Network Applications: Email; DNS;

Qiao Xiang, Congming Gao, Qiang Su

https://sngroup.org.cn/courses/cnns-xmuf25/index.shtml

09/16/2025

This deck of slides are heavily based on CPSC 433/533 at Yale University, by courtesy of Dr. Y. Richard Yang.

Outline

- Admin. and recap
- Email
  - How to handle spam
- DNS
  - High-level design
  - Details
  - Extensions/alternatives

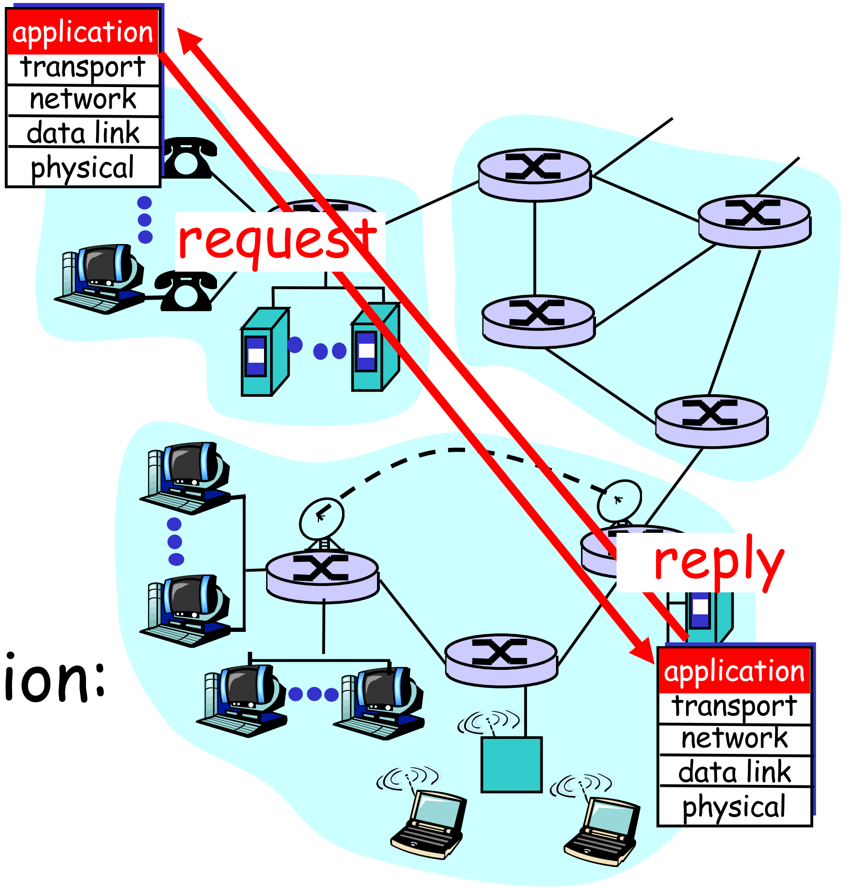
Admin

- ❑ Assignment One to be posted this week

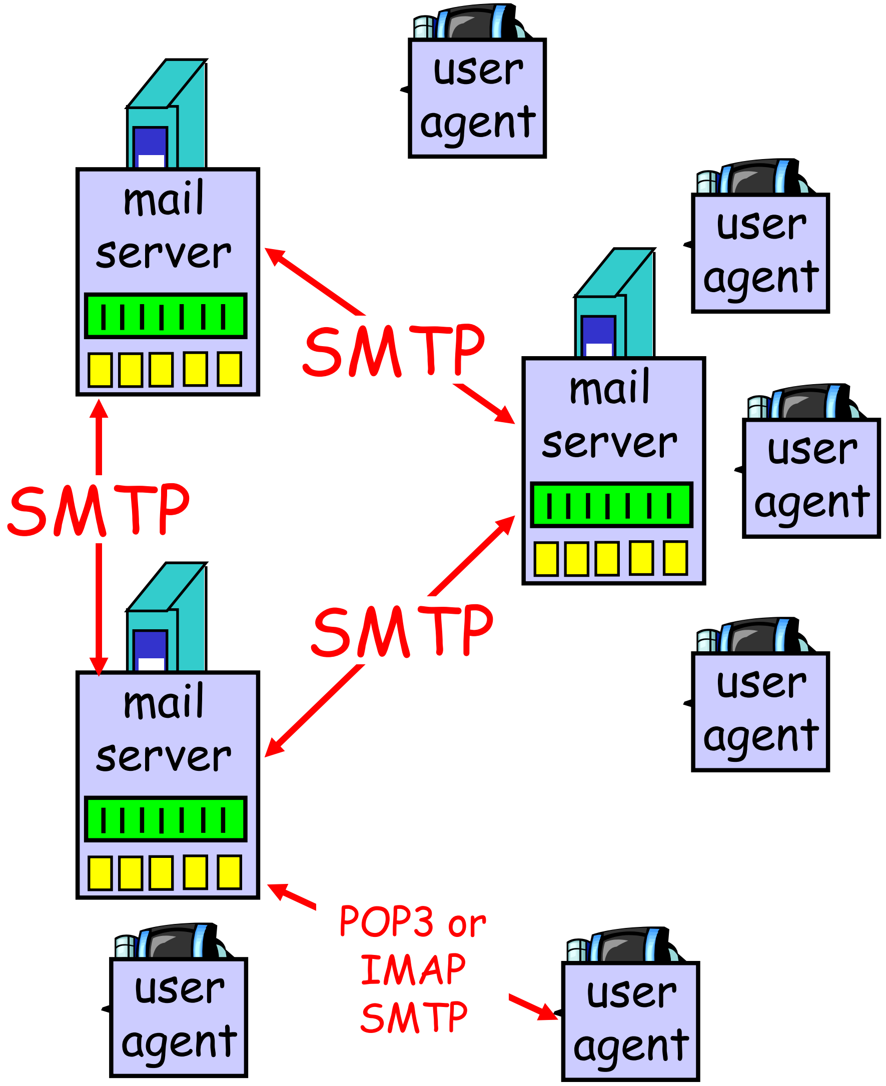
Recap: Client-Server Paradigm

- 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



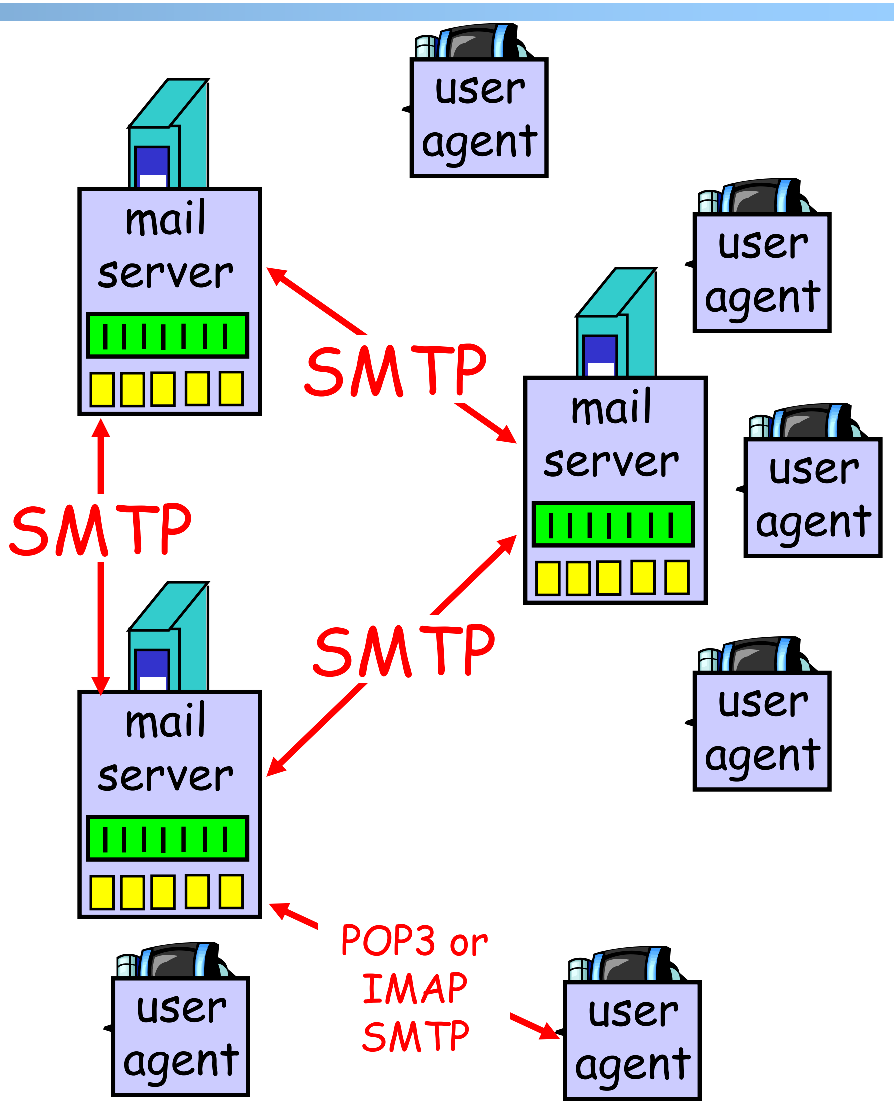
Some key design features of Email

- Separate protocols for different functions
  - email access (e.g., POP3, IMAP)
  - email transport (SMTP)
- Separation of envelop and message body (end-to-end arguments)
  - envelop: simple/basic requests to implement transport control;
  - message body: fine-grain control through ASCII header and message body
    - MIME type as self-describing data type
- Status code in response makes message easy to parse

Evaluation of SMTP/POP/IMAP

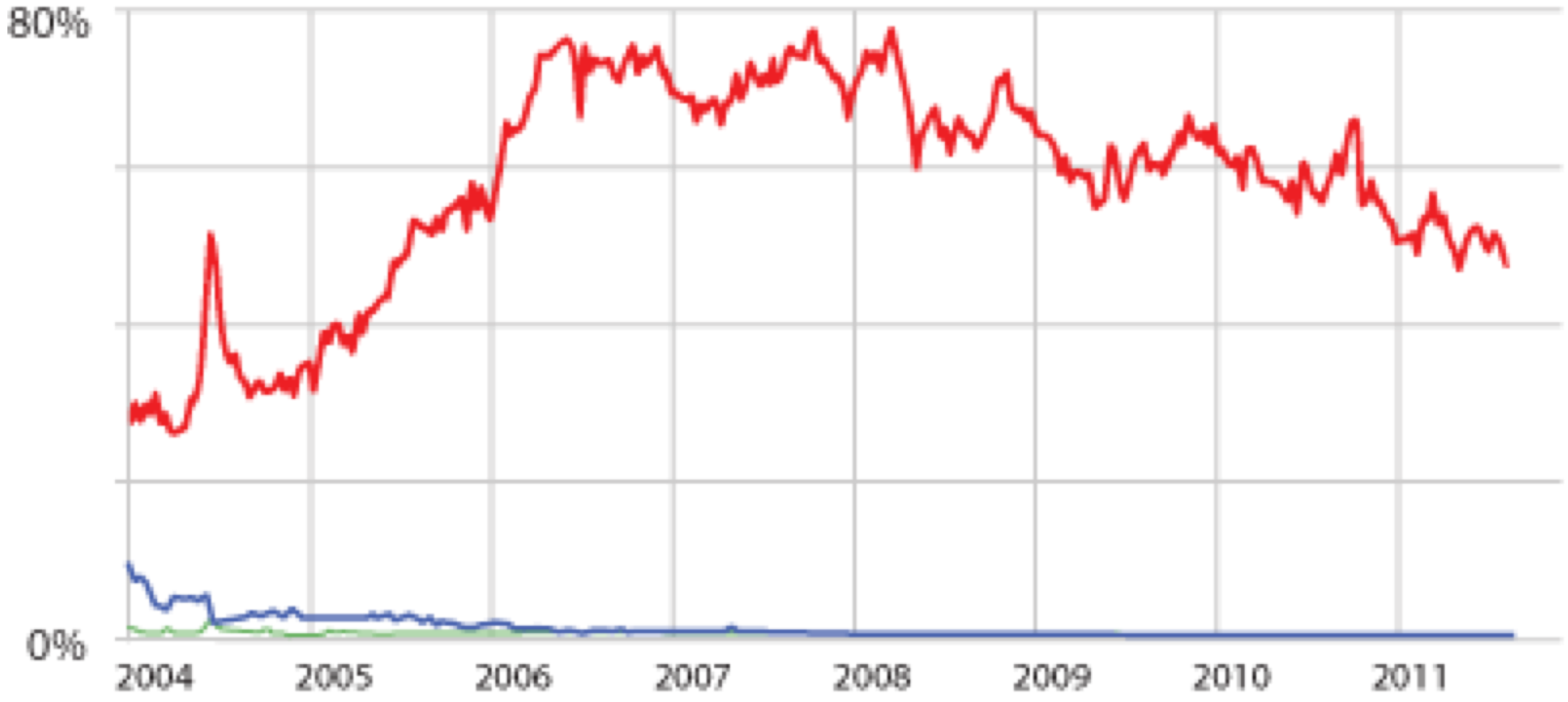
Key questions to ask about a C-S application

- extensible?
- scalable?
- robust?
- security?

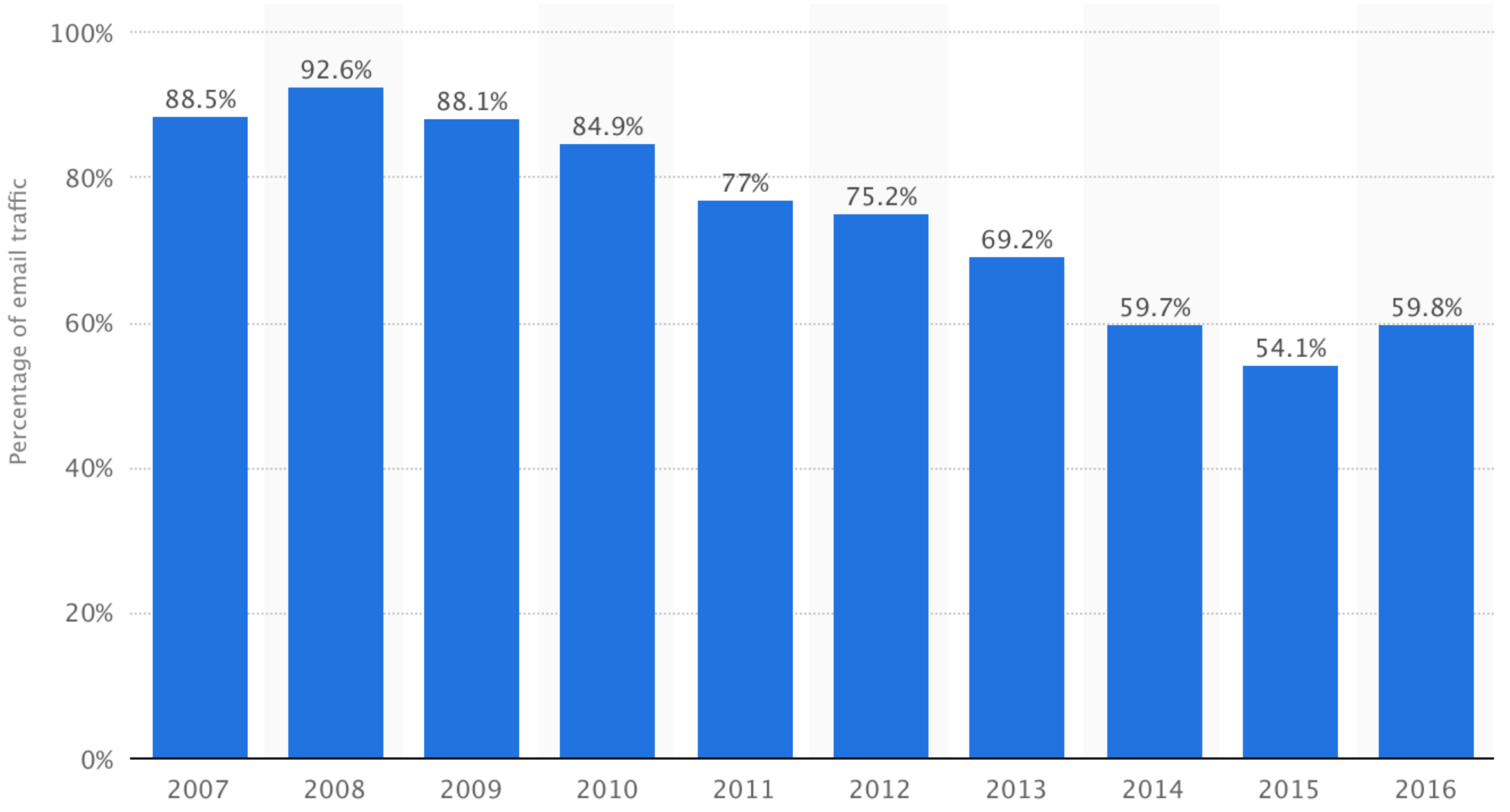


Email Security: Spam

- Spam (Google)



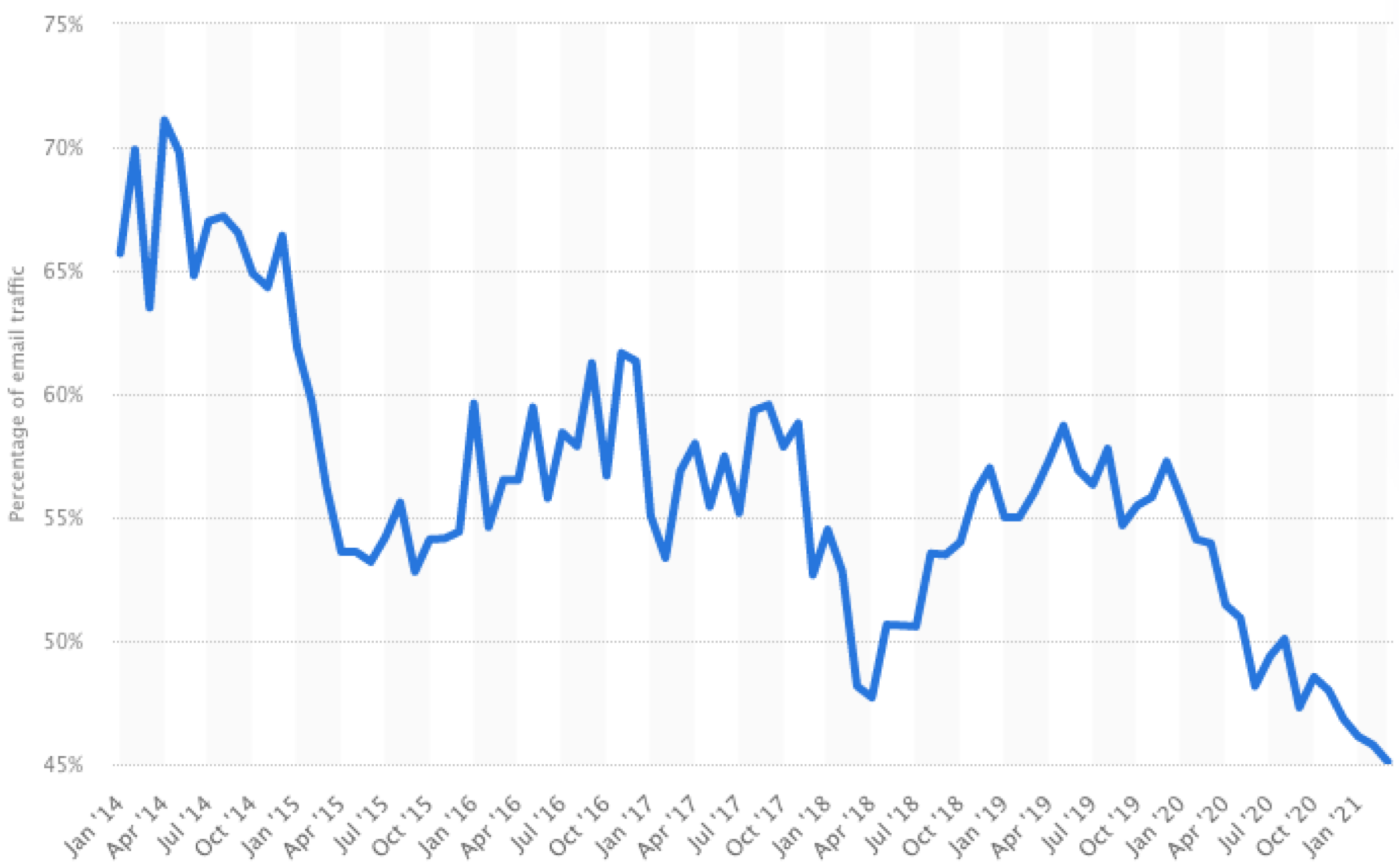
Email Security Issue: Spam



© Statista 2017

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

Email Security Issue: Spam



Source: https://www.statista.com/statistics/420391/spam-email-traffic-share/

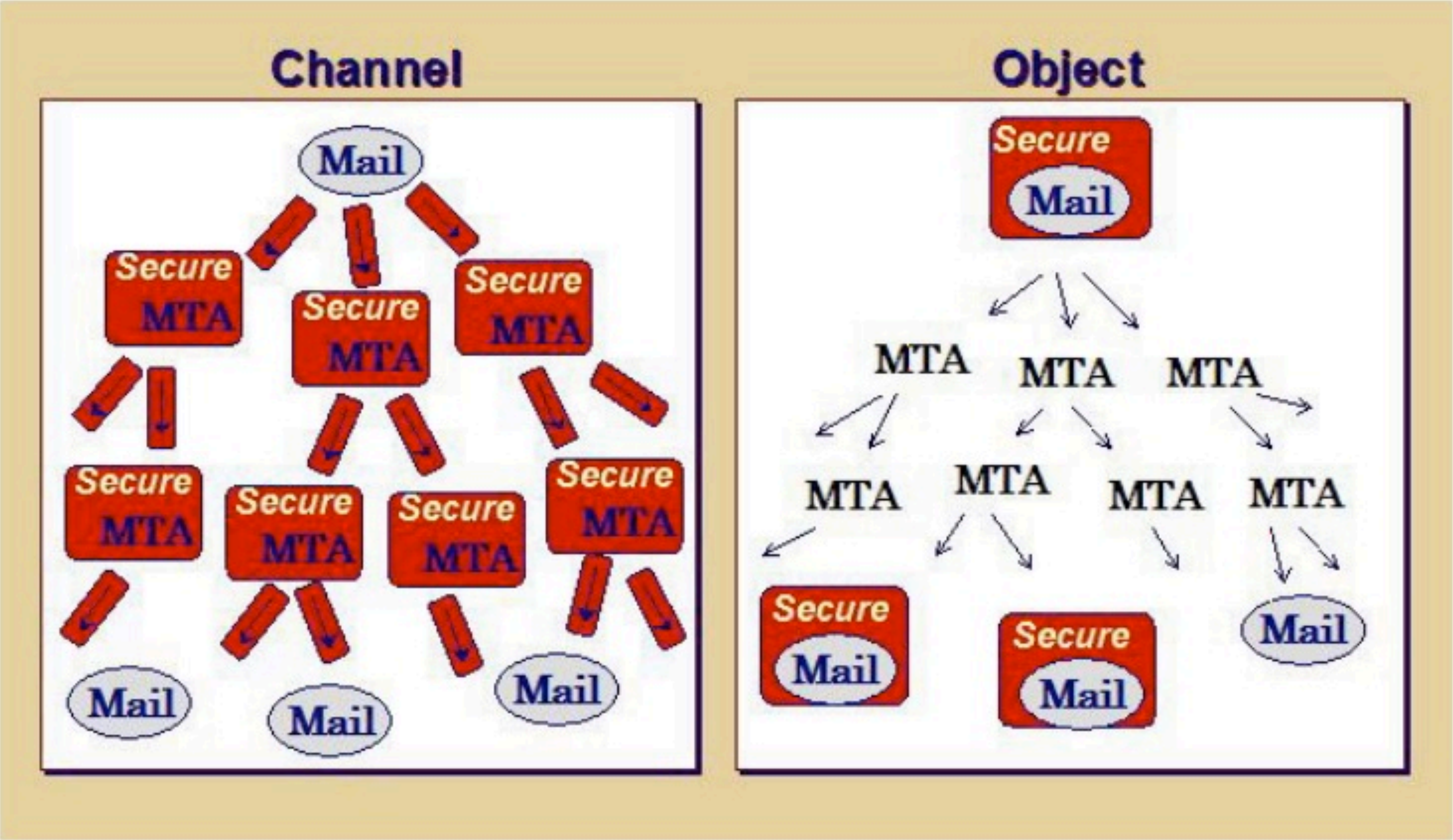
Discussion: How May One Handle Email Spams?

Detection Methods Used by GMail

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

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

Email Authentication Approaches

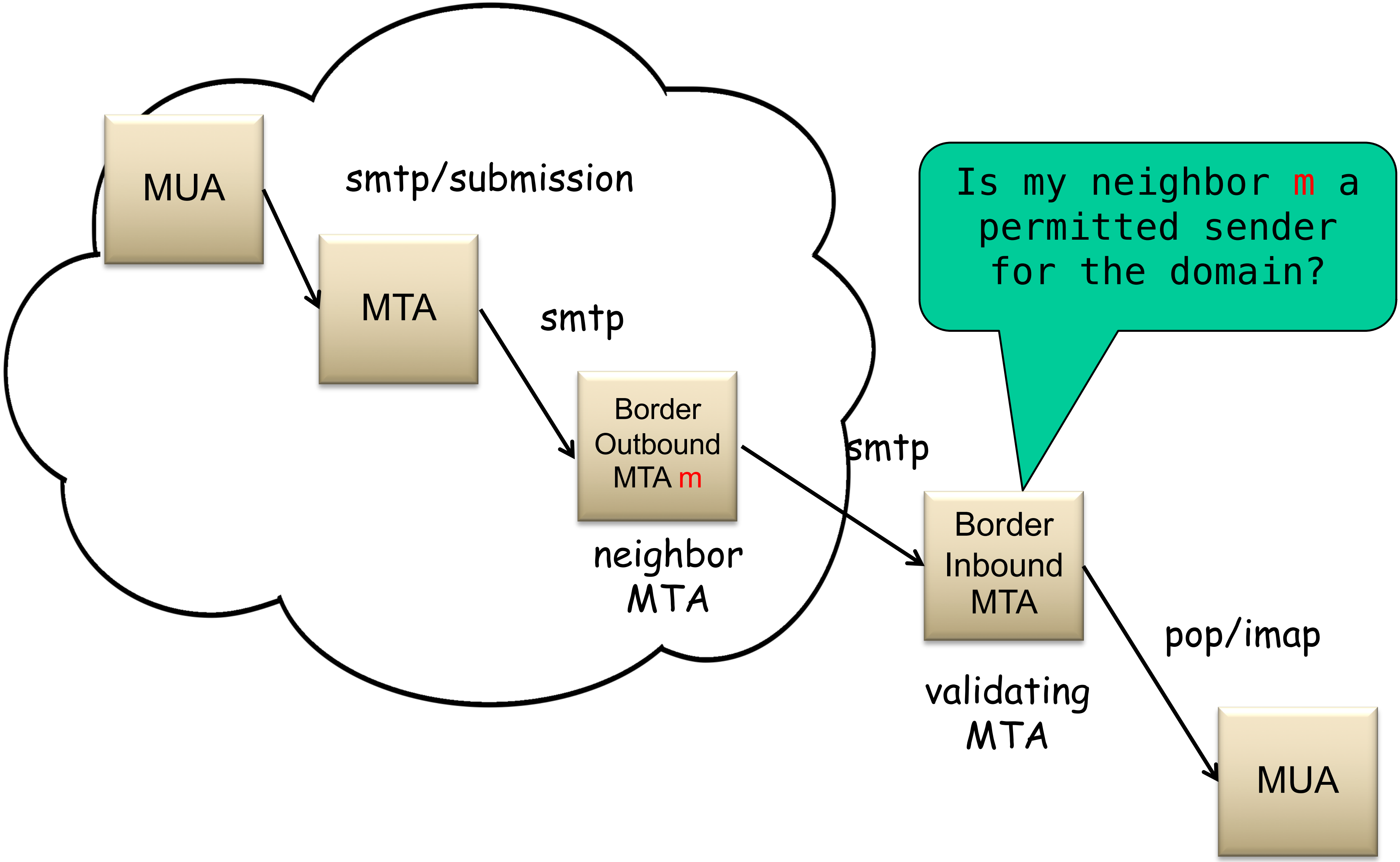


Sender Policy Frame (SPF)

DomainKeys Identified Mail (DKIM)
Authenticated Results Chain (ARC)

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

Sender Policy Framework (SPF RFC7208)



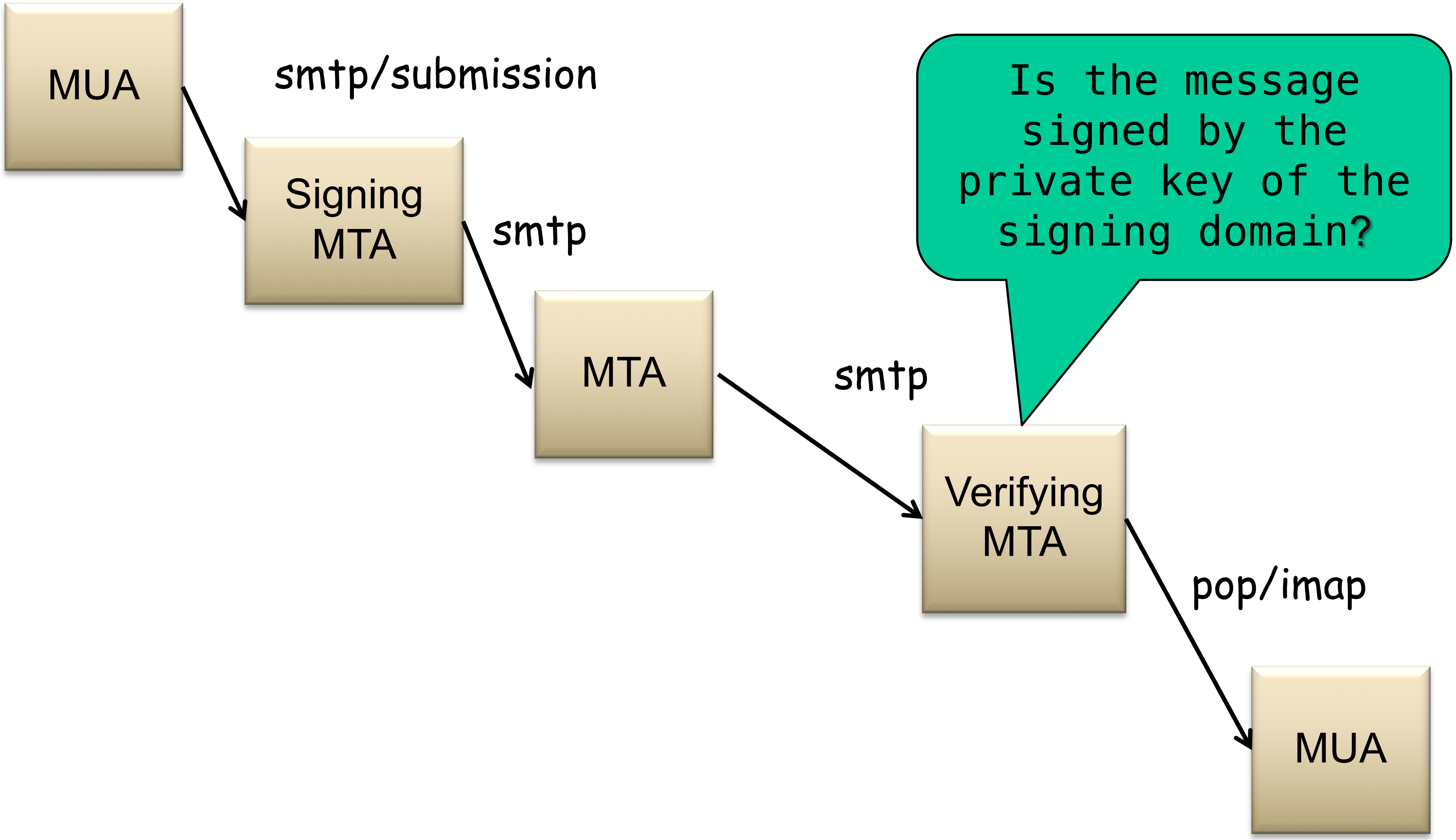
Key Question for SPF?

- 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., mail.sina.com signs that the message is sent by mail.sina 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
  - Assumption: difficult to get private key even w/ public key distributed

DomainKeys Identified Mail (DKIM)



Is the message signed by the private key of the signing domain?

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

Key Question about DKIM?

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

Summary: Some Key Remaining Issues about Email

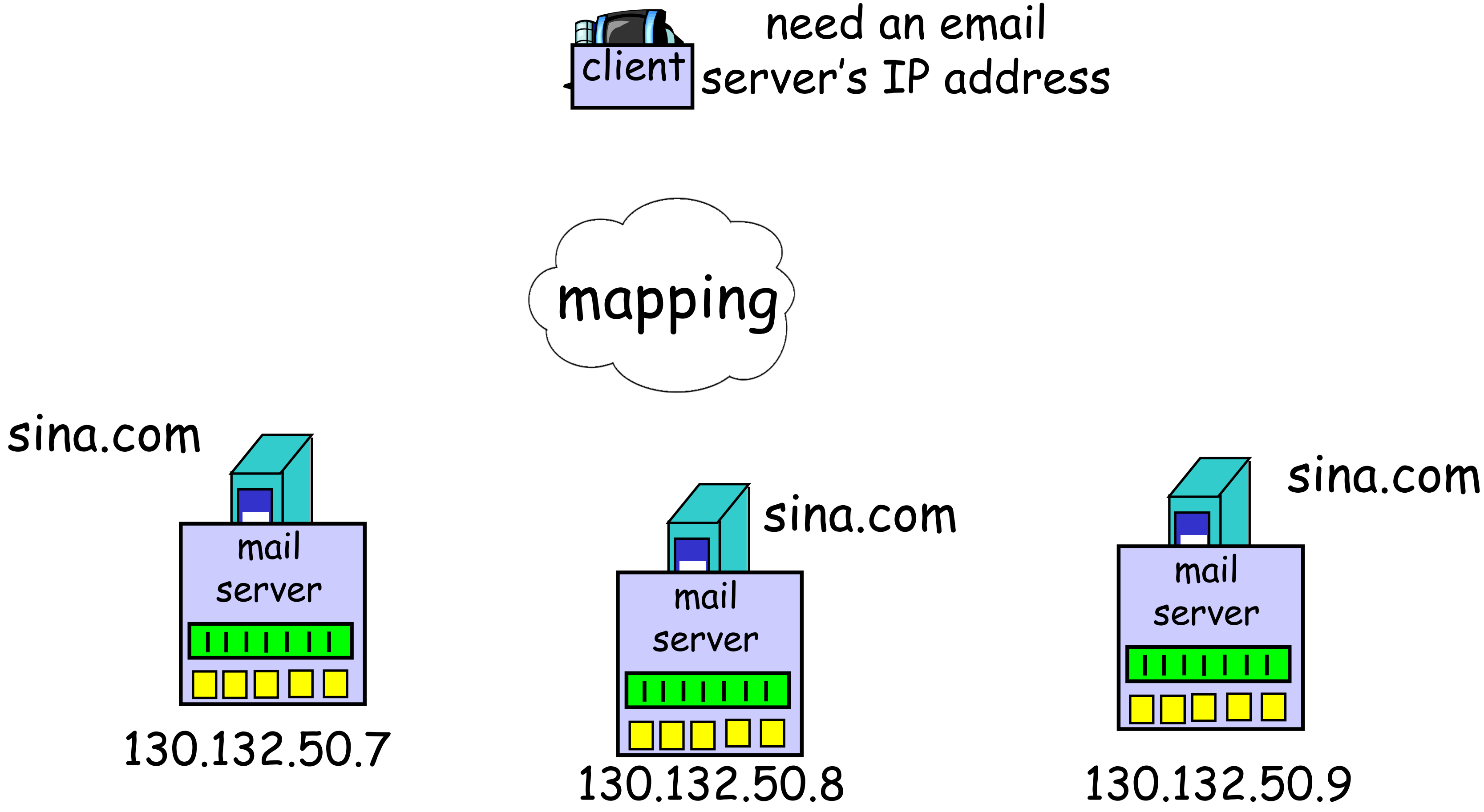
- Basic: How to find the email server of a domain?

- Scalability/robustness: how to find multiple servers for the email domain?

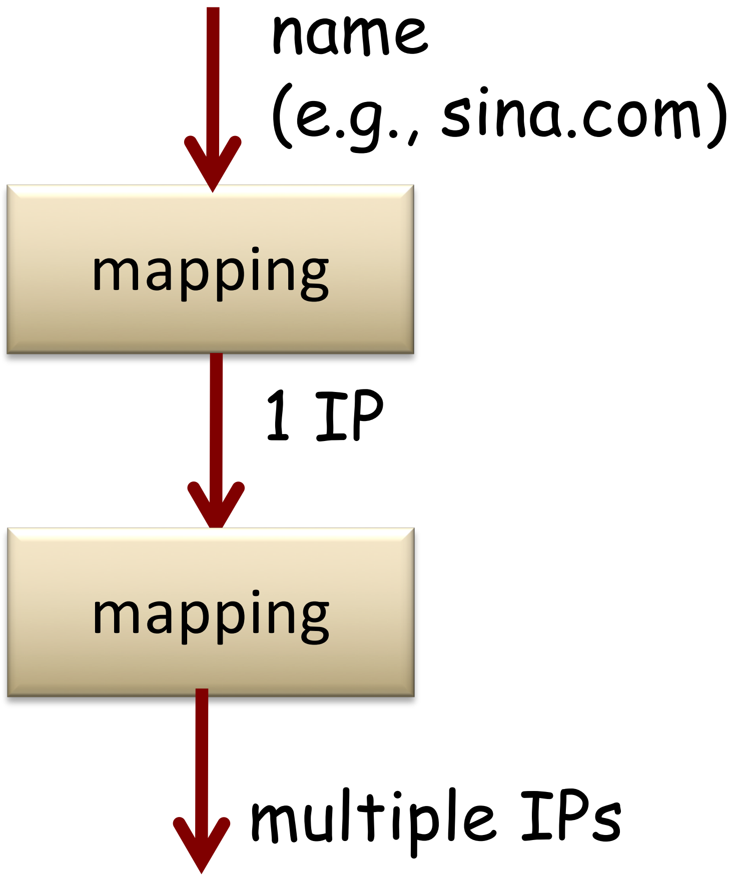
- Security
  - SPF: How does SPF know if its neighbor MTA is a permitted sender of the domain?
  - DKIM: How does DKIM retrieve the public key of the author domain?

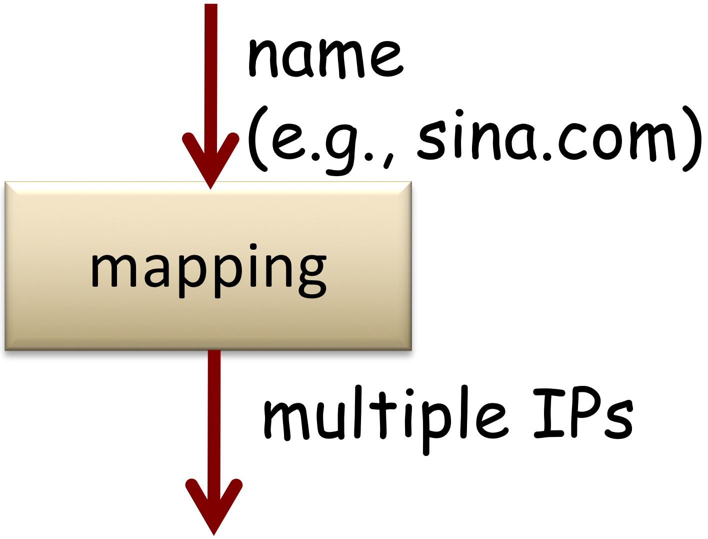
Scalability/Robustness

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

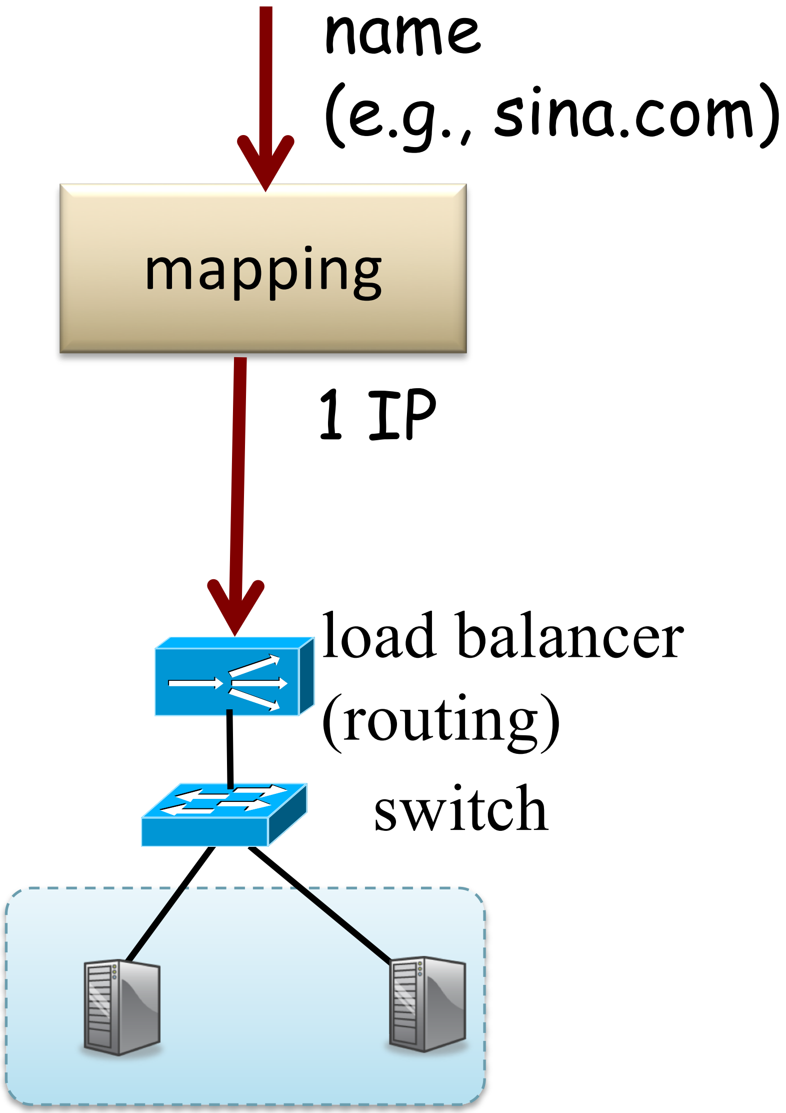


Mapping Functions Design Alternatives





Mapping Functions Design Alternatives



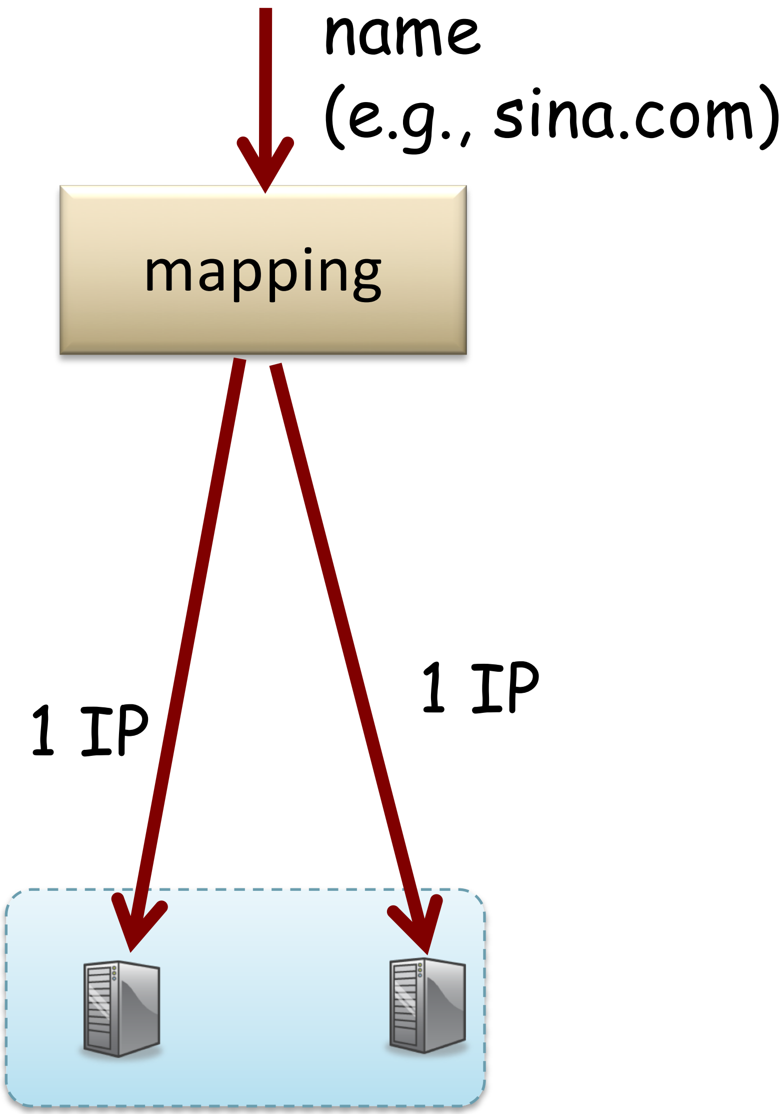
name
(e.g., sina.com)

mapping

1 IP

load balancer
(routing)

switch



name
(e.g., sina.com)

mapping

1 IP

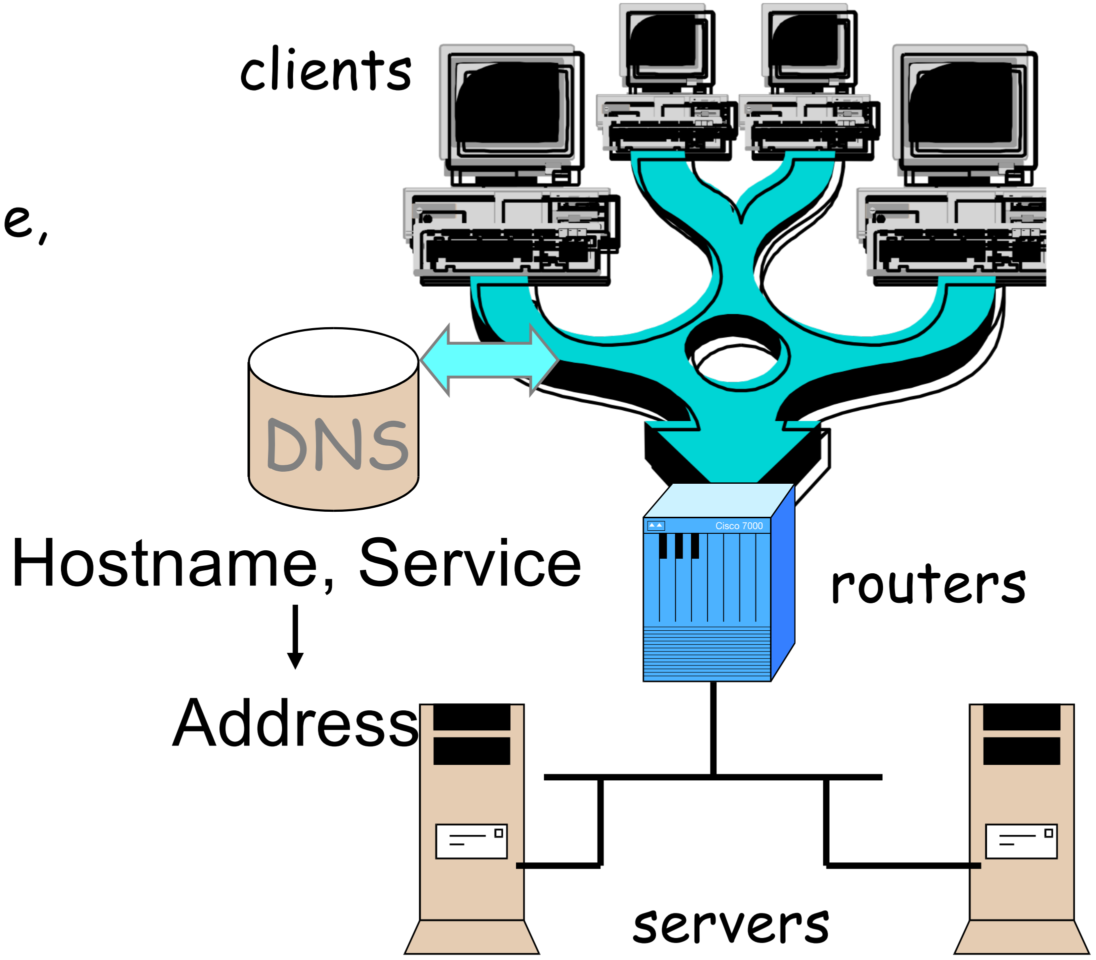
1 IP

Outline

- Admin. and recap
- Layered network architecture
- Application layer overview
- Network applications
  - Email
  - *DNS*

DNS: Domain Name System

- ❑ Function
  - map between (domain name, service) to value, e.g.,
    - (xmu.edu.cn, addr) -> 210.34.0.35
    - (xmu.edu.cn, email) -> cmsn1.xmu.edu.cn



Hostname, Service

↓

Address

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. xmu.edu.cn)
  - ○ **value** is the name of the authoritative name server for this domain
- Type=TXT
  - ○ general txt
- Type=CNAME
  - ○ **name** is an alias of a "canonical" (real) name
  - ○ **value** is canonical name
- Type=MX
  - ○ **value** is hostname of mail server associated with **name**
- Type=SRV
  - ○ general extension for services
- Type=PTR
  - ○ a pointer to another name

Discussion

- Can DNS handle multiple values for the same (name, service)?

Try DNS: Examples

- dig <name> <type>
  - Try xmu.edu.cn / others and various types

- dig <domain> txt to retrieve spf

http://www.zytrax.com/books/dns/ch9/spf.html

Observations

- MX can return multiple servers
- DNS may rotate the servers in answer
- Address can also return multiple addresses
- SPF is encoded as the txt type

Outline

- ❑ Admin. and recap
- ❑ DNS
  - ➢ High-level design
  - ➢ *Details*

DKIM Example

- Send email from hotmail and check message

```
S: +OK sina pop3 server ready
C: user xmucnns
S: +OK welcome to sina mail
C: pass 334f5605df1504f9
S: +OK 4 messages (32377 octets)
```

DKIM Example

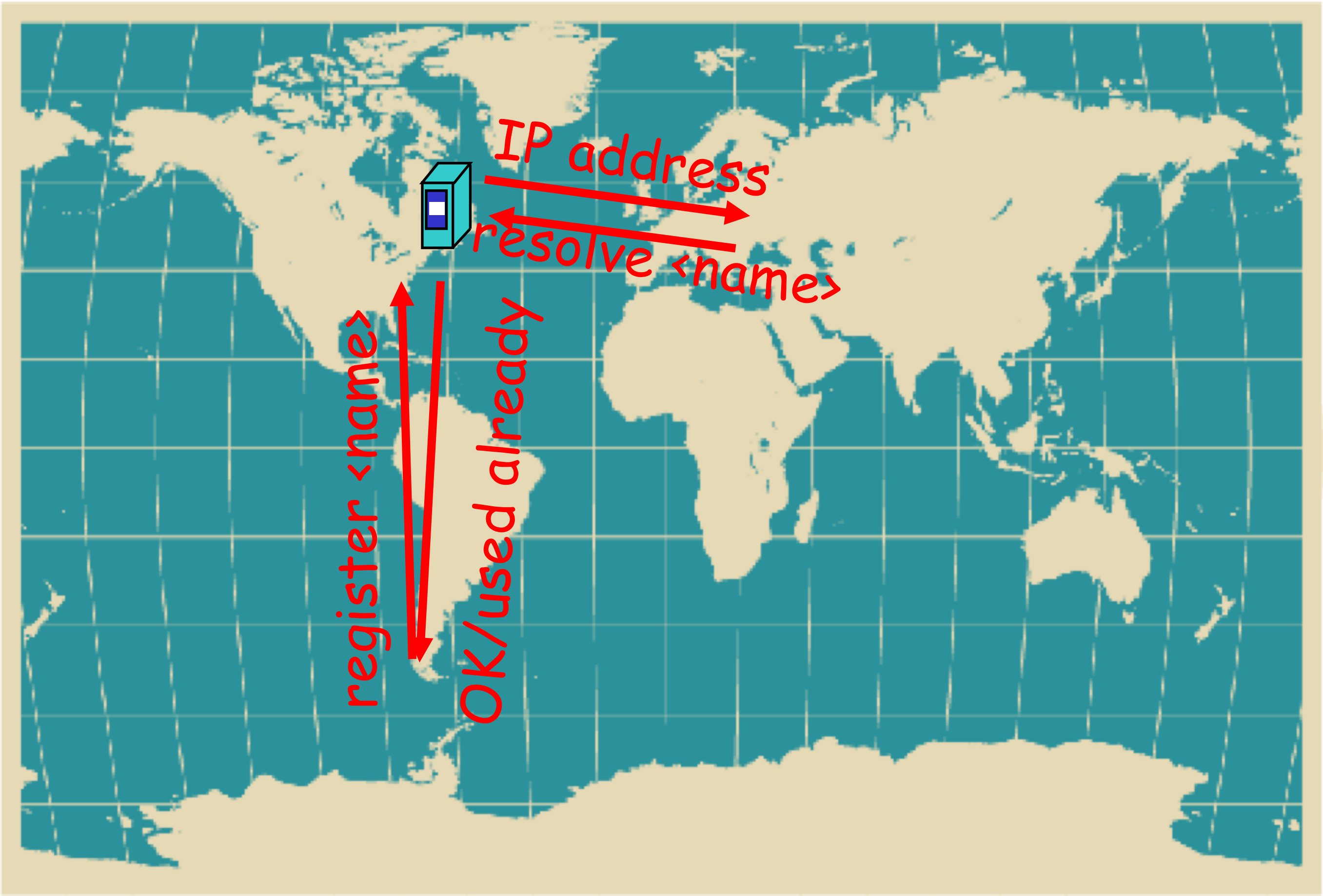
- DKIM / ARC:
  Msg: ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector9901; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version; bh=bO91TxHI+4MjgAusrfg0EWGiDmvQ5hZRZ/aqb1MKLY8=; …

  DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=hotmail.com; s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;…
- Query: dig arcselector9901._domainkey.microsoft.com txt
- DKIM introduces a session key to allow multiple public keys
  - <session>._domainkey.<domain>

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

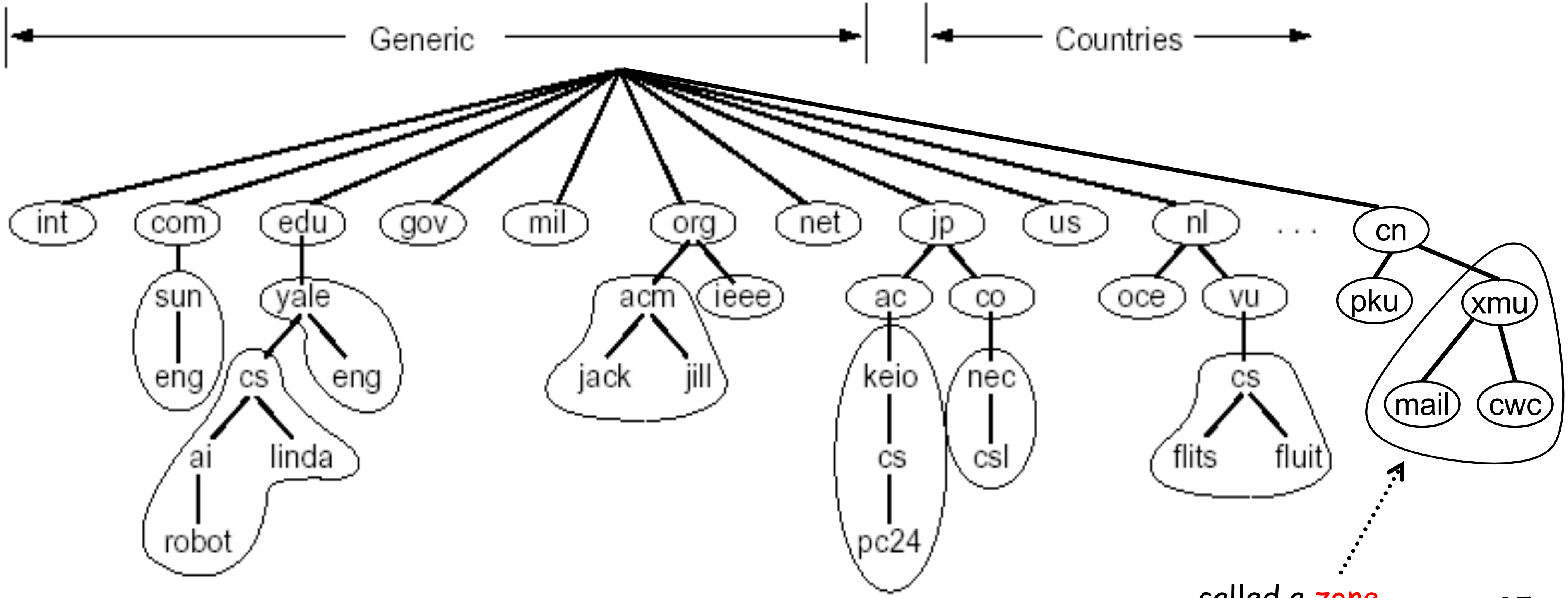


Problems of a Single DNS Server

- Scalability and robustness bottleneck
- Administrative bottleneck

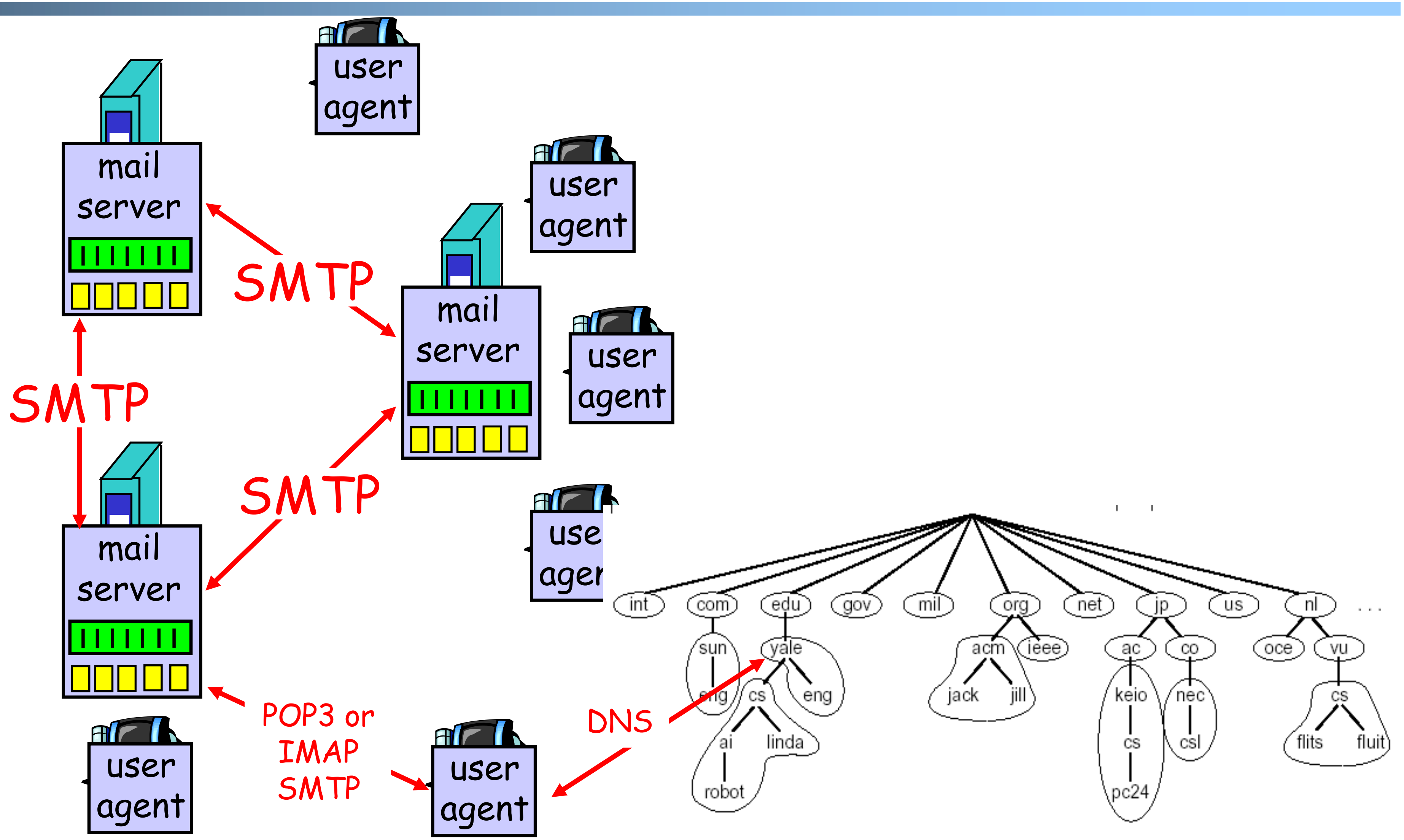
DNS: Distributed Management of the Domain Name Space

- 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



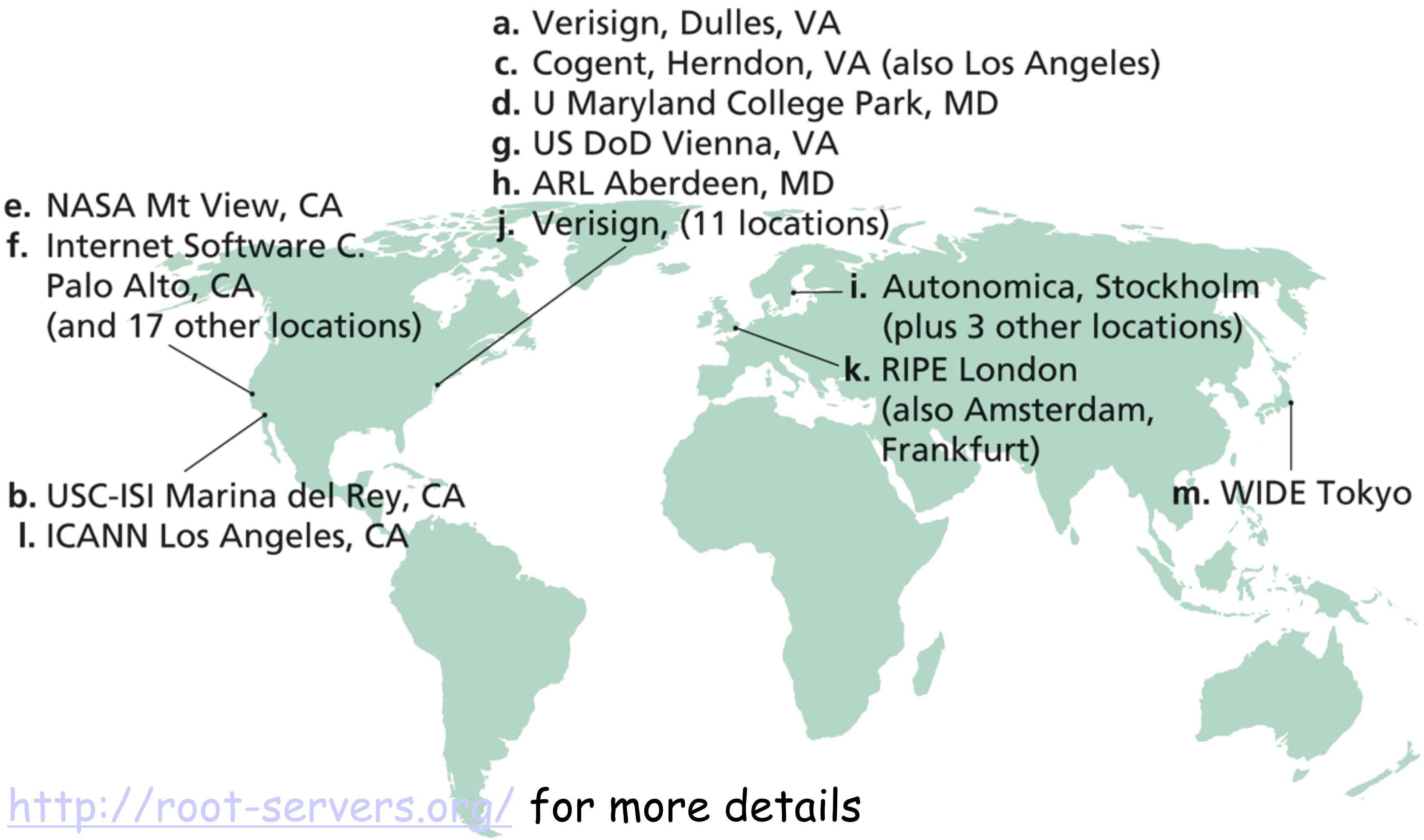
called a zone

Email Architecture + DNS



Root Zone and Root Servers

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

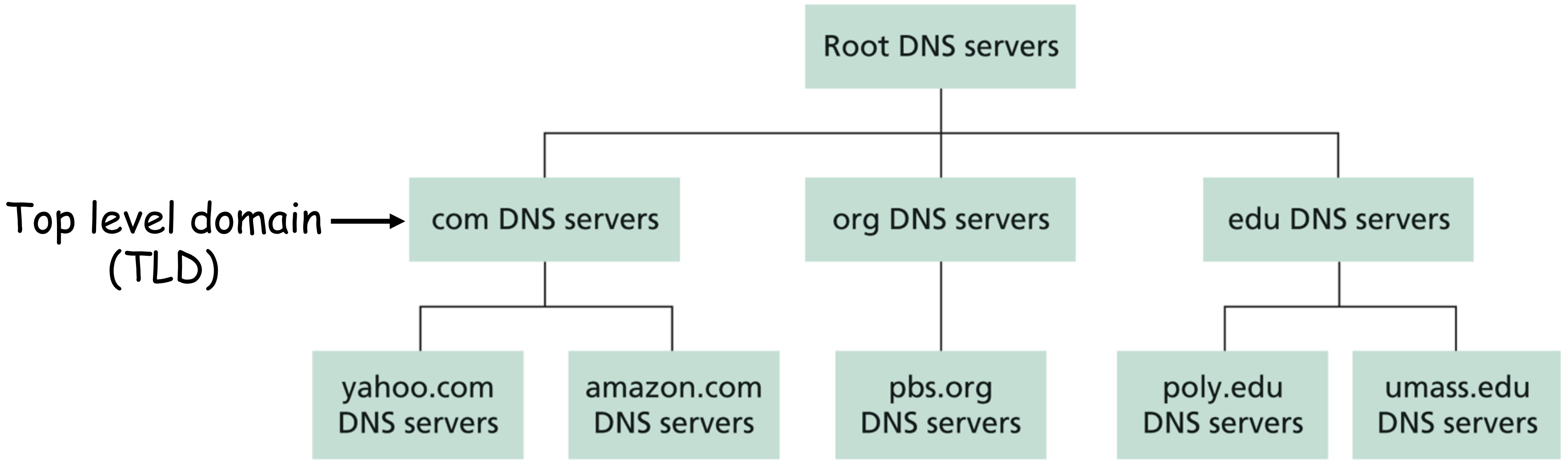


a. Verisign, Dulles, VA
c. Cogent, Herndon, VA (also Los Angeles)
d. U Maryland College Park, MD
g. US DoD Vienna, VA
h. ARL Aberdeen, MD
j. Verisign, (11 locations)
e. NASA Mt View, CA
f. Internet Software C. Palo Alto, CA (and 17 other locations)
i. Autonomica, Stockholm (plus 3 other locations)
k. RIPE London (also Amsterdam, Frankfurt)
m. WIDE Tokyo
b. USC-ISI Marina del Rey, CA
l. ICANN Los Angeles, CA

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

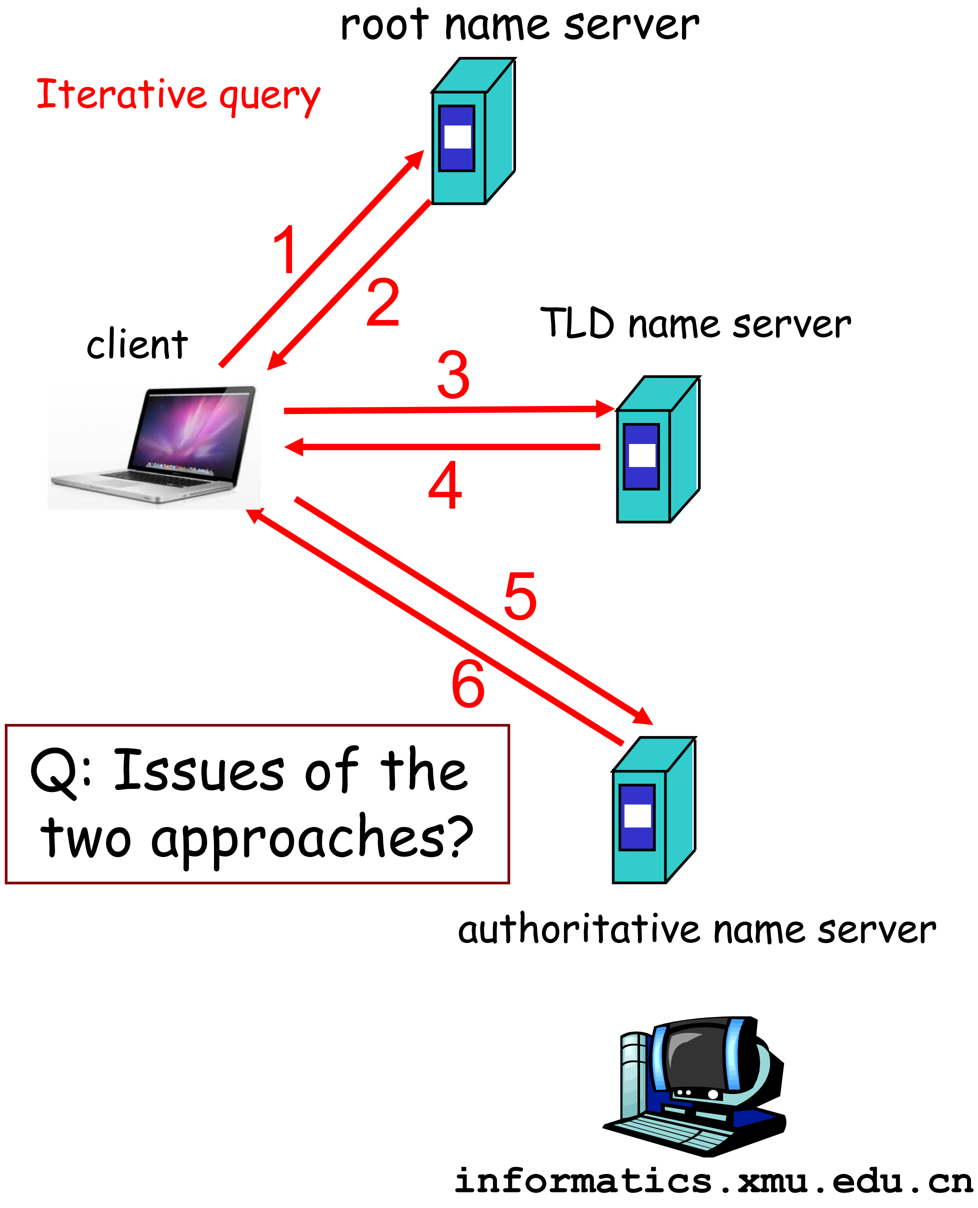
Recursive query:

- The contacted name server resolves the name completely

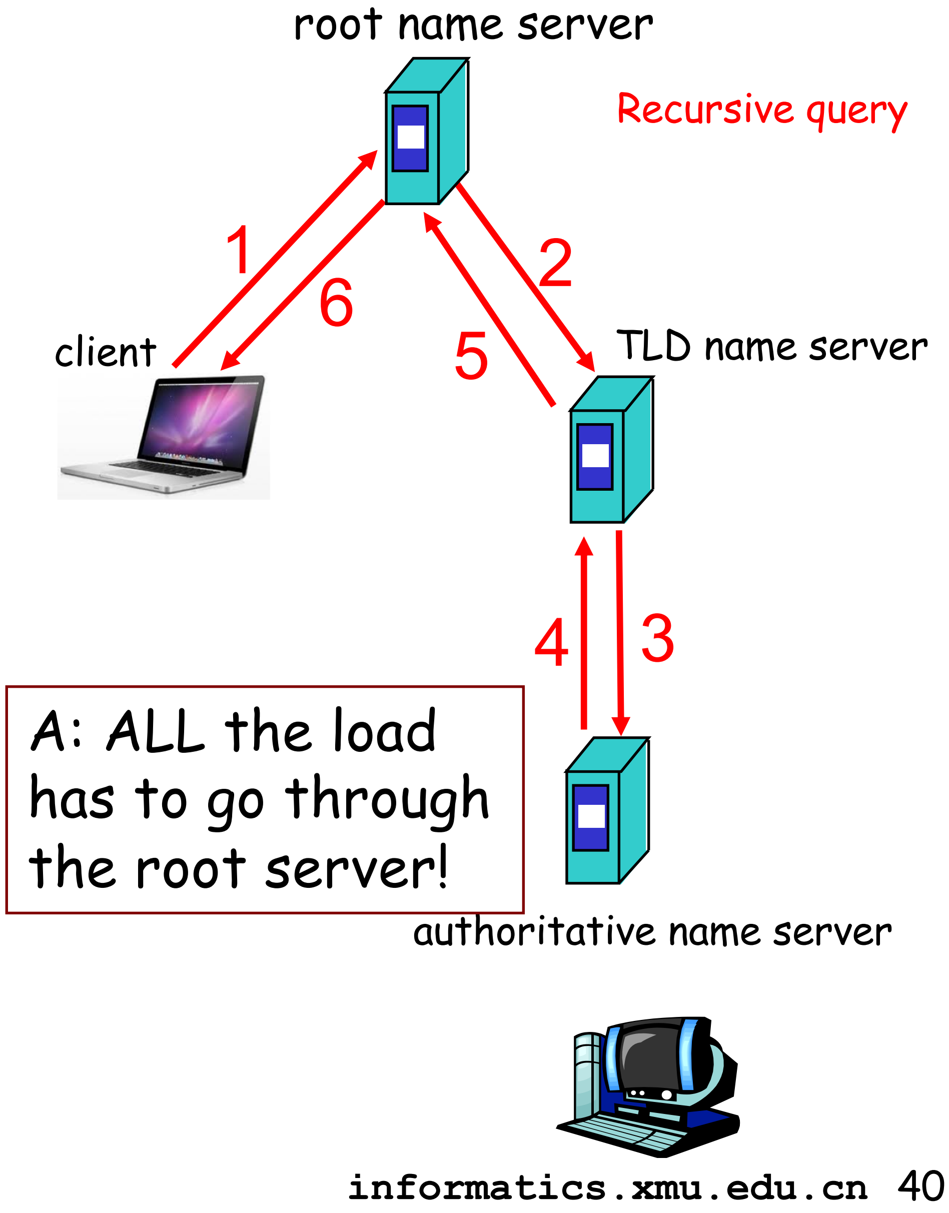
Iterated query:

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

Two Extreme DNS Message Flows



Q: Issues of the two approaches?



A: ALL the load has to go through the root server!