Southern Connecticut State University

SCSU

Computer Networking and Security

Instructor: Dr. Hao Wu

Week 1

What is a computer network?

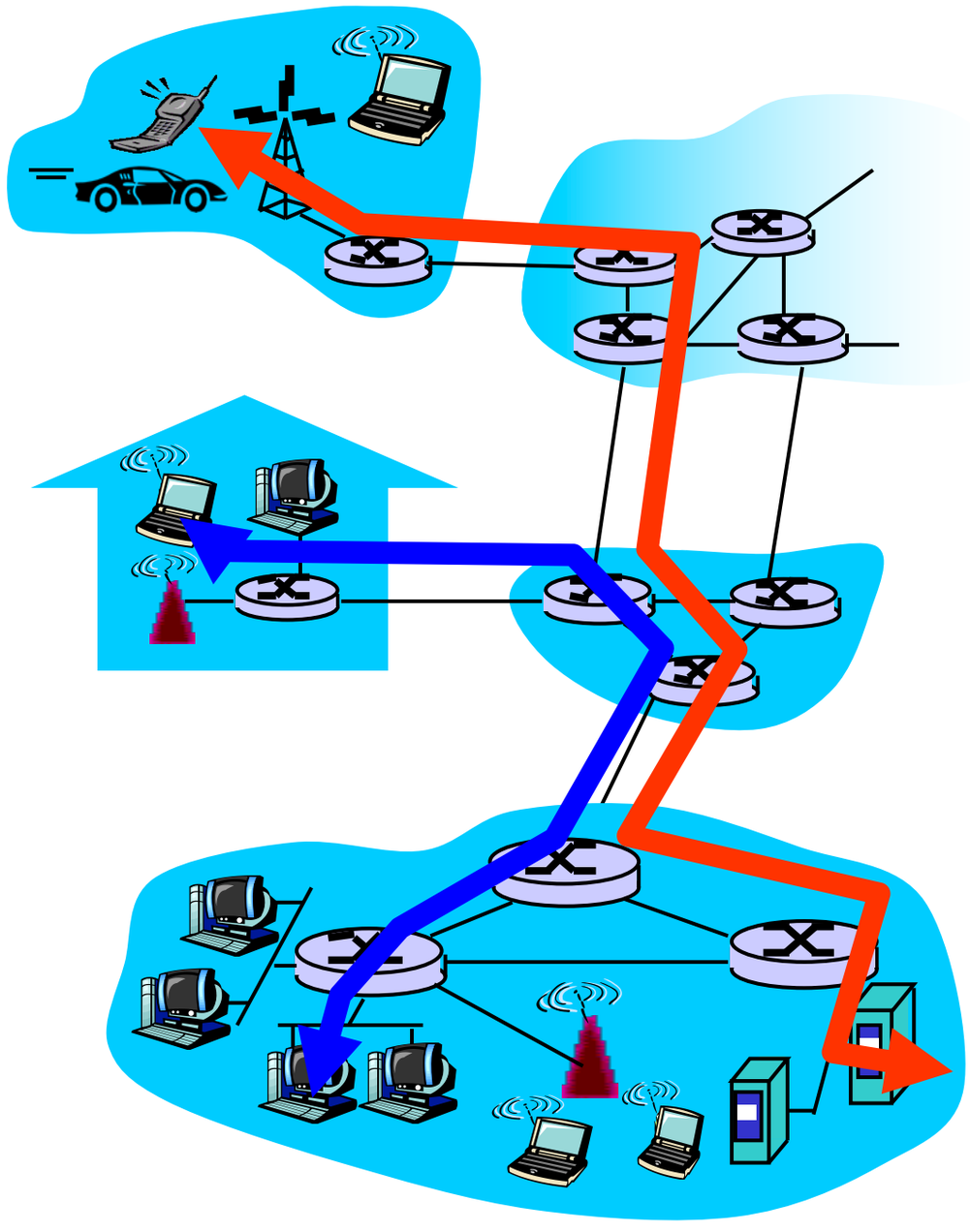
A Computer Network, or simply a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.

What is a Internet?

Circuit Switching

End-end resources reserved for "call"

- link bandwidth, switch capacity
- dedicated resources: no sharing
- circuit-like (guaranteed) performance
- call setup required



Circuit Switching

network resources (e.g., bandwidth) divided into "pieces"

- pieces allocated to calls
- resource piece *idle* if not used by owning call *(no sharing)*

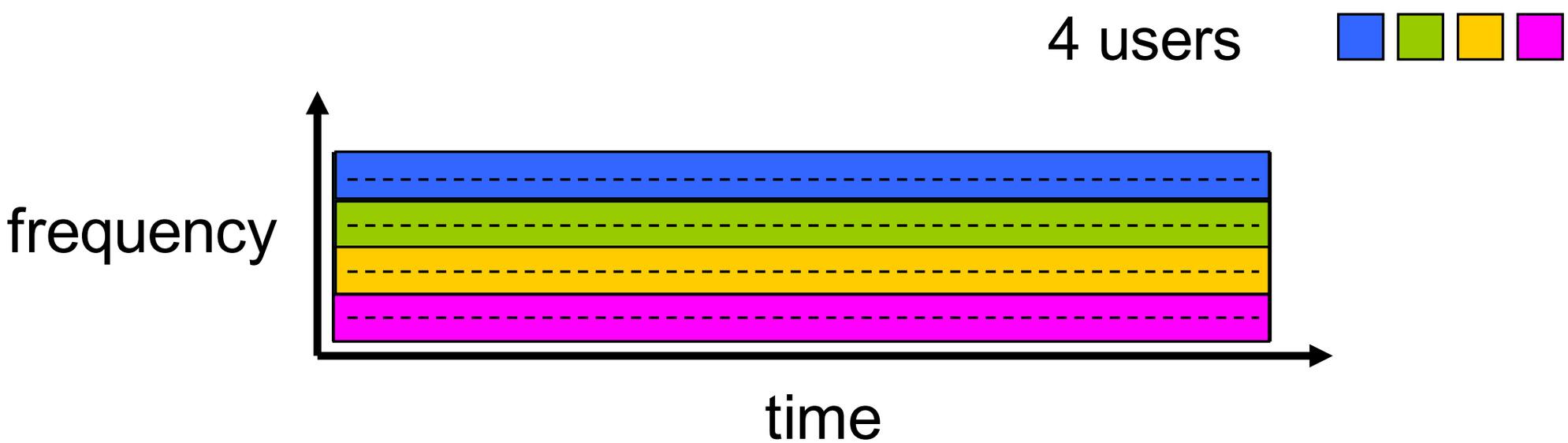
- dividing link bandwidth into "pieces"
  - frequency division
  - time division

Circuit Switching: FDM and TDM

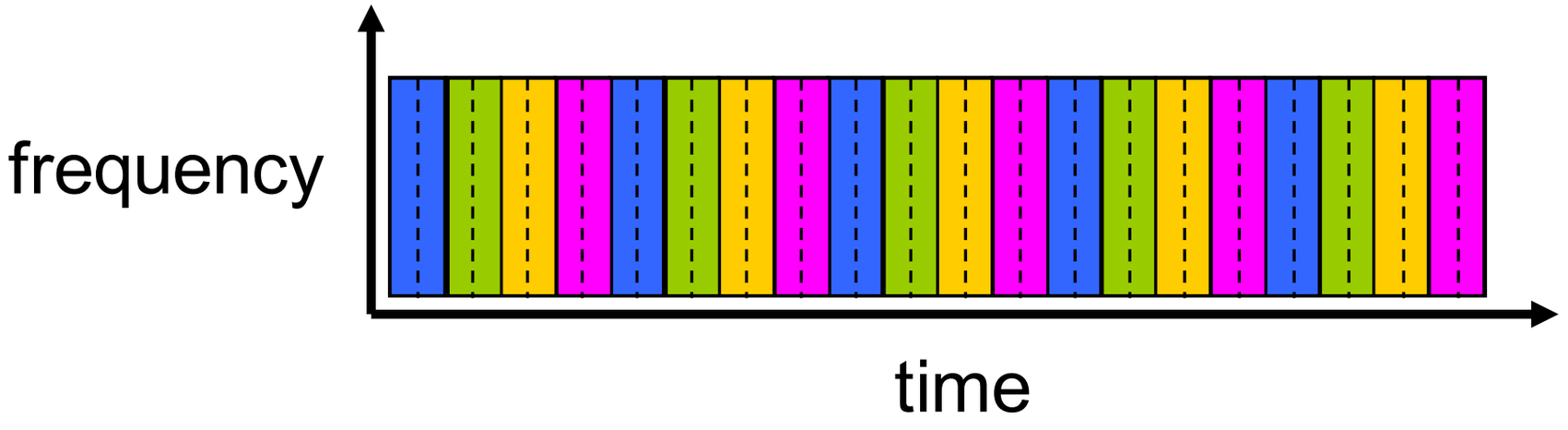
FDM

Example:

4 users



TDM



Circuit Switching

- How long does it take to send a file of 640,000 bits from host A to host B over a circuit-switched network?
  - All links are 1.536 Mbps
  - Each link uses TDM with 24 slots/sec
  - 500 msec to establish end-to-end circuit

Let's work it out!

Circuit Switching

Any problems with circuit switching?

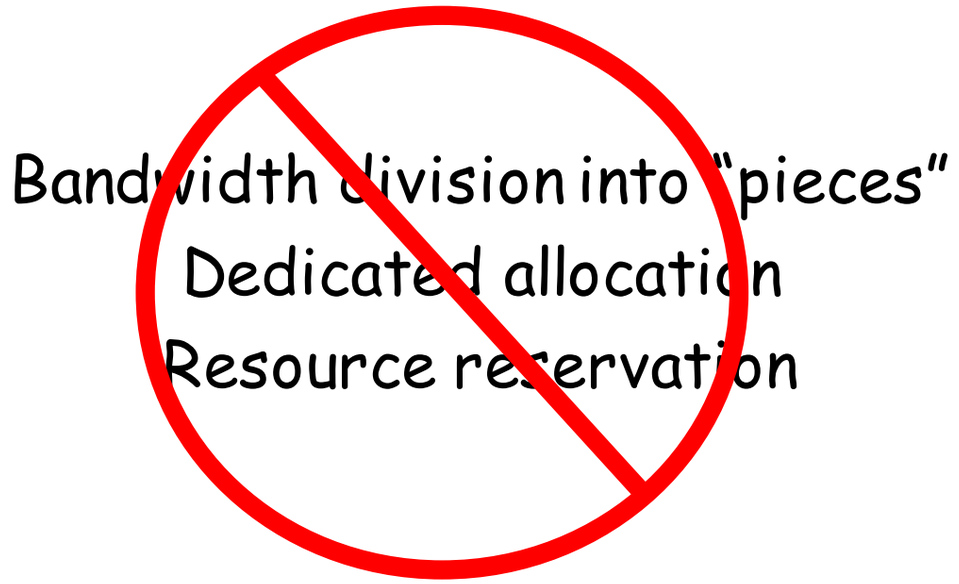
- Internet traffic is bursty

- Circuit switching is unsuitable for computer networks where the transfers have varies rate(bursty)

Packet Switching

each end-end data stream divided into *packets*

- user A, B packets *share* network resources
- each packet uses full link bandwidth
- resources used *as needed*



Roberts published an overall plan for the ARPAnet (Advanced Research Projects Agency) in 1967, the first packet-switched computer network and a direct ancestor of today's public Internet!

Packet Switching

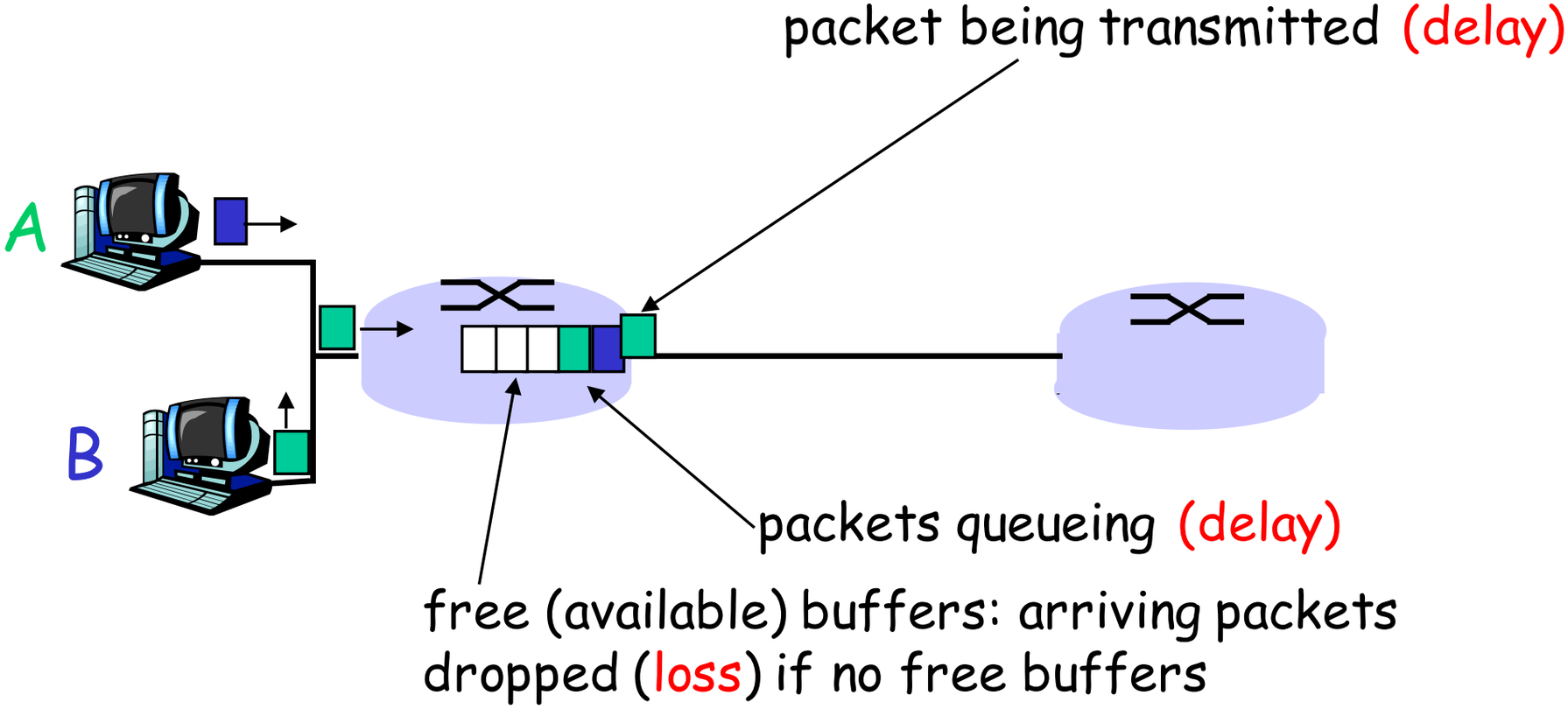
- Resource contention:
  - Aggregate resource demand can exceed amount available
  - Congestion: packets queue, wait for link use
  - Store and forward: packets move one hop at a time

- Node receives complete packet before forwarding

Packet Switching — loss and delay

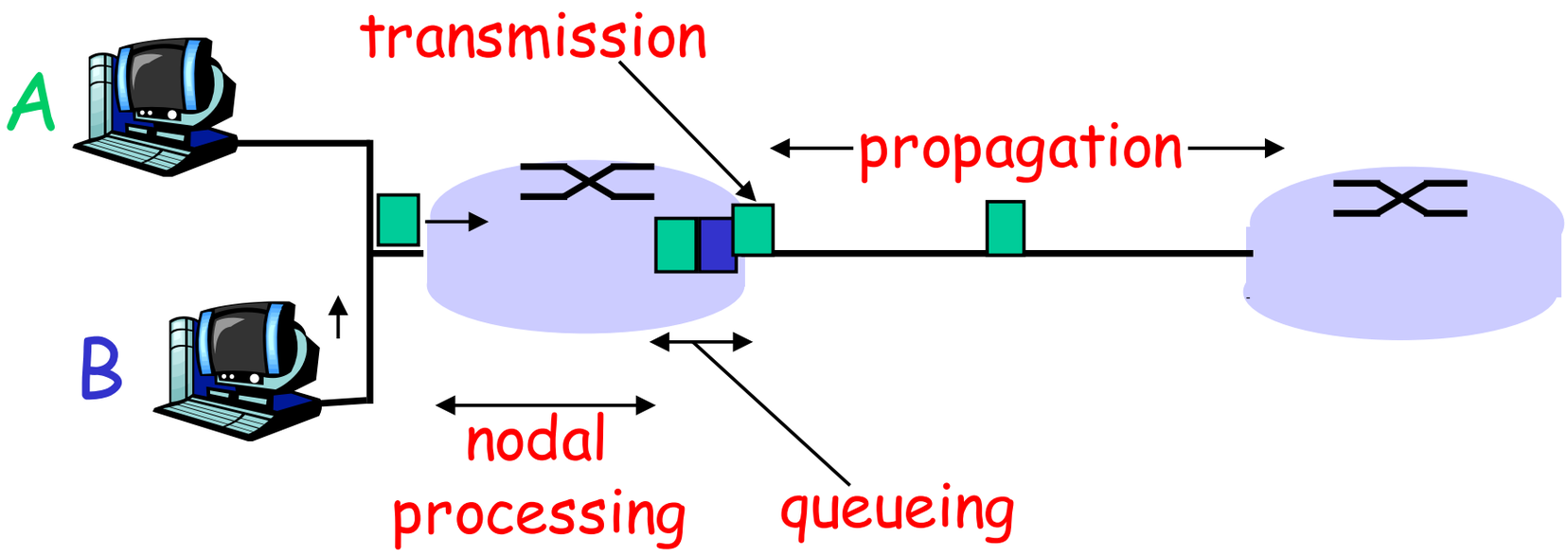
packets *queue* in router buffers

- packet arrival rate to link exceeds output link capacity
- packets queue, wait for turn



Four sources of packet delay

- 1. nodal processing:
  - check bit errors
  - determine output link
- 2. queueing
  - time waiting at output link for transmission
  - depends on congestion level of router



Delay in packet-switched networks

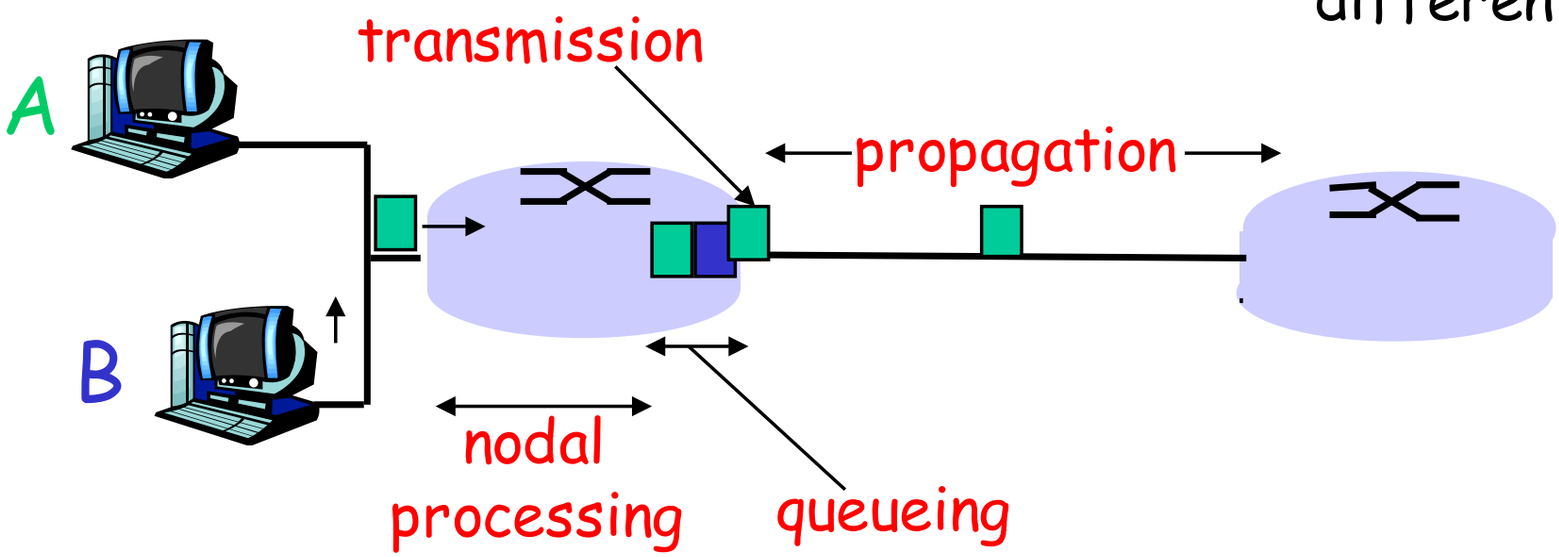
3. Transmission delay:

- R=link bandwidth (bps)
- L=packet length (bits)
- time to send bits into link = L/R

4. Propagation delay:

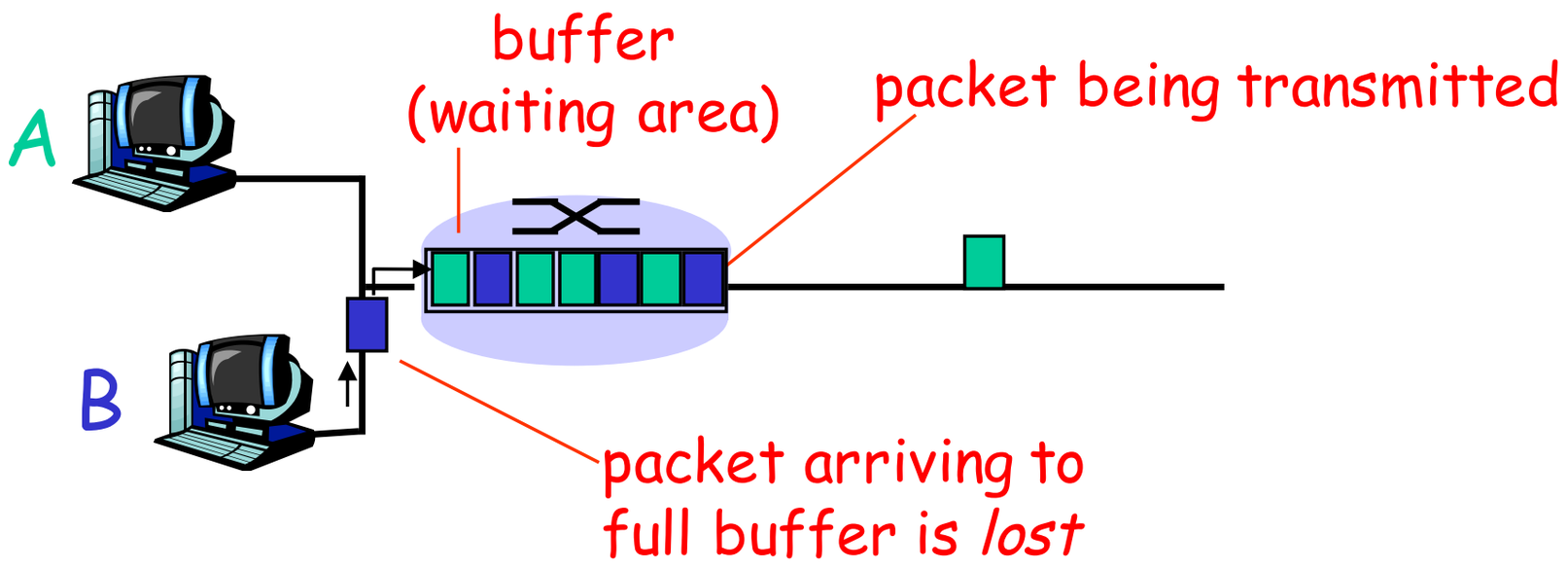
- d = length of physical link
- s = propagation speed in medium (~2×10^8 m/sec)
- propagation delay = d/s

Note: s and R are *very* different quantities!



Packet Loss

- queue (aka buffer) preceding link in buffer has finite capacity
- packet arriving to full queue dropped (aka lost)
- lost packet may be retransmitted by previous node, by source end system, or not at all



Circuit Switching v.s. Package Switching

Circuit Switching	Packet Switching
Guaranteed capacity	No guarantees (best effort)
Capacity is wasted if data is bursty	More efficient
Before sending data establishes a path	Send data immediately
All data in a single flow follow one path	Different packets might follow different paths
No reordering; constant delay; no packet drops	Packets may be reordered, delayed, or dropped

Protocol

- What is 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

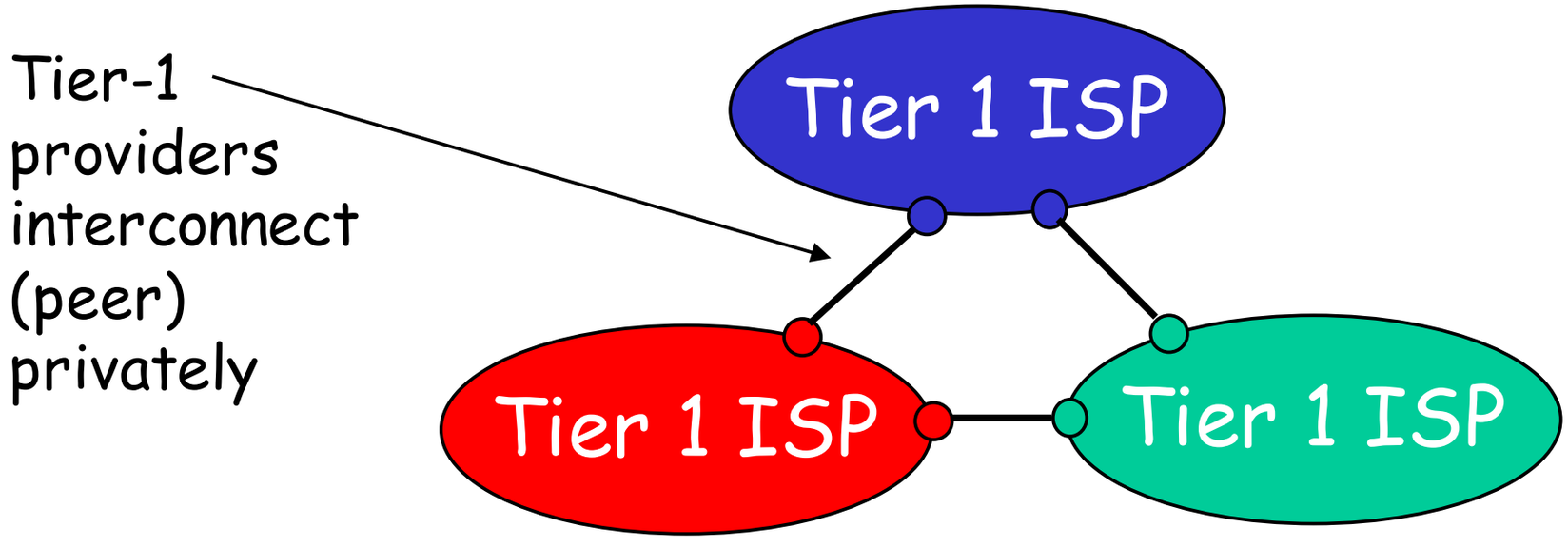
protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

Protocol

- Three key Internet protocols that we see today:
  - TCP: Transmission Control Protocol, Internet's reliable data transfer service
  - UDP: User Datagram Protocol, best effort (unreliable) data transfer service
  - IP: Internet Protocol, specifies the format of the packets that are sent and received among routers and end systems.

Network of Network

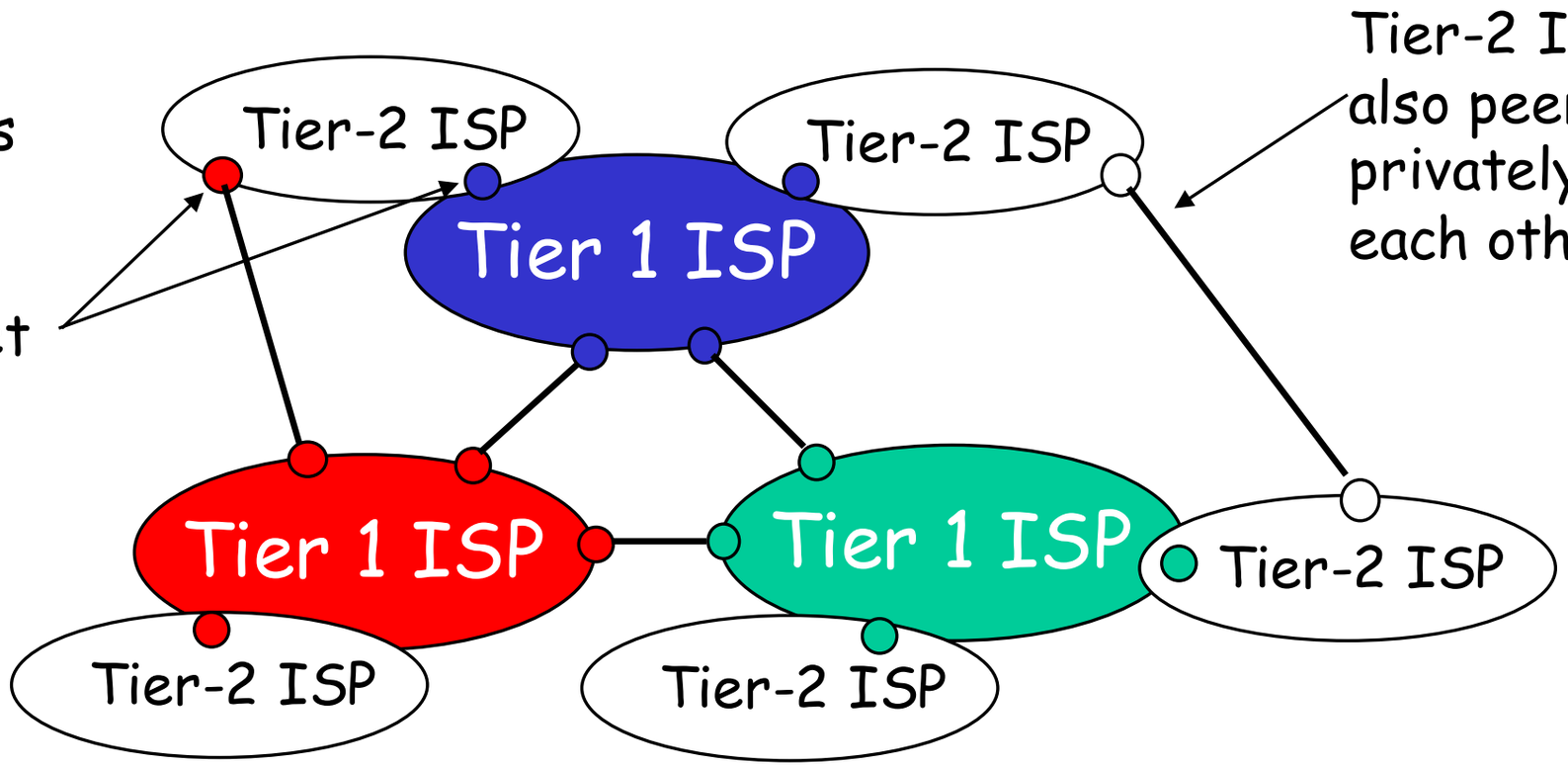
- roughly hierarchical
- at center: "tier-1" ISPs (e.g., Verizon, Sprint, AT&T, Cable and Wireless), national/international coverage
  - treat each other as equals



Network of Network

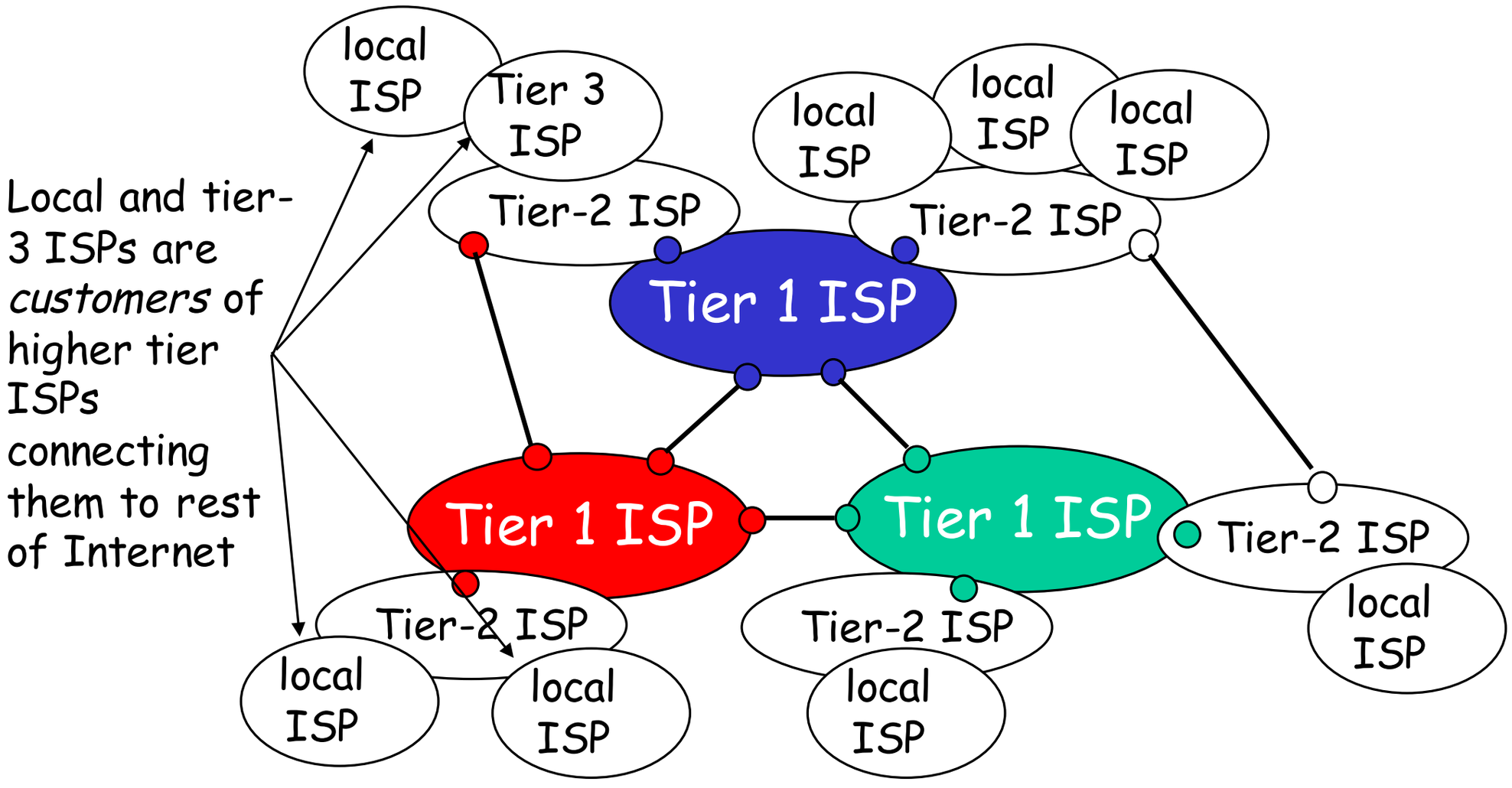
- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

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



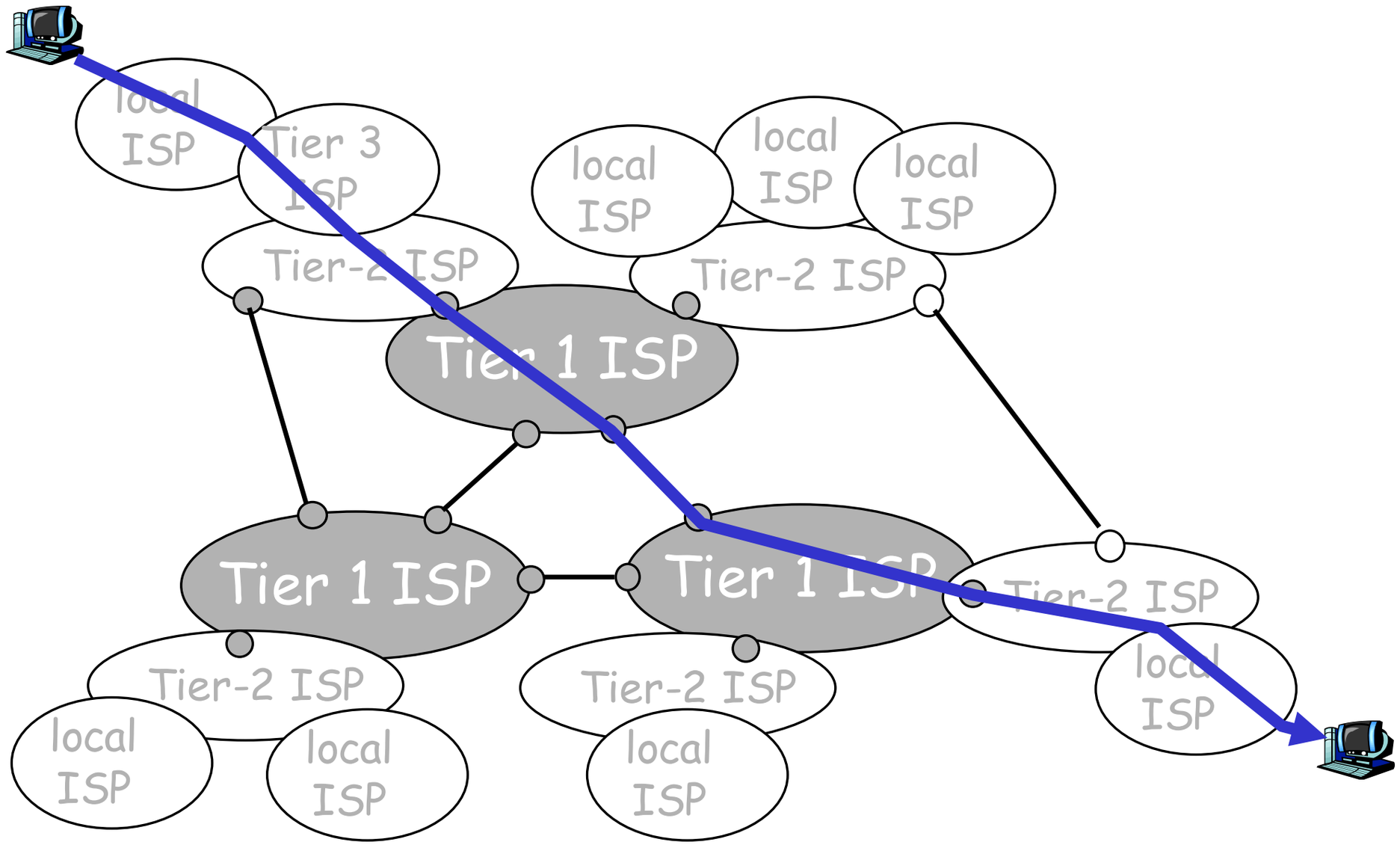
Network of Network

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



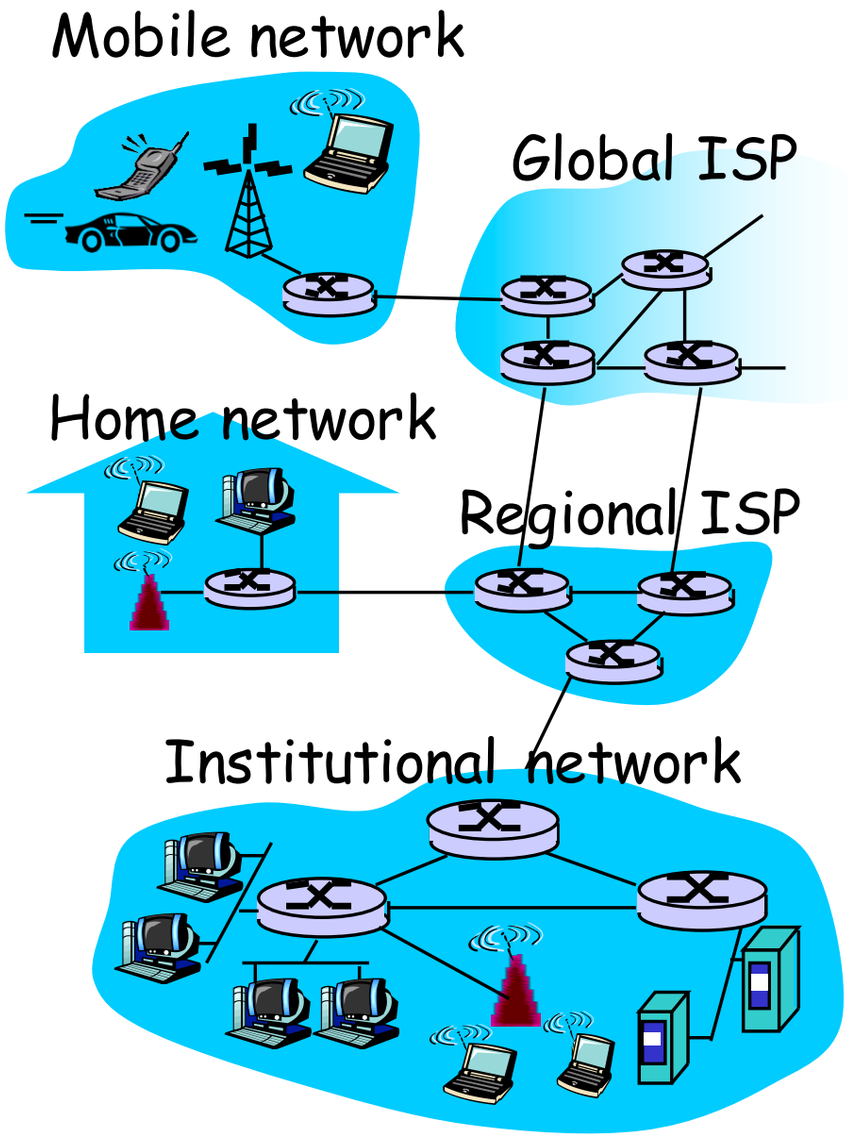
Network of Network

- a packet passes through many networks!



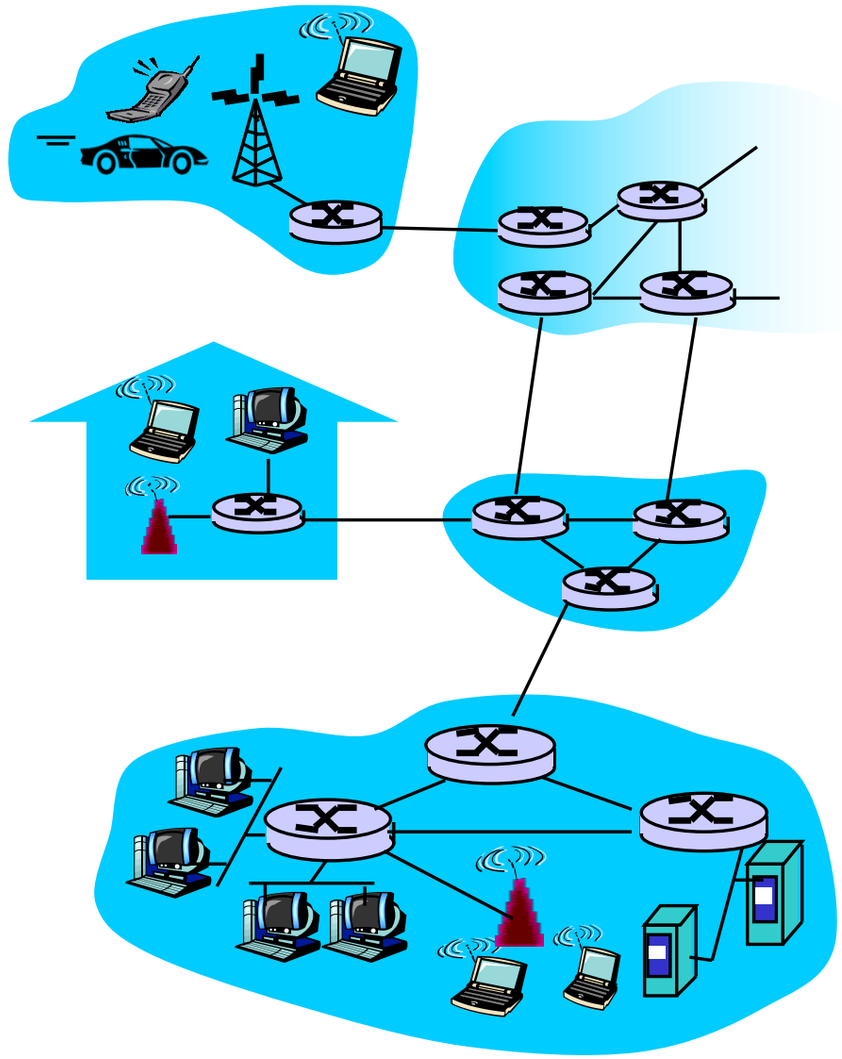
Internet

- millions of connected computing devices: *hosts = end systems*
  - running *network apps*
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = *bandwidth*
- *routers:* forward packets (chunks of data)



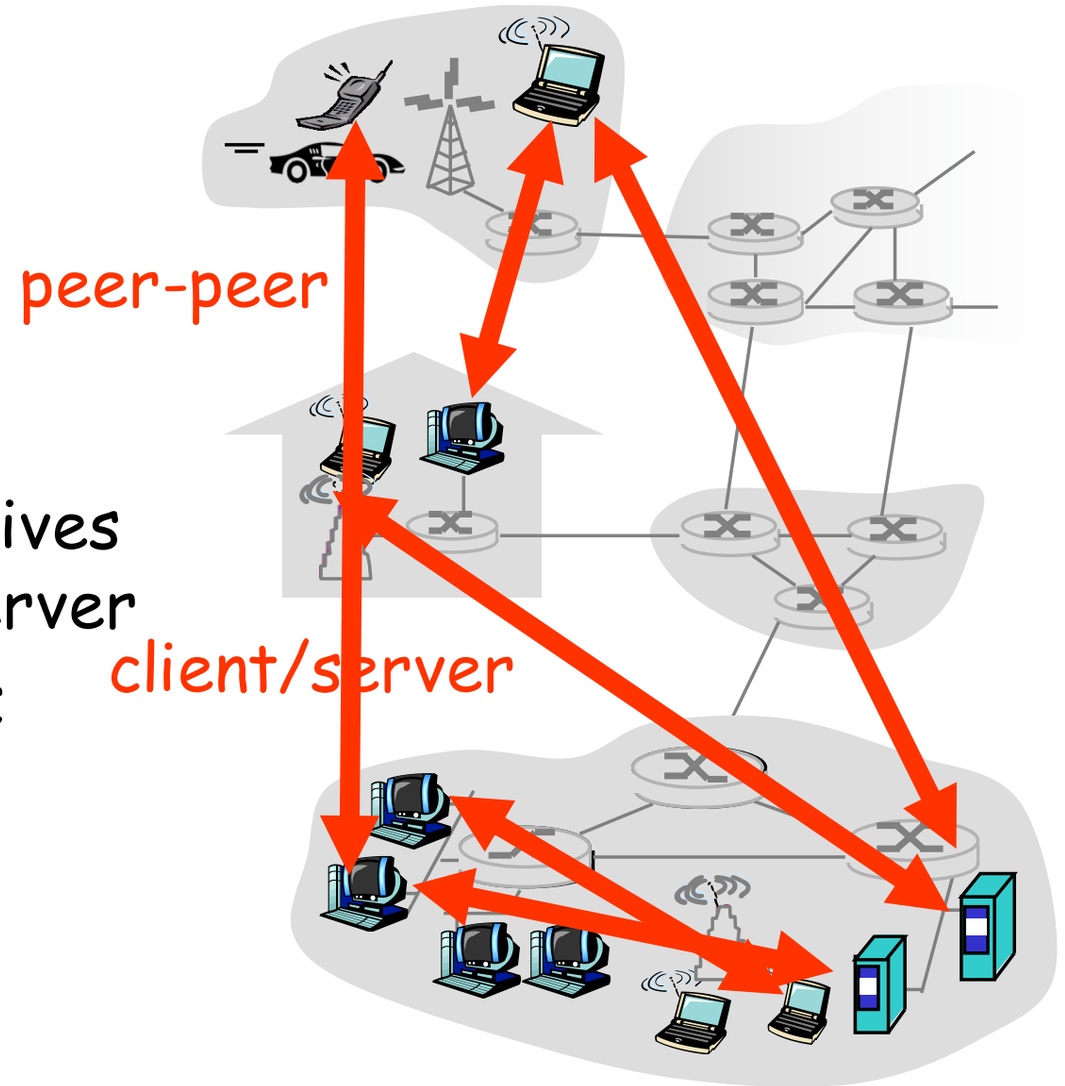
Internet

- 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, BitTorrenth



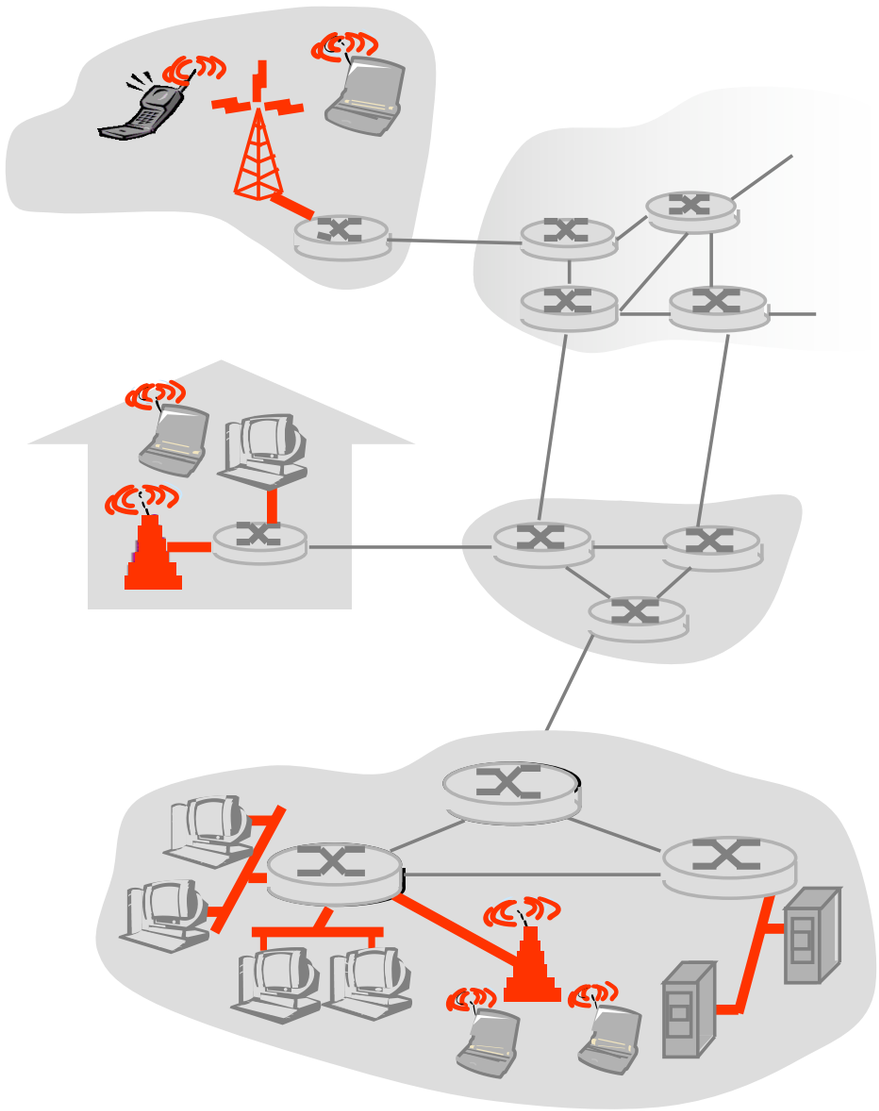
Access Networks and Physical Media

Q: How to connect end systems to edge router?

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

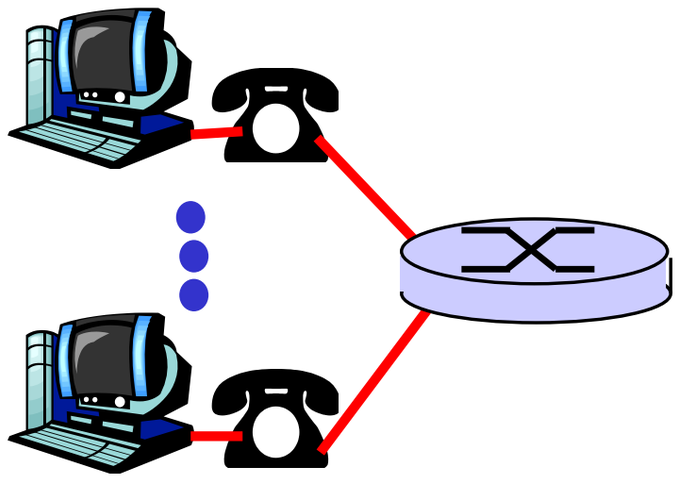
Keep in mind:

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



Residential Access

- Dialup via modem
  - up to 56Kbps direct access to router (often less)
  - Can't surf and phone at same time: can't be "always on"

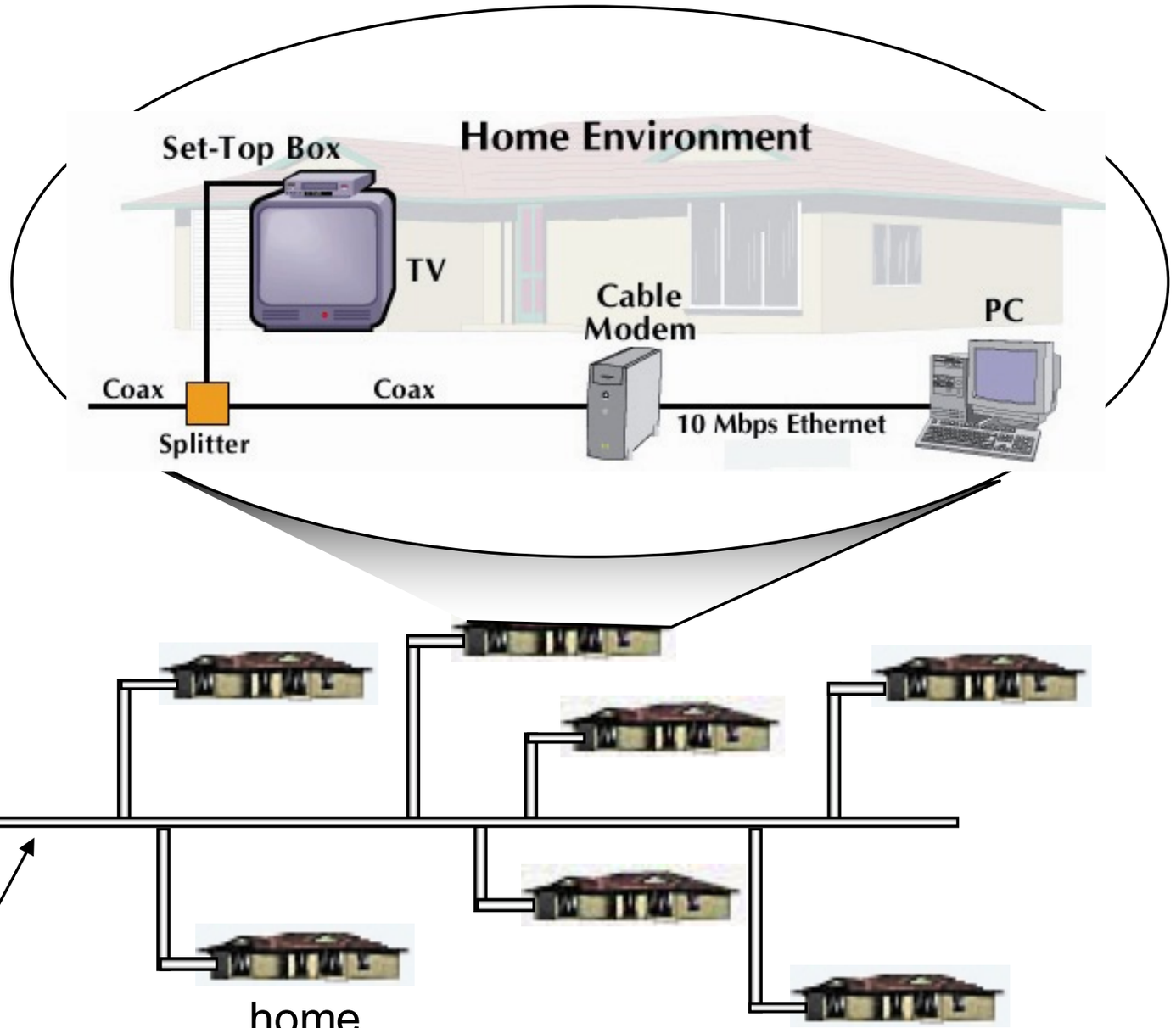


- DSL: digital subscriber line
  - deployment: telephone company (typically)
  - up to 1 Mbps upstream (today typically < 256 kbps)
  - up to 8 Mbps downstream (today typically < 1 Mbps)
  - dedicated physical line to telephone central office

Residential Access

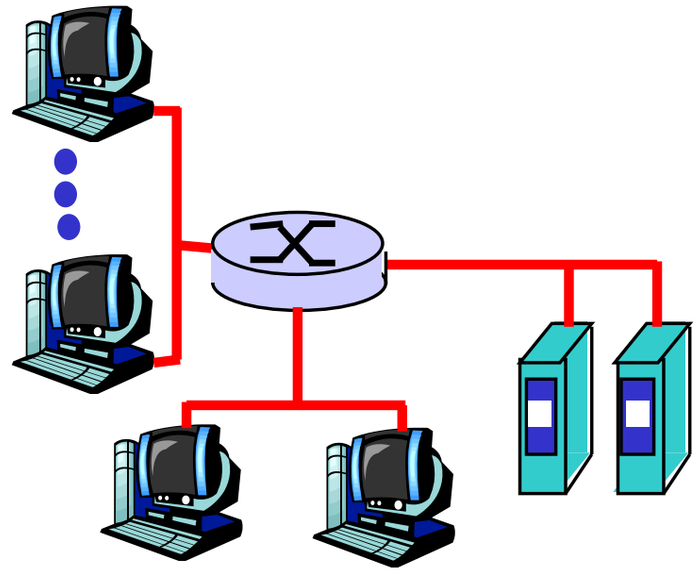
- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream, 2 Mbps upstream
- network of cable and fiber attaches homes to ISP router
  - homes share access to router
- deployment: available via cable TV companies

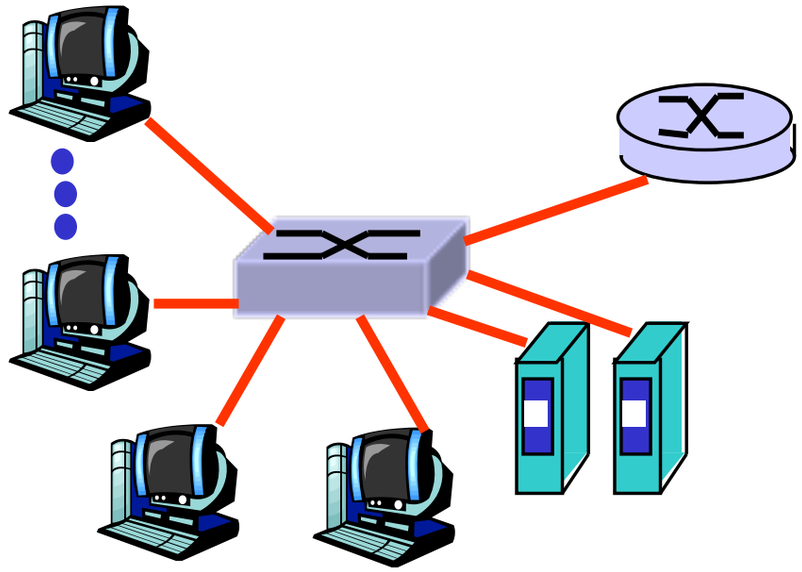
Cable Network Architecture



Company Access: Local Area Networks

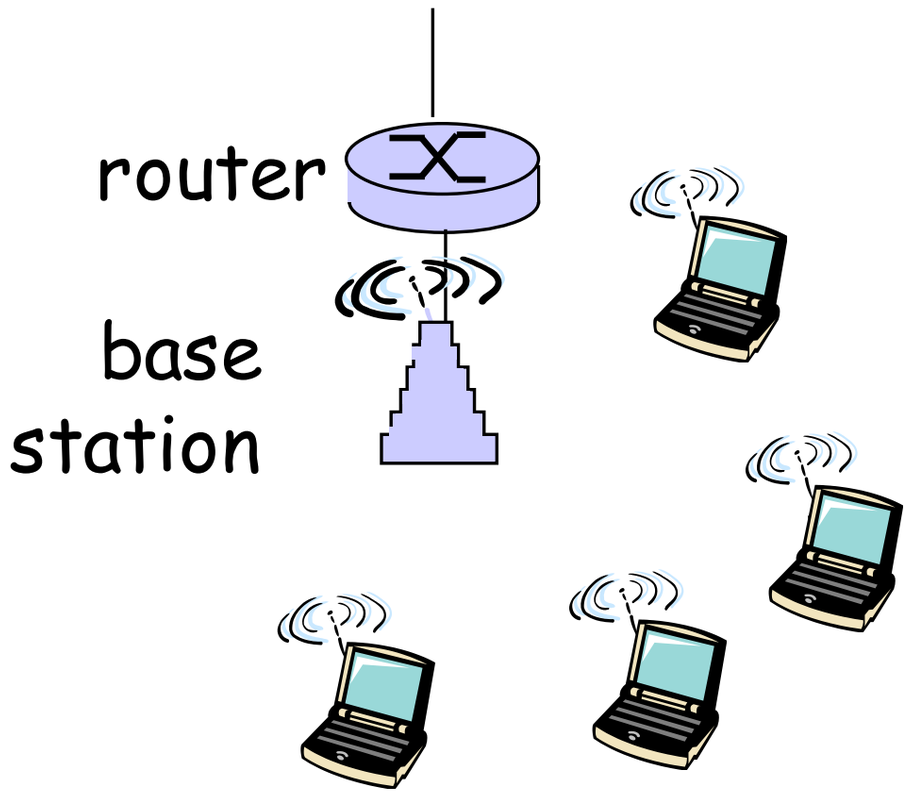
- company/univ local area network (LAN) connects end system to edge router
- Ethernet:
  - 10 Mbs, 100Mbps, 1Gbps, 10Gbps Ethernet
  - modern configuration: end systems connect into *Ethernet switch*





Wireless Access Network

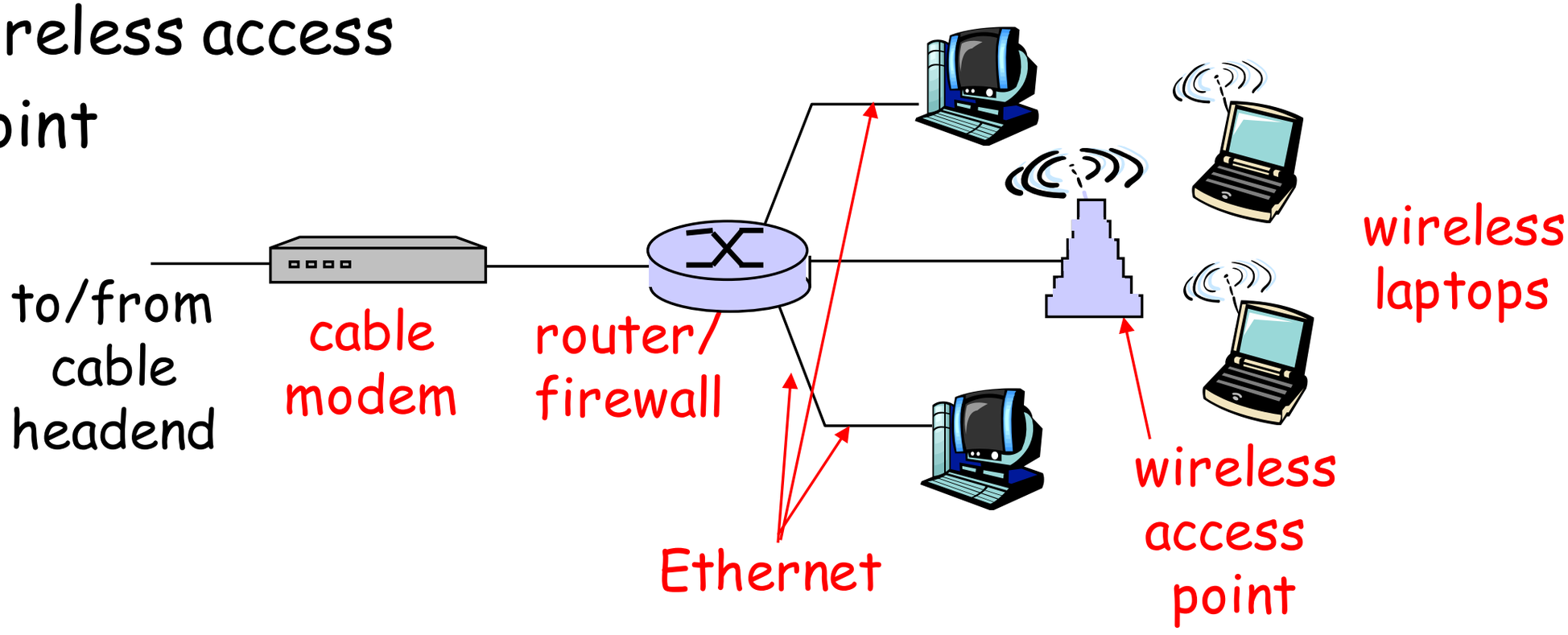
- shared *wireless* access network connects end system to router
  - via base station aka "access point"
- wireless LANs:
  - 802.11b/g/n/ac (WiFi): up to 866Mbps
- wider-area wireless access
  - provided by telco operator
  - ~1Mbps over cellular system (3G, 4G)
  - Long-Term Evolution (LTE)(10's Mbps) over wide area



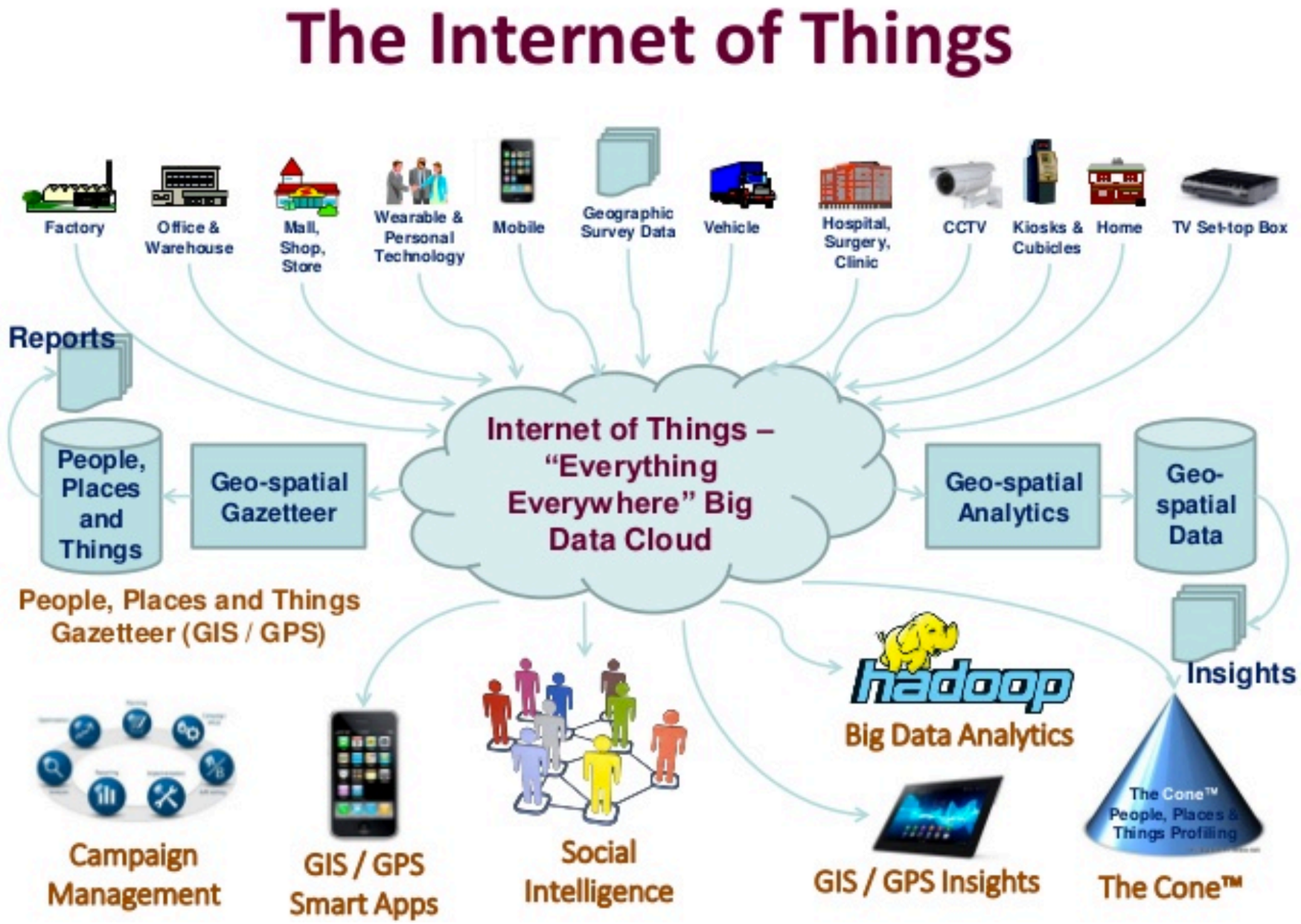
Home Network

Typical home network components:

- Cable modem
- router/firewall/NAT
- Ethernet
- wireless access point



Internet-of-things



Picture from: https://www.slideshare.net/NigelTebbutt1/the-internet-of-things-iot-pdf

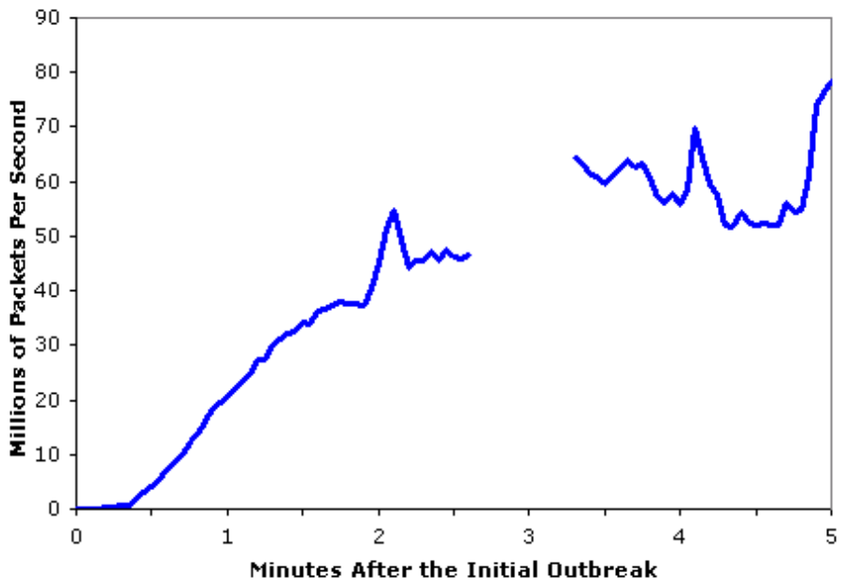
Network Security

- attacks on Internet infrastructure:
  - infecting/attacking hosts: malware, spyware, worms, unauthorized access (data stealing, user accounts)
  - denial of service: deny access to resources (servers, link bandwidth)
- 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!

What can bad guys do

- Spyware:
  - infection by downloading web page with spyware
  - records keystrokes, web sites visited, upload info to collection site
- 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

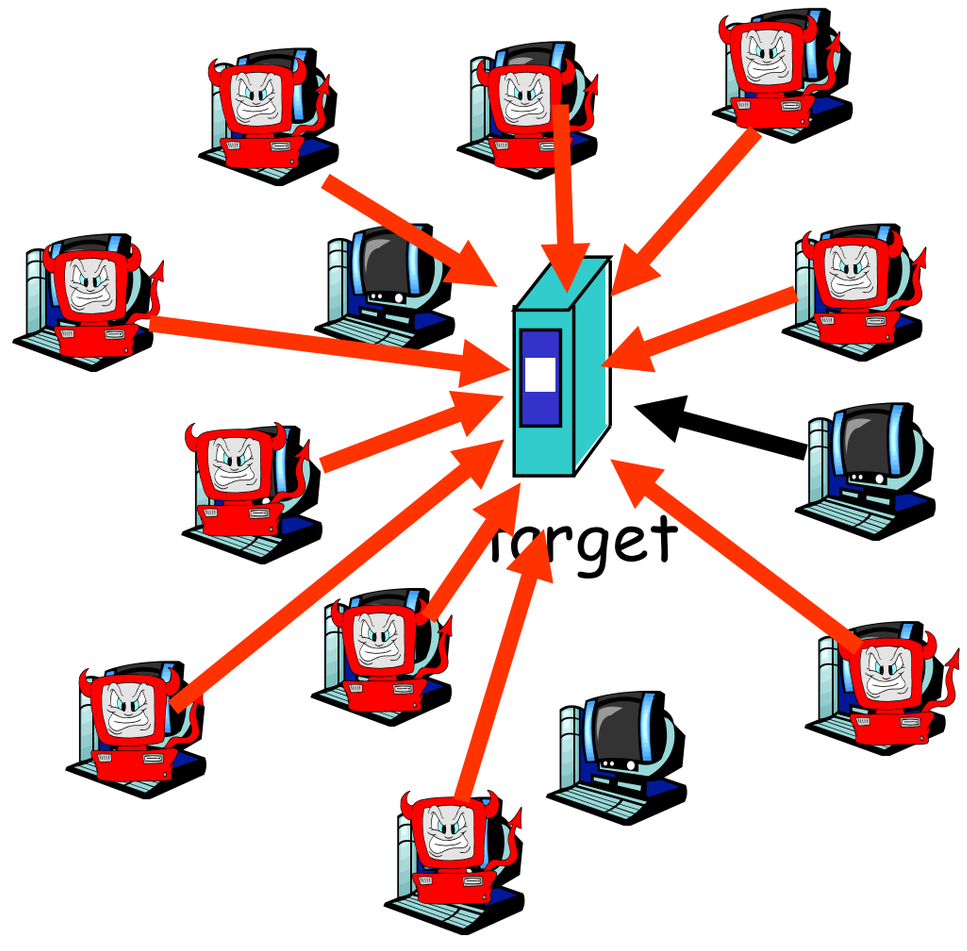
Sapphire Worm: aggregate scans/sec in first 5 minutes of outbreak (CAIDA, UWisc data)



Denial of Service Attacks

- attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

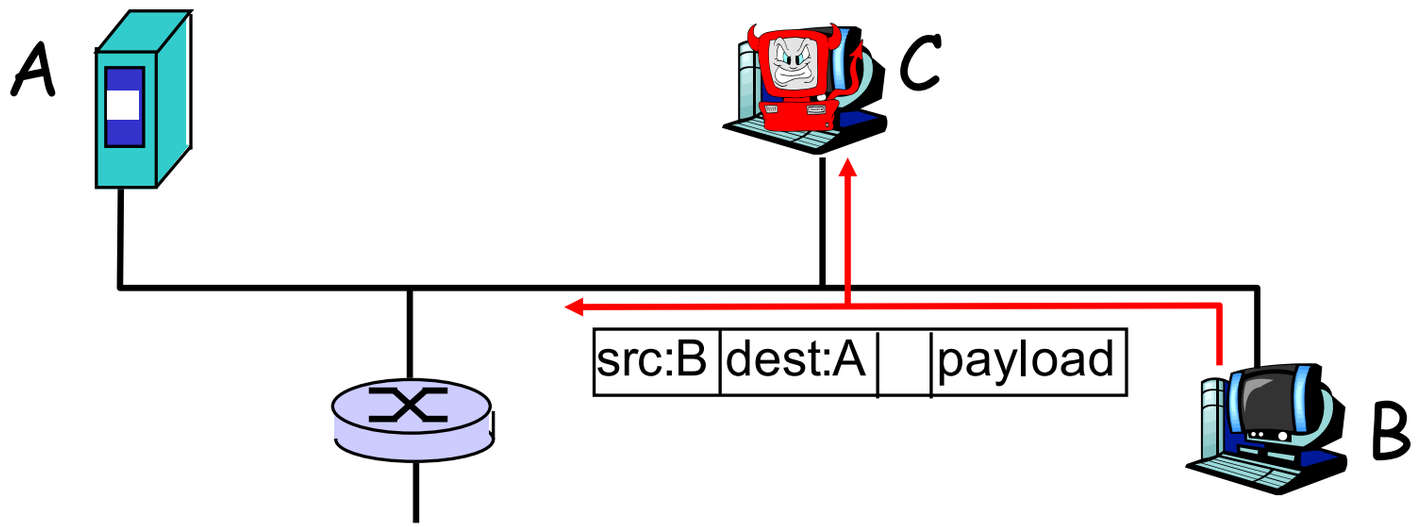
1. select target
2. break into hosts around the network (see malware)
3. send packets toward target from compromised hosts



Sniff, Modify, Delete Your Packets

Packet sniffing:

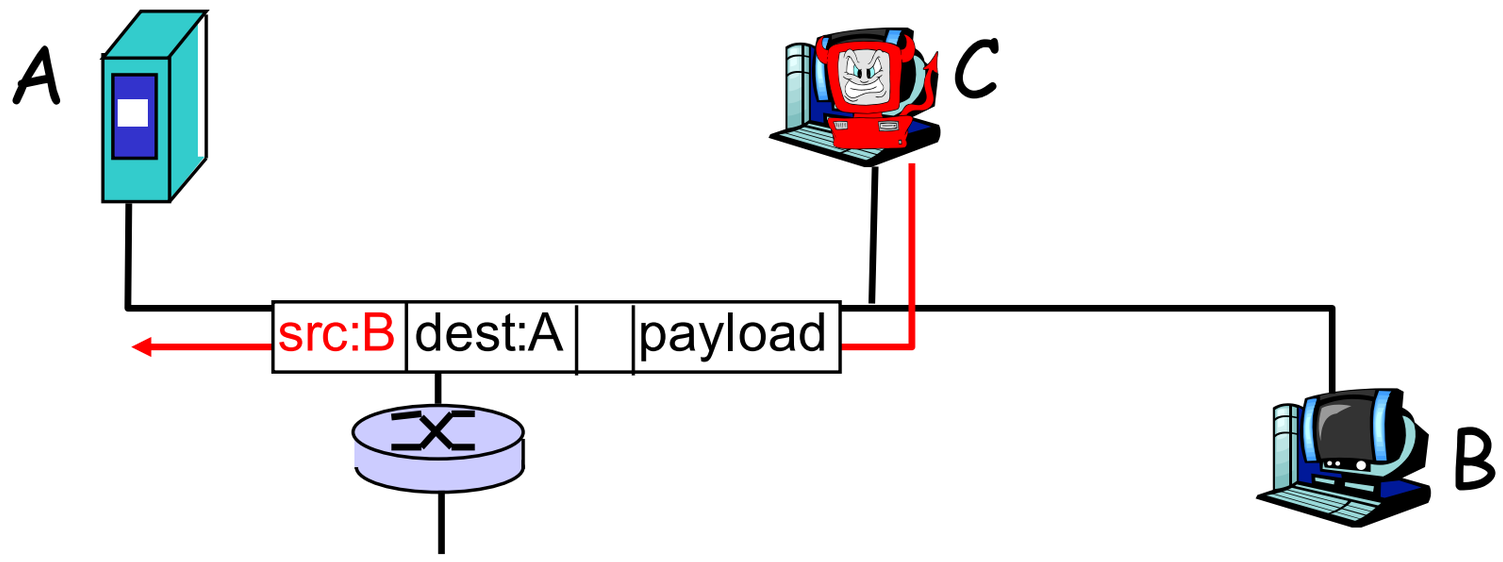
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- Wireshark used for end-of-chapter labs is a (free) packet-sniffer
- more on modification, deletion later

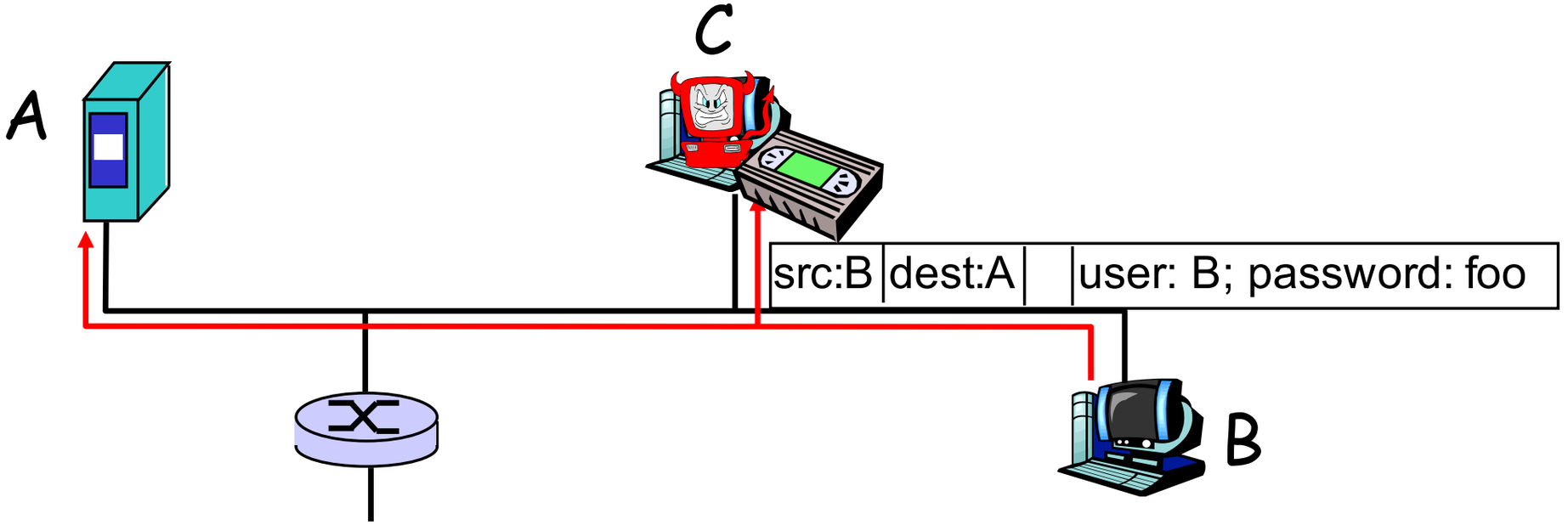
Masquerade as You

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



Masquerade as You

- *IP spoofing:* send packet with false source address
- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view



Masquerade as You

- *IP spoofing:* send packet with false source address
- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view