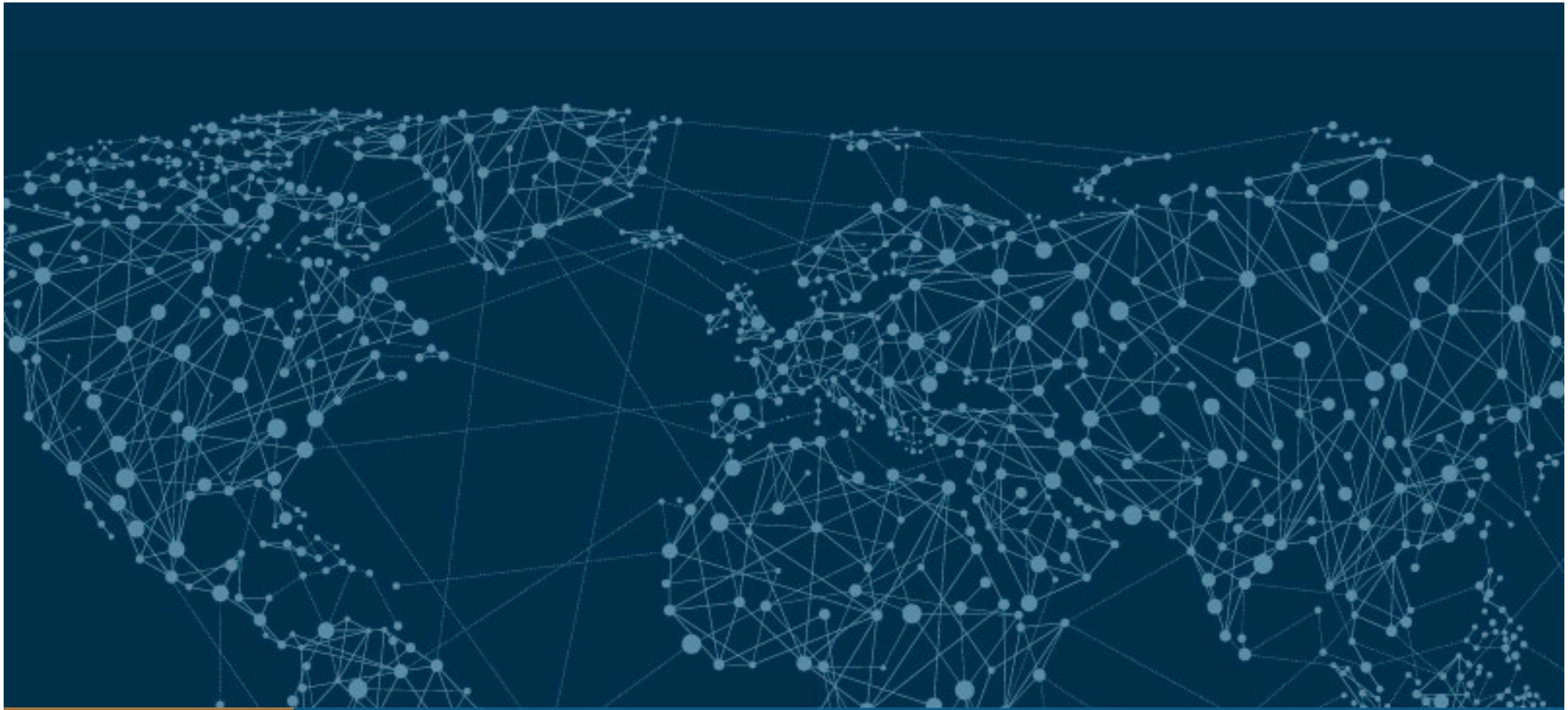


APRALO Slides

Steve Sheng | July 2015

Outline

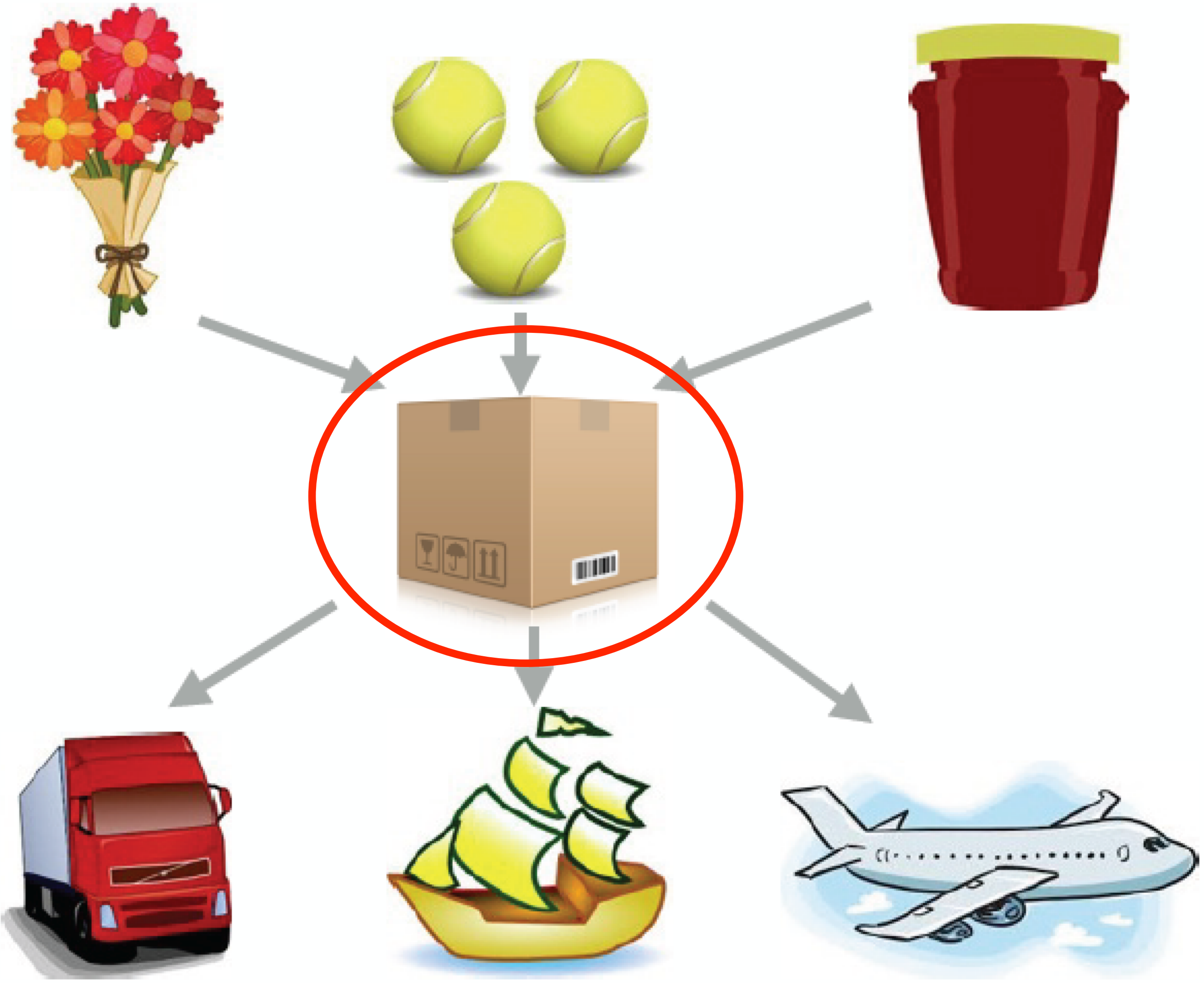
1. Overview of IP Addressing
2. Overview of DNS
3. Domain Name registration process
4. Domain name resolution process
5. DNS Security and Privacy

Credits

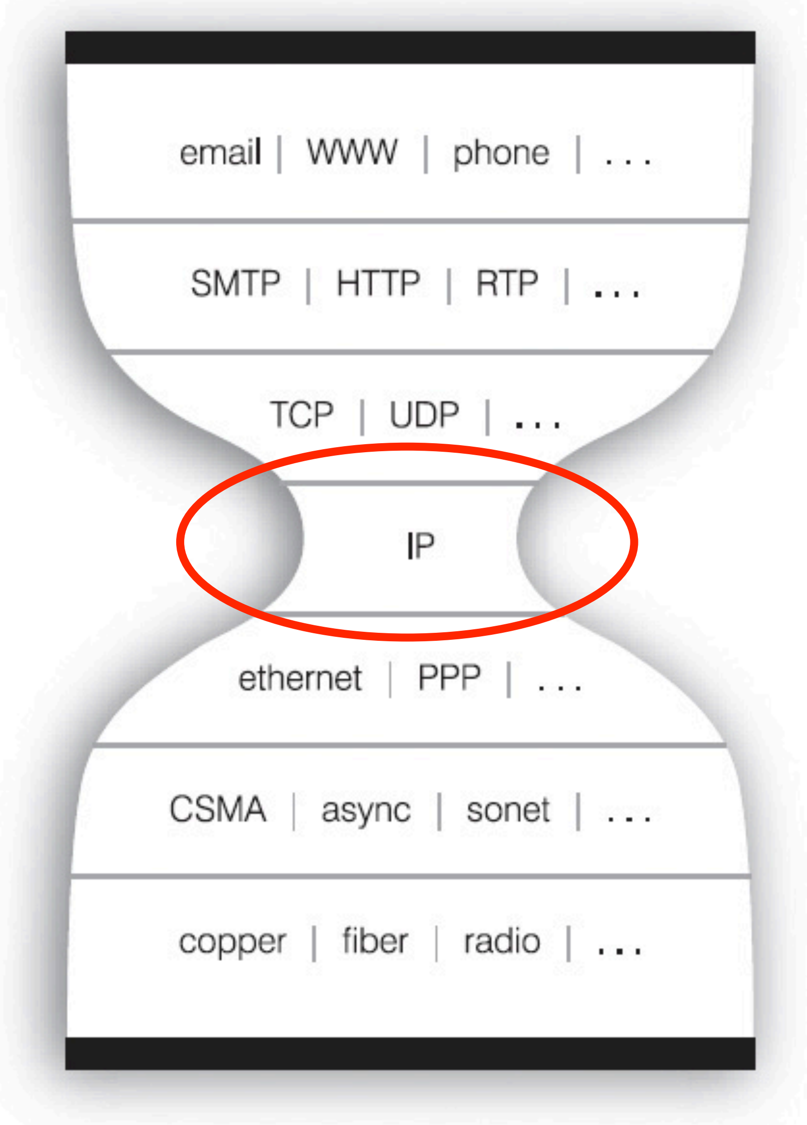
- Slides 4-11, RIPE NCC IETF 89 presentation, ASO updates
- Slide 22, SSAC Report on Registration Data Model
- Slides 24 – 29, Olaf Kolkman, an Introduction to the Domain Name System
- Slides 30 – 50, Steve Crocker, Kim Davies, Stephane Bortzmeyer

Introduction to IP Addressing

Packet Networking



Hour Glass Model



email | WWW | phone | . . .

SMTP | HTTP | RTP | . . .

TCP | UDP | . . .

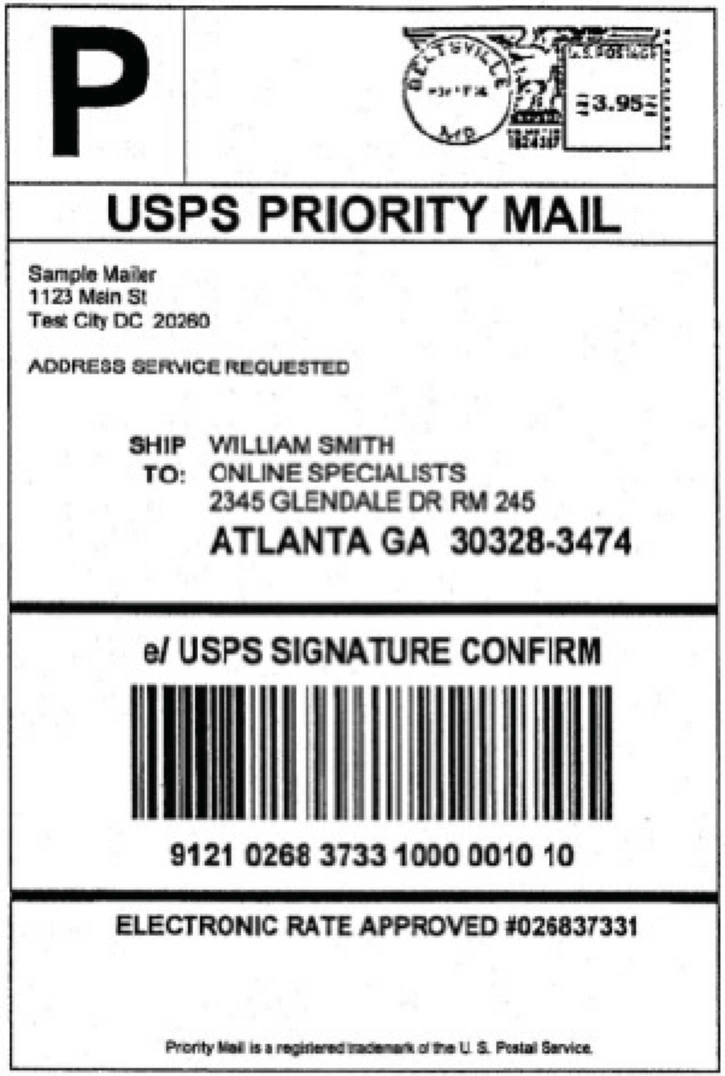
IP

ethernet | PPP | . . .

CSMA | async | sonet | . . .

copper | fiber | radio | . . .

Packet header



P

BELTSVILLE MD

U.S. POSTAGE

$3.95

USPS PRIORITY MAIL

Sample Mailer
1123 Main St
Test City DC 20260

ADDRESS SERVICE REQUESTED

SHIP TO: WILLIAM SMITH
ONLINE SPECIALISTS
2345 GLENDALE DR RM 245
ATLANTA GA 30328-3474

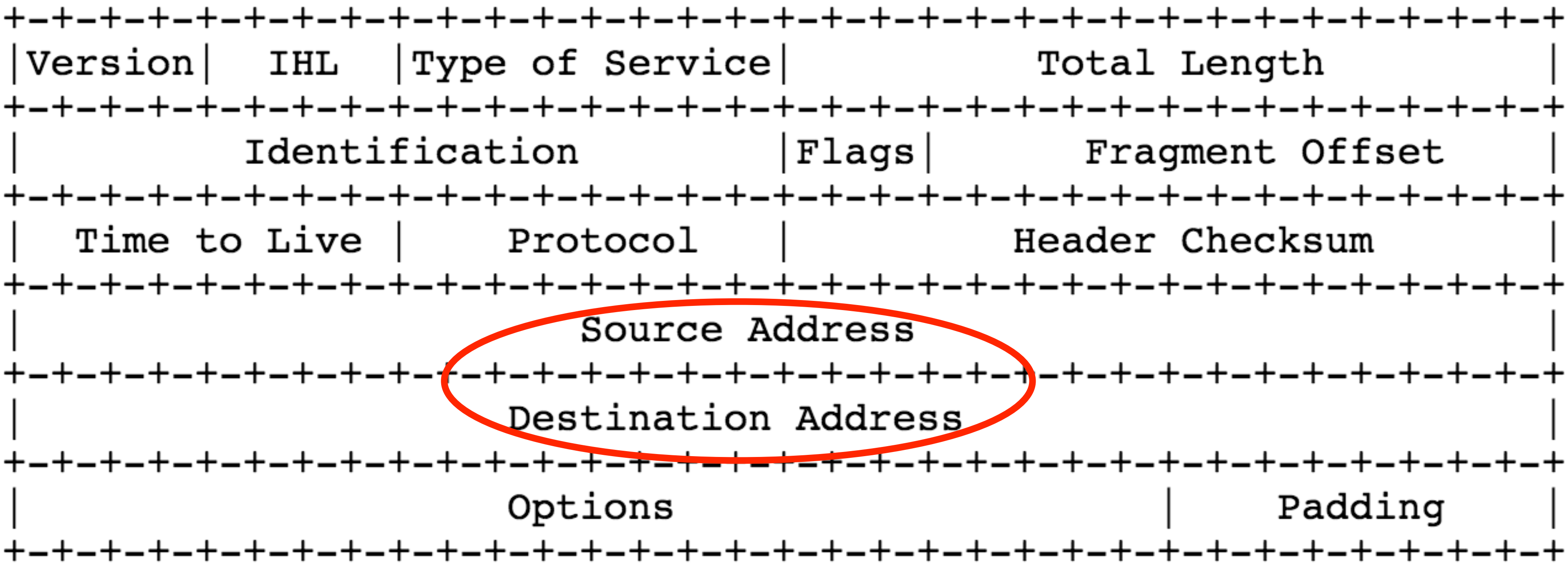
e/ USPS SIGNATURE CONFIRM

9121 0268 3733 1000 0010 10

ELECTRONIC RATE APPROVED #026837331

Priority Mail is a registered trademark of the U. S. Postal Service.

IP Packet Header



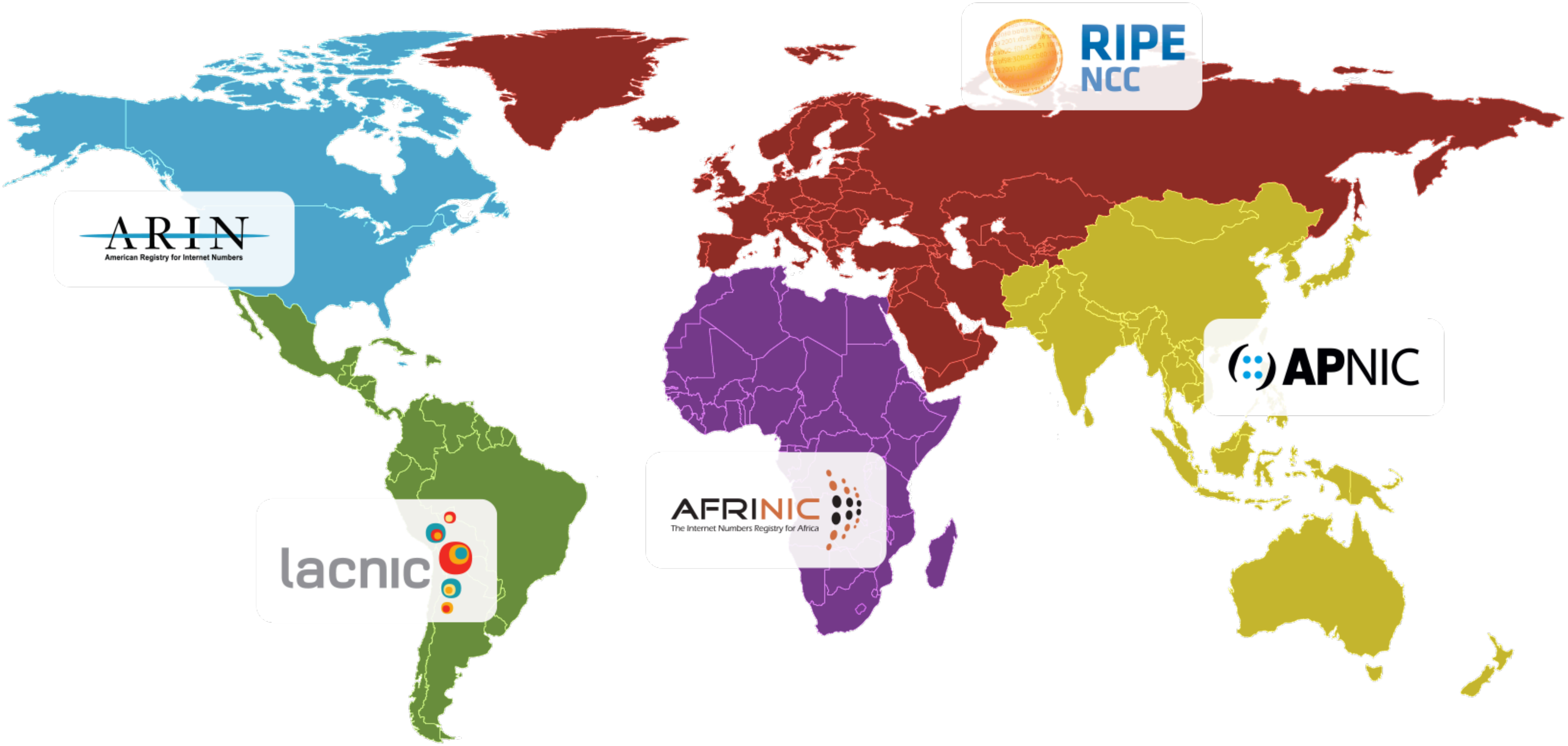
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reference: https://www.ietf.org/rfc/rfc791.txt

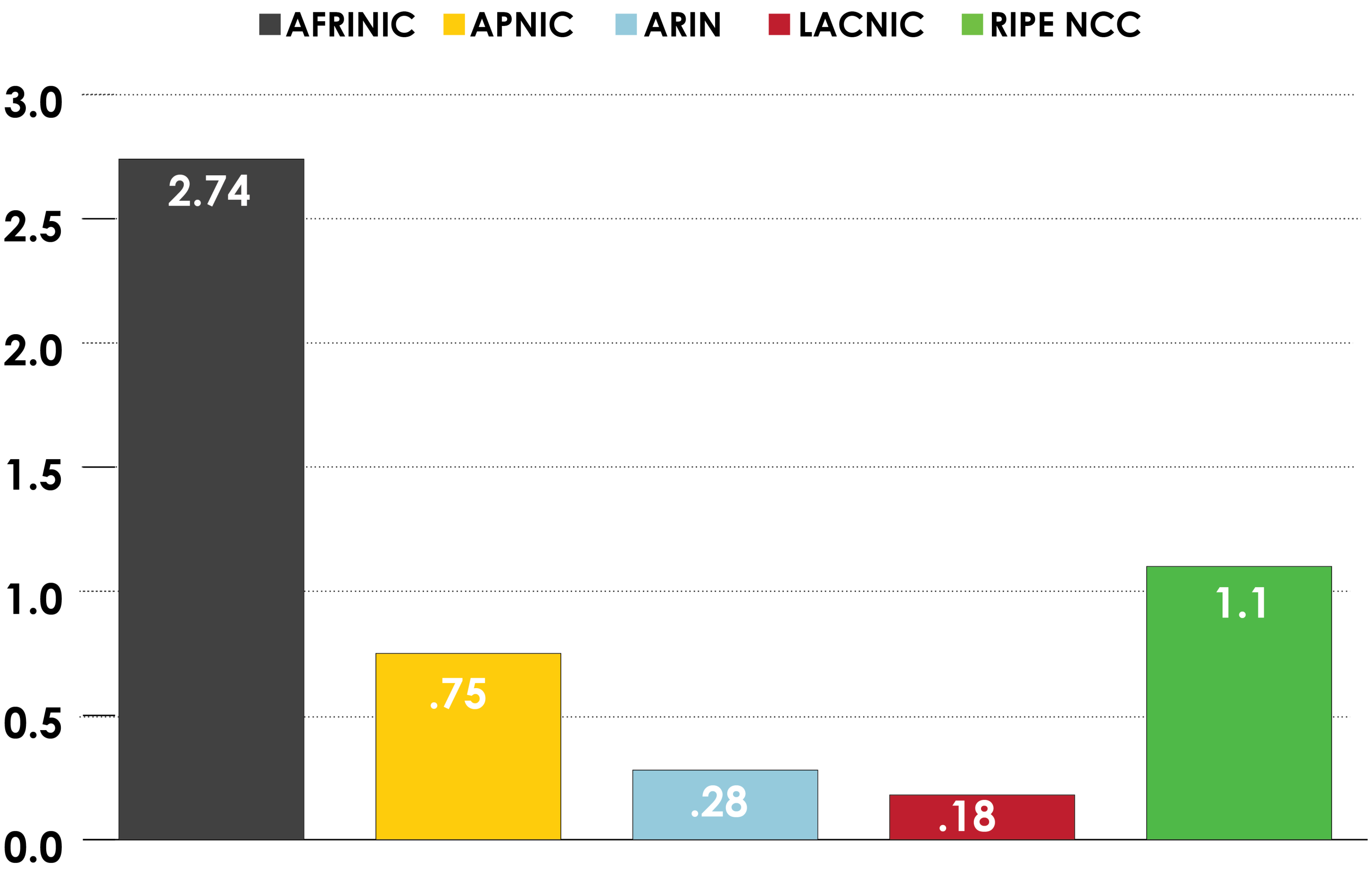
IP Address

- An Internet Protocol (IP) address is a number that identifies a device on a computer network.
- Fixed format:
  - IPv4 – 32 bits (192.0.43.7)
  - IPv6 - 128 bits (2001:0db8:85a3:0000:0000:8a2e:0370:7334)
- Properties
  - Machine readable - every entity handling packets be able to read and understand the address
  - "Globally unique" - the address is unambiguous

Regional Internet Registries


RIPE NCC
ARIN
American Registry for Internet Numbers
APNIC
AFRINIC
The Internet Numbers Registry for Africa
lacnic

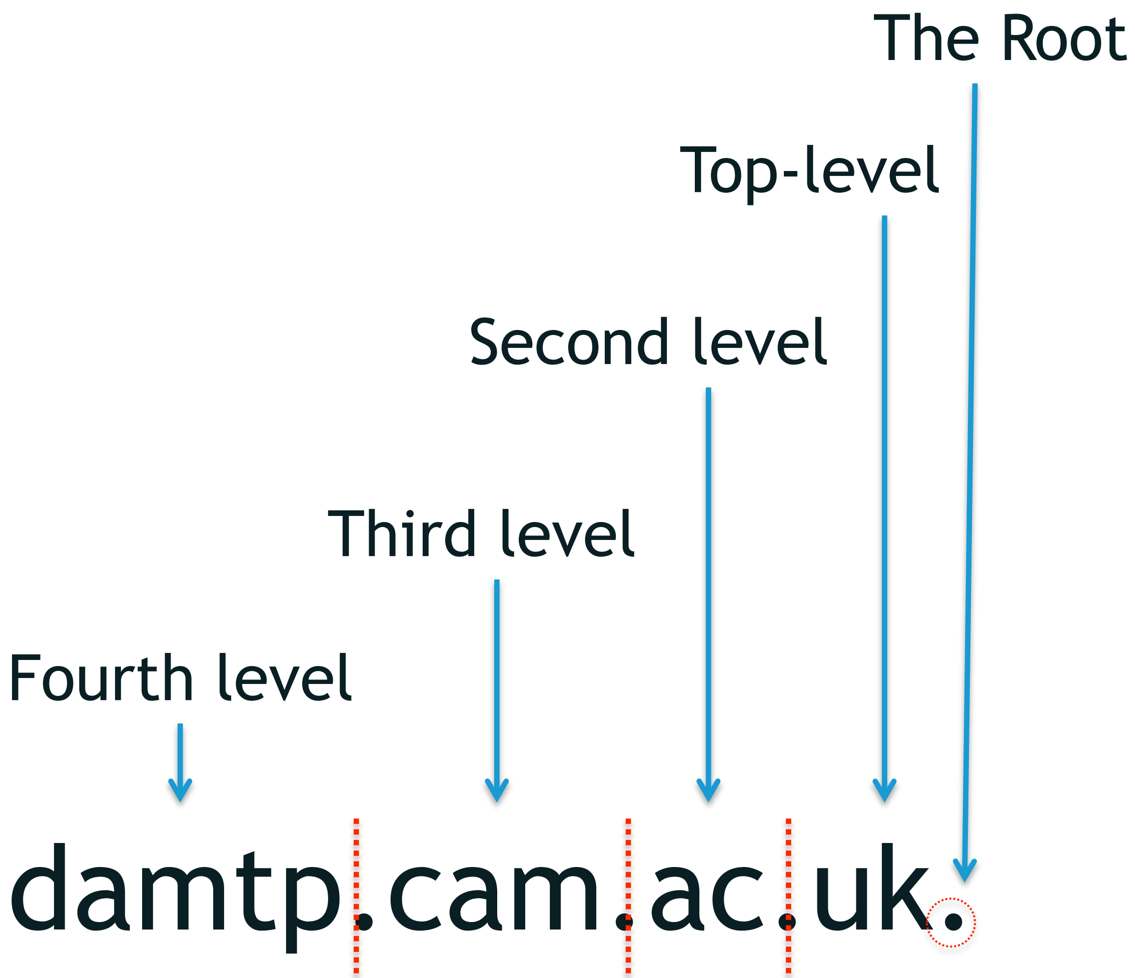
AVAILABLE IPv4 /8s IN EACH RIR

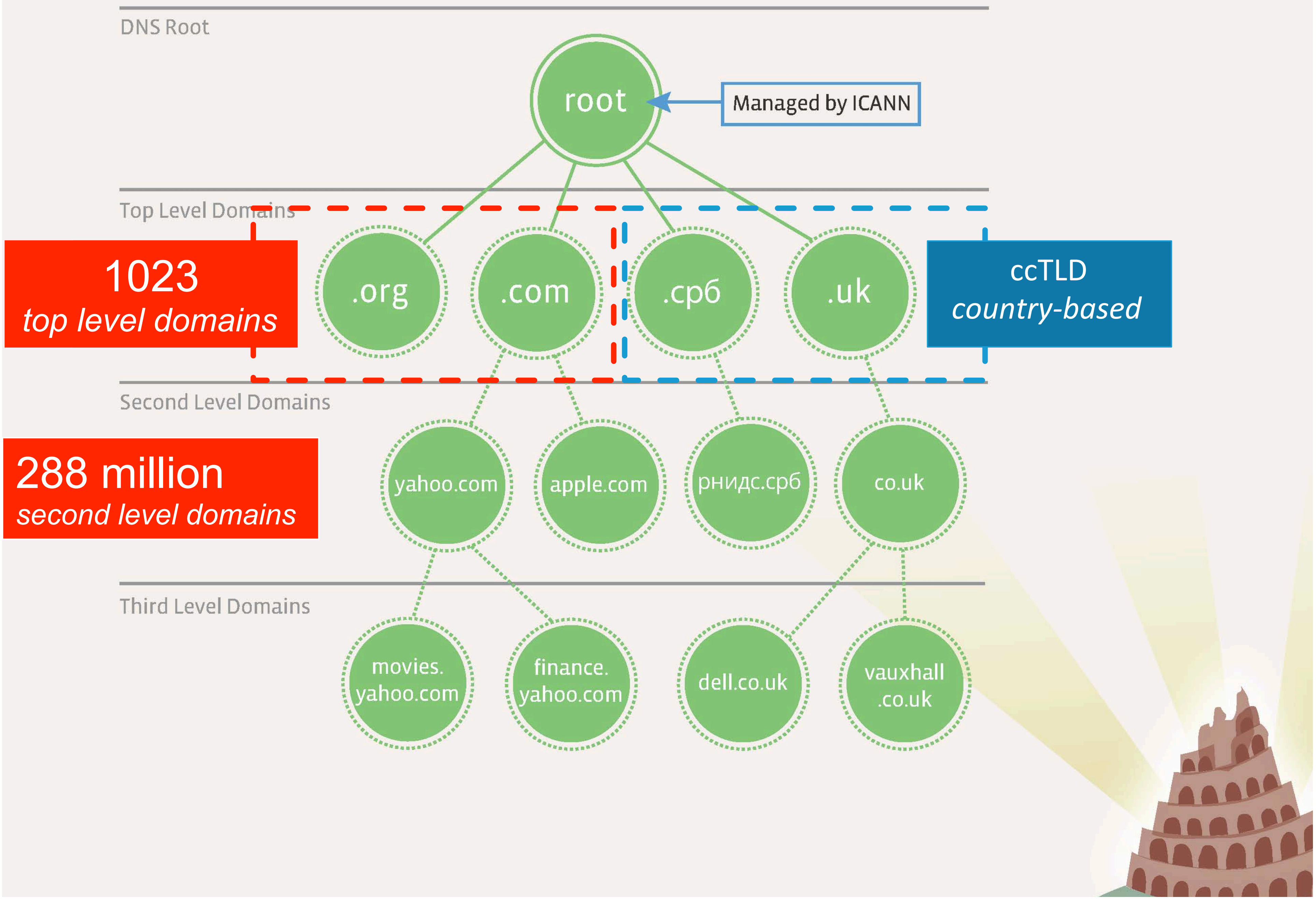


March 2015

Introduction to Domain Names, Registries and Registrars

Domain Name's Structure





DNS Root

root

Managed by ICANN

Top Level Domains

1023
top level domains

.org

.com

.срб

.uk

ccTLD
country-based

Second Level Domains

288 million
second level domains

yahoo.com

apple.com

рнидс.срб

co.uk

Third Level Domains

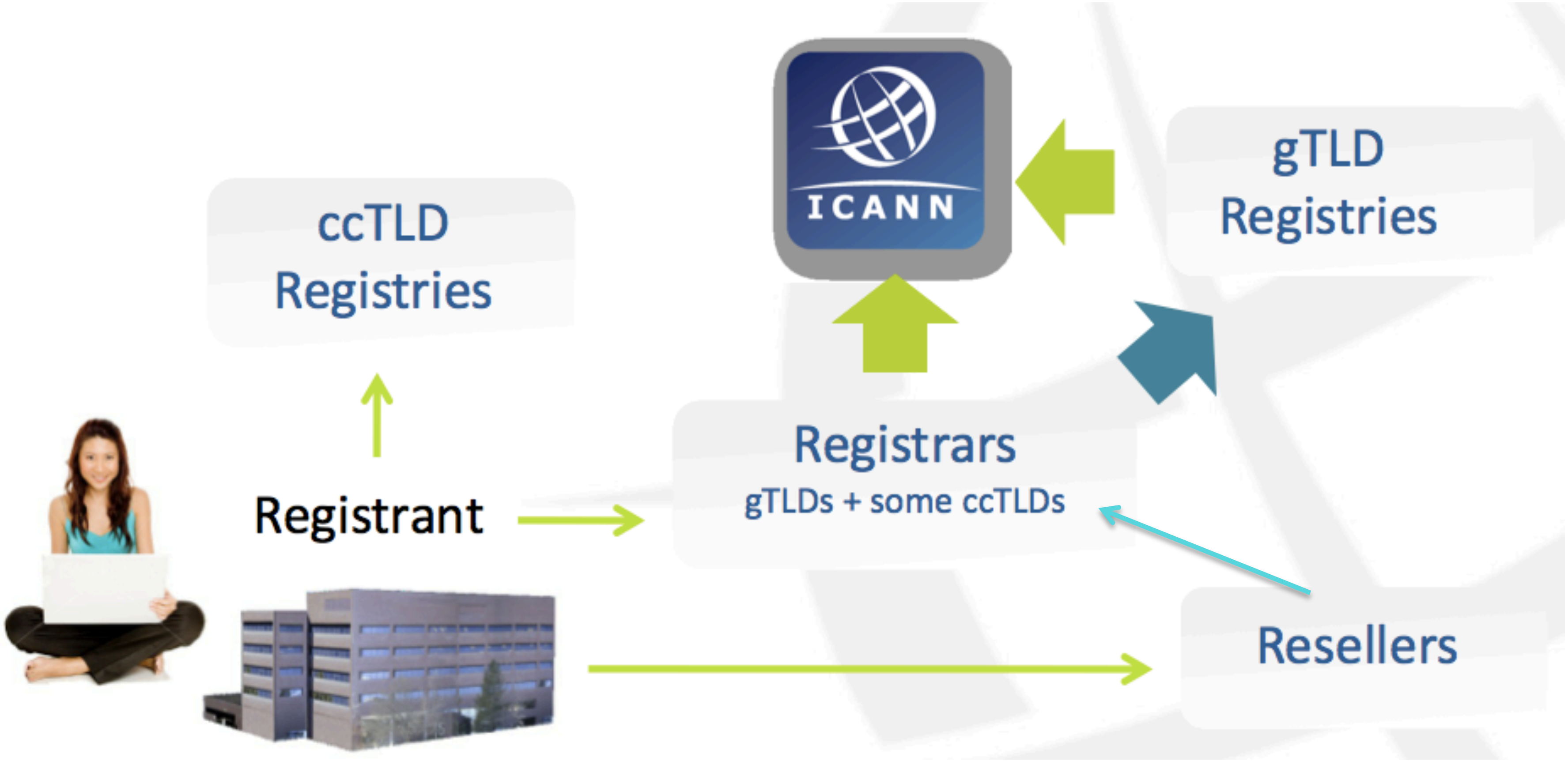
movies.
yahoo.com

finance.
yahoo.com

dell.co.uk

vauxhall
.co.uk

The Registry/Registrar Ecosystem



Registrant

- Individual or Organization seeking to have presence on the Internet
- Is the customer in the provision chain of the domain name industry
- Is the service provider to Internet users (selling goods/services, publishing, etc.)

Registrar

- Many TLDs can be registered through many different Registrars
- Market and compete against one and other
- Interact directly with Registrants and are the “point-of-sale”

Registry

- Authoritative master database of all domain names registered in the TLD
- Exactly one per TLD
- Offers a Shared Registration System (SRS) for the TLD
- Generate zone file for the TLD

Internet User

- Outside the provision model of the domain name industry
- Interested on goods/services offered through the Internet
- Billions of users around the world

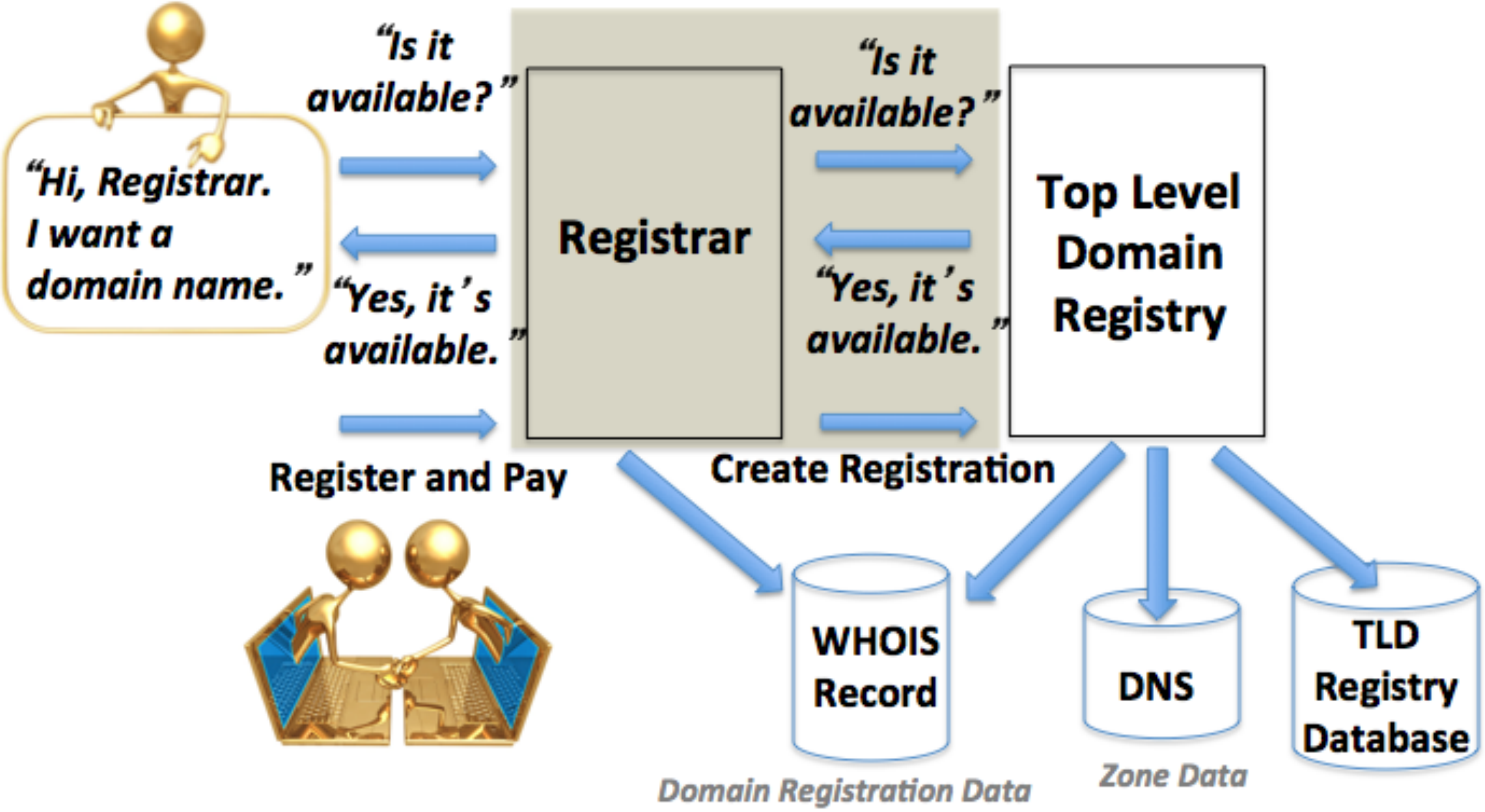
Reseller

- Some registrars use them as their actual point of contact with the registrant
- They are an agent of their respective registrar

Privacy Proxy

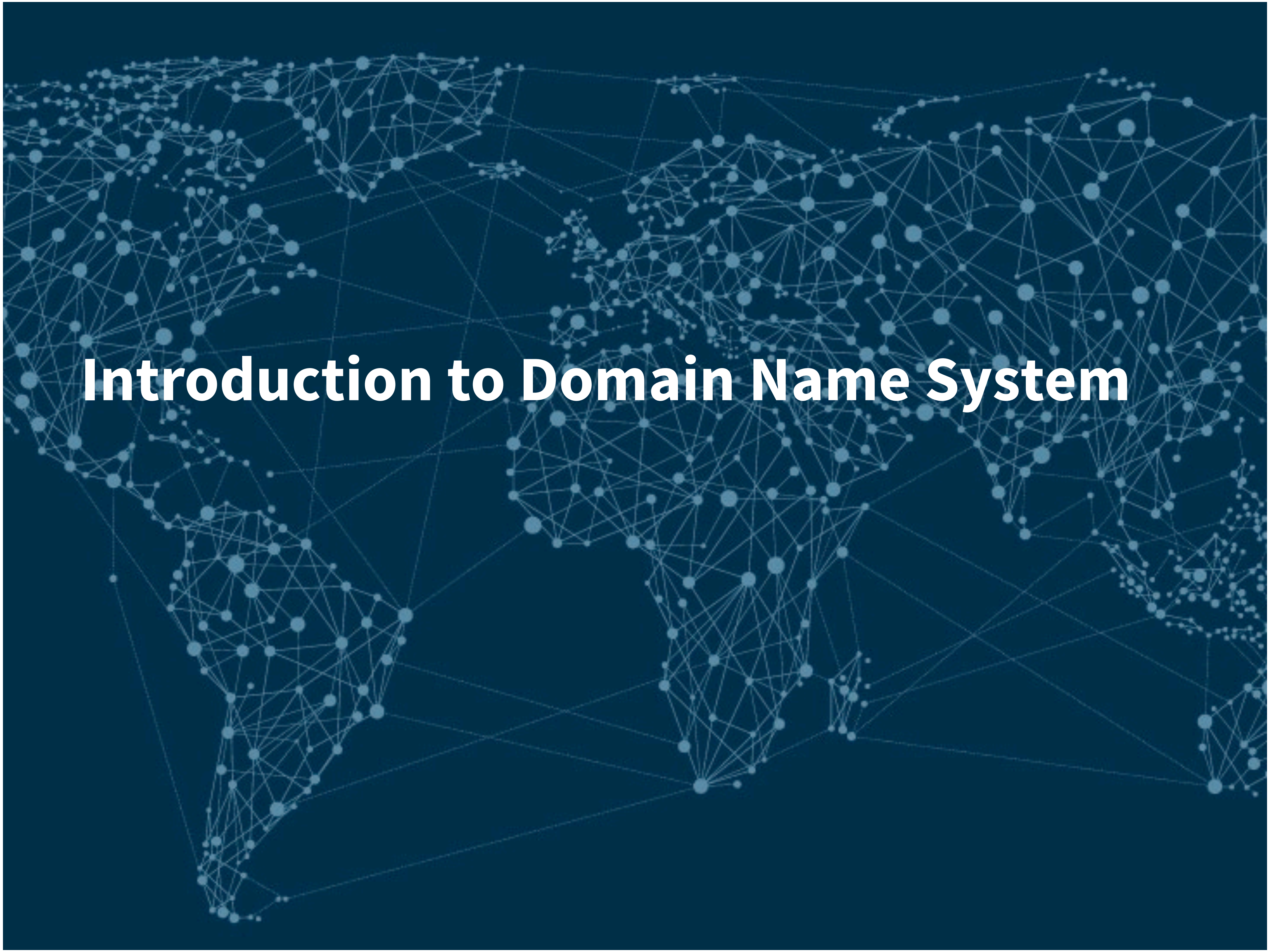
- A third party appearing as the registrant in registration data
- Either offered by the registrar or contracted independently by the registrant
- Ongoing Policy Development Progress on potential accreditation

Domain name registration process



ICANN’s operational role

- Establishes Registries
- Accredits Registrars
- Ongoing compliance activities
- Performance monitoring
- Emergency transition



Introduction to Domain Name System

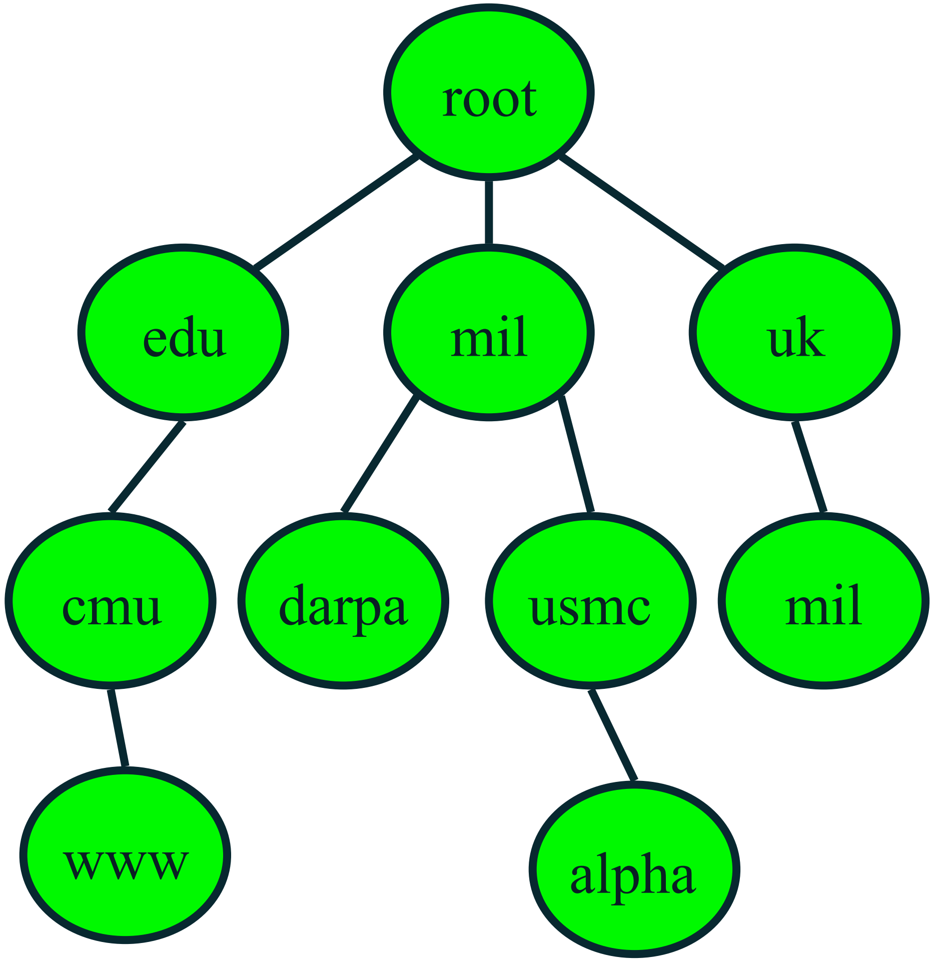
Recap: Identifiers on the Internet

- The fundamental identifier on the internet is an IP address.
- Each host connected to the Internet has a unique IP address
- IPv4 or IPv6 (128.2.42.52, 2607:fb28::4)
- Uniqueness guaranteed through allocation from on single pool (IANA-RIR system)

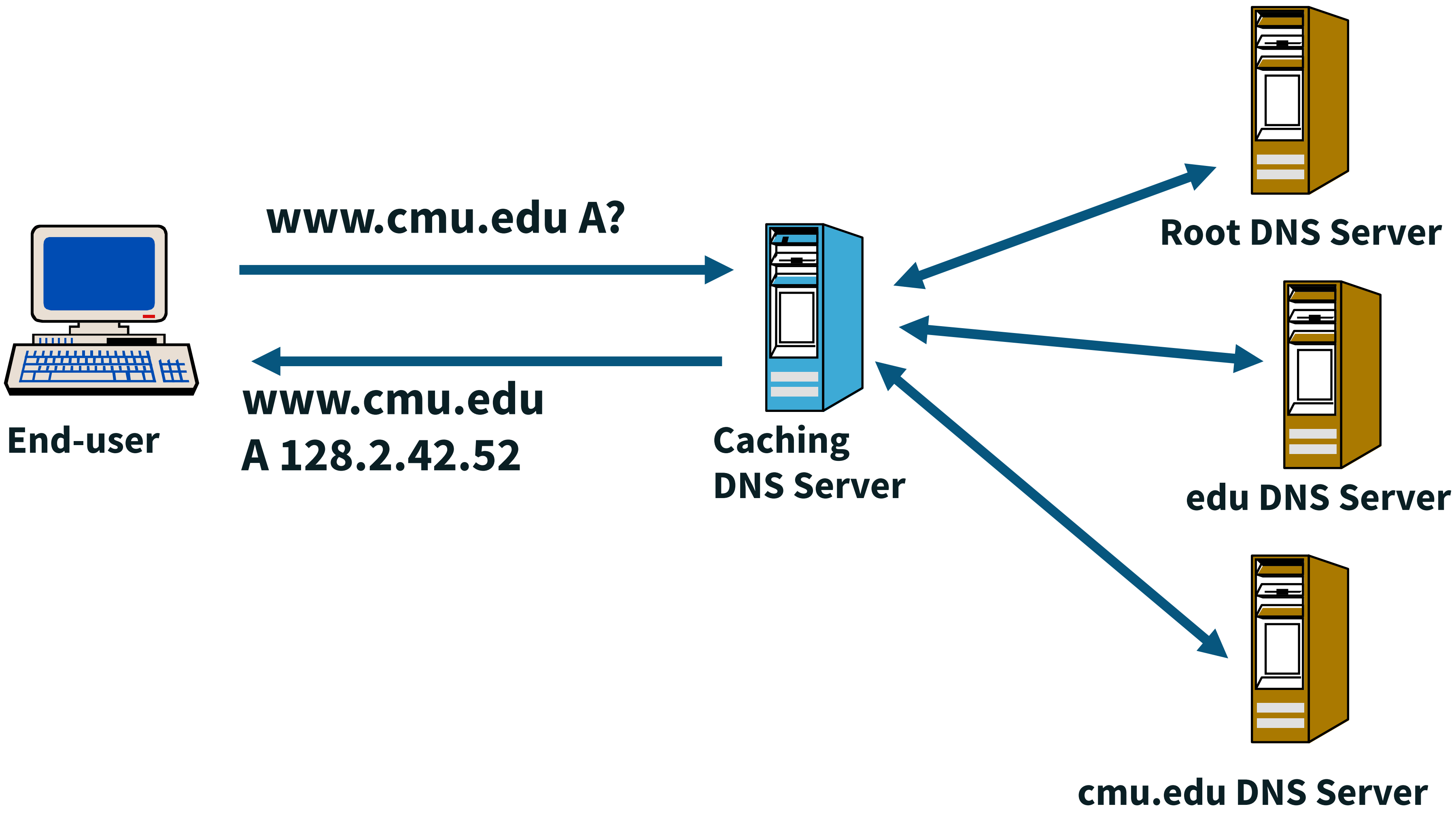
- PROBLEM: These numbers are hard to remember, and often changes

The Domain Name System

- A look up mechanism for translating objects into other objects:
  - Name to IP address www.cmu.edu = 128.2.42.52
  - And many other mappings (mail servers, IPv6, reverse…)
- Globally distributed, loosely coherent, scalable reliable, dynamic database



Domain Name Resolution Process



End-user

www.cmu.edu A?

www.cmu.edu
A 128.2.42.52

Caching
DNS Server

Root DNS Server

edu DNS Server

cmu.edu DNS Server

Four Components of DNS

- A “name space”
- Servers making namespace available
- Resolvers (clients) query the server about the namespace
- The DNS protocol

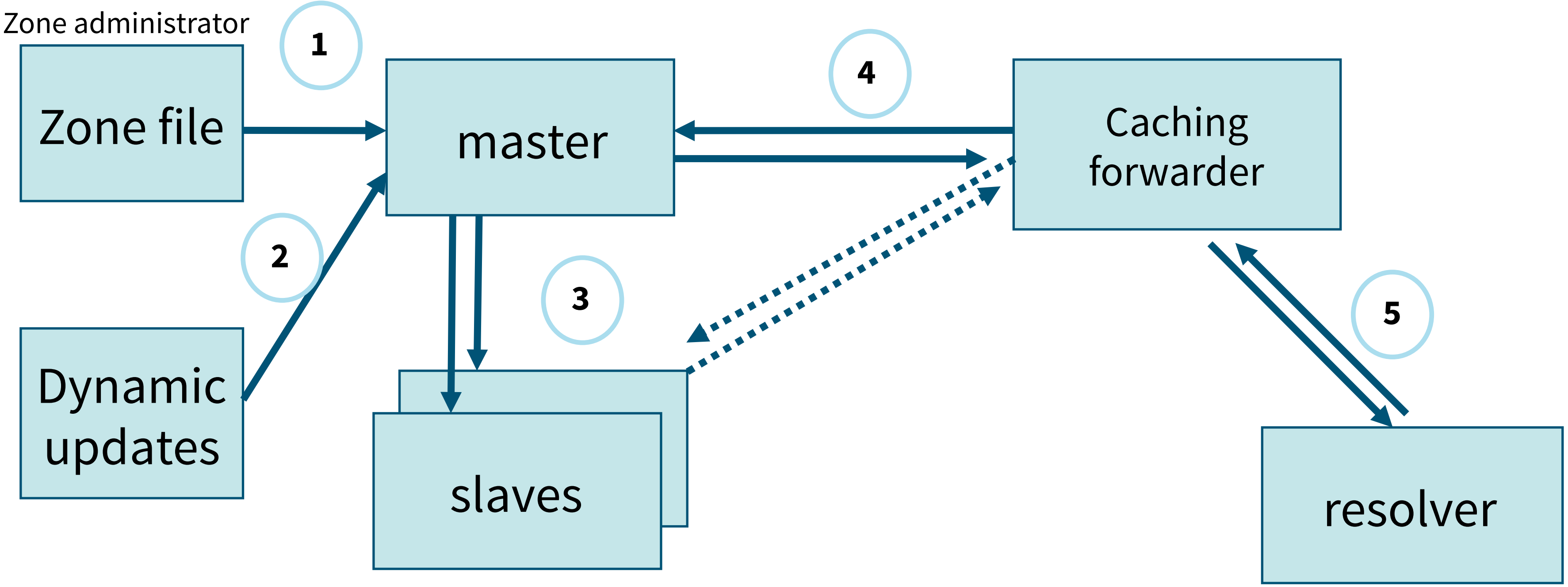
DNS – Some Numbers

- ~ 10^6 authoritative DNS servers around the world
- 3 – 10 DNS looks ups on an average web page load
- ~ 2 trillion queries / day

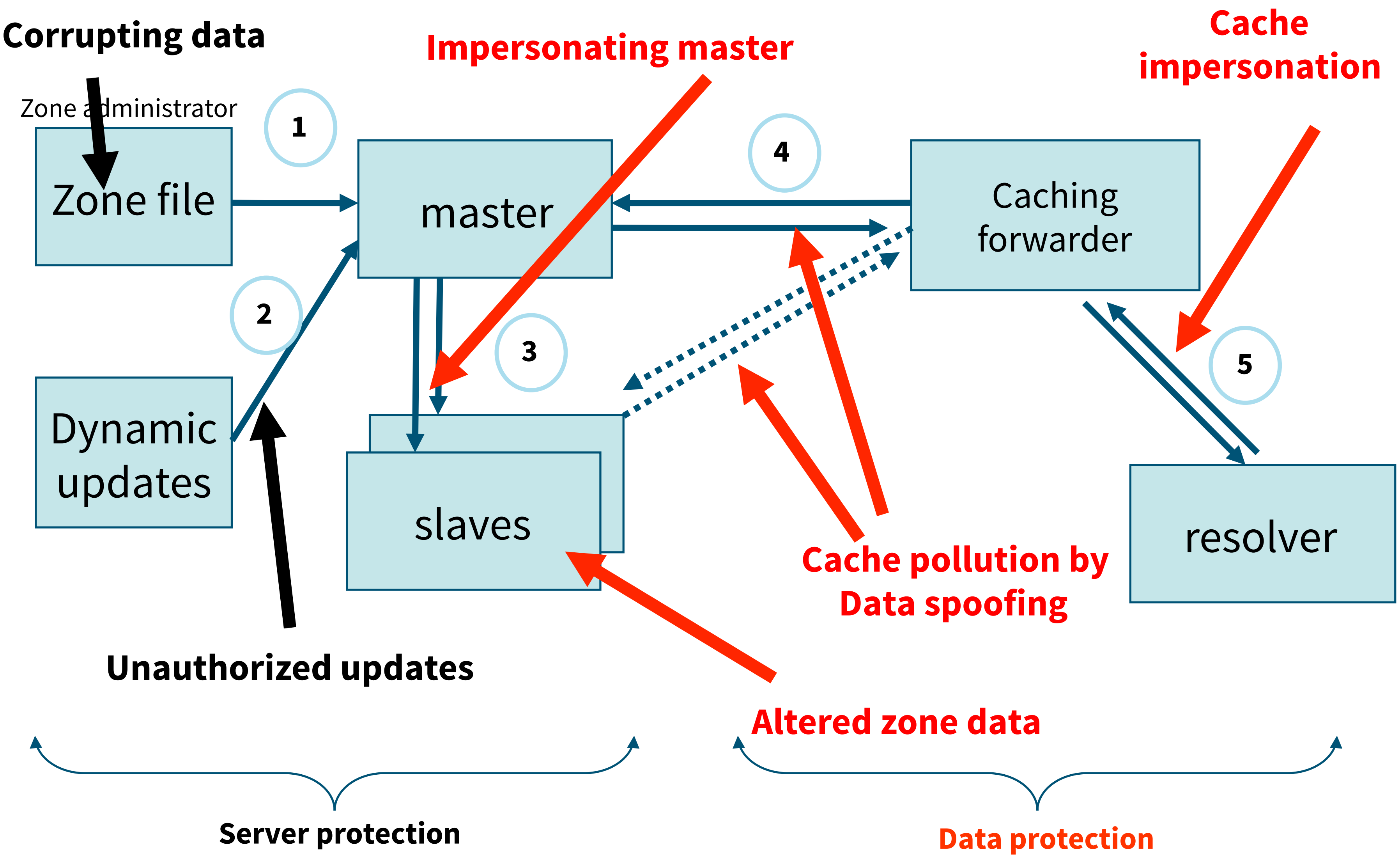
Domain name system is fundamental to the Internet.

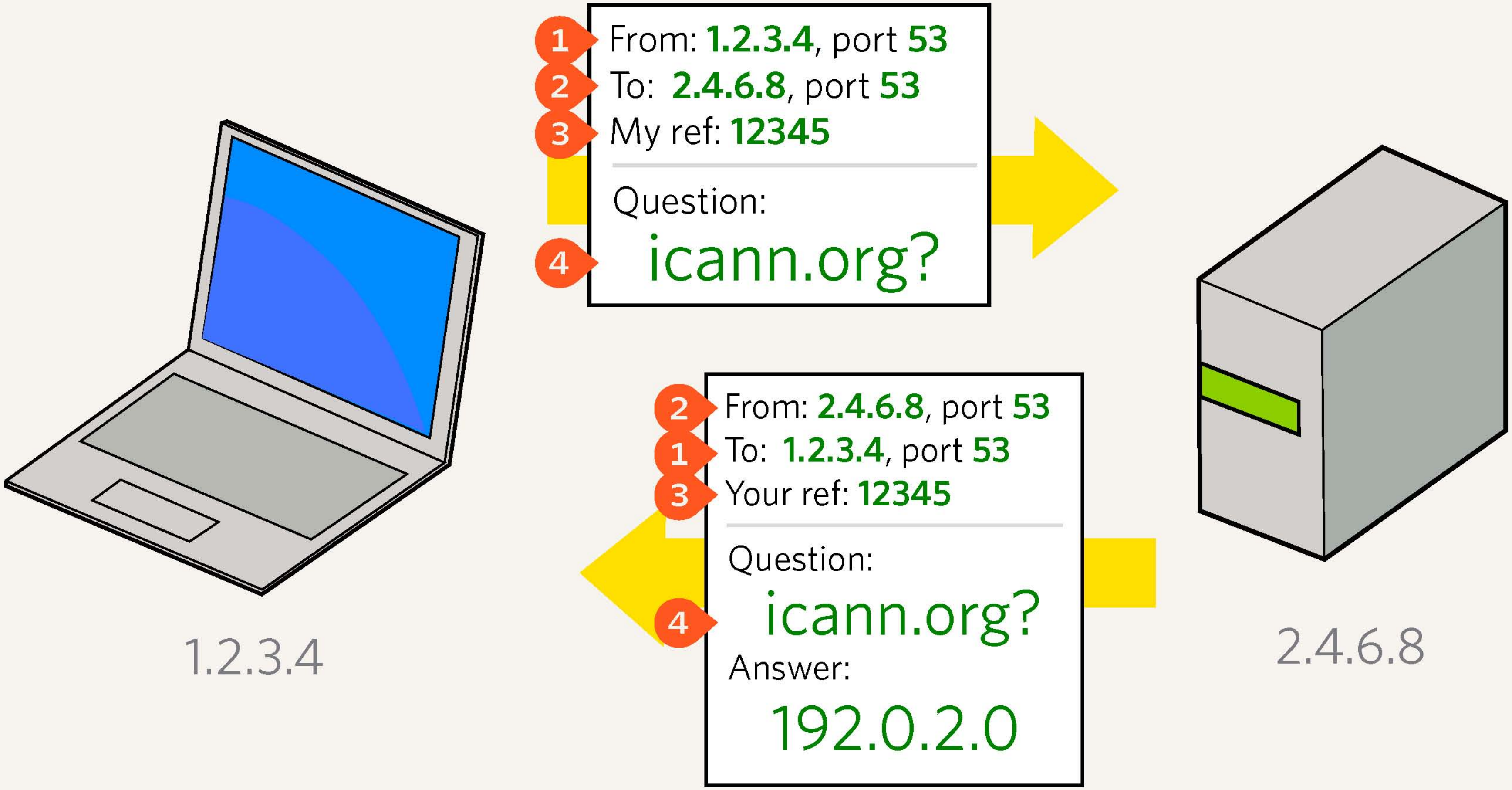
DNS Security and Privacy

DNS: Data Flow



DNS Vulnerabilities





1 From: 1.2.3.4, port 53
2 To: 2.4.6.8, port 53
3 My ref: 12345

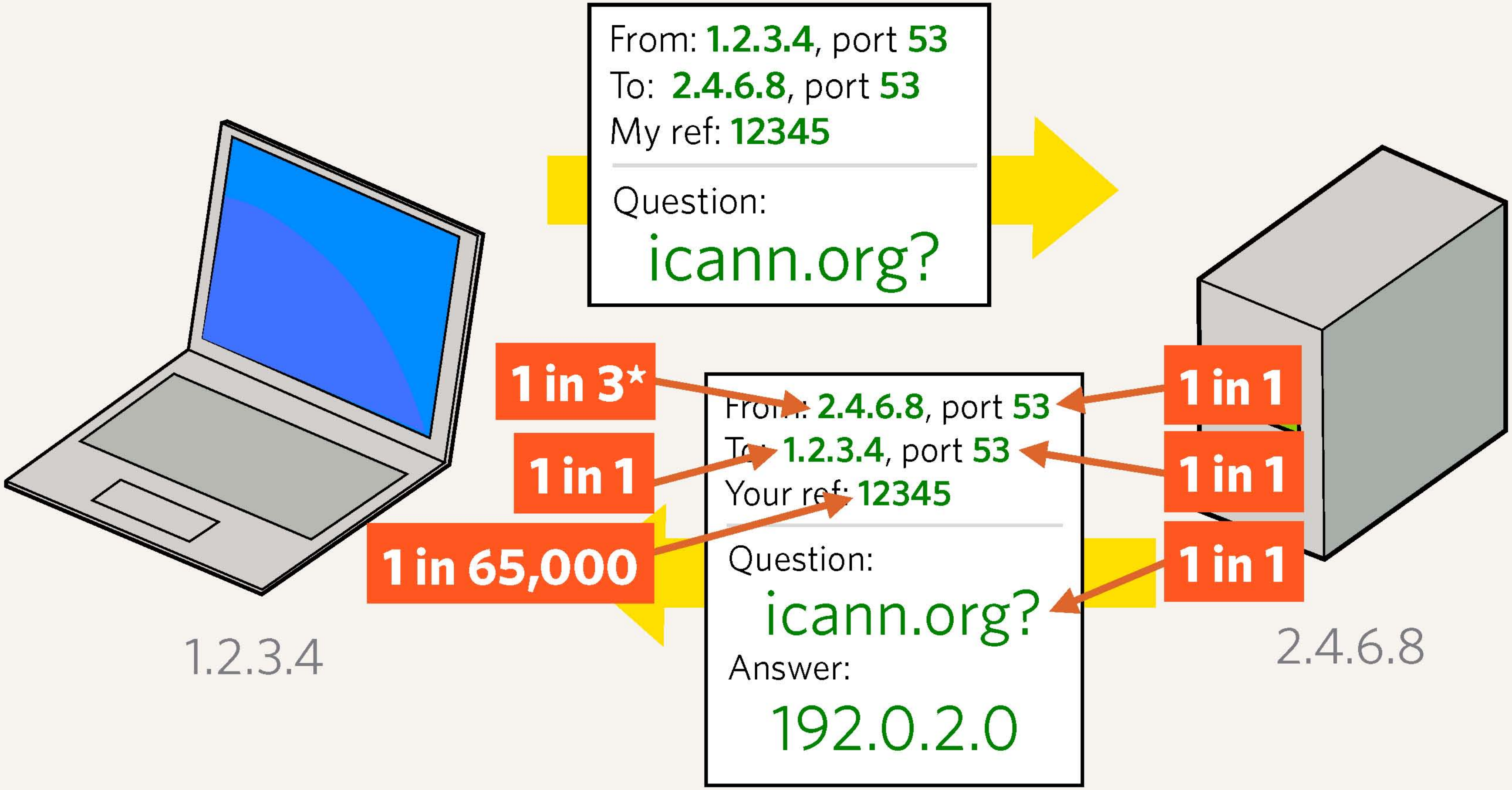
Question:
4 icann.org?

2 From: 2.4.6.8, port 53
1 To: 1.2.3.4, port 53
3 Your ref: 12345

Question:
4 icann.org?
Answer:
192.0.2.0

What should match in a DNS transaction

① Source address and port ② Destination address and port
③ Reference (Transaction) number ④ Question being asked



From: 1.2.3.4, port 53
To: 2.4.6.8, port 53
My ref: 12345

Question:
icann.org?

1 in 3* → From: 2.4.6.8, port 53 ← 1 in 1
1 in 1 → To: 1.2.3.4, port 53 ← 1 in 1
1 in 65,000 → Your ref: 12345

Question:
icann.org? ← 1 in 1
Answer:
192.0.2.0

1.2.3.4

2.4.6.8

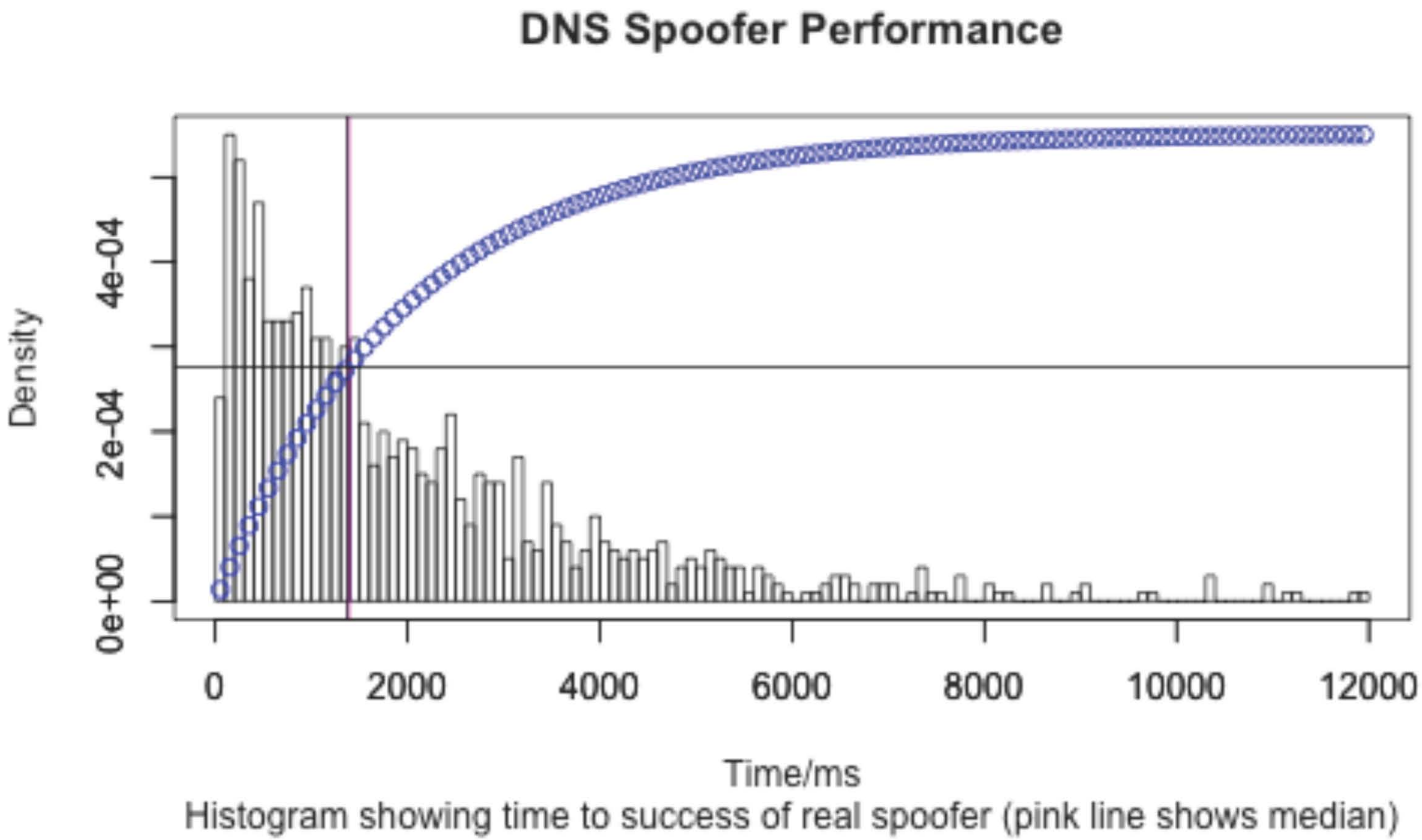
Approximate possible combinations

The key variability is in the reference number. Other values are mostly deterministic.

* Number of authoritative name servers for the domain (average is 2.5)

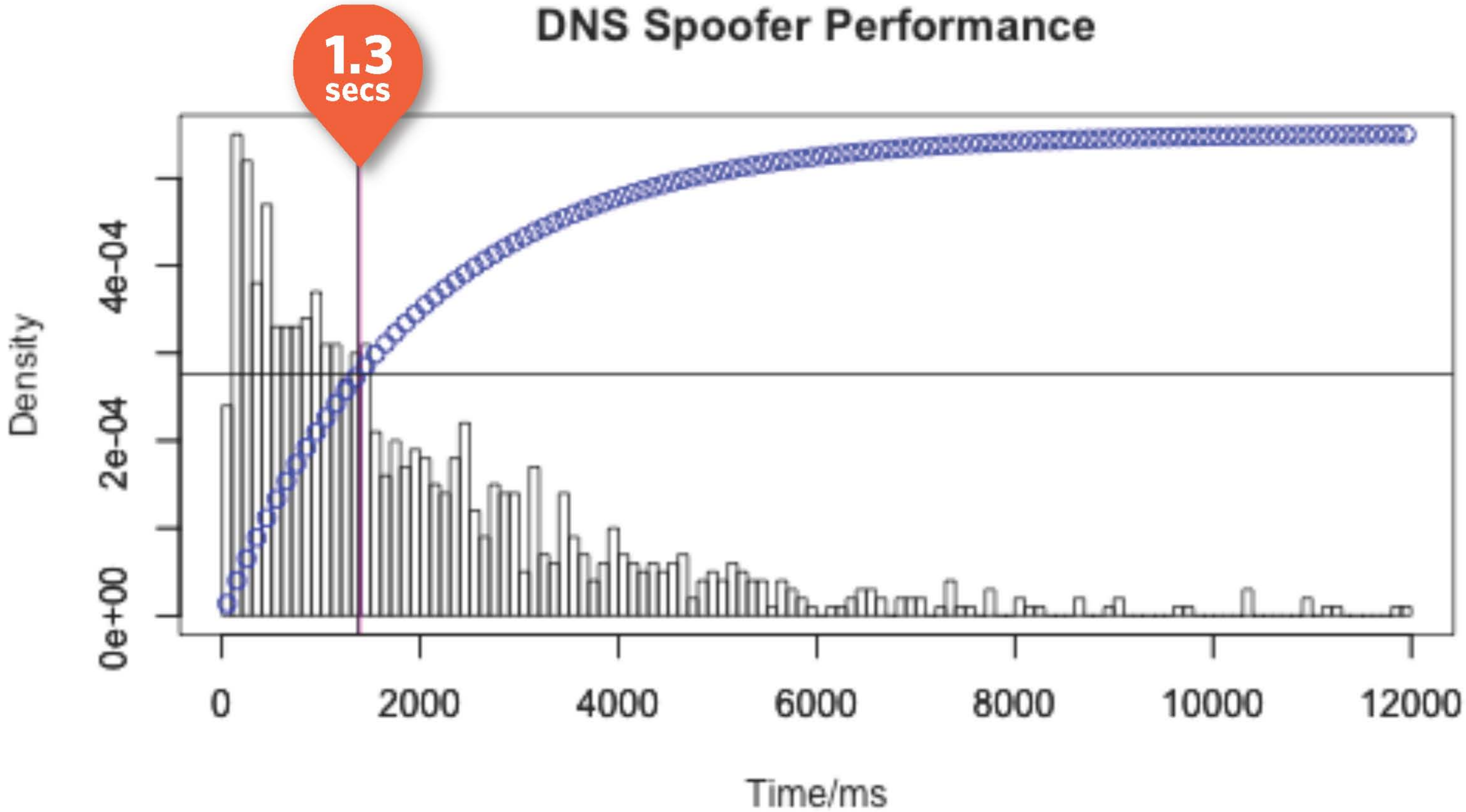
Kaminsky Attack

- Dan Kaminsky identified there is a straightforward way to flood an attack target with lots of answers, so that the right combination could be found quickly (within seconds)
- By querying for random hosts within a domain (0001.targetdomain.com, 0002.targetdomain.com, etc.), you can take over the target domain by filling the cache with bad referral information.



How effective?

Courtesy John Dickinson (jadickinson.co.uk)



Histogram showing time to success of real spoofer (pink line shows median)

How effective?

Courtesy John Dickinson (jadickinson.co.uk)

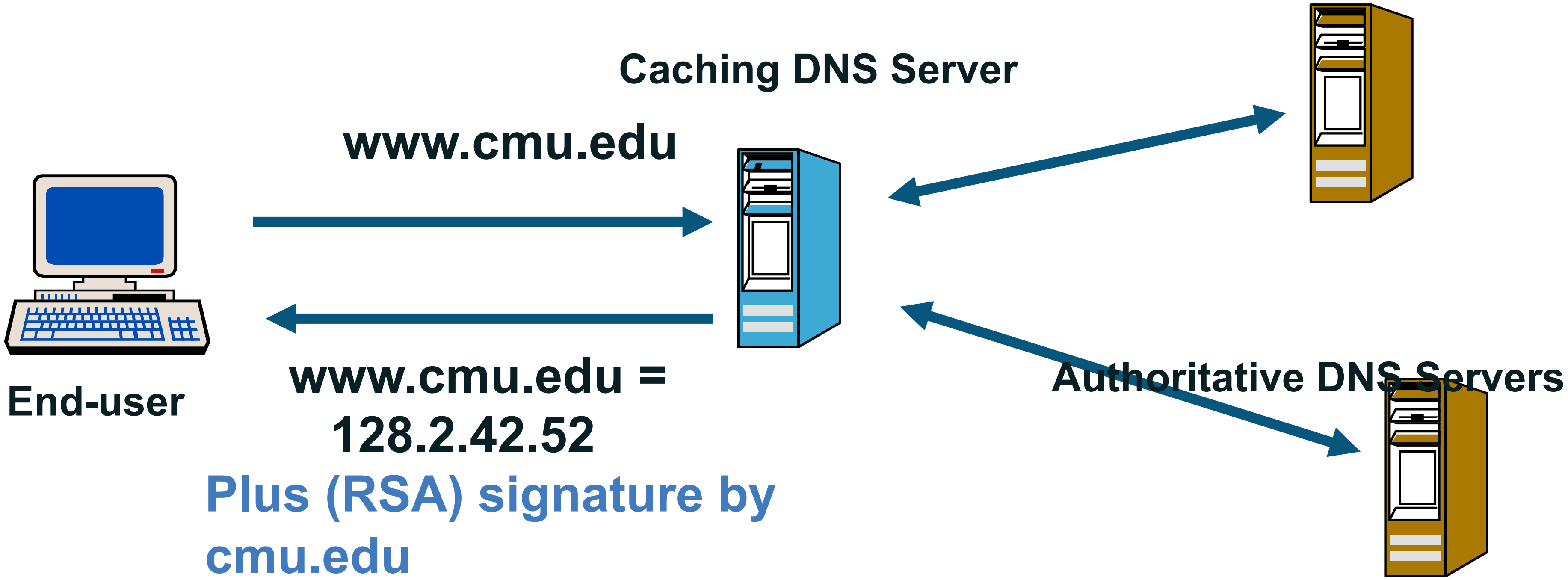
DNS Security Extensions

- Uses public key cryptography to verify the authenticity of DNS zone data (records)
  - DNSSEC zone data is digitally signed using a *private key for that zone*
  - A DNS server receiving DNSSEC signed zone data can verify the origin and integrity of the data by checking the signature using the *public key for that* Zone

Authentication DNS Responses

- Each DNS zone signs its data using a private key.
  - Recommend signing done offline in advance
- Query for a particular record returns:
  - The requested resource record set.
  - A signature (SIG) of the requested resource record set.
- Resolver authenticates response using public key.
  - Public key is pre-configured or learned via a sequence of key records in the DNS hierarchy.

Secure DNS Query and Response



Caching DNS Server

www.cmu.edu

End-user

www.cmu.edu = 128.2.42.52

Authoritative DNS Servers

Plus (RSA) signature by cmu.edu

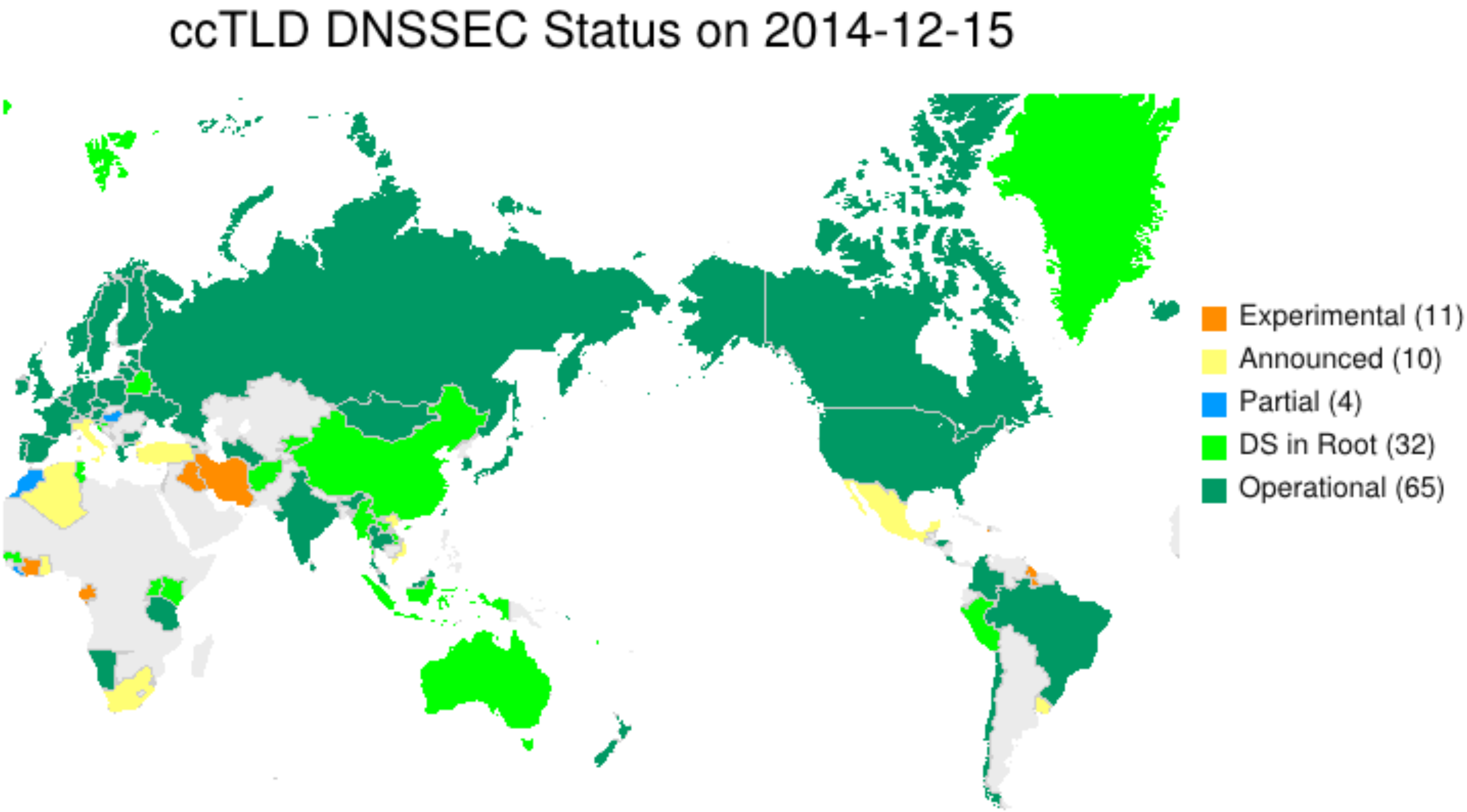
Attacker can not forge this answer without the cmu.edu private key.

DNSSEC RFCs define the process for including signatures and keys in DNS

What DNSSEC does and doesn’t do

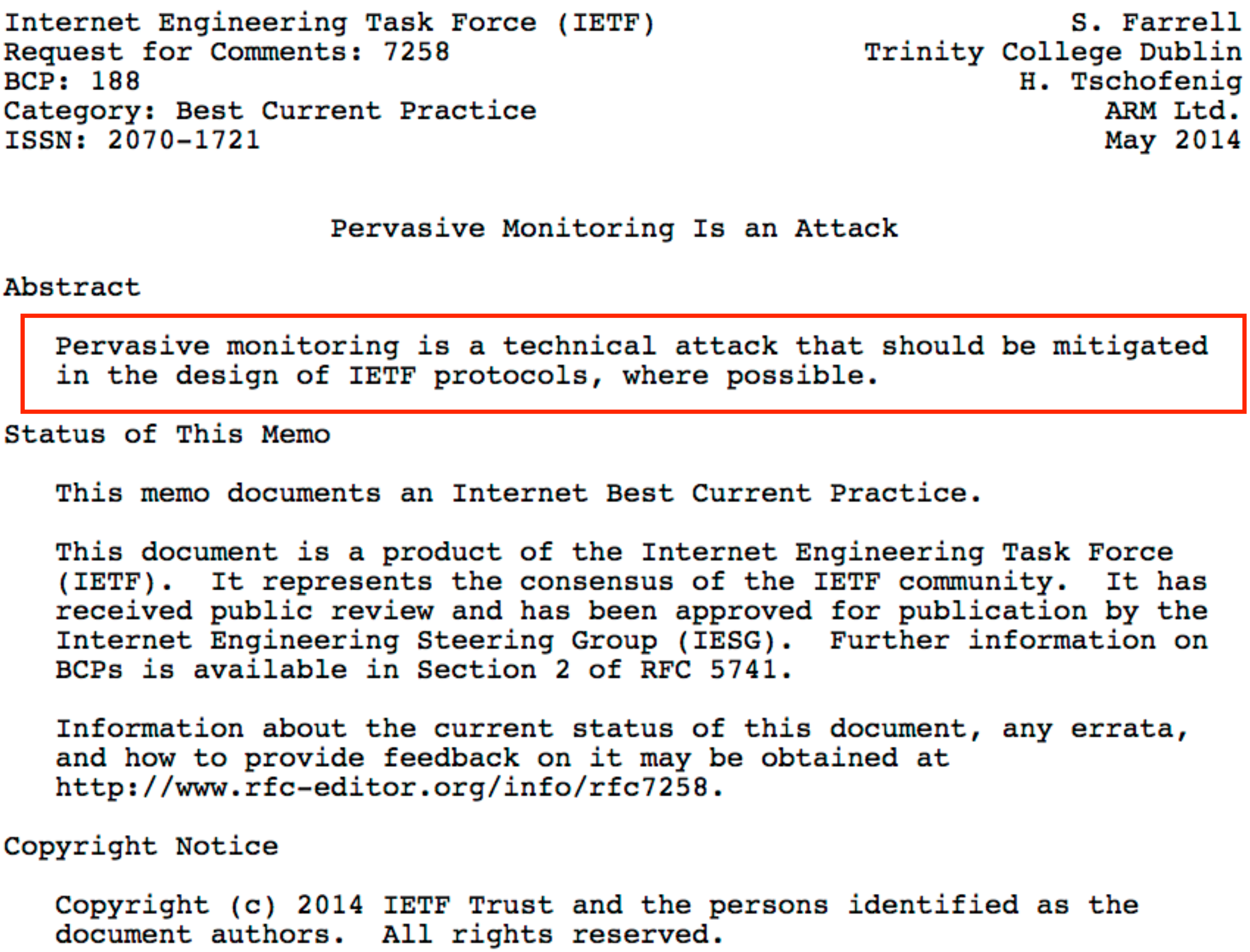
- Does not do
  - Protect against host threats (DDoS, buffer overruns in code, etc.)
  - Keep DNS data private
  - Ensure correctness of DNS data
- Does Do: Establish the legitimacy of data retrieved from the DNS
  - Protects end users from being redirected to malicious sites
  - Allows *any data stored in the DNS to be* validated as trustworthy

DNSSEC Status



DNS Privacy - Context

- Vancouver, November 2013: IETF pledged to “harden the Internet”
- Actual Work, RFC 7258.



Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.
May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 5741.

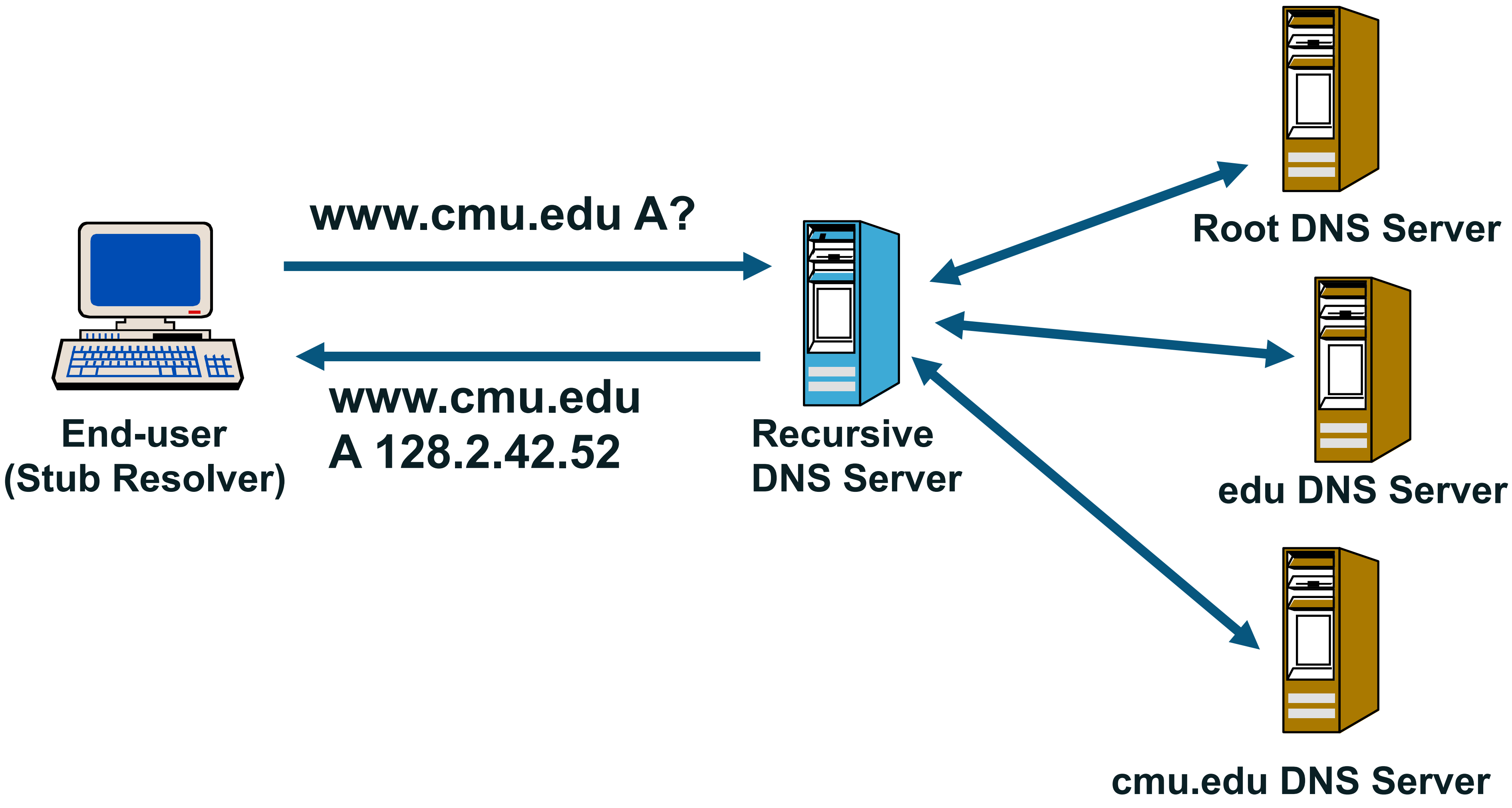
Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7258.

Copyright Notice

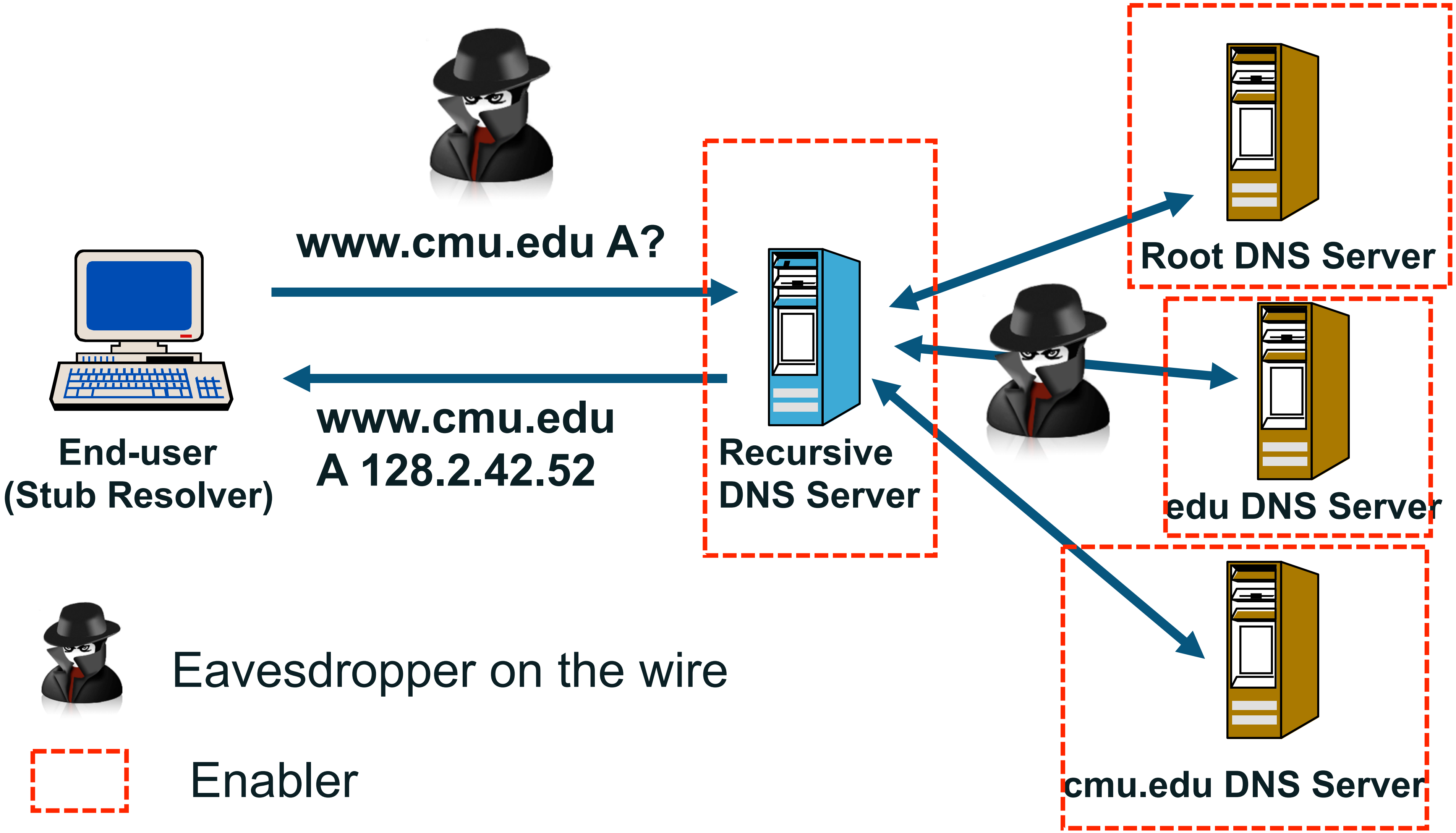
DNS Privacy

- An actual DNS query reveals:
  - Who is requesting?
  - What is requested?
    - www.political-party.example (Sensitive information)
    - _bittorrent-tracker._tcp.domain.example (MPAA may be interested)
    - stevesheng-5561woodmont.domain.example (Personal information)

Who can listen?



Who can listen?



www.cmu.edu A?

www.cmu.edu
A 128.2.42.52

End-user
(Stub Resolver)

Recursive
DNS Server

Root DNS Server

edu DNS Server

cmu.edu DNS Server

Eavesdropper on the wire

Enabler

Two principles of privacy engineering

1. Send as little data as possible (RFC 6973, section 6.1)
2. Encrypt it

IETF Approach

- Minimize the amount of data sent from the DNS resolvers
- Discussing approaches to take to provide confidentiality in the DNS
  - encrypt the query
  - secure the channel

MORE INFORMATION

- Read latest internet drafts (DPRIV, DNSOP)
- Participate in mailing list discussions and IETF meetings