Chapter 1: Introduction

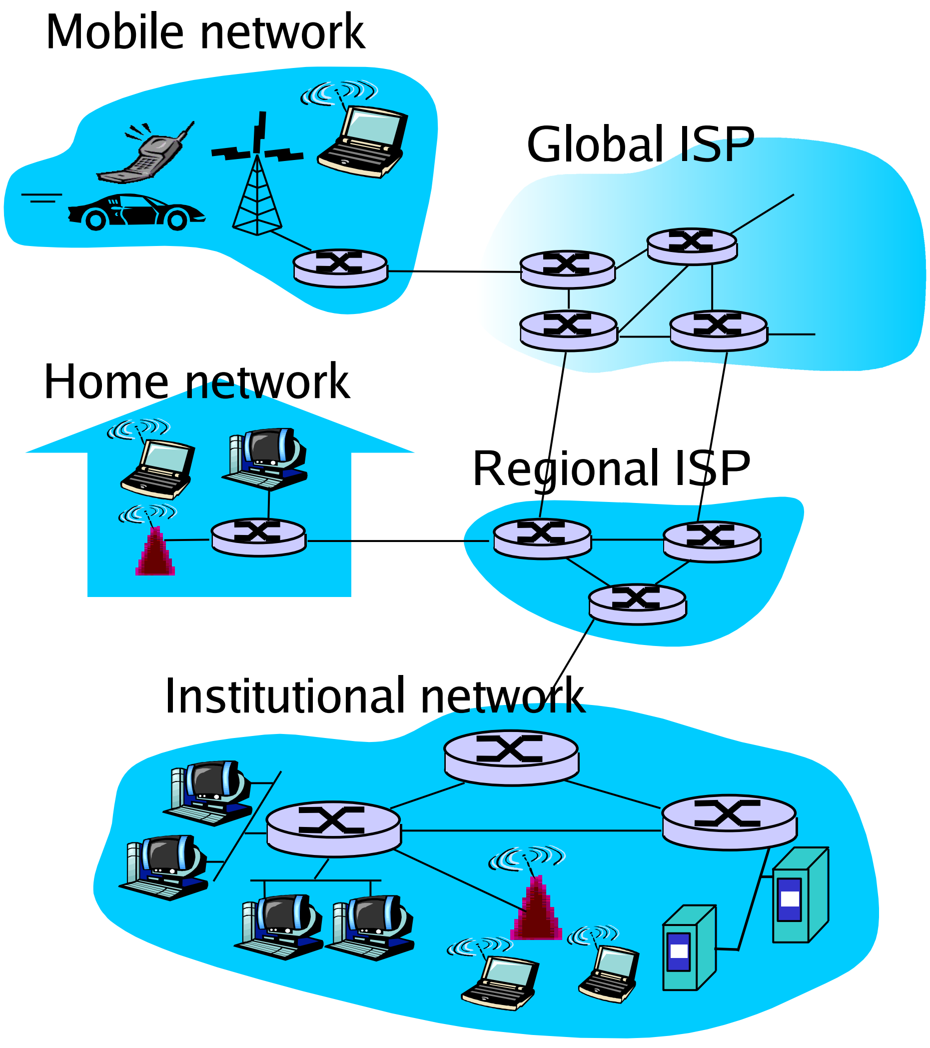
Overview:

- Internet components
- Network edge; hosts, access net, physical media
- Network core: packet/circuit switching, Internet structure
- Performance: loss, delay, throughput
- Protocol layers, service models
- Security

Internet Components

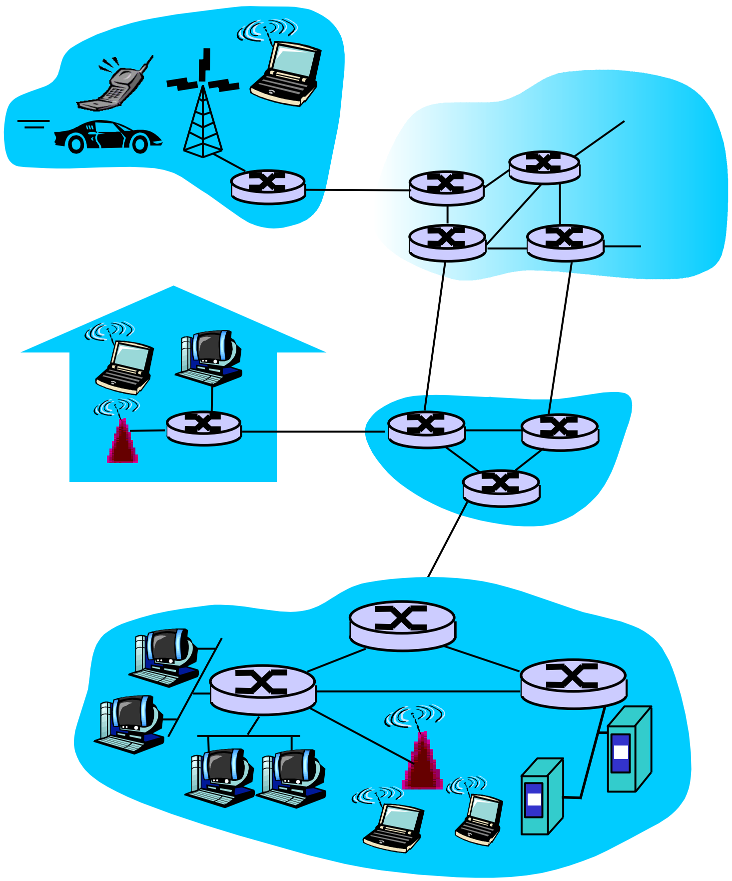
"network of networks"

- Hosts/End systems
- Communication links
  - Physical media
  - Transmission rate/ Bandwidth
- Routers
- Protocols : Timing and format of message exchange
- RFCs: Internet standards



Internet Service

- Communication infrastructure enables distributed applications:
  - Web, VoIP, email, games, e-commerce, file sharing
- Communication services provided to apps:
  - Reliable data delivery
  - “best effort” (unreliable) data delivery



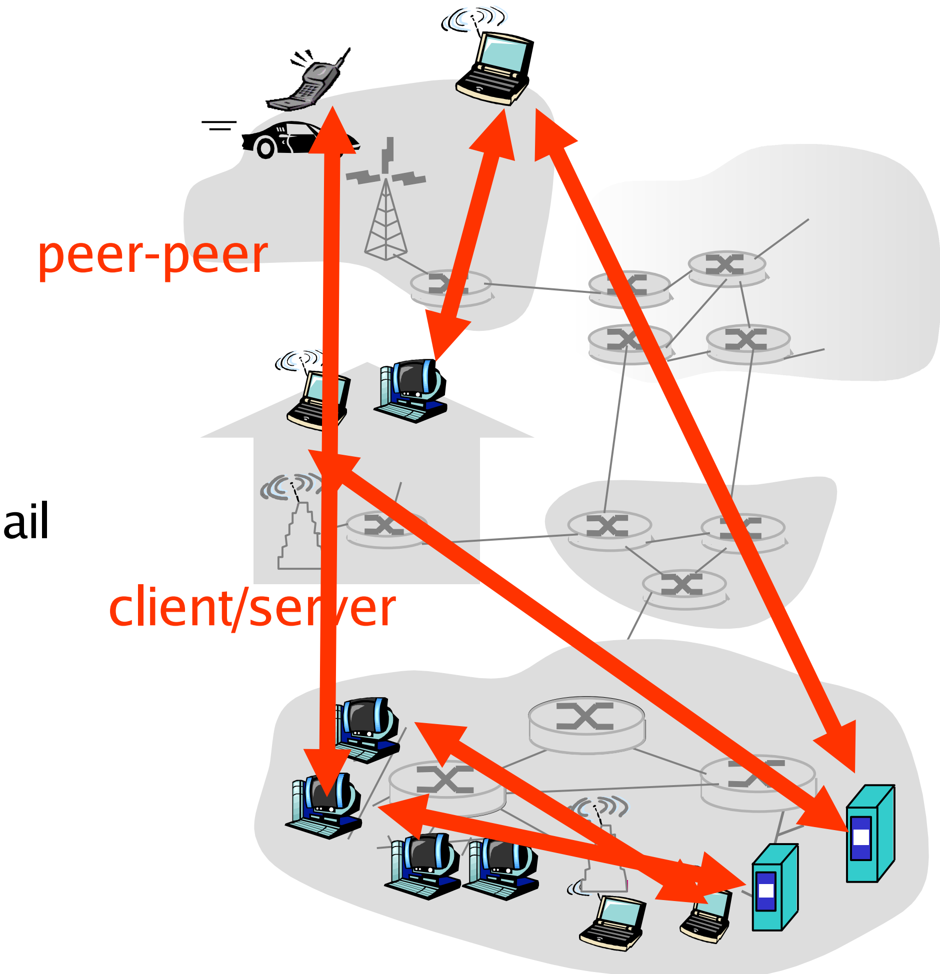
The Network Edge

- End systems (hosts):
  - Run application programs

    e.g. Web, email
- Client/Server model:

    e.g. Web browser/server; email client/server
- Peer-peer model:
  - Minimal (or no) use of dedicated servers

    e.g. Skype, BitTorrent



Reliable Data Transfer Service

- Handshaking: Setup the connection ahead of time
- **TCP - Transmission Control Protocol**
  - Internet's reliable data transfer service

TCP service [RFC 793]

- **Reliable, in-order byte-stream** data transfer
  - Packet loss: **acknowledgements** and **retransmissions**
- **Flow control**:
  - Ensures that a sender does not overwhelm a receiver
- **Congestion control**:
  - Senders "reduce the sending rate" when network is congested

Apps using TCP: HTTP, FTP, Telnet, SMTP

Best effort (unreliable) Data Transfer service

- UDP - User Datagram Protocol [RFC 768]:
  - Connectionless
  - Unreliable data transfer
  - No flow control
  - No congestion control

Apps using UDP:

- Streaming media, Teleconferencing, DNS, Internet telephony

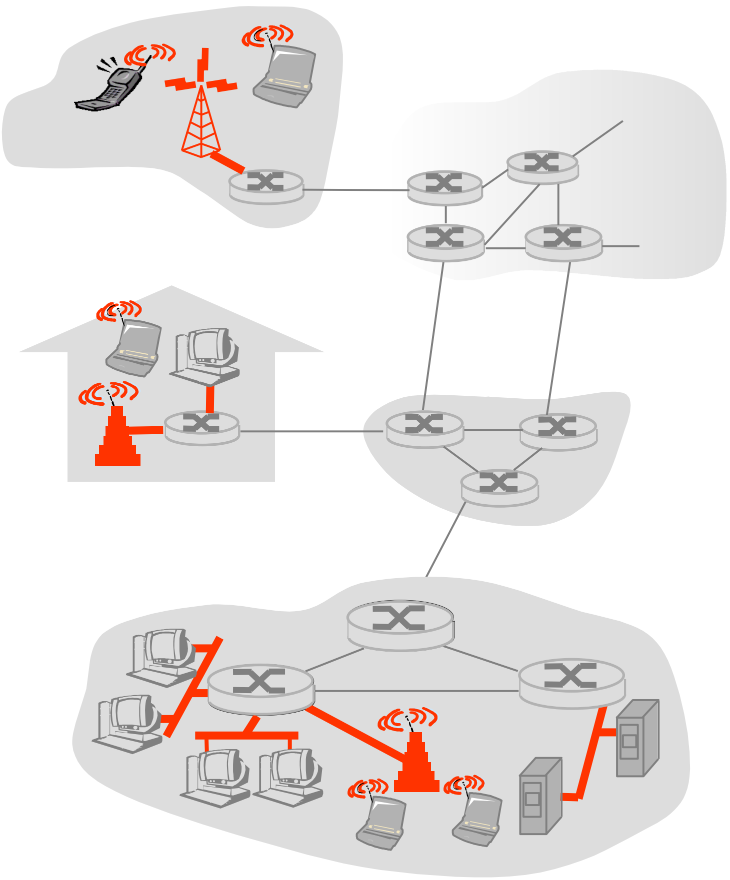
Access Networks and Physical Media

Q: How to connect end systems to edge routers?

- Residential access nets
- Institutional access networks (school, company)
- Mobile access networks

Key Issues:

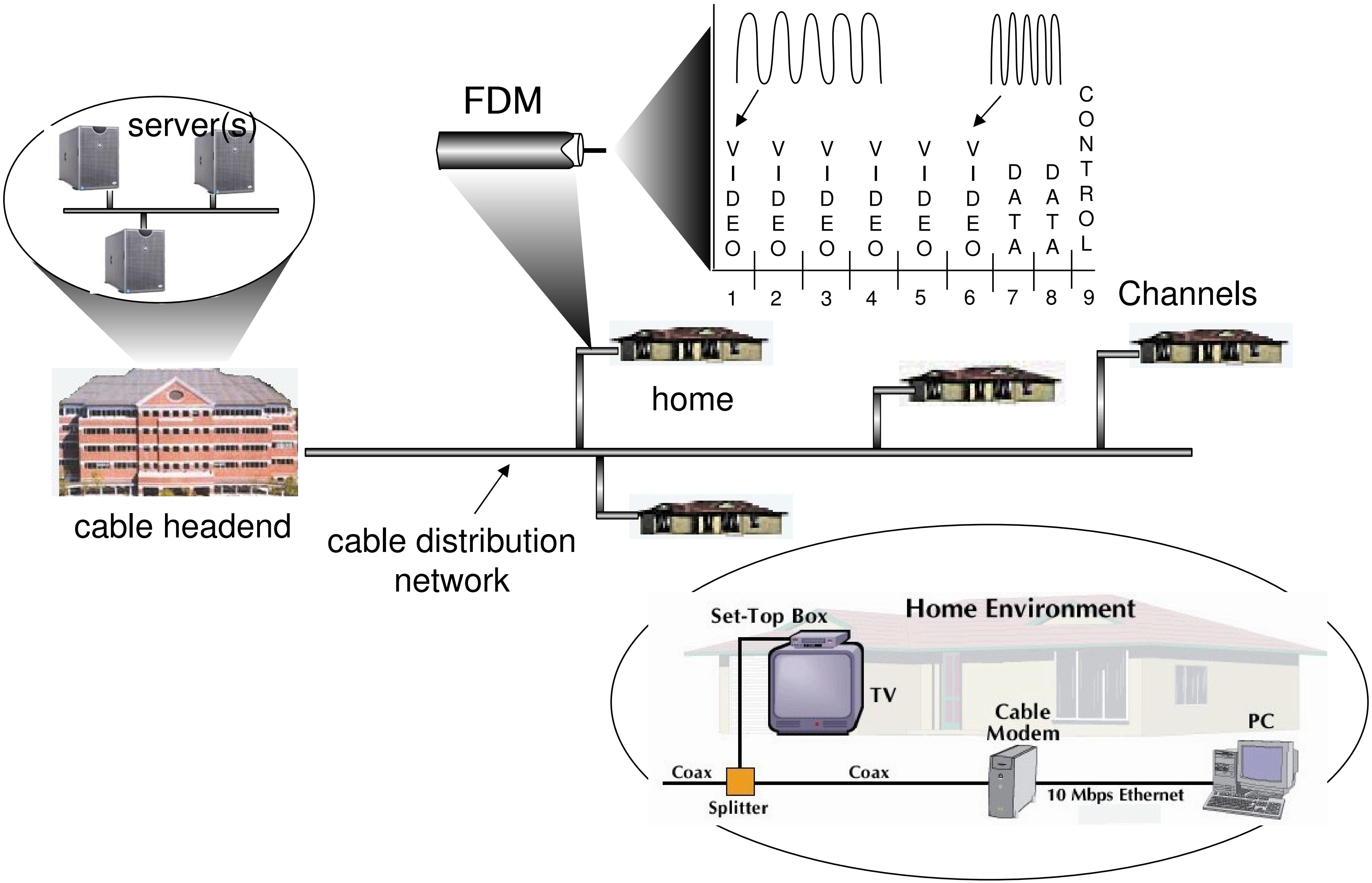
- Bandwidth (bits per second) of access network?
- Shared or dedicated?



Access Networks - Residential Access

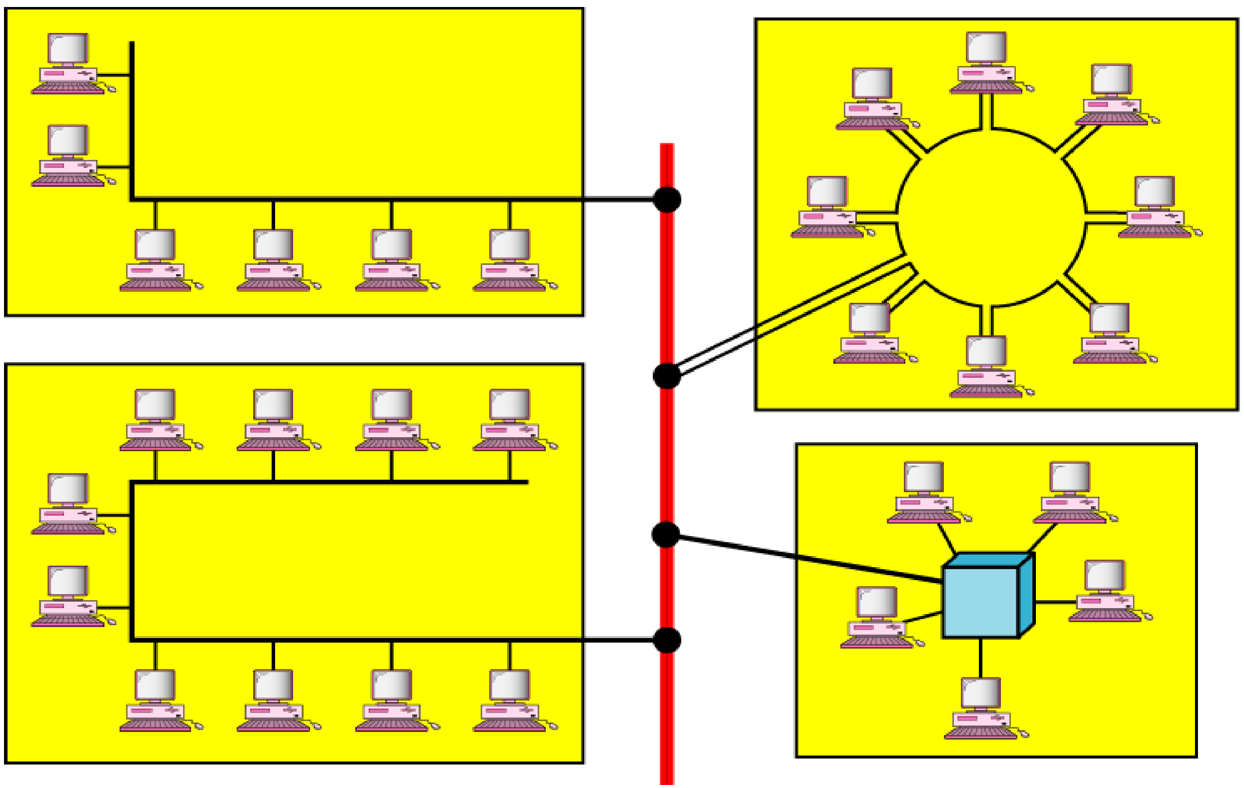
- Dialup via modem
  - Up to 56Kbps direct access to router (often less)
  - Can't surf and phone at same time
- DSL: Digital Subscriber Line
  - Deployment: telephone company (typically)
  - Up to 1 Mbps upstream (today typically < 256 kbps)
  - Up to 8 Mbps downstream (today typically < 1 Mbps)
  - 3 nonoverlapping frequency bands
  - Dedicated physical line to telephone central office
- HFC: Hybrid Fiber Coax
  - Deployment: available via cable TV companies
  - Up to 30Mbps downstream, 2 Mbps upstream
  - Network of cable and fiber attaches homes to ISP router
  - Homes share access to router

Cable Network Architecture: Overview



Company access: Local Area Networks

- Ethernet:
  - 10 Mbs, 100Mbps, 1Gbps, 10Gbps Ethernet
  - Modern configuration: end systems connect into *Ethernet switch*



Wireless Access Networks

- Shared *wireless* access network connects end system to router
  - via a Base Station aka "Access Point (AP)"

- Wireless LANs:

  802.11b/g (WiFi): 11 or 54 Mbps
- Wider-area wireless access
  - provided by telco operator
  - ~1Mbps over cellular system (EVDO (Evolution, Data Only), HSDPA (High-Speed Downlink Packet Access))
  - next up (?): WiMAX (10's Mbps) over wide area

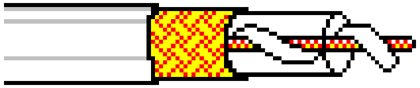
Physical Media - Guided

Twisted Pair (TP)

- Two insulated copper wires

Coaxial Cable

- Two concentric copper conductors
- Bidirectional



Fiber Optic Cable

- Glass fiber carrying light pulses, each pulse a bit
- High-speed operation: e.g., 10’s-100’s Gps
- Low error rate: repeaters spaced far apart; immune to electromagnetic noise

Physical media - Unguided

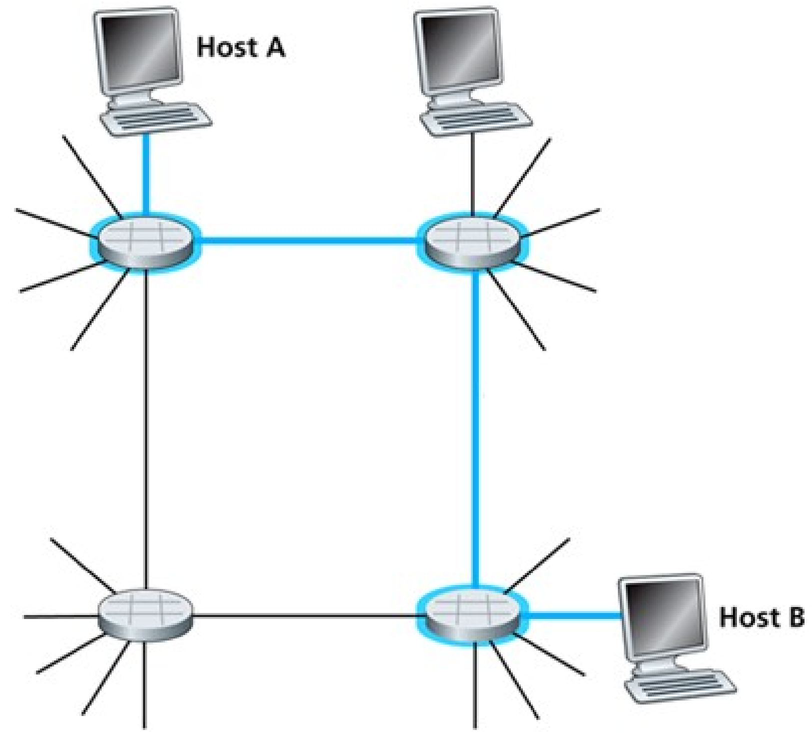
Radio

- Signal carried in electromagnetic spectrum
- Propagation environment effects:
  - Fading
  - Obstruction and absorption by objects
  - Interference from external sources

Radio link types:

- Terrestrial microwave: up to 45 Mbps channels
- LAN (e.g., Wifi): 11Mbps, 54 Mbps
- Wide-area (e.g., cellular): 3G cellular: ~ 1 Mbps
- Satellite
  - Kbps to 45Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - Geosynchronous versus low altitude

Network Core: Circuit Switching



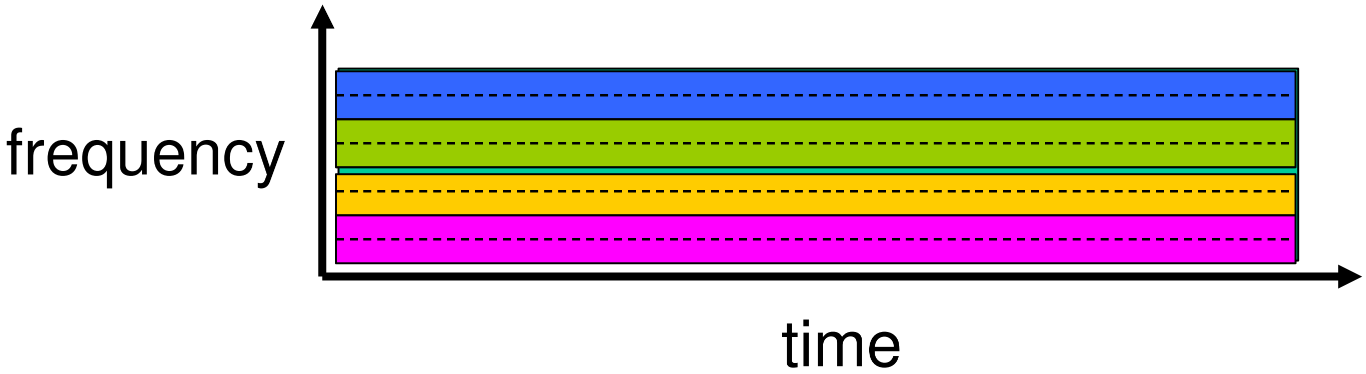
- End-to-End resources are reserved for "session"
- Dedicated resources: no sharing
- Guaranteed performance
- Call setup required
- Network resources (e.g., bandwidth) divided into "segments"
- Segments are allocated to individual sessions
- Resource segment is *idle* if not used by owning session *(no sharing)*

Circuit Switching: FDM and TDM

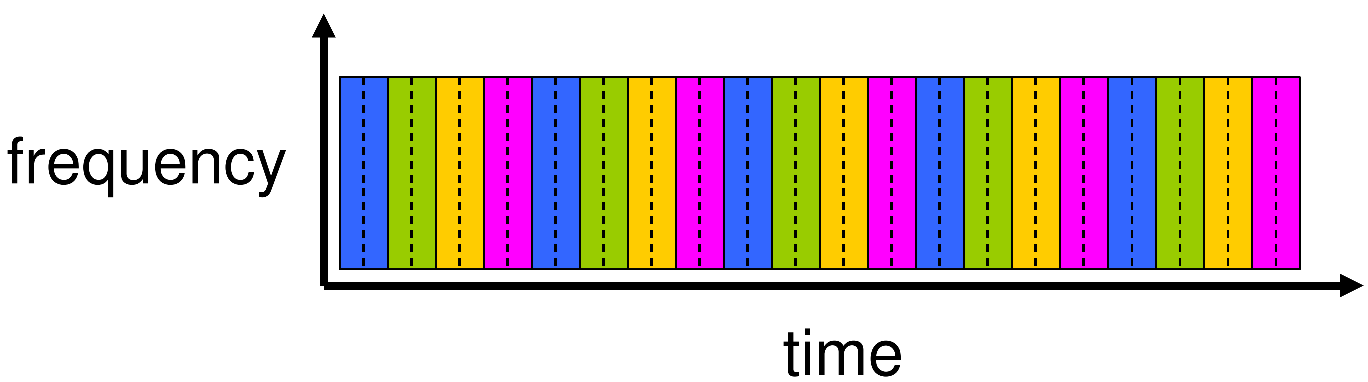
- Dividing link bandwidth into “segments”

FDM

Example: 4 users



TDM



Numerical example

- 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

$$T_{file} = 24 \text{ slots} \times \frac{1 \text{ sec}}{1.536 \times 10^6 \text{ bits}} \times 640000 \text{ bits} + 5 \text{ ms} = 10.5 \text{ sec}$$

Network Core: Packet Switching

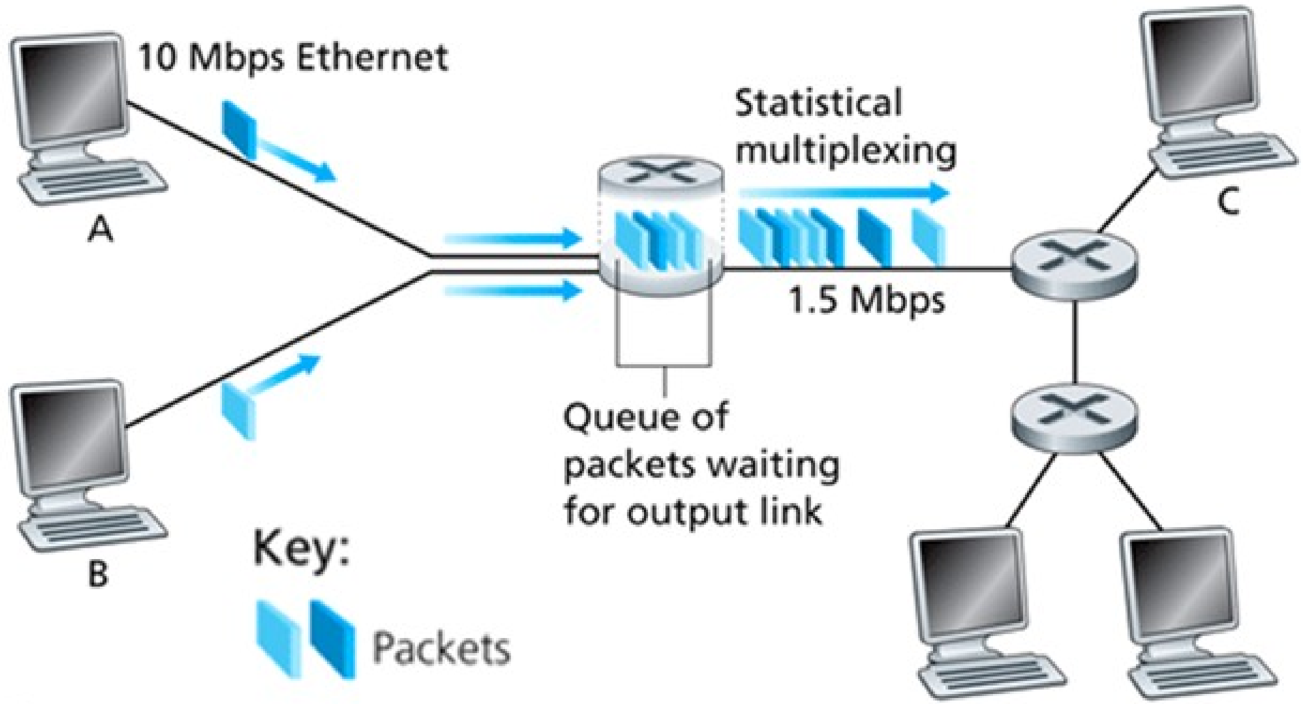
Each end-end data stream divided into **packets**

- Packets *share* network resources
- Each packet uses the full link bandwidth
- Resources are used *as required*

Resource contention:

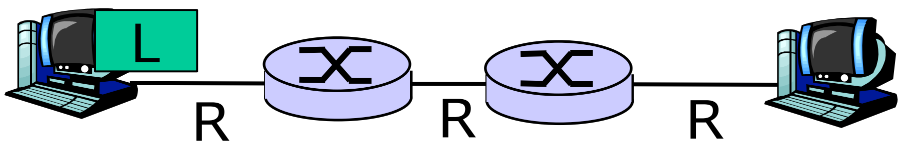
- Aggregate resource demand can exceed amount available
- Congestion: packets queue, wait for link use
- Store and forward: packets move one hop at a time

Packet Switching: Statistical Multiplexing



- Sequence of A & B packets does not have fixed pattern, bandwidth shared on demand
  - ➨ ***statistical multiplexing***.
- TDM: each host gets same slot in revolving TDM frame.

Packet-switching: store-and-forward



- Takes L/R seconds to transmit (push out) packet of L bits on to link at R bps
- *Store and forward:* entire packet must arrive at router before it can be transmitted on next link
- Delay = **3L/R** (assuming zero propagation delay)

  … more on delay shortly …

Example: L = 7.5 Mbits, R = 1.5 Mbps

Transmission delay
3 * 7.5/1.5 = 15 sec

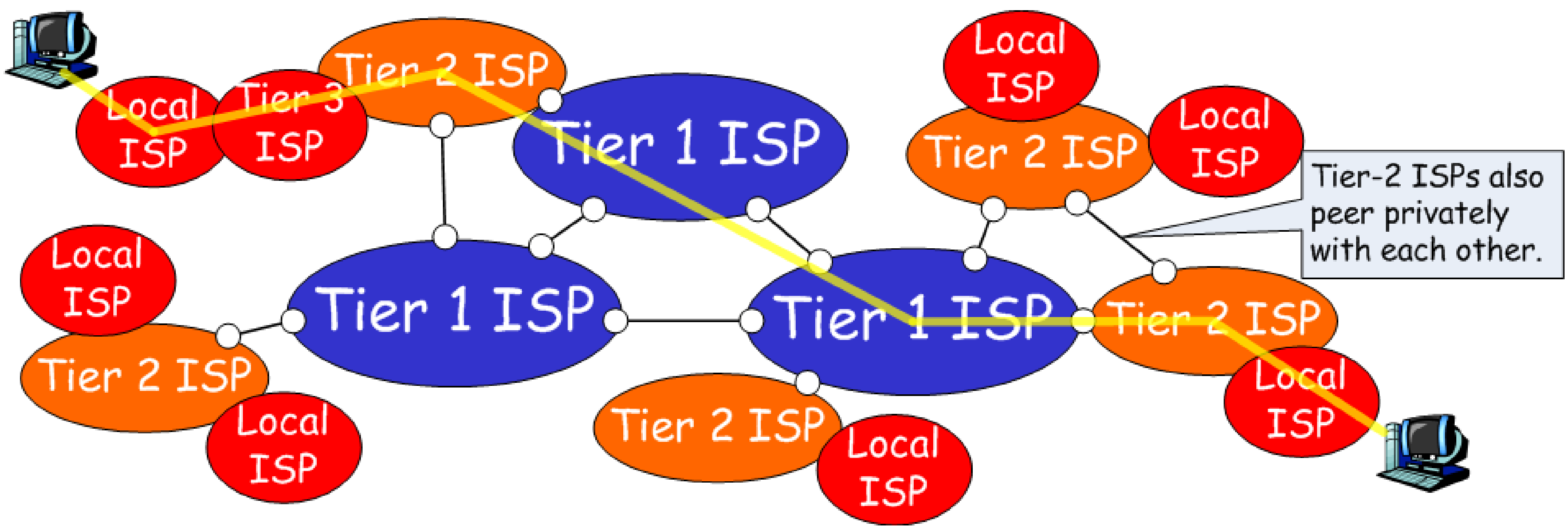
Packet Switching vs Circuit Switching

Is packet switching better?”

- Great for **bursty data**
  - Resource sharing => *more users to use network*
  - Simpler, no call setup
- Excessive congestion: packet delay and loss
  - Protocols needed for reliable data transfer, congestion control
- Q: How to provide circuit-like behavior?
  - Bandwidth guarantees needed for audio/video apps
  - still an unsolved problem (chapter 7)

Internet structure: network of networks

- **"Tier-1" ISPs: National/international coverage**
  e.g., Verizon, Sprint, AT&T, Cable and Wireless
- **"Tier-2" ISPs:** smaller (often **regional**) ISPs
  - Tier-2 ISP is *customer* of tier-1 provider
- **"Tier-3" ISPs and local ISPs**
  - Last hop ("access") network (closest to end systems)

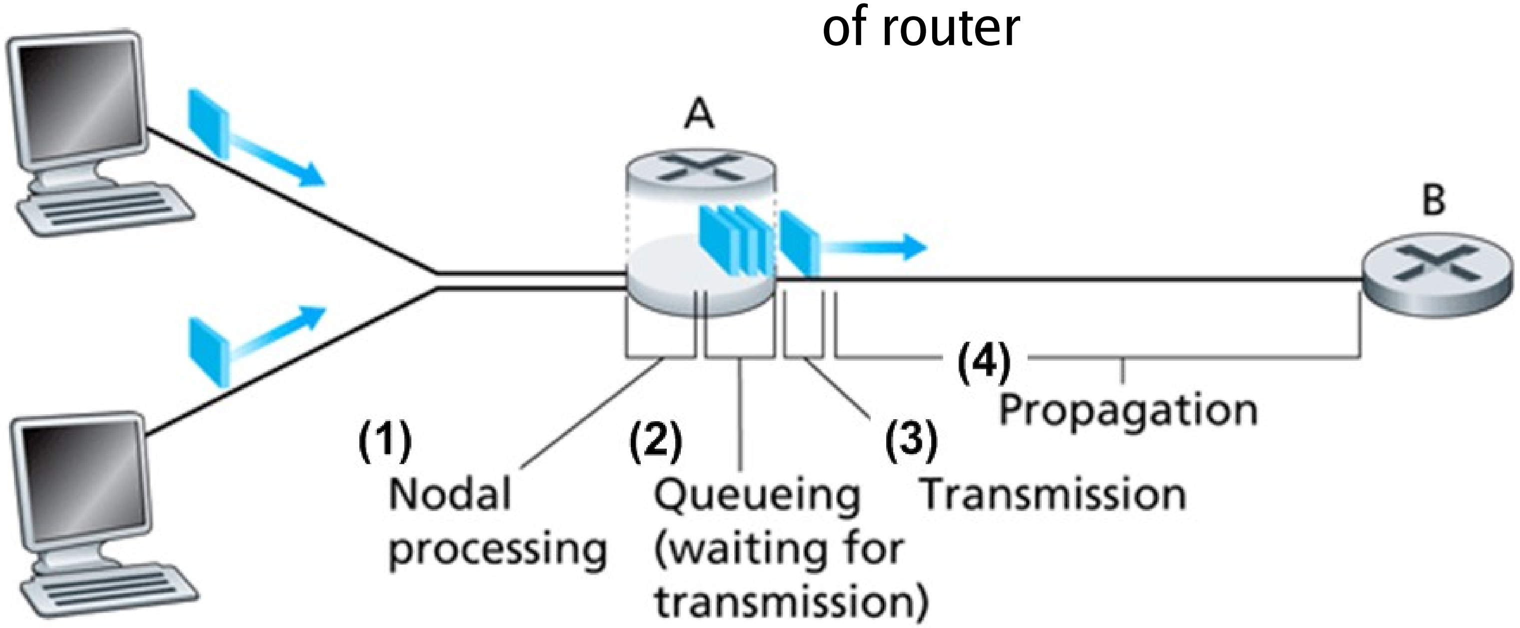


Four Sources of Packet Delay

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

1. Nodal processing delay
   - Examine the header to determine output link
   - Check bit errors

2. Queuing delay
   - Time waiting at output link for transmission
   - Depends on congestion level of router



Four Sources of Packet Delay

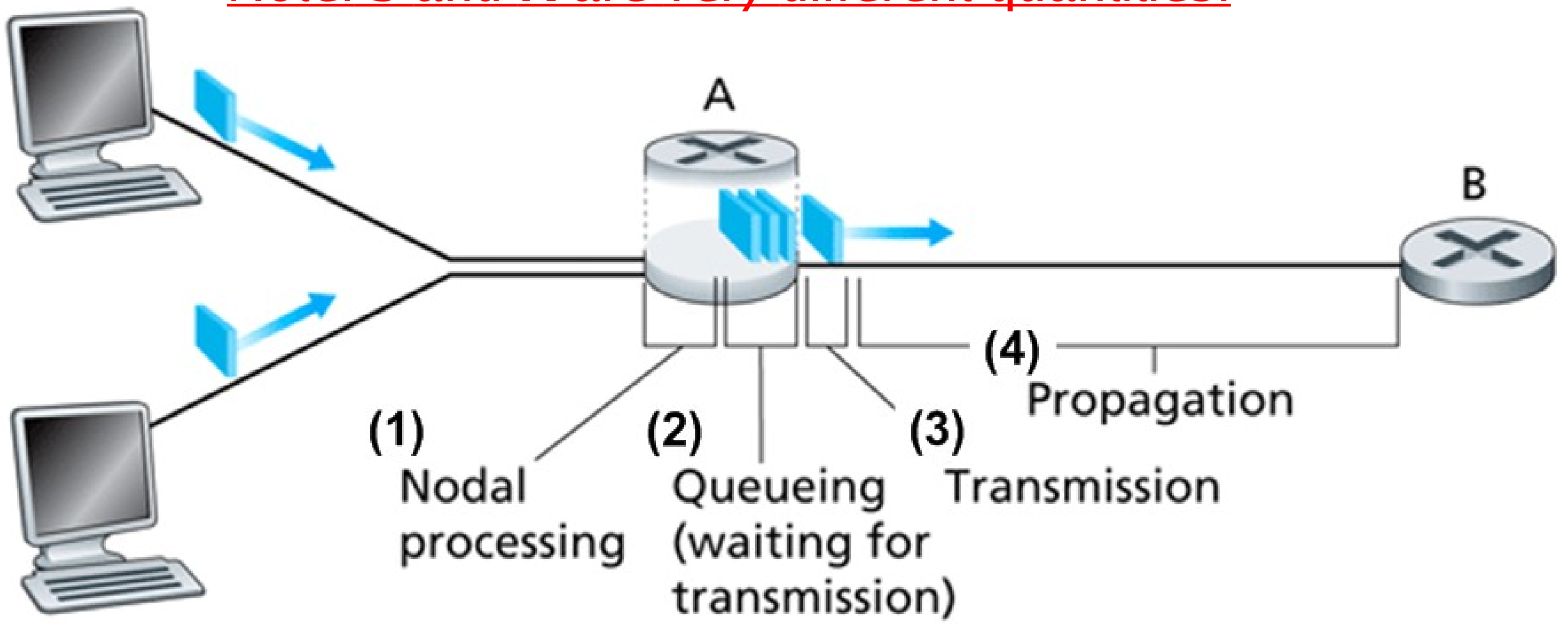
3. Transmission delay

- **R**=link bandwidth (bps)
- **L**=packet length (bits)
- Time to push bits onto link = **L/R**

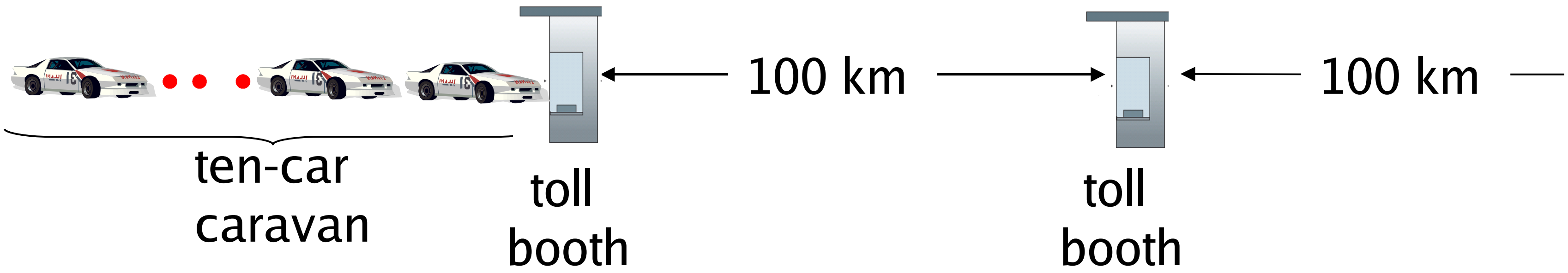
4. Propagation delay

- **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!

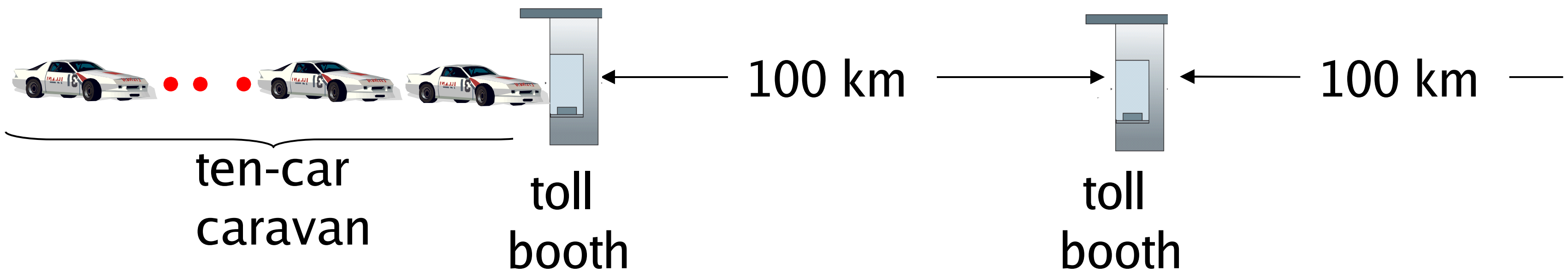


Caravan analogy



- Analogy:
  - car = bit;
  - caravan = packet;
  - toll booth = router;
- cars "propagate" at 100 km/hr
- toll booth takes 12 sec to service car (transmission time)
- Q: How long until caravan is lined up before 2nd toll booth?
- Time to "push" entire caravan through toll booth onto highway = 12*10 = 120 sec = 2 minutes
- Time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr = 60 minutes
- Ans: (60 + 2) = 62 minutes

Caravan analogy (more)



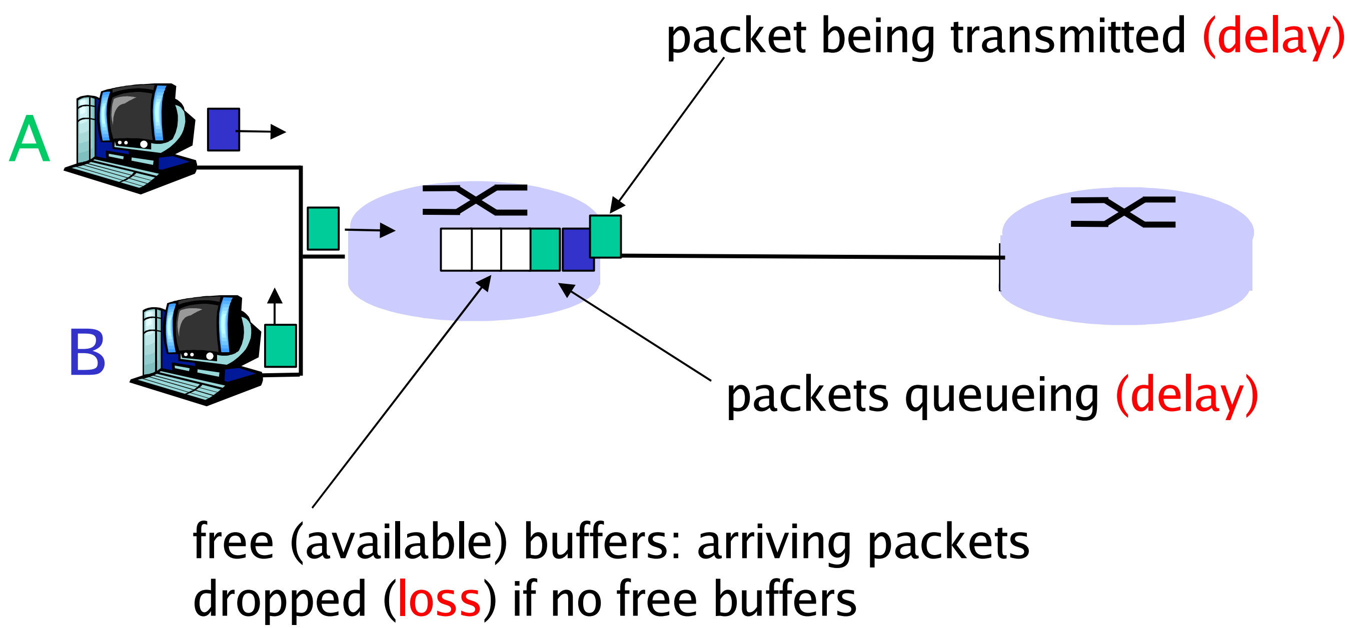
- Cars now "propagate" at 1000 km/hr
- Toll booth now takes 1 min to service a car

Q: Will cars arrive at 2nd booth before all cars serviced at 1st booth?

- Yes! After 7 min, 1st car is at 2nd booth and 3 cars still at 1st booth.
- 1st bit of packet can arrive at 2nd router before packet is fully transmitted at 1st router!

Packet Loss

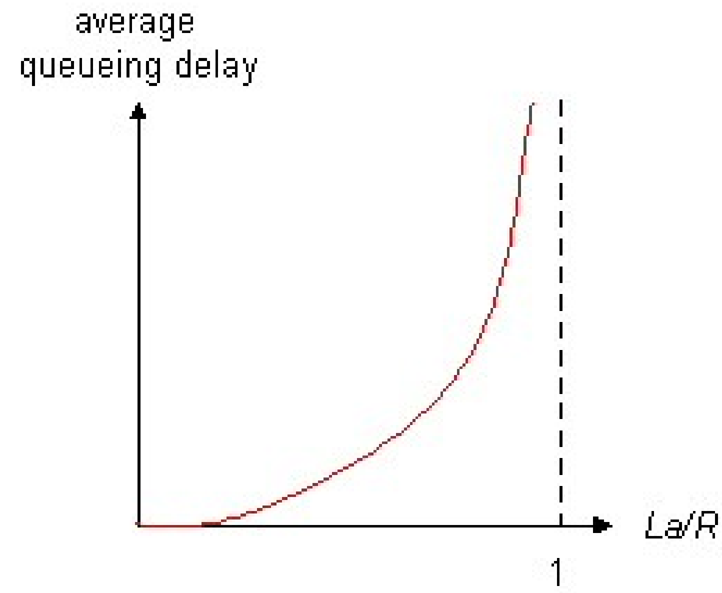
- Packets are ***queued*** in router buffers
- Buffer has finite capacity
- Packet arriving to full buffer is dropped
- Packet arrival rate to input link exceeds output link capacity



Queuing Delay

- **R** = Link bandwidth (bit/sec)
- **L** = Packet length (bits/packet)
- **a** = Average packet arrival rate (packet/sec) => **La** bits/sec

Traffic intensity = La/R

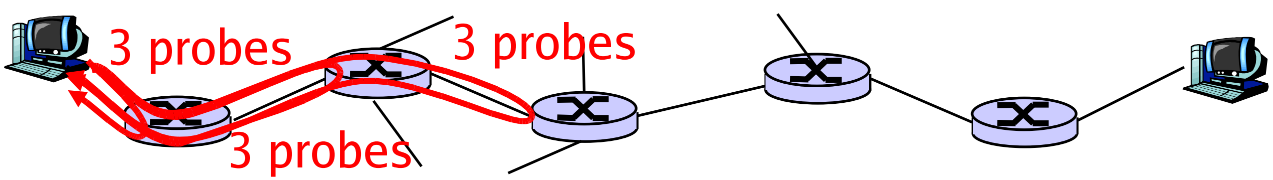


- La/R < 0: Average queueing delay small
- La/R ≥ 1: Delays become large
- La/R > 1: More "work" arriving than can be serviced, average delay infinite!

"Real" Internet Delays and Routes

Traceroute program:

- Provides delay measurement from source to router along end-end Internet path towards destination.
- For all *i*:
  - Sends three packets that will reach router *i* on path towards destination
  - Router *i* will return packets to sender
  - Sender times interval between transmission and reply.



Traceroute

> traceroute www.eurecom.fr

Three delay measurements from the source

1 cs-gw (128.119.240.254) 1 ms 1 ms 2 ms

2 border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145) 1 ms 1 ms 2 ms

3 cht-vbns.gw.umass.edu (128.119.3.130) 6 ms 5 ms 5 ms

4 jn1-at1-0-0-19.wor.vbns.net (204.147.132.129) 16 ms 11 ms 13 ms

5 jn1-so7-0-0-0.wae.vbns.net (204.147.136.136) 21 ms 18 ms 18 ms

trans-oceanic link

6 abilene-vbns.abilene.ucaid.edu (198.32.11.9) 22 ms 18 ms 22 ms

7 nycm-wash.abilene.ucaid.edu (198.32.8.46) 22 ms 22 ms 22 ms

8 62.40.103.253 (62.40.103.253) 104 ms 109 ms 106 ms

9 de2-1.de1.de.geant.net (62.40.96.129) 109 ms 102 ms 104 ms

10 de.fr1.fr.geant.net (62.40.96.50) 113 ms 121 ms 114 ms

11 renater-gw.fr1.fr.geant.net (62.40.103.54) 112 ms 114 ms 112 ms

12 nio-n2.cssi.renater.fr (193.51.206.13) 111 ms 114 ms 116 ms

13 nice.cssi.renater.fr (195.220.98.102) 123 ms 125 ms 124 ms

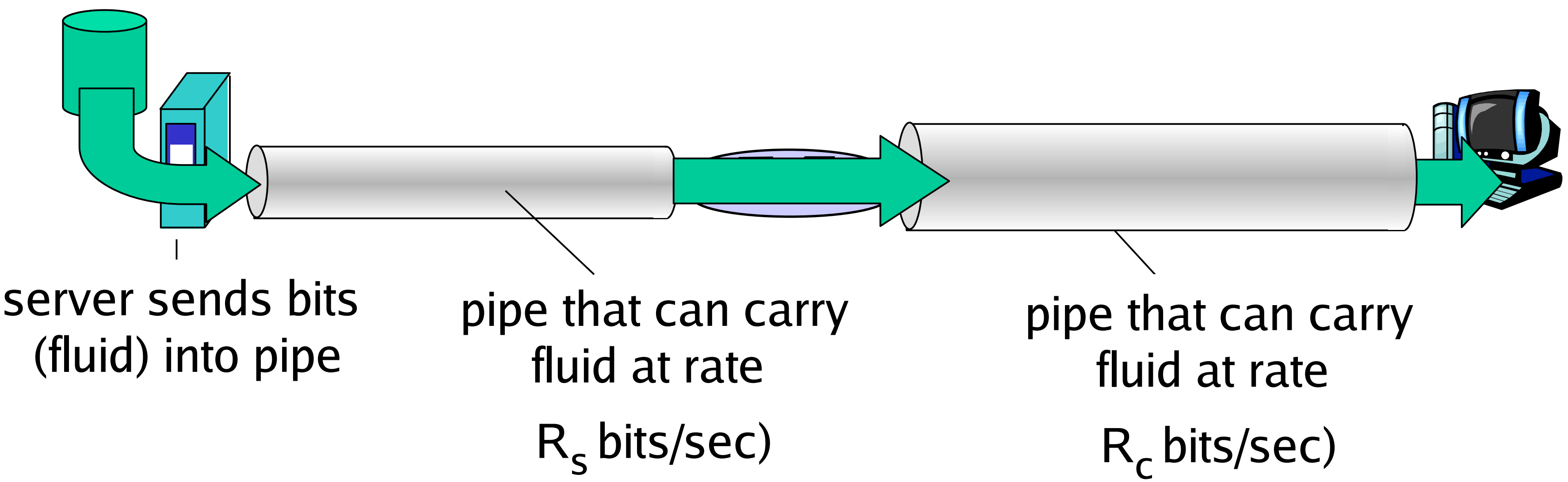
* means no response (probe lost, router not replying)

14 r3t2-nice.cssi.renater.fr (195.220.98.110) 126 ms 126 ms 124 ms

15 eurecom-valbonne.r3t2.ft.net (193.48.50.54) 135 ms 128 ms 133 ms

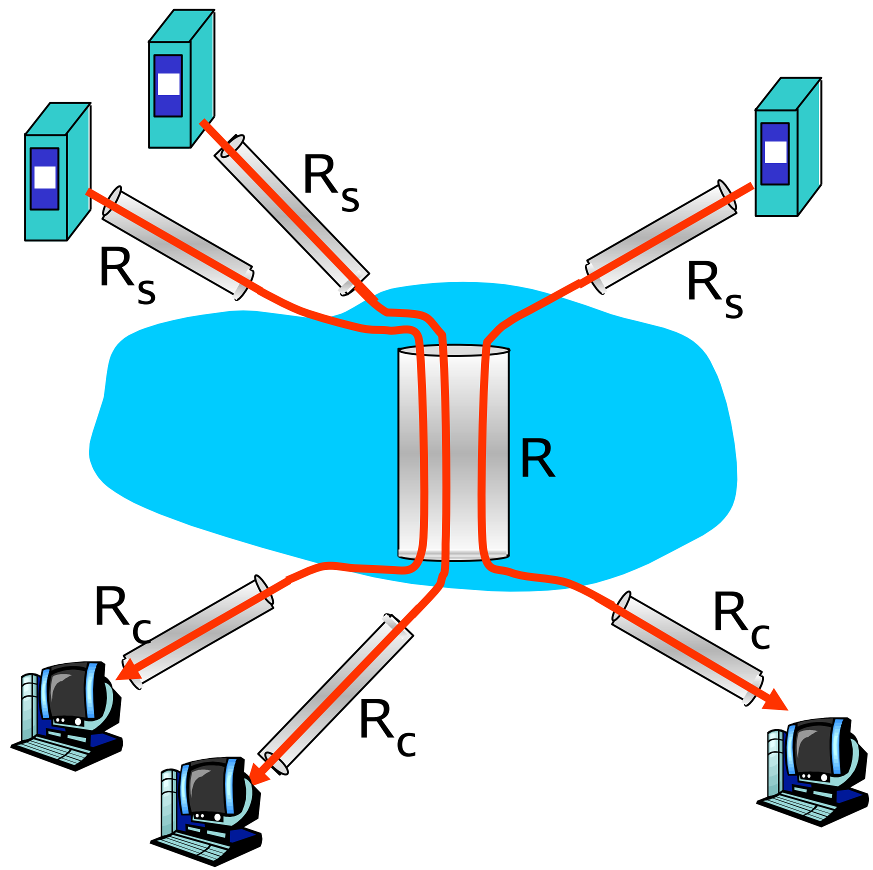
Throughput

- ***Throughput:*** rate (bits/time unit) at which bits transferred between sender/receiver
  - *instantaneous:* rate at given point in time
  - *average:* rate over long(er) period of time



Throughput: Internet scenario

- Per-connection end-end throughput: $\min(R_c,R_s,R/10)$
- In practice: R_c or R_s is often bottleneck



Connections (fairly) share backbone bottleneck link R bits/sec

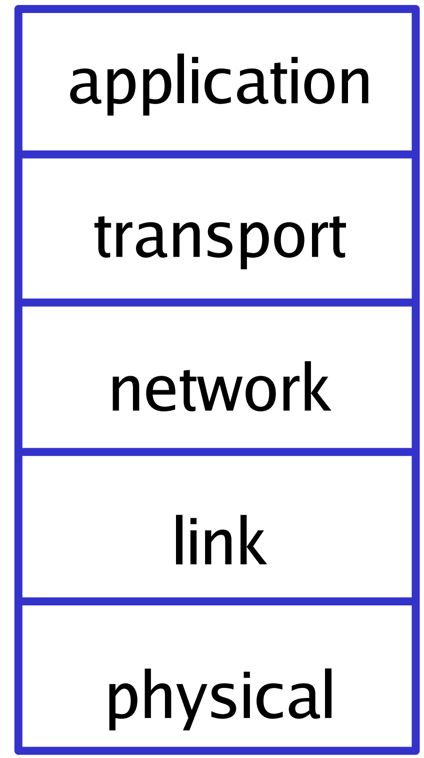
Protocol “Layers”- Why Layering?

Dealing with complex systems:

- Explicit structure allows identification, relationship of complex system’s pieces
- Eases maintenance, updating of system (Modularization)
  - Change of implementation of layer’s service transparent to rest of system
  - e.g., change in gate procedure doesn’t affect rest of system
- Allow different platforms to communicate (e.g., *NIX, Windows)

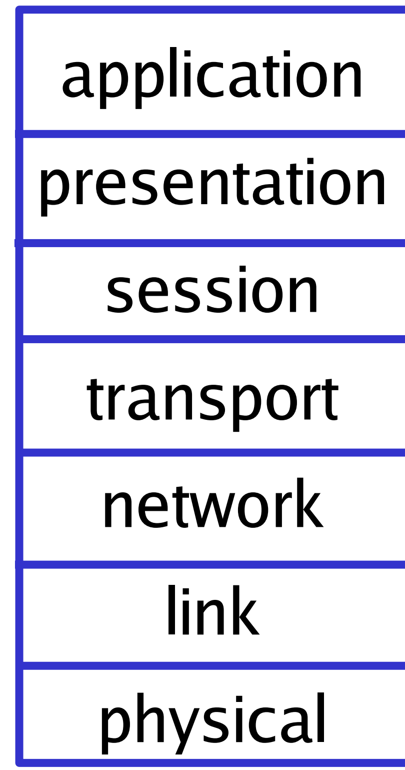
Internet Protocol Stack

- 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”

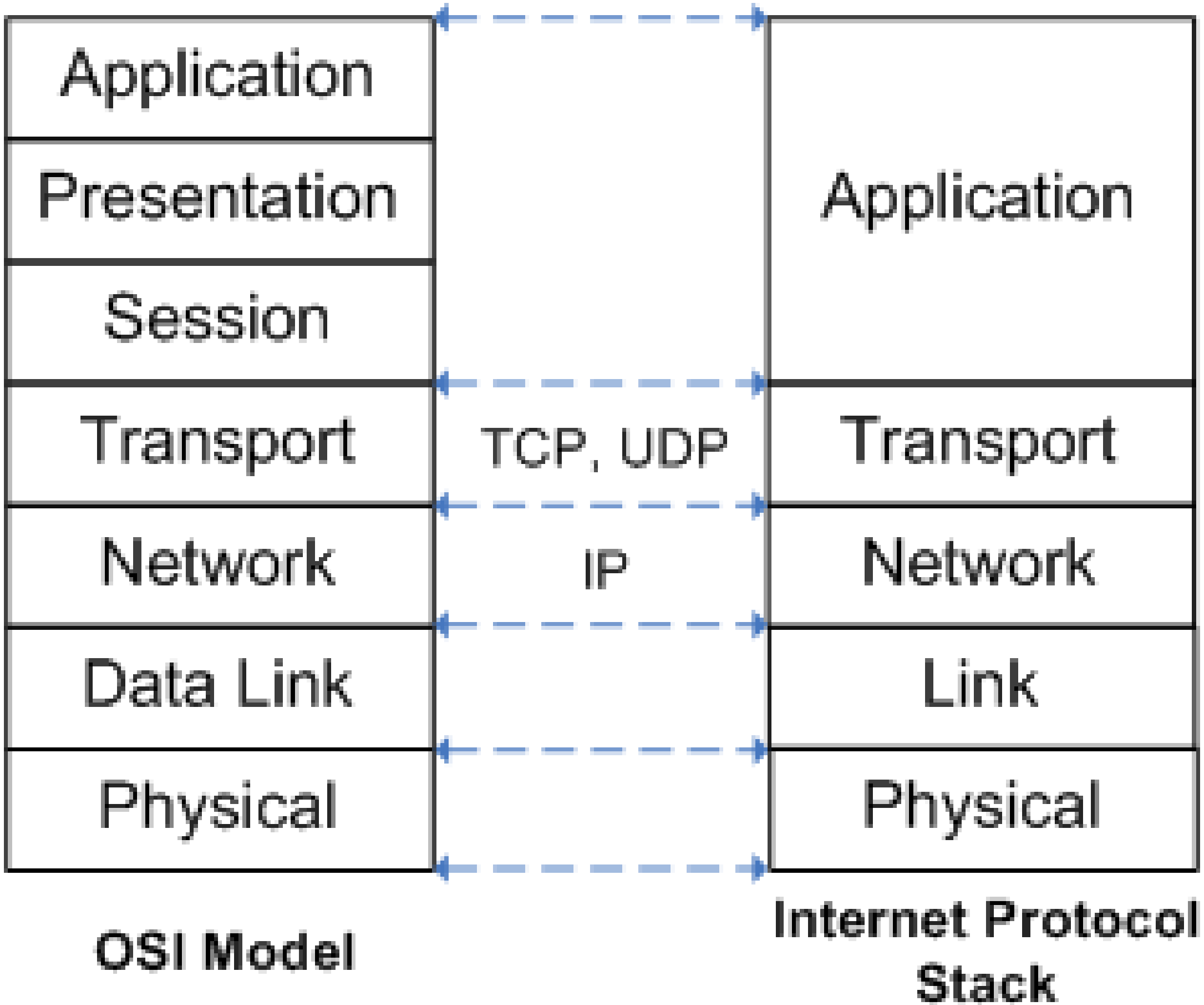


ISO/OSI Reference Model

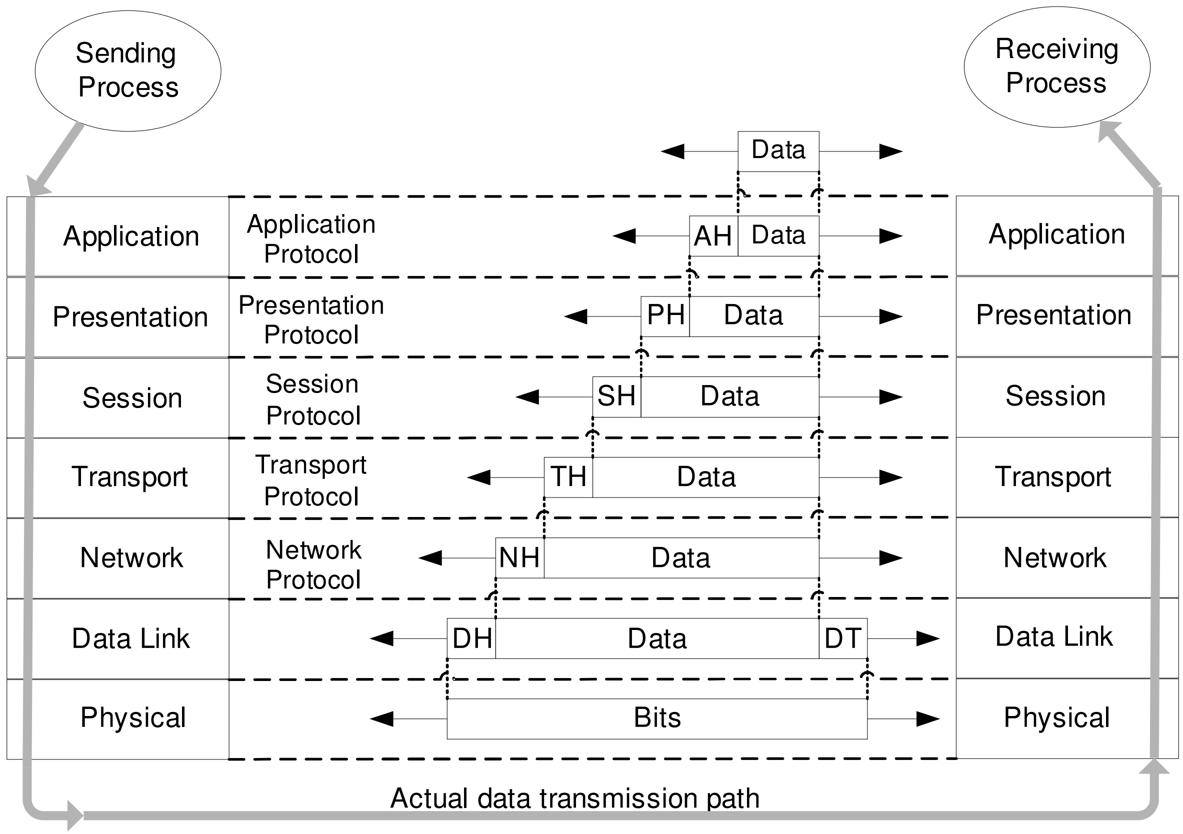
- Presentation: allow applications to interpret meaning of data,
  - e.g., encryption, compression, machine-specific conventions
- Session: synchronization, checkpointing, recovery of data exchange
- Internet stack "missing" these layers!
  - must be implemented in the application itself, *if needed*



Internet Protocol Stack and OSI



OSI Data Encapsulation



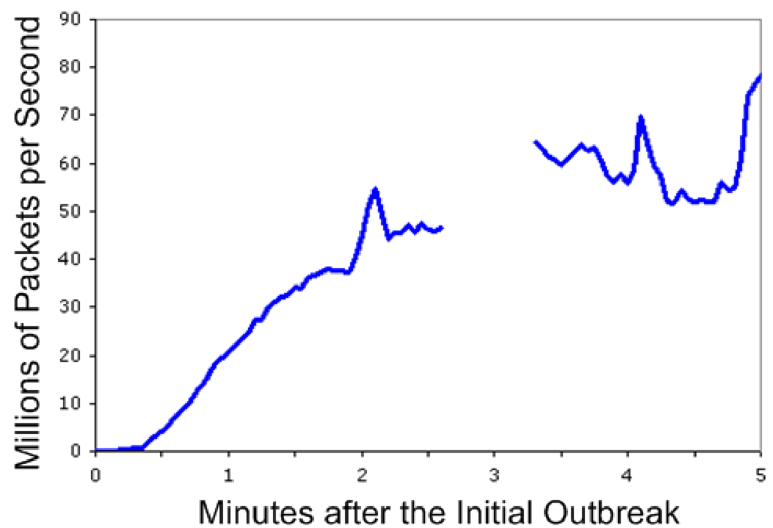
Network Security

- Attacks on Internet infrastructure:
  - Infecting/attacking hosts: malware, spyware, worms, unauthorized access (data stealing, compromise user accounts)
  - Denial of service: deny access to resources (take servers offline, usurp link bandwidth)
- Internet not originally designed with (much) security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network"
  - TCP/IP protocol suite designers playing "catch-up" vis-à-vis security
  - Security considerations permeate all layers.

Different Types of Attacks

- Spyware:
  - infection by downloading web page with spyware
  - records keystrokes, web sites visited, upload private info to a collection server
- Virus
  - infection by receiving object (e.g., e-mail attachment), actively executes malicious code
  - self-replicating: propagates 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)



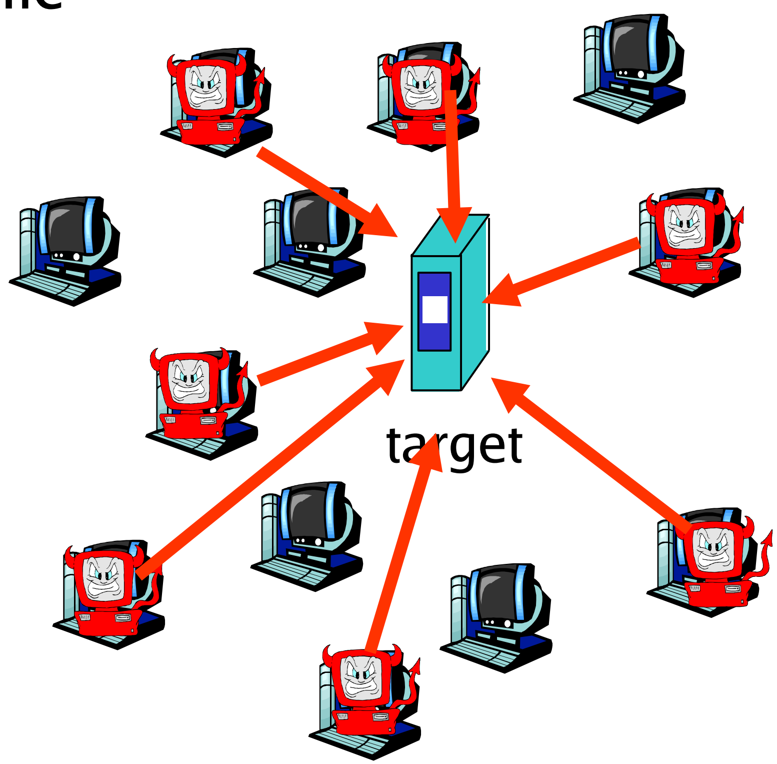
Distributed Denial of Service Attacks (DDOS)

- Attackers cause resources (server, bandwidth) to be unavailable to legitimate users by overwhelming resource with malicious traffic

1. Identify target network

1. Compromise hosts on the network

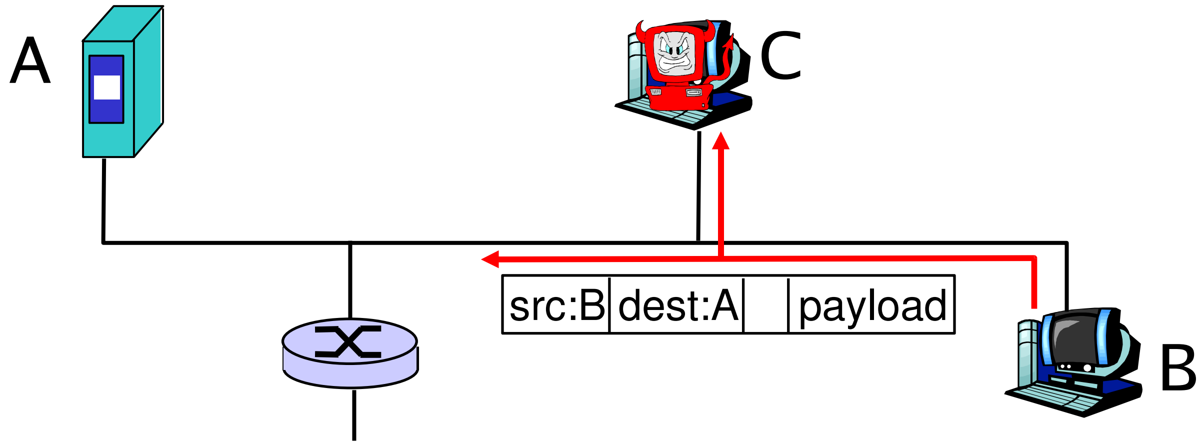
1. Send packets toward target from compromised hosts



Monitoring Network Traffic

Packet sniffing:

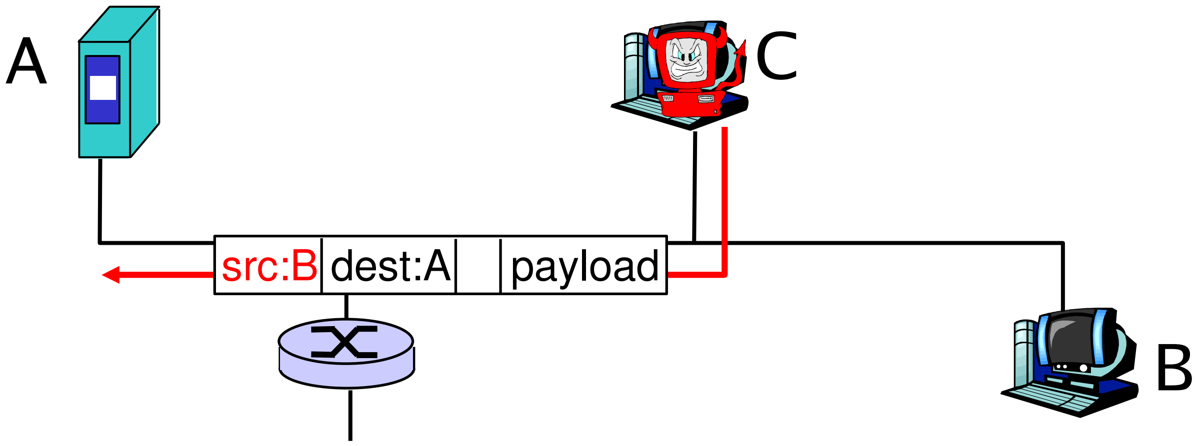
- Broadcast media (shared Ethernet, wireless)
- Promiscuous network interface reads/records all packets (e.g., including passwords) on the shared medium



Packet-sniffing software (**Wireshark**) can be used.

IP Masquerading

- **IP spoofing:** send packet with a source address other than the true sender IP address



IP Masquerading

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