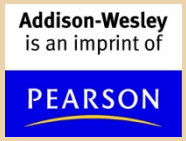
Networking and the Internet

Slides derived from those available on the web site of the book:

Computer Science: An Overview, 11th Edition, by J. Glenn Brookshear



Networking and the Internet

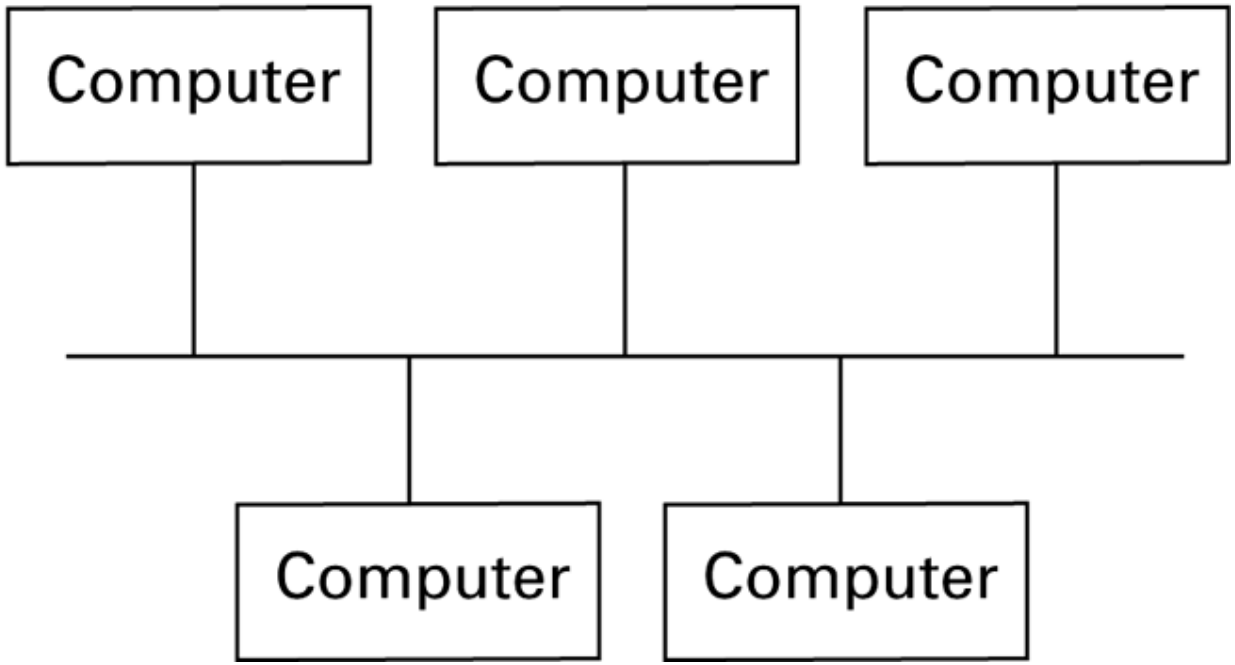
- Network Fundamentals
- The Internet
- The World Wide Web
- Internet Protocols
- Security

Network Classifications

- Scope
  - Local area network (LAN)
  - Metropolitan area (MAN)
  - Wide area network (WAN)
- Ownership
  - Closed versus open
- Topology (configuration)
  - Bus (Ethernet)
  - Star (Wireless networks with central Access Point)

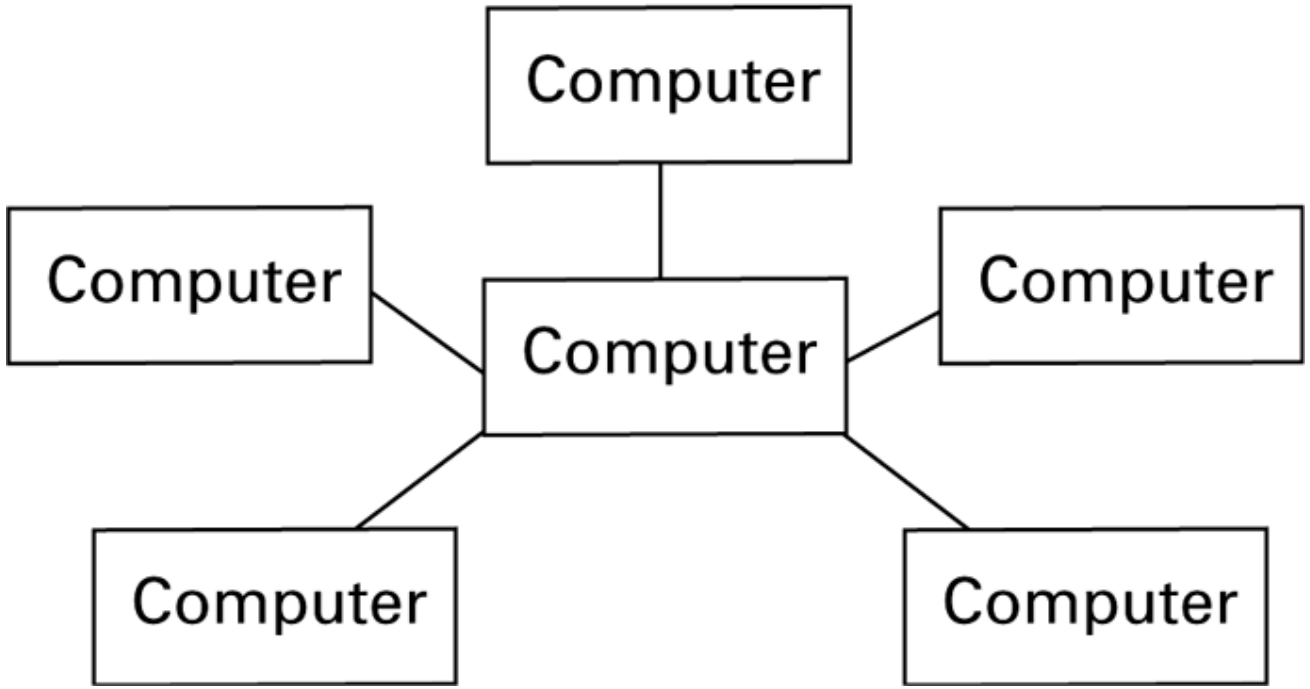
Network topologies

a. Bus



Network topologies (continued)

b. Star



What's a protocol?

human protocols:

- "what's the time?"
- "I have a question"
- introductions

… specific msgs sent

… specific actions taken when msgs received, or other events

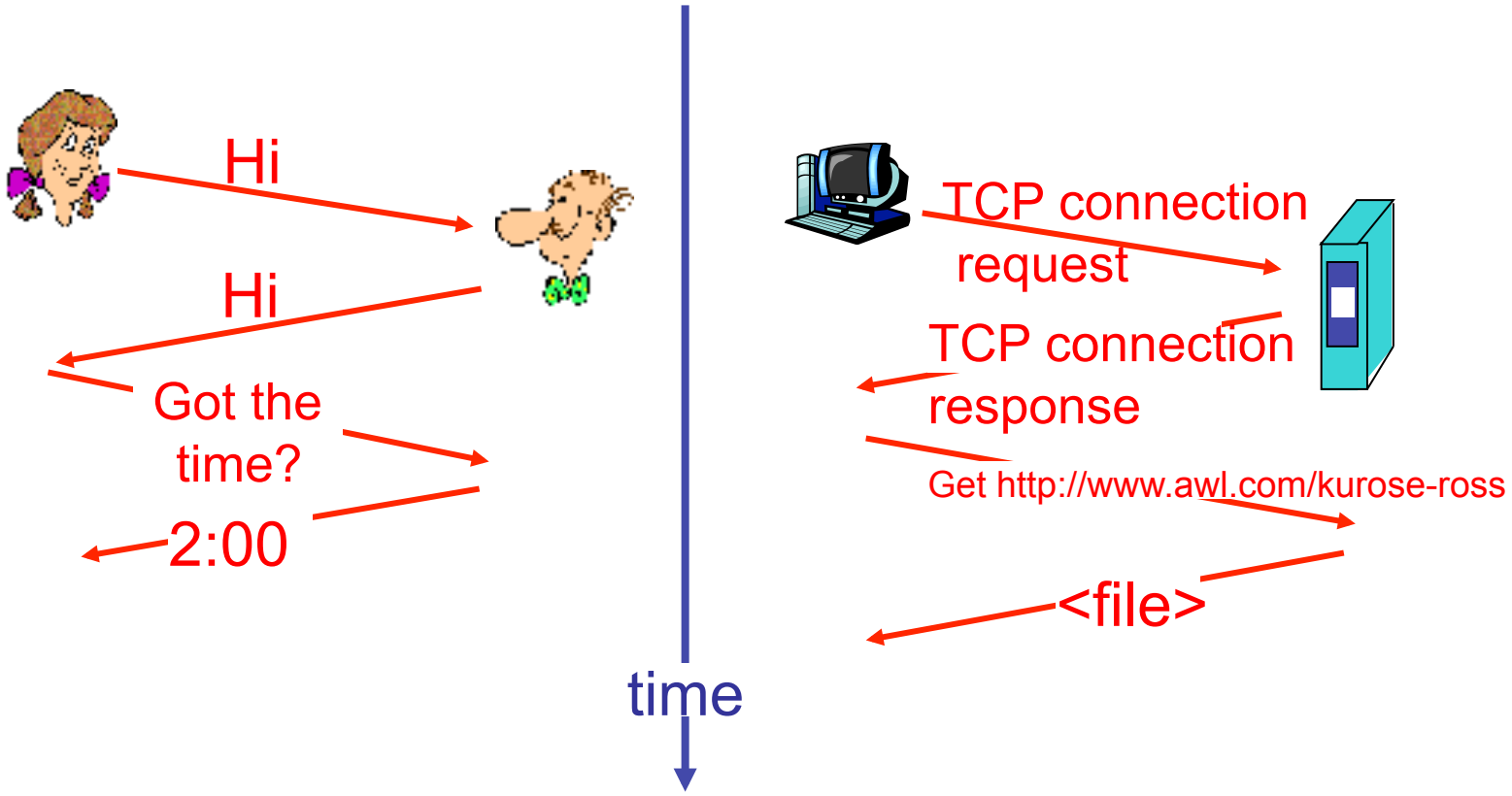
network protocols:

- machines rather than humans
- all communication activity in Internet governed by protocols

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

What's a protocol?

a human protocol and a computer network protocol:

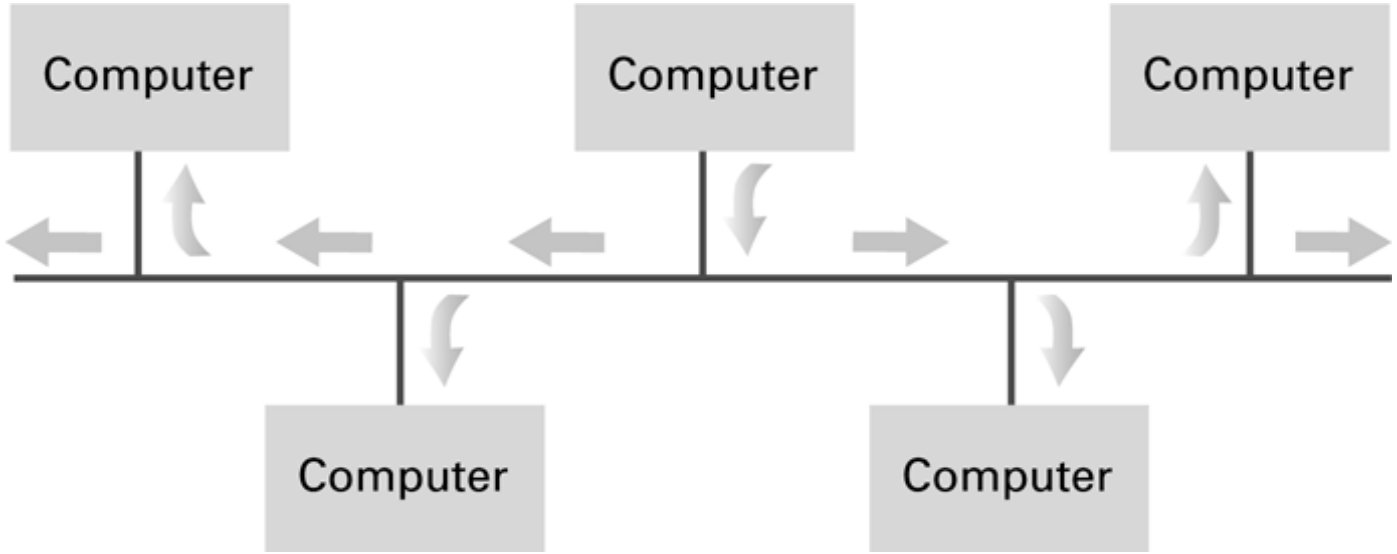


Q: Other human protocols?

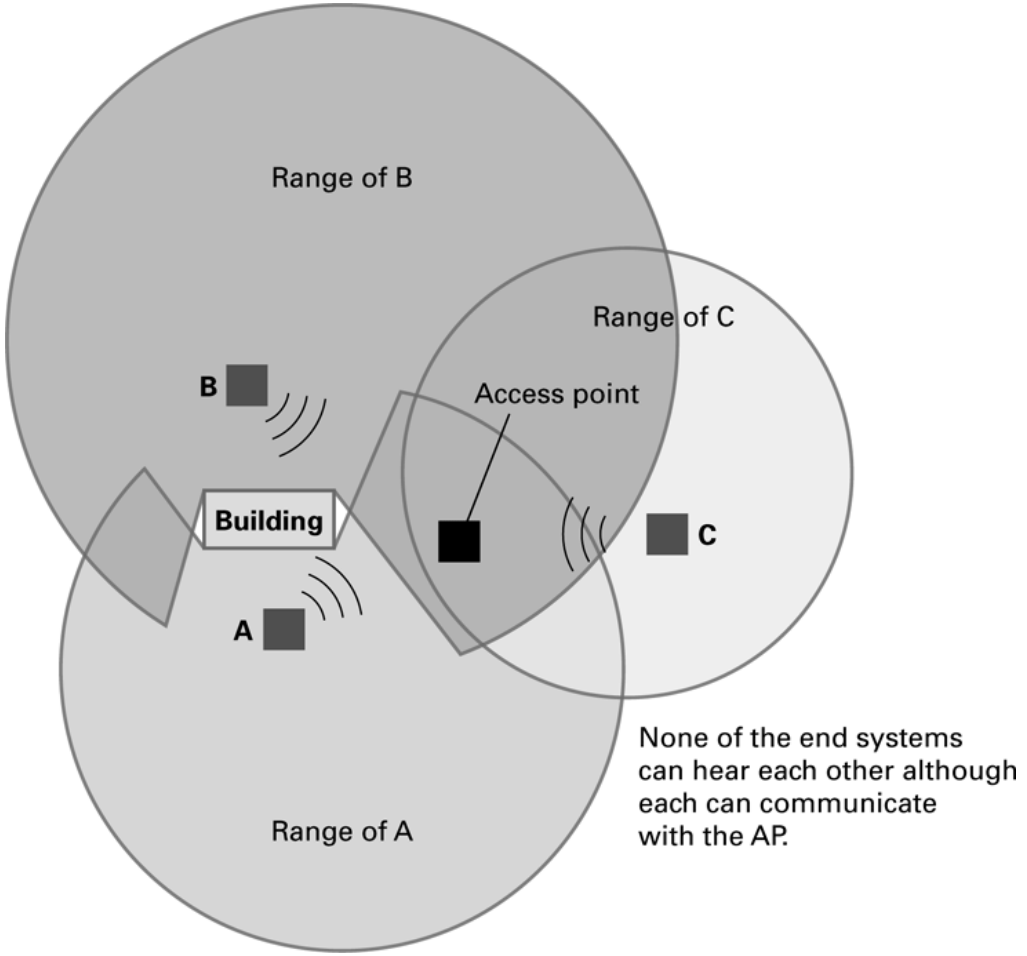
Protocols

- CSMA/CD
  - Used in Ethernet
  - Silent bus provides right to introduce new message
- CSMA/CA
  - Used in WiFi
  - Hidden terminal problem

Communication over a bus network



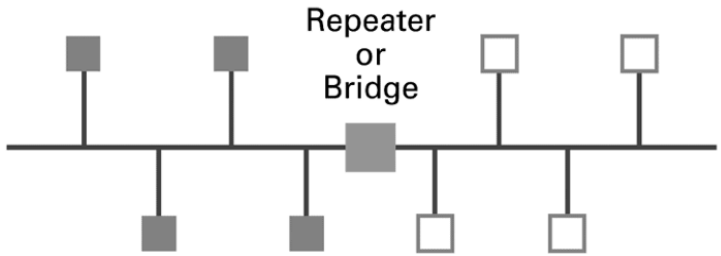
The hidden terminal problem



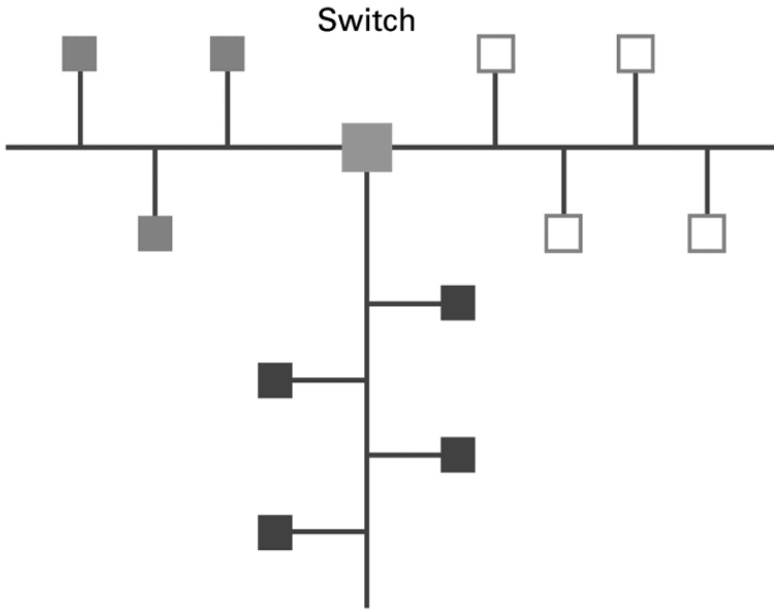
Connecting Networks

- **Repeater:** Extends a network
- **Bridge:** Connects two compatible networks
- **Switch:** Connects several compatible networks
- **Router:** Connects two incompatible networks resulting in a network of networks called an **internet**

Building a large bus network from smaller ones

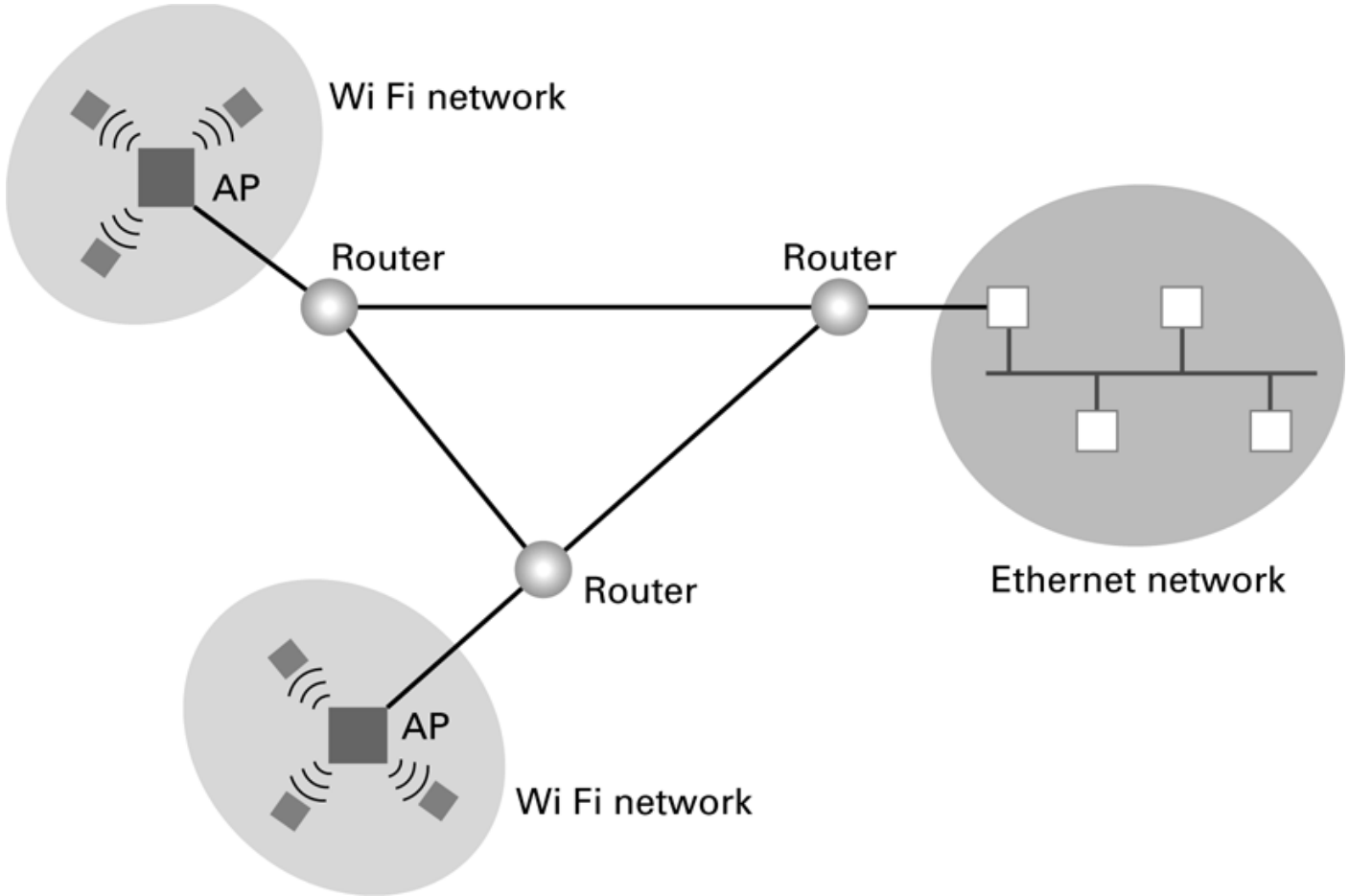


a. A repeater or bridge connecting two buses



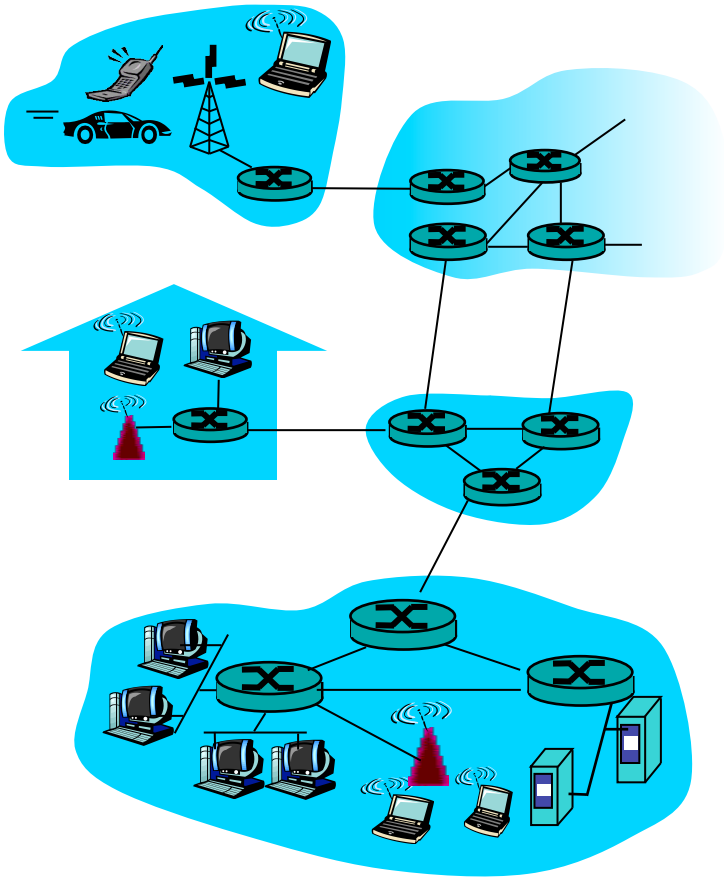
b. A switch connecting multiple buses

Routers connecting two WiFi networks and an Ethernet network to form an internet



A closer look at network structure:

- network edge:
  applications and hosts
- access networks, physical media:
  wired, wireless communication links
- network core:
  - interconnected routers
  - network of networks



The network edge:

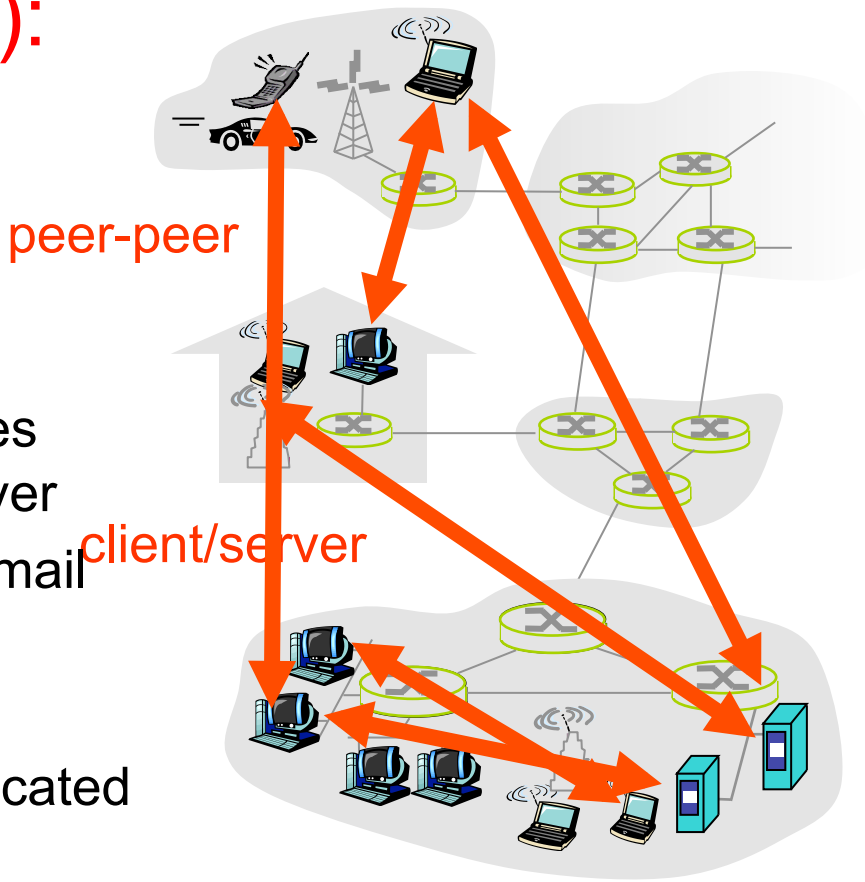
- end systems (hosts):
  - run application programs
  - e.g. Web, email
  - at “edge of network”

❑ client/server model

- client host requests, receives service from always-on server
- e.g. Web browser/server; email client/server

❑ peer-peer model:

- minimal (or no) use of dedicated servers
- e.g. Skype, BitTorrent



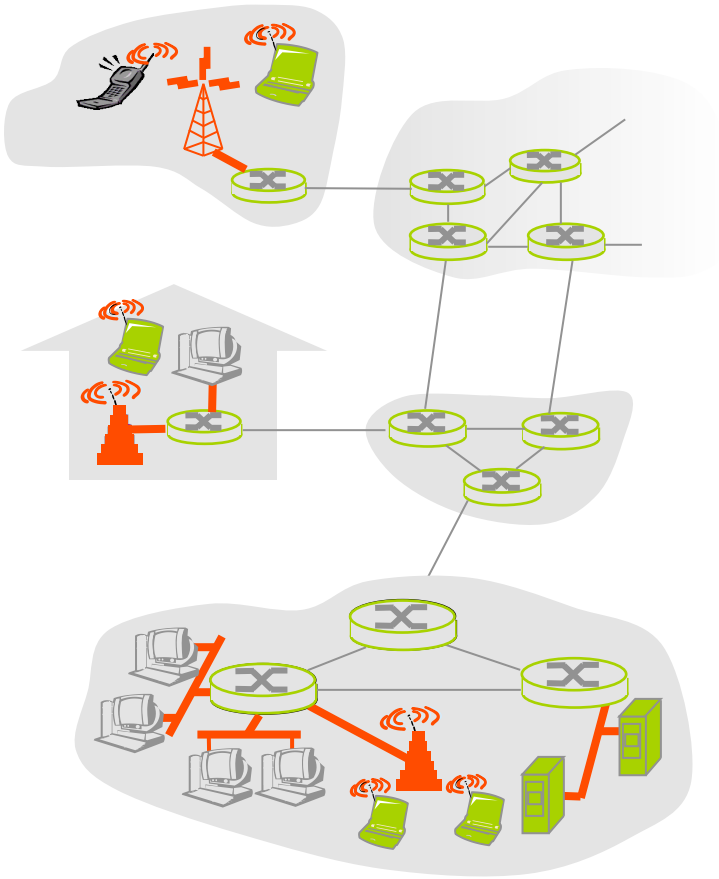
Access networks and physical media

Q: How to connect end systems to edge router?

- residential access nets
- institutional access networks (school, company)
- mobile access networks

Keep in mind:

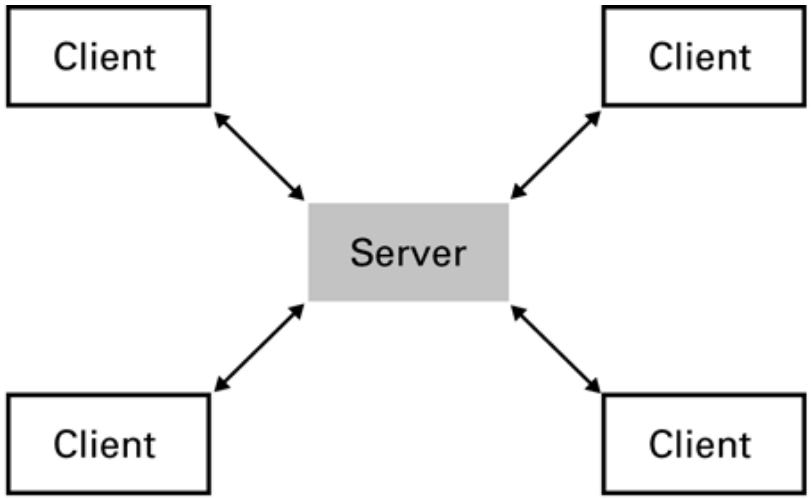
- bandwidth (bits per second) of access network?
- shared or dedicated?



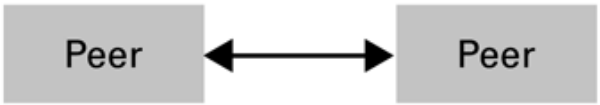
Inter-process Communication

- Client-server
  - One server, many clients
  - Server must execute continuously
  - Client initiates communication
- Peer-to-peer (P2P)
  - Two processes communicating as equals
  - Peer processes can be short-lived

The client/server model compared to the peer-to-peer model



a. Server must be prepared to serve multiple clients at any time.



b. Peers communicate as equals on a one-to-one basis.

Distributed Systems

- Systems with parts that run on different computers
  - Infrastructure can be provided by standardized toolkits
    - Example: Enterprise Java Beans from Oracle
    - Example: .NET framework from Microsoft

Networking and the Internet

- Network Fundamentals
- The Internet
- The World Wide Web
- Internet Protocols
- Security

The Internet

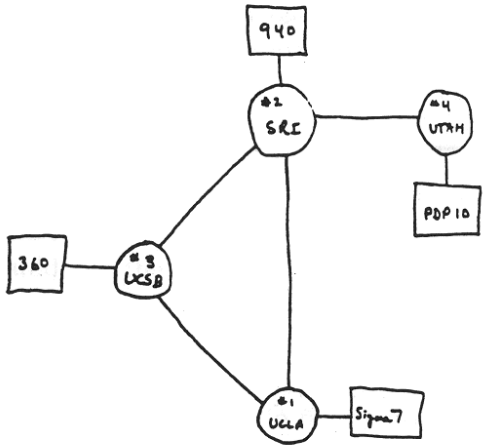
- The Internet: An internet that spans the world
  - Original goal was to develop a means of connecting networks that would not be disrupted by local disasters.
  - Today it has shifted from an academic research project to a commercial undertaking.

Internet History

1961-1972: Early packet-switching principles

- 1961: Kleinrock - queueing theory shows effectiveness of packet-switching
- 1964: Baran - packet-switching in military nets
- 1967: ARPAnet conceived by Advanced Research Projects Agency
- 1969: first ARPAnet node operational

- 1972:
  - ARPAnet public demonstration
  - NCP (Network Control Protocol) first host-host protocol
  - first e-mail program
  - ARPAnet has 15 nodes



THE ARPA NETWORK

Internet History

1972-1980: Internetworking, new and proprietary nets

- 1970: ALOHAnet satellite network in Hawaii
- 1974: Cerf and Kahn - architecture for interconnecting networks
- 1976: Ethernet at Xerox PARC
- late70's: proprietary architectures: DECnet, SNA, XNA
- late 70's: switching fixed length packets (ATM precursor)
- 1979: ARPAnet has 200 nodes

Cerf and Kahn's internetworking principles:

- minimalism, autonomy - no internal changes required to interconnect networks
- best effort service model
- stateless routers
- decentralized control

define today's Internet architecture

Internet History

1980-1990: new protocols, a proliferation of networks

- 1983: deployment of TCP/IP
- 1982: smtp e-mail protocol defined
- 1983: DNS defined for name-to-IP-address translation
- 1985: ftp protocol defined
- 1988: TCP congestion control

- new national networks: Csnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks

Internet History

1990, 2000's: commercialization, the Web, new apps

- Early 1990's: ARPAnet decommissioned
- 1991: NSF lifts restrictions on commercial use of NSFnet (decommissioned, 1995)
- early 1990s: Web
  - hypertext [Bush 1945, Nelson 1960's]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, later Netscape
  - late 1990's: commercialization of the Web

Late 1990's – 2000's:

- more killer apps: instant messaging, P2P file sharing
- network security to forefront
- est. 50 million host, 100 million+ users
- backbone links running at Gbps

Internet History

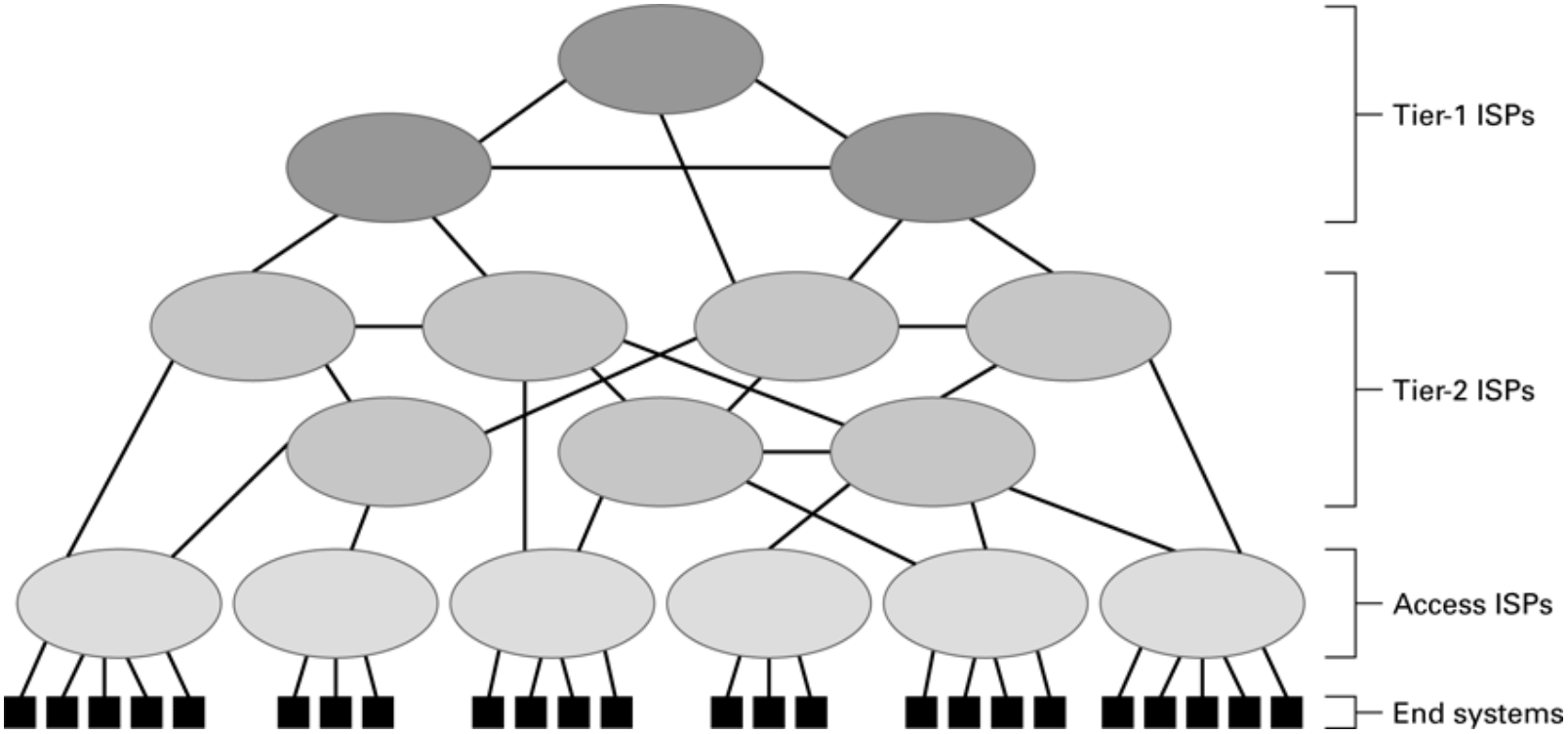
2007:

- ~500 million hosts
- Voice, Video over IP
- P2P applications: BitTorrent (file sharing) Skype (VoIP), PPLive (video)
- more applications: YouTube, gaming
- wireless, mobility

Internet Architecture

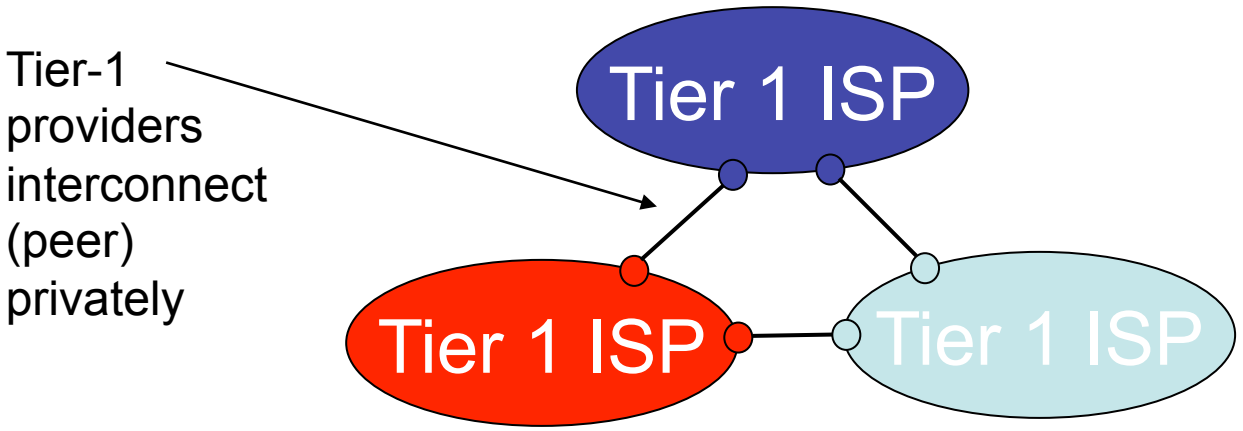
- Internet Service Provider (ISP)
  - Tier-1
  - Tier-2
- Access ISP: Provides connectivity to the Internet
  - Traditional telephone (dial up connection)
  - Cable connections
  - DSL
  - Wireless

Internet Composition

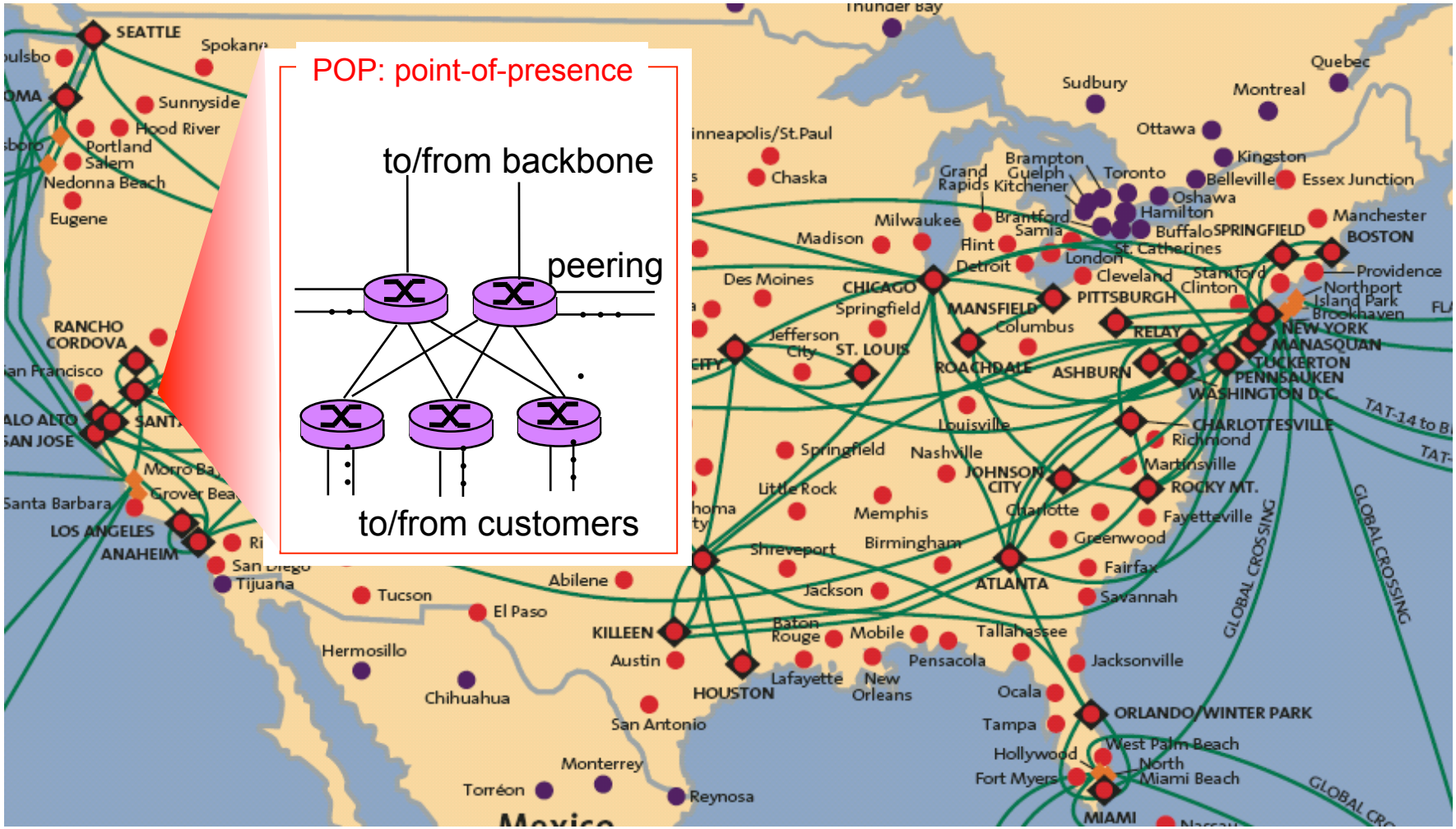


Internet structure: network of networks

- at center: “tier-1” ISPs (e.g., Verizon, Sprint, AT&T, Cable and Wireless), national/international coverage
  - treat each other as equals



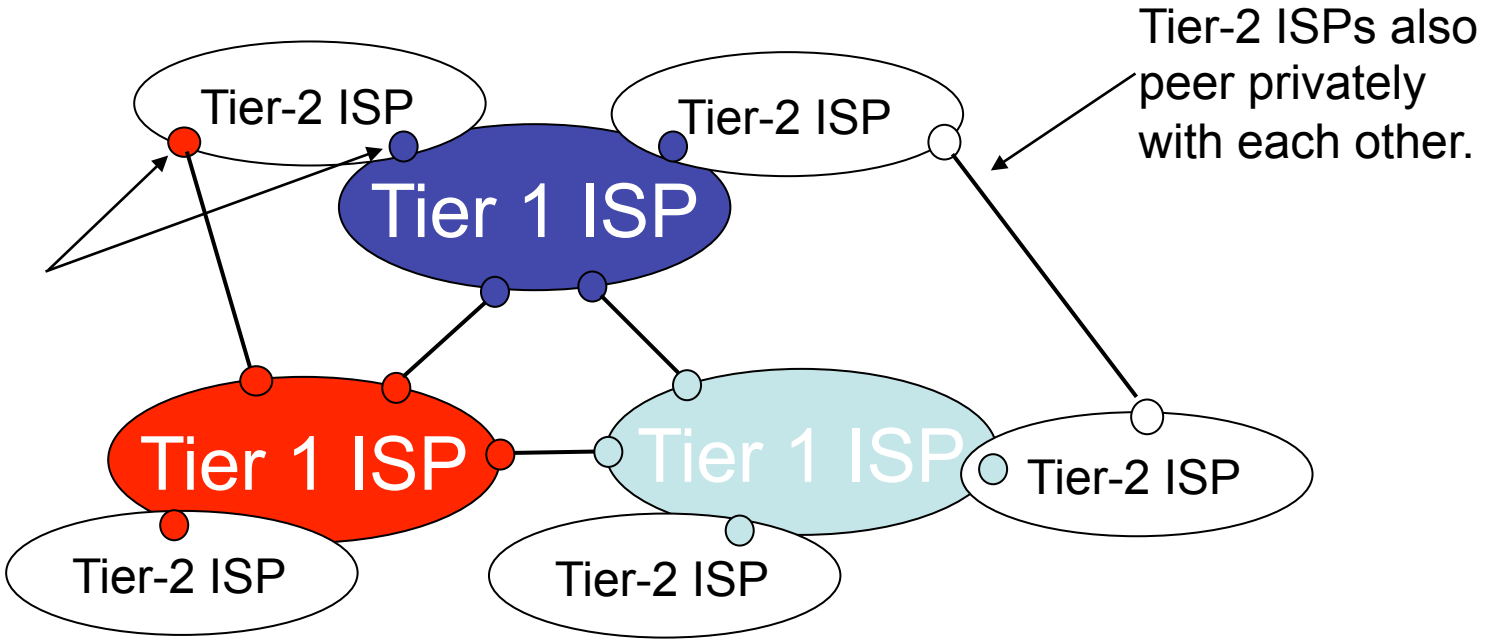
Tier-1 ISP: e.g., Sprint



Internet structure: network of networks

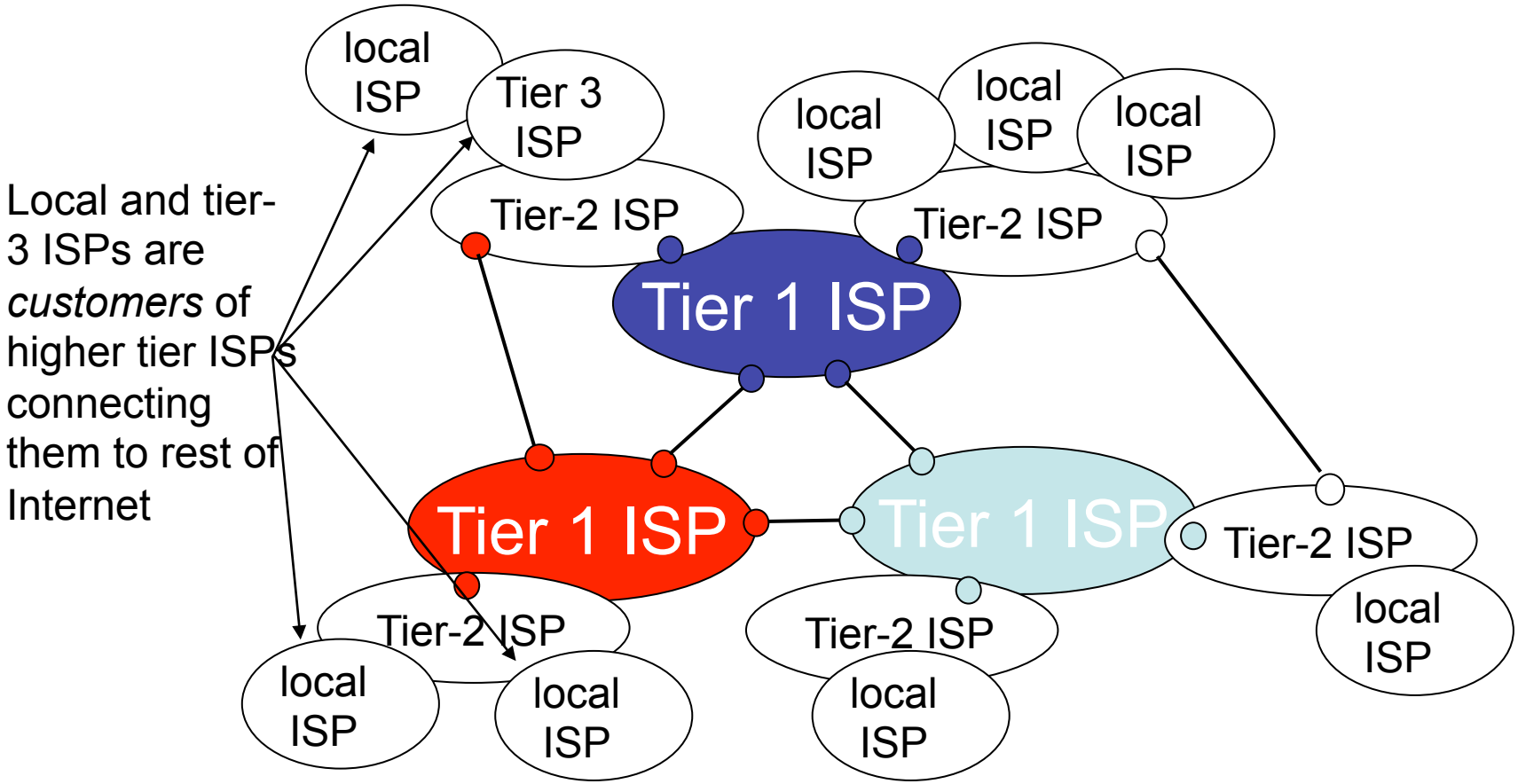
- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

Tier-2 ISP pays tier-1 ISP for connectivity to rest of Internet
- tier-2 ISP is *customer* of tier-1 provider



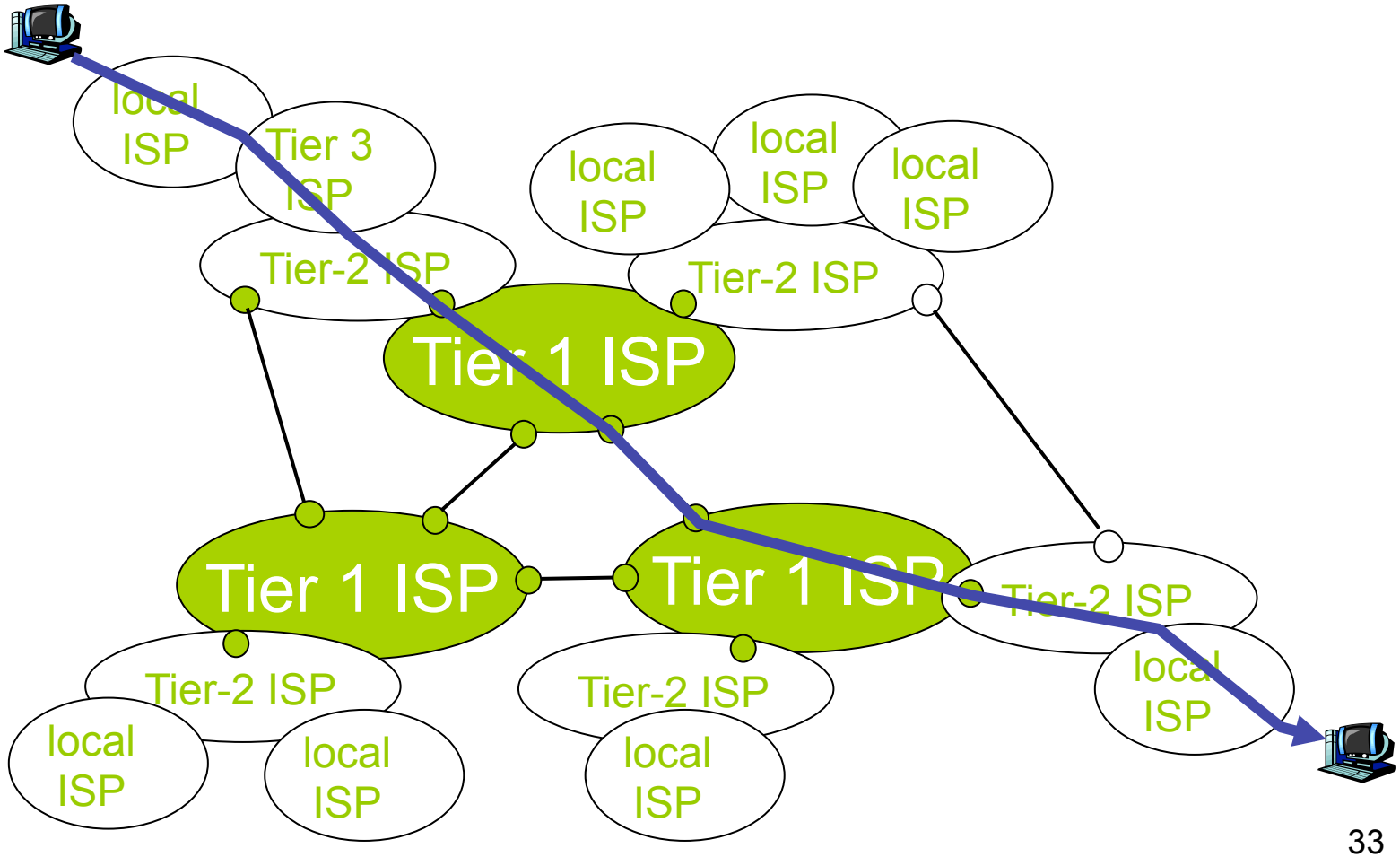
Internet structure: network of networks

- "Tier-3" ISPs and local ISPs
  - last hop ("access") network (closest to end systems)



Internet structure: network of networks

- a packet passes through many networks!



Internet Addressing

- IP address: pattern of 32 or 128 bits often represented in dotted decimal notation (e.g., 194.146.151.45)
- Mnemonic address:
  - Domain names (www.google.com)
  - Top-Level Domains (TLD) (e.g., .ir, .com, .edu, …)
- Domain name system (DNS)
  - Name servers
  - DNS lookup

Internet Corporation for Assigned Names & Numbers (ICANN)

- Allocates IP addresses to ISPs who then assign those addresses within their regions.
- Oversees the registration of domains and domain names.

Traditional Internet Applications

- Electronic Mail (email)
  - Domain mail server collects incoming mail and transmits outing mail
  - Mail server delivers collected incoming mail to clients via POP3 or IMAP
- File Transfer Protocol (FTP)
  - Anonymous vs Protected ftp sites
  - “binary file” vs “text file” (windows vs apple definition of new line)
- Telnet and SSH

More Recent Applications

- Voice Over IP (VoIP)
  - The Battle for Broadband (TV, Radio, Telephone, Internet)
- Internet Radio
  - N-unicast
  - Multicast

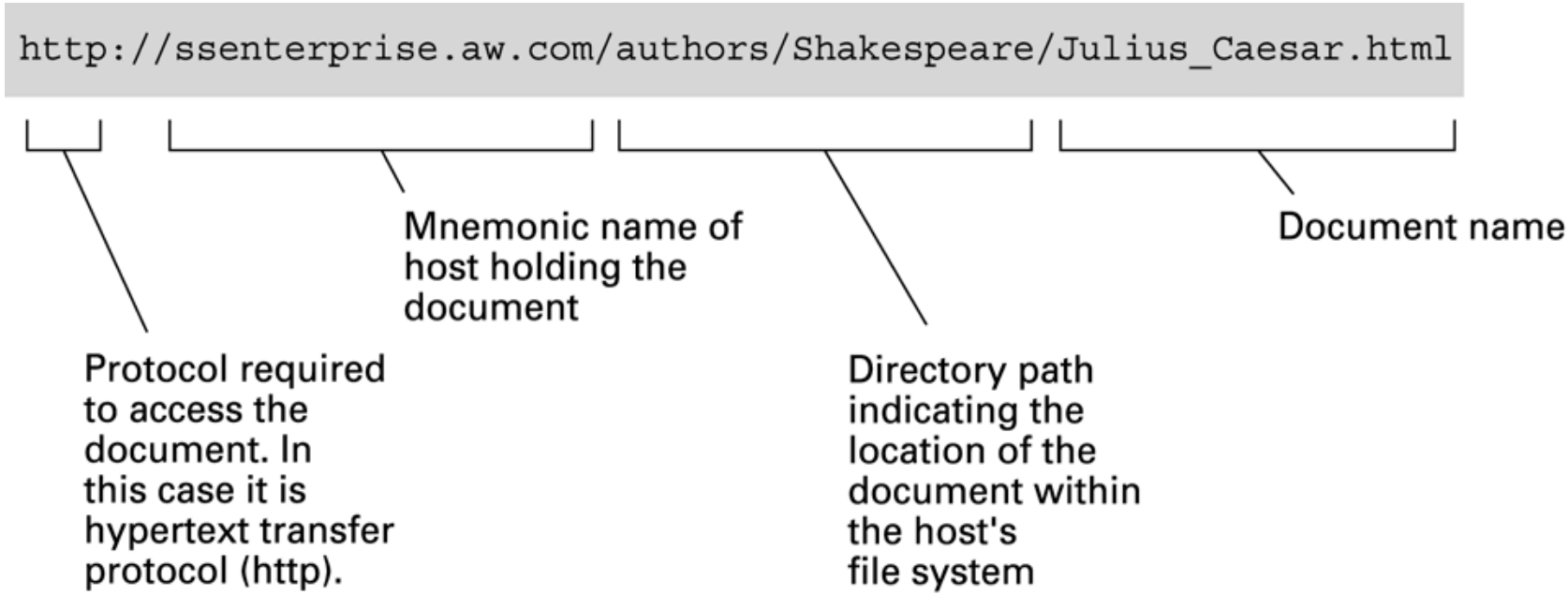
Networking and the Internet

- Network Fundamentals
- The Internet
- The World Wide Web
- Internet Protocols
- Security

World Wide Web (Tim Berners-Lee, Dec. 1990)

- Hypertext (hyperlink and hypermedia) and HTTP
- Browser (web client) gets documents from Web server
- Documents identified by URLs

A typical URL (Uniform Resource Locator)



Search engines:

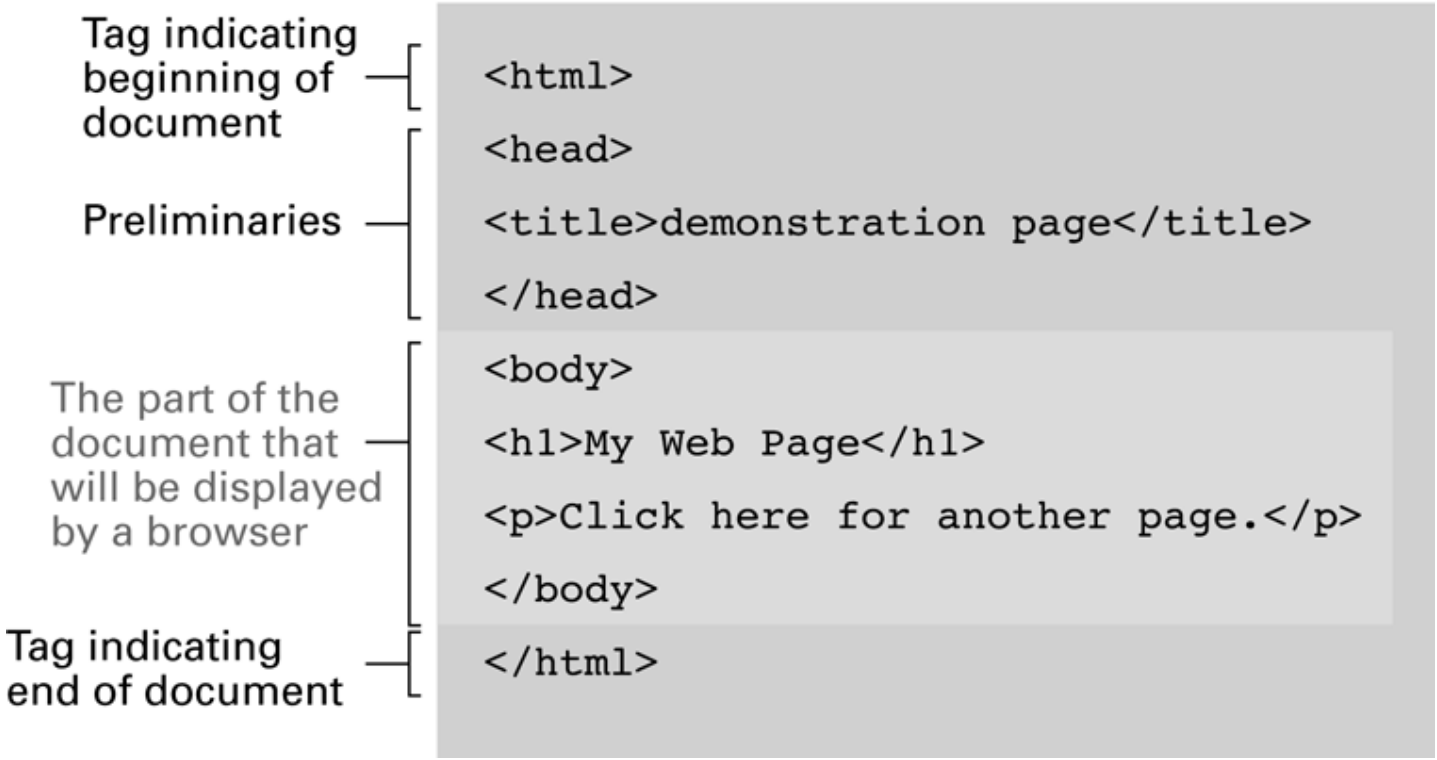
Software package that helps to find documents in the Internet

Hypertext Document Format

- Encoded as text file
- Contains tags to communicate with browser
  - Appearance
    - <h1> to start a level one heading
    - <p> to start a new paragraph
  - Links to other documents and content
    - <a href = . . . >
  - Insert images
    - <img src = . . . >

A simple Web page

a. The page encoded using HTML.



A simple Web page (continued)

b. The page as it would appear on a computer screen.

An enhanced simple Web page

a. The page encoded using HTML.

```
<html>
<head>
<title>demonstration page</title>
</head>
<body>
<h1>My Web Page</h1>
<p>Click
   <a href="http://crafty.com/demo.html">
   here
   </a>
   for another page.</p>
</body>
</html>
```

Anchor tag containing parameter

Closing anchor tag

An enhanced simple Web page (continued)

b. The page as it would appear on a computer screen.

Extensible Markup Language (XML)

- XML: A language for constructing markup languages similar to HTML
  - A descendant of SGML (Standard Generalized Markup Language)
  - Opens door to a World Wide *Semantic* Web

Using XML

<staff clef = “treble”> <key>C minor</key>

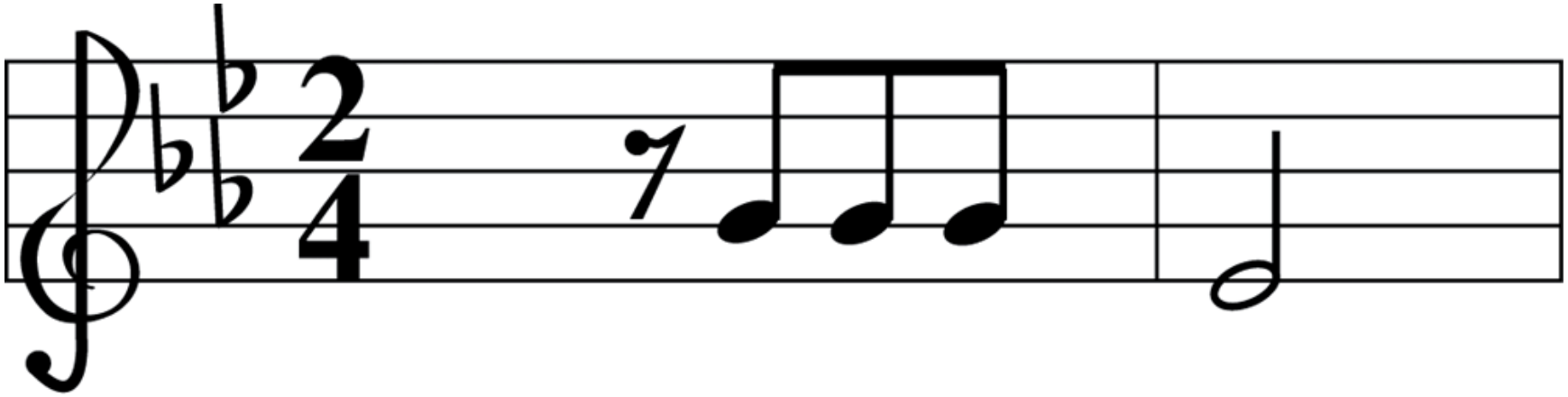
<time> 2/4 </time>

<measure> < rest> egth </rest> <notes>
egth G, egth G, egth G </notes></
measure>

<measure> <notes> hlf E </notes></
measure>

</staff>

The first two bars of Beethoven's Fifth Symphony



Client Side Versus Server Side

- Client-side activities
  - Examples: java applets, javascript, Macromedia Flash
- Server-side activities
  - Common Gateway Interface (CGI)
  - Servlets
  - PHP
- Example: Online Ticket Reservation

Networking and the Internet

- Network Fundamentals
- The Internet
- The World Wide Web
- Internet Protocols
- Security

Protocol "Layers"

Networks are complex!

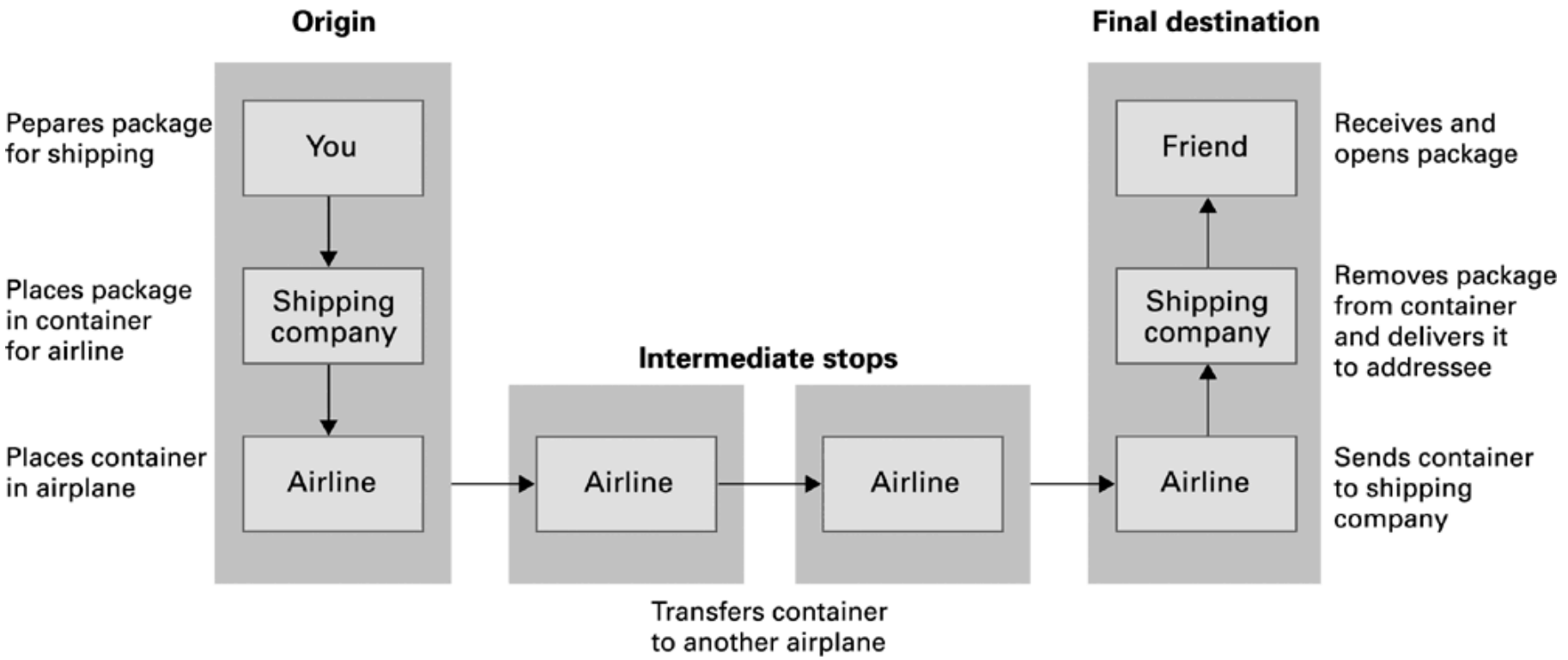
- many "pieces":
  - hosts
  - routers
  - links of various media
  - applications
  - protocols
  - hardware, software

Question:

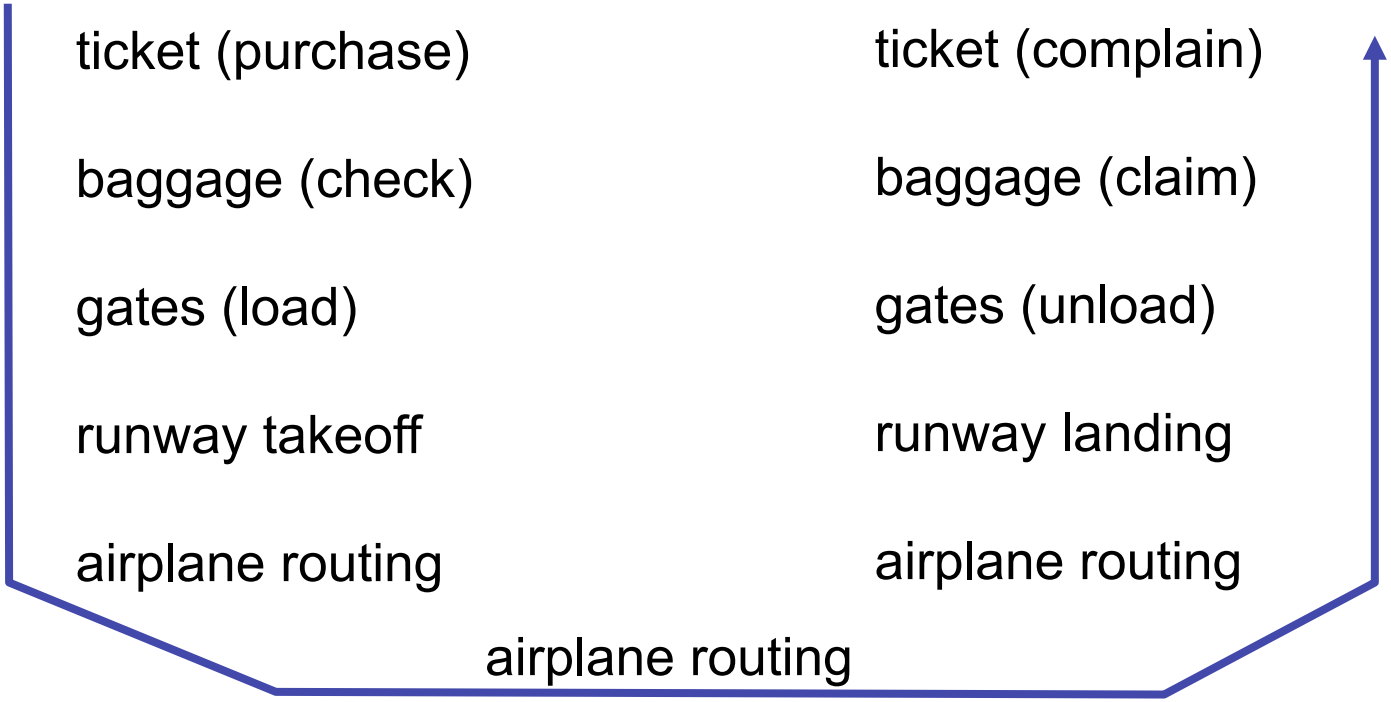
Is there any hope of *organizing* structure of network?

Or at least our discussion of networks?

Package-shipping example

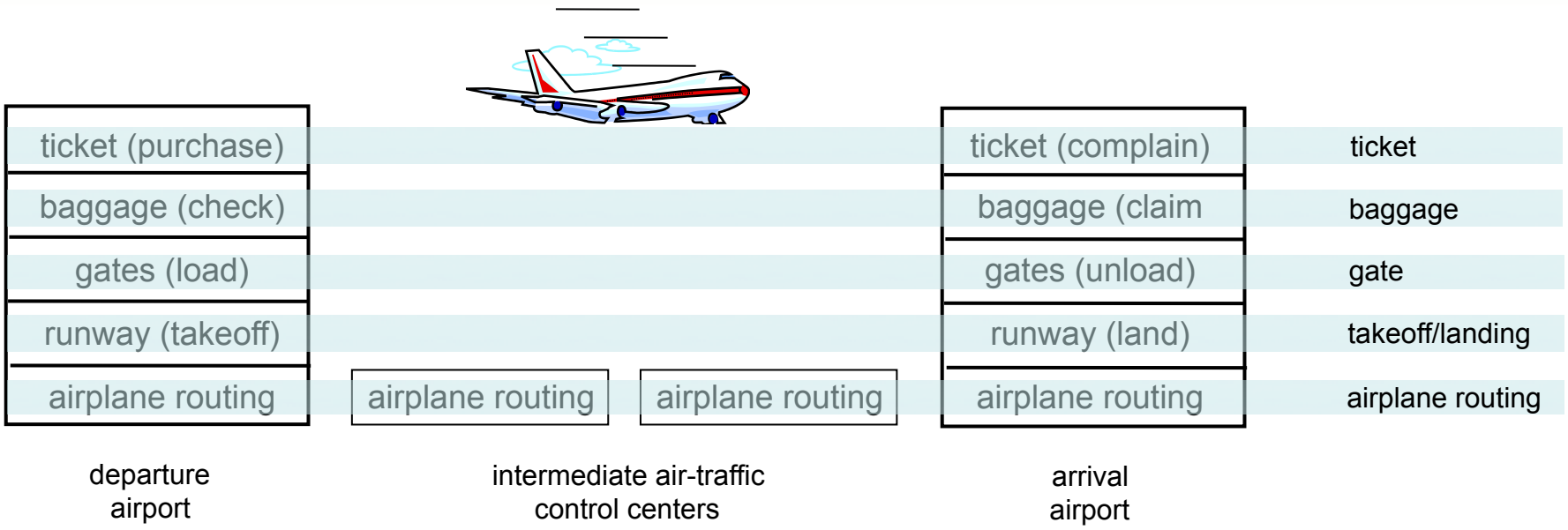


Organization of air travel



- a series of steps

Layering of airline functionality



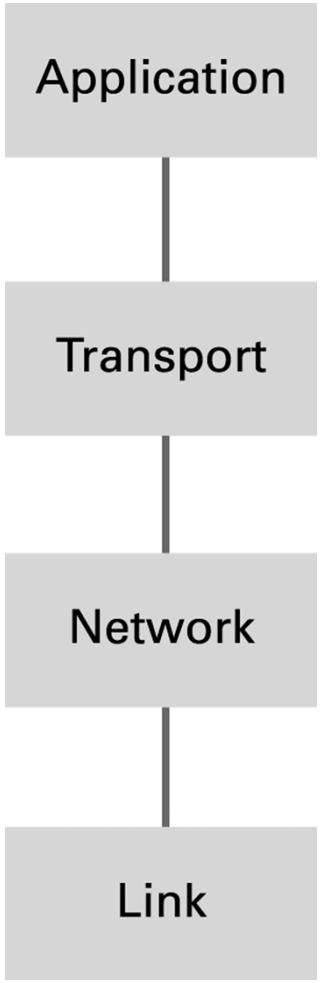
Layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

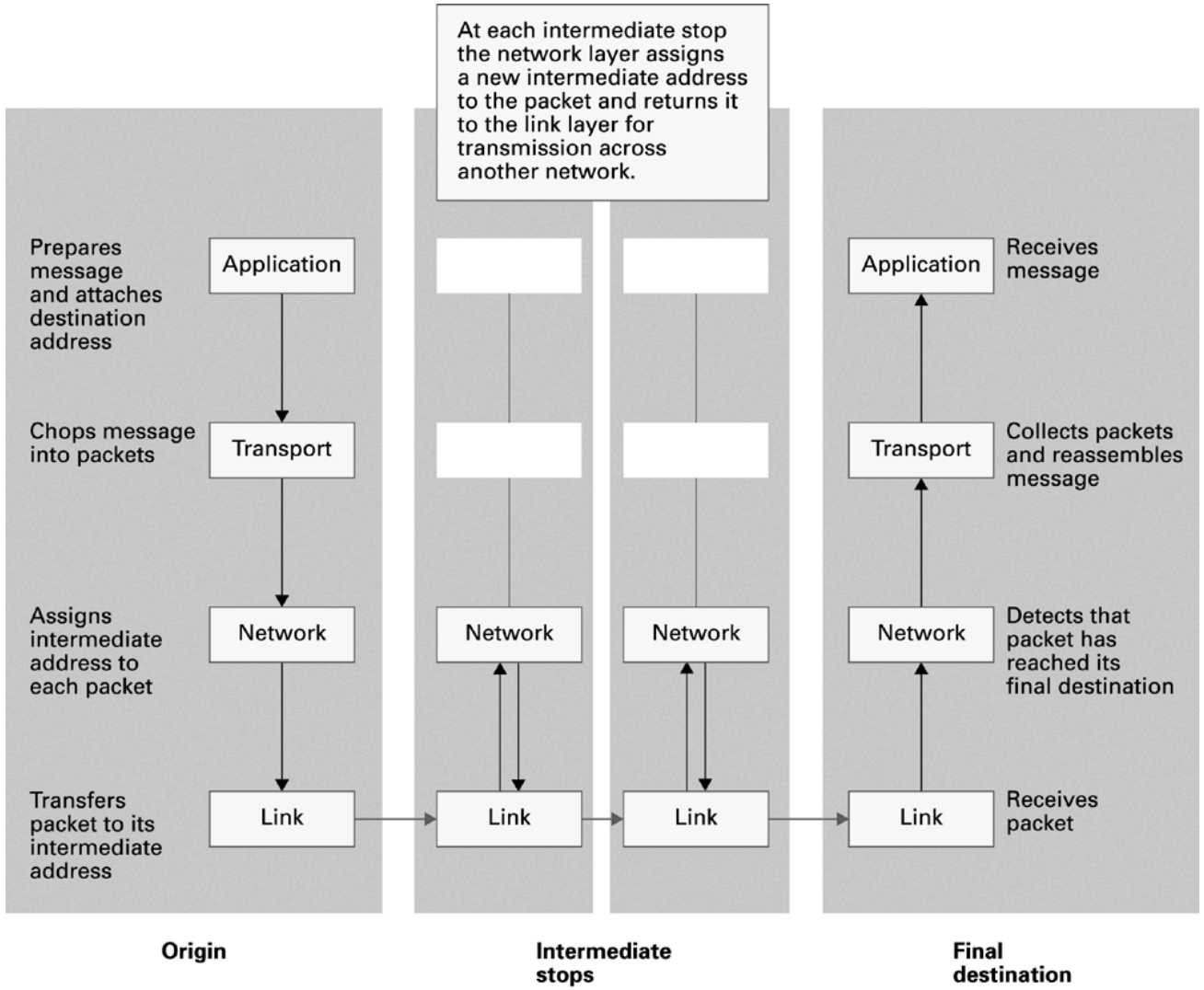
Internet Software Layers

- **Application:** Constructs message with address
- **Transport:** Chops message into packets
- **Network:** Handles routing through the Internet
- **Link:** Handles actual transmission of packets

The Internet software layers

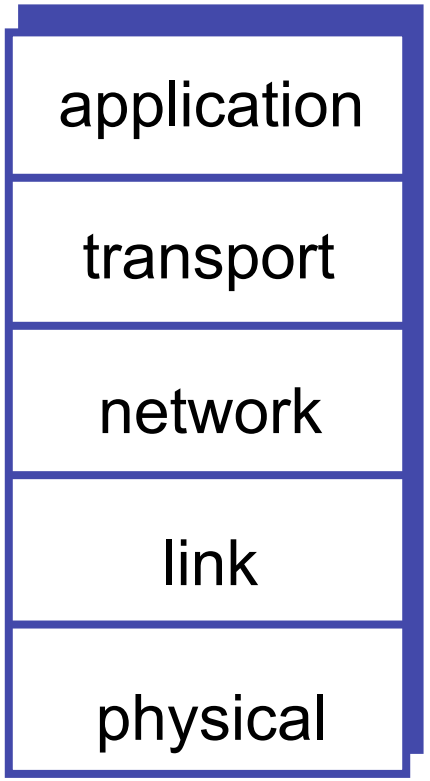


Following a message through the Internet

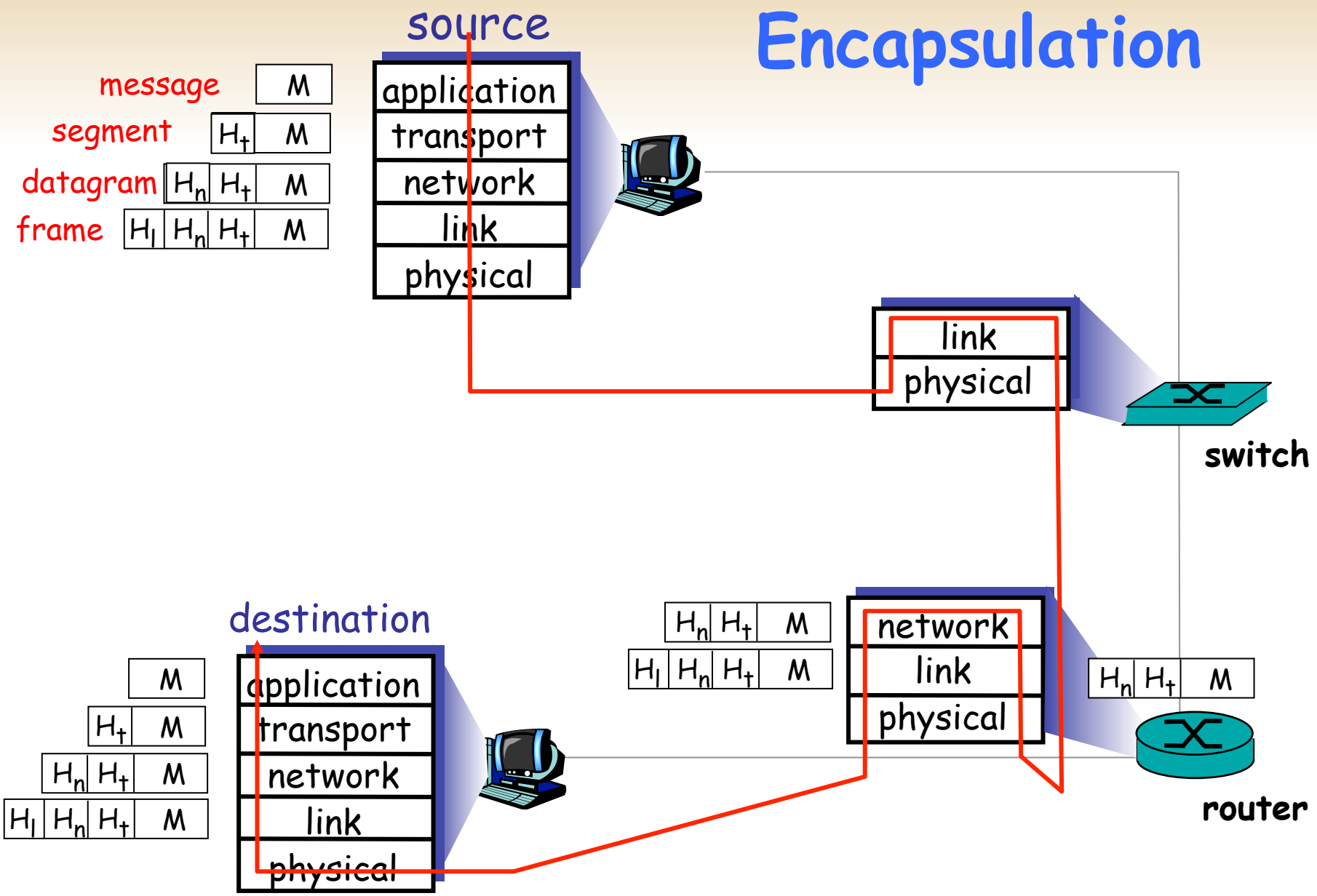


Internet protocol stack

- application: supporting network applications
  - FTP, SMTP, HTTP
- transport: process-process data transfer
  - TCP, UDP
- network: routing of datagrams from source to destination
  - IP, routing protocols
- link: data transfer between neighboring network elements
  - PPP, Ethernet
- physical: bits “on the wire”



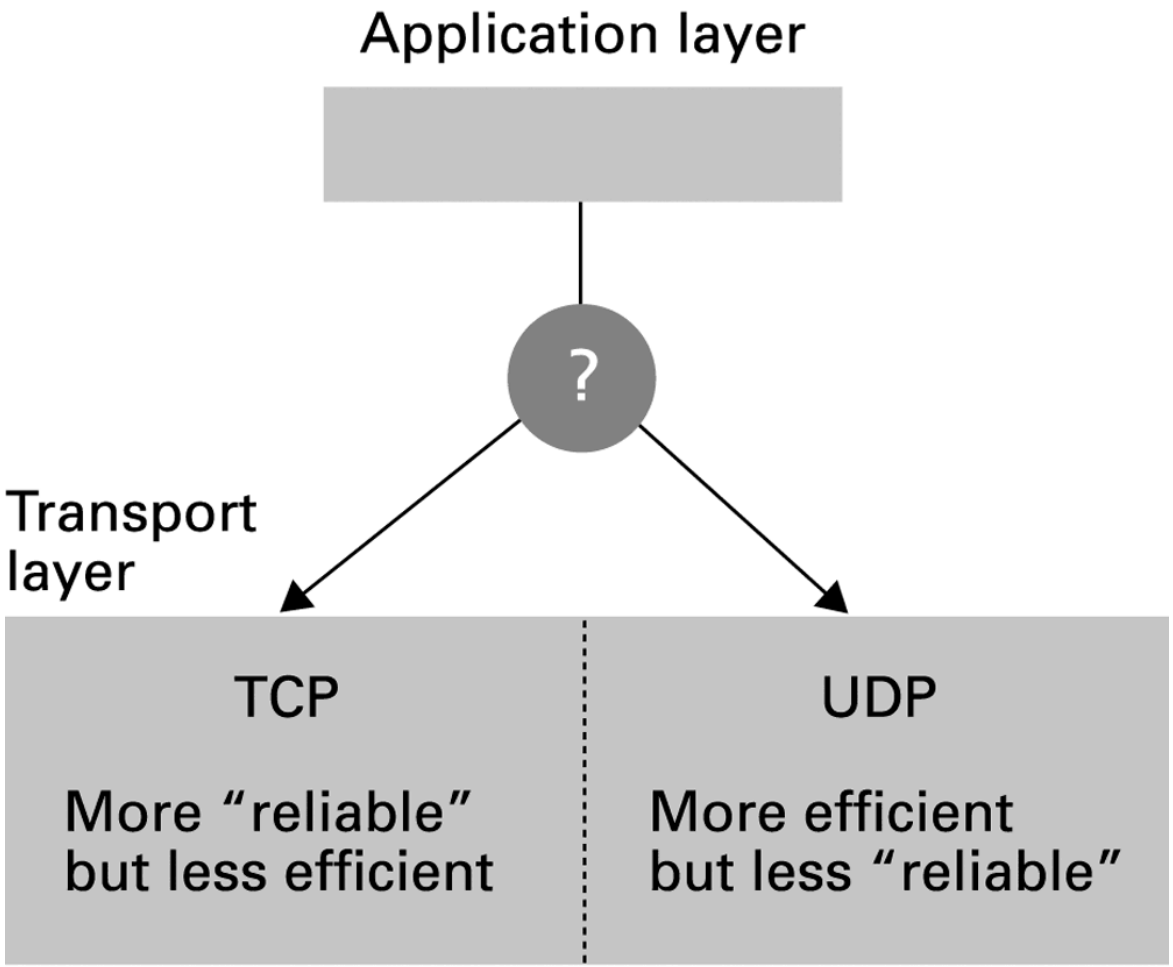
Encapsulation



TCP/IP Protocol Suite

- Transport Layer
  - TCP
  - UDP
- Network Layer
  - IP (IPv4 and IPv6)

Choosing between TCP and UDP



Networking and the Internet

- Network Fundamentals
- The Internet
- The World Wide Web
- Internet Protocols
- Security

Network Security

- The field of network security is about:
  - how bad guys can attack computer networks
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks
- Internet not originally designed with (much) security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network" ☺
  - Internet protocol designers playing "catch-up"
  - Security considerations in all layers!

Bad guys can put malware into hosts via Internet

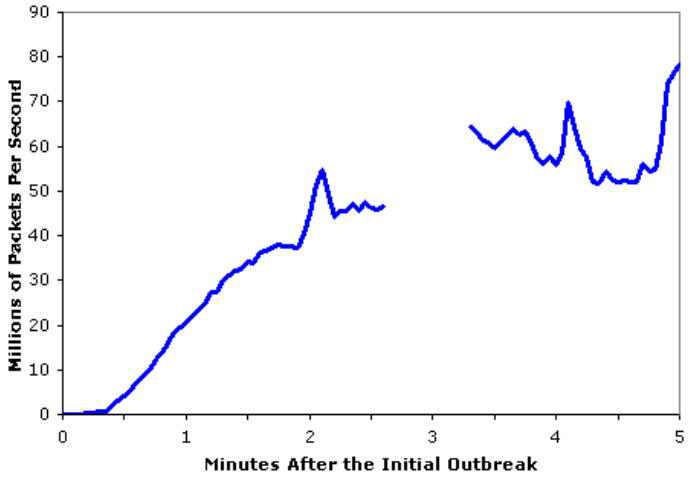
- Malware can get in host from a virus, worm, or trojan horse.
- Spyware malware can record keystrokes, web sites visited, upload info to collection site.
- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.
- Malware is often self-replicating: from an infected host, seeks entry into other hosts

Bad guys can put malware into hosts via Internet

- Trojan horse
  - Hidden part of some otherwise useful software
  - Today often on a Web page (Active-X, plugin)
- Virus
  - infection by receiving object (e.g., e-mail attachment), actively executing
  - self-replicating: propagate itself to other hosts, users

- Worm:
  - infection by passively receiving object that gets itself executed
  - self- replicating: propagates to other hosts, users

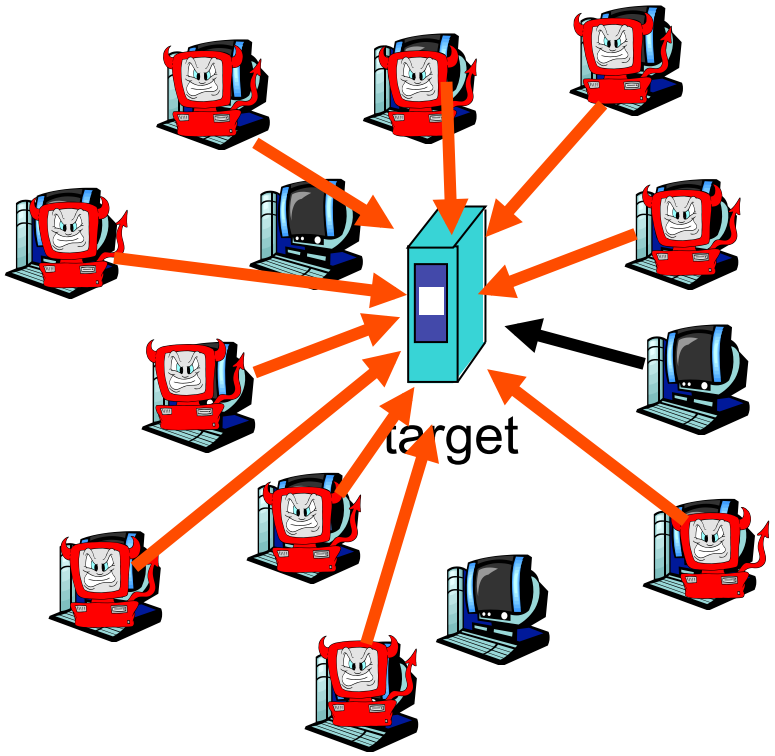
Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)



Bad guys can attack servers and network infrastructure

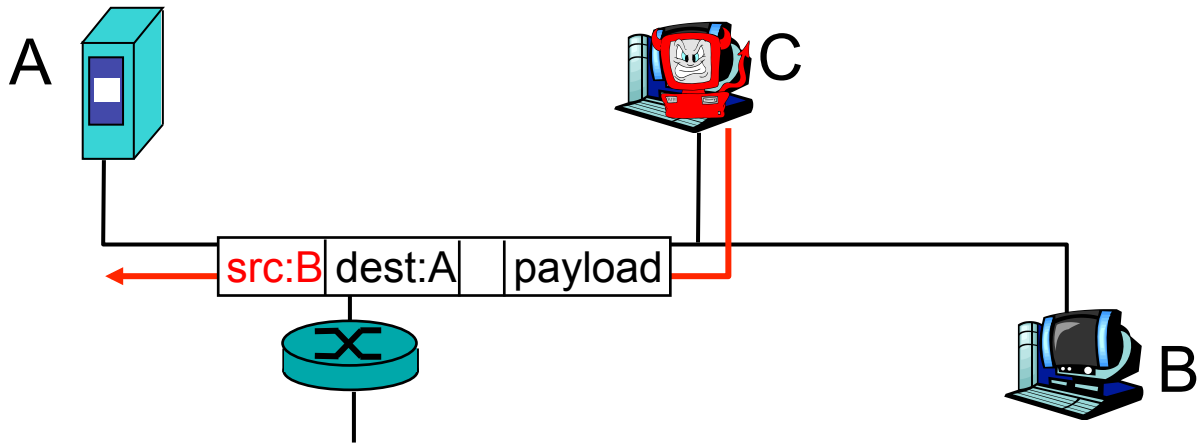
- Denial of service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts



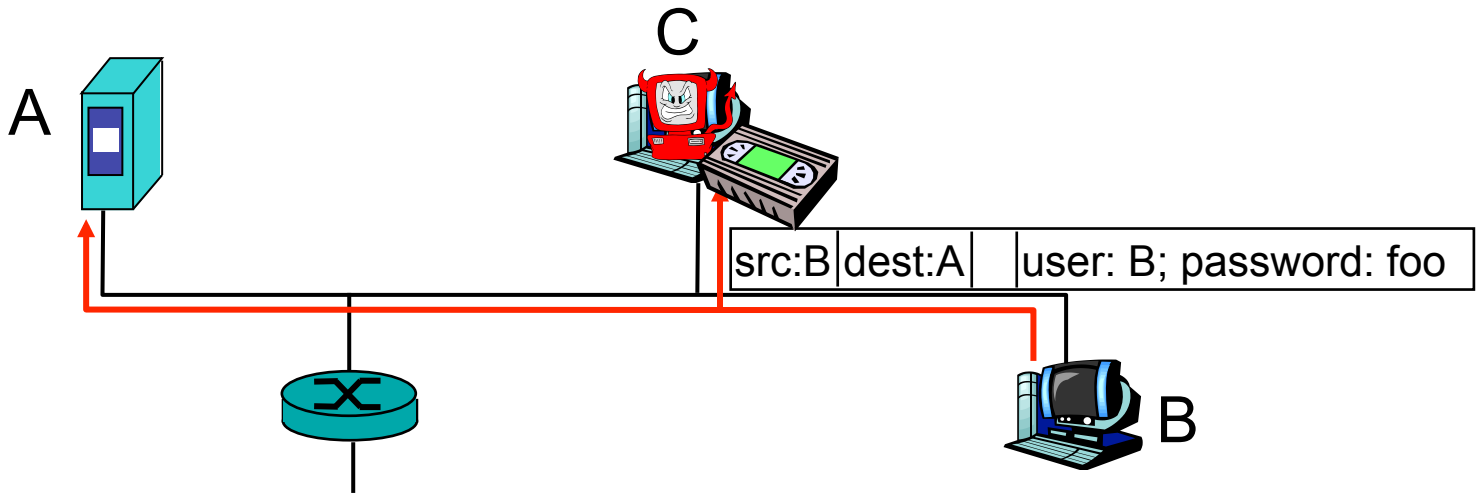
The bad guys can use false source addresses

- *IP spoofing:* send packet with false source address



The bad guys can record and playback

- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view



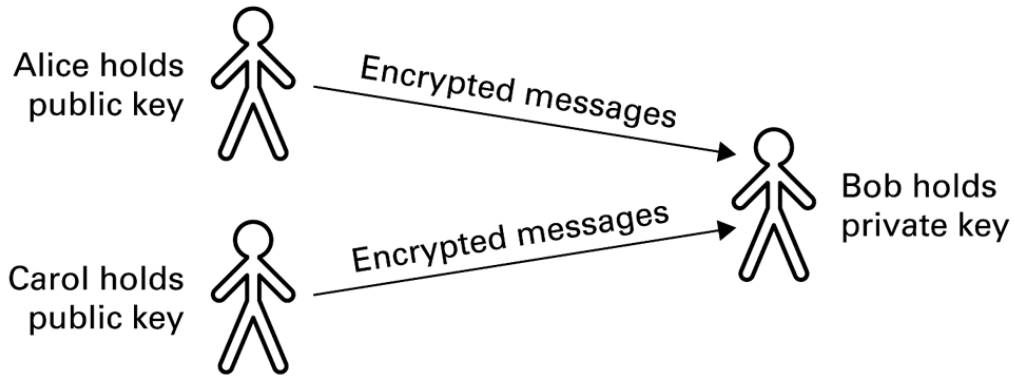
Security

- Attacks
  - Malware (viruses, worms, Trojan horses, spyware, phishing software)
  - Denial of service
  - Spam
- Protection
  - Firewalls
  - Spam filters
  - Proxy Servers
  - Antivirus software

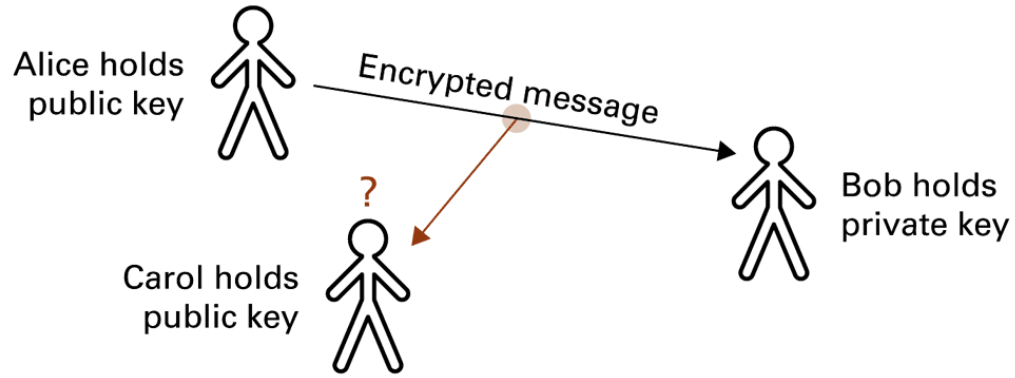
Encryption

- FTPS, HTTPS, SSL
- Public-key Encryption
  - Public key: Used to encrypt messages
  - Private key: Used to decrypt messages
- Certificates and Digital Signatures

Public-key encryption

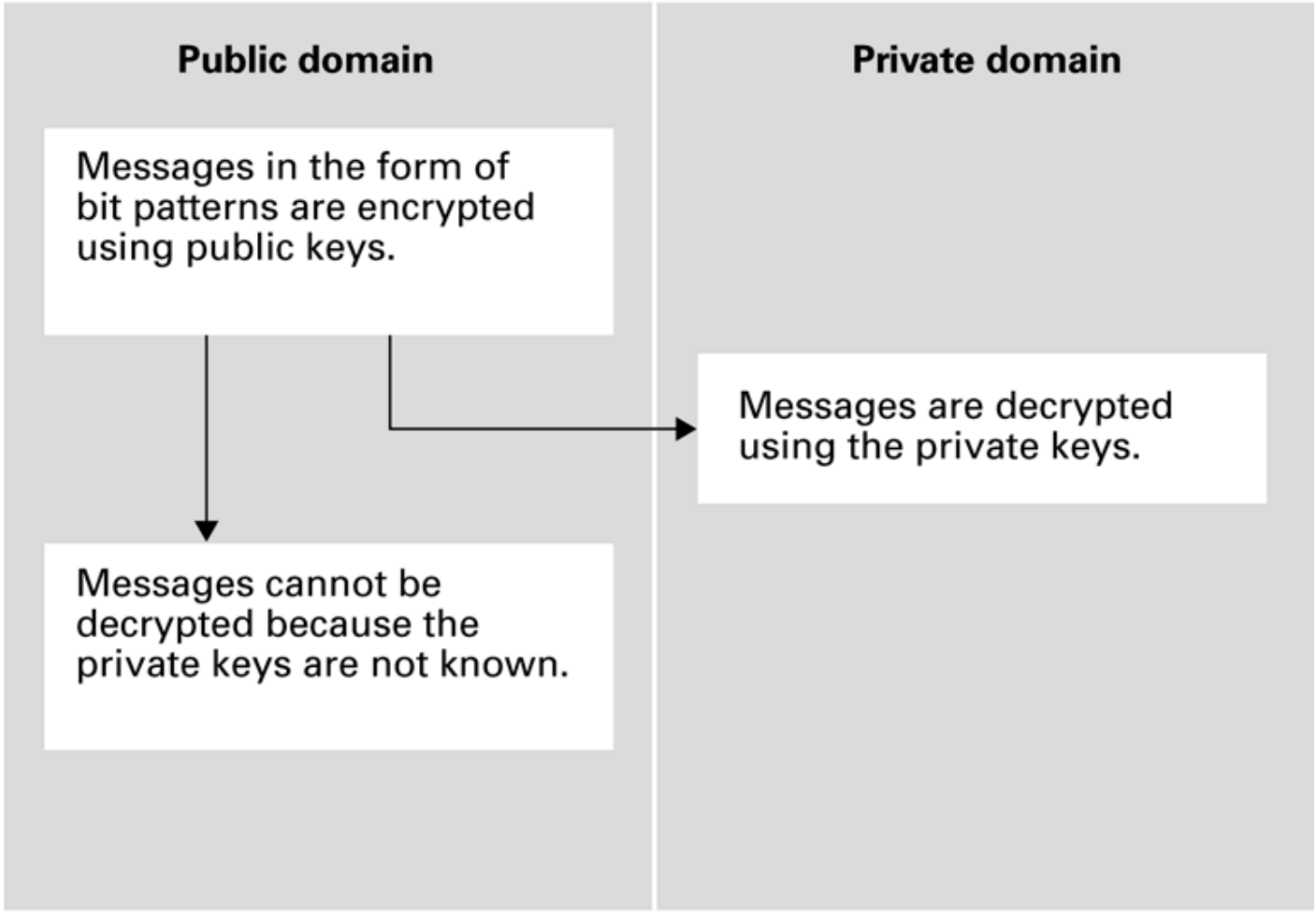


Both Alice and Carol can send encrypted messages to Bob.

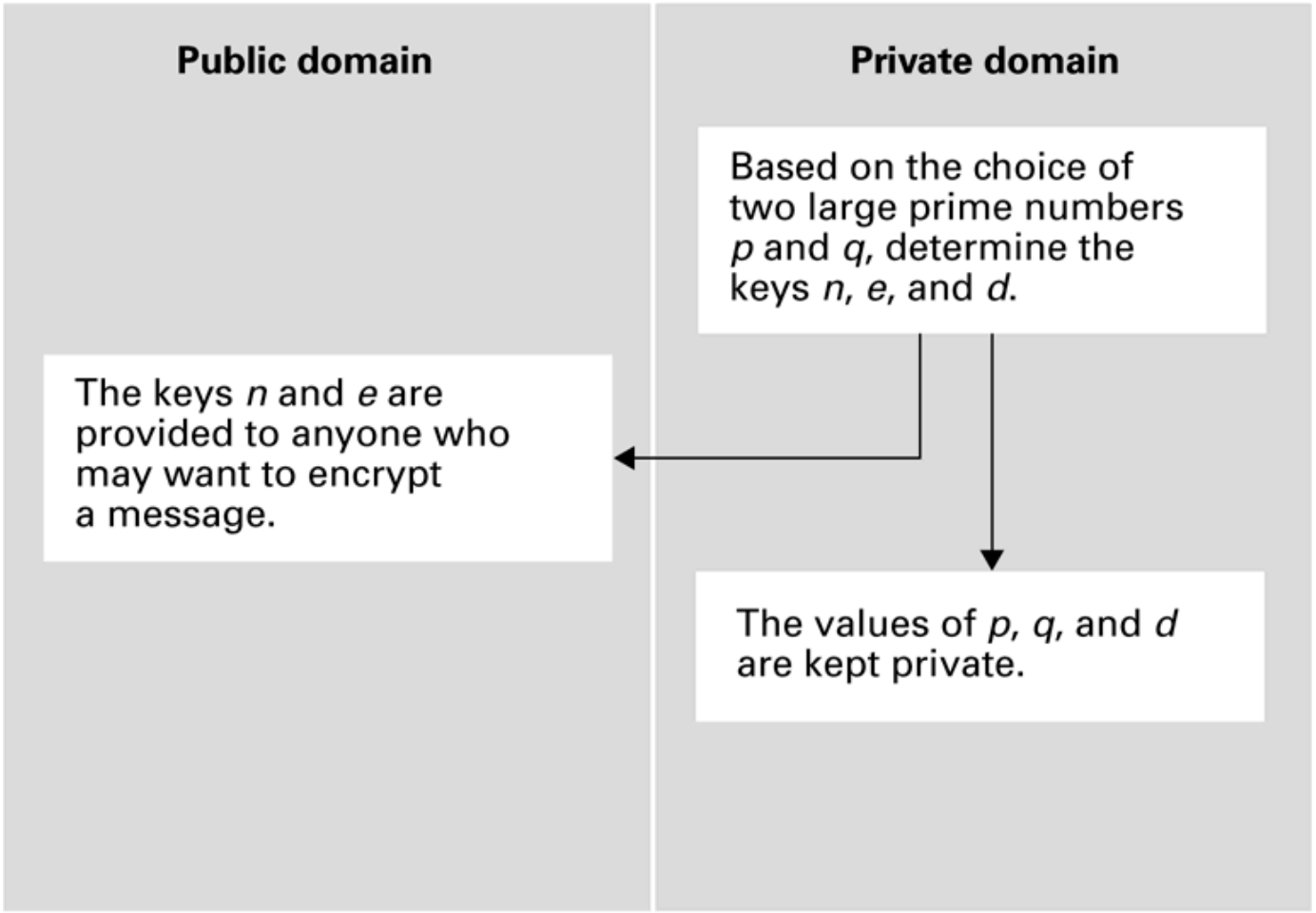


Carol cannot decrypt Alice's message even though she knows how Alice encrypted it.

Public key cryptography



Establishing an RSA public key encryption system



Public-Key Cryptography

- **Key:** A value used to encrypt or decrypt a message
  - **Public key**: Used to encrypt messages
  - **Private key**: Used to decrypt messages
- **RSA:** A popular public key cryptographic algorithm
  - Relies on the (presumed) intractability of the problem of factoring large numbers

Encrypting the Message 10111

- Encrypting keys: n = 91 and e = 5
- $10111_{two} = 23_{ten}$
- $23^{e} = 23^{5} = 6{,}436{,}343$
- 6,436,343 ÷ 91 has a remainder of 4
- $4_{ten} = 100_{two}$
- Therefore, encrypted version of 10111 is 100.

Decrypting the Message 100

- Decrypting keys: d = 29, n = 91
- $100_{two} = 4_{ten}$
- $4^{d} = 4^{29} = 288{,}230{,}376{,}151{,}711{,}744$
- 288,230,376,151,711,744 ÷ 91 has a remainder of 23
- $23_{ten} = 10111_{two}$
- Therefore, decrypted version of 100 is 10111.