Network Applications: DNS

Y. Richard Yang

http://zoo.cs.yale.edu/classes/cs433/

2/1/2016

Outline

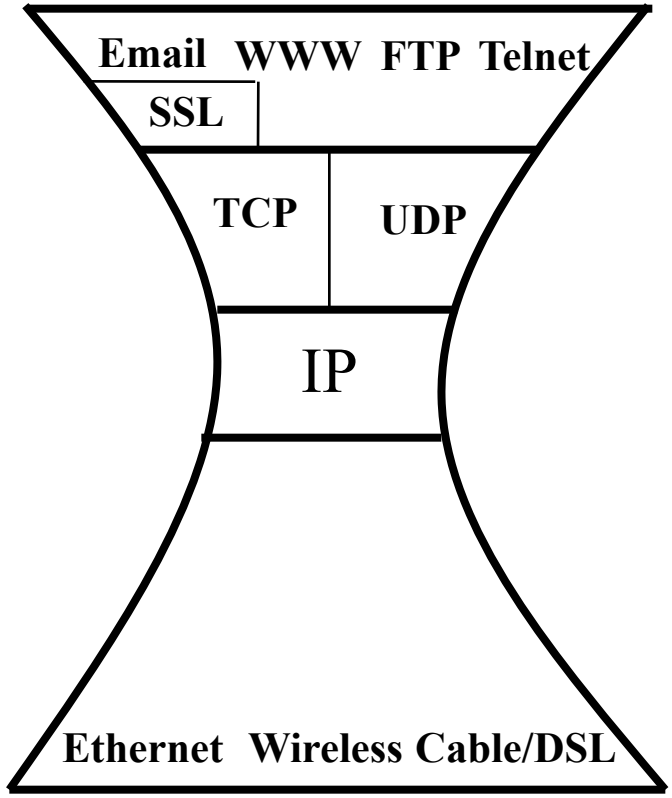
- Admin and recap
- DNS

Admin

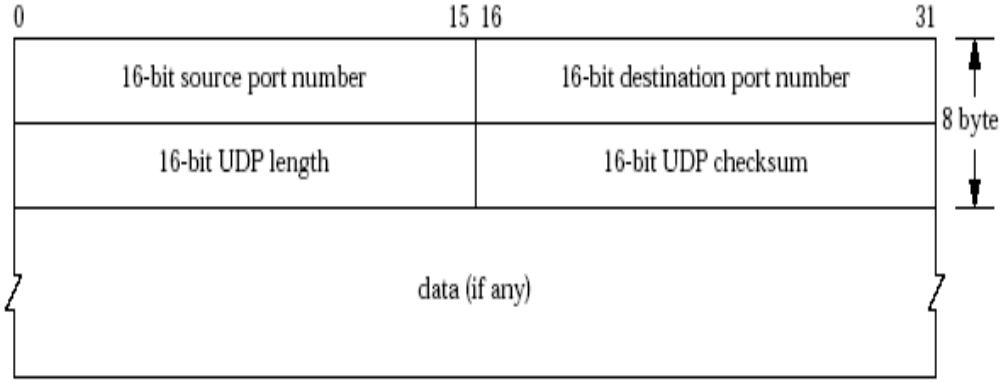
- 72 discretionary late hours for assignments across the semester

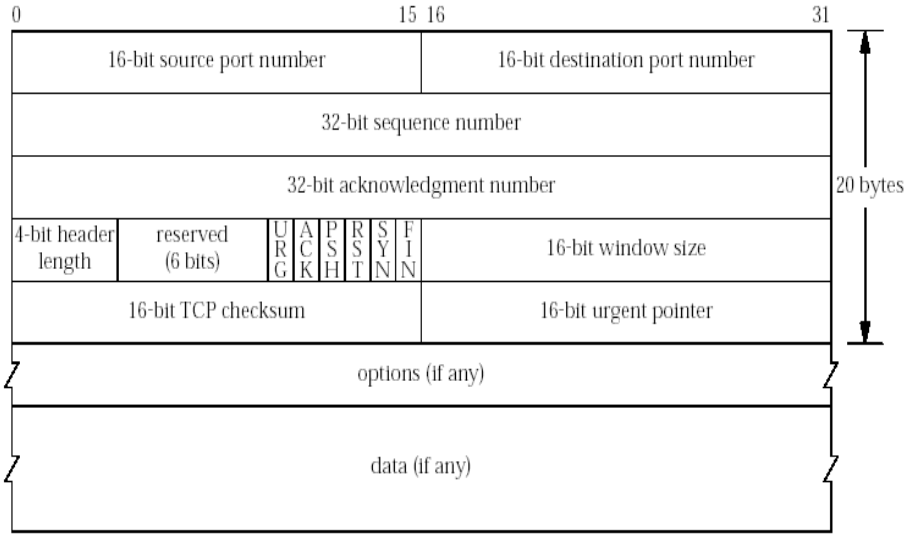
Recap: The Big Picture of the Internet

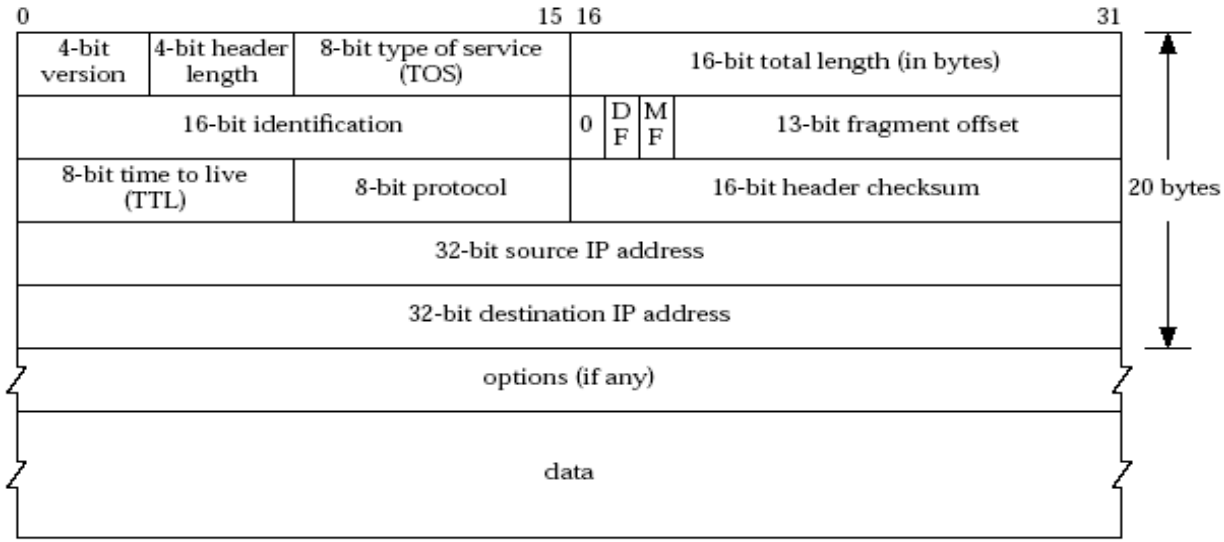
- Hosts and routers:
  - ~ 1 bill. hosts (2015)
  - organized into ~50K networks
  - backbone links 100 Gbps
- Software:
  - datagram switching with virtual circuit support
  - layered network architecture
    - use end-to-end arguments to determine the services provided by each layer
  - the hourglass architecture of the Internet

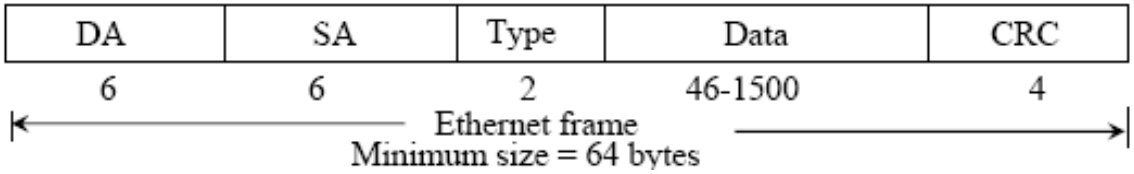


Protocol Formats

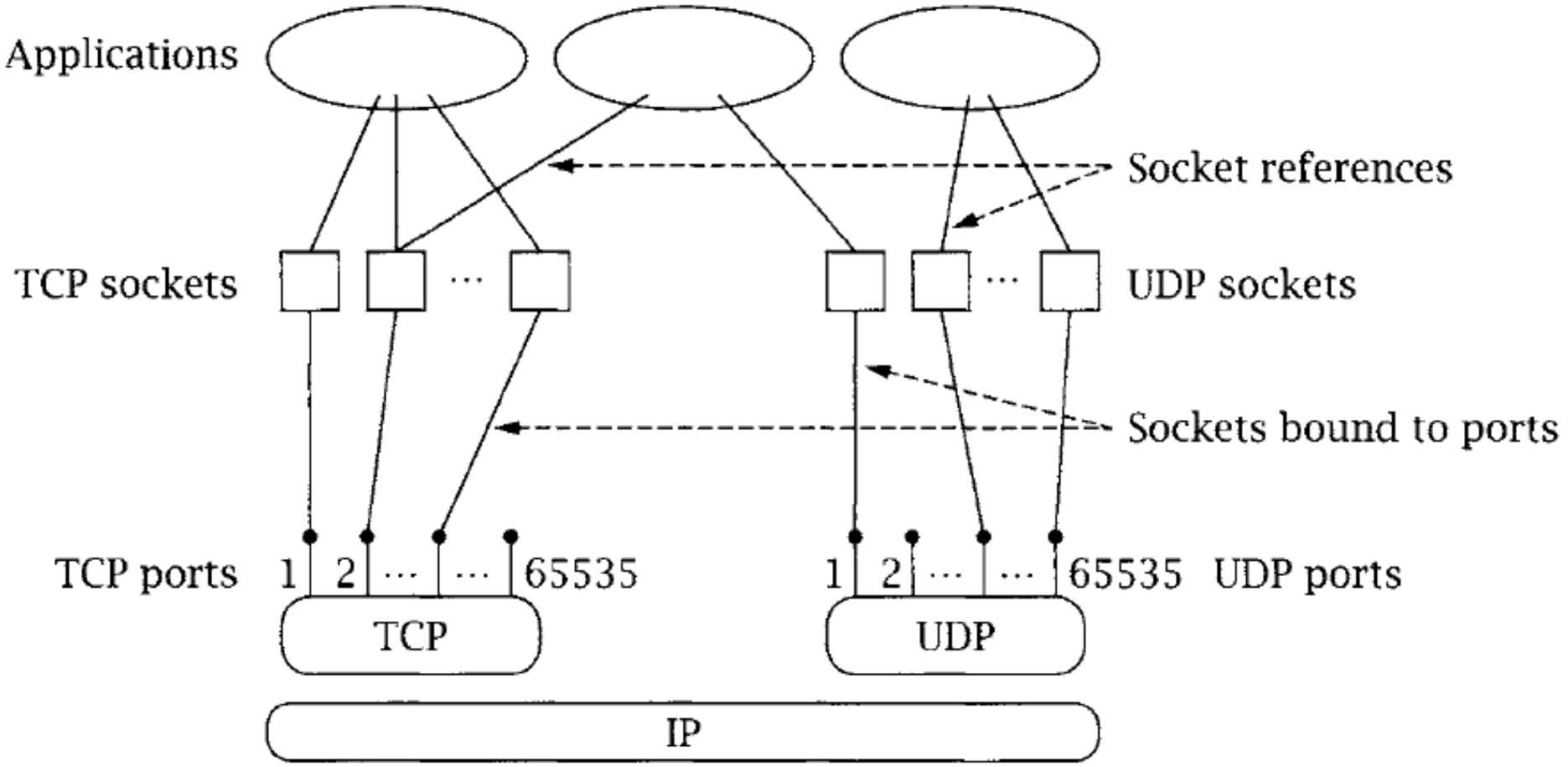








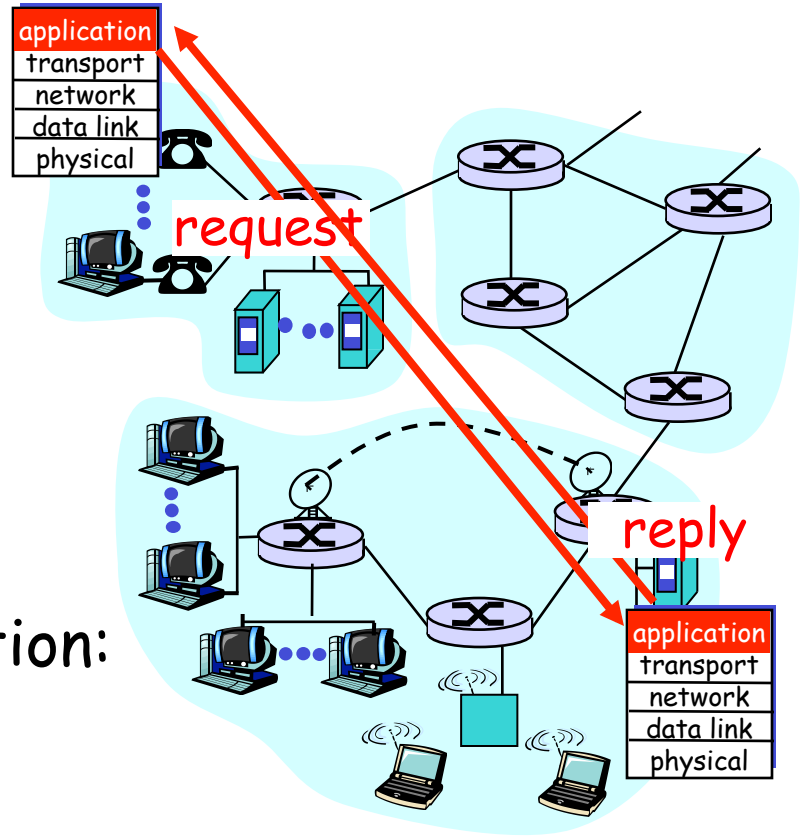
Multiplexing/Demultiplexing



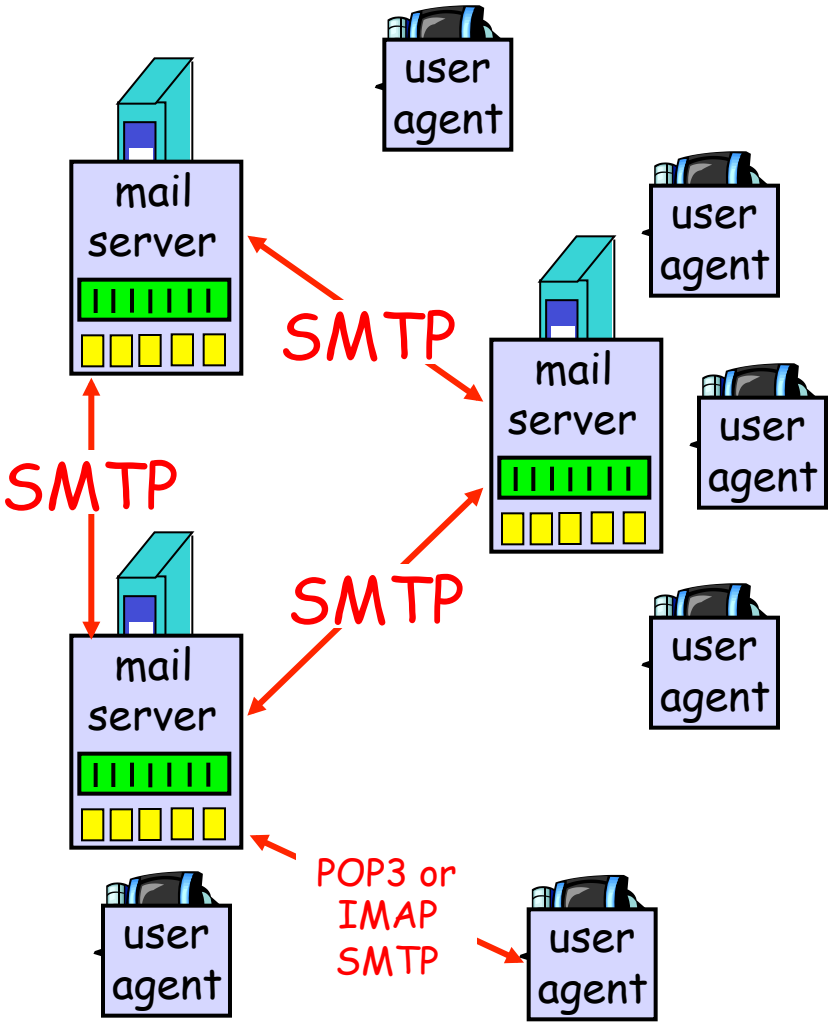
Recap: Client-Server Paradigm

- The basic paradigm of network applications is the client-server (C-S) paradigm

- Some key design questions to ask about a C-S application:
  - extensibility
  - scalability
  - robustness
  - security



Recap: Email App

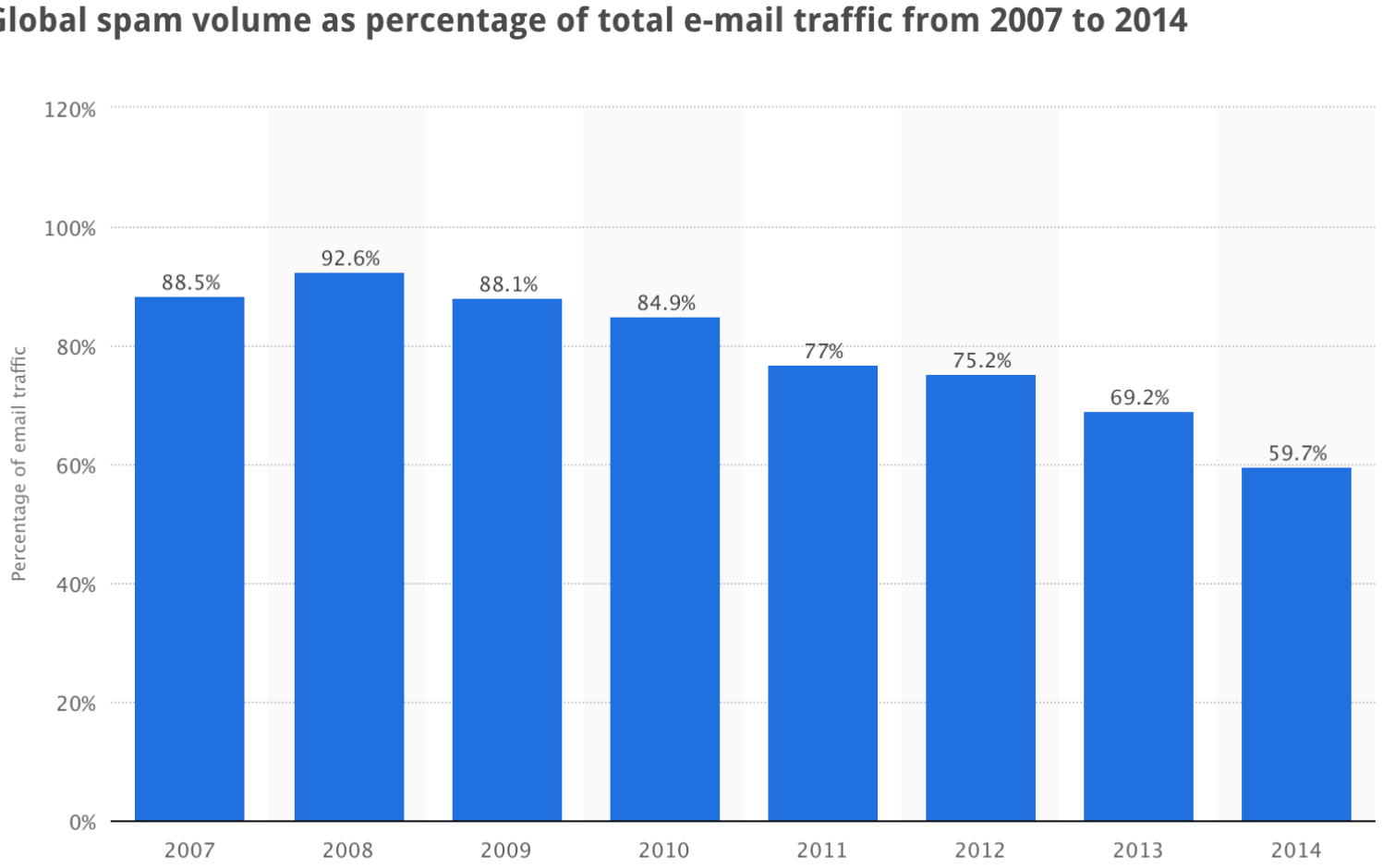


Some nice protocol extensibility design features

- separate protocols for different functions
- simple/basic (smtp) requests to implement basic control; fine-grain control through ASCII header and message body
- status code in response makes message easy to parse

Email: Challenge

- A large percentage of spam/phish



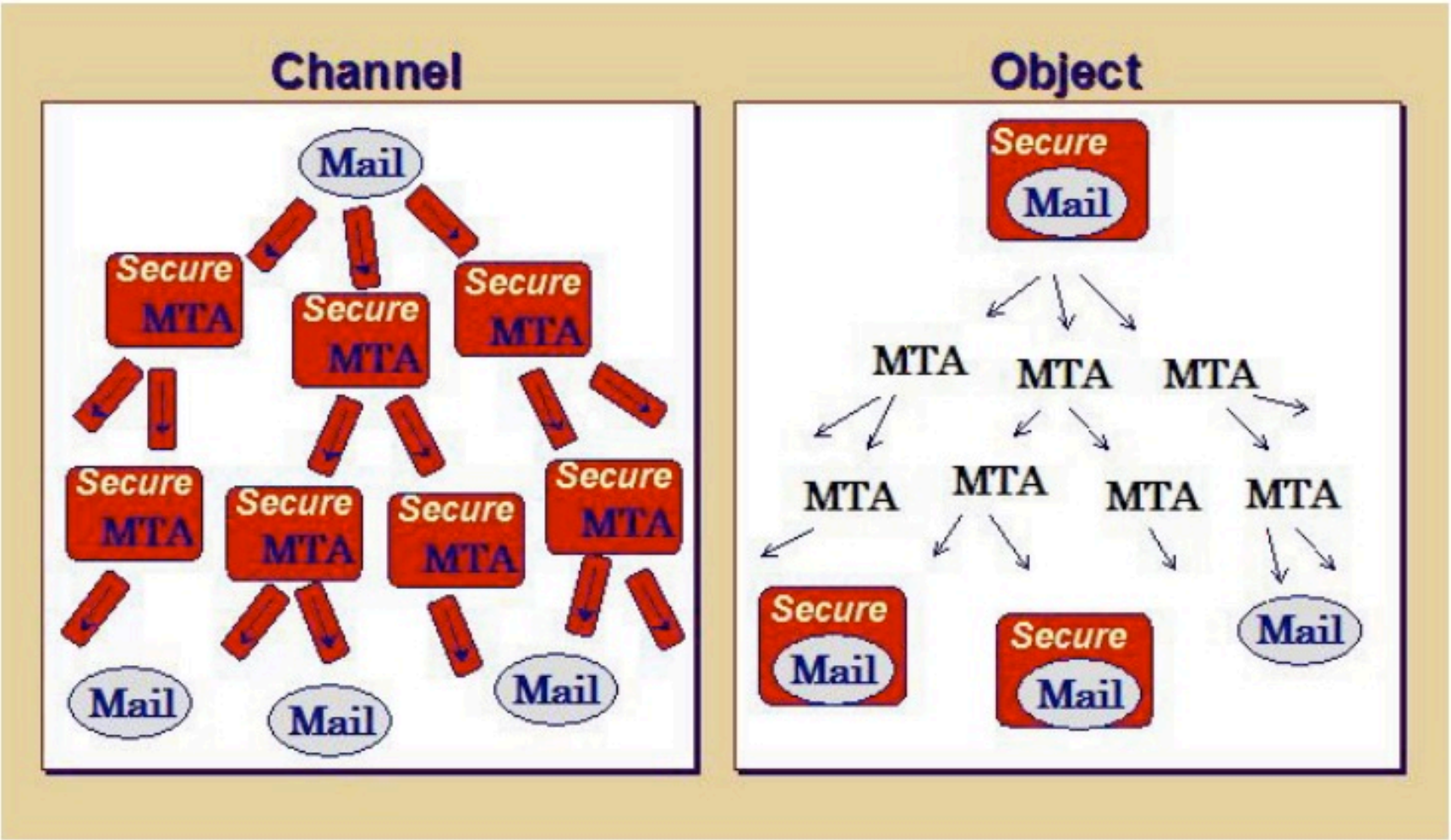
Source: http://www.statista.com/statistics/420400/spam-email-traffic-share-annual/

Recap: Spam Detection Methods by GMail

- Known phishing scams
- Message from unconfirmed sender identity
- Message you sent to Spam/similarity to suspicious messages
- Administrator-set policies
- Empty message content

https://support.google.com/mail/answer/1366858?hl=en

Current Email Authentication Approaches

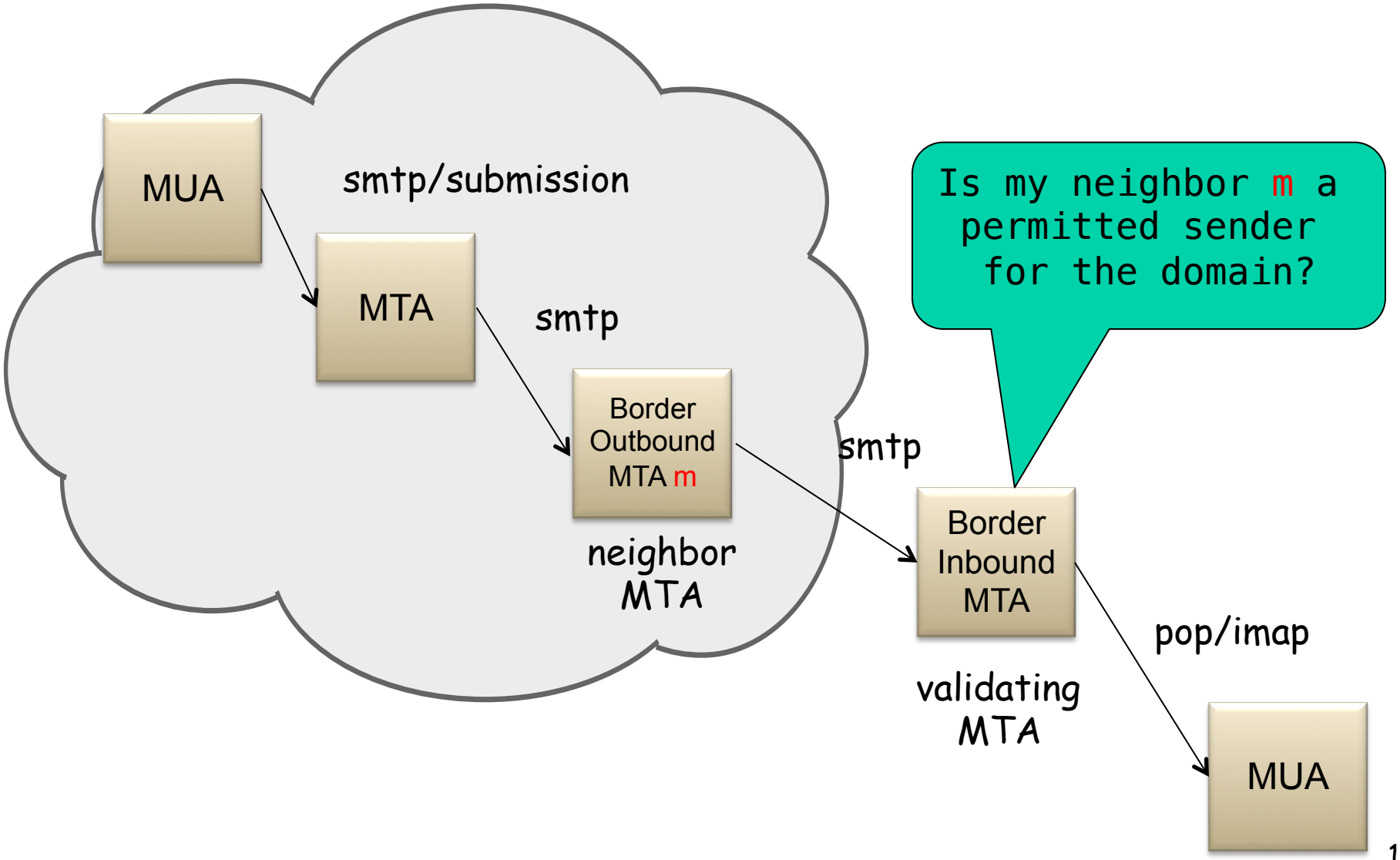


Sender Policy Frame (SPF)

DomainKeys Identified Mail (DKIM)

https://tools.ietf.org/html/rfc7208

Sender Policy Framework (SPF RFC7208)



SPF Exercise

- Test 1
  - Send real email by gmail
  - POP retr
- Test 2
  - Send using telnet
  - POP retr

Key Remaining Question for SPF?

- How does SPF know if its neighbor MTA is a permitted sender of the domain?

DomainKeys Identified Mail (DKIM; RFC 5585)

- A domain-level digital signature authentication framework for email, using public key crypto
  - E.g., gmail.com signs that the message is sent by gmail server
- Basic idea of public key signature
  - Owner has both public and private keys
  - Owner uses private key to sign a message to generate a signature
  - Others with public key can verify signature

Example: RSA

1. Choose two large prime numbers *p*, *q*. (e.g., 1024 bits each)

2. Compute *n* = *pq*, *z* = *(p-1)(q-1)*

3. Choose *e* (with *e* < *n*) that has no common factors with z. (*e*, *z* are "relatively prime").

4. Choose *d* such that *ed-1* is exactly divisible by *z*. (in other words: *ed* mod *z* = *1*).

5. *Public* key is *(n,e)*. *Private* key is *(n,d)*.

RSA: Signing/Verification

0. Given (n,e) and (n,d) as computed above

1. To sign message, m, compute h = hash(m), then sign with private key

   $s = h^d \bmod n$ (i.e., remainder when h^d is divided by n)

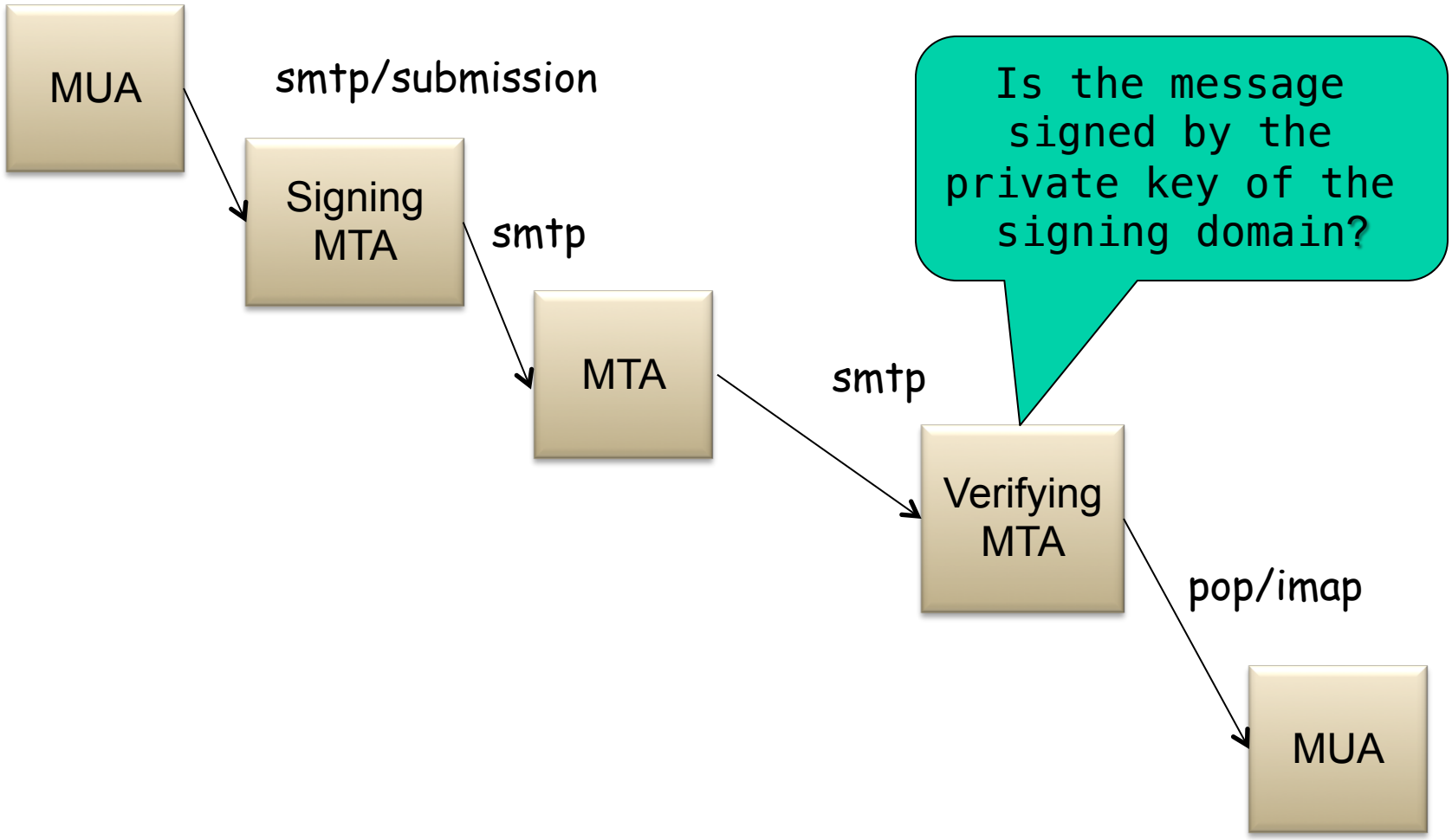
2. To verify signature s, compute

   $h' = s^e \bmod n$ (i.e., remainder when s^e is divided by n)

Magic happens! $h = (h^d \bmod n)^e \bmod n$

The magic is a simple application of Euler's generalization of Fermat's little theorem

DomainKeys Identified Mail (DKIM)



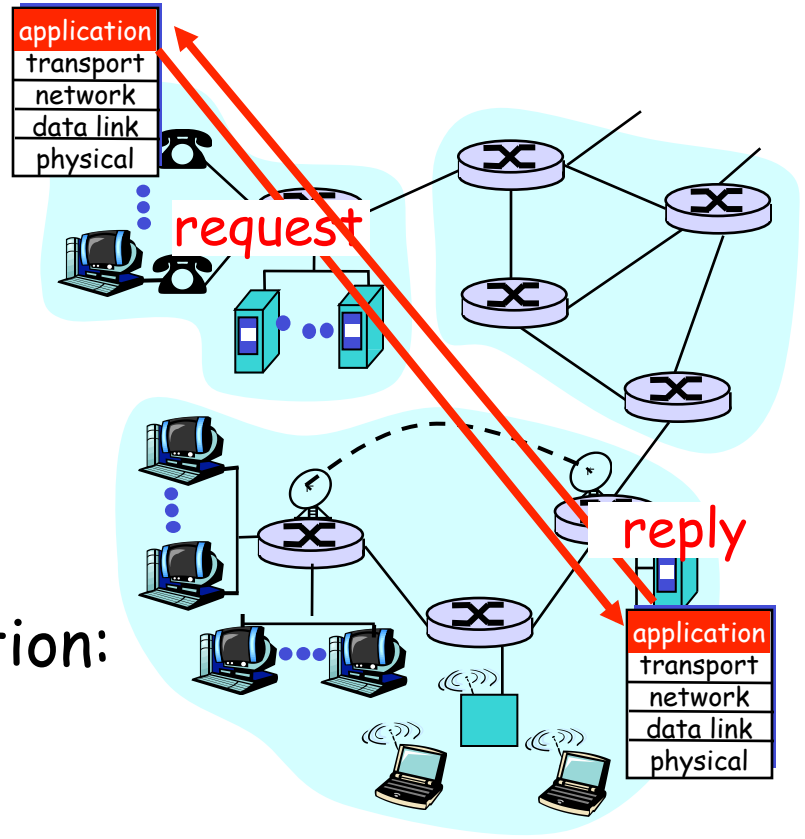
Key Remaining Question about DKIM?

- How does DKIM retrieve the public key of the author domain?

Summary: Client-Server Paradigm

- The basic paradigm of network applications is the client-server (C-S) paradigm

- Some key design questions to ask about a C-S application:
  - ✓ extensibility
  - ○ scalability
  - ○ robustness
  - ✓ security

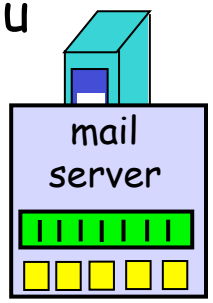


Scalability/Robustness

- High scalability and robustness fundamentally require that multiple email servers serve the same email address

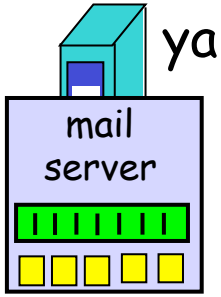
need an email server's IP address

yale.edu



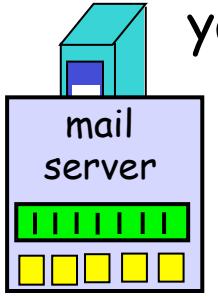
130.132.50.7

yale.edu



130.132.50.8

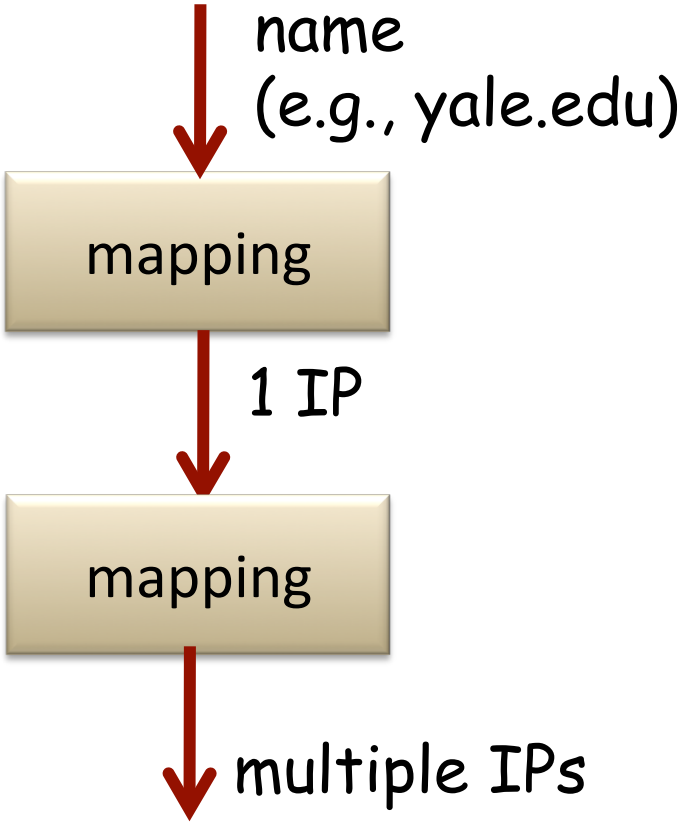
yale.edu

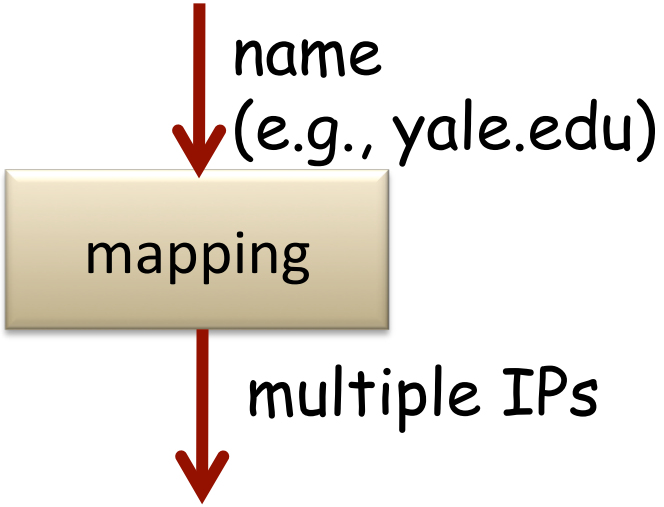


130.132.50.9

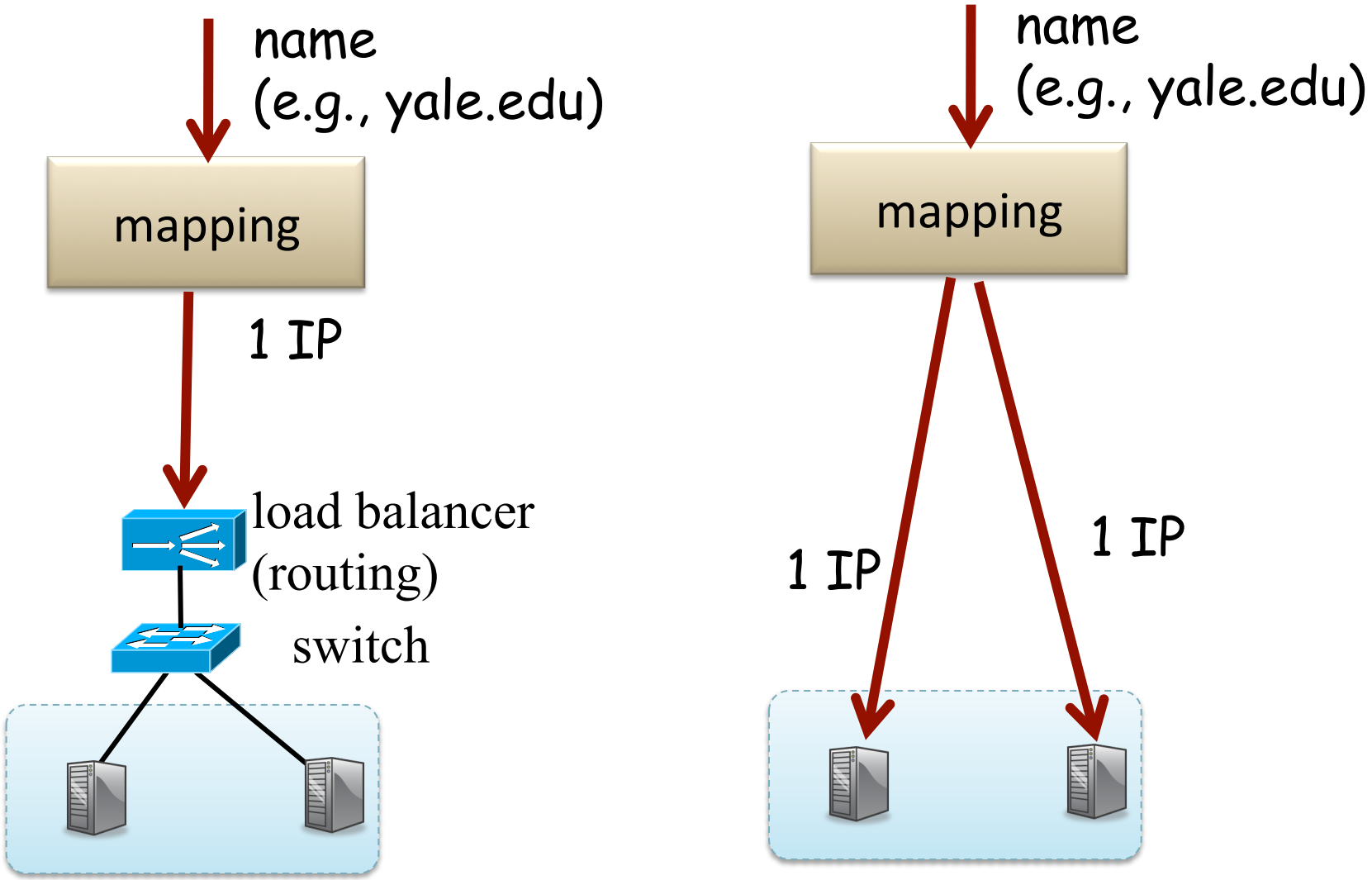
Mapping Functions Design Alternatives

- Map from an email address server name to IP address of email server





Mapping Functions Design Alternatives



Summary: Some Key Remaining Issues about Email

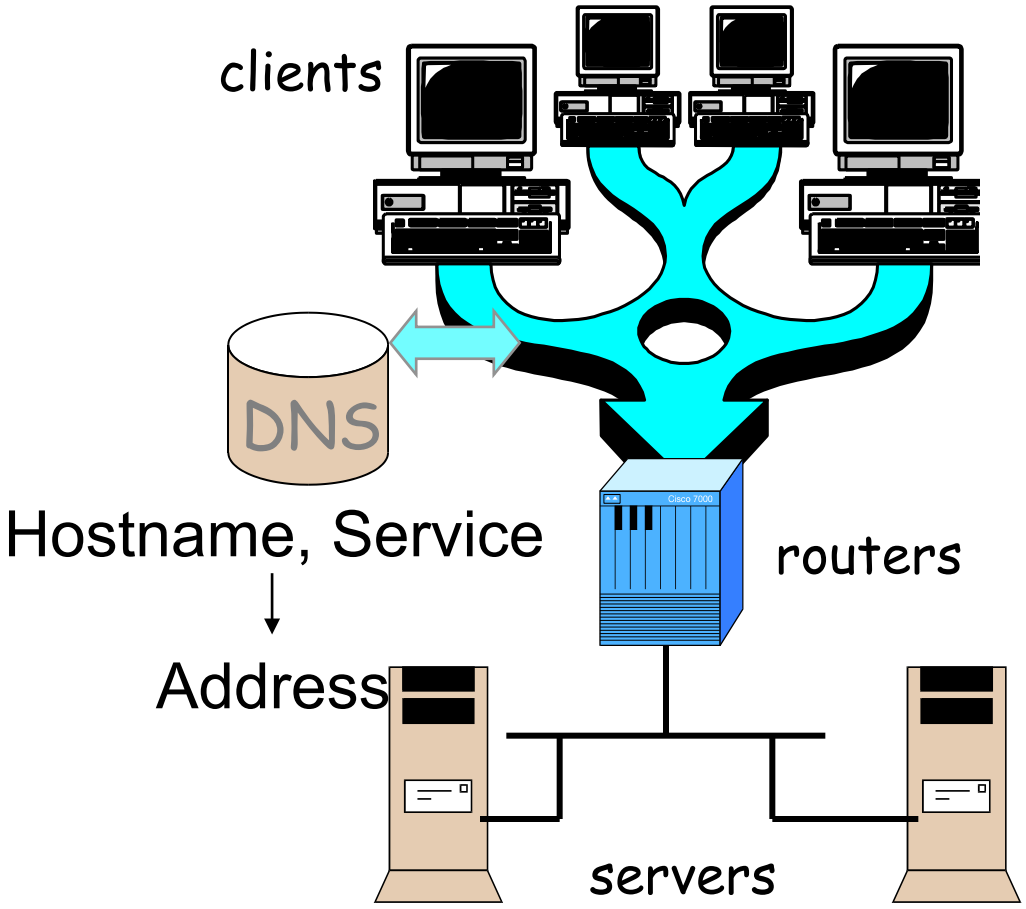
- Basic: How to find the email server of a domain?
- Scalability/robustness: how to find multiple servers for the email domain?
- Security
  - SPF: How does SPF know if its neighbor MTA is a permitted sender of the domain?
  - DKIM: How does DKIM retrieve the public key of the author domain?

Outline

- Recap
- Email security (authentication)
- DNS

DNS: Domain Name System

- Function
  - map between (domain name, service) to value, e.g.,
    - (www.cs.yale.edu, Addr) -> 128.36.229.30
    - (cs.yale.edu, Email) -> netra.cs.yale.edu



DNS Records

http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml

DNS: stores resource records (RR)

RR format: **(name, type, value, ttl)**

- Type=A
  - **name** is hostname
  - **value** is IP address
- Type=NS
  - **name** is domain (e.g. yale.edu)
  - **value** is the name of the authoritative name server for this domain
- Type=TXT
  - general txt
- Type=CNAME
  - **name** is an alias name for some "canonical" (the real) name
  - **value** is canonical name
- Type=MX
  - **value** is hostname of mail server associated with **name**
- Type=SRV
  - general extension for services

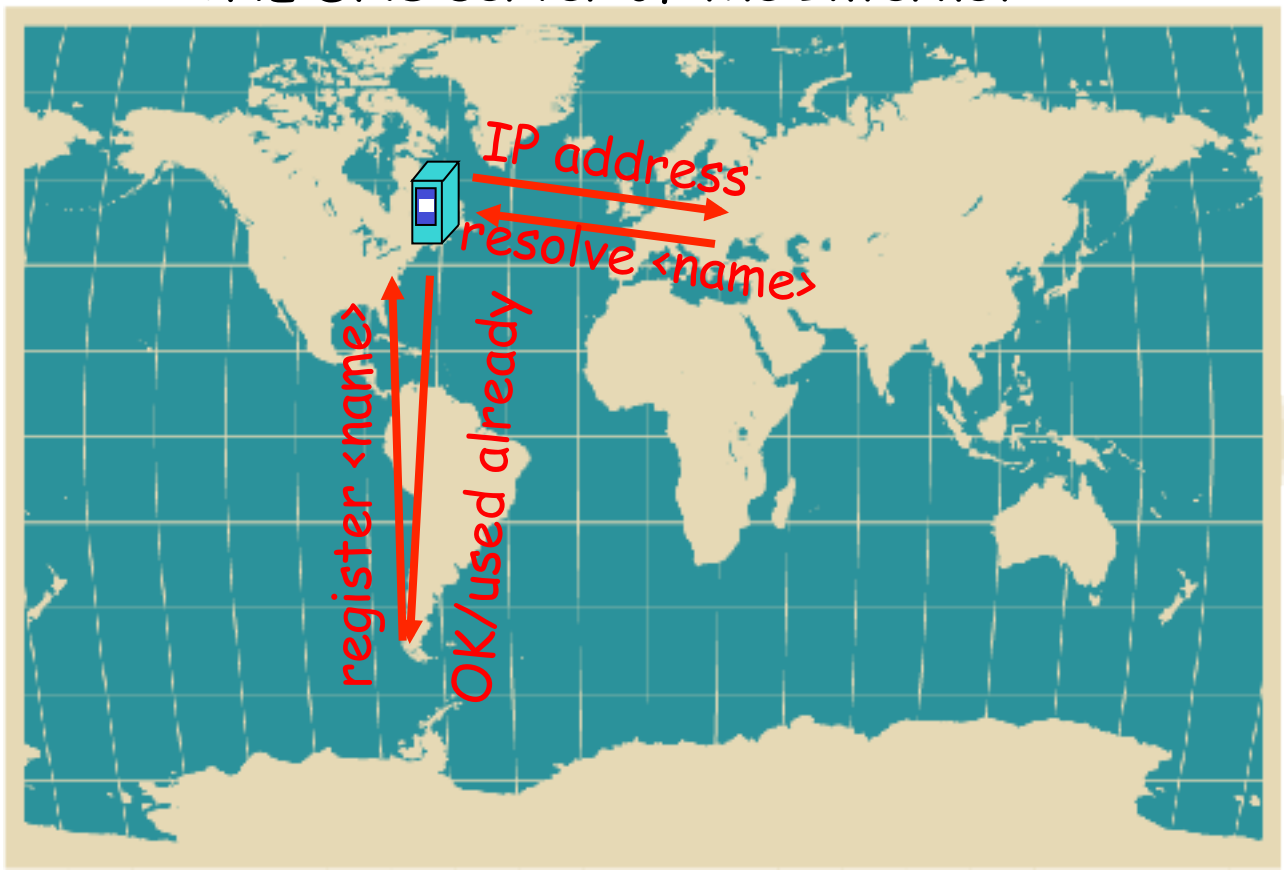
Try DNS: Examples

- dig <type> <domain>
  - type=MX
    - gmail.com
  - type=A
  - type=TXT
    - gmail.com
    - 20120113._domainkey.gmail.com

DNS Design: Dummy Design

- DNS itself can be considered as a client-server system as well
- How about a dummy design: introducing one super Internet DNS server?

THE DNS server of the Internet

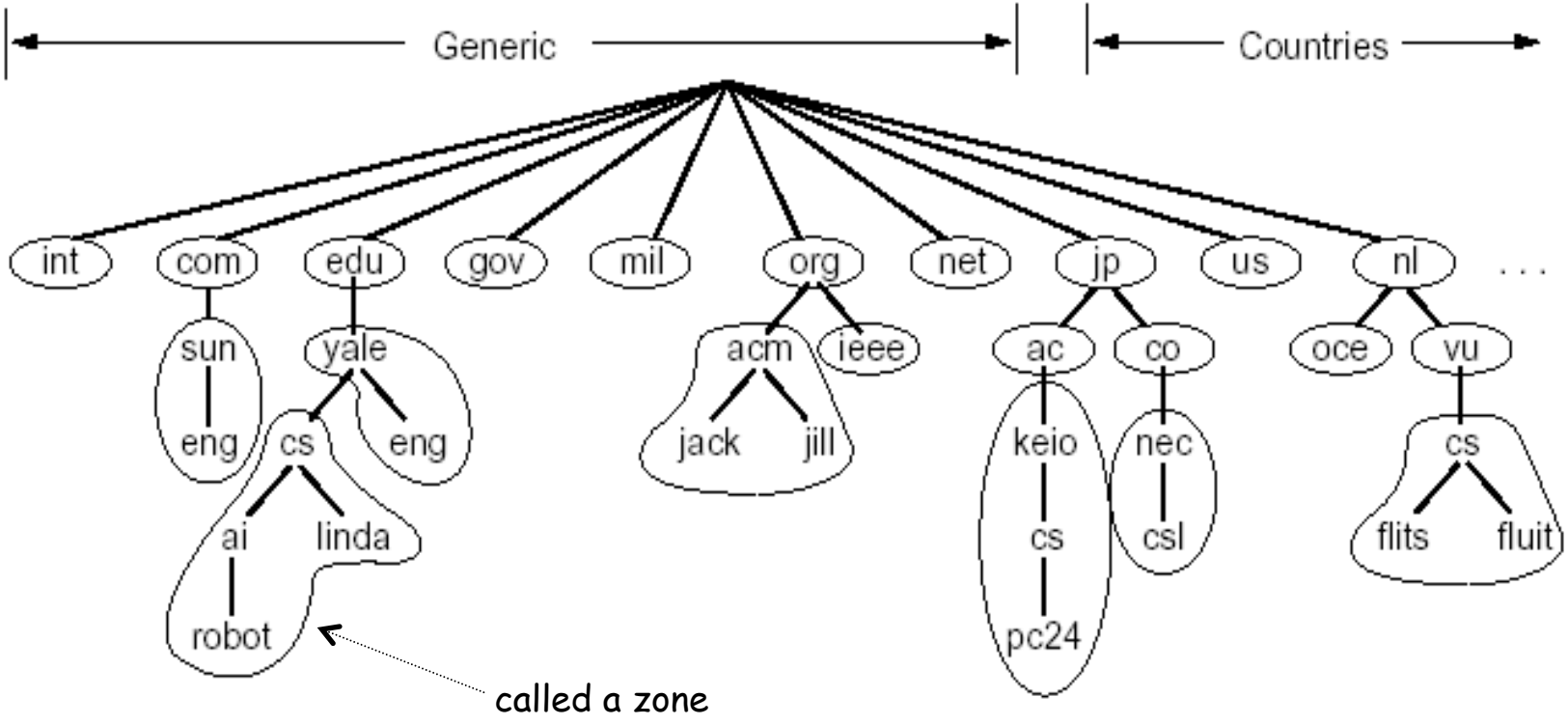


Problems of a Single DNS Server

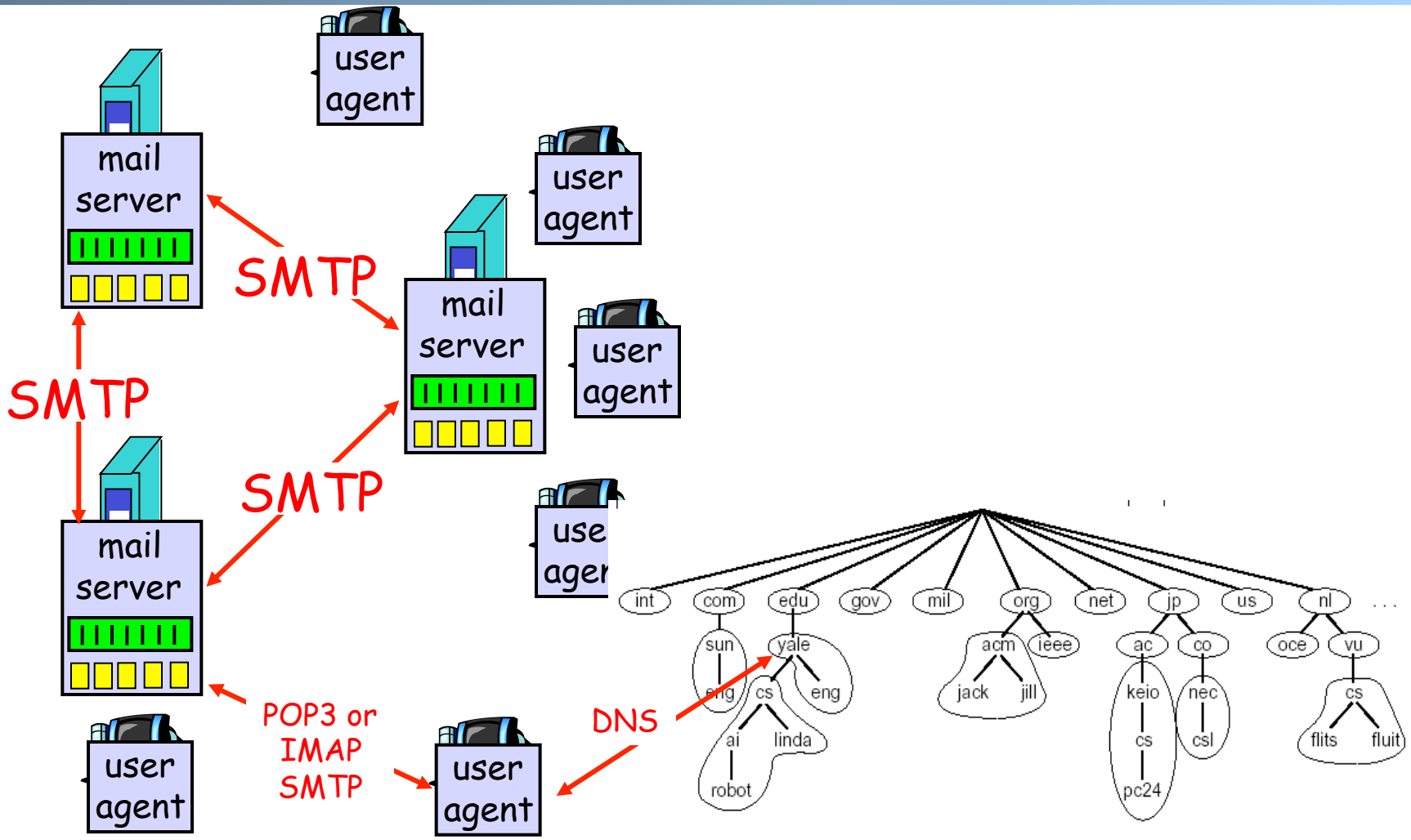
- Scalability and robustness bottleneck
- Administrative bottleneck

DNS: Distributed Management of the Domain Name Space

- A distributed database managed by authoritative name servers
  - divided into zones, where each zone is a sub-tree of the global tree
  - each zone has its own **authoritative name servers**
  - an authoritative name server of a zone may delegate a subset (i.e. a sub-tree) of its zone to another name server

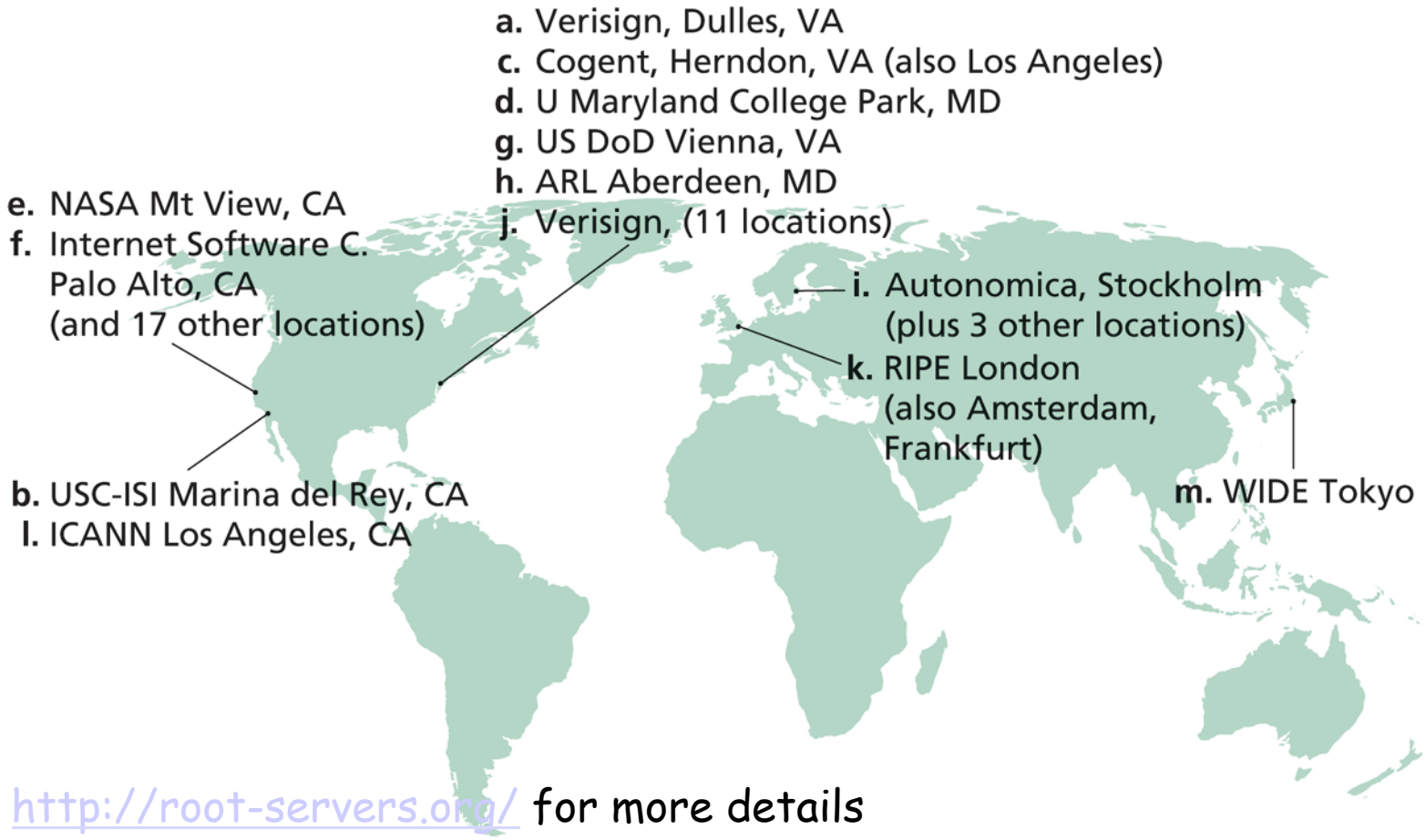


Email Architecture + DNS



Root Zone and Root Servers

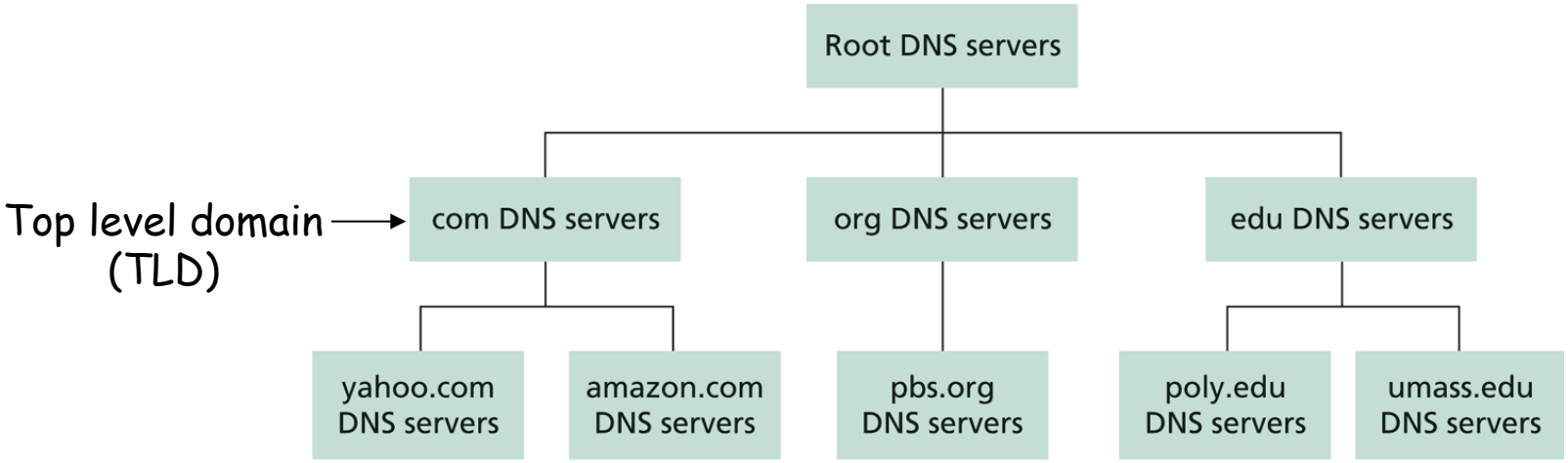
- The root zone is managed by the root name servers
  - 13 root name servers worldwide



See http://root-servers.org/ for more details

Linking the Name Servers

- Each name server knows the addresses of the root servers
- Each name server knows the addresses of its immediate children (i.e., those it delegates)



Q: how to query a hierarchy?

DNS Message Flow: Two Types of Queries

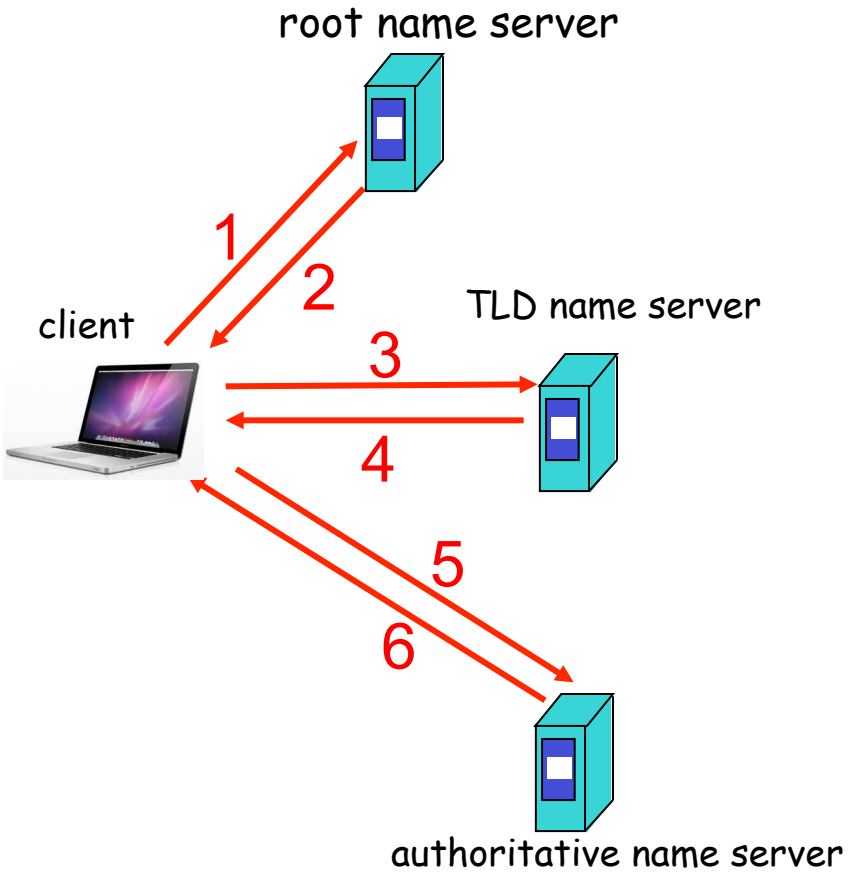
Recursive query:

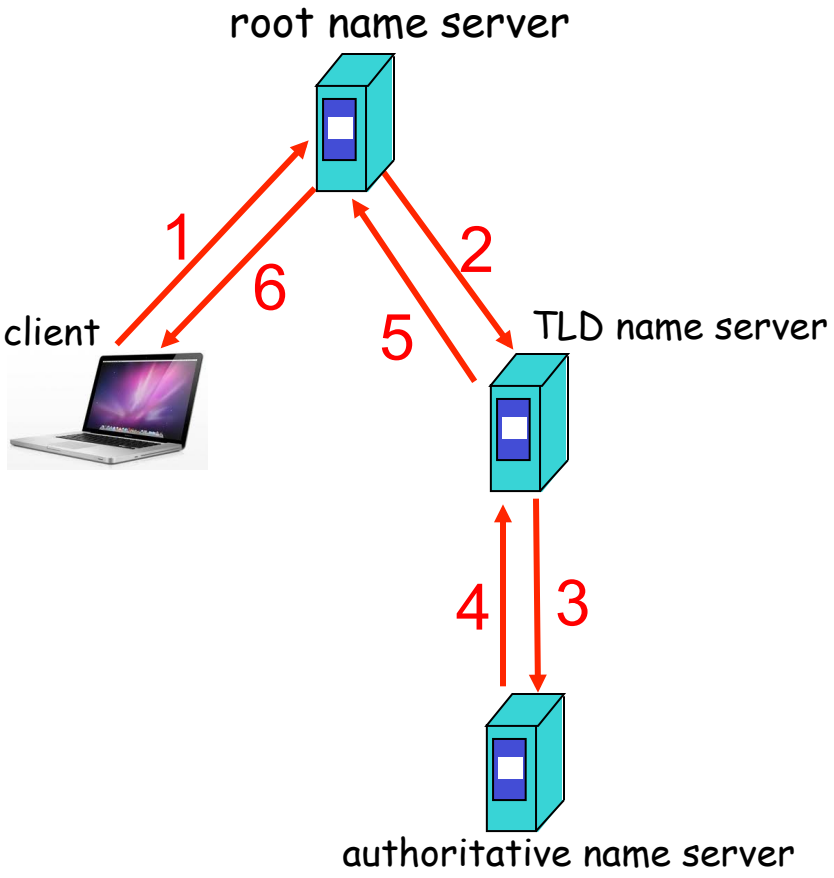
- The contacted name server resolves the name completely

Iterated query:

- Contacted server replies with name of server to contact
  - "I don't know this name, but ask this server"

Two Extreme DNS Message Flows



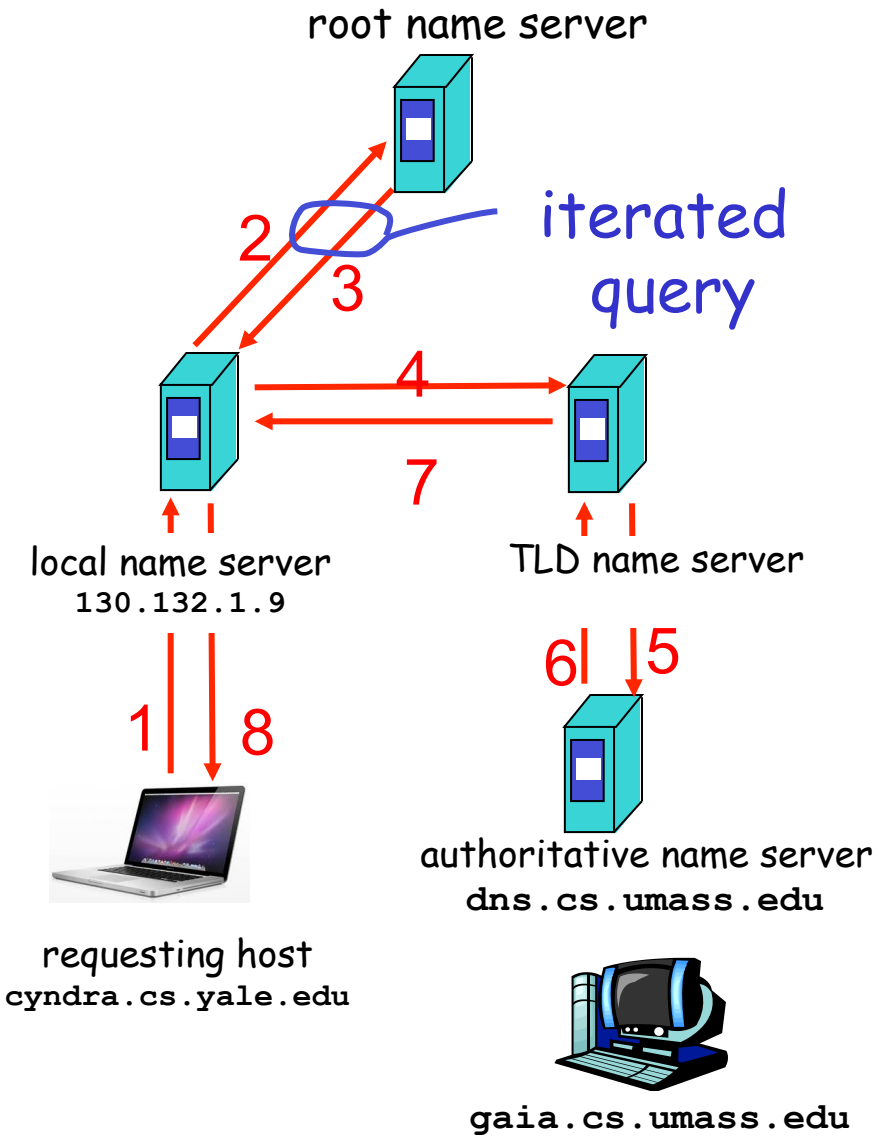


Issues of the two approaches?

cicada.cs.yale.edu

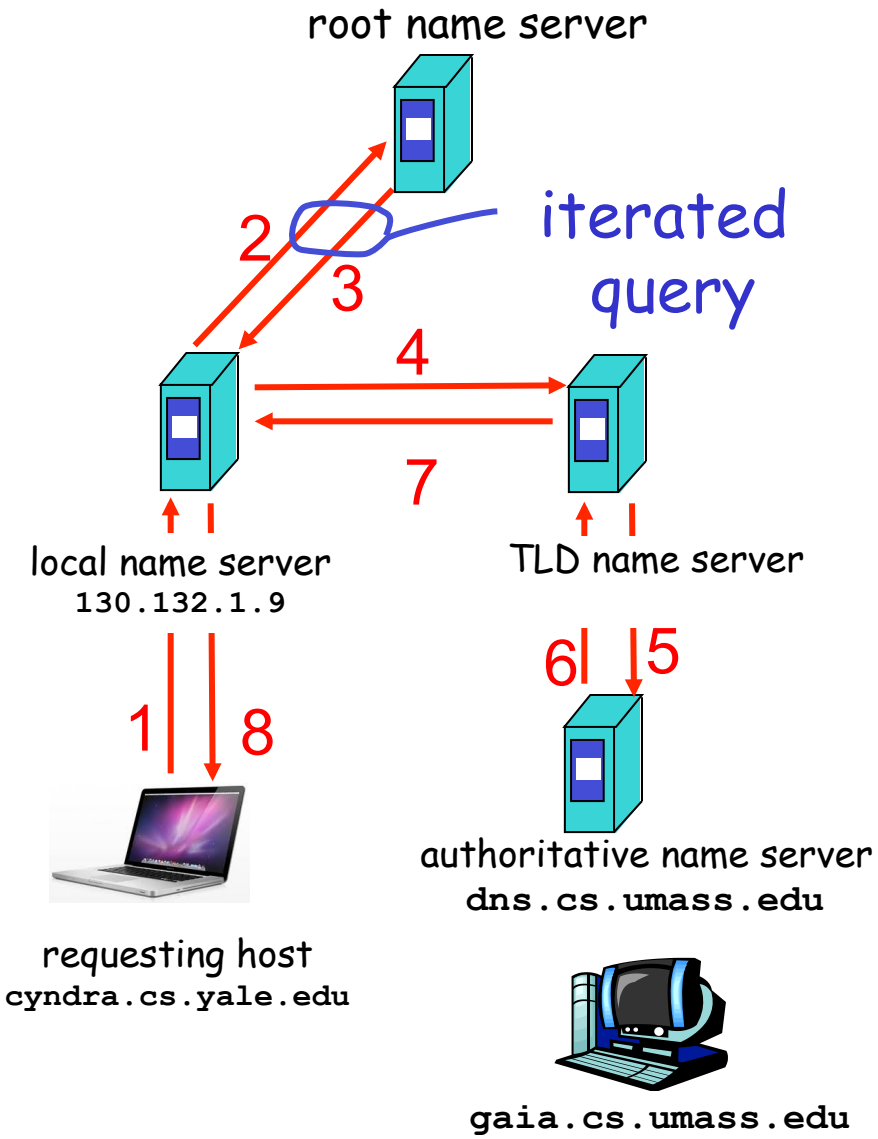
Typical DNS Message Flow: The Hybrid Case

- Host knows only local name server
- Local name server is learned from DHCP, or configured, e.g. /etc/resolv.conf
- Local DNS server helps clients resolve DNS names



Typical DNS Message Flow: The Hybrid Case

- Host knows only local name server
- Local name server is learned from DHCP, or configured, e.g. /etc/resolv.conf
- Local DNS server helps clients resolve DNS names
- Benefits of local name servers
  - simplifies client
  - Caches/reuses results



Outline

- Recap
- Email security (authentication)
- DNS
  - High-level design
  - Details

DNS Message Format?