The Application Layer

Chapter 7

DNS – The Domain Name System

A support protocol

- The DNS name space
- Domain Resource records
- Name servers

Domain name system

- Decouple machine names from machine addresses.

  {WWW.}CSIE.NTNU.EDU.TW (informative for humans) ↔ IP address=? (informative for networks)

  - ✓ In the ARPNET days, a file hosts.txt that listed all the computer names and their IP address, was maintained at one site and fetched every night by each host.
  - ✓ DNS, invented in 1983, to resolve issues on the file size and host name conflicts.

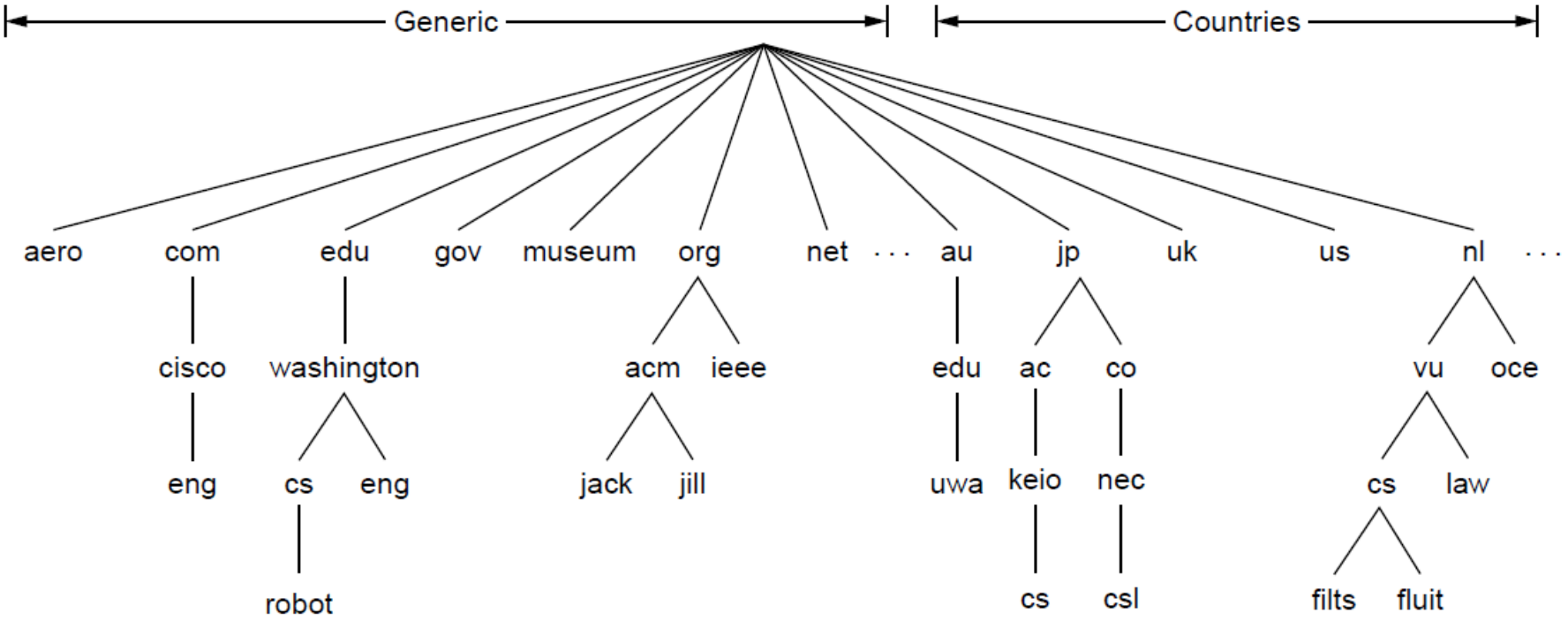
Domain name system

- Problems with a centralized design
  - ✓ A single point of failure
  - ✓ Traffic volume
  - ✓ Distant centralized database
  - ✓ Maintenance

Domain name system

- A hierarchical, domain-based naming scheme
- A distributed database system
- Use:
  - ✓ Map IP host names to IP addresses
  - ✓ … other purposes
- Example: *gethostbyname( )*, a library procedure called the **resolver**. The query and response are primarily sent as UDP packets on port 53.

The DNS Name Space (1)



A portion of the Internet domain name space.

The DNS Name Space (2)

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

Generic top-level domains

The DNS Name Space

- Hierarchical
  - ✓ Each domain is named by the path upward from it to the root.
  - ✓ csie.ntnu.edu.tw.
- Domain names can be either absolute or relative.
  - ✓ An absolute domain name ends with a period.

a) Domain names are case-insensitive
  - ✓ EDU, Edu, and edu mean the same thing.

- Each domain control how it allocates the domains under it.
- Naming follows organizational boundary, not physical networks.

DNS Name space

- Component names, each label, can be up from zero (reserved for root zone) to 63 bytes long.
  - ✓ In the domain name hierarchy, each label to the left specifies a subdivision, or subdomain of the domain to the right→ www.example.com.
  - ✓ The full domain name must not exceed the length of 253 characters. In the internal binary representation, the maximum length requires 255 octets of storage, because the length of the domain name is also stored.

Domain Resource Records

- Every domain can have a set of resource records(RR) associated with it.
  - They are the DNS database.
- The primary function of DNS is to map domain names on RRs.

Domain Resource records (RR), in RFC1035

- NAME (Variable, domain_name)
- TYPE (2 bytes)
- CLASS (2 bytes, *IN* for Internet information)
- TTL (4 bytes, counted in sec)
- RDLENGTH (2 bytes)
- RDATA (variable, determined by RDLENGTH)

Domain Resource Records (1)

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

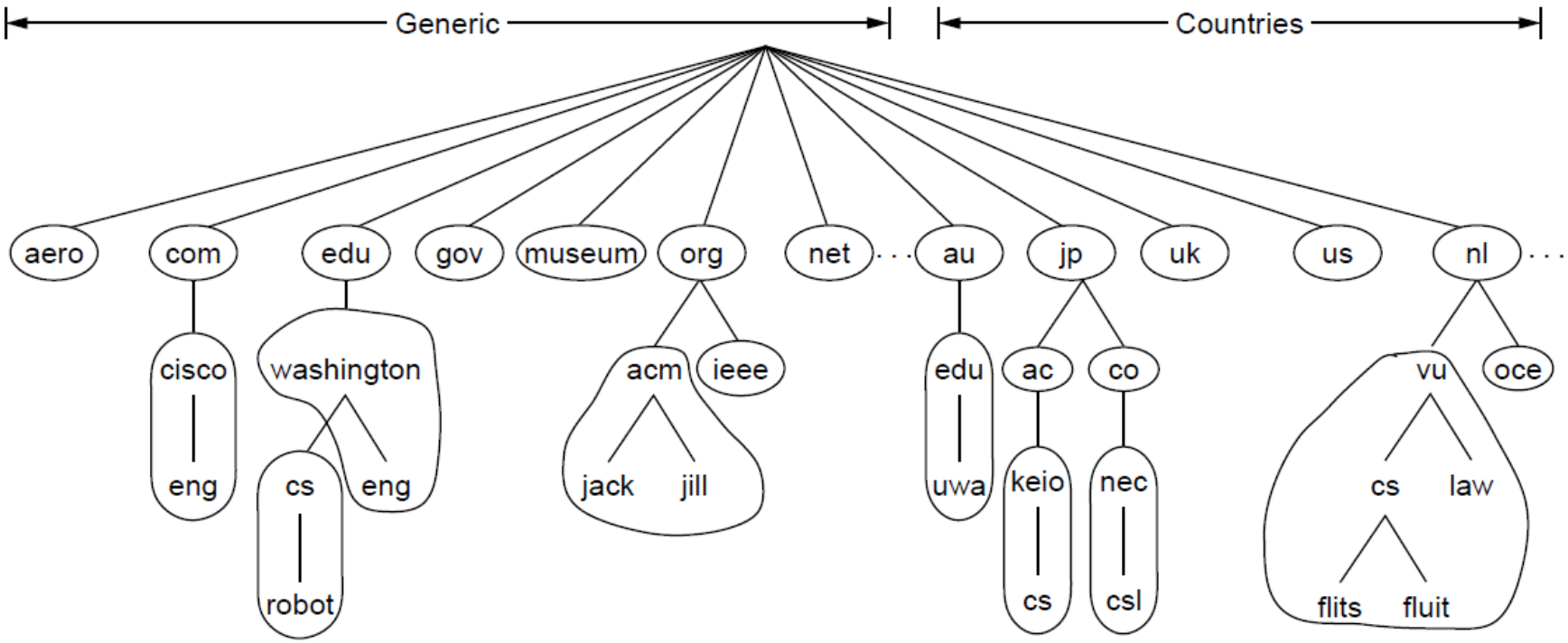
The principal DNS resource record types

Domain Resource Records (2)

```
; Authoritative data for cs.vu.nl
cs.vu.nl.       86400   IN   SOA      star boss (9527,7200,7200,241920,86400)
cs.vu.nl.       86400   IN   MX       1 zephyr
cs.vu.nl.       86400   IN   MX       2 top
cs.vu.nl.       86400   IN   NS       star

star            86400   IN   A        130.37.56.205
zephyr          86400   IN   A        130.37.20.10
top             86400   IN   A        130.37.20.11
www             86400   IN   CNAME    star.cs.vu.nl
ftp             86400   IN   CNAME    zephyr.cs.vu.nl

flits           86400   IN   A        130.37.16.112
flits           86400   IN   A        192.31.231.165
flits           86400   IN   MX       1 flits
flits           86400   IN   MX       2 zephyr
flits           86400   IN   MX       3 top

rowboat                 IN   A        130.37.56.201
                        IN   MX       1 rowboat
                        IN   MX       2 zephyr

little-sister           IN   A        130.37.62.23

laserjet                IN   A        192.31.231.216
```

A portion of a possible DNS database for *cs.vu.nl.*

Name Servers (1)

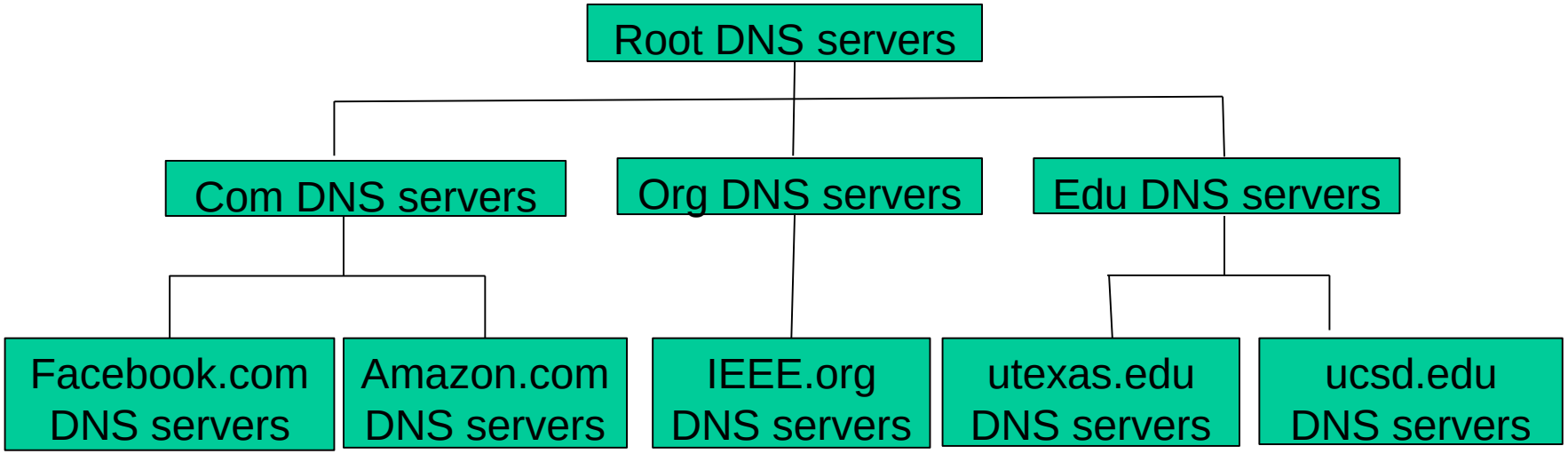


Part of the DNS name space divided into zones (which are circled).

A distributed, hierarchical database

Three classes of DNS servers

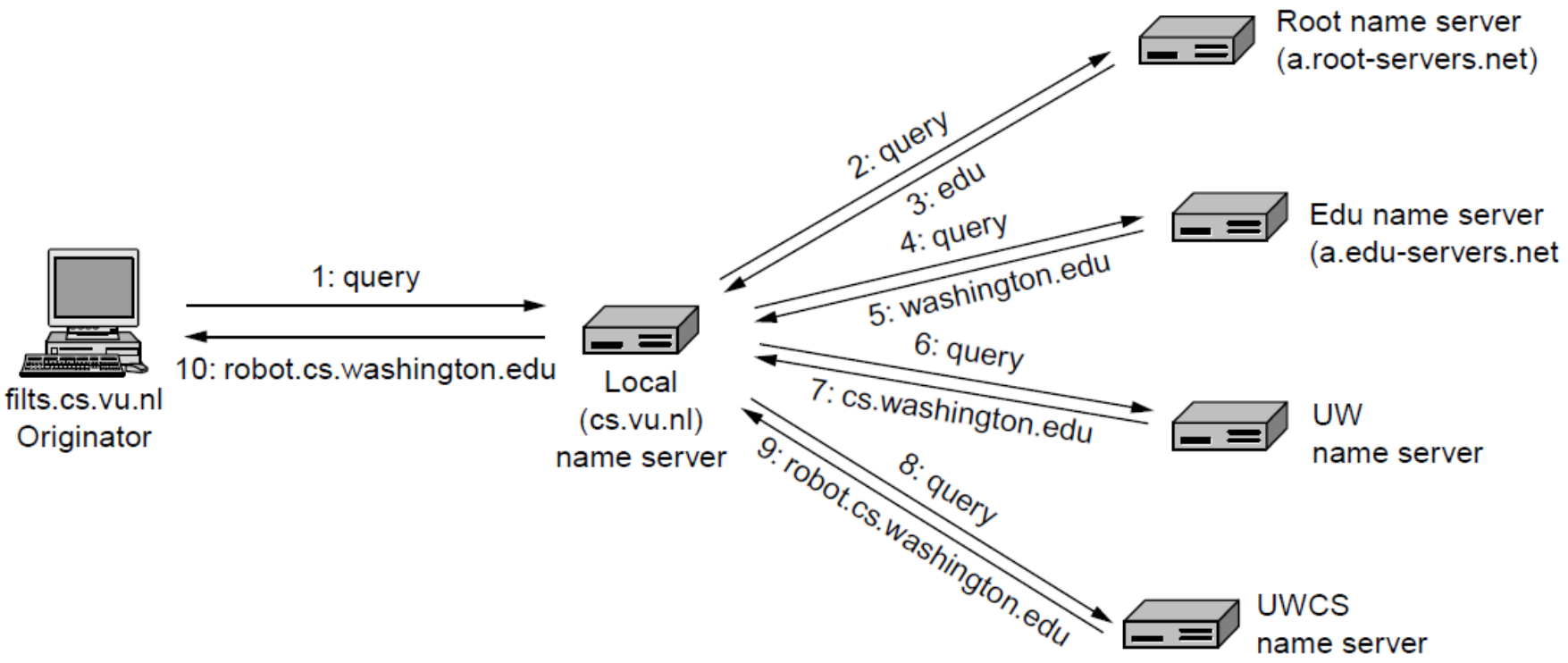
- Root DNS servers
  - ✓ Provide the IP addresses of the TLD servers
- Top-level domain (TLD) servers
- Authoritative DNS servers



Root DNS servers

- Managed by 13 different organizations (limited to 13 server address)
  - ✓ called *a-root-servers.net* through *m-root-servers.net*
- The root domain does not have a formal name and its label in the DNS hierarchy is an empty string.
  - ✓ WWW.example.com.
- Protocols: UDP and anycast
- More than 984 instances all over the world as of 2 May 2019
- The root domain contains all top-level domains of the Internet, more than 1058 TLDs (generic, country-code, ARPA, test)

Name Servers (2)



Example of a resolver looking up a remote name in 10 steps.

(By both *recursive* queries and *iterative* queries)

Try: *nslookup* hostname

dig @a.edu-servers.net robot.cs.washington.edu

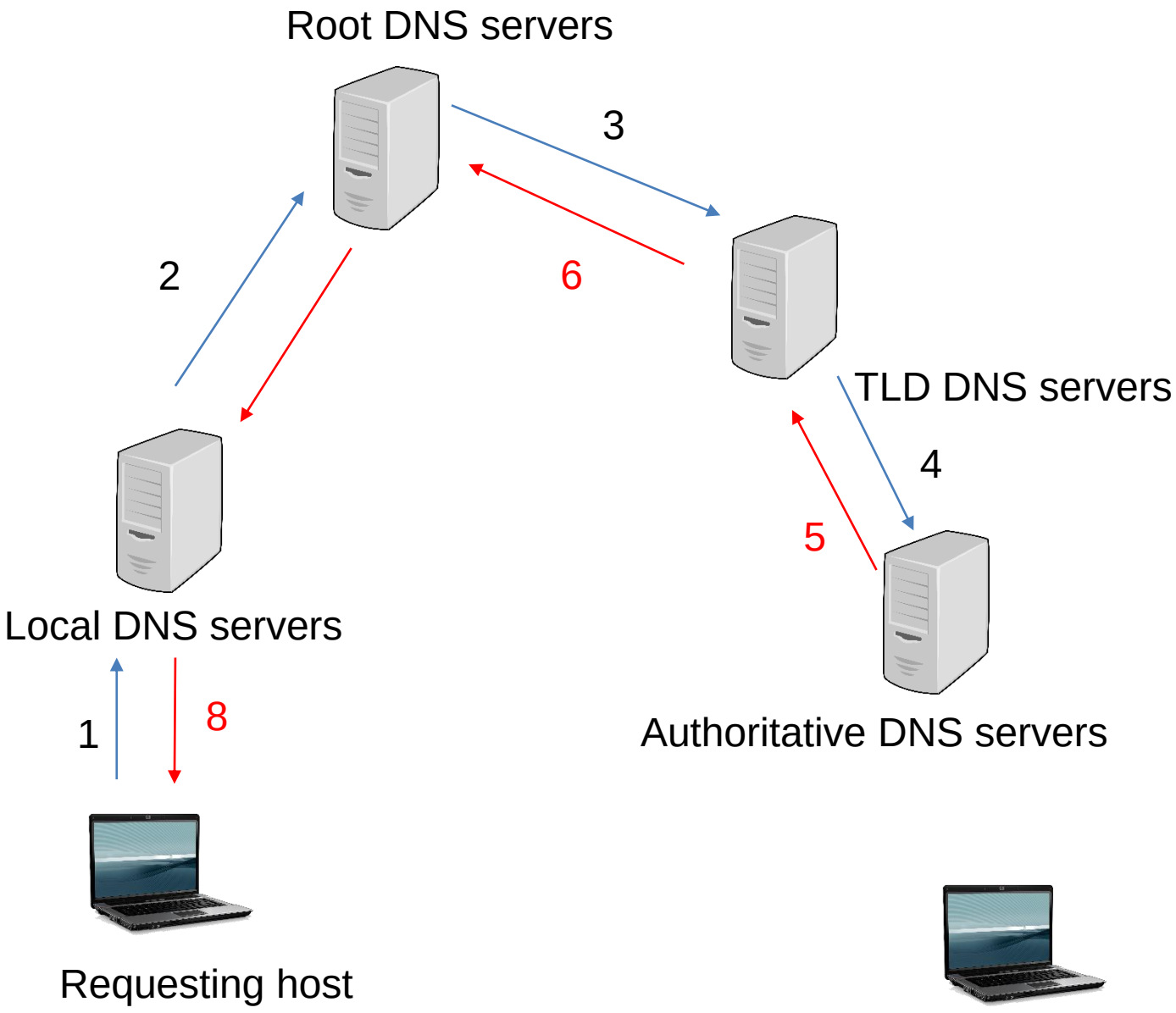
```
; <<>> DiG 9.7.3 <<>> @a.edu-servers.net robot.cs.washington.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56566
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;robot.cs.washington.edu.       IN      A

;; AUTHORITY SECTION:
washington.edu.         172800  IN      NS      marge.cac.washington.edu.
washington.edu.         172800  IN      NS      hanna.cac.washington.edu.
washington.edu.         172800  IN      NS      holly.s.uw.edu.

;; ADDITIONAL SECTION:
marge.cac.washington.edu. 172800 IN     A       140.142.5.13
marge.cac.washington.edu. 172800 IN     AAAA    2607:4000:200:43::13
hanna.cac.washington.edu. 172800 IN     A       140.142.5.5
hanna.cac.washington.edu. 172800 IN     AAAA    2607:4000:200:42::5
holly.s.uw.edu.         172800  IN      A       173.250.227.69
holly.s.uw.edu.         172800  IN      AAAA    2607:4000:301:1::69

;; Query time: 82 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sun Jun  2 20:51:37 2019
;; MSG SIZE  rcvd: 242
```

DNS

On Name resolution

- An **authoritative record** is one that comes from the authority that manages the record. ↔ **cached record**
- Queries, by both methods
  - ✓ Recursive
  - ✓ Iterative
- DNS caching
  - Using cached answers reduces the steps in query and improve performance.
- DNS messages are sent in UDP packets.
  - A 16-bit identifier is included in each query and copied into the response.
- Replication and cashing for performance

BIND, a widely used DNS software on the Internet.



Recursive queries in DNS

Electronic Mail

- Architecture and services
- The user agent
- Message formats
- Message transfer
- Final delivery

Electronic Mail

- 1st email systems consisted of file transfer protocols.
  - ✓ 1st line of each message(file) contained the recipient's address.
- Added features:
  - ✓ To a list of recipients
  - ✓ Multimedia: Send messages with images and other non-text material
- Mail readers, mail transfer protocol, spam…

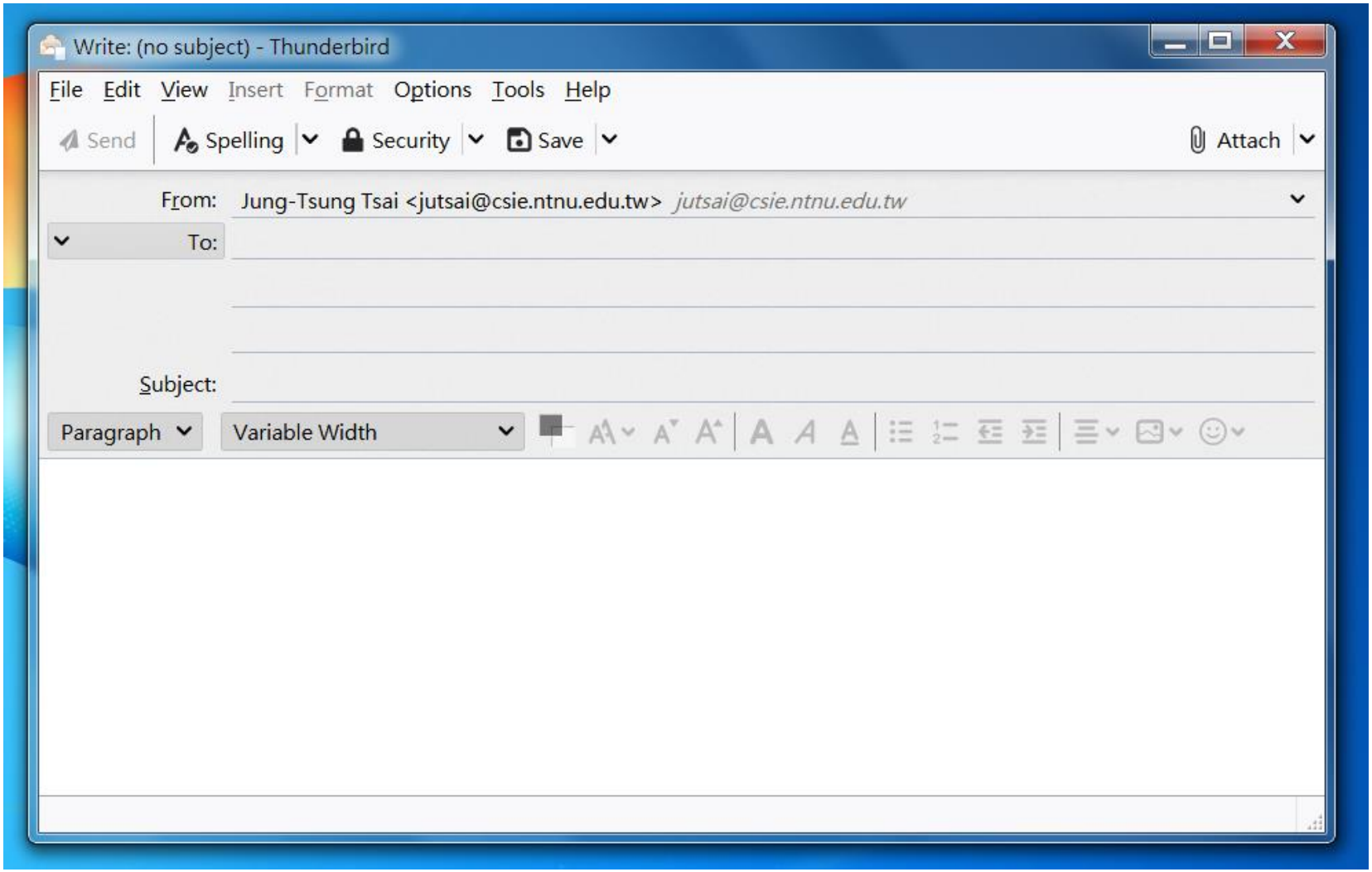
The Architecture of email system

Two kind of subsystems:

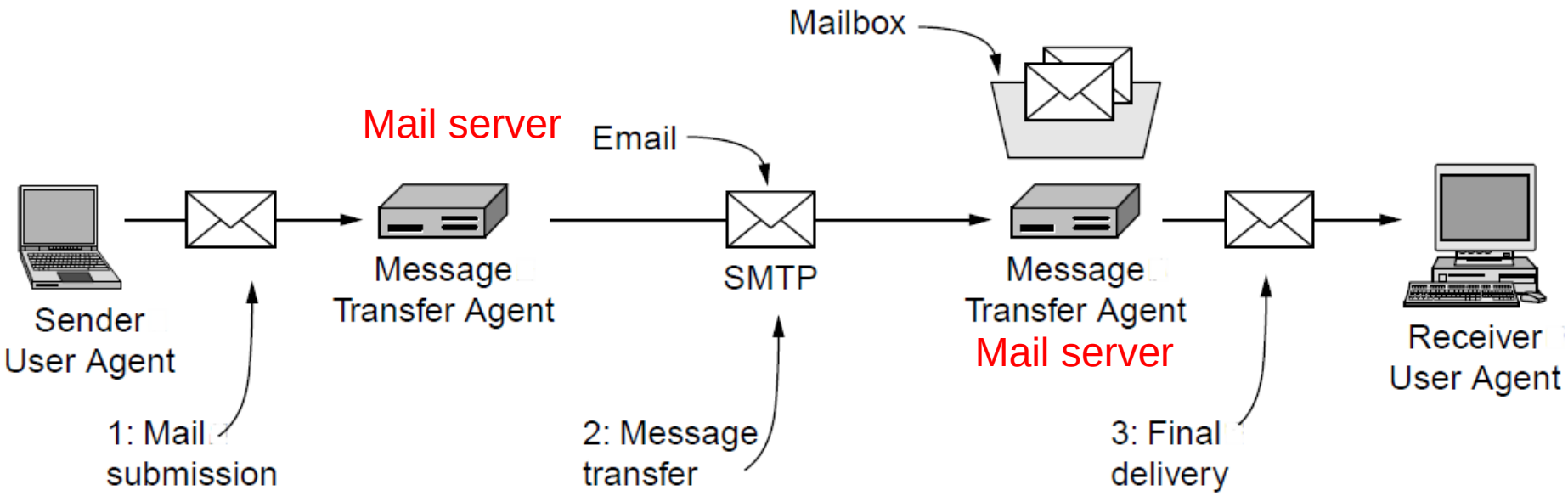
- User agents (called email readers sometimes)
  - ✓ Allow people to read and write email.
- Message transfer agents
  - ✓ Mail servers
  - ✓ Move email through the system from the originator to the recipient with SMTP (Simple Mail Transfer Protocol, a push protocol)
  - ✓ Mailing lists, Cc, Bcc, …

Both are linked through the concept of mailboxes and a standard format for email messages.

Write an email through an email reader



Architecture and Services (1)



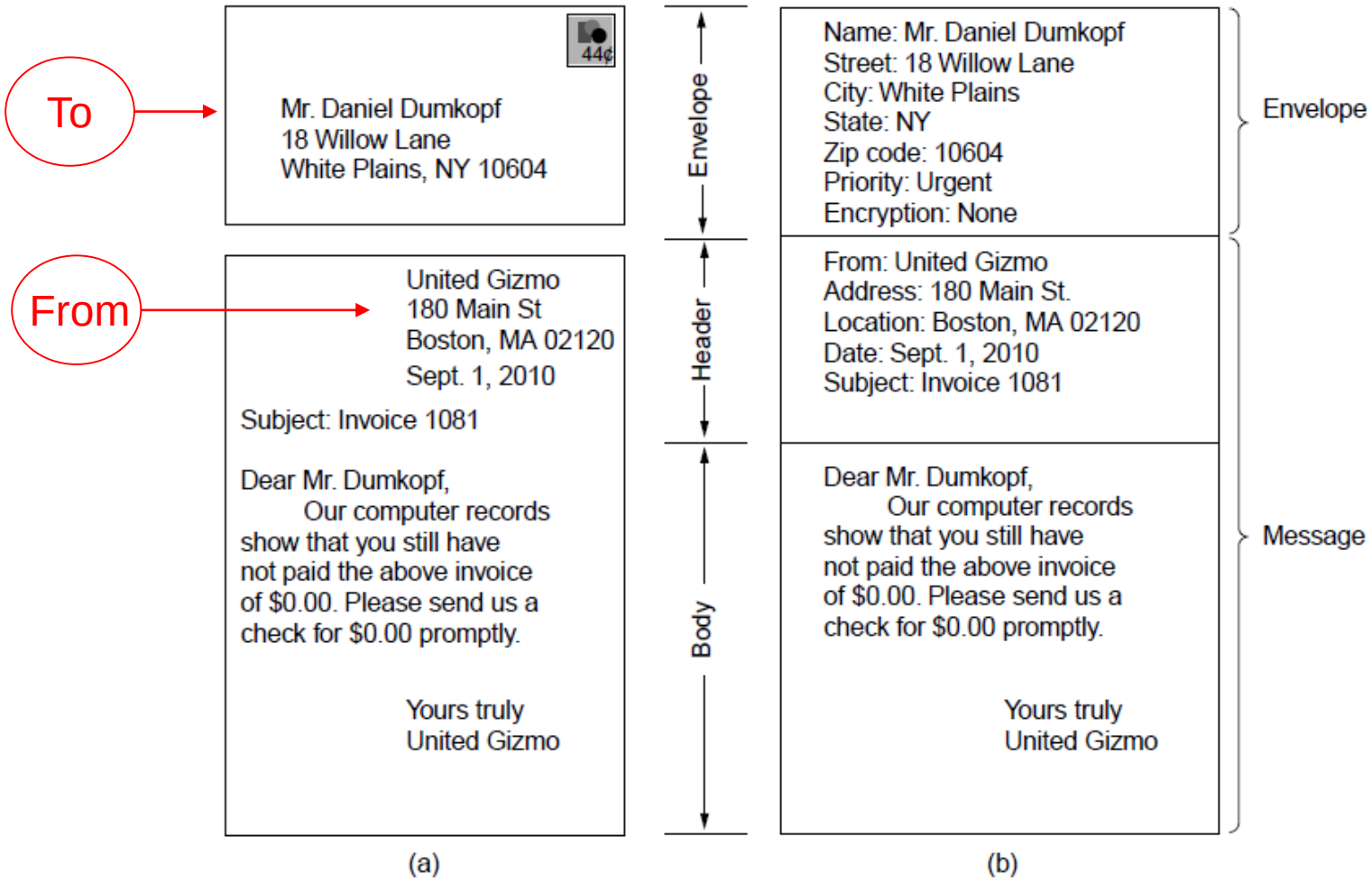
Architecture of the email system

Architecture and Services

- Mailboxes store the email that is received for a user.
- User agents present users with a view of the contents of their mailboxes.
- Email message format
  - ✓ Envelope
    - ✓ All information needed for transporting the message.
    - ✓ The message transport agent use the envelope for routing.
  - ✓ Contents (messages)
    - ✓ Header

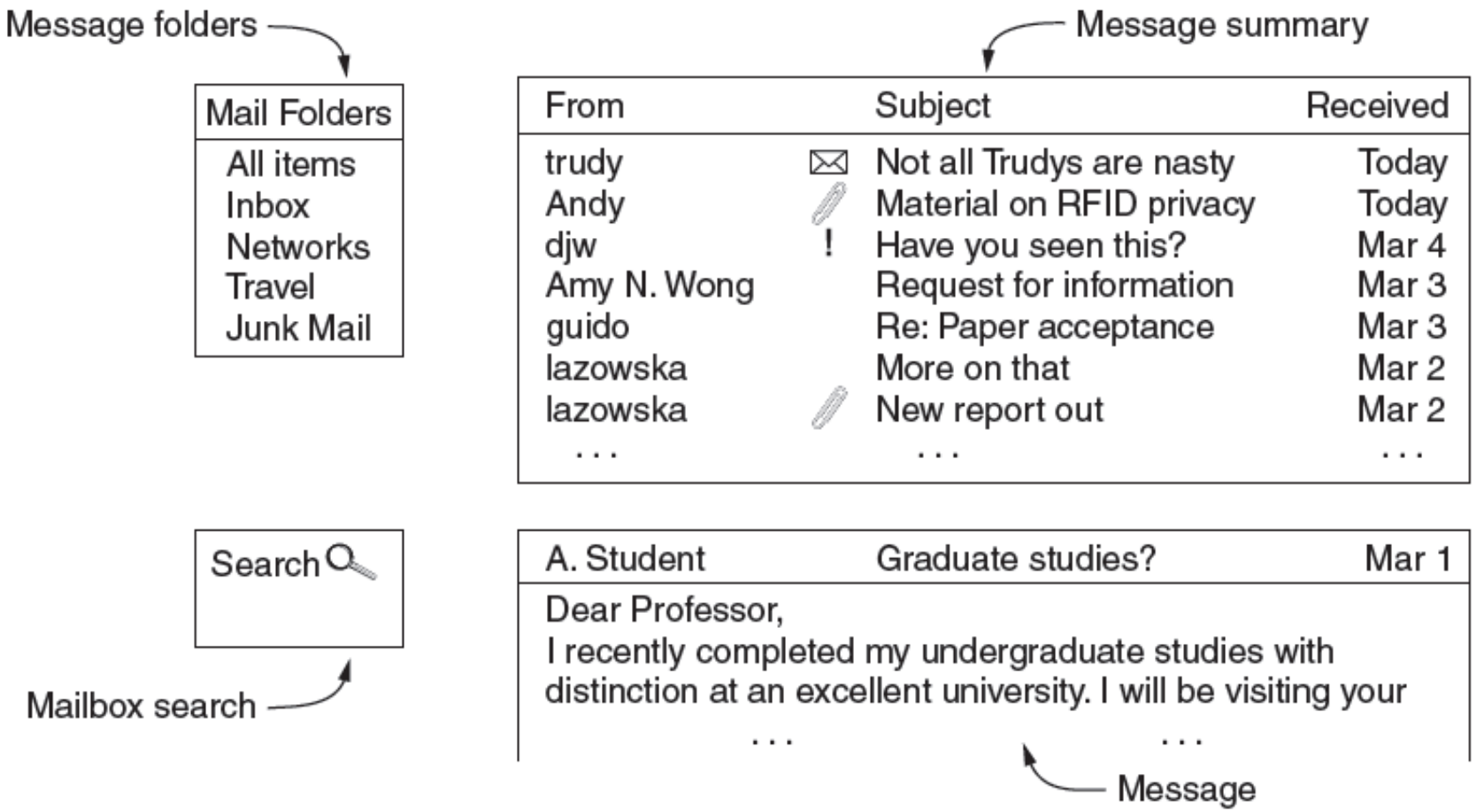
      Control information for user agents
    - ✓ Body

Architecture and Services (2)



Envelopes and messages. (a) Paper mail. (b) Electronic mail.

The User Agent



Typical elements of the user agent interface

Message Formats (1)

Header	Meaning
To:	Email address(es) of primary recipient(s)
Cc:	Email address(es) of secondary recipient(s)
Bcc:	Email address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	Email address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

RFC 5322 header fields related to message transport.

Message Formats (2)

Header	Meaning
Date:	The date and time the message was sent
Reply-To:	Email address to which replies should be sent
Message-Id:	Unique number for referencing this message later
In-Reply-To:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User-chosen keywords
Subject:	Short summary of the message for the one-line display

Some fields used in the RFC 5322 message header.

Message Formats (3)

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

Message headers added by MIME.

Message Formats (4)

Type	Example subtypes	Description
text	plain, html, xml, css	Text in various formats
image	gif, jpeg, tiff	Pictures
audio	basic, mpeg, mp4	Sounds
video	mpeg, mp4, quicktime	Movies
model	vrml	3D model
application	octet-stream, pdf, javascript, zip	Data produced by applications
message	http, rfc822	Encapsulated message
multipart	mixed, alternative, parallel, digest	Combination of multiple types

MIME content types and example subtypes.

Message Transfer (1)

```
From: alice@cs.washington.edu
To: bob@ee.uwa.edu.au
MIME-Version: 1.0
Message-Id: <0704760941.AA00747@cs.washington.edu>
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
Subject: Earth orbits sun integral number of times

This is the preamble. The user agent ignores it. Have a nice day.

--qwertyuiopasdfghjklzxcvbnm
Content-Type: text/html

<p>Happy birthday to you<br>
Happy birthday to you<br>
Happy birthday dear <b> Bob </b><br>
Happy birthday to you</p>
```

. . .

A multipart message containing HTML and audio alternatives.

Message Transfer (2)

. . .

```
--qwertyuiopasdfghjklzxcvbnm
Content-Type: message/external-body;
        access-type="anon-ftp";
        site="bicycle.cs.washington.edu";
        directory="pub";
        name="birthday.snd"

content-type: audio/basic
content-transfer-encoding: base64
--qwertyuiopasdfghjklzxcvbnm--
```

A multipart message containing HTML and audio alternatives.

Message Transfer (3)

```
                    S: 220 ee.uwa.edu.au SMTP service ready
C: HELO abcd.com
                    S: 250 cs.washington.edu says hello to ee.uwa.edu.au
C: MAIL FROM: <alice@cs.washington.edu>
                    S: 250 sender ok
C: RCPT TO: <bob@ee.uwa.edu.au>
                    S: 250 recipient ok
C: DATA
                    S: 354 Send mail; end with "." on a line by itself
C: From: alice@cs.washington.edu
C: To: bob@ee.uwa.edu.au
C: MIME-Version: 1.0
C: Message-Id: <0704760941.AA00747@ee.uwa.edu.au>
C: Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
C: Subject: Earth orbits sun integral number of times
C:
C: This is the preamble. The user agent ignores it. Have a nice day.
C:
C: --qwertyuiopasdfghjklzxcvbnm
C: Content-Type: text/html
C:
```

. . .

Sending a message from *alice@cs.washingt n.edu* to *bob@ee.uwa.edu.au.*

Message Transfer (4)

. . .

```
C: <p>Happy birthday to you
C: Happy birthday to you
C: Happy birthday dear <bold> Bob </bold>
C: Happy birthday to you
C:
C: --qwertyuiopasdfghjklzxcvbnm
C: Content-Type: message/external-body;
C:          access-type="anon-ftp";
C:          site="bicycle.cs.washington.edu";
C:          directory="pub";
C:          name="birthday.snd"
C:
C: content-type: audio/basic
C: content-transfer-encoding: base64
C: --qwertyuiopasdfghjklzxcvbnm
C: .
                        S: 250 message accepted
C: QUIT
                        S: 221 ee.uwa.edu.au closing connection
```

Sending a message from *alice@cs.washington.edu* to *bob@ee.uwa.edu.au.*

Message Transfer (5)

Keyword	Description
AUTH	Client authentication
BINARYMIME	Server accepts binary messages
CHUNKING	Server accepts large messages in chunks
SIZE	Check message size before trying to send
STARTTLS	Switch to secure transport (TLS; see Chap. 8)
UTF8SMTP	Internationalized addresses

Some SMTP extensions.

Final Delivery (1)

Command	Description
CAPABILITY	List server capabilities
STARTTLS	Start secure transport (TLS; see Chap. 8)
LOGIN	Log on to server
AUTHENTICATE	Log on with other method
SELECT	Select a folder
EXAMINE	Select a read-only folder
CREATE	Create a folder
DELETE	Delete a folder
RENAME	Rename a folder
SUBSCRIBE	Add folder to active set
UNSUBSCRIBE	Remove folder from active set

. . .

IMAP (version 4) commands.

Final Delivery (2)

...

LIST	List the available folders
LSUB	List the active folders
STATUS	Get the status of a folder
APPEND	Add a message to a folder
CHECK	Get a checkpoint of a folder
FETCH	Get messages from a folder
SEARCH	Find messages in a folder
STORE	Alter message flags
COPY	Make a copy of a message in a folder
EXPUNGE	Remove messages flagged for deletion
UID	Issue commands using unique identifiers
NOOP	Do nothing
CLOSE	Remove flagged messages and close folder
LOGOUT	Log out and close connection

IMAP (version 4) commands.

The World Wide Web

- Architectural overview
- Static web pages
- Dynamic web pages, web applications
- The hypertext transfer protocol
- The mobile web
- Web search