# Chapter 1
Introduction

A note on the use of these Powerpoint slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

GLOBAL EDITION

Computer Networking
A Top-Down Approach

SEVENTH EDITION

Kurose • Ross
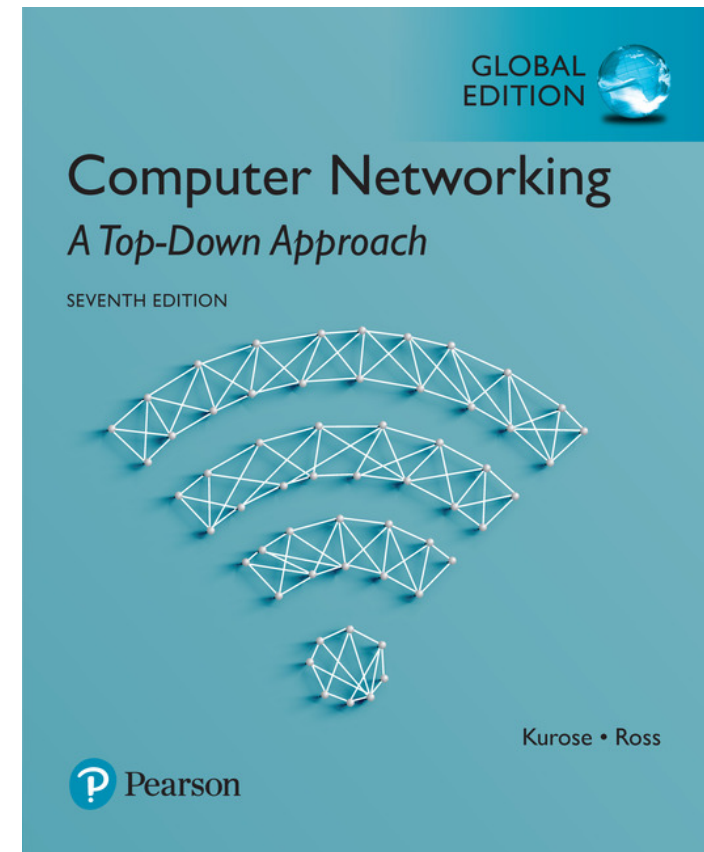
Pearson

Computer Networking: A Top Down Approach

7th Edition, Global Edition
Jim Kurose, Keith Ross
Pearson
April 2016

Q: Group the Similar Terms!

- Human
- Calculator
- Computer
- System
- Device
- Network
- Communication
- Information
- Data

Polly's Language IQ

❑ Entities

  ○ Human, Calculator, Computer, System, Device

❑ A group of associated entities

  ○ Network (of human, calculator, computer, system, device)

❑ Interaction/exchange over the group of associated entities

  ○ Communication [over the network (of human, calculator, computer, system, device)]

❑ Stuff to be interacted/exchanged over the group of associated entities

  ○ Information, Data {communicated [over the network (of human, calculator, computer, system, device)]

Think Human Network

We getting to know each other

Becoming connected!

Is it easy now to think…

What a computer network is?

A network of computers?

Yes and No

Computer Network

❑ **In a general sense**

  ❍ Yes, a network of computers

❑ **In a professional sense**

  ❍ Not exactly, it implies specifically the Internet

❑ **In other words,**

  ❍ You could define and create your own computer network (running non-Internet stuff)

  ❍ But it won't be THE computer network (the Internet)

The Objectives

❑ **In a long term**

- ○ To train students who could create their own computer (or whatever) network

❑ **In a short term (in this course)**

- ○ Let's start from the most popular example -- the Internet

Chapter 1: Introduction

Our goal:

- ❑ get context, overview, "feel" of networking
- ❑ more depth, detail *later* in course
- ❑ approach:
  - ○ descriptive
  - ○ use Internet as example

Overview:

- ❑ what's the Internet
- ❑ what's a protocol?
- ❑ network edge
- ❑ network core
- ❑ performance: loss, delay
- ❑ protocol layers, service models
- ❑ network under attack
- ❑ history

Chapter 1: roadmap

What's the Internet: "nuts and bolts" view

PC

server

wireless laptop

cellular handheld

access points

— wired links
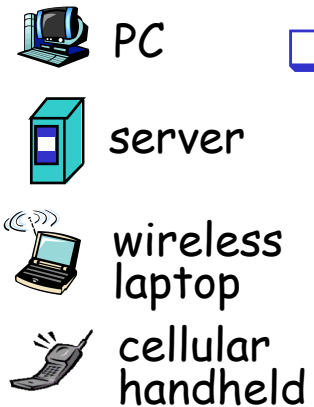
router

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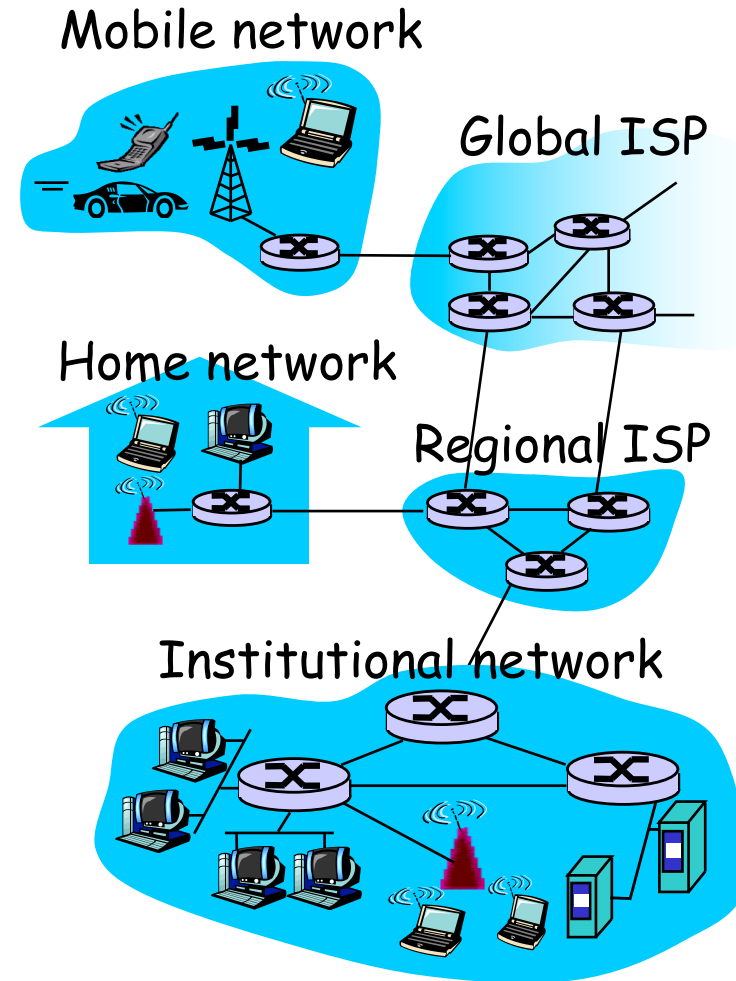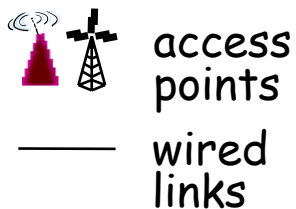 - ○ running *network apps*
- ❑ *communication links*
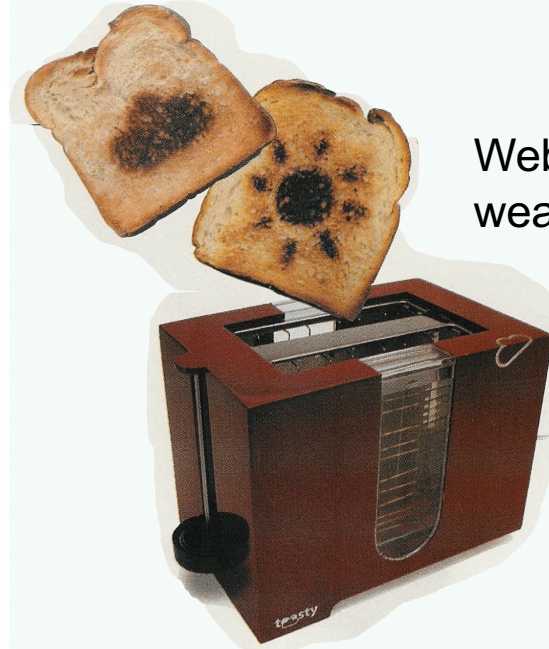 - ❖ fiber, copper, radio, satellite
  - ❖ transmission rate = *bandwidth*
- ❑ *routers:* forward packets (chunks of data)

Mobile network

Global ISP

Home network

Regional ISP

Institutional network

"Fun" Internet-connected devices

IP picture frame
http://www.ceiva.com/

Web-enabled toaster +
weather forecaster

Tweet-a-watt:
monitor energy use

Slingbox: watch,
control cable TV remotely

Internet
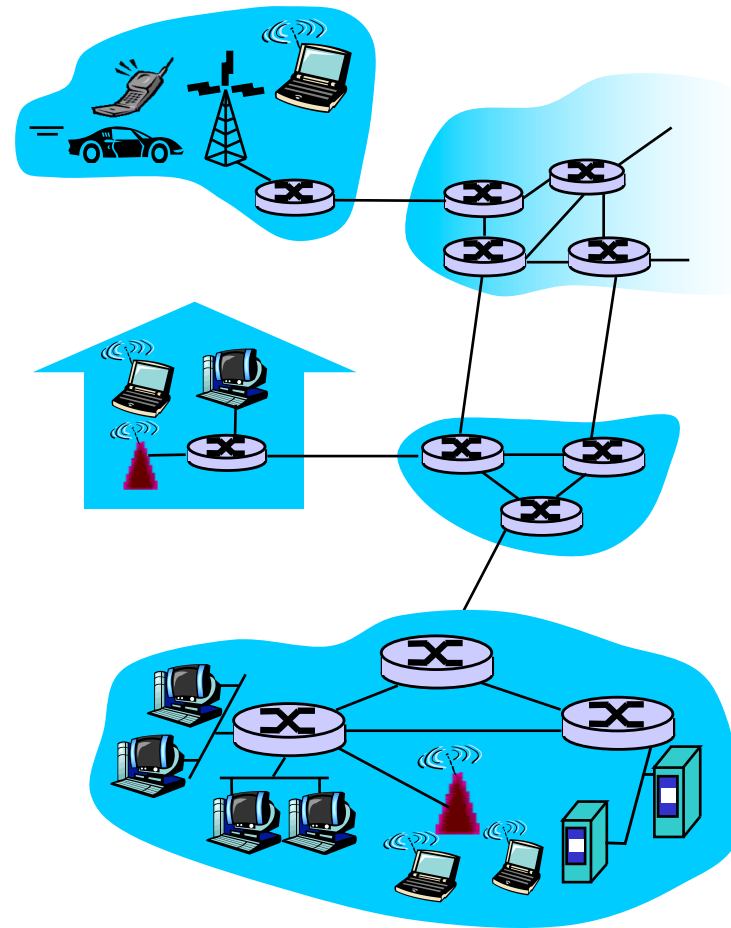refrigerator

sensorized,
bed
mattress

Internet phones

What's the Internet: "nuts and bolts" view

❑ *protocols* control sending, receiving of msgs
  ○ e.g., TCP, IP, HTTP, Skype, Ethernet

❑ *Internet:* "network of networks"
  ○ loosely hierarchical
  ○ public Internet versus private intranet

Mobile network

Global ISP

Home network
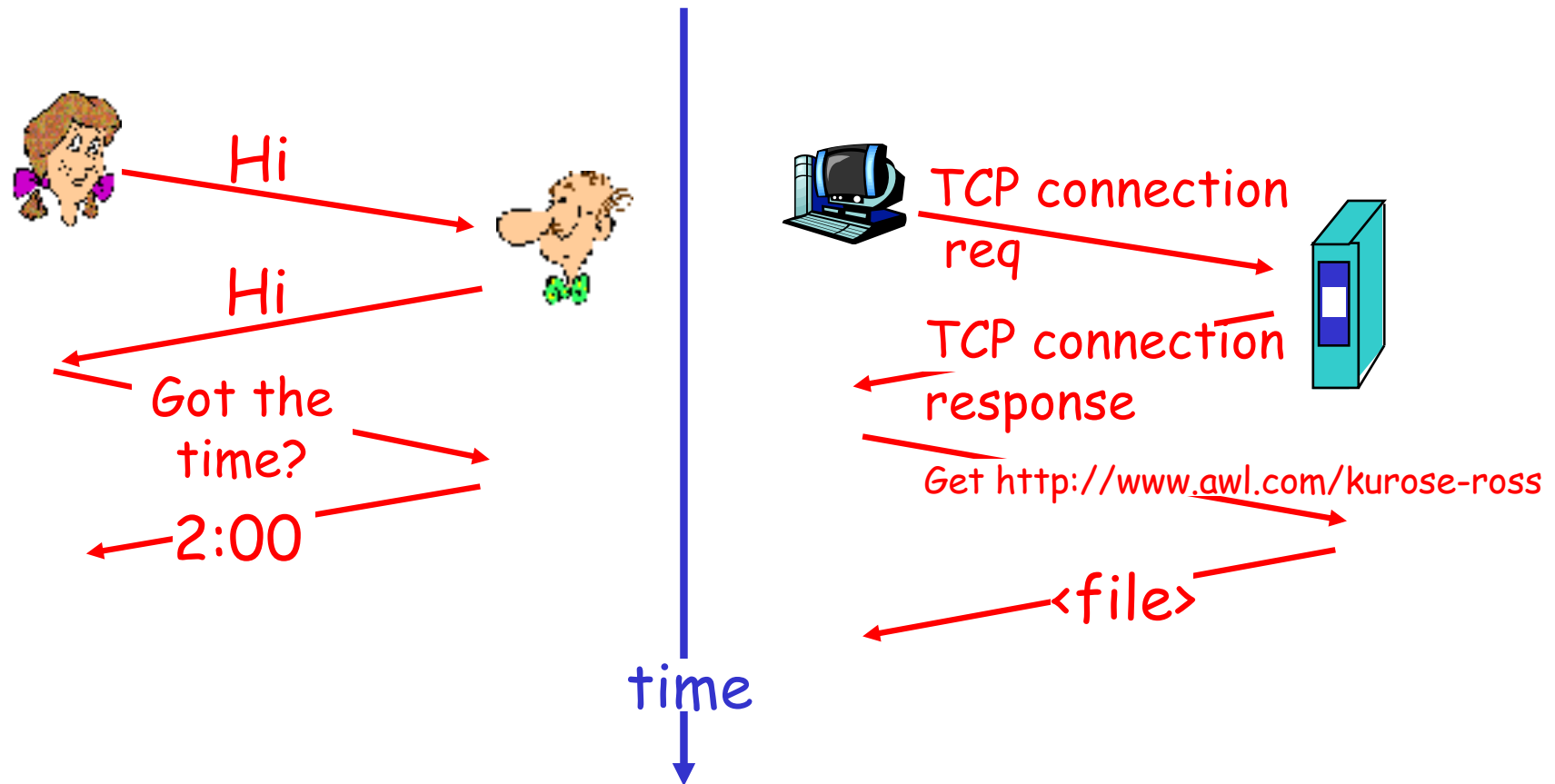
Regional ISP

Institutional network
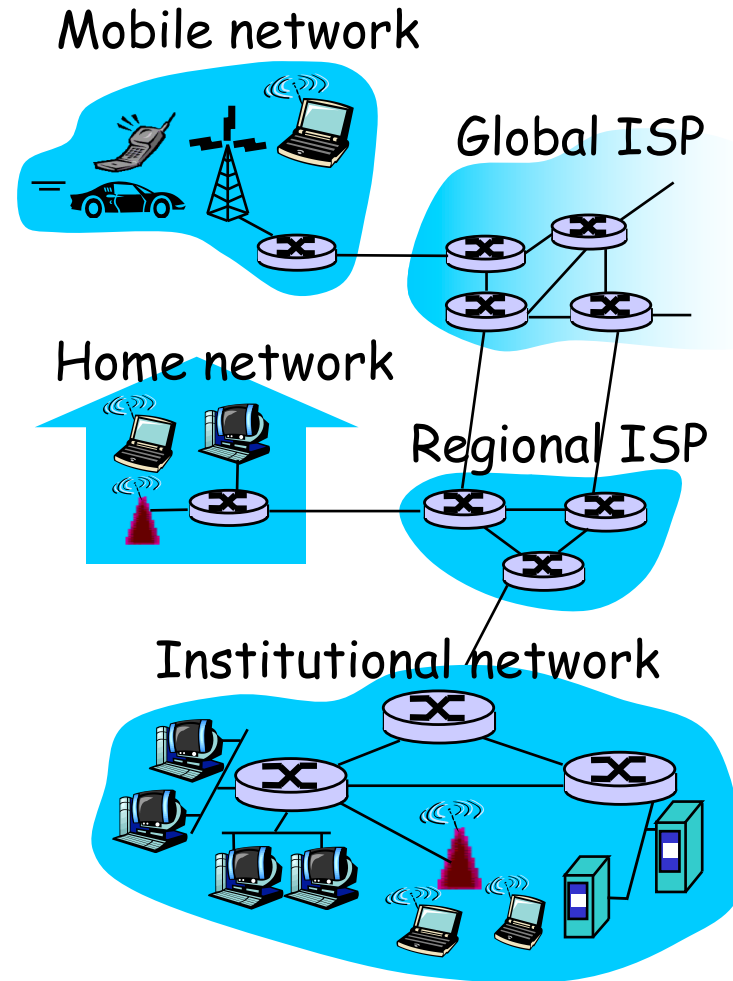
What's the Internet: a service view

❑ **communication**
   infrastructure enables
   distributed applications:

   ○ Web, VoIP, email, games,
      e-commerce, file sharing

❑ **communication services**
   provided to apps:

   ○ reliable data delivery
      from source to
      destination

   ○ "best effort" (unreliable)
      data delivery

What's a protocol?

a human protocol and a computer network protocol:

Hi

Hi

Got the time?

2:00

TCP connection req

TCP connection response

Get http://www.awl.com/kurose-ross

<file>

time

A protocol

human protocols:

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

… specific messages sent

… specific actions taken when messages received, or other events

network protocols:

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

protocols define **format**, **order** of messages sent and received among network entities, and **actions** taken on message transmission, receipt

Quiz Time!

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
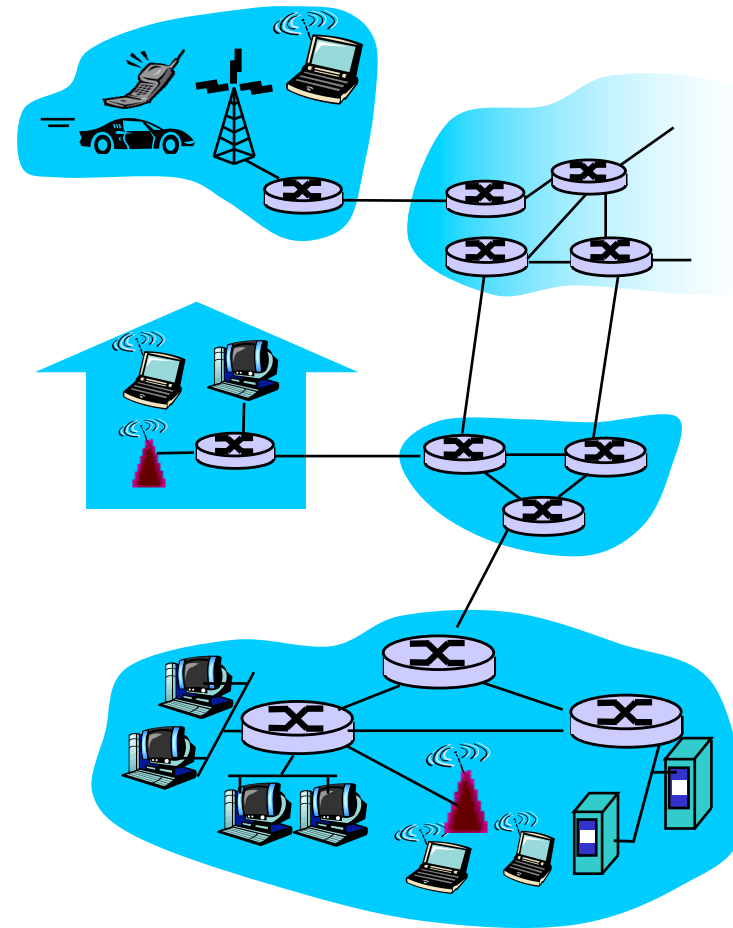
Chapter 1: roadmap

The network edge:

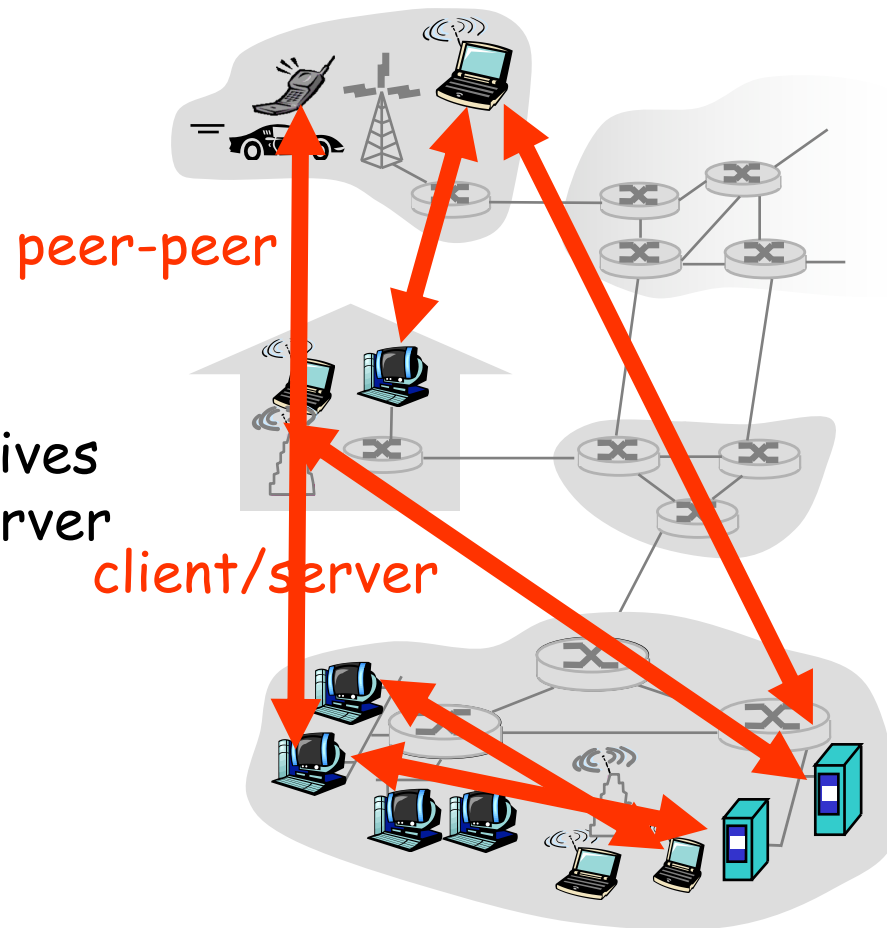❑ **end systems (hosts):**
  ○ run application programs
  ○ e.g. Web, email
  ○ at "edge of network"

❑ **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
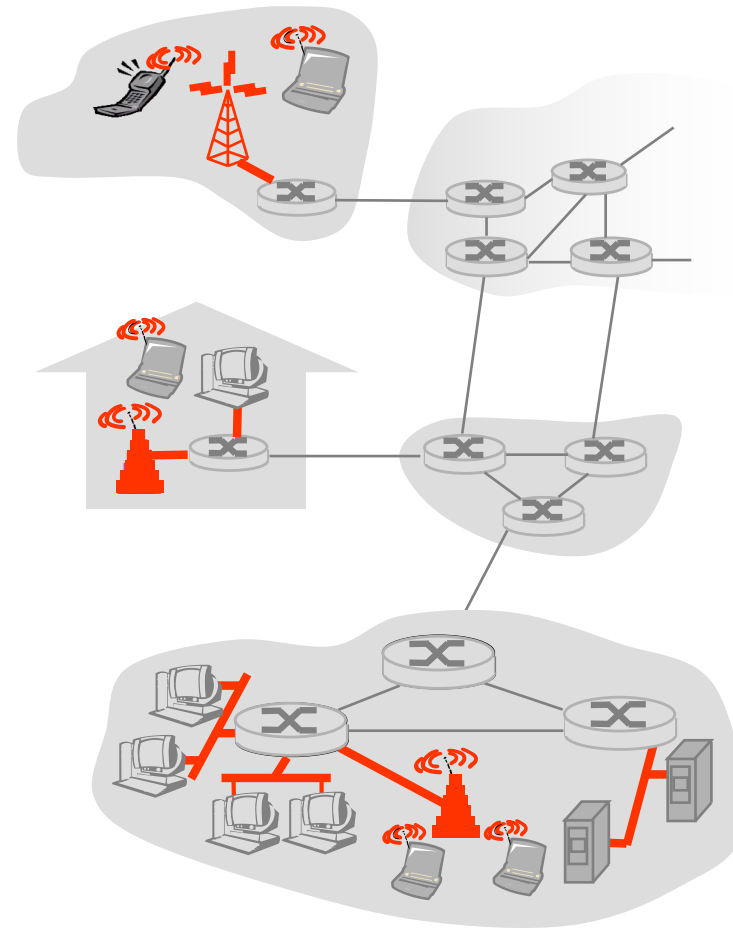 ❖ e.g. Skype, BitTorrent

peer-peer

client/server

Access networks and physical media

Q: How to connect end systems to edge router?
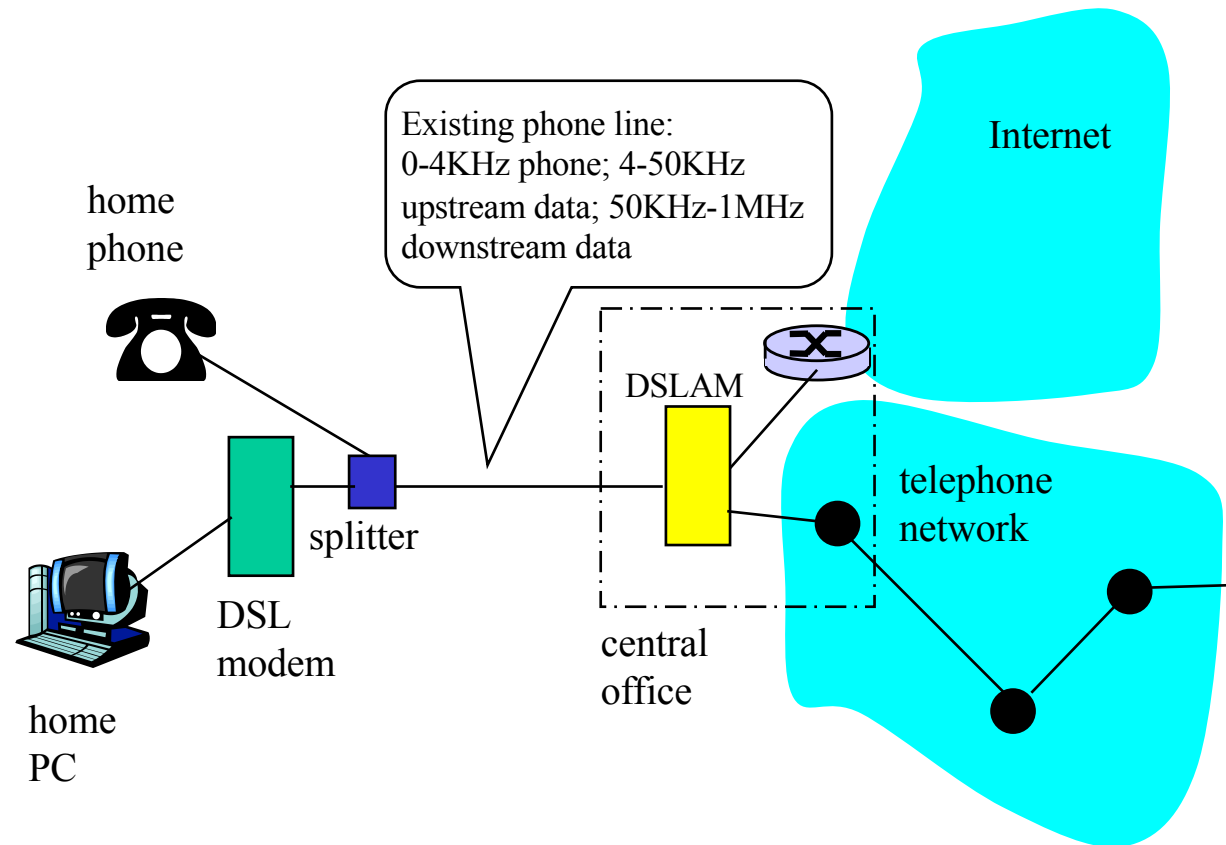
- residential access nets
- institutional access networks (school, company)
- mobile access networks

Keep in mind:

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

Digital Subscriber Line (DSL)

home
phone

Existing phone line:
0-4KHz phone; 4-50KHz
upstream data; 50KHz-1MHz
downstream data

Internet

DSLAM

splitter

DSL
modem

telephone
network

central
office

home
PC

❖ Uses existing telephone infrastructure
❖ up to 1 Mbps upstream
❖ up to 8 Mbps downstream
❖ dedicated physical line to telephone central office

Residential access: cable modems

- Does not use telephone infrastructure
  - Instead uses cable TV infrastructure
- 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
  - unlike DSL, which has dedicated access

Cable Network Architecture: Overview

Typically 500 to 5,000 homes
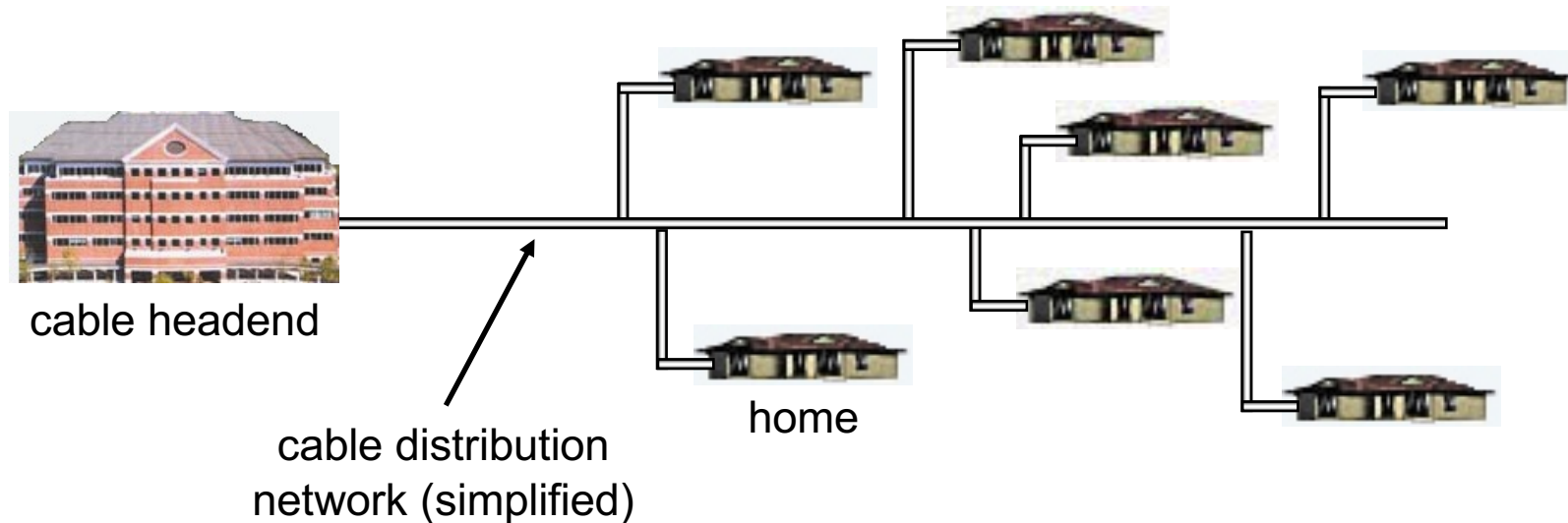
cable headend

cable distribution
network (simplified)

home

Cable Network Architecture: Overview

server(s)

cable headend

cable distribution
network

home

Cable Network Architecture: Overview

cable headend

cable distribution
network (simplified)

home

Set-Top Box

Home Environment

TV

Cable
Modem

PC

Coax

Coax

10 Mbps Ethernet

Splitter
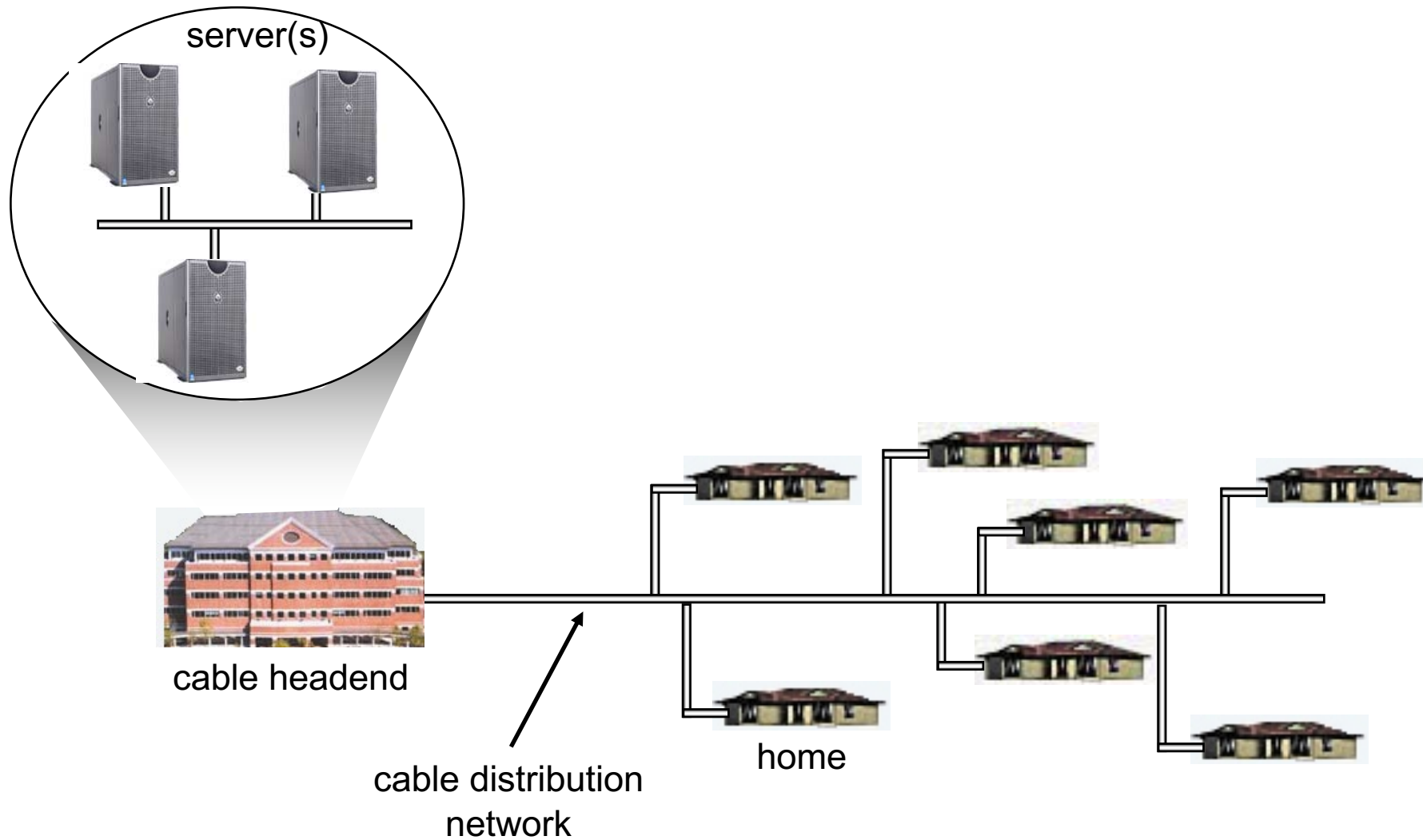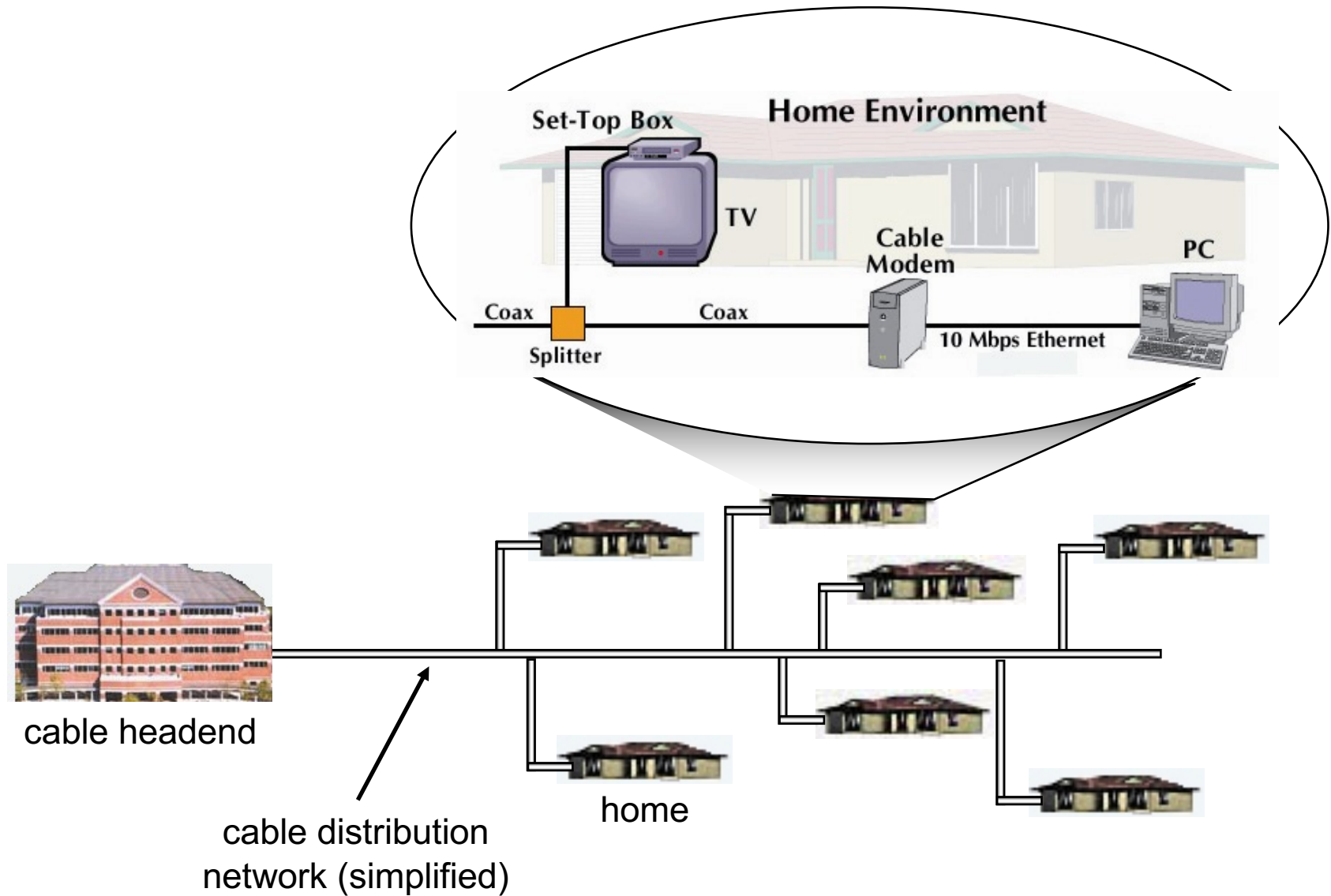
Cable Network Architecture: Overview

FDM (more shortly):

								C
V	V	V	V	V	V	D	D	O
I	I	I	I	I	I	A	A	T
D	D	D	D	D	D	T	T	R
E	E	E	E	E	E	A	A	O
O	O	O	O	O	O			L
1	2	3	4	5	6	7	8	9

Channels
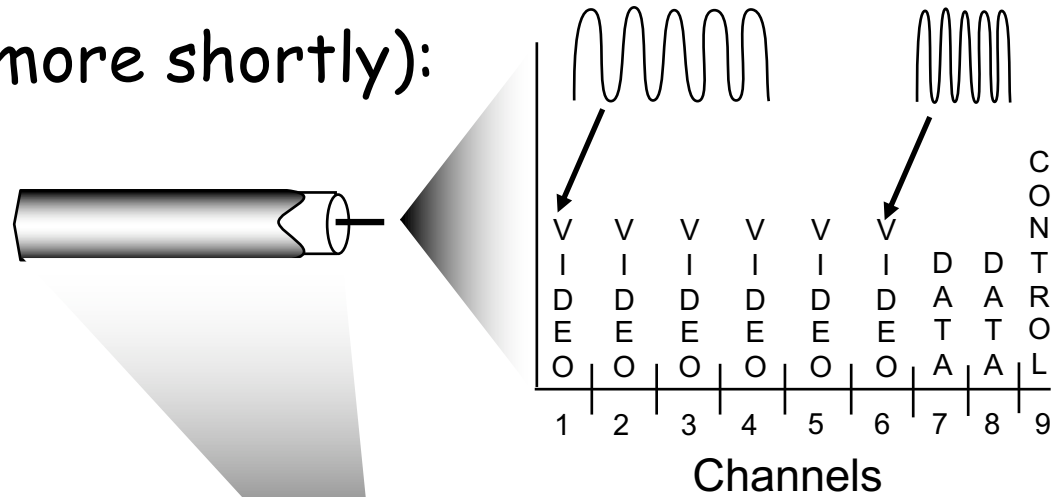
cable headend

cable distribution network

home

Fiber to the Home

Internet
central office
OLT
optical fiber
optical splitter
optical fibers
ONT
ONT
ONT
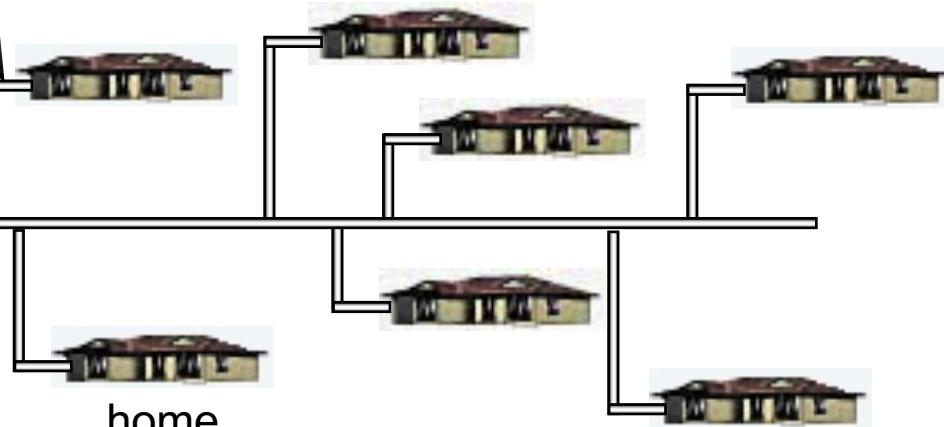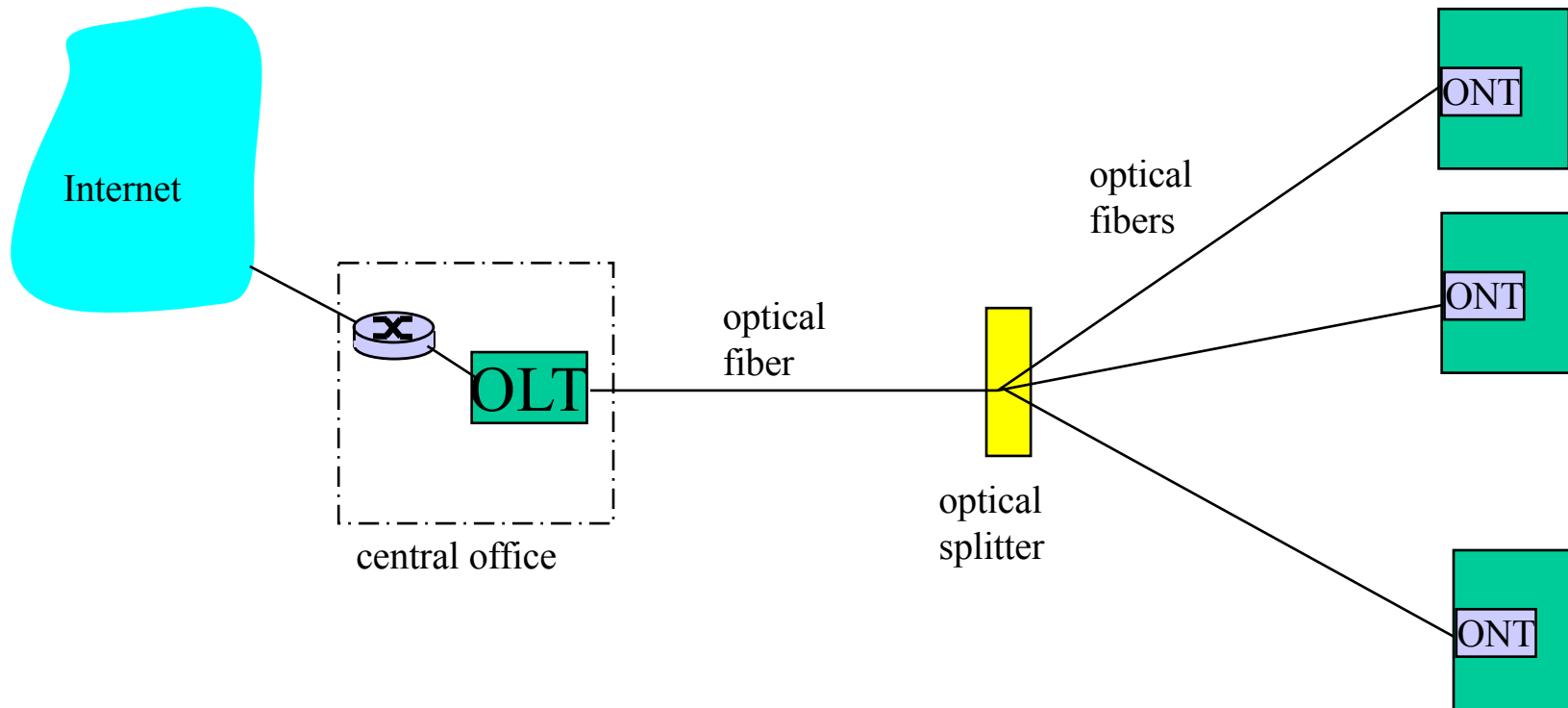
❑ Optical links from central office to the home
❑ Two competing optical technologies:
  ○ Passive Optical network (PON)
  ○ Active Optical Network (AON)
❑ Much higher Internet rates; fiber also carries television and phone services

Ethernet Internet access
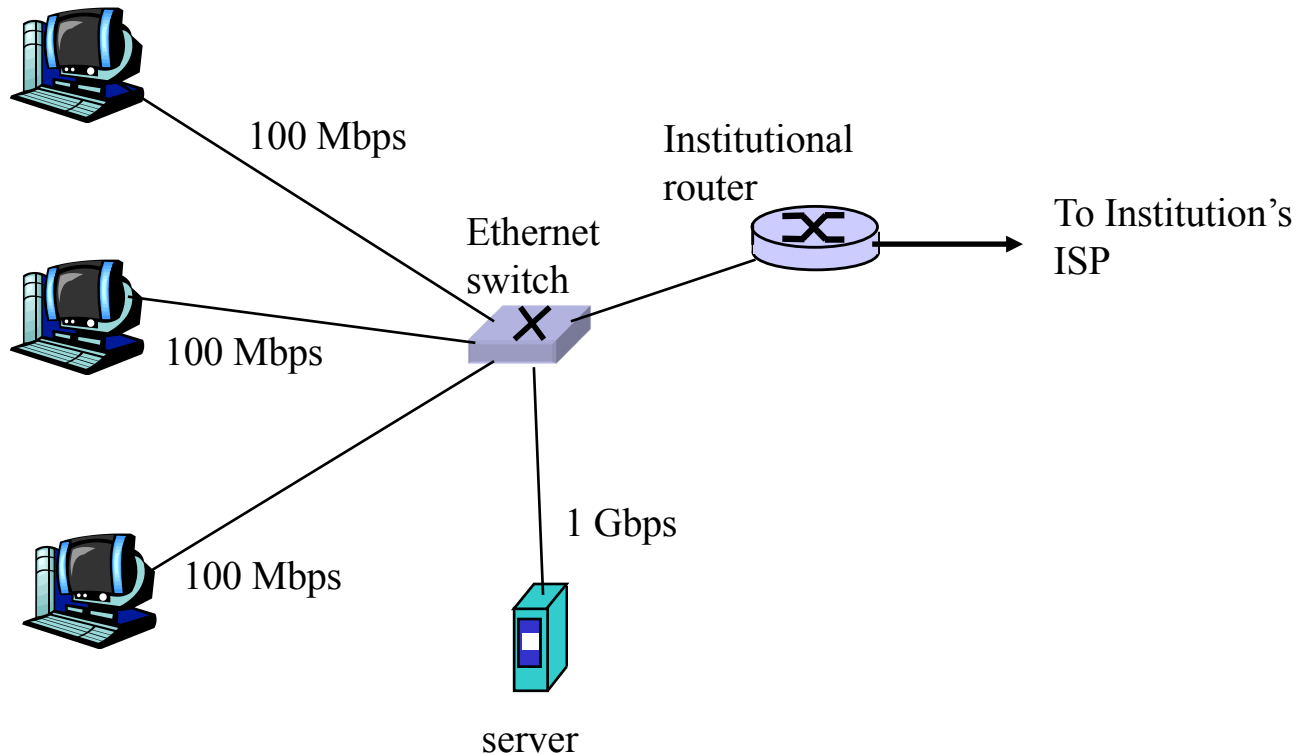
- □ Typically used in companies, universities, etc
- □ 10 Mbs, 100Mbps, 1Gbps, 10Gbps Ethernet
- □ Today, end systems typically connect into Ethernet switch

Wireless access networks

- shared *wireless* access network connects end system to router
  - via base station aka "access point"
- wireless LANs:
  - 802.11b/g (WiFi): 11 or 54 Mbps
- wider-area wireless access
  - provided by telco operator
  - ~1Mbps over cellular system (EVDO, HSDPA)
  - next up (?): WiMAX (10's Mbps) over wide area, 5G

router

base station

mobile hosts
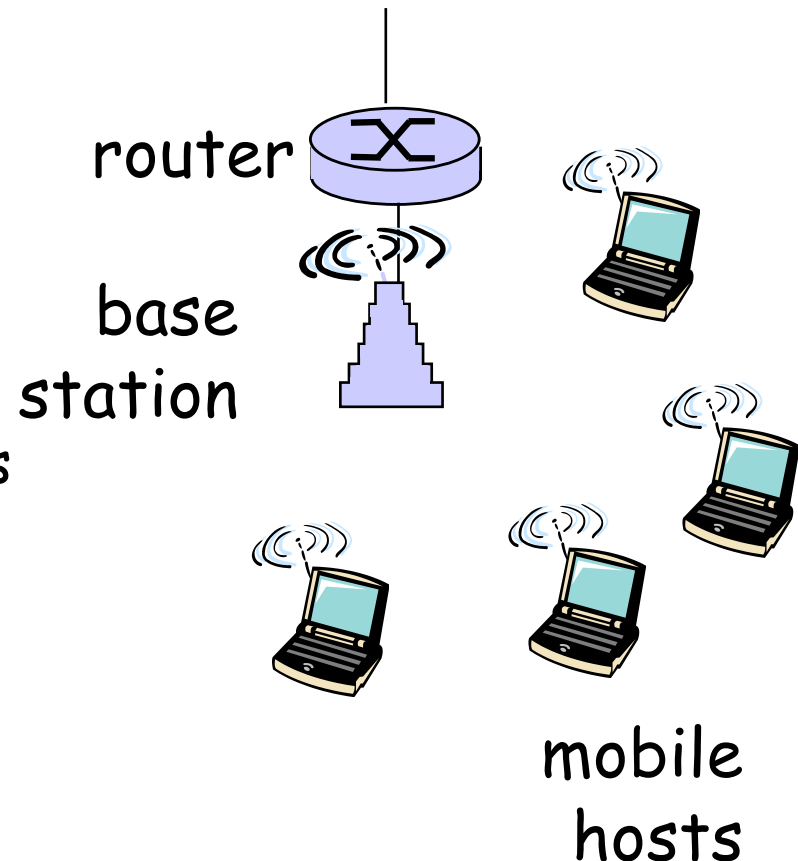
Home networks

Typical home network components:
- ❑ DSL, cable modem, or FTTH
- ❑ router/firewall/NAT
- ❑ Ethernet
- ❑ wireless access point

to/from cable headend

cable modem

router/ firewall

Ethernet

wireless access point

wireless laptops
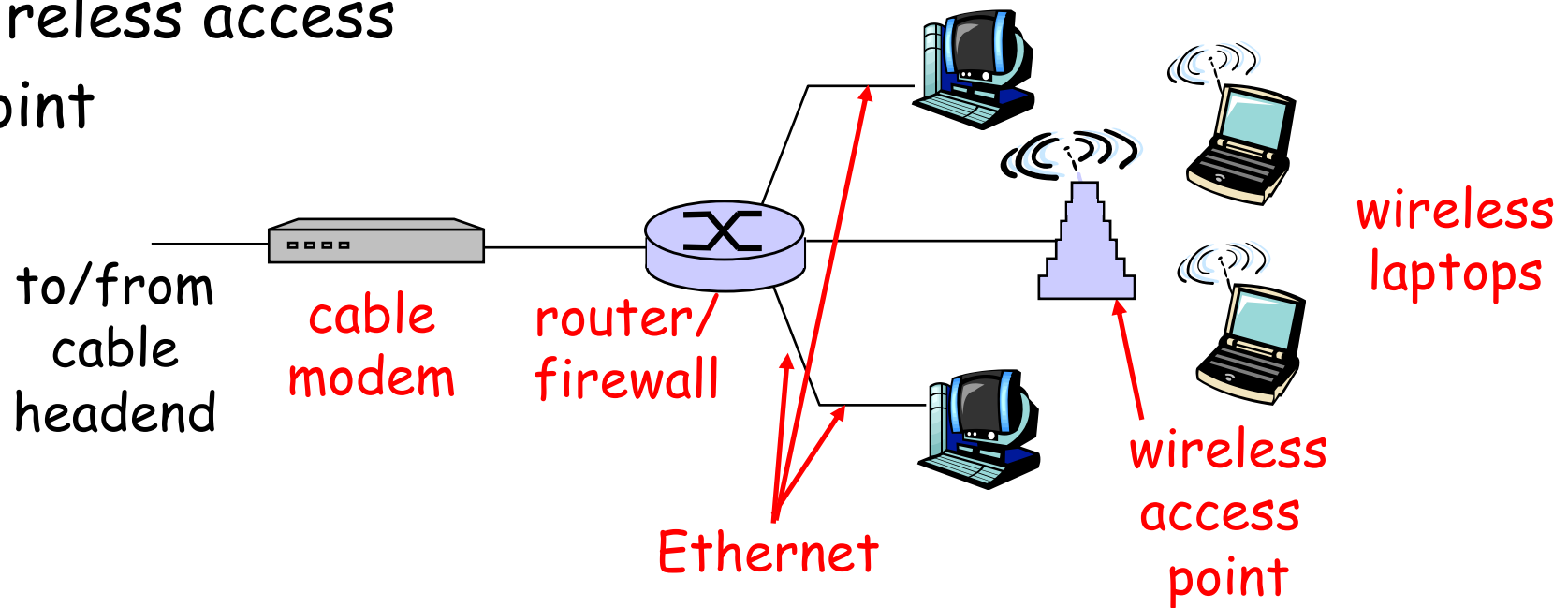
Physical Media

❑ **Bit:** propagates between transmitter/rcvr pairs

❑ **physical link:** what lies between transmitter & receiver

❑ **guided media:**
  ○ signals propagate in solid media: copper, fiber, coax

❑ **unguided media:**
  ○ signals propagate freely, e.g., radio

Twisted Pair (TP)

❑ two insulated copper wires
  ○ Category 3: traditional phone wires, 10 Mbps Ethernet
  ○ Category 5: 100Mbps Ethernet

Physical Media: coax, fiber

Coaxial cable:

- two concentric copper conductors
- bidirectional
- baseband:
  - single channel on cable
  - legacy Ethernet
- broadband:
  - multiple channels on cable
  - HFC

Fiber optic cable:

- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10's-100's Gps)
- low error rate: repeaters spaced far apart ; immune to electromaanetic noise

Physical media: radio

- signal carried in electromagnetic spectrum
- no physical "wire"
- bidirectional
- propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

Radio link types:

- terrestrial microwave
  - e.g. up to 45 Mbps
- LAN (e.g., Wifi)
  - 11Mbps, 54 Mbps
- wide-area (e.g., cellular)
  - 4G cellular: ~ 1+ Mbps
- satellite
  - Kbps to 45Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - geosynchronous versus low altitude

Chapter 1: roadmap

The Network Core

- ❑ **mesh of interconnected routers**
- ❑ *the* fundamental question: how is data transferred through net?
  - ○ **circuit switching:** dedicated circuit per call: telephone net
  - ○ **packet-switching:** data sent thru net in discrete "chunks"
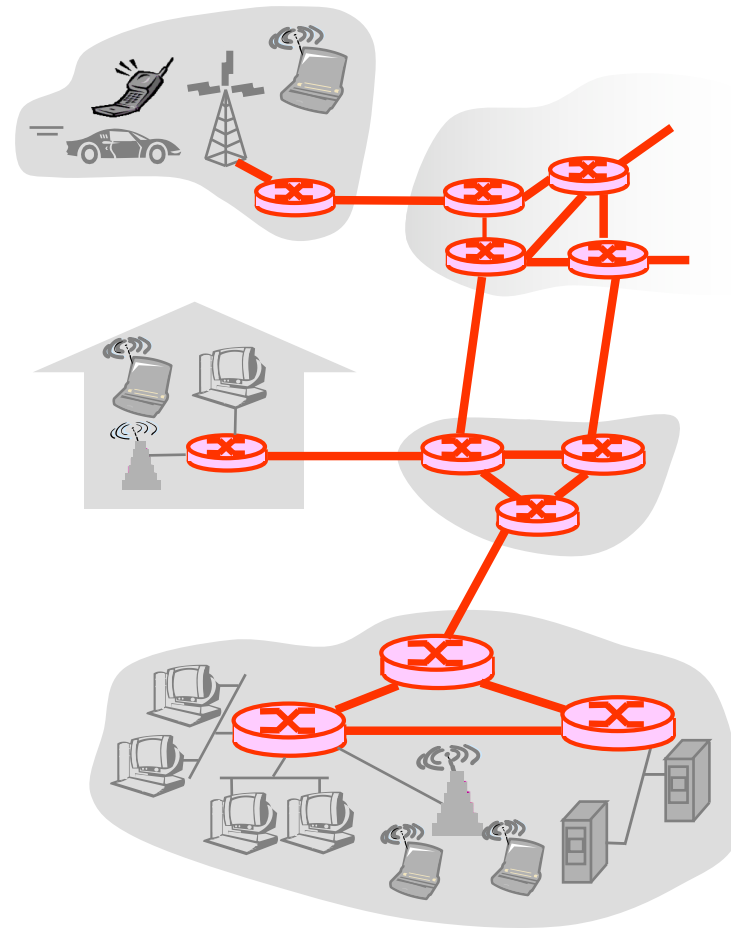
Network Core: Circuit Switching

End-end resources reserved for "call"

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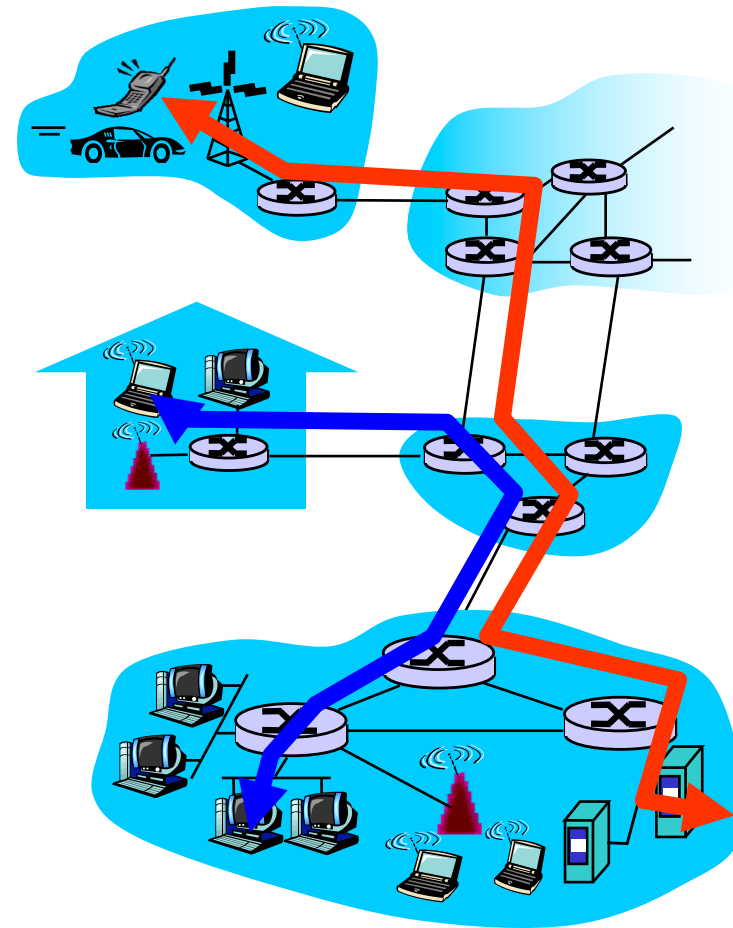
Network Core: Circuit Switching

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
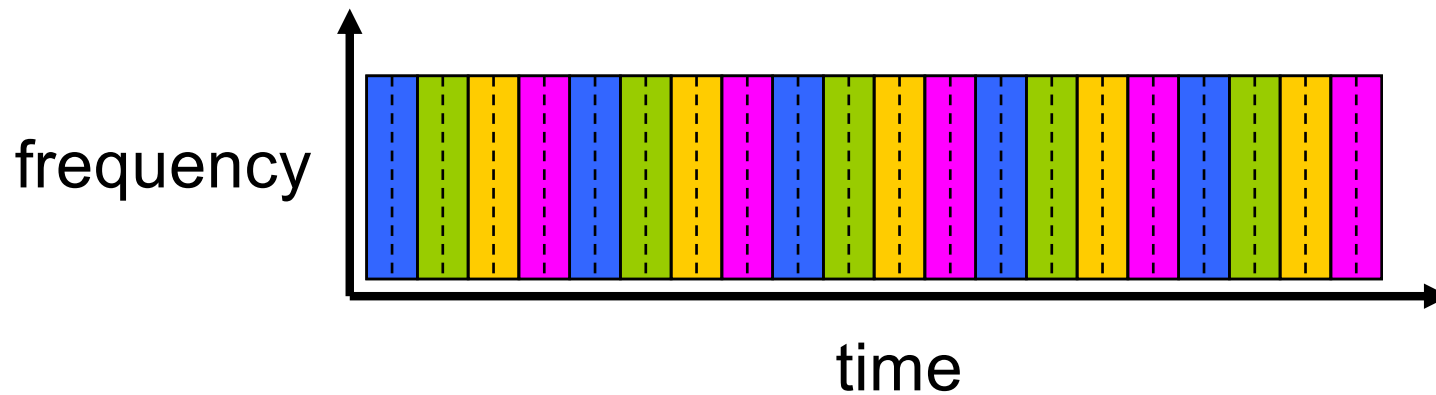
Example:

4 users

FDM

frequency

time

TDM

frequency

time
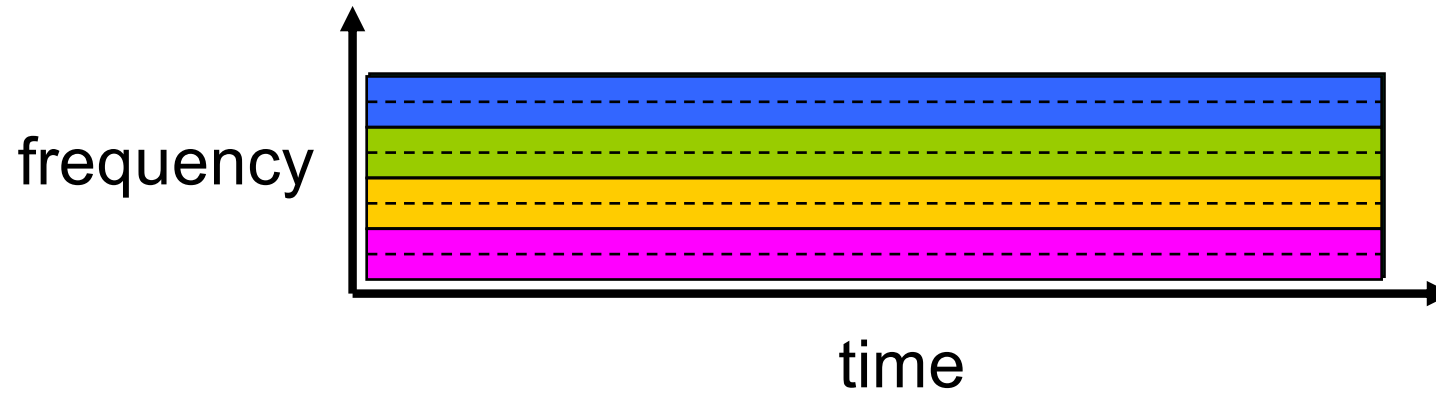
Numerical example

❑ 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

Let's work it out!

Network Core: 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*

Bandwidth division into "pieces"
Dedicated allocation
Resource reservation

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: store-and-forward

L bits
per packet

3 2 1

source

R bps

R bps

destination
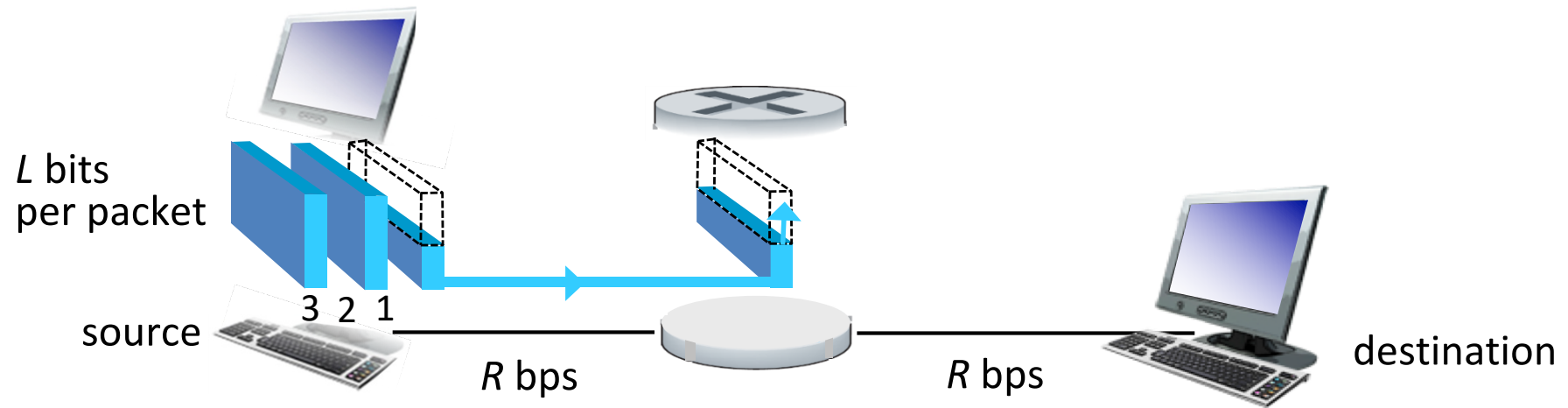
- takes *L/R* seconds to transmit (push out) *L*-bit packet into link at *R* bps

- *store and forward:* entire packet must arrive at router before it can be transmitted on next link

- end-end delay = 2*L/R* (assuming zero propagation delay)

one-hop numerical example:

- *L* = 7.5 Mbits
- *R* = 1.5 Mbps
- one-hop transmission delay = 5 sec

more on delay shortly …

Packet Switching: Statistical Multiplexing

100 Mb/s
Ethernet

A

B

statistical multiplexing

C

1.5 Mb/s

queue of packets
waiting for output
link

D

E
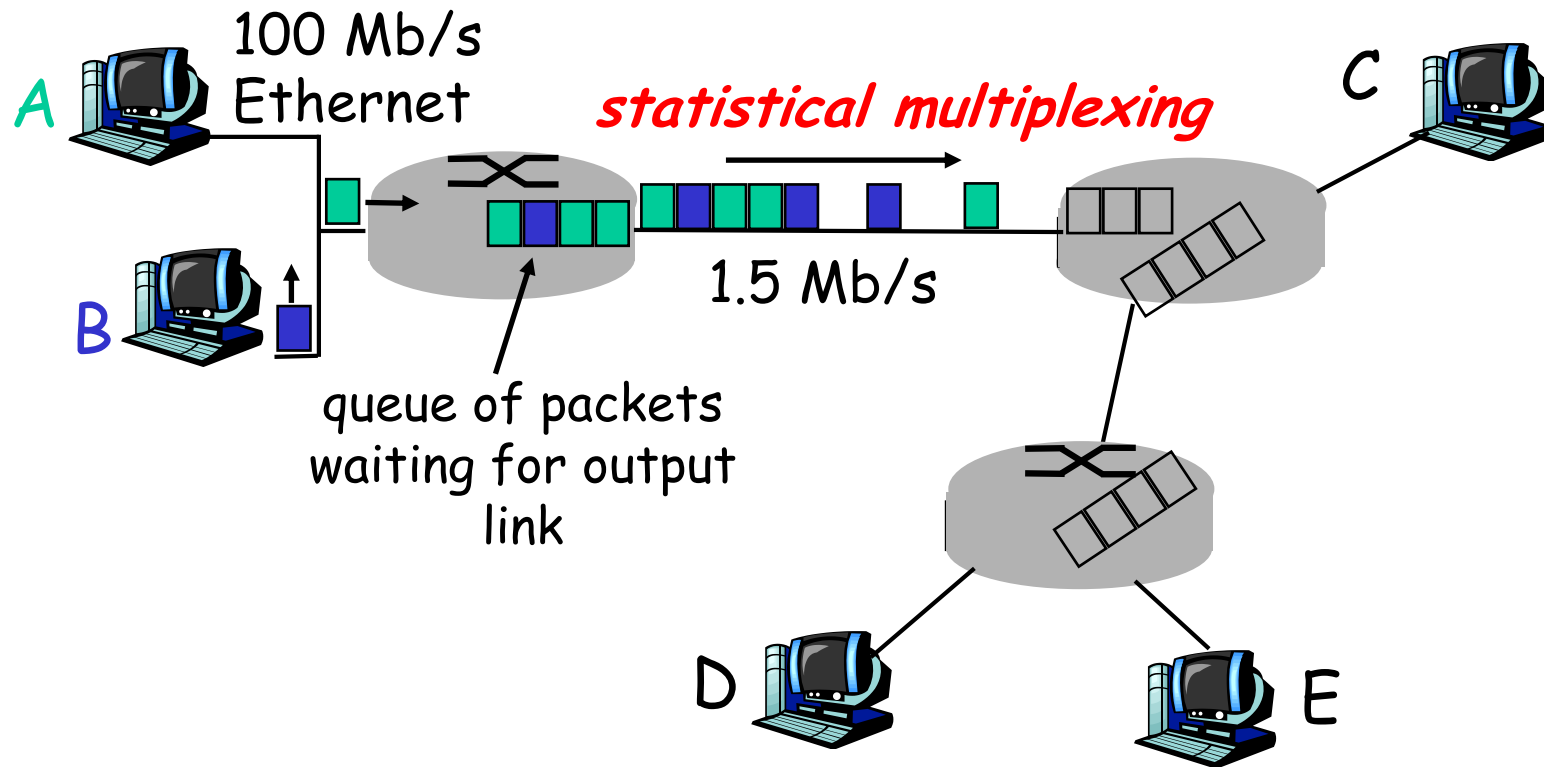
Sequence of A & B packets does not have fixed pattern,
bandwidth shared on demand ➡ *statistical multiplexing*.

In contrast of TDM: each host gets same slot in revolving
TDM frame.

Packet switching versus circuit switching

Packet switching allows more users to use network!

- 1 Mb/s link
- each user:
  - 100 kb/s when "active"
  - active 10% of time
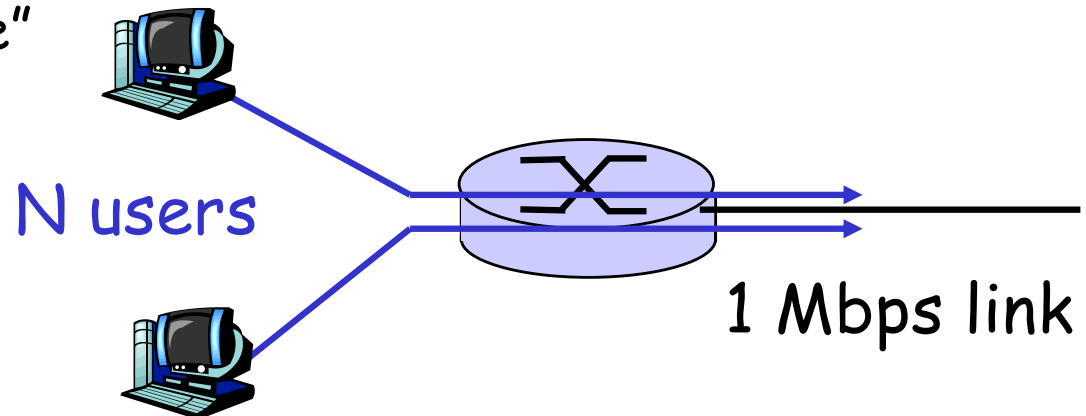
- *circuit-switching:*
  - 10 users
- *packet switching:*
  - with 35 users, probability > 10 active at same time is less than .0004

N users

1 Mbps link

Q: how did we get value 0.0004?

Quiz Time!

Packet switching versus circuit switching

Is packet switching a "slam dunk winner?"

❑ Great for bursty data
   ○ resource sharing
   ○ 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 9)

human analogies of reserved resources (circuit switching)
versus on-demand allocation (packet-switching)

Packet-switching: store-and-forward
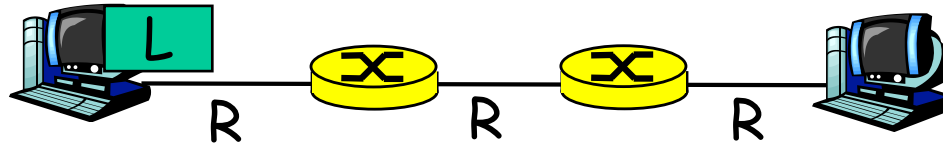
- Takes L/R seconds to transmit (push out) packet of L bits on to link of R bps
  - bps: bits per second
- Entire packet must arrive at router before it can be transmitted on next link: *store and forward*
- 'store and forward' delay = 3L/R

Example:

- L = 7.5 Mbits
- R = 1.5 Mbps

- Total delay
  - 3L/R = 15 sec

Packet Switching: Message Segmenting
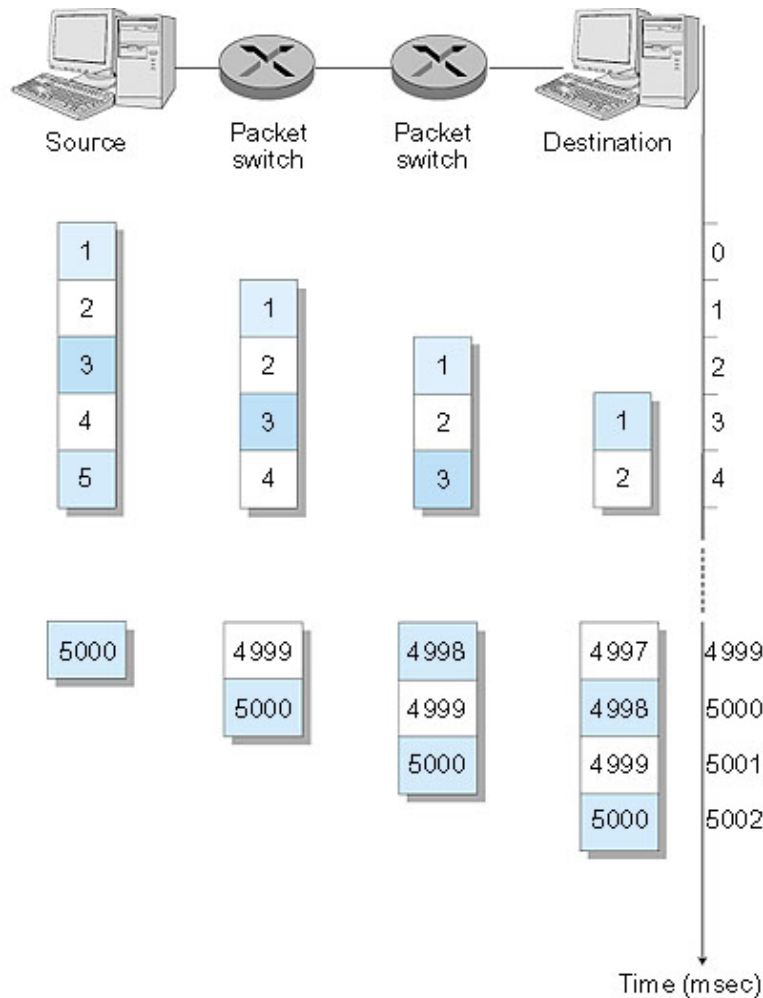
Now break up the message into 5000 packets

- ❑ Each packet 1,500 bits
- ❑ 1 msec to transmit packet on one link
- ❑ *pipelining:* each link works in parallel
- ❑ Delay reduced from 15 sec to 5.002 sec

5.002 vs 15.000
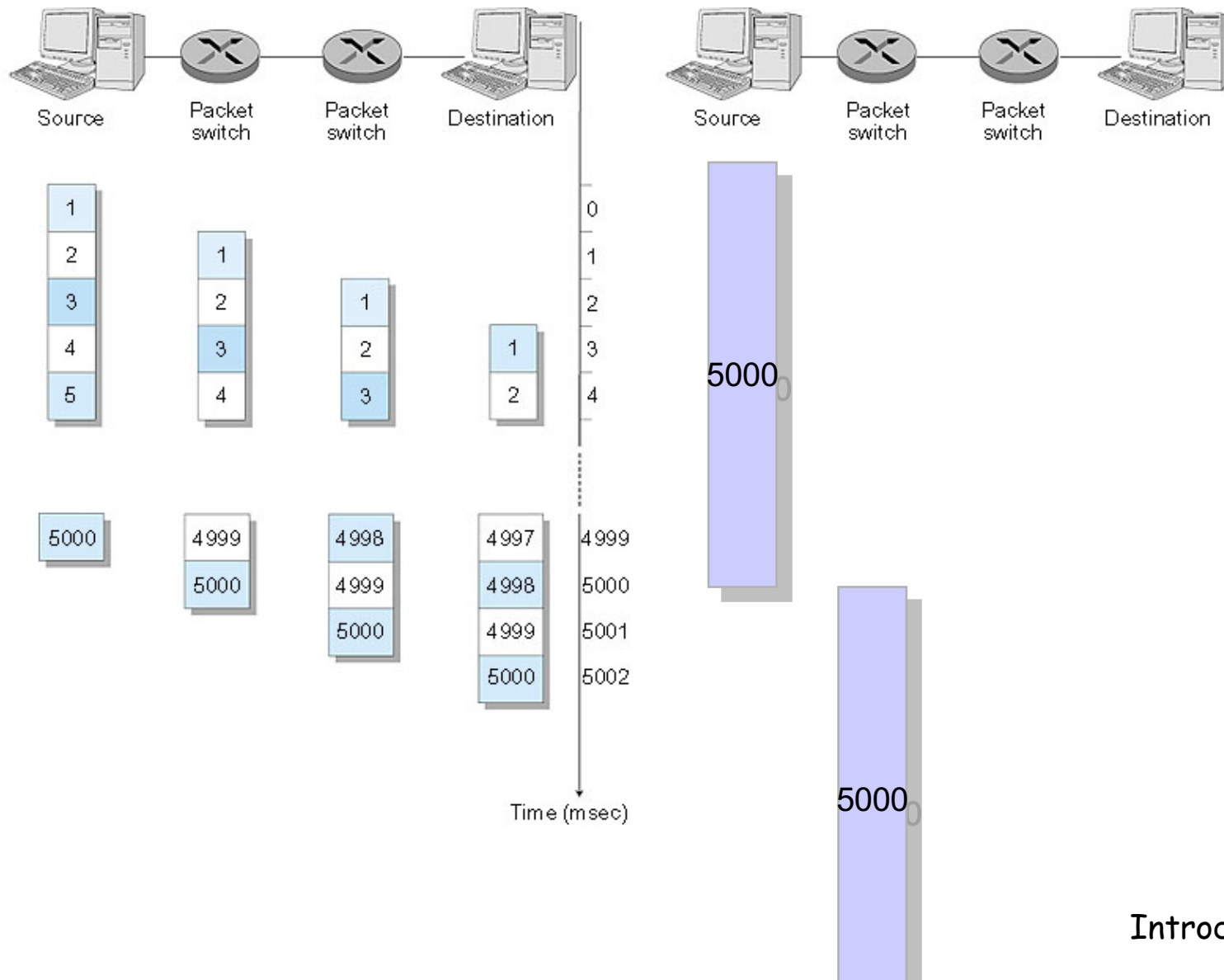
Two key network-core functions

routing: determines source-destination route taken by packets

- *routing algorithms*

forwarding: move packets from router's input to appropriate router output

local forwarding table	
header value	output link
0100	3
0101	2
0111	2
1001	1

routing algorithm

0111

destination address in arriving packet's header
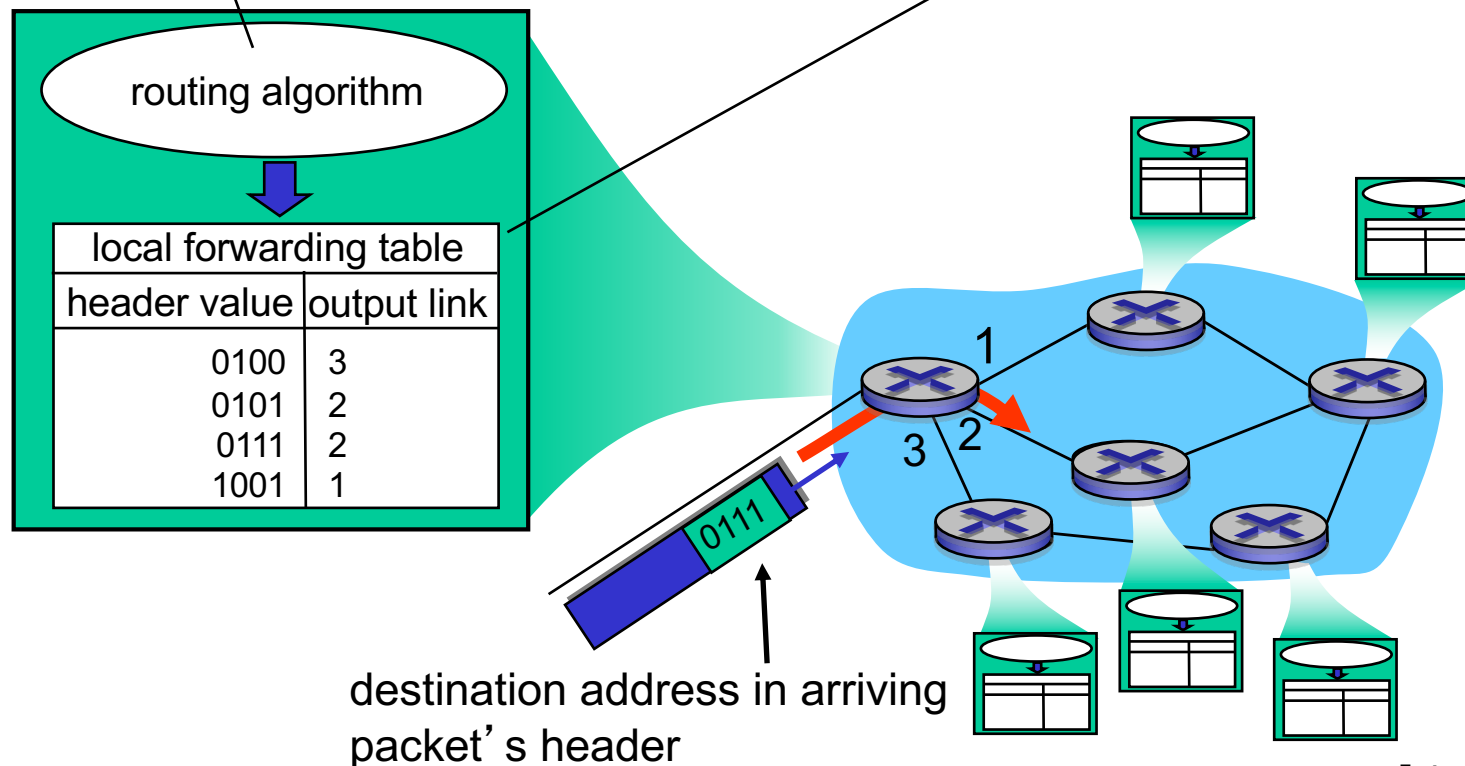
Packet-switched networks: forwarding

❑ *Goal:* move packets through routers from source to destination

  ○ we'll study several path selection (i.e. routing)algorithms (chapter 5)

❑ datagram network:

  ○ *destination address* in packet determines next hop

  ○ routes may change during session

  ○ analogy: driving, asking directions

❑ virtual circuit network:

  ○ each packet carries tag (virtual circuit ID), tag determines next hop

  ○ fixed path determined at *call setup time*, remains fixed thru call

  ○ *routers maintain per-call state*

Network Taxonomy

```
                    ┌─────────────────────┐
                    │  Telecommunication  │
                    │      networks       │
                    └─────────────────────┘
                               │
              ┌────────────────┴────────────────┐
    ┌──────────────────┐              ┌──────────────────┐
    │  Circuit-switched │              │  Packet-switched  │
    │     networks      │              │     networks      │
    └──────────────────┘              └──────────────────┘
         │        │                        │          │
    ┌─────┐   ┌─────┐              ┌──────────┐  ┌──────────┐
    │ FDM │   │ TDM │              │ Networks │  │ Datagram │
    │     │   │     │              │ with VCs │  │ Networks │
    └─────┘   └─────┘              └──────────┘  └──────────┘
```
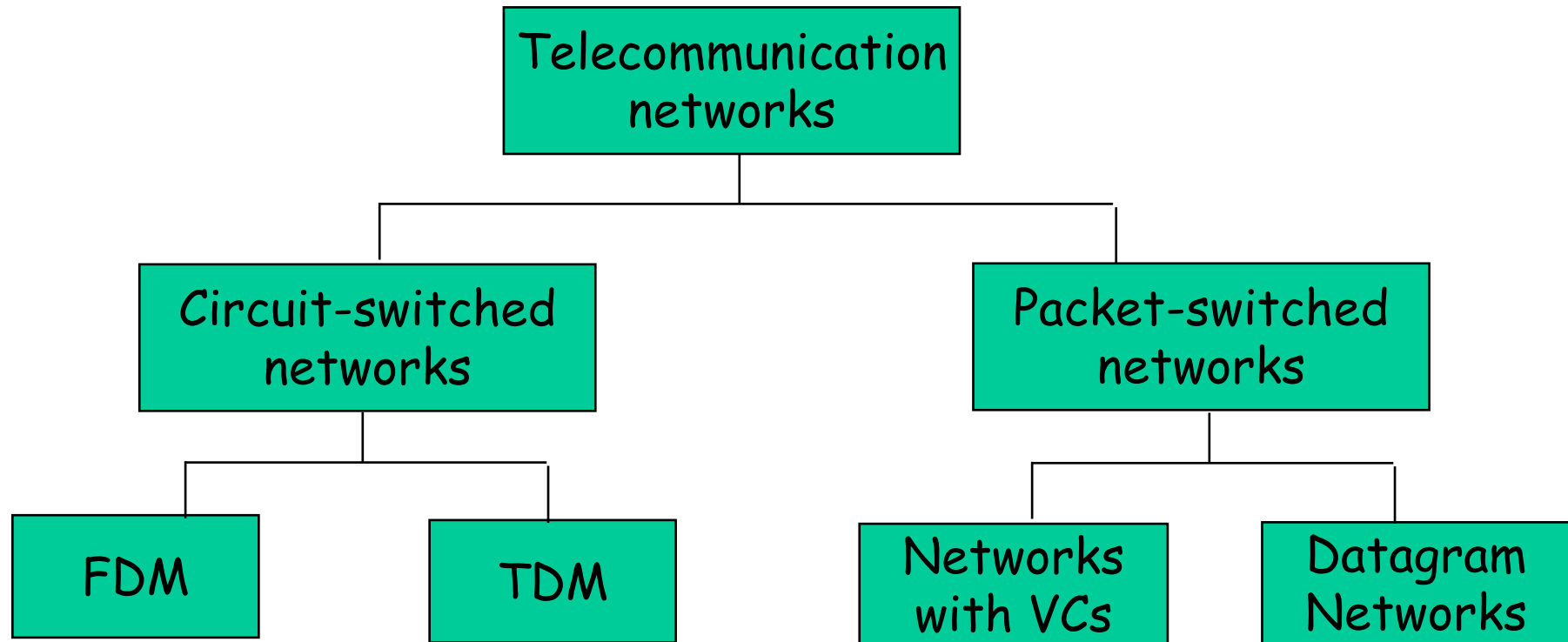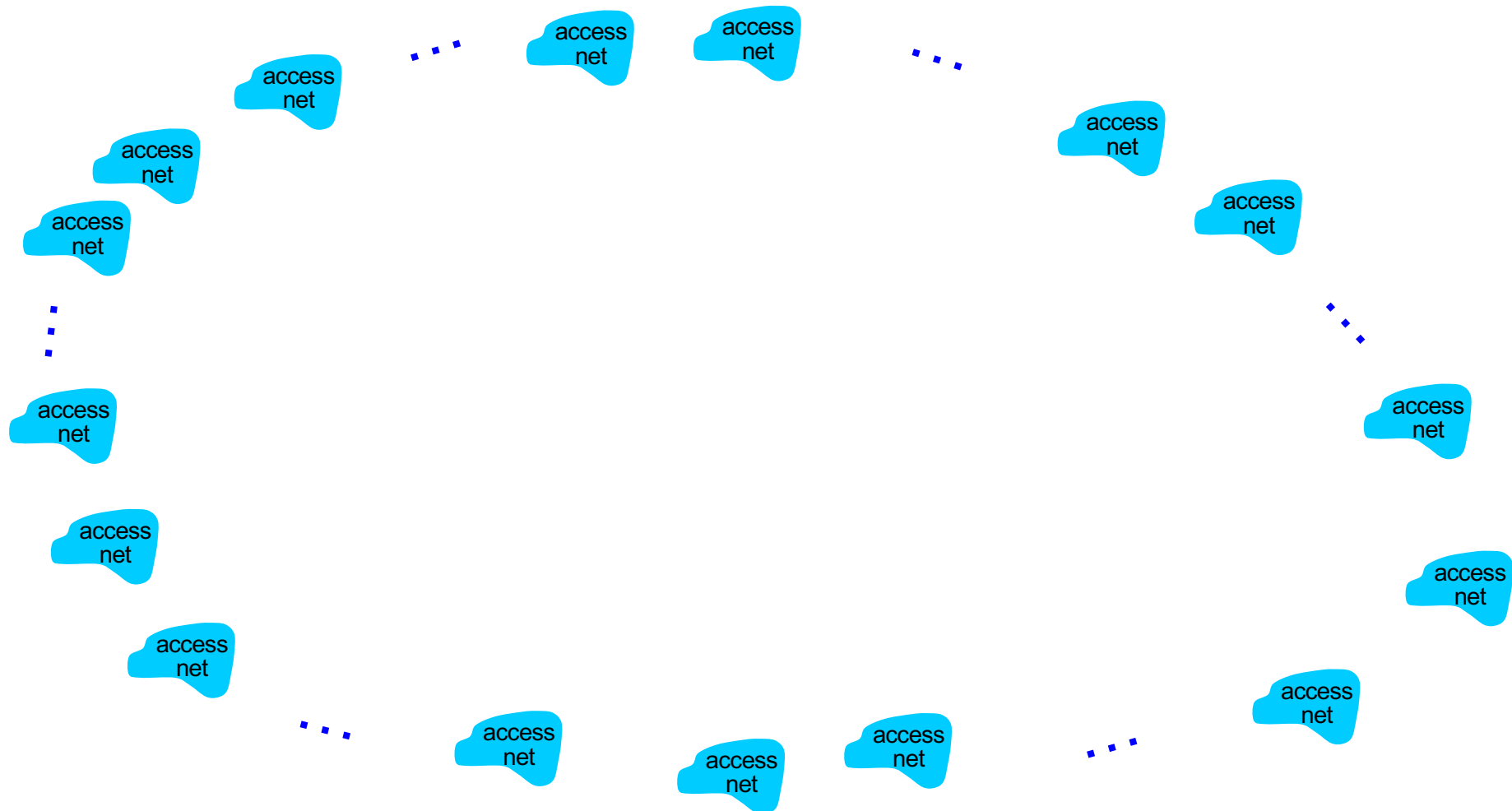
Internet structure: network of networks

- End systems connect to Internet via **access ISPs** (Internet Service Providers)
  - residential, company and university ISPs
- Access ISPs in turn must be interconnected.
  - so that any two hosts can send packets to each other
- Resulting network of networks is very complex
  - evolution was driven by **economics** and **national/business policies**
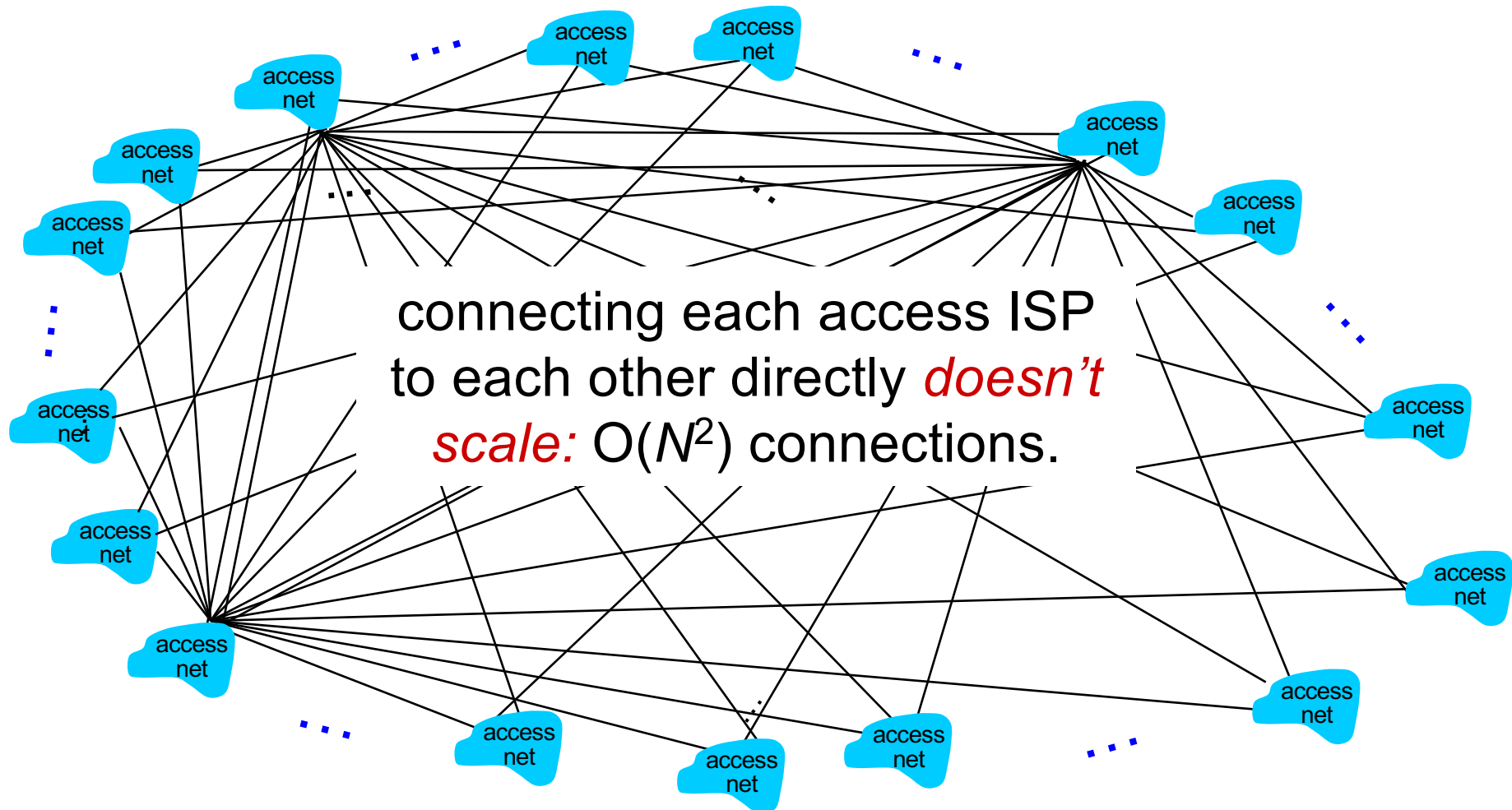- Let's take a stepwise approach to describe current Internet structure

Internet structure: network of networks

Question: given *millions* of access ISPs, how to connect them together?

Internet structure: network of networks

Option: connect each access ISP to every other access ISP?

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

access net

connecting each access ISP to each other directly *doesn't scale:* O(N^2) connections.

Internet structure: network of networks

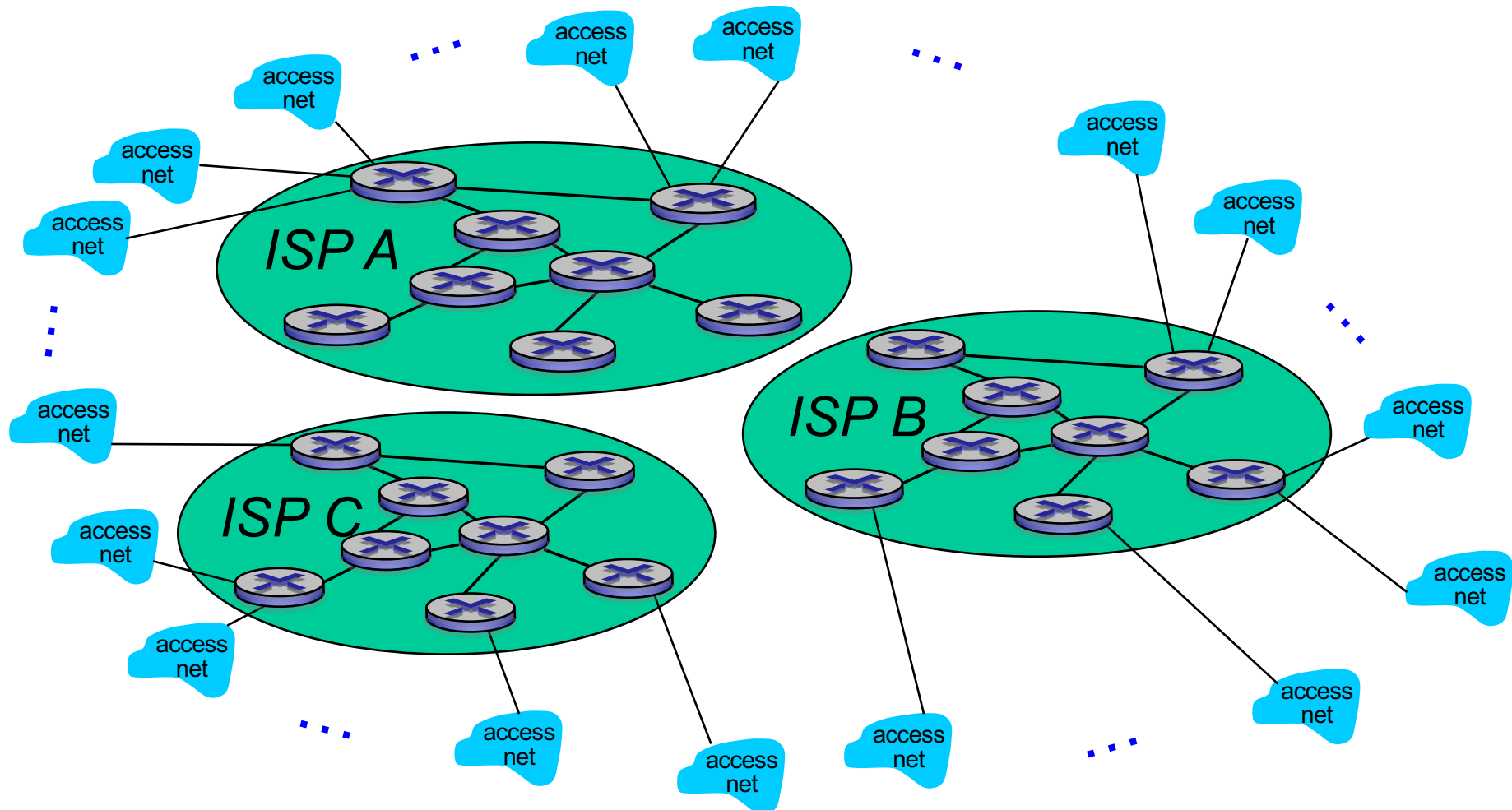*Option:* connect each access ISP to one global transit ISP?
Customer and *provider* ISPs have economic agreement.
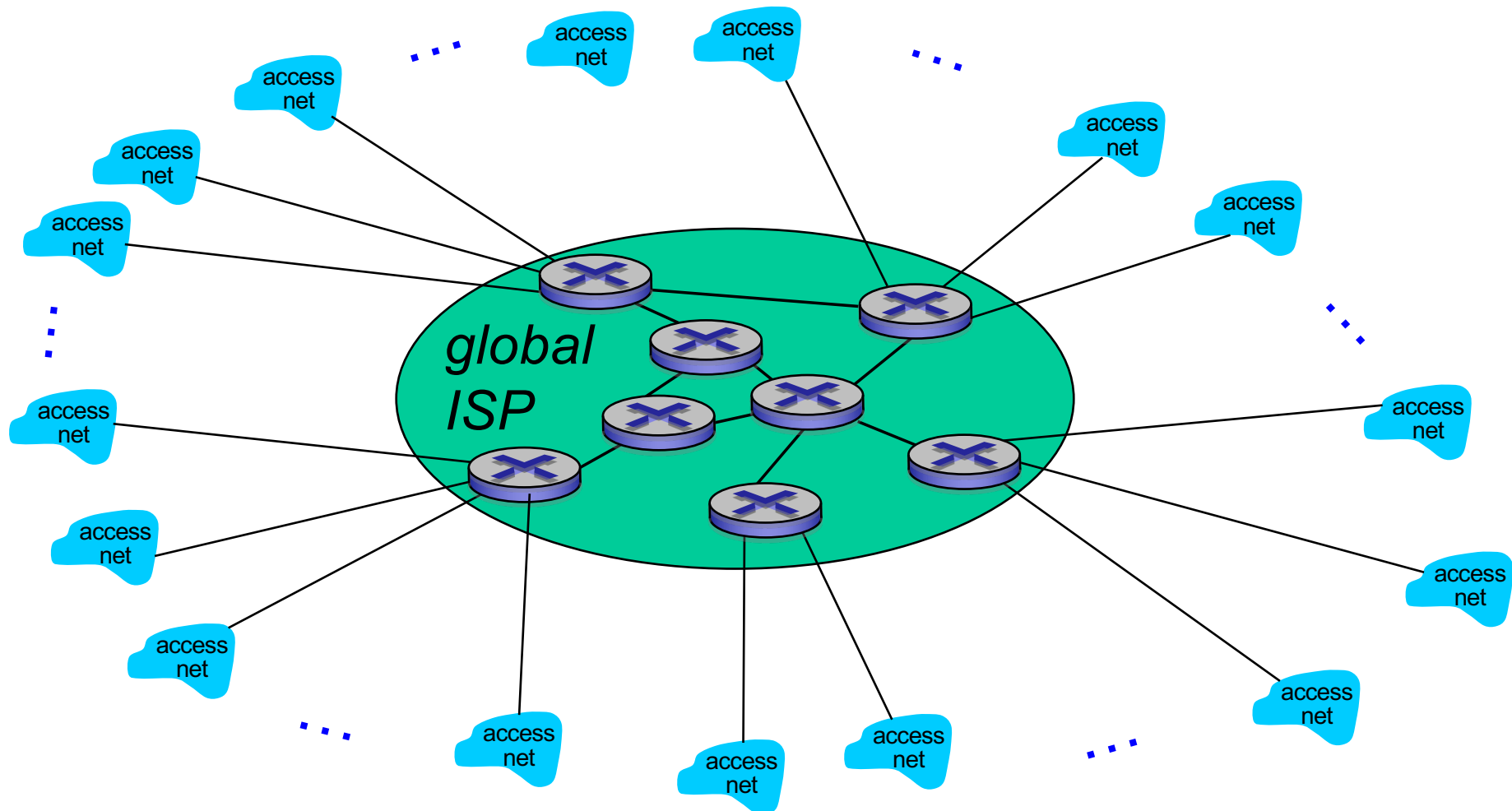
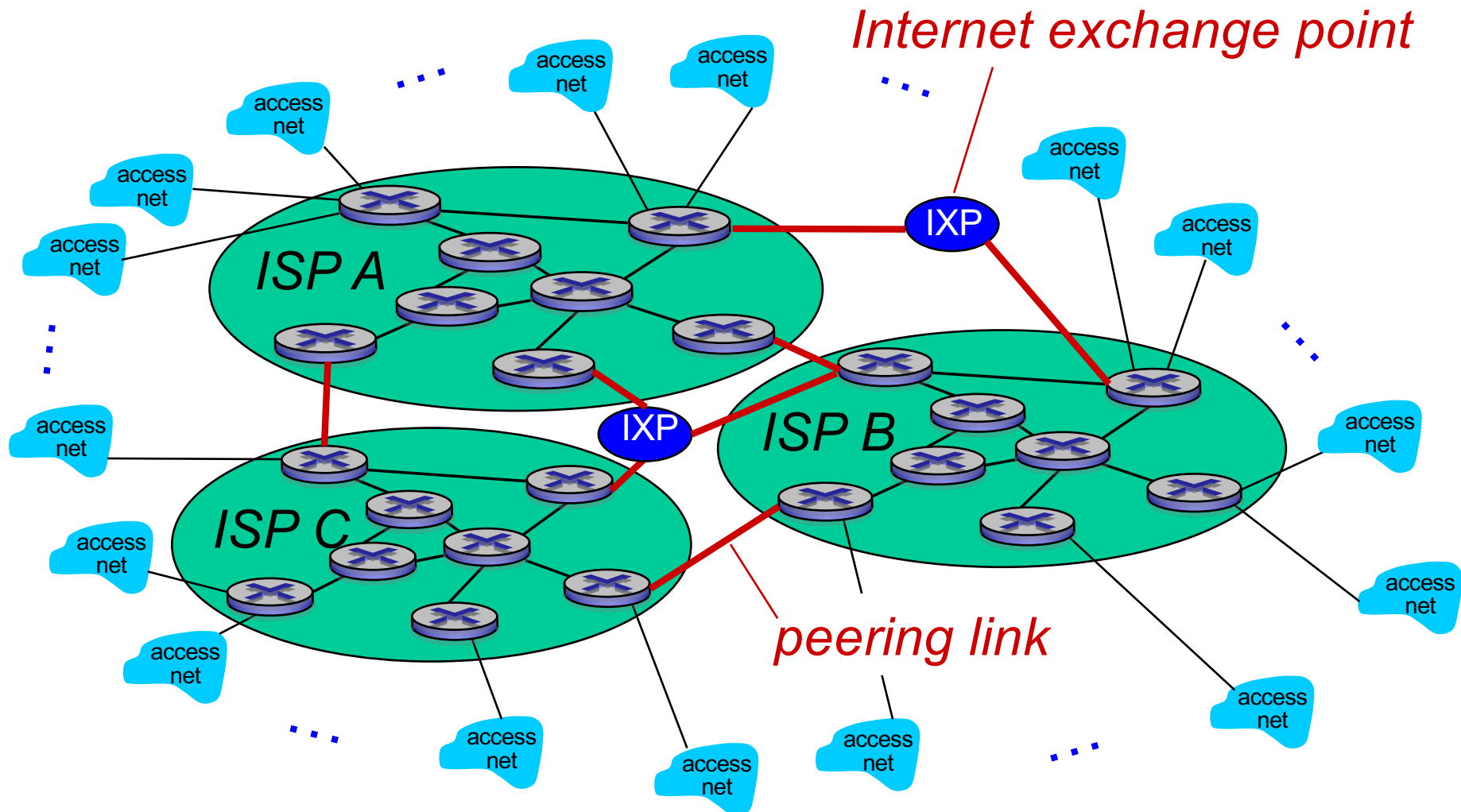# Internet structure: network of networks

But if one global ISP is viable business, there will be competitors ....
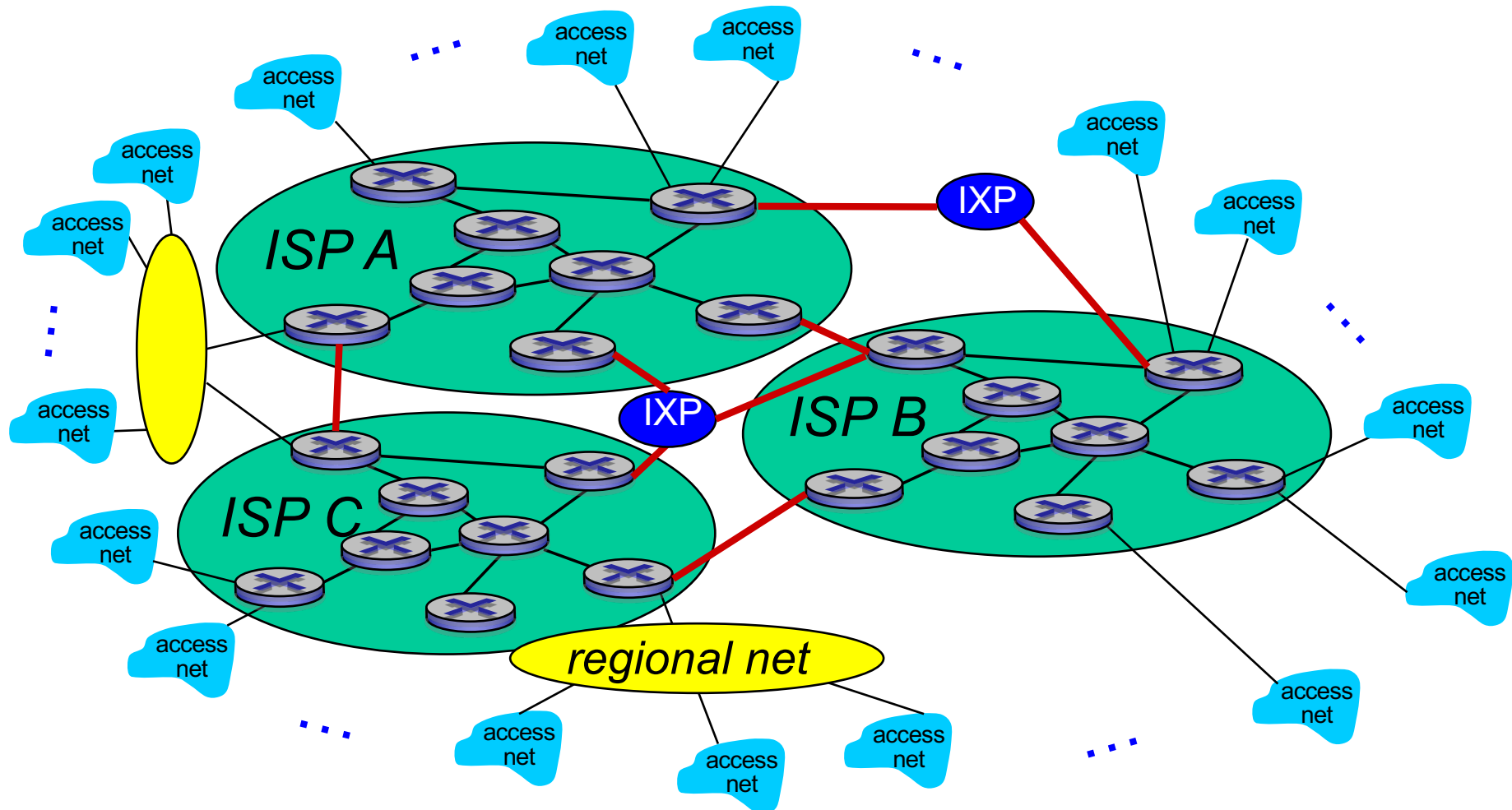
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors
.... which must be interconnected

Internet exchange point

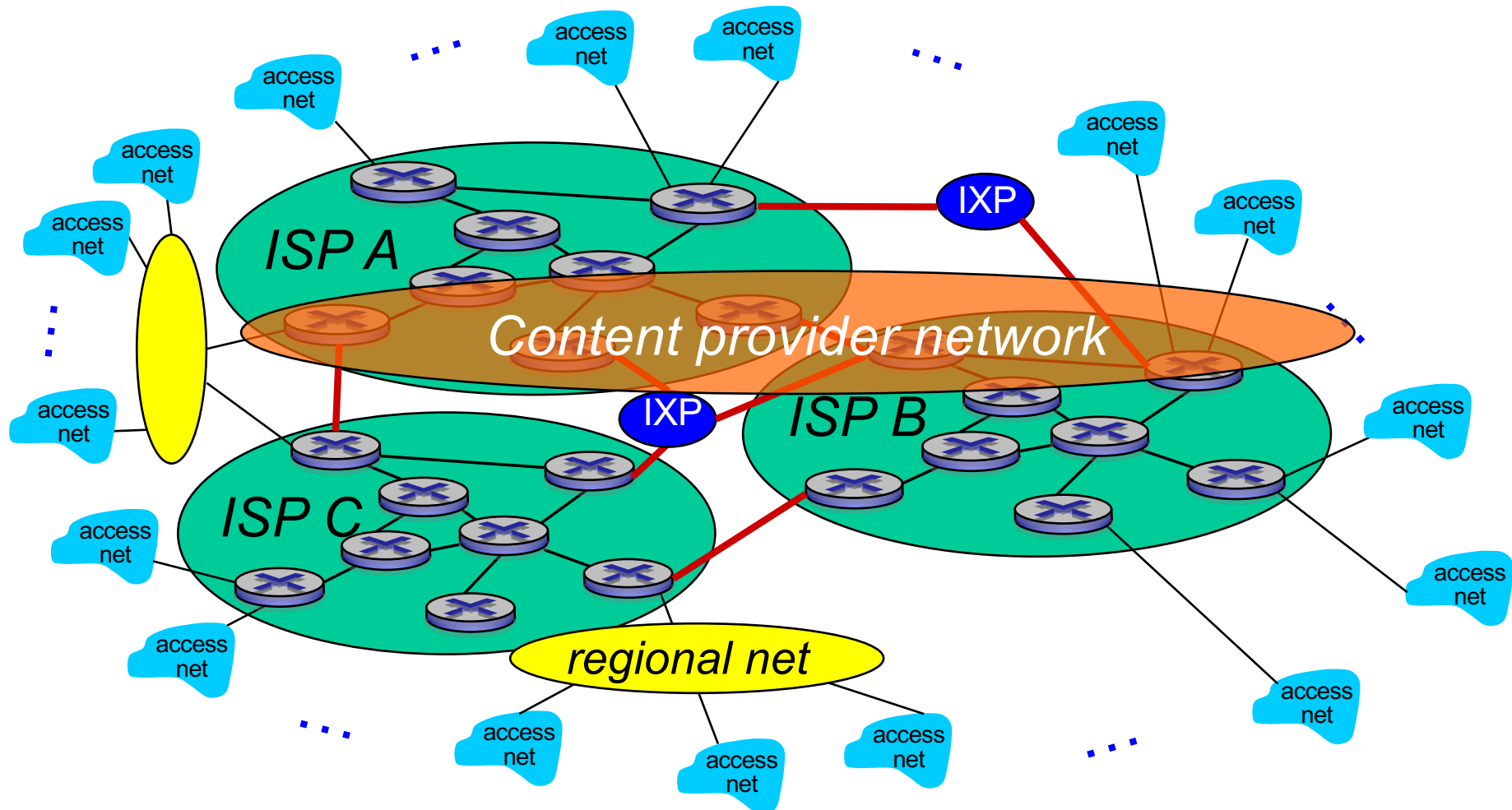*peering link*

access net

ISP A

ISP B

ISP C

IXP

IXP

Internet structure: network of networks

… and regional networks may arise to connect access nets to ISPs

Internet structure: network of networks

… and content provider networks (e.g., Google, Microsoft, Akamai) may run their own network, to bring services, content close to end users

Internet structure: network of networks
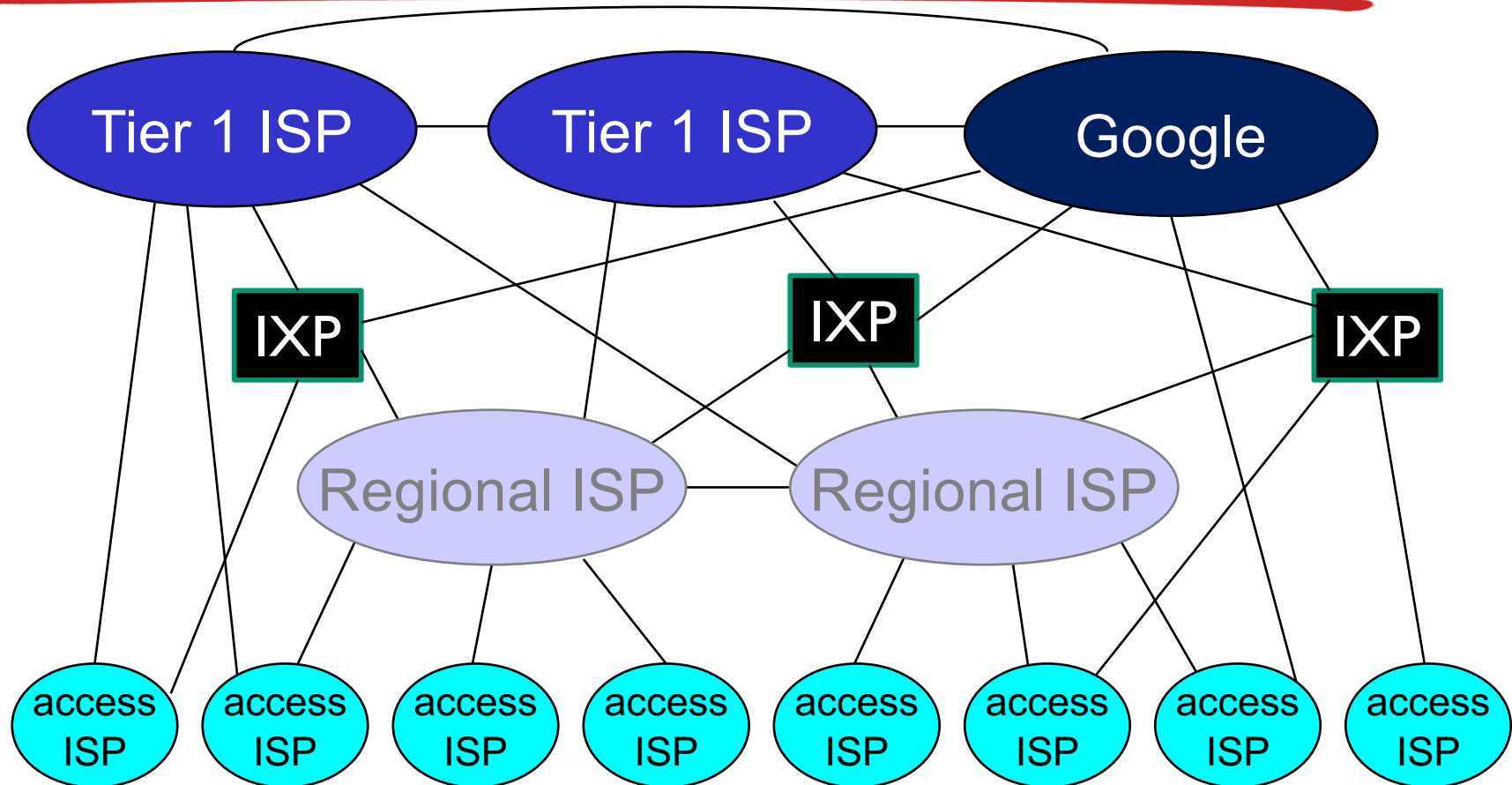
❑ at center: small # of well-connected large networks

  ❍ "tier-1" commercial ISPs (e.g., Level 3, Sprint, AT&T, NTT), national & international coverage

  ❍ content provider network (e.g., Google): private network that connects its data centers to Internet, often bypassing tier-1, regional ISPs

Tier-1 ISP: e.g., Sprint
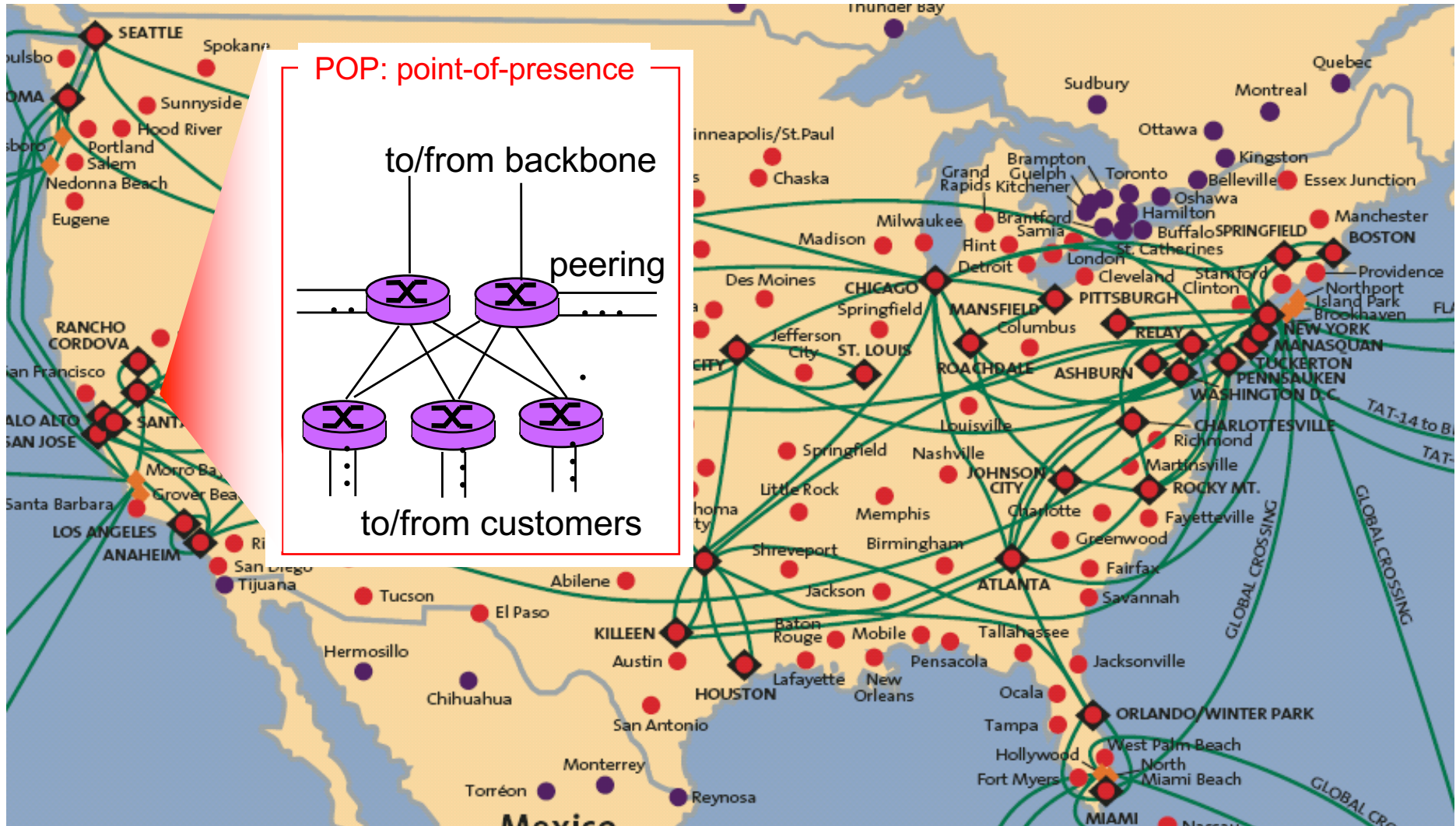
POP: point-of-presence

to/from backbone

peering

to/from customers

Chapter 1: roadmap

How do loss and delay occur?

packets *queue* in router buffers

❑ packet arrival rate to link exceeds output link capacity

❑ packets queue, wait for turn

packet being transmitted (delay)

packets queueing (delay)

free (available) buffers: arriving packets dropped (loss) if no free buffers
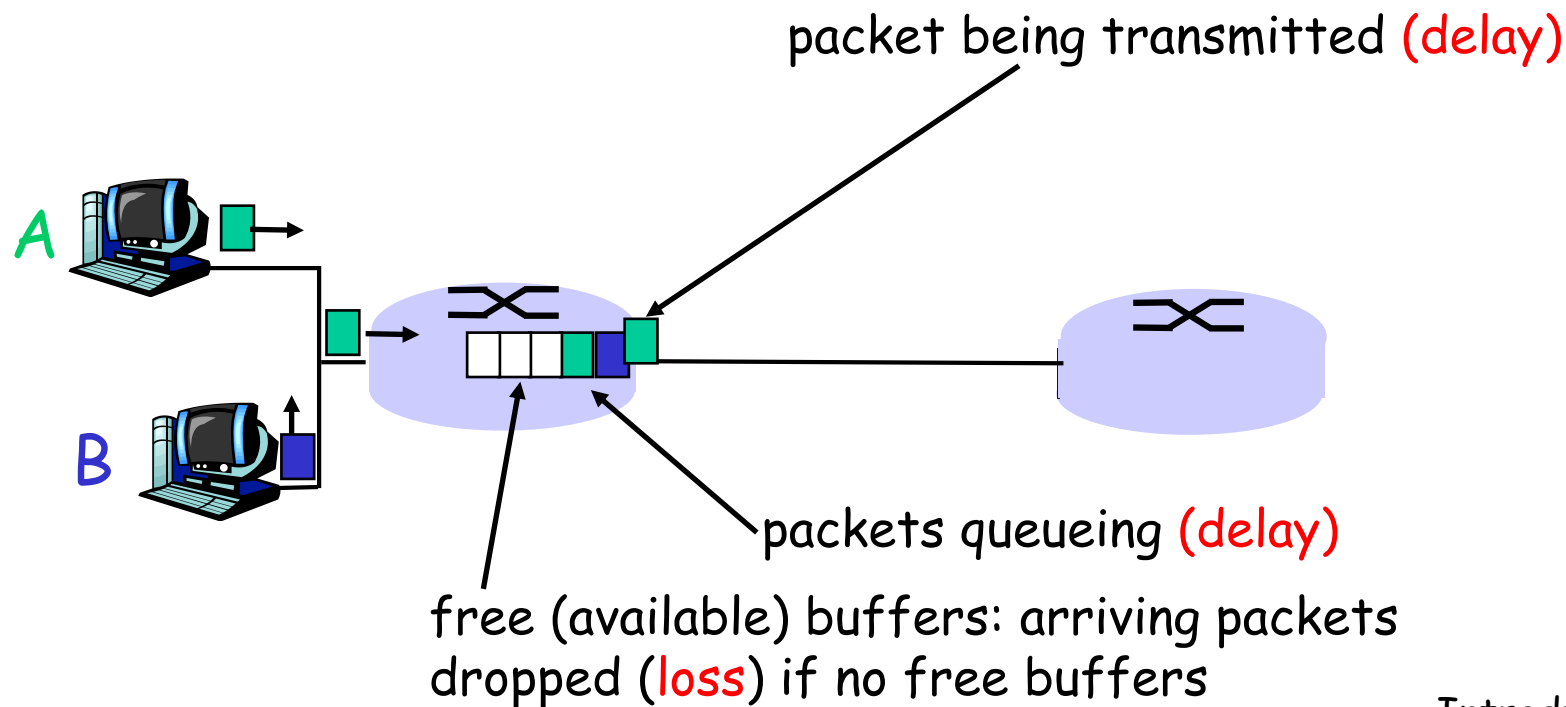
Four sources of packet delay

❑ **1. nodal processing:**
- ○ check bit errors
- ○ determine output link

❑ **2. queueing**
- ❖ time waiting at output link for transmission
- ❖ depends on congestion level of router

A

B

transmission

propagation

nodal processing

queueing
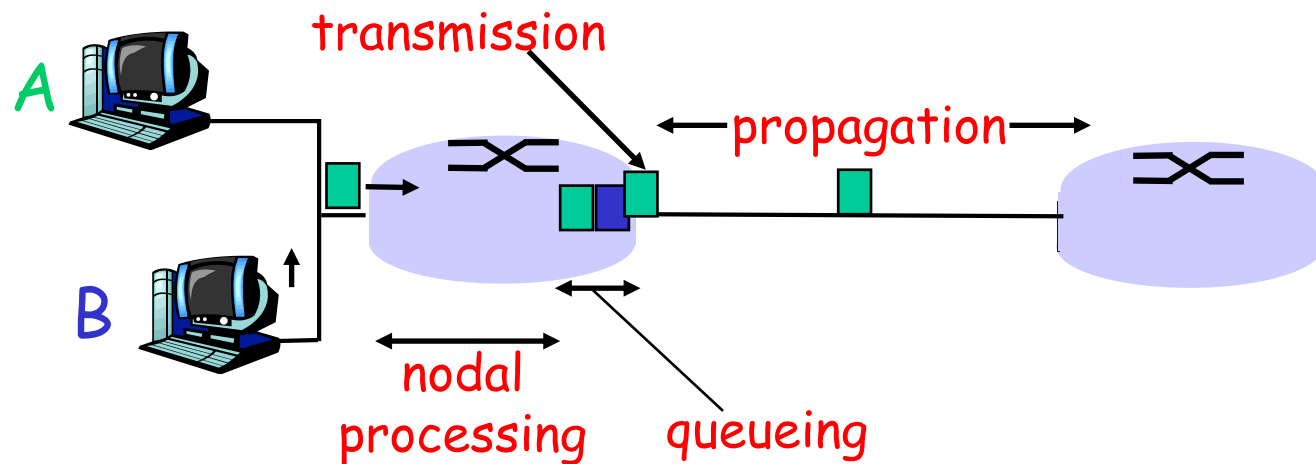
Delay in packet-switched networks

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 (~2x10^8 m/sec)
- propagation delay = d/s

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

A

B

transmission

propagation

nodal processing

queueing

Caravan analogy

ten-car caravan
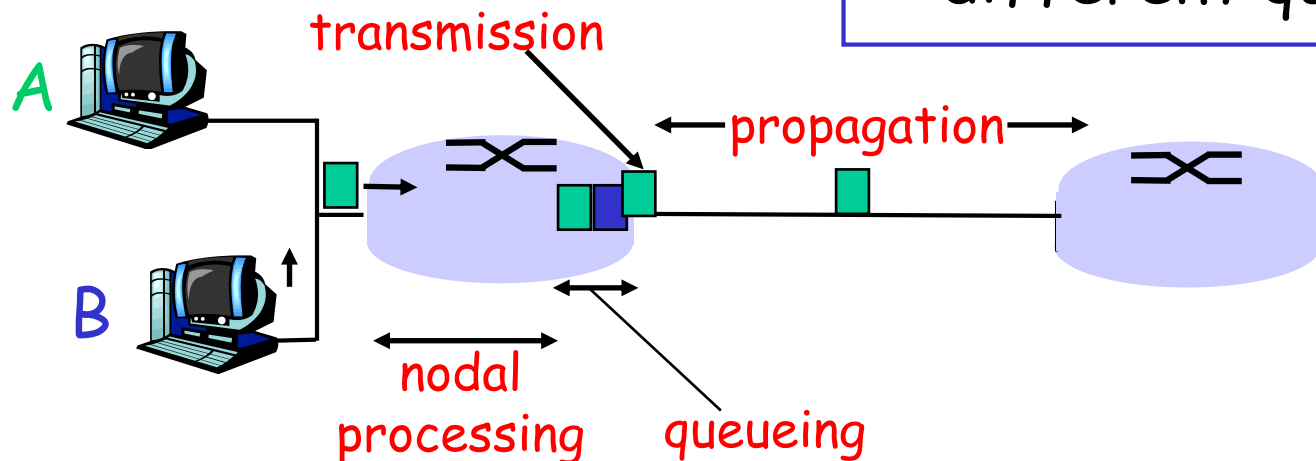
toll booth

100 km
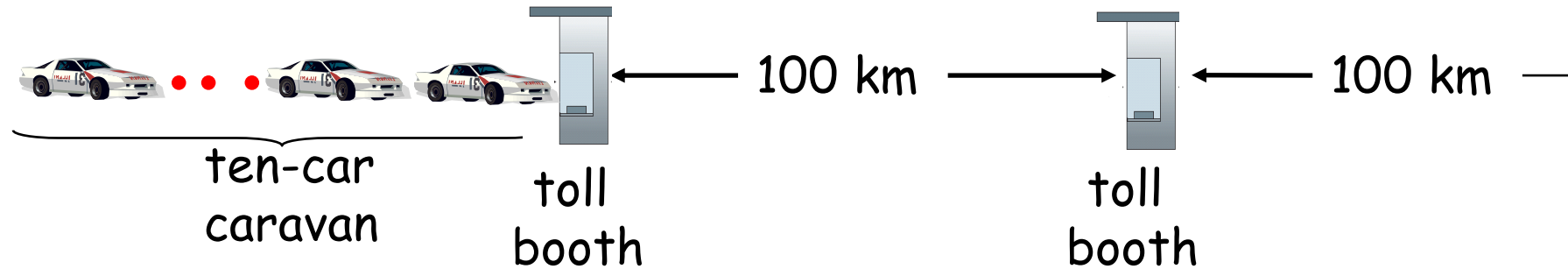
toll booth

100 km

- cars "propagate" at 100 km/hr
- toll booth takes 12 sec to service car (transmission time)
- car~bit; caravan ~ packet
- 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
- Time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr
- A: 62 minutes

Caravan analogy (more)

ten-car caravan

toll booth

← 100 km →

← 100 km —
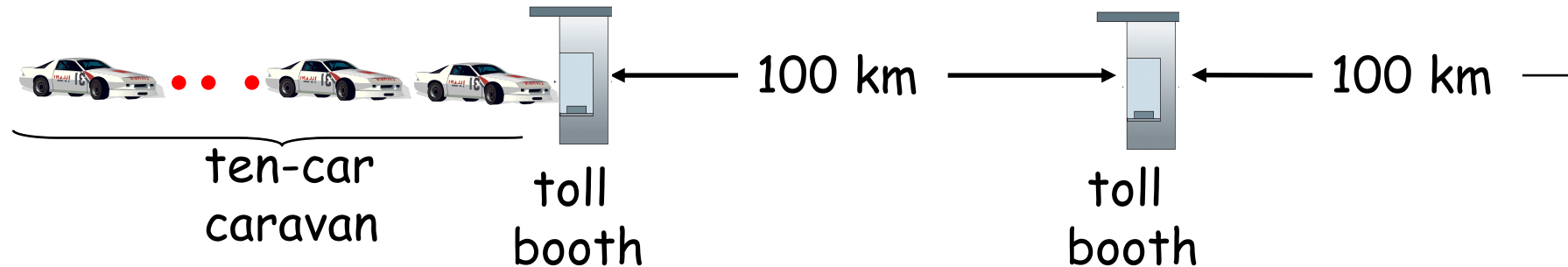
toll booth

- Cars now "propagate" at 1000 km/hr
- Toll booth now takes 1 min to service a car
- Q: Will 1st car arrive at 2nd booth before all cars serviced at 1st booth?

- Yes! After 7 min, 1st car 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!
  - See Ethernet applet at AWL Web site

Nodal delay

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

- ❏ d_{proc} = processing delay
  - ○ typically a few microsecs or less
- ❏ d_{queue} = queuing delay
  - ○ depends on congestion
- ❏ d_{trans} = transmission delay
  - ○ = L/R, significant for low-speed links
- ❏ d_{prop} = propagation delay
  - ○ a few microsecs to hundreds of msecs

Queueing delay (revisited)

- R=link bandwidth (bps)
- L=packet length (bits)
- a=average packet arrival rate

traffic intensity = La/R

average queueing delay

La/R

1
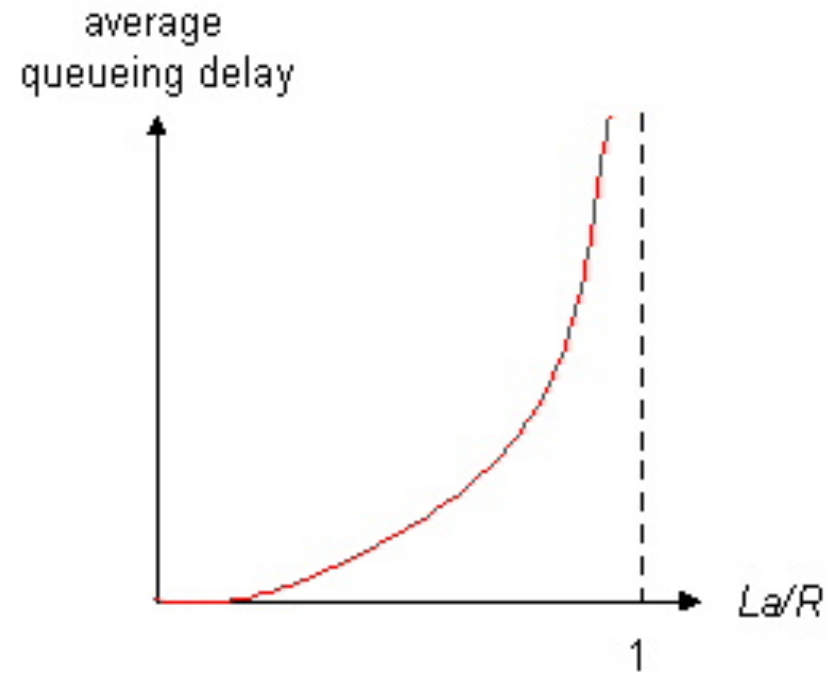
- La/R ~ 0: average queueing delay small
- La/R -> 1: delays become large
- La/R > 1: more "work" arriving than can be serviced, average delay infinite!

"Real" Internet delays and routes

❑ What do "real" Internet delay & loss look like?

❑ **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.

3 probes   3 probes

3 probes
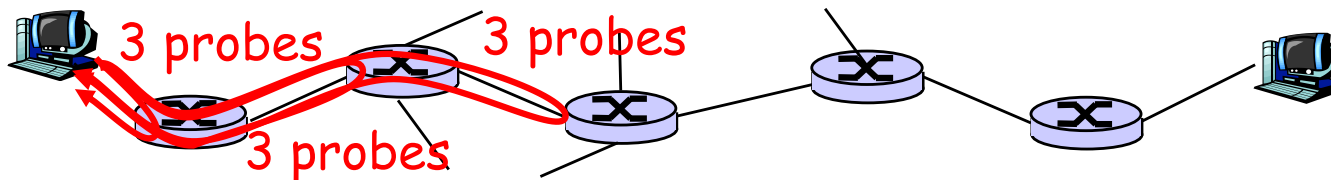
"Real" Internet delays and routes

traceroute: gaia.cs.umass.edu to www.eurecom.fr

Three delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

```
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
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
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
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

trans-oceanic link
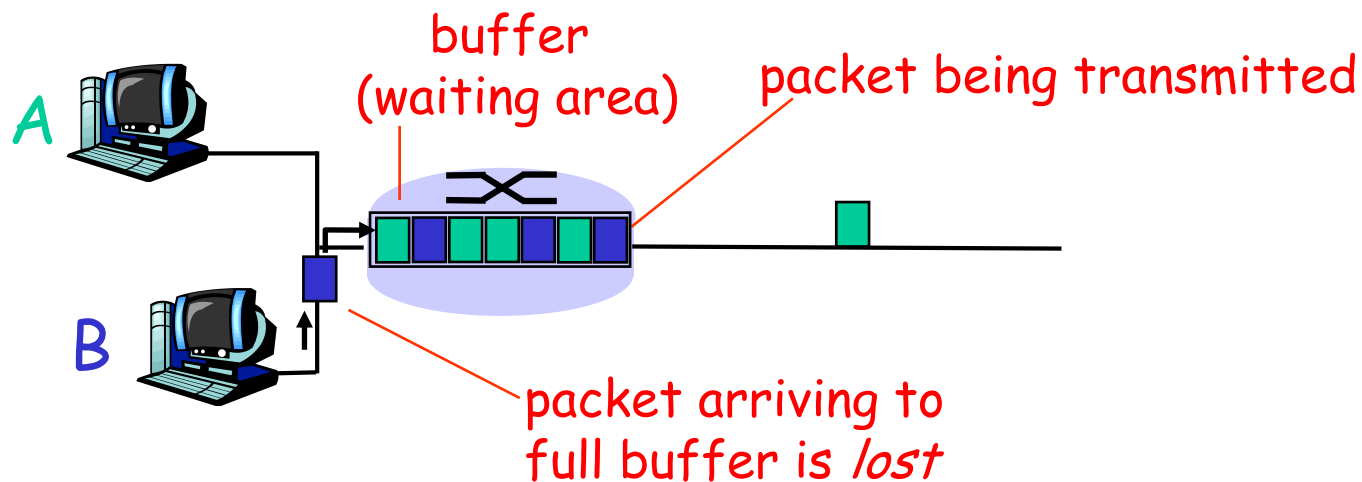
* means no response (probe lost, router not replying)

Quiz Time!

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

buffer
(waiting area)

packet being transmitted

A

B

packet arriving to
full buffer is *lost*

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

server sends bits
(fluid) into pipe

pipe that can carry
fluid at rate
R_s bits/sec)

pipe that can carry
fluid at rate
R_c bits/sec)
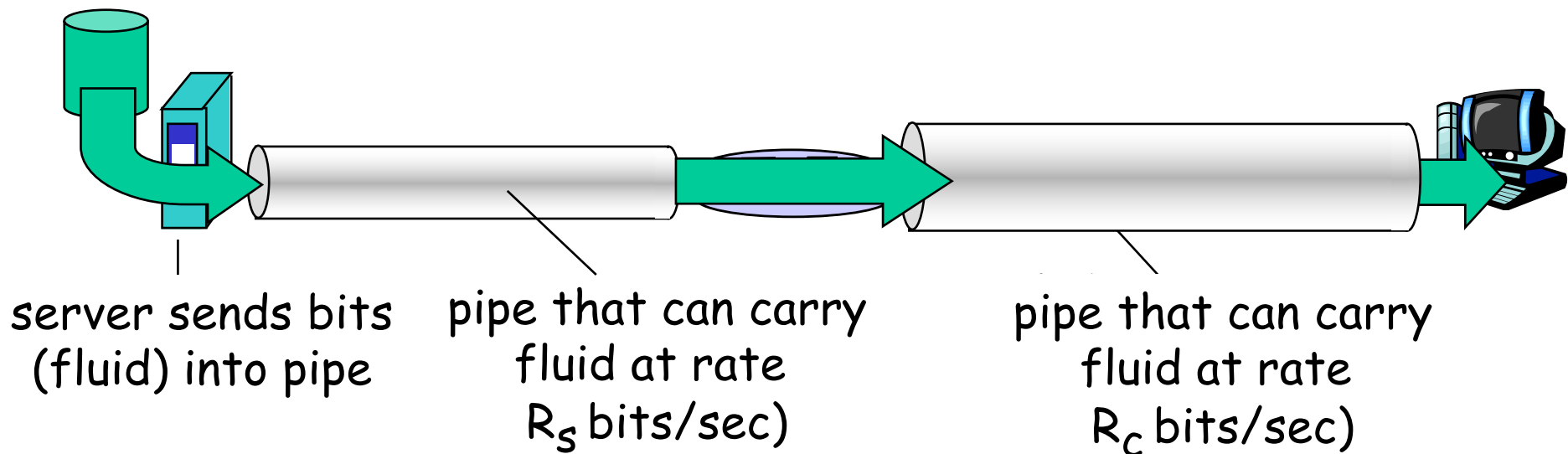
Throughput (more)

- $R_s < R_c$ What is average end-end throughput?

R_s bits/sec R_c bits/sec

- $R_s > R_c$ What is average end-end throughput?

R_s bits/sec R_c bits/sec
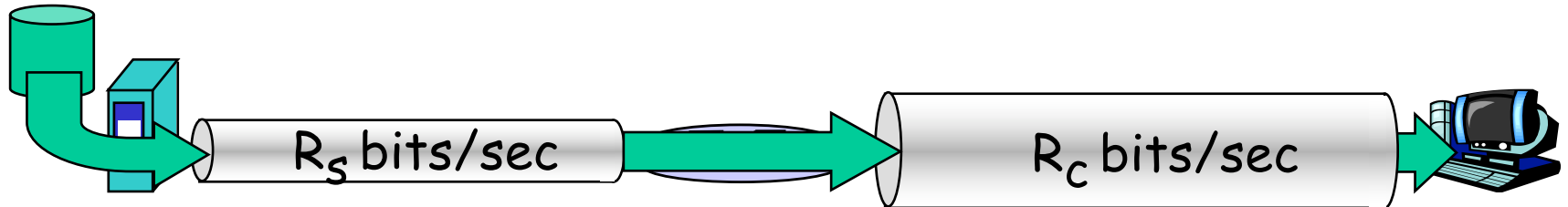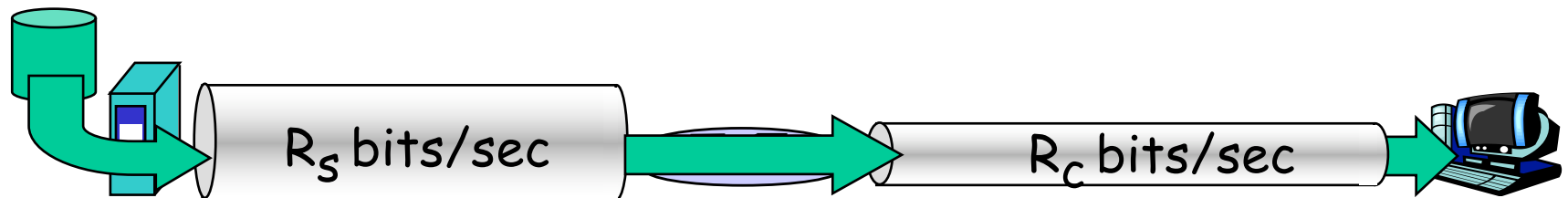
bottleneck link

link on end-end path that constrains end-end throughput

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

R_s
R_s
R_s
R_s
R
R_c
R_c
R_c
R_c
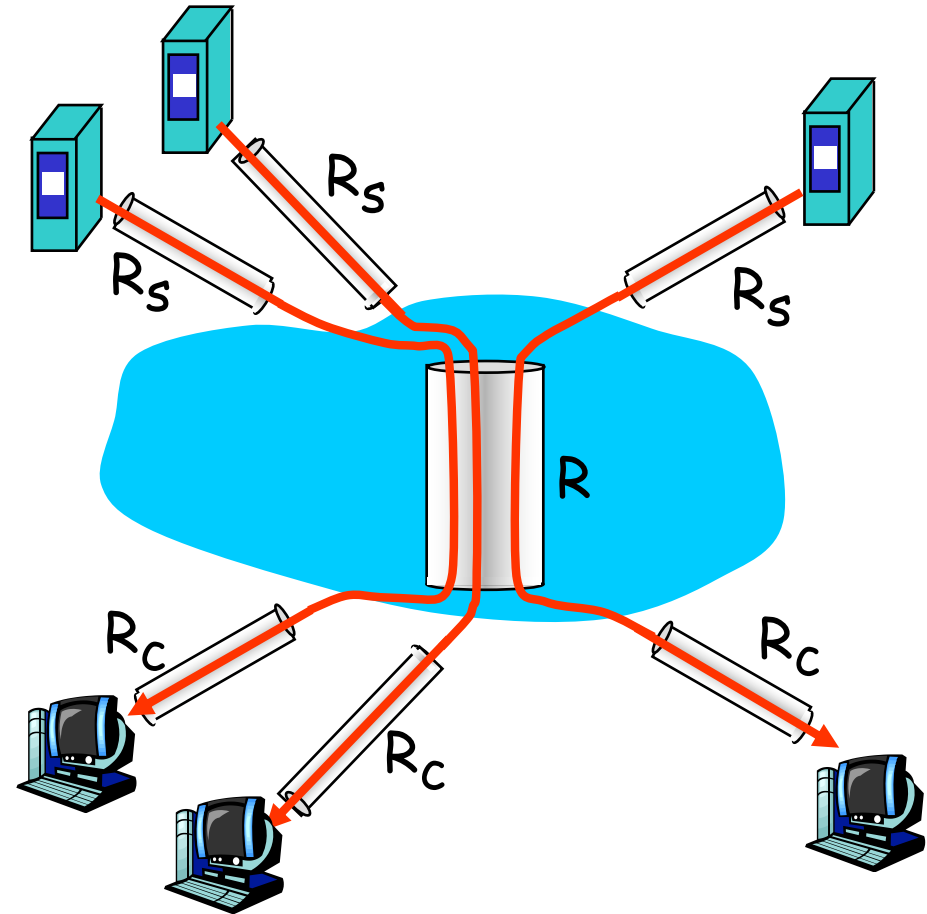
10 connections (fairly) share backbone bottleneck link R bits/sec

Chapter 1: roadmap

Protocol "Layers"

Networks are complex!

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

Question:

Is there any hope of *organizing* the "pieces" (of the network)?

Or at least our discussion of the network?

Organization of air travel

ticket (purchase)   ticket (complain)

baggage (check)   baggage (claim)

gates (load)   gates (unload)

runway takeoff   runway landing

airplane routing   airplane routing

airplane routing
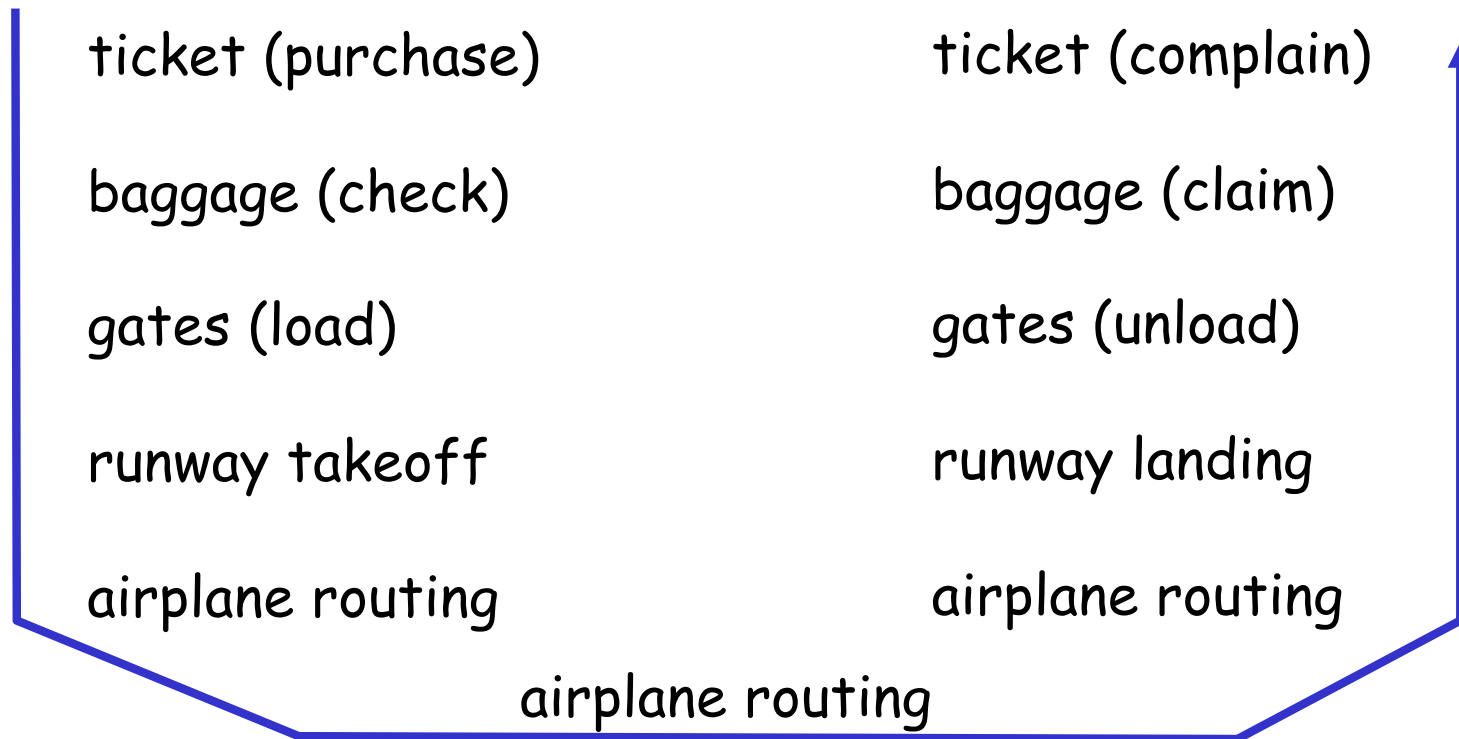
❑ a series of steps

Layering of airline functionality

departure airport	intermediate air-traffic control centers	arrival airport	
ticket (purchase)		ticket (complain)	ticket
baggage (check)		baggage (claim	baggage
gates (load)		gates (unload)	gate
runway (takeoff)		runway (land)	takeoff/landing
airplane routing	airplane routing airplane routing	airplane routing	airplane routing

departure
airport

intermediate air-traffic
control centers

arrival
airport

Layers: each layer implements a service

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

Why layering?

Dealing with complex systems:

❑ explicit structure allows identification, relationship of complex system's pieces
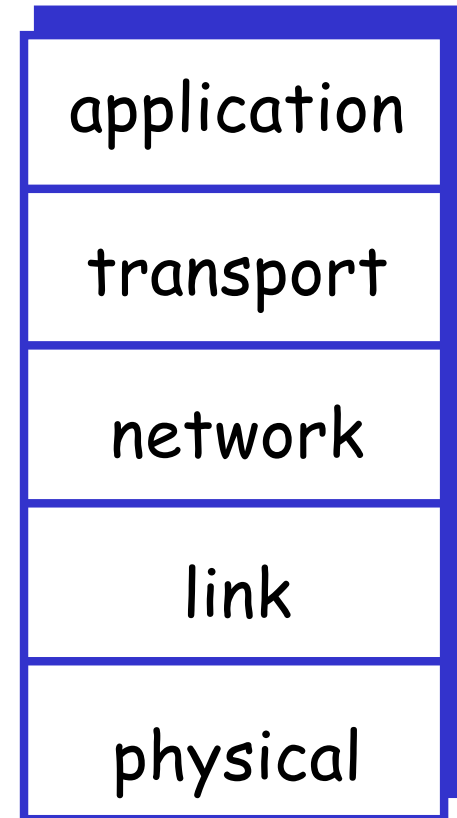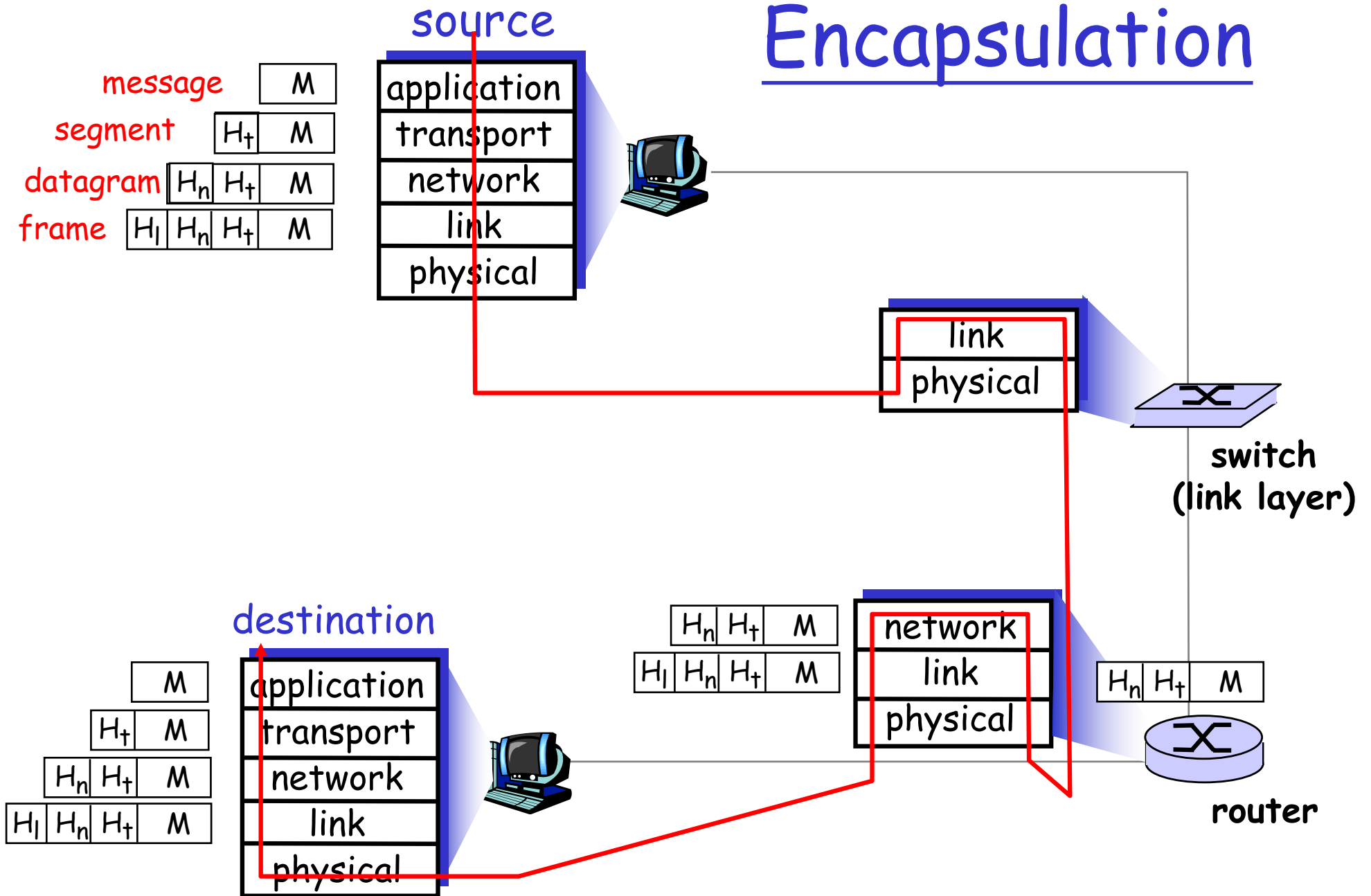
  ◻ layered reference model for discussion

❑ modularization eases maintenance, updating of system

  ◻ change of implementation of layer's service transparent to rest of system

  ◻ e.g., change in gate procedure doesn't affect rest of system

❑ layering considered harmful?

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"

application
transport
network
link
physical

Encapsulation

message	M
segment	H_t M
datagram	H_n H_t M
frame	H_l H_n H_t M

source

application
transport
network
link
physical

link
physical

switch (link layer)

destination

M	
H_t M	
H_n H_t M	
H_l H_n H_t M	

application
transport
network
link
physical

H_n H_t M
H_l H_n H_t M

network
link
physical

H_n H_t M

router

Chapter 1: roadmap

Network security

❏ **field of network security:**
- ○ 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: put malware into hosts via Internet

❑ malware can get in host from:

   ❍ *virus:* self-replicating infection by receiving/executing object (e.g., e-mail attachment)

   ❍ *worm:* self-replicating infection by passively receiving object that gets itself executed

❑ **spyware malware** can record keystrokes, web sites visited, upload info to collection site

❑ infected host can be enrolled in botnet, used for spam. DDoS attacks

Bad guys: attack server, 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 to target from
   compromised hosts

target
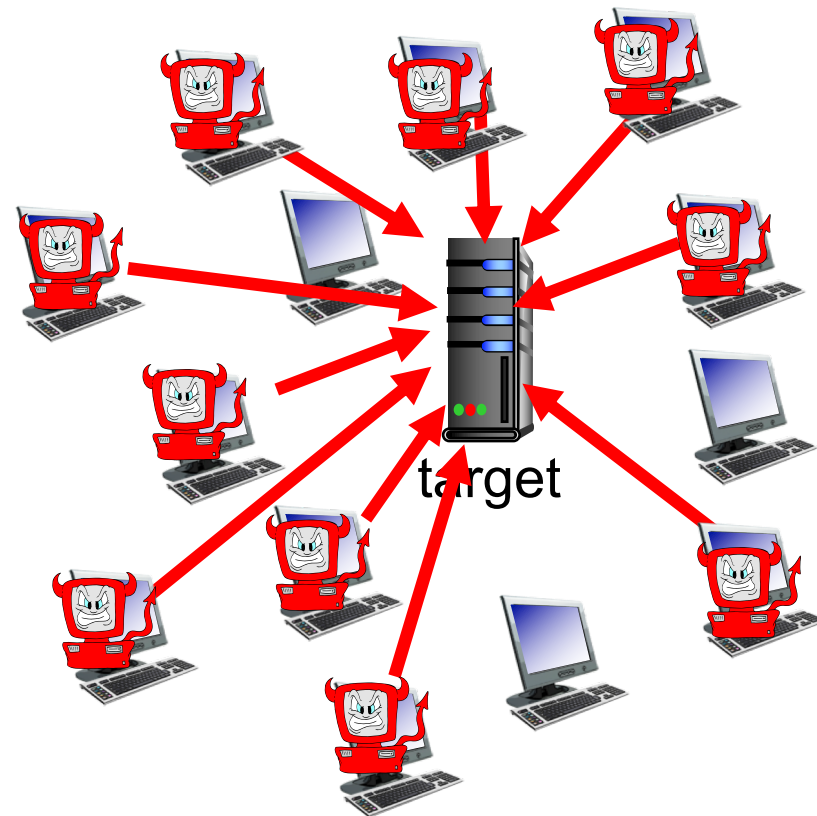
Bad guys can sniff packets

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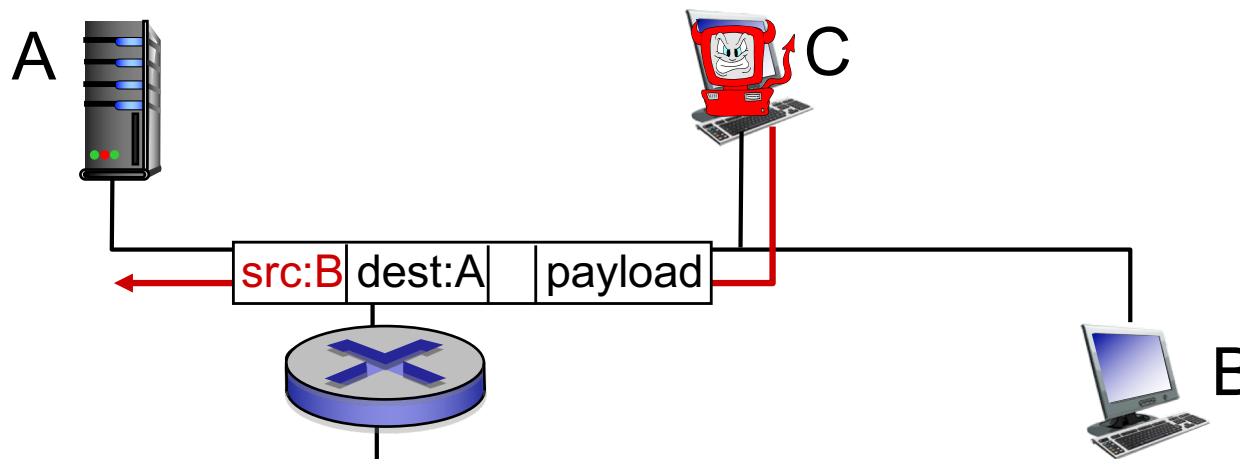
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by

A

C

src:B | dest:A | payload

B
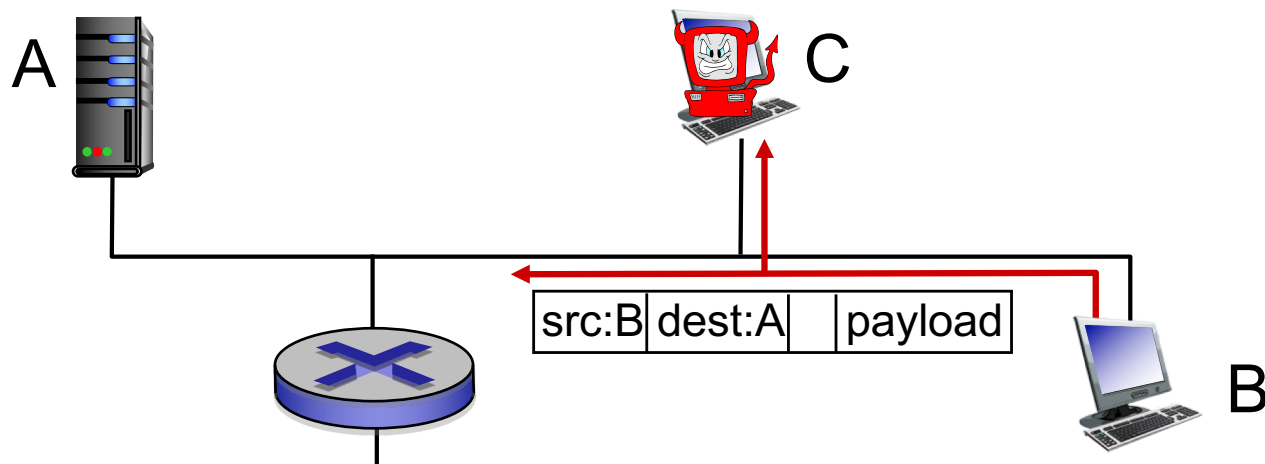
- wireshark software used for end-of-chapter labs is a (free) packet-sniffer

Bad guys can use fake addresses

IP spoofing: send packet with false source address

A

src:B | dest:A | payload

C

B

… lots more on security (throughout, Chapter 8)

Network Security

❑ more throughout this course

❑ chapter 8: focus on security

❑ crypographic techniques: obvious uses and not so obvious uses

Introduction: Summary

Covered a "ton" of material!

❑ Internet overview

❑ what's a protocol?

❑ network edge, core, access network

   ❍ packet-switching versus circuit-switching

   ❍ Internet structure

❑ performance: loss, delay, throughput

❑ layering, service models

❑ security

❑ history

You now have:

❑ context, overview, "feel" of networking

❑ more depth, detail *to follow!*