Application Layer

MODULE-2

Chapter 2: Application layer

Creating a network app

write programs that:

- ❖ run on (different) *end systems*
- ❖ communicate over network
- ❖ e.g., web server software communicates with browser software

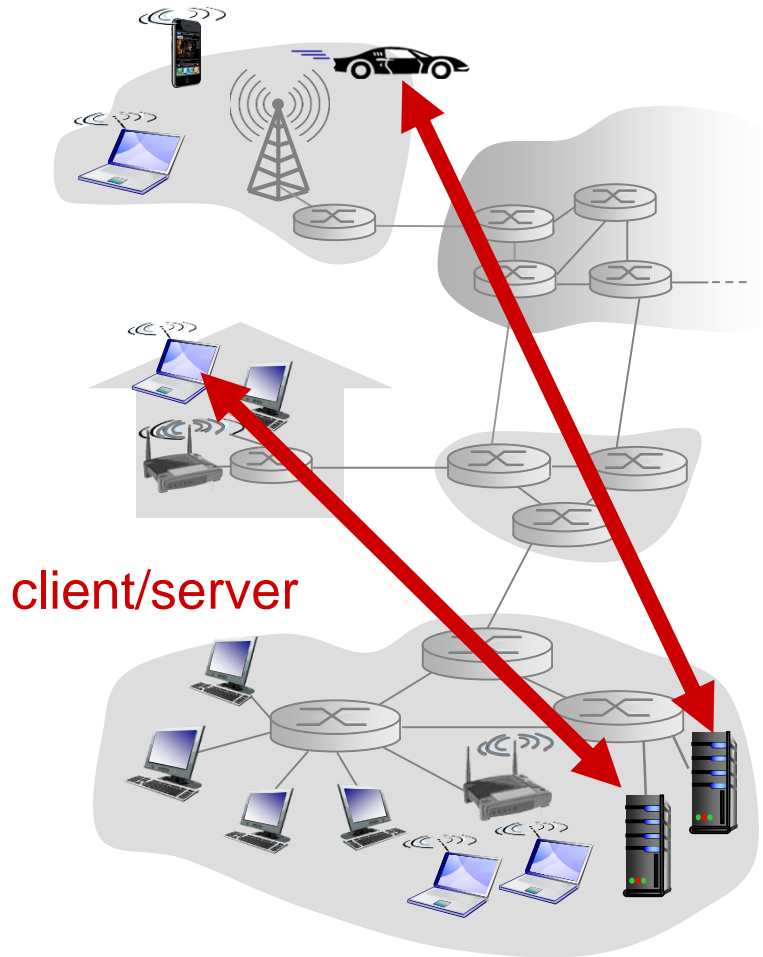no need to write software for network-core devices

- ❖ network-core devices do not run user applications
- ❖ applications on end systems allows for rapid app development, propagation
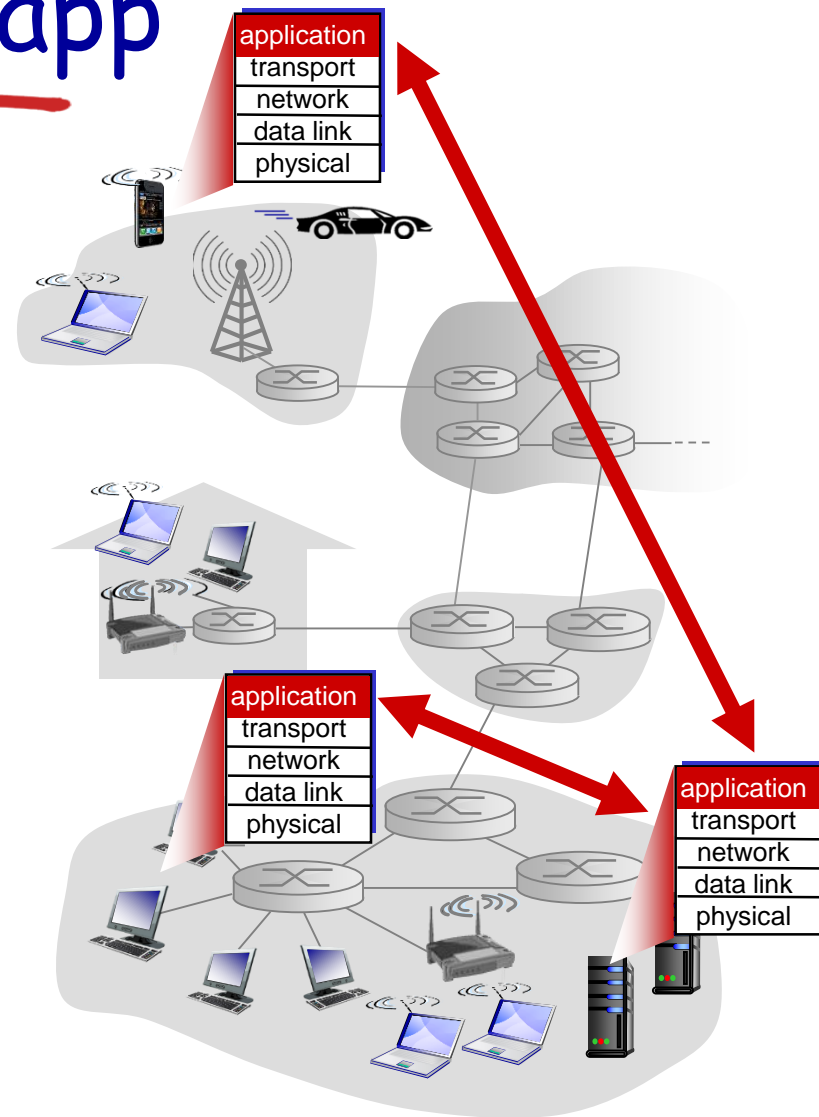
Application architectures

☐ Client-server

☐ Peer-to-peer (P2P)

☐ Hybrid of client-server and P2P

Client-server architecture

client/server

server:
- always-on host
- permanent IP address
- data centers for scaling

clients:
- communicate with server
- may be intermittently connected
- may have dynamic IP addresses
- do not communicate directly with each other

P2P architecture

- ❖ *no* always-on server
- ❖ arbitrary end systems directly communicate
- ❖ peers request service from other peers, provide service in return to other peers
  - ▪ *self scalability* – new peers bring new service capacity, as well as new service demands
- ❖ peers are intermittently connected and change IP addresses
  - ▪ complex management

peer-peer
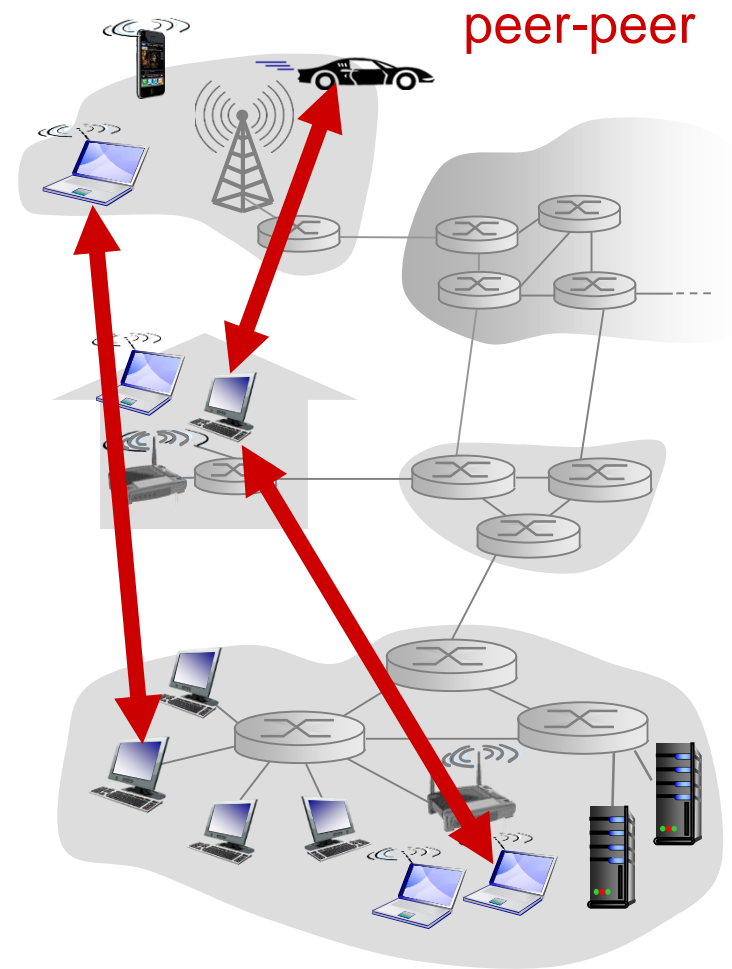
Hybrid of client-server and P2P

Skype
- ❖ voice-over-IP P2P application
- ❖ centralized server: finding address of remote party:
- ❖ client-client connection: direct (not through server)

Instant messaging
- ❖ chatting between two users is P2P
- ❖ centralized service: client presence detection/location
  - • user registers its IP address with central server when it comes online
  - • user contacts central server to find IP addresses of buddies

Processes communicating

Process: program running within a host.

- within same host, two processes communicate using inter-process communication (defined by OS).
- processes in different hosts communicate by exchanging messages
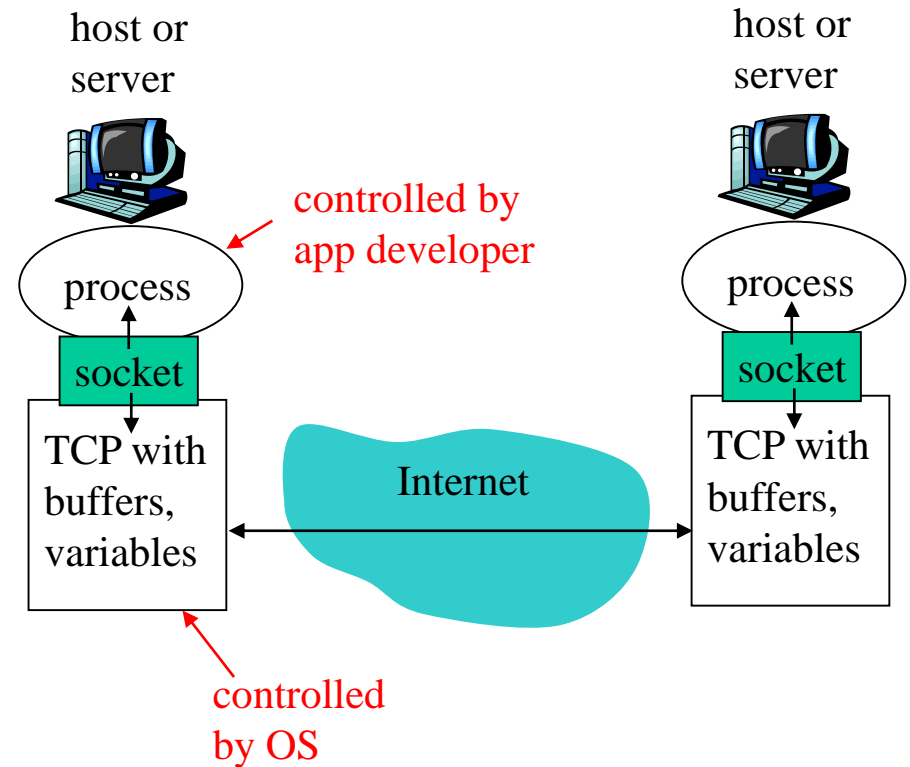
Client process: process that initiates communication

Server process: process that waits to be contacted

- Note: applications with P2P architectures have client processes & server processes

Sockets

- process sends/receives messages to/from its software interface **socket**

- socket analogous to door
  - ❖ sending process shoves message out door
  - ❖ sending process relies on transport infrastructure on other side of door which brings message to socket at receiving process

host or server

host or server

controlled by app developer

process

process

socket

socket

TCP with buffers, variables

Internet

TCP with buffers, variables

controlled by OS

- API: (1) choice of transport protocol; (2) ability to fix a few parameters(Buffer, segment…)

Addressing processes

- ❒ to receive messages, process must have *identifier*

- ❒ host device has unique 32-bit IP address

- ❒ *Q:* does IP address of host suffice for identifying the process?

Addressing processes

□ to receive messages, process must have *identifier*

□ host device has unique 32-bit IP address

□ *Q:* does IP address of host on which process runs suffice for identifying the process?

  ❖ *A:* No, *many processes can be running on same host*

□ *identifier* includes both IP address and port numbers associated with process on host.

□ Example port numbers:
  ❖ HTTP server: 80
  ❖ Mail server: 25

□ to send HTTP message to gaia.cs.umass.edu web server:
  ❖ IP address: 128.119.245.12
  ❖ Port number: 80

App-layer protocol defines

□ Types of messages exchanged,
  ❖ e.g., request, response
□ Message syntax:
  ❖ what fields in messages & how fields are delineated
□ Message semantics
  ❖ meaning of information in fields
□ Rules for when and how processes send & respond to messages

Public-domain protocols:
□ defined in RFCs
□ allows for interoperability
□ e.g., HTTP, SMTP
Proprietary protocols:
□ e.g., Skype

What transport service does an app need?

Data loss

□ some apps (e.g., audio) can tolerate some loss

□ other apps (e.g., file transfer, telnet) require 100% reliable data transfer

Timing

□ some apps (e.g., Internet telephony, interactive games) require low delay to be "effective".

Throughput

□ some apps (e.g., multimedia) require minimum amount of throughput to be "effective"

□ other apps ("elastic apps") make use of whatever throughput they get

Security

□ Encryption, data integrity, …

Transport service requirements of common apps

Application	Data loss	Throughput	Time Sensitive
file transfer	no loss	elastic	no
e-mail	no loss	elastic	no
Web documents	no loss	elastic	no
real-time audio/video	loss-tolerant	audio: 5kbps-1Mbps video:10kbps-5Mbps	yes, 100's msec
stored audio/video	loss-tolerant	same as above	yes, few secs
interactive games	loss-tolerant	few kbps up	yes, 100's msec
instant messaging	no loss	elastic	yes and no

Internet transport protocols services

TCP service:

- *connection-oriented:* setup required between client and server processes
- *reliable transport* between sending and receiving process
- *flow control:* sender won't overwhelm receiver
- *congestion control:* throttle sender when network overloaded
- *does not provide:* timing, minimum throughput guarantees, security

UDP service:

- unreliable data transfer between sending and receiving process
- does not provide: connection setup, reliability, flow control, congestion control, timing, throughput guarantee, or security

Q: why bother? Why is there a UDP?

Internet apps: application, transport protocols

Application	Application layer protocol	Underlying transport protocol
e-mail	SMTP [RFC 2821]	TCP
remote terminal access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
file transfer	FTP [RFC 959]	TCP
streaming multimedia	HTTP (eg Youtube), RTP [RFC 1889]	TCP or UDP
Internet telephony	SIP, RTP, proprietary (e.g., Skype)	typically UDP

Chapter 2: Application layer

Web and HTTP

First some jargon

- Web page consists of objects
- Object can be HTML file, JPEG image, Java applet, audio file,…
- Web page consists of base HTML-file which includes several referenced objects
- Each object is addressable by a URL
- Example URL:

```
www.someschool.edu/someDept/pic.gif
```

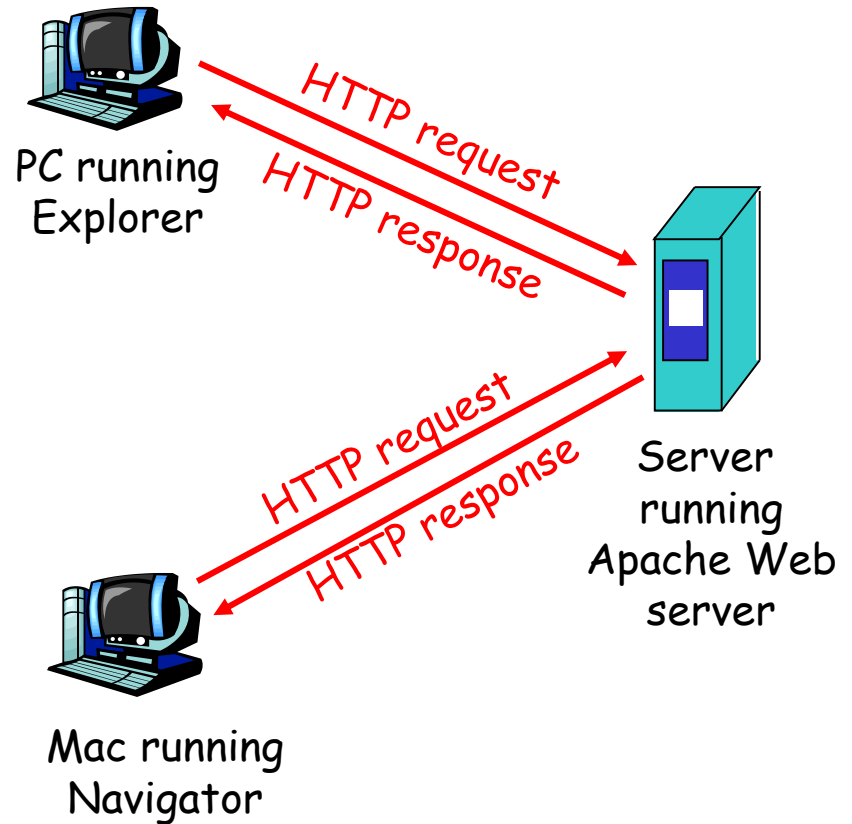host name   path name

HTTP overview

HTTP: hypertext transfer protocol

□ Web's application layer protocol

□ client/server model

❖ *client:* browser that requests, receives, "displays" Web objects

❖ *server:* Web server sends objects in response to requests

PC running Explorer

HTTP request

HTTP response

Mac running Navigator

HTTP request

HTTP response

Server running Apache Web server

HTTP overview (continued)

Uses TCP:

- client initiates TCP connection (creates socket) to server, port 80
- server accepts TCP connection from client
- HTTP messages (application-layer protocol messages) exchanged between browser (HTTP client) and Web server (HTTP server)
- TCP connection closed

HTTP is "stateless"

- server maintains no information about past client requests

aside

Protocols that maintain "state" are complex!

- past history (state) must be maintained
- if server/client crashes, their views of "state" may be inconsistent, must be reconciled

HTTP connections

Nonpersistent HTTP
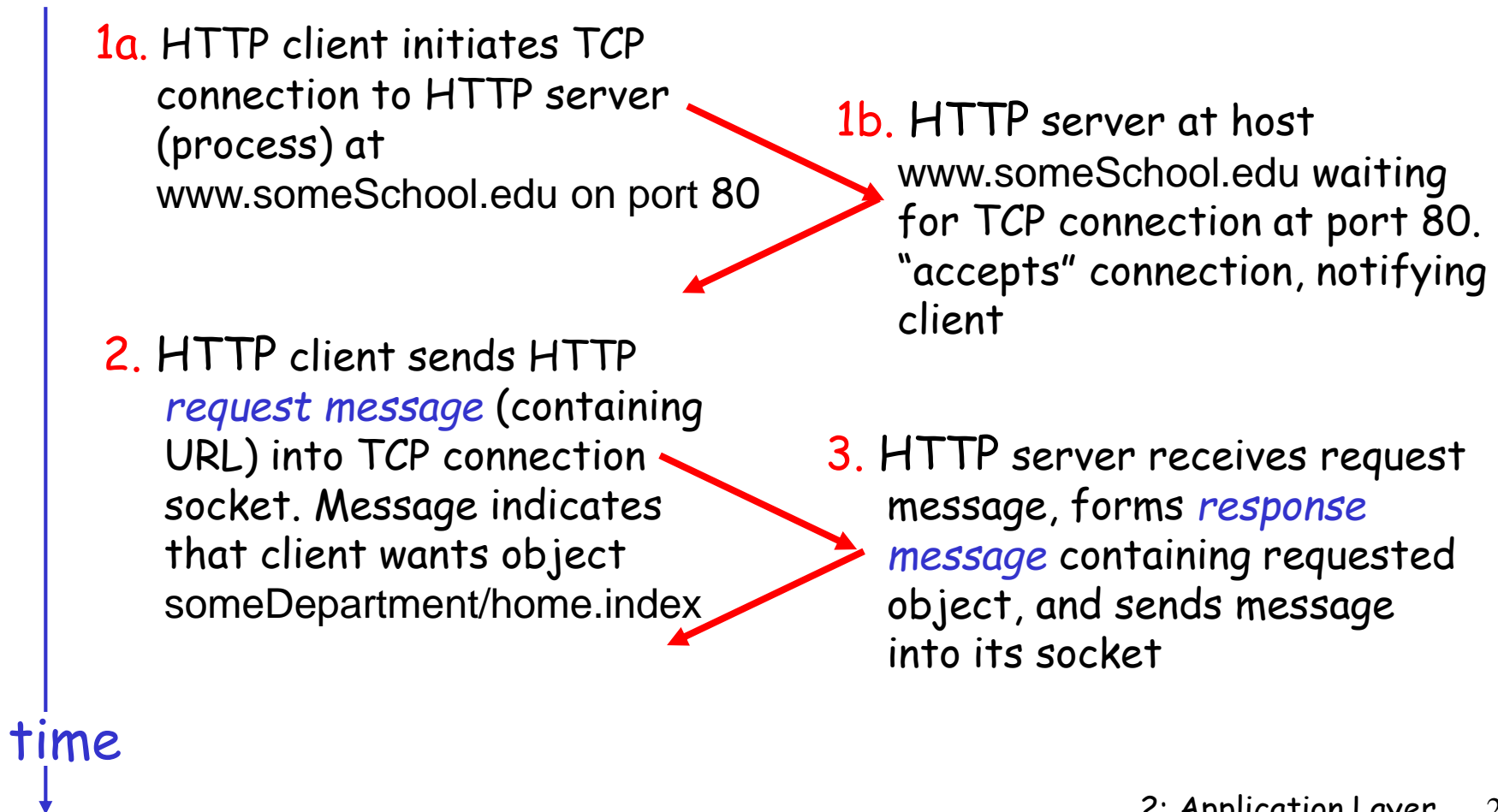
☐ At most one object is sent over a TCP connection. Connection then closed.

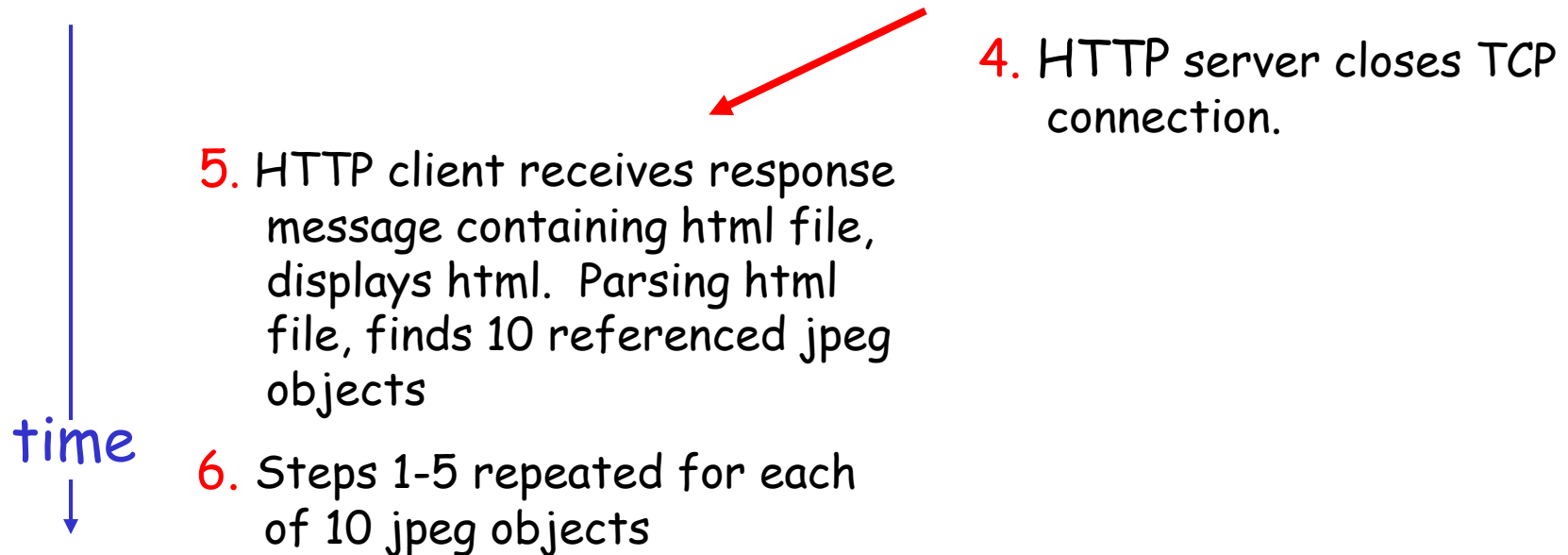☐ downloading multiple objects required multiple connections

Persistent HTTP

☐ Multiple objects can be sent over single TCP connection between client and server.

Nonpersistent HTTP

Suppose user enters URL `www.someSchool.edu/someDepartment/home.index` (contains text, references to 10 jpeg images)

1a. HTTP client initiates TCP connection to HTTP server (process) at www.someSchool.edu on port 80

1b. HTTP server at host www.someSchool.edu waiting for TCP connection at port 80. "accepts" connection, notifying client

2. HTTP client sends HTTP *request message* (containing URL) into TCP connection socket. Message indicates that client wants object someDepartment/home.index

3. HTTP server receives request message, forms *response message* containing requested object, and sends message into its socket

time

Nonpersistent HTTP (cont.)

time

4. HTTP server closes TCP connection.

5. HTTP client receives response message containing html file, displays html. Parsing html file, finds 10 referenced jpeg objects

6. Steps 1-5 repeated for each of 10 jpeg objects

Non-Persistent HTTP: Response time

Definition of RTT: time for a small packet to travel from client to server and back.

Response time:

☐ one RTT to initiate TCP connection

☐ one RTT for HTTP request and first few bytes of HTTP response to return

☐ file transmission time

total = 2RTT+transmit time

initiate TCP connection

RTT

request file

RTT

time to transmit file

file received

time   time
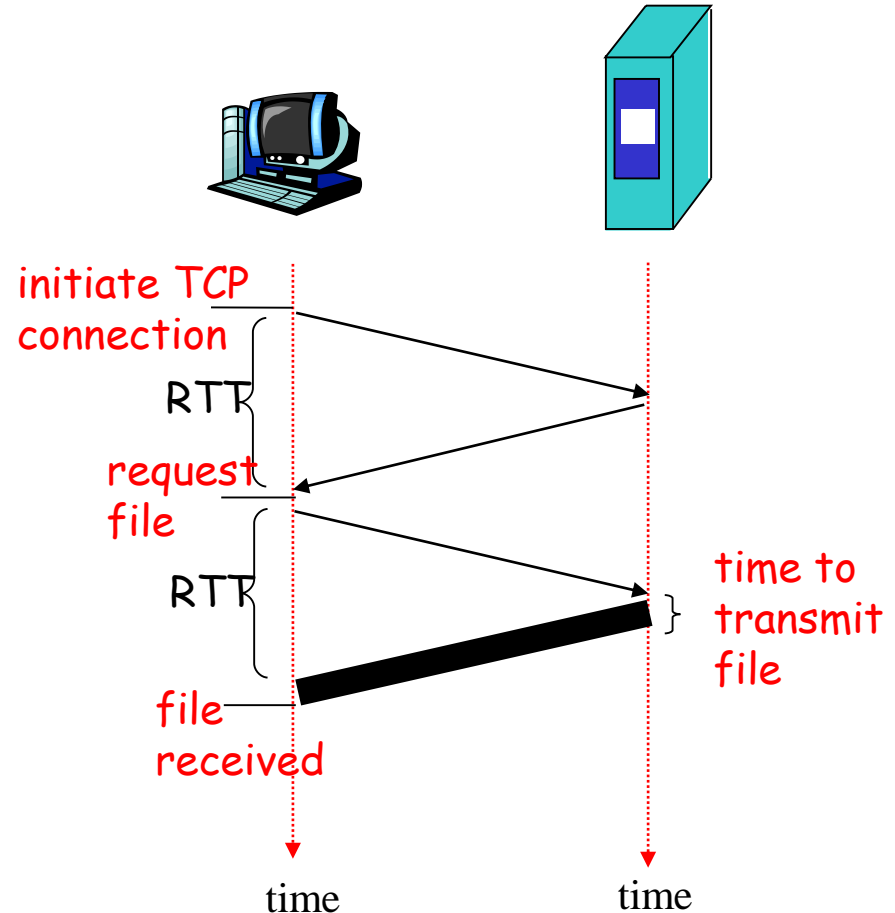
Persistent HTTP

Nonpersistent HTTP issues:

- requires 2 RTTs per object
- OS overhead for *each* TCP connection –significant burden on server.
- browsers often open parallel TCP connections to fetch referenced objects

Persistent HTTP

- server leaves connection open after sending response
- subsequent HTTP messages between same client/server sent over open connection
- client sends requests as soon as it encounters a referenced object
- as little as one RTT for all the referenced objects

HTTP request message

☐ two types of HTTP messages: *request, response*

☐ HTTP request message:
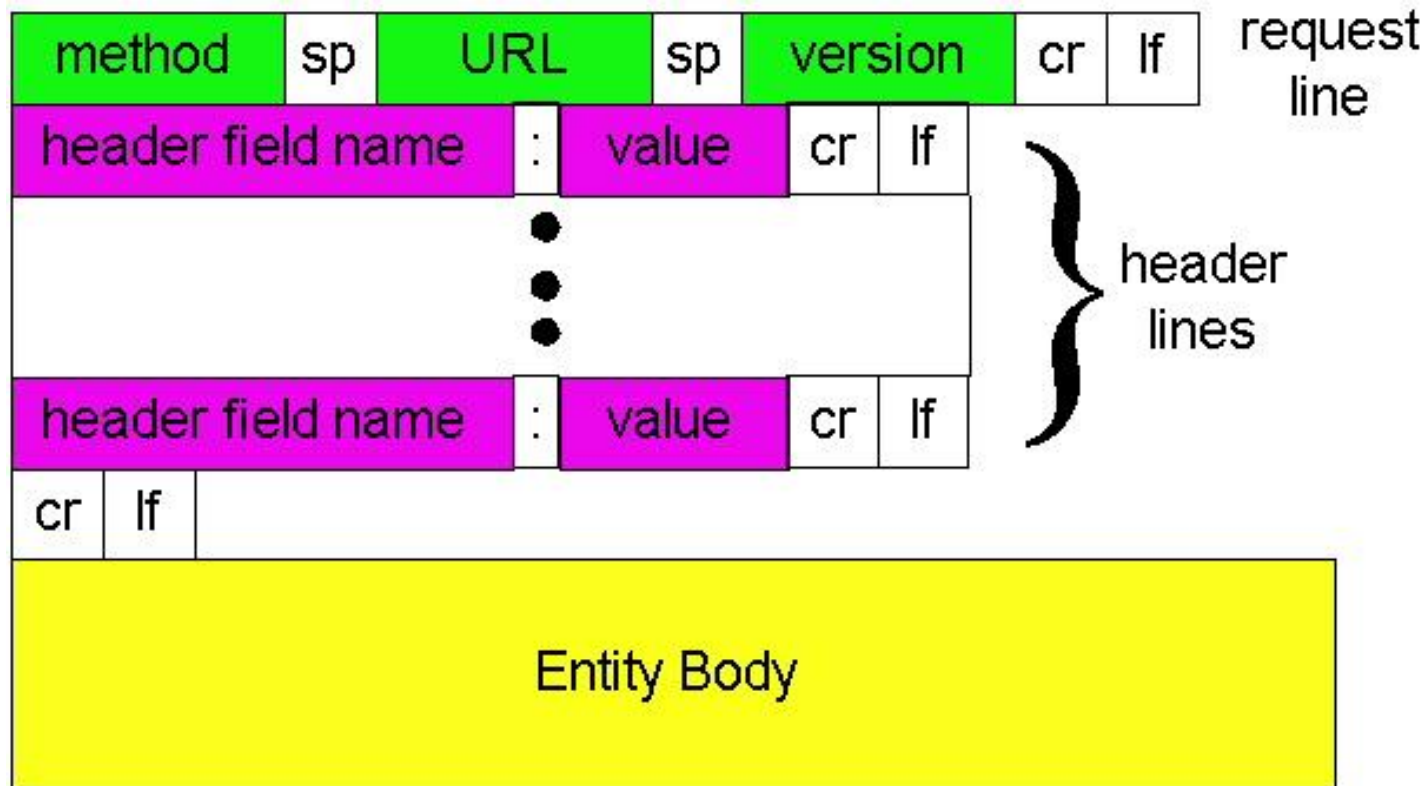 ❖ ASCII (human-readable format)

request line
(GET, POST,
HEAD commands)

```
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
User-agent: Mozilla/5.0
Connection: close
Accept-language:fr
```

header
lines

Carriage return,
line feed
indicates end
of message

(extra carriage return, line feed)

HTTP request message: general format

Uploading form input

POST method:

- ❖ web page often includes form input
- ❖ input is uploaded to server in entity body

URL method:

- ❖ uses GET method
- ❖ input is uploaded in URL field of request line:

    `www.somesite.com/animalsearch?monkeys&banana`

Contact Form

Fill out this form and we'll get back to you ASAP
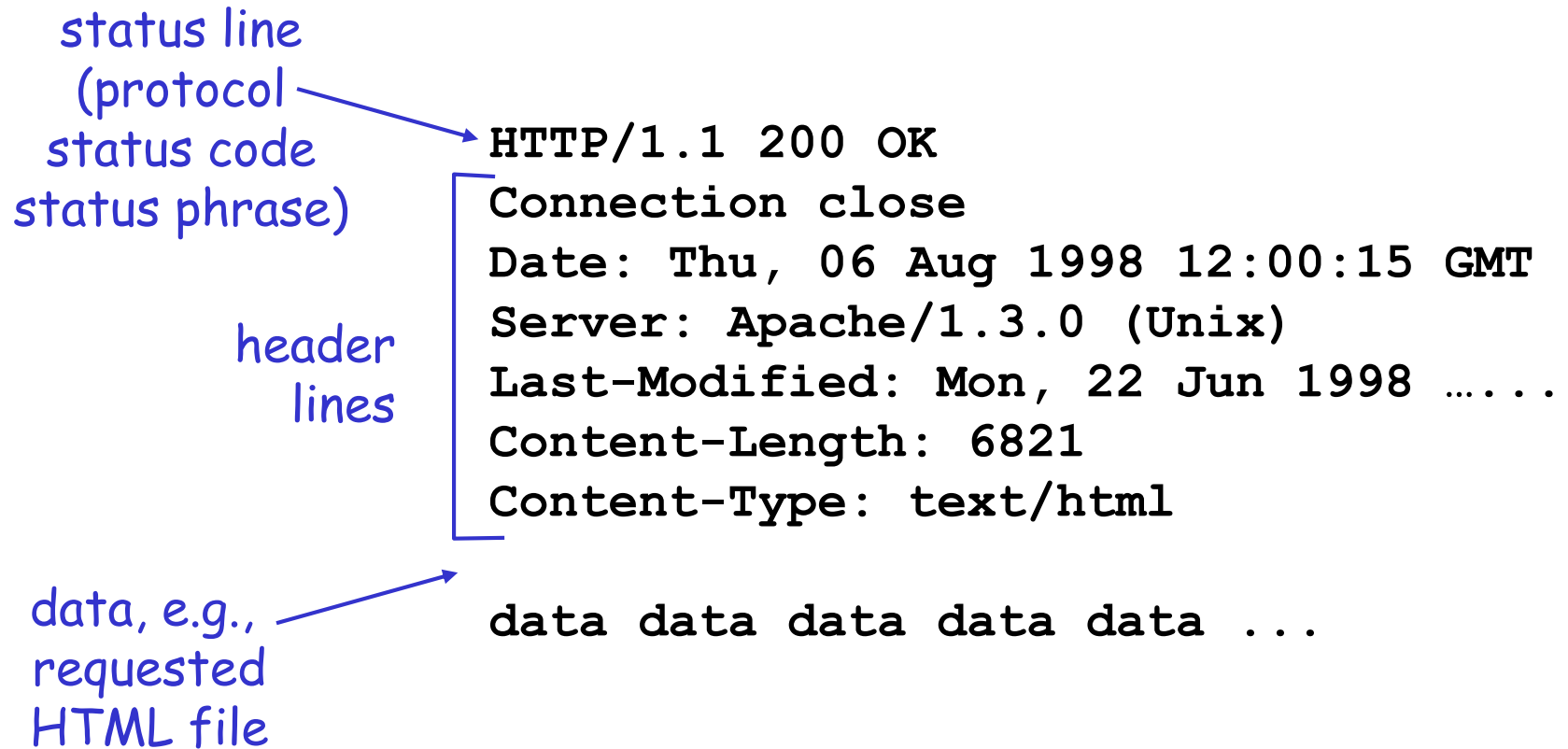
Your Name

Email

Message

Submit!

Method types

HTTP/1.0
- GET
- POST
- HEAD
  - asks server to leave requested object out of response

HTTP/1.1
- GET, POST, HEAD
- PUT
  - uploads file in entity body to path specified in URL field
- DELETE
  - deletes file specified in the URL field

HTTP response message

status line
(protocol
status code
status phrase)

```
HTTP/1.1 200 OK
Connection close
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 1998 …...
Content-Length: 6821
Content-Type: text/html
```

header
lines

data, e.g.,
requested
HTML file

```
data data data data data ...
```

HTTP response status codes

In first line in server->client response message.
A few sample codes:

200 OK

- ❖ request succeeded, requested object later in this message

301 Moved Permanently

- ❖ requested object moved, new location specified later in this message (Location:)

400 Bad Request

- ❖ request message not understood by server

404 Not Found

- ❖ requested document not found on this server

505 HTTP Version Not Supported

User-server state: cookies
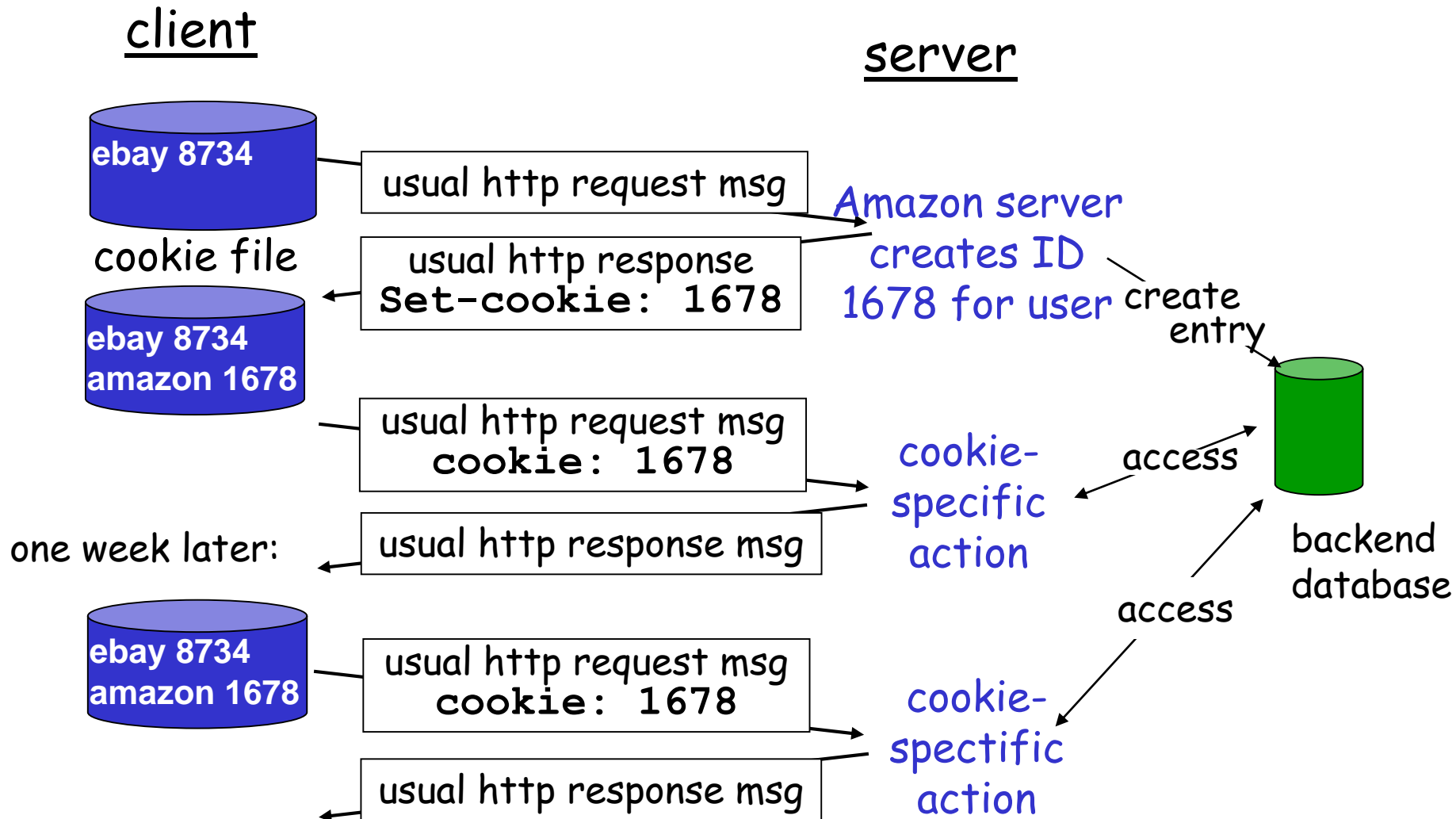
Many major Web sites use cookies

Four components:
  1) cookie header line of HTTP *response* message
  2) cookie header line in HTTP *request* message
  3) cookie file kept on user's host, managed by user's browser
  4) back-end database at Web site

Example:
- Susan always access Internet always from PC
- visits specific e-commerce site for first time
- when initial HTTP requests arrives at site, site creates:
  - unique ID
  - entry in backend database for ID

Cookies: keeping "state" (cont.)

client

server

ebay 8734

cookie file

usual http request msg

usual http response
Set-cookie: 1678

Amazon server
creates ID
1678 for user

create
entry

ebay 8734
amazon 1678

usual http request msg
cookie: 1678

usual http response msg

cookie-
specific
action

access

backend
database

one week later:

ebay 8734
amazon 1678

usual http request msg
cookie: 1678

usual http response msg

cookie-
spectific
action

access

Cookies (continued)

What cookies can bring:

- authorization
- shopping carts
- recommendations
- user session state (Web e-mail)

How to keep "state":

- protocol endpoints: maintain state at sender/receiver over multiple transactions
- cookies: http messages carry state

Cookies and privacy:

- cookies permit sites to learn a lot about you
- you may supply name and e-mail to sites

Web caches (proxy server)

Goal: satisfy client request without involving origin server

□ user sets browser: Web accesses via cache

□ browser sends all HTTP requests to cache
  - ❖ object in cache: cache returns object
  - ❖ else cache requests object from origin server, then returns object to client
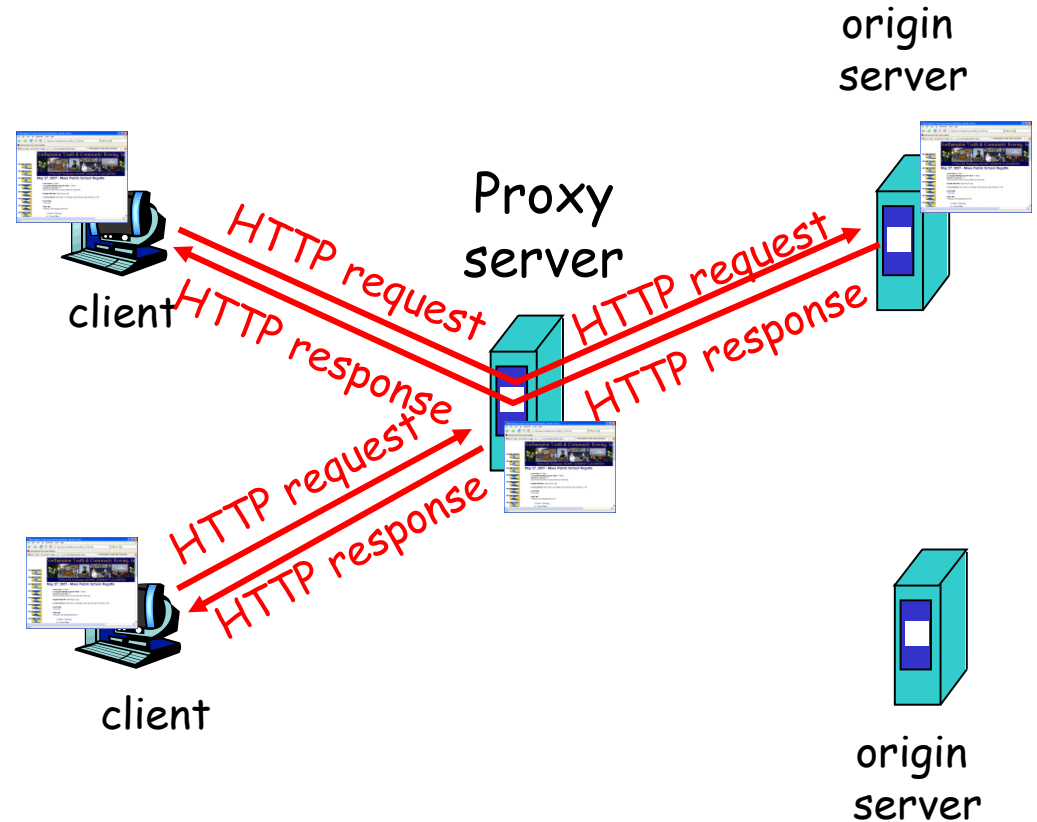
More about Web caching

- cache acts as both client and server
- typically cache is installed by ISP (university, company, residential ISP)

Why Web caching?

- reduce response time for client request
- reduce traffic on an institution's access link.
- Internet dense with caches: enables "poor" content providers to effectively deliver content.

Conditional GET

❖ *Goal:* don't send object if cache has up-to-date cached version
   ▪ no object transmission delay
   ▪ lower link utilization
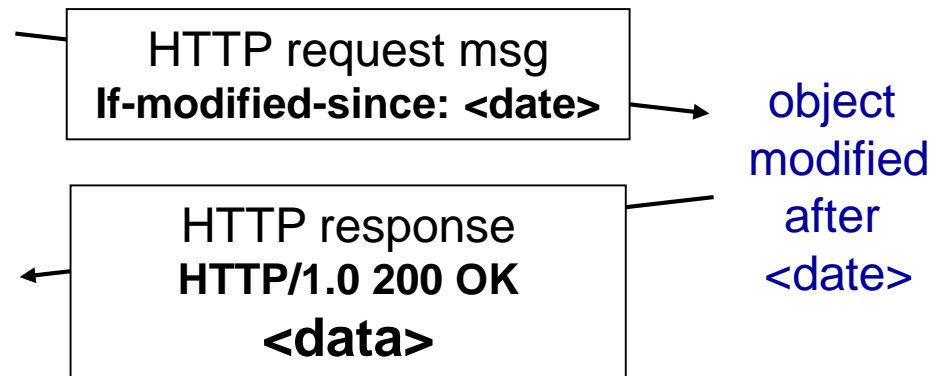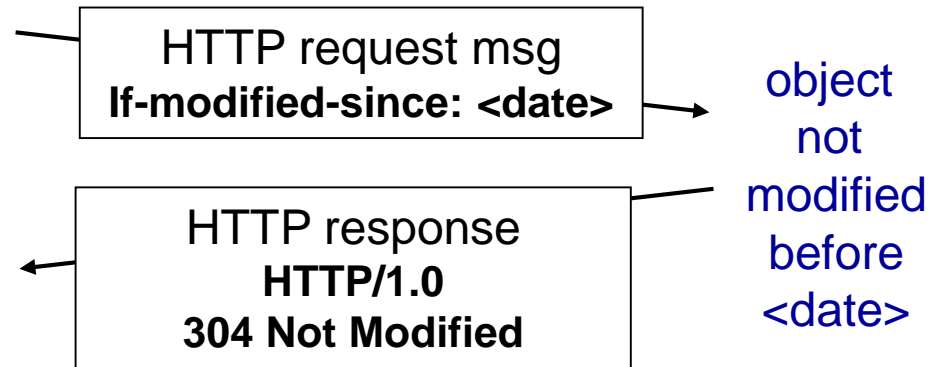
❖ *cache:* specify date of cached copy in HTTP request
   If-modified-since: <date>

❖ *server:* response contains no object if cached copy is up-to-date:
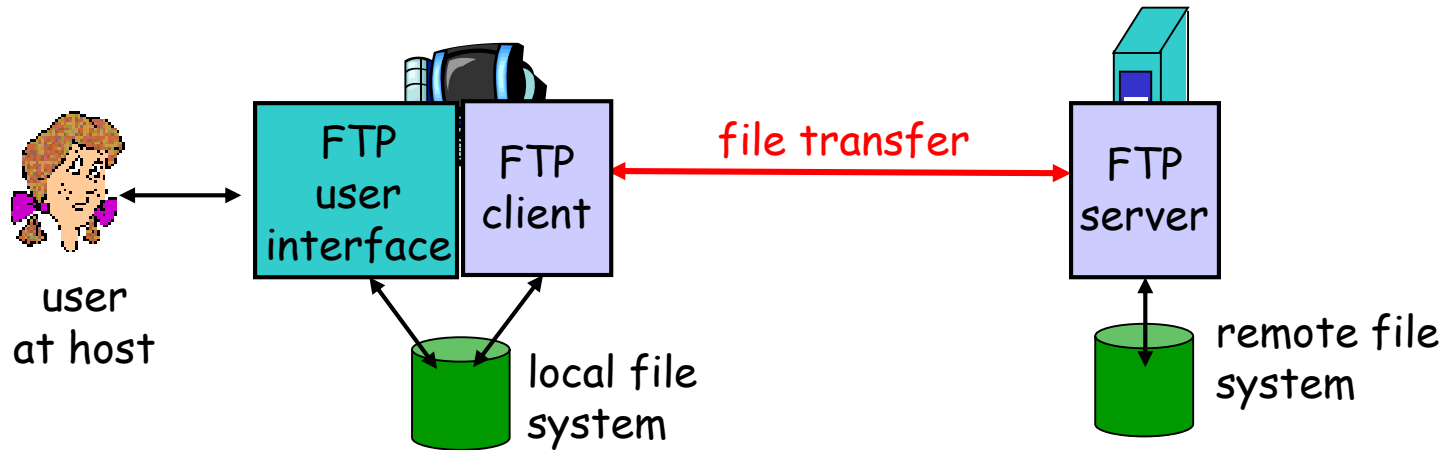   **HTTP/1.0 304 Not Modified**

client

server

| HTTP request msg |
| **If-modified-since: <date>** |

object not modified before <date>

| HTTP response |
| **HTTP/1.0** |
| **304 Not Modified** |

- -

| HTTP request msg |
| **If-modified-since: <date>** |

object modified after <date>

| HTTP response |
| **HTTP/1.0 200 OK** |
| **<data>** |

Chapter 2: Application layer

FTP: the file transfer protocol

- transfer file to/from remote host
- client/server model
  - *client:* side that initiates transfer (either to/from remote)
  - *server:* remote host
- ftp: RFC 959
- ftp server: port 21

FTP: separate control, data connections

- FTP client contacts FTP server at port 21, TCP is transport protocol
- client authorized over control connection
- client browses remote directory by sending commands over control connection.
- when server receives file transfer command, server opens 2nd TCP connection (for file) to client
- after transferring one file, server closes data connection.

TCP control connection
port 21

FTP client

TCP data connection
port 20
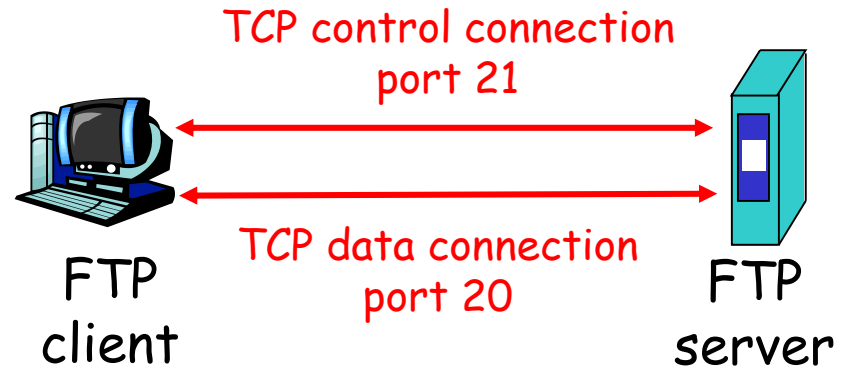
FTP server

- server opens another TCP data connection to transfer another file.
- control connection: "out of band"
- FTP server maintains "state": current directory, earlier authentication

FTP commands, responses

Sample commands:

- sent as ASCII text over control channel
- **USER** *username*
- **PASS** *password*
- **LIST** return list of file in current directory
- **RETR filename** retrieves (gets) file
- **STOR filename** stores (puts) file onto remote host

Sample return codes

- status code and phrase (as in HTTP)
- **331 Username OK, password required**
- **125 data connection already open; transfer starting**
- **425 Can't open data connection**
- **452 Error writing file**

Figure 2.18: Example 2.11
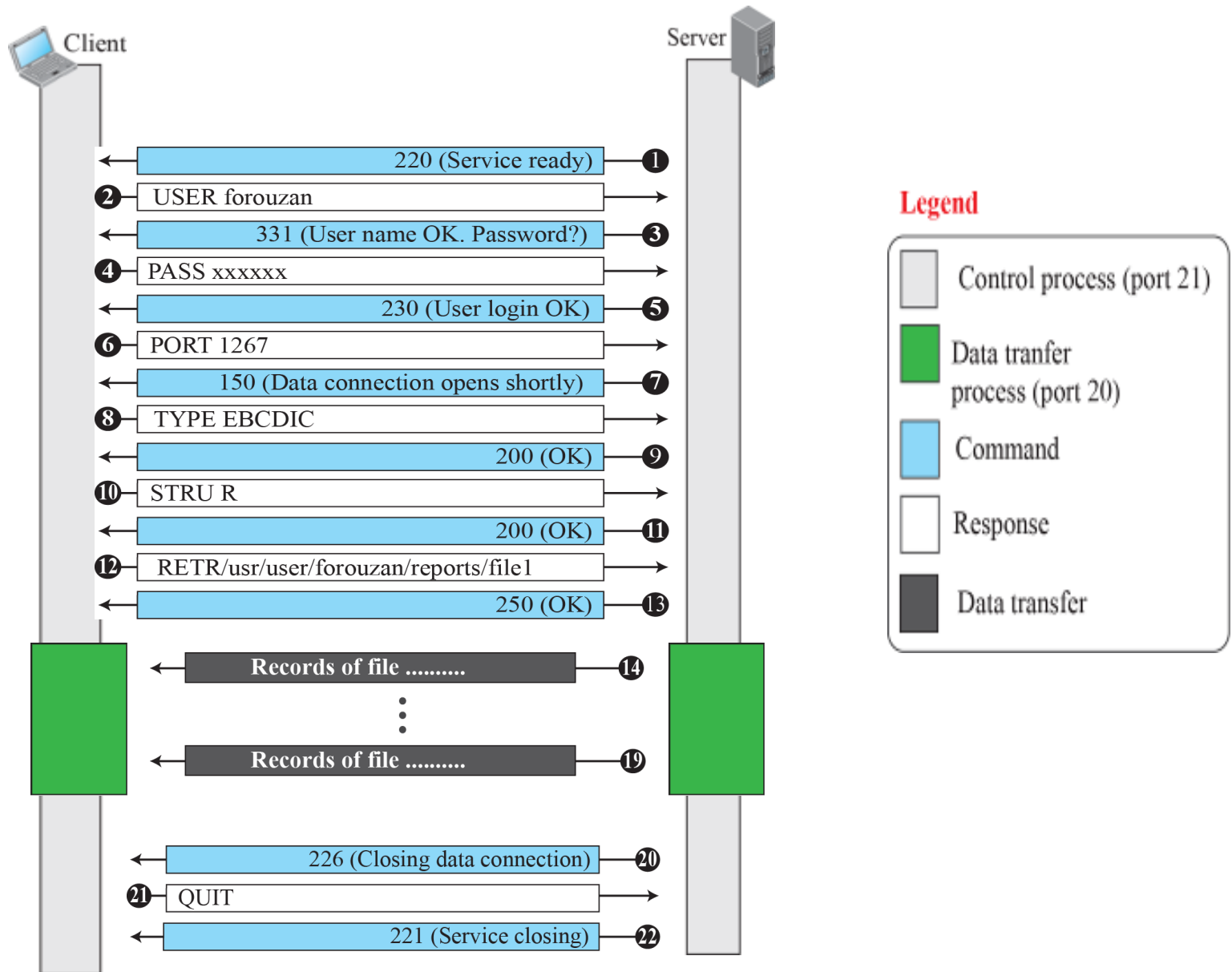
Chapter 2: Application layer
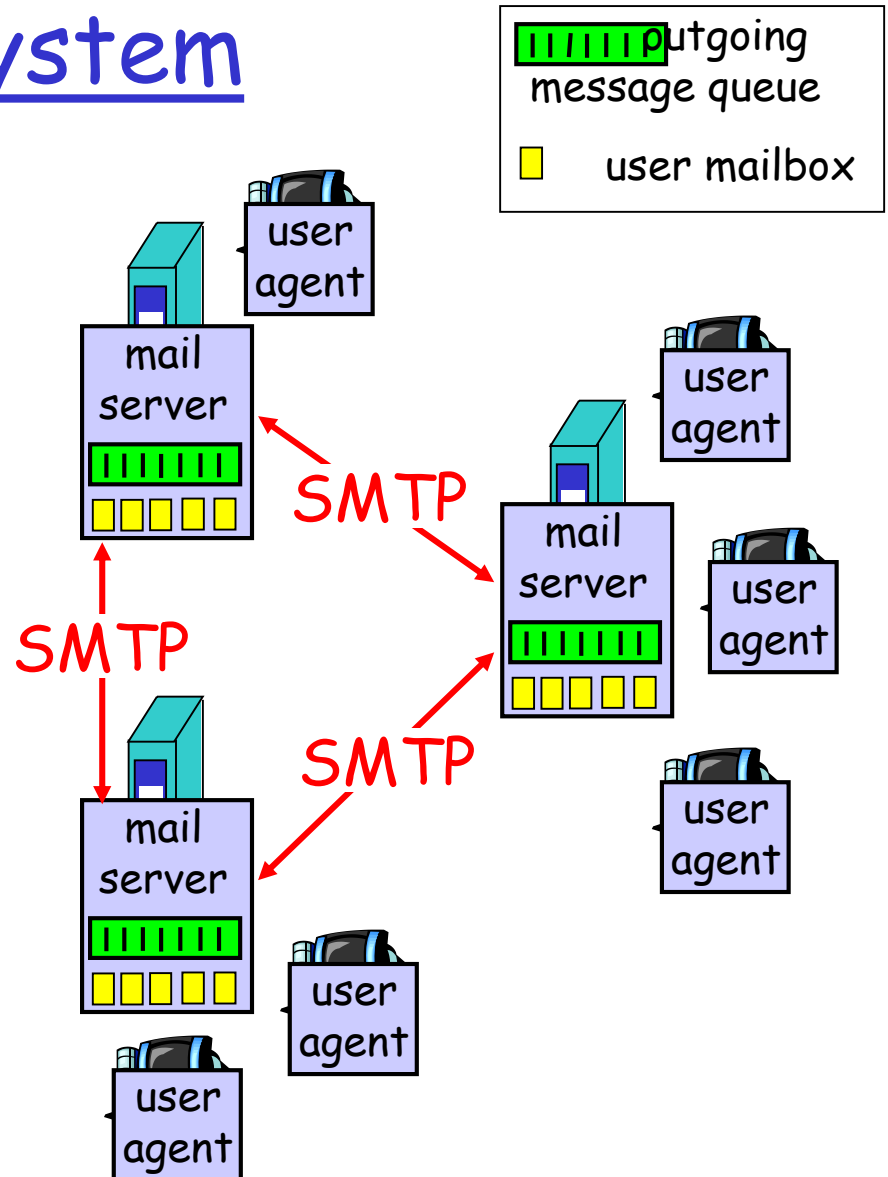
Internet e-mail System

Three major components:

- [ ] user agents
- [ ] mail servers
- [ ] simple mail transfer protocol: SMTP

User Agent

- [ ] a.k.a. "mail reader"
- [ ] composing, editing, reading, forwarding mail messages
- [ ] e.g., Outlook, Apple mail.
- [ ] outgoing, incoming messages stored on server

outgoing message queue

user mailbox

SMTP

SMTP

SMTP

Electronic Mail: mail servers

Mail Servers

□ **mailbox** contains incoming messages for user

□ **message queue** of outgoing (to be sent) mail messages

□ **SMTP protocol** between mail servers to send email messages

  ❖ client: sending mail server

  ❖ "server": receiving mail server
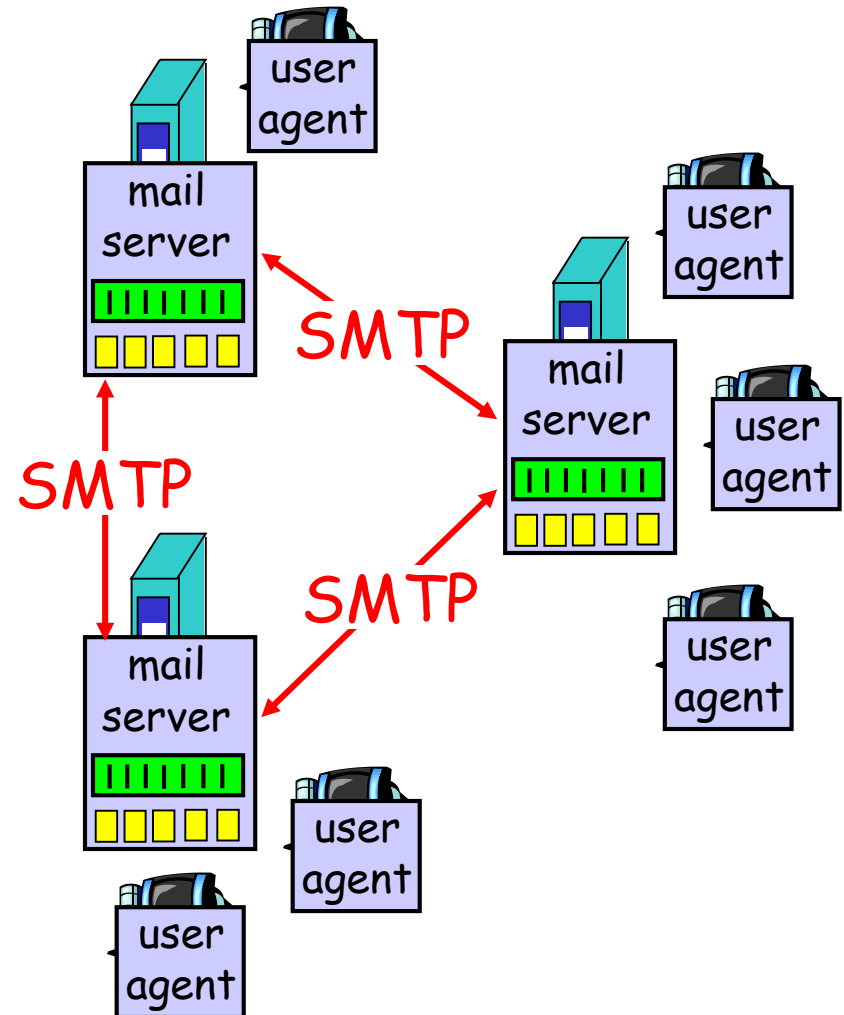
Electronic Mail: SMTP [RFC 5321]

- uses TCP to reliably transfer email message from client to server, port 25.
- direct transfer: sending server to receiving server
- three phases of transfer
  - ❖ handshaking (greeting)
  - ❖ transfer of messages
  - ❖ closure
- command/response interaction
  - ❖ commands: ASCII text
  - ❖ response: status code and phrase
- messages must be in 7-bit ASCII

Scenario: Alice sends message to Bob

1) Alice uses UA to compose message and "to" `bob@someschool.edu`

2) Alice's UA sends message to her mail server; message placed in message queue

3) Client side of SMTP opens TCP connection with Bob's mail server

4) SMTP client sends Alice's message over the TCP connection

5) Bob's mail server places the message in Bob's mailbox

6) Bob invokes his user agent to read message
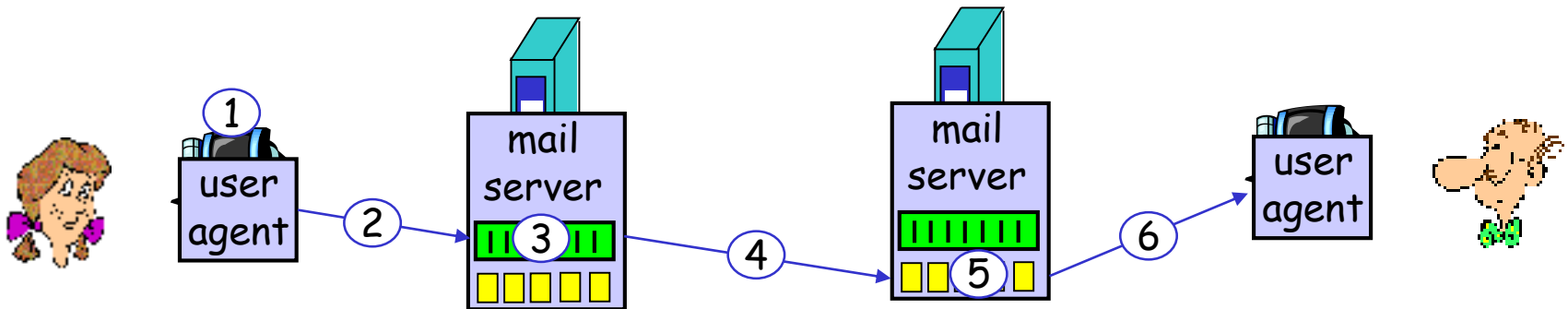
Sample SMTP interaction

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

SMTP: final words

- SMTP uses persistent connections
- SMTP requires message (header & body) to be in 7-bit ASCII
- SMTP server uses `CRLF.CRLF` to determine end of message

Comparison with HTTP:

- HTTP: pull protocol
- SMTP: push protocol

- both have ASCII command/response interaction, status codes

- HTTP: each object encapsulated in its own response msg
- SMTP: multiple objects sent in multipart msg

Mail message format

SMTP: protocol for exchanging email msgs

RFC 5322: standard for text message format:

□ header lines, e.g.,
  ❖ To:
  ❖ From:
  ❖ Subject:

  different from SMTP commands!

□ body
  ❖ the "message", ASCII characters only

header

body

blank line

Mail access protocols

SMTP   SMTP   access protocol

user agent → sender's mail server → receiver's mail server → user agent
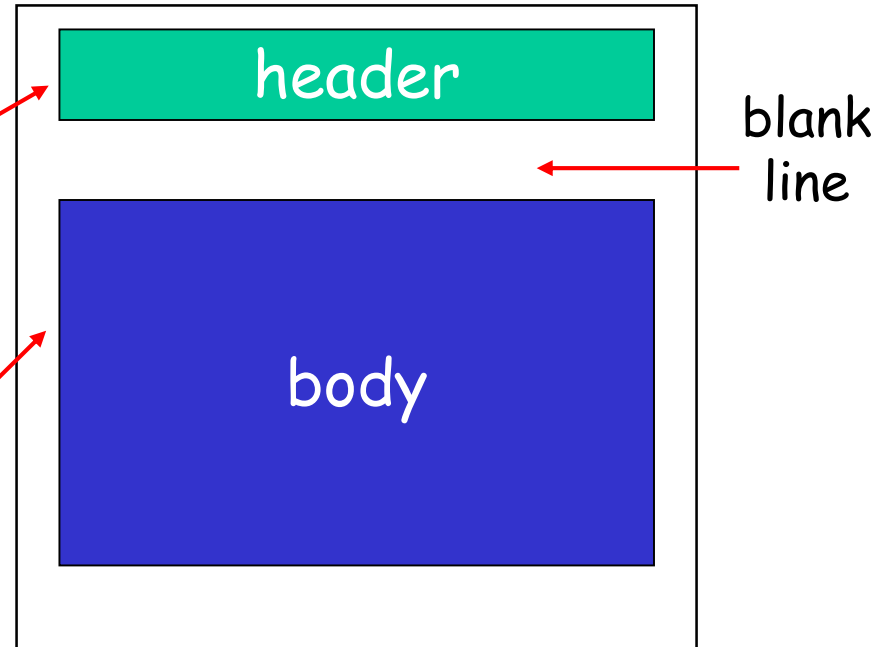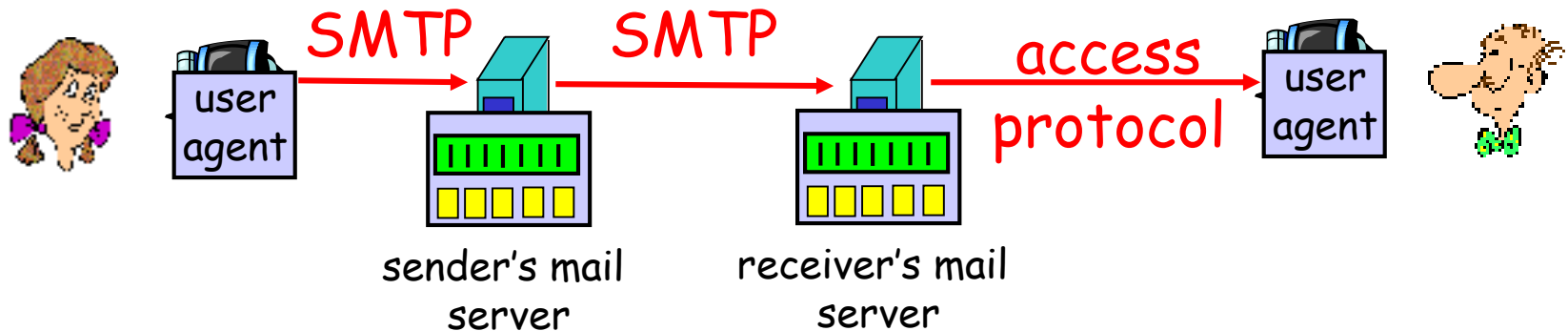
□ SMTP: delivery/storage to receiver's server
□ Mail access protocol: retrieval from server
  ❖ POP3: Post Office Protocol- Version 3 [RFC 1939]
    • authorization (agent <-->server) and download
  ❖ IMAP: Internet Mail Access Protocol [RFC 1730]
    • more features (more complex)
    • manipulation of stored msgs on server
  ❖ HTTP: gmail, Hotmail, Yahoo! Mail, etc.

POP3 protocol

authorization phase
- client commands:
    - **user**: declare username
    - **pass**: password
- server responses
    - **+OK**
    - **-ERR**

transaction phase, client:
- **list**: list message numbers
- **retr**: retrieve message by number
- **dele**: delete
- **Quit**

Update

```
S: +OK POP3 server ready
C: user bob
S: +OK
C: pass hungry
S: +OK user successfully logged on
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

POP3 (more) and IMAP

More about POP3

- Previous example uses "download and delete" mode.
- Bob cannot re-read e-mail if he changes client
- "Download-and-keep": copies of messages on different clients
- POP3 is stateless across sessions

IMAP

- Keep all messages in one place: the server
- Allows user to organize messages in folders
- IMAP keeps user state across sessions:
  - names of folders and mappings between message IDs and folder name

Web-based e-mail

❖ With this service, the user agent is an ordinary Web browser, and the user communicates with its remote mailbox via HTTP.

❖ When a recipient, such as Bob, wants to access a message in his mailbox, the e-mail message is sent from **Bob's mail server to Bob's browser** using the HTTP protocol rather than the POP3 / IMAP protocol.

❖ When a sender, such as Alice, wants to send an e-mail message, the e-mail message is sent from her browser to her mail server over HTTP rather than over SMTP.

Figure 2.29: Web-based e-mail, cases I and II
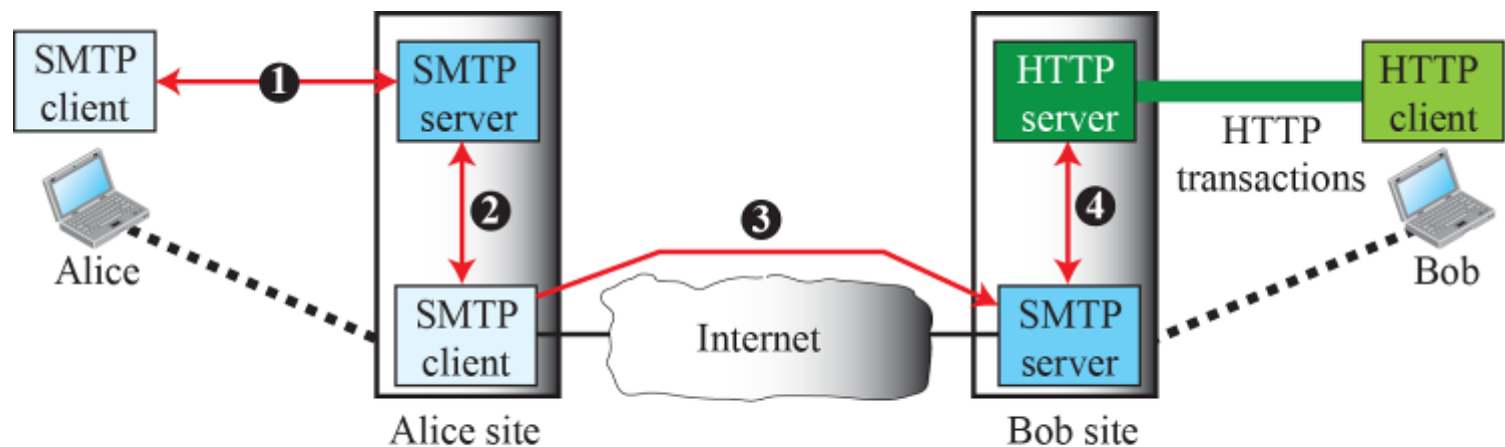
Case 1: Only receiver uses HTTP
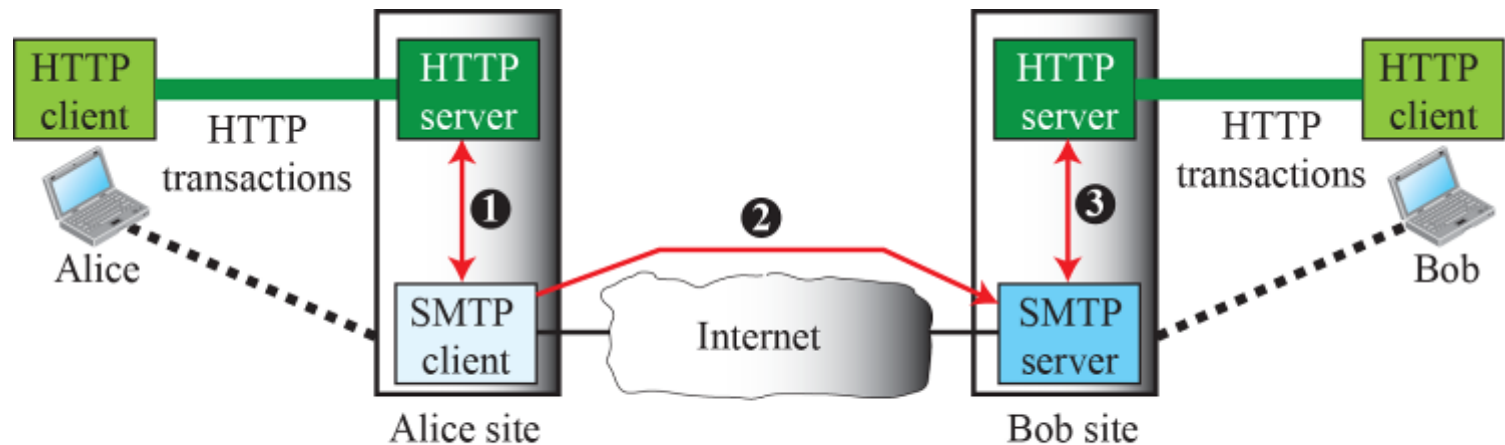
Case 2: Both sender and receiver use HTTP

Chapter 2: Application layer

- 2.1 Principles of network applications
- 2.2 Web and HTTP
- 2.3 FTP
- 2.4 Electronic Mail
  - SMTP, POP3, IMAP
- 2.5 DNS

- 2.6 Socket programming with TCP
- 2.7 Socket programming with UDP

DNS: Domain Name System

People: many identifiers:

- ❖ SSN, name, passport #

Internet hosts, routers:

- ❖ IP address (32 bit) - used for addressing datagrams
- ❖ "name", e.g., ww.yahoo.com - used by humans

Q: map between IP addresses and name ?

Domain Name System:

- ❑ *distributed database* implemented in hierarchy of many *name servers*
- ❑ *application-layer protocol* host, routers, name servers to communicate to *resolve* names (address/name translation)
  - ❖ note: core Internet function, implemented as application-layer protocol
  - ❖ DNS runs over UDP,uses port 53.

DNS – How it works?

❖ In order for the user's host to be able to send an HTTP request message to the Web server www.someschool.edu, the user's host must first obtain the **IP address of** www.someschool.edu. This is done as follows.

1. The same user machine runs the client side of the DNS application.

2. The browser extracts the hostname, www.someschool.edu, from the URL and passes the hostname to the client side of the DNS application.

3. The DNS client sends a query containing the hostname to a DNS server.

4. The DNS client eventually receives a reply, which includes the IP address for the hostname.

5. Once the browser receives the IP address from DNS, it can initiate a TCP connection to the HTTP server process located at port 80 at that IP address.

DNS

DNS services

- hostname to IP address translation
- host aliasing
  - ❖ Canonical, alias names
- mail server aliasing
- load distribution
  - ❖ replicated Web servers: set of IP addresses for one canonical name
  - ❖ Rotated order of IP addresses

Why not centralize DNS?

- single point of failure
- traffic volume
- distant centralized database
- Maintenance

doesn't *scale!*

Distributed, Hierarchical Database

Root DNS Servers

com DNS servers   org DNS servers   edu DNS servers

yahoo.com   amazon.com   pbs.org   poly.edu   umass.edu
DNS servers   DNS servers   DNS servers   DNS serversDNS servers
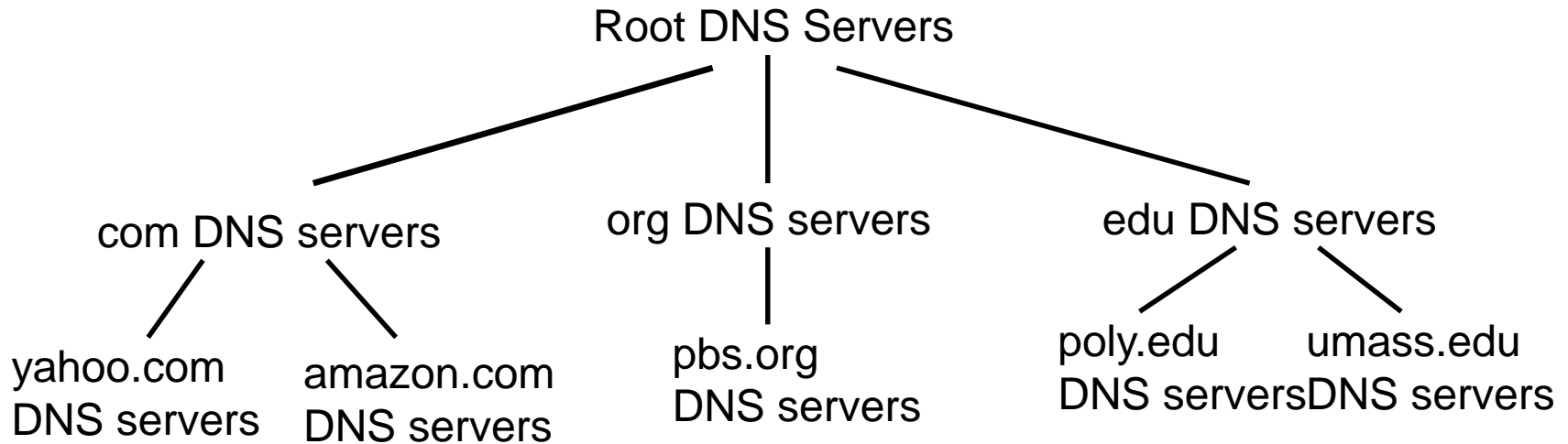
Client wants IP for www.amazon.com; 1st approx:

☐ client queries a root server to find com DNS server

☐ client queries com DNS server to get amazon.com DNS server

☐ client queries amazon.com DNS server to get IP address for www.amazon.com

DNS: root name servers

- ❖ contacted by local name server that can not resolve name

- ❖ root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server

c. Cogent, Herndon, VA (5 other sites)
d. U Maryland College Park, MD
h. ARL Aberdeen, MD
j. Verisign, Dulles VA (69 other sites)

k. RIPE London (17 other sites)

i. Netnod, Stockholm (37 other sites)

e. NASA Mt View, CA
f. Internet Software C.
Palo Alto, CA (and 48 other sites)

a. Verisign, Los Angeles CA
   (5 other sites)
b. USC-ISI Marina del Rey, CA
l. ICANN Los Angeles, CA
   (41 other sites)

g. US DoD Columbus, OH (5 other sites)

m. WIDE Tokyo
(5 other sites)

13 root name "servers" worldwide

TLD and Authoritative Servers

□ **Top-level domain (TLD) servers:**

  ❖ responsible for com, org, net, edu, etc, and all top-level country domains uk, fr, ca, jp.

  ❖ Verisign Global Services maintains servers for com TLD

  ❖ Educause for edu TLD

□ **Authoritative DNS servers:**

  ❖ organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web, mail).

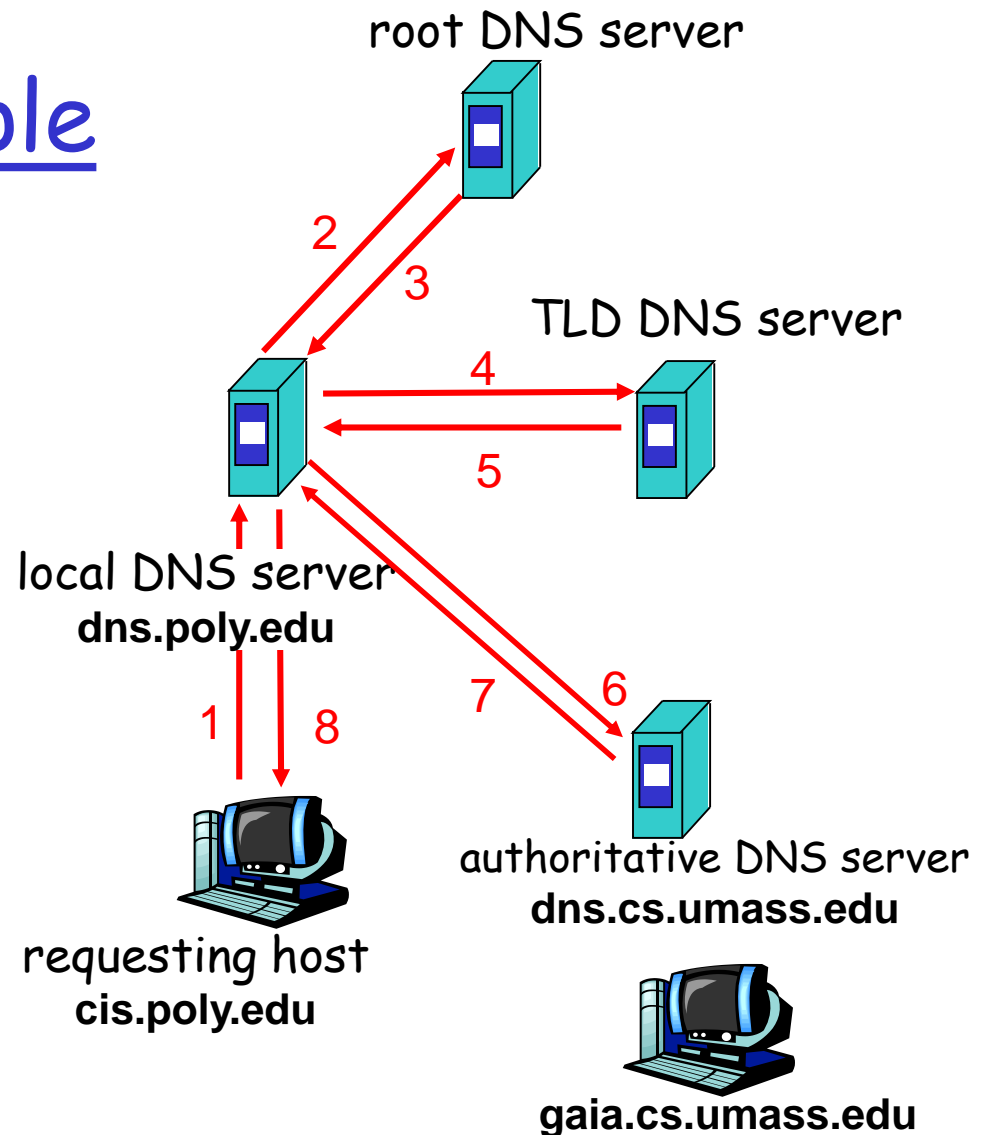 ❖ can be maintained by organization or service provider

Local Name Server

□ does not strictly belong to hierarchy

□ each ISP (residential ISP, company, university) has one.

  ❖ also called "default name server"

□ when host makes DNS query, query is sent to its local DNS server

  ❖ acts as proxy, forwards query into hierarchy

  ❖ has local cache of recent name-to-address translation pairs.

DNS name resolution example

☐ Host at cis.poly.edu wants IP address for gaia.cs.umass.edu

iterated query:
☐ contacted server replies with name of server to contact
☐ "I don't know this name, but ask this server"

root DNS server

2
3

TLD DNS server

4
5

local DNS server
dns.poly.edu

1   8

7   6

requesting host
cis.poly.edu

authoritative DNS server
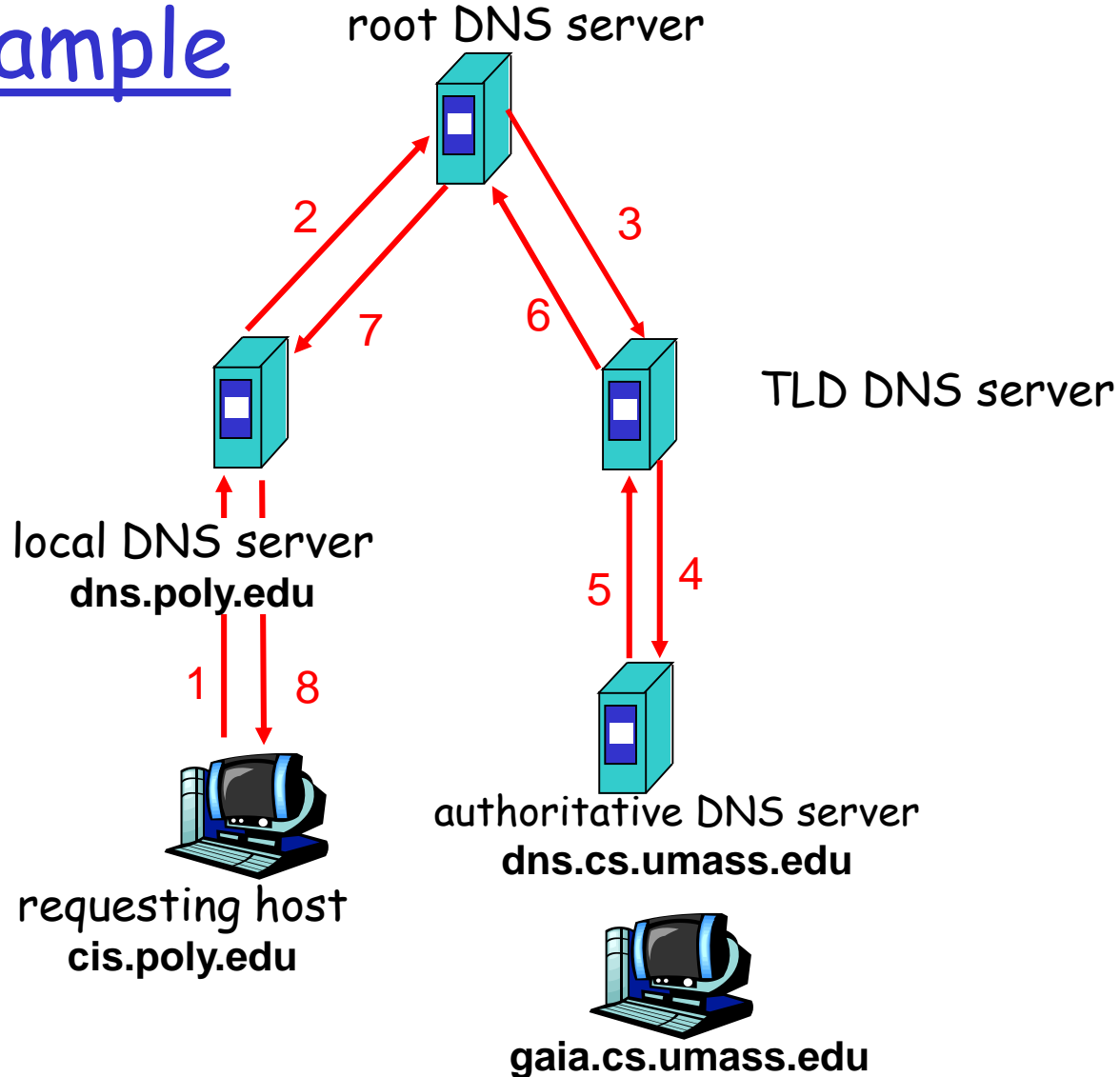**dns.cs.umass.edu**

gaia.cs.umass.edu

DNS name resolution example

root DNS server

recursive query:

- ☐ puts burden of name resolution on contacted name server
- ☐ heavy load?

local DNS server
dns.poly.edu

TLD DNS server

authoritative DNS server
dns.cs.umass.edu

requesting host
cis.poly.edu

gaia.cs.umass.edu

2
3
7
6
5
4
1
8

DNS: caching and updating records

□ once (any) name server learns mapping, it *caches* mapping
  ❖ cache entries timeout (disappear) after some time
  ❖ TLD servers typically cached in local name servers
    • Thus root name servers not often visited
□ update/notify mechanisms under design by IETF
  ❖ RFC 2136
  ❖ http://www.ietf.org/html.charters/dnsind-charter.html

DNS records

DNS: distributed db storing resource records (RR)

> RR format: `(name, value, type, ttl)`

□ **Type=A**
  - ❖ `name` is hostname
  - ❖ `value` is IP address

□ Type=NS
  - ❖ `name` is domain (e.g. foo.com)
  - ❖ `value` is hostname of authoritative name server for this domain

□ **Type=CNAME**
  - ❖ `name` is alias name for some "canonical" (the real) name

    `www.ibm.com` is really

    `servereast.backup2.ibm.com`
  - ❖ `value` is canonical name

□ **Type=MX**
  - ❖ `value` is name of mailserver associated with `name`

DNS protocol, messages

DNS protocol : *query* and *reply* messages, both with same *message format*

msg header

❒ identification: 16 bit # for query, reply to query uses same #

❒ flags:
  ❖ query or reply
  ❖ recursion desired
  ❖ recursion available
  ❖ reply is authoritative

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs

12 bytes

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)

DNS protocol, messages

Name, type fields for a query

RRs in response to query

records for authoritative servers

additional "helpful" info that may be used

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs

12 bytes

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)