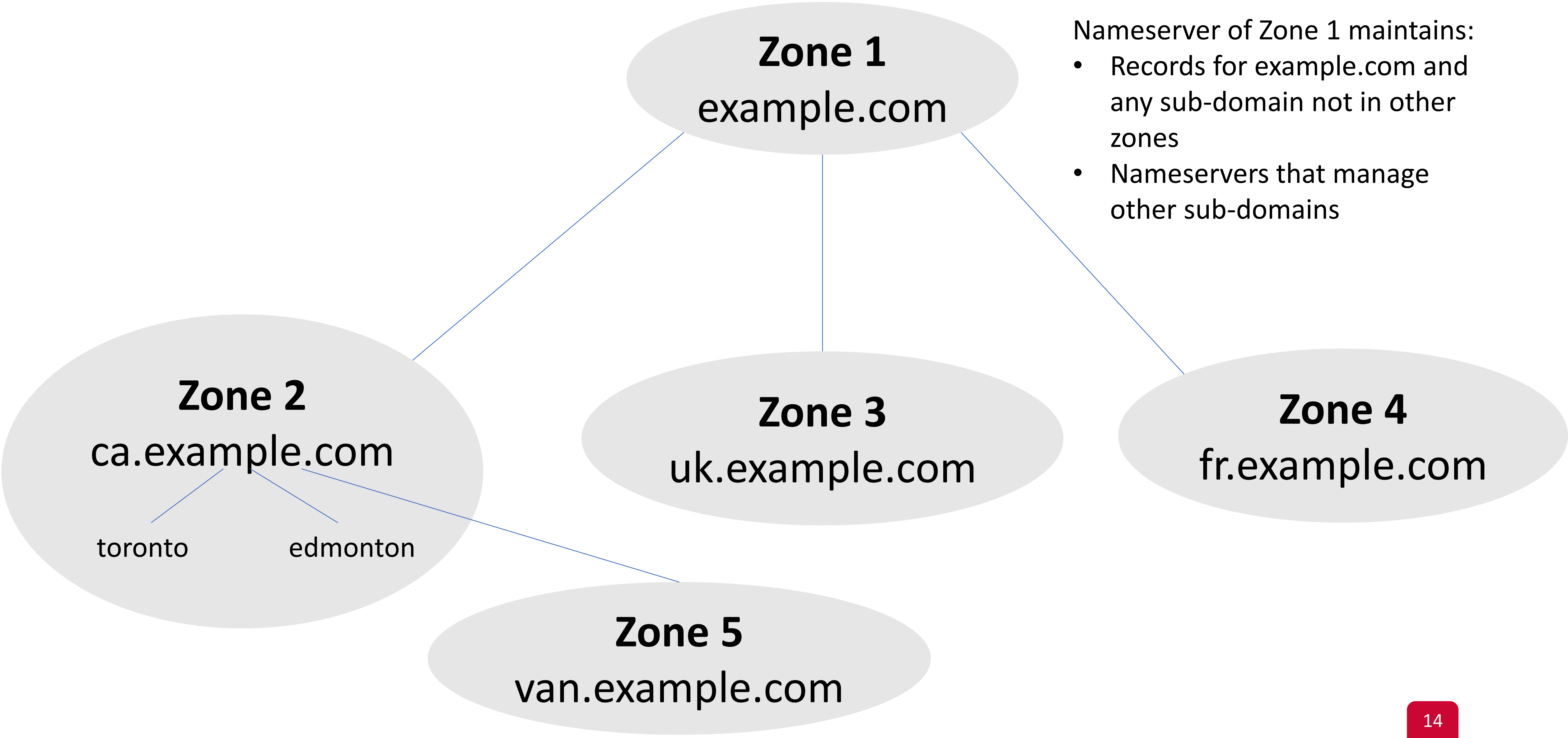
DNS Domain Hierarchy

- Official list of all TLDs is managed by IANA
  - The Internet Assigned Numbers Authority
- IANA delegates each TLD to a manager, called a *registry*:
  - VeriSign → .com and .net domains
  - CIRA → .ca domain
  - EDUCASE → .edu domain
- A TLD registry contracts with other entities, called *registrars*:
  - To provide registration services to the public
  - When an end-user purchases a domain name: The registrar works with the TLD registrar to add the required information
  - Examples of registrars?

DNS Zones

- DNS is organized into *zones* for management purposes
- Each zone:
  - groups a contiguous domains and sub-domains, and
  - assigns the management authority to an entity
- The nameserver of a zone maintains DNS records for all domains managed by this zone
- A domain can be managed by multiple authorities
  - If it’s divided into multiple zones

DNS Zones: An Example



Nameserver of Zone 1 maintains:

- Records for example.com and any sub-domain not in other zones
- Nameservers that manage other sub-domains

Authoritative Name Servers

- Each DNS zone has at least one authoritative nameserver:
  - It publishes information about that zone
  - It provides definitive answer to DNS queries
- Primary and secondary nameservers
  - Primary: stores the original copy of all zone records
  - Secondary: maintains an identical copy of the primary server
- Each zone should provide multiple authoritative nameservers
  - For redundancy and reliability
- A single authoritative nameserver may maintain records for multiple zones

Zone Organization on the Internet

- Goal: ask an authoritative nameserver for answers
- Options:
    - Each host maintains a list of all authoritative nameservers
    - A central server that maintains that list
    - Issues?
- Instead,
    - Organize DNS zones on the Internet in a tree structure

Zone Organization on the Internet

- The root of the tree (root zone):
  - Managed by IANA
  - It has 13 authoritative nameservers
  - a.root-servers.net – m.root-servers.net
  - These servers are given to the OS (through conf. files)

- Every name resolution either:
  - Starts with a query to one of the root servers, or
  - Uses info. that was once obtained from these root servers

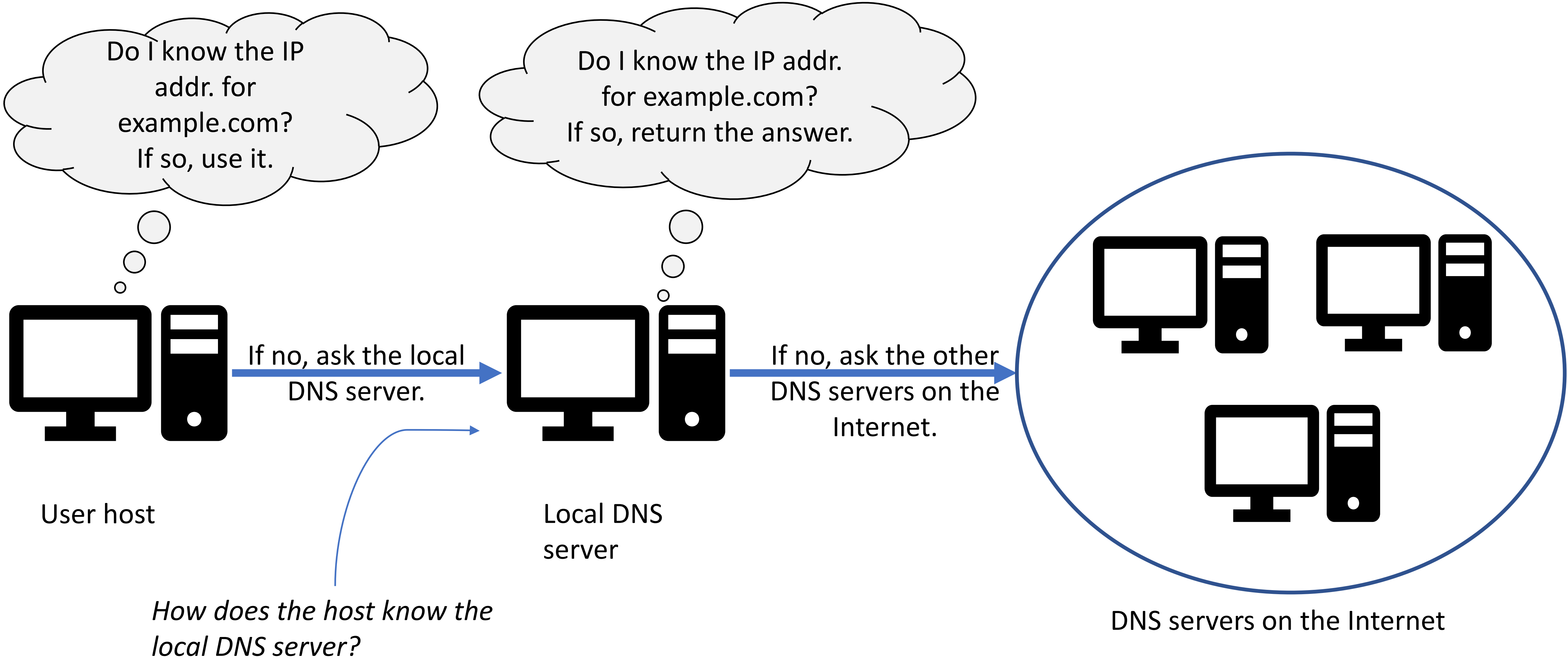
Zone Organization on the Internet

- Each of the TLD zones has authoritative nameservers
- They are registered with the root servers

- Each domain name has at least two nameservers

DNS Query Process

DNS Query Process: Overview



Do I know the IP addr. for example.com? If so, use it.

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

If no, ask the local DNS server.

If no, ask the other DNS servers on the Internet.

User host

Local DNS server

DNS servers on the Internet

How does the host know the local DNS server?

Local DNS Files

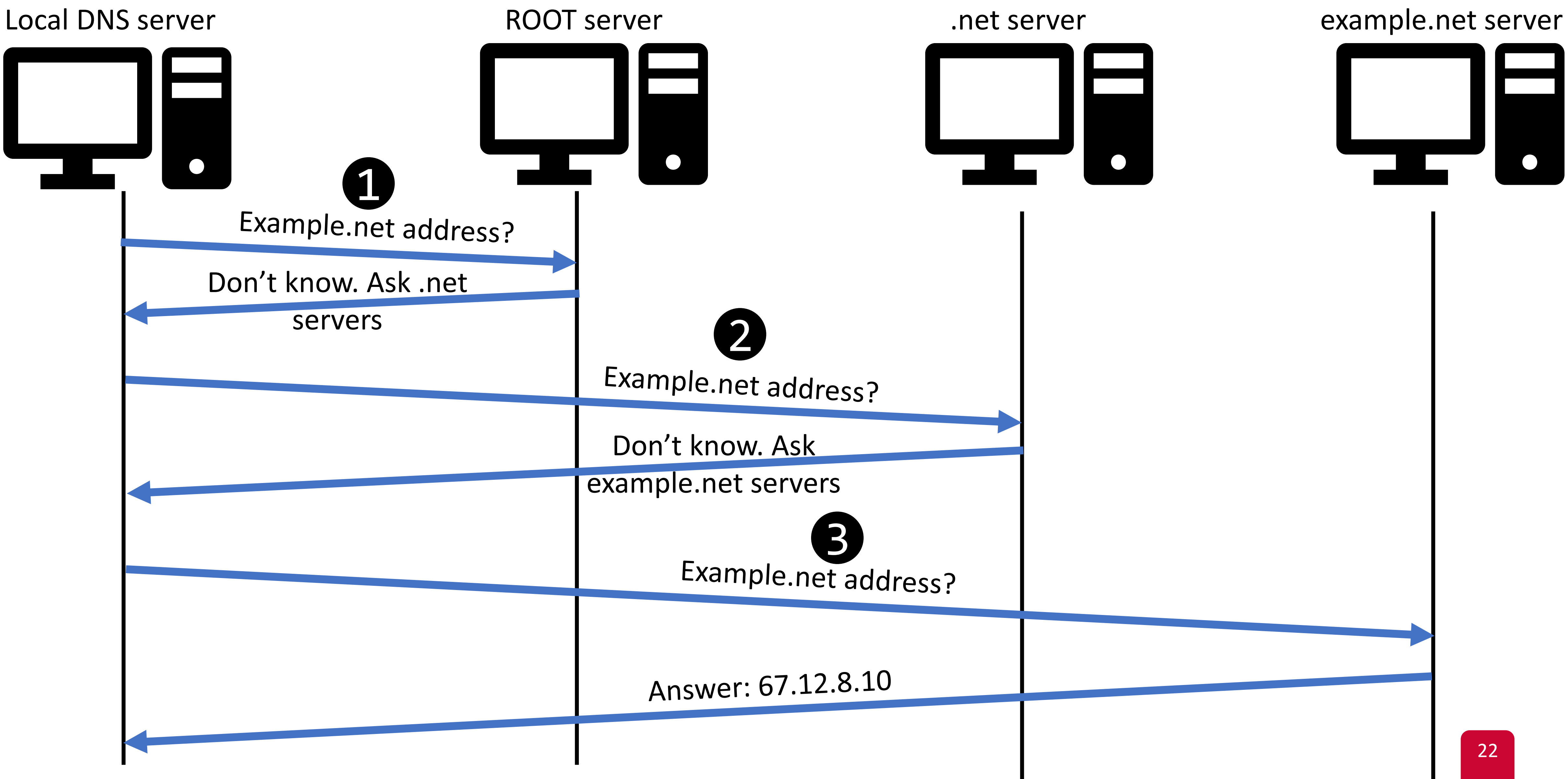
- Two files in Linux that DNS resolvers use:
- `/etc/hosts`
  - Stores static IP addresses for hostnames

```
127.0.0.1       localhost
123.45.1.2      example.com
```

- `/etc/resolv.conf`
  - If the domain doesn’t exist in `/etc/hosts`, the host needs to ask the local DNS server
  - May be automatically generated if using DHCP
  - The IP address of the local DNS server is stored in `/etc/resolv.conf`

```
nameserver 127.0.1.1
search cmpt.sfu.ca
```

Local DNS Server and the Iterative Query



To do list

- Quiz 2 at 10:00 am
- Assignment 2 is due next week
- Assignment 3 will be released soon