Data Communication and Computer Networks

1. Computer Networks & The Internet

Dr. Aiman Hanna

Department of Computer Science & Software Engineering
Concordia University, Montreal, Canada

These slides has mainly been extracted, modified and updated from original slides of :
Computer Networking: A Top Down Approach, 6th edition Jim Kurose, Keith Ross
Addison-Wesley, 2013

Additional materials have been extracted, modified and updated from:
Understanding Communications and Networking, 3e by William A. Shay 2005

History of Communications

For 1000s of years through auditory & visual senses

- Visual senses:
  - » Face to face
  - » Reading messages/letters/symbols/sketches
  - » Seeing visual signals (smoke, fire, ..etc).
  - » …
- Auditory senses:
  - » Direct listening
  - » Listening through messengers
  - » ...

History of Communications

- Drastic change in **1837**
  - The invention of the **telegraph** by Samuel Morse
  - Characters of a message were translated into long and short electrical impulses
  - These impulses were then transmitted over a copper wire
  - The association between the characters and the impulses was called **Morse Code**

- **1876**: The Magical invention of **Telephony** by Alexander Graham Bell
  - Bell showed that voice can be converted directly into electrical energy
  - This energy can then be transmitted over a wire using continuously varying voltages

History of Communications

- **Switchboards**
  - Early telephones required a pair of wires that connects telephones at both ends
  - That changed with the invention of the switchboard, a switching device that connected lines between two phones
  - Establishing connections was activated through an operator at the switchboard

OLD SWITCHBOARD OF BELL EXCHANGE SERVING CHINATOWN, SAN FRANCISCO CALIFORNIA

History of Communications

- **1945: ENIAC**
  - **E**lectronic **N**umerical **I**ntegrator **A**nd **C**alculator
  - The 1st electronic computer
  - Designed for computing ballistics for World War II
  - Although did not play a direct role in communication, it did show that calculations and decision making could be done electronically

- **1947:** The **Transistor**
  - Allowed smaller and affordable computers to be built
  - Computers applications developed during the 1960s made routing and processing telephone calls economically possible
  - The increased utilization of computers by businesses resulted in a growing need to transfer information between these computers as well

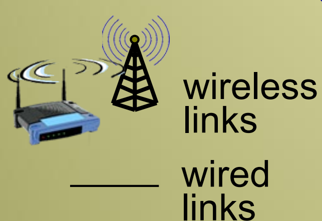
History of Communications

- **Electronic Communications -**
  The massive need in relatively short time
  - The 1st form of communication between systems were done through magnetic *tapes*
  - Information were copied from on system into a tape; which is transferred to another system, possibly a remote one
  - The development of the Personal Computer (PC) in the 1980s was a milestone in electronic communication
  - The infusion of millions of PCs into, virtually, everywhere created a further massive need to make information easily accessible
  - At this point it was clear that the need for electronic communication was no longer a luxury, rather a necessity and a must

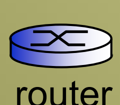
- **1990s:** The **World Wide Web (WWW)** & The **Internet**
  - WWW is *application* that enabled information from around the world to become easily accessible from one's desk.
  - The Internet is an electronic network of computers that includes nearly every university, government, and research facility in the world, as well as many commercial sites
  - The Internet started with four interconnected computers in 1969 and was known as ARPAnet

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

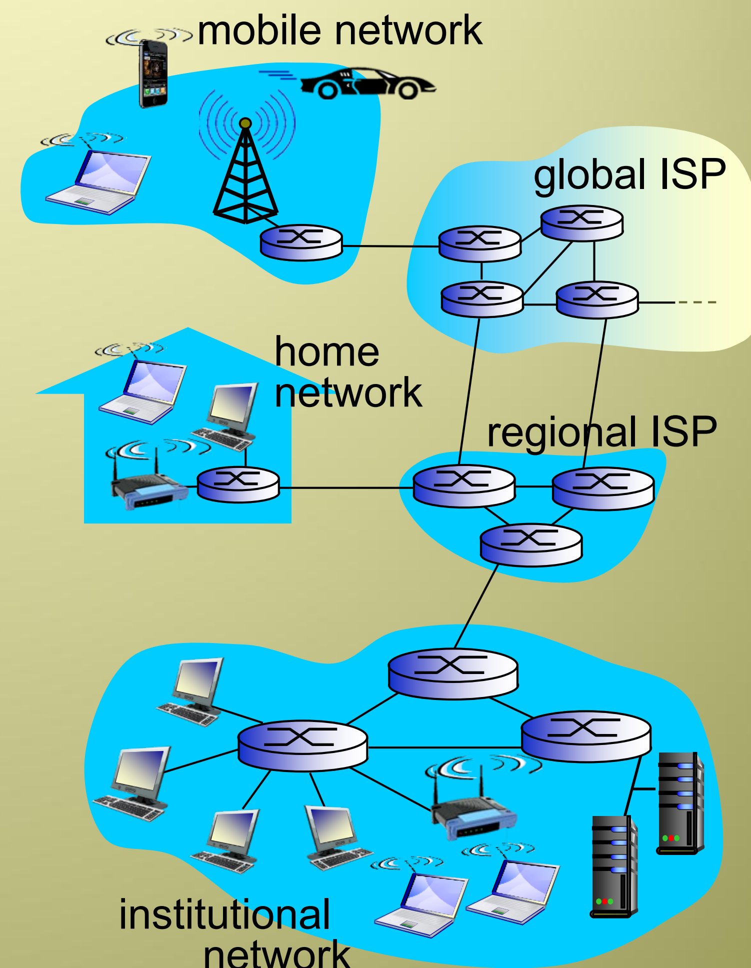
- millions of connected computing devices:
  - *hosts* = *end systems*
  - running *network apps*



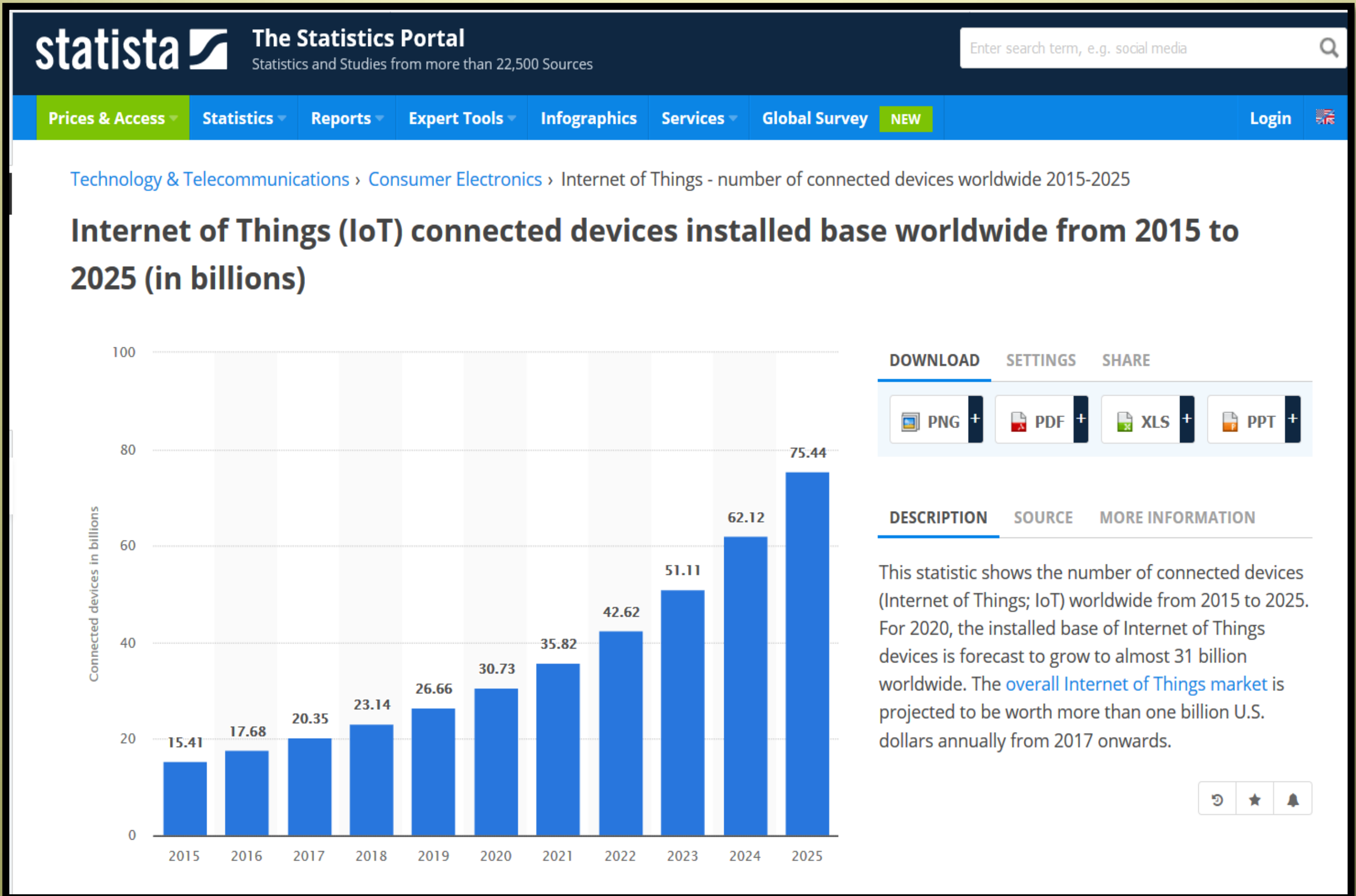
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate: *bandwidth*



- *Packet switches:* forward packets (chunks of data)
  - *routers* and *switches*

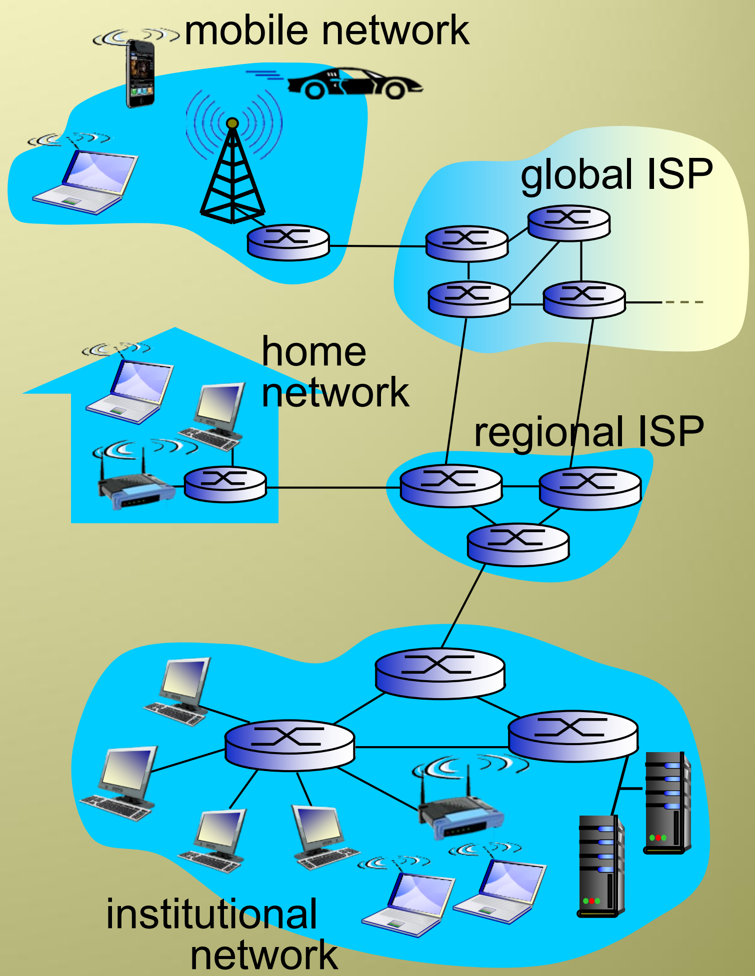


"Computer Networks"; an Outdated Term?



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

- *Internet:* "network of networks"
  - Interconnected ISPs
- *protocols* control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, Skype, 802.11
- *Internet standards*
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force



“Fun” Internet appliances

Internet refrigerator

Web-enabled toaster:
Designs, weather, news, etc.

Tweet-a-watt:
monitor energy use

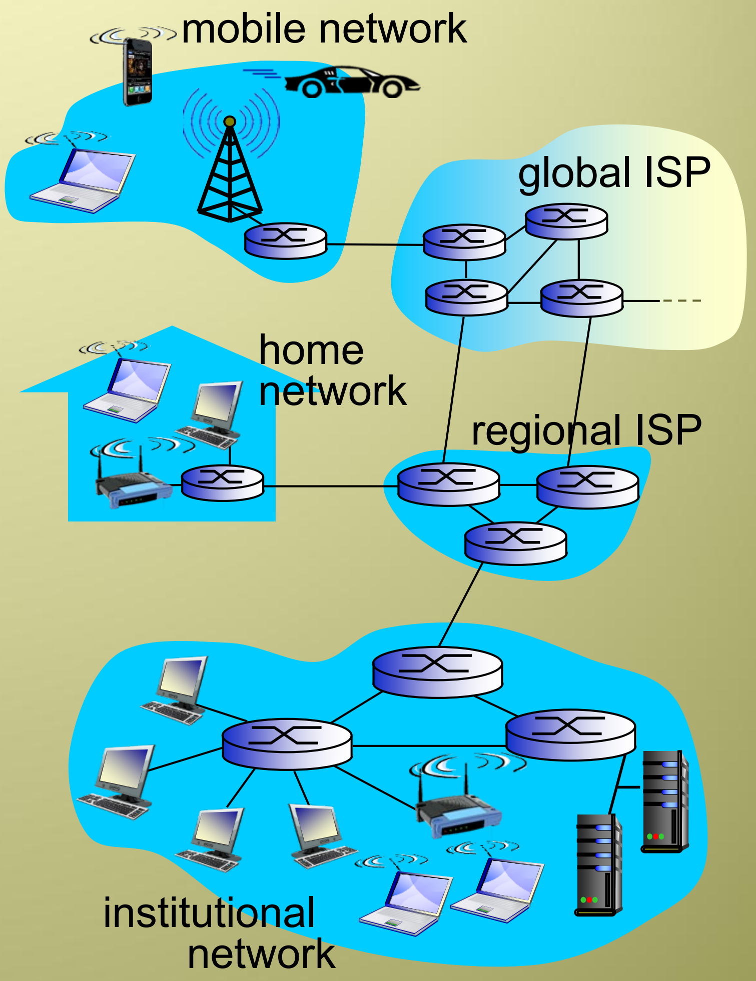
PoIP: IP picture frame
http://www.ceiva.com/

Slingbox:
Control & watch cable TV remotely

Internet phones

What's the Internet: a service view

- *Infrastructure that provides services to applications:*
  - Web, VoIP, email, games, e-commerce, social nets, …
  - Distributed applications
- *provides programming interface to apps*
  - hooks that allow sending and receiving app programs to "connect" to Internet
  - Provides various service options, analogous to postal service



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

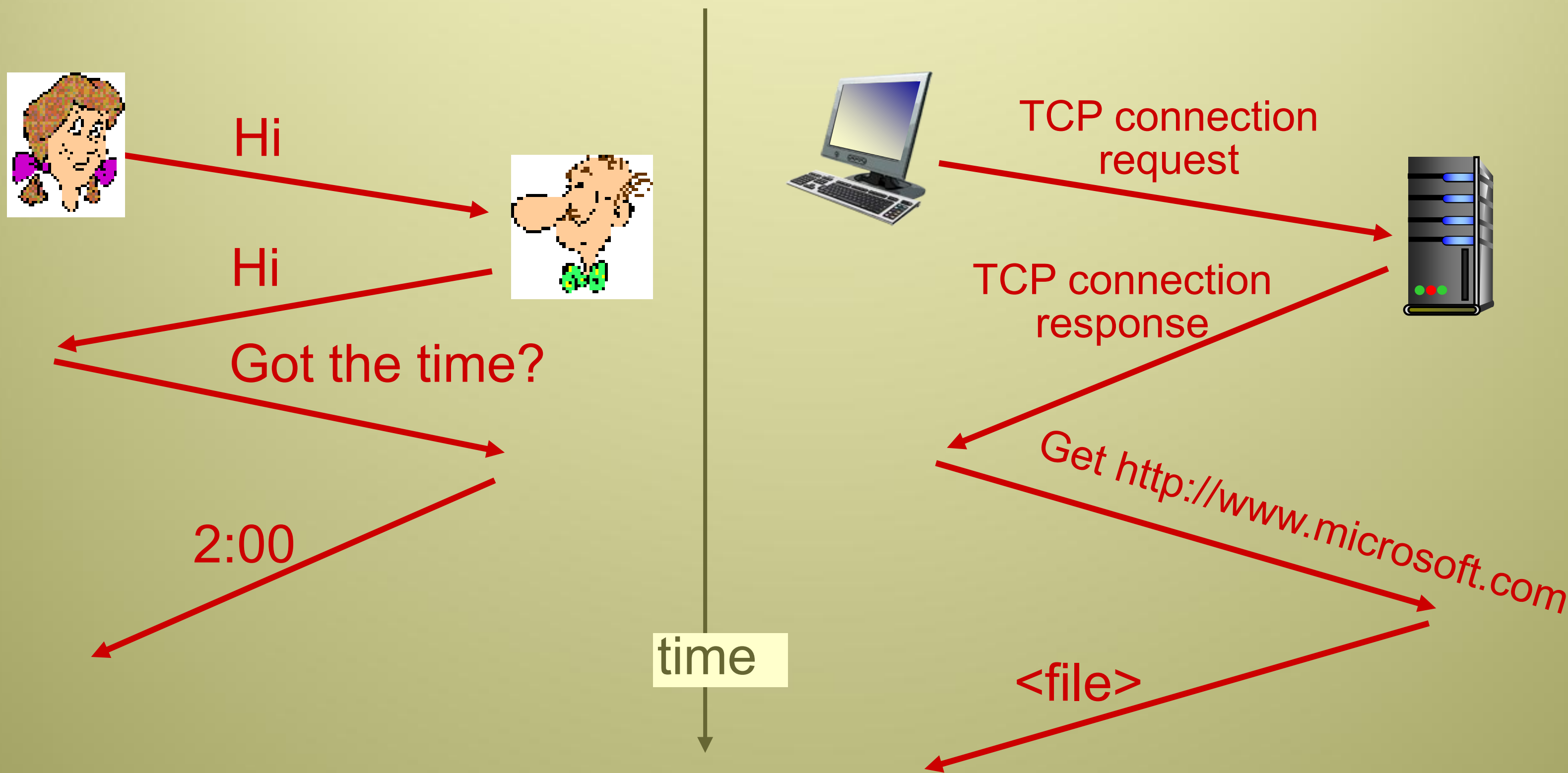
network protocols:

- 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?

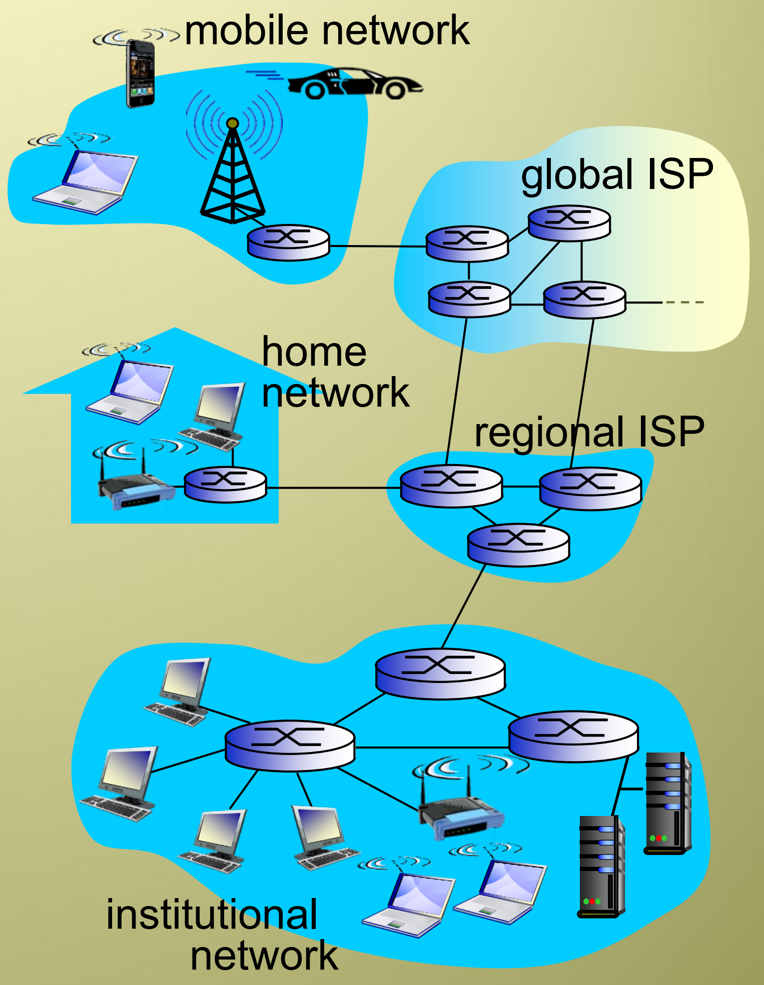
a human protocol and a computer network protocol:



Q: other human protocols?

A closer look at network structure:

- *network edge:*
  - Hosts/end systems: clients and servers
  - servers often in data centers
- *access networks, physical media:* wired, wireless communication links
- *network core:*
  - interconnected routers
  - network of networks



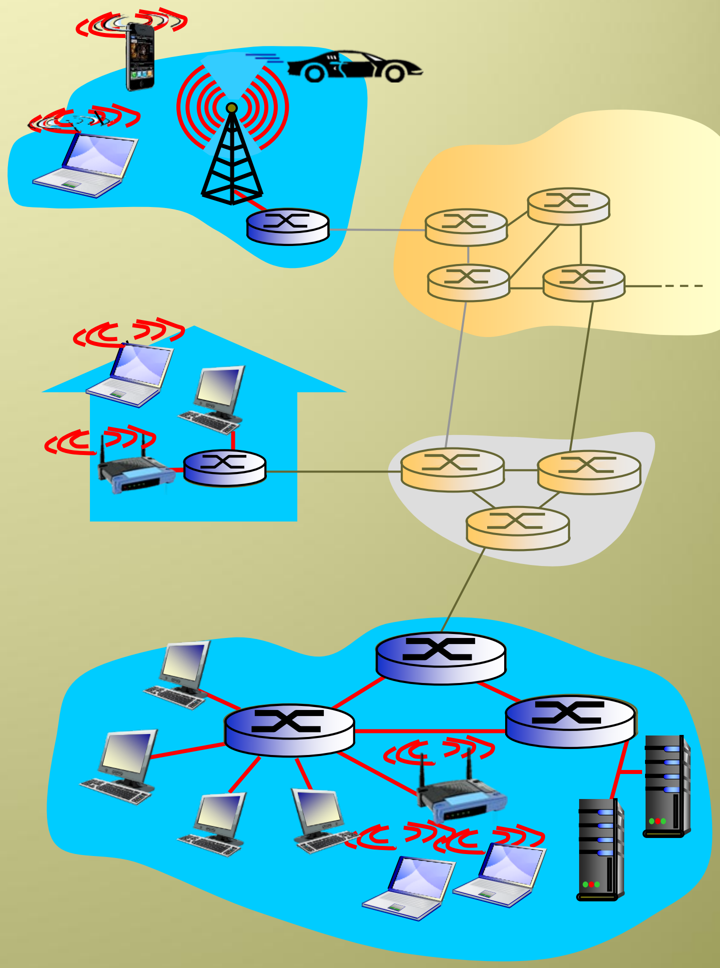
Access networks and physical media

Q: How to connect end systems to edge router?

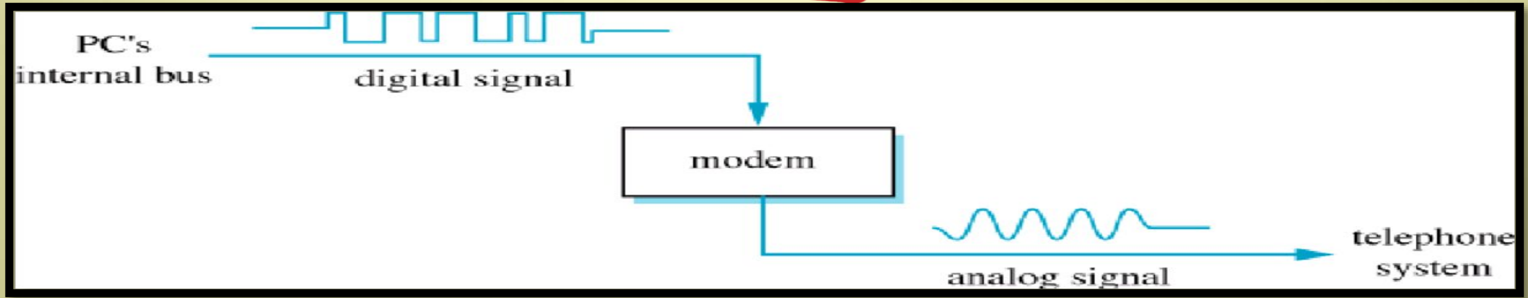
- residential access nets
- institutional access networks (school, company)
- mobile access networks

keep in mind:

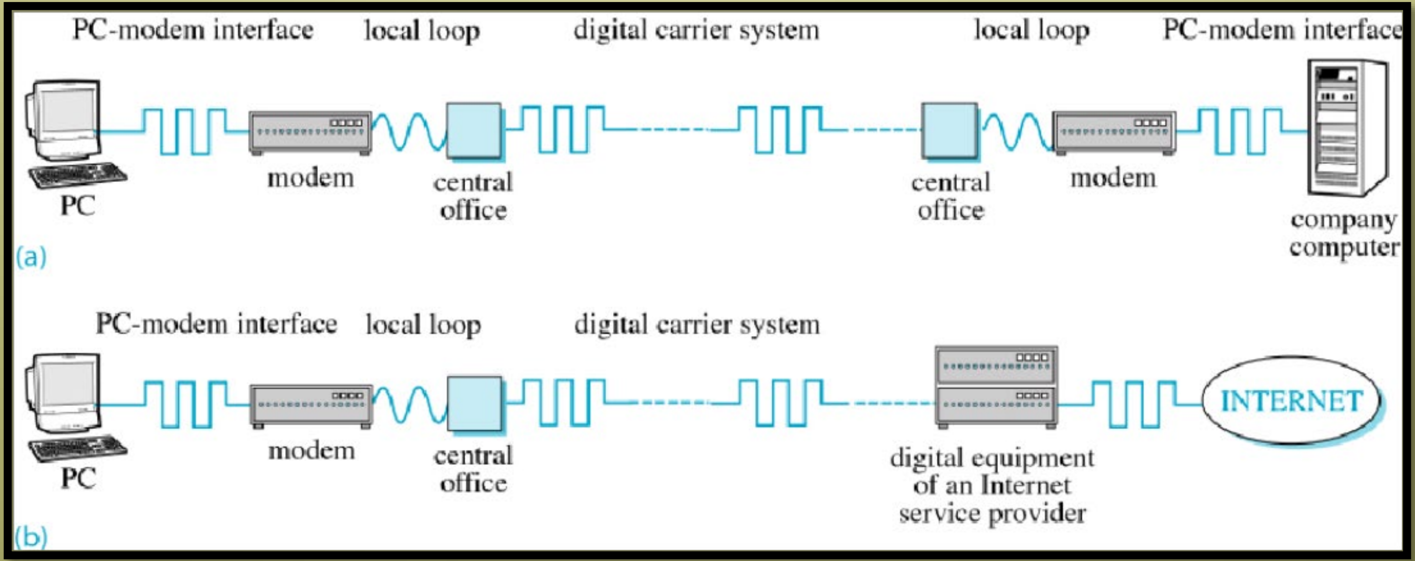
- bandwidth (bits per second) of access network?
- shared or dedicated?



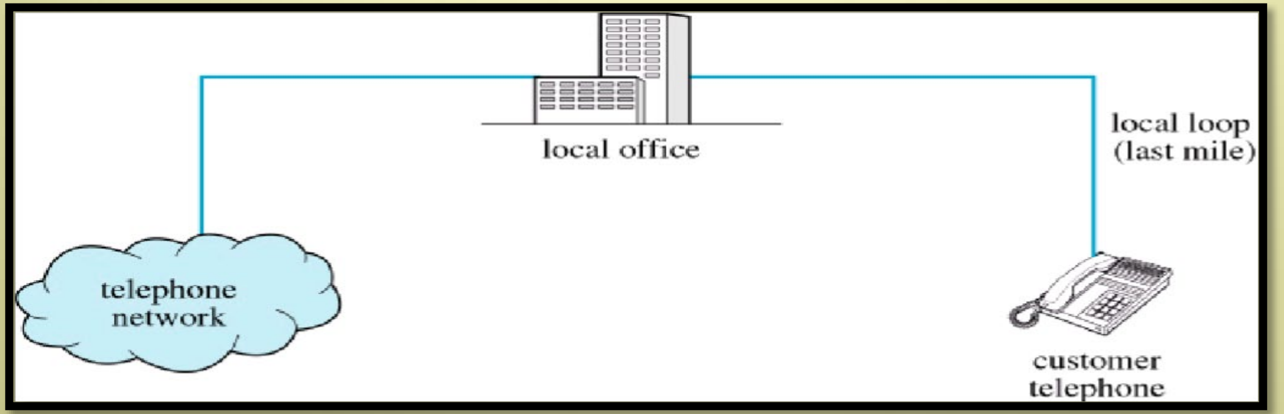
Modems and early ISP connections



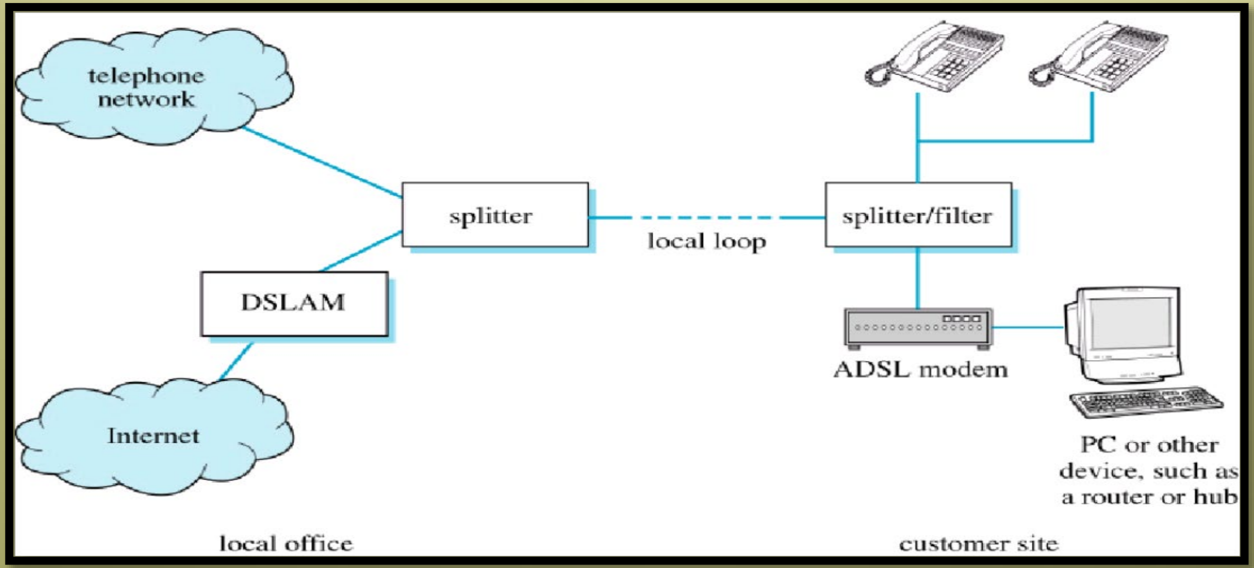
- During the 1980s, 2400 & 9600 bps modems became common
- In early 1990s, modems with a rate of 28.8 and 33.6 kbps became common
- Not longer after that, 56 kbps modems were achievable when connecting directly with ISPs



Access net: digital subscriber line (DSL)

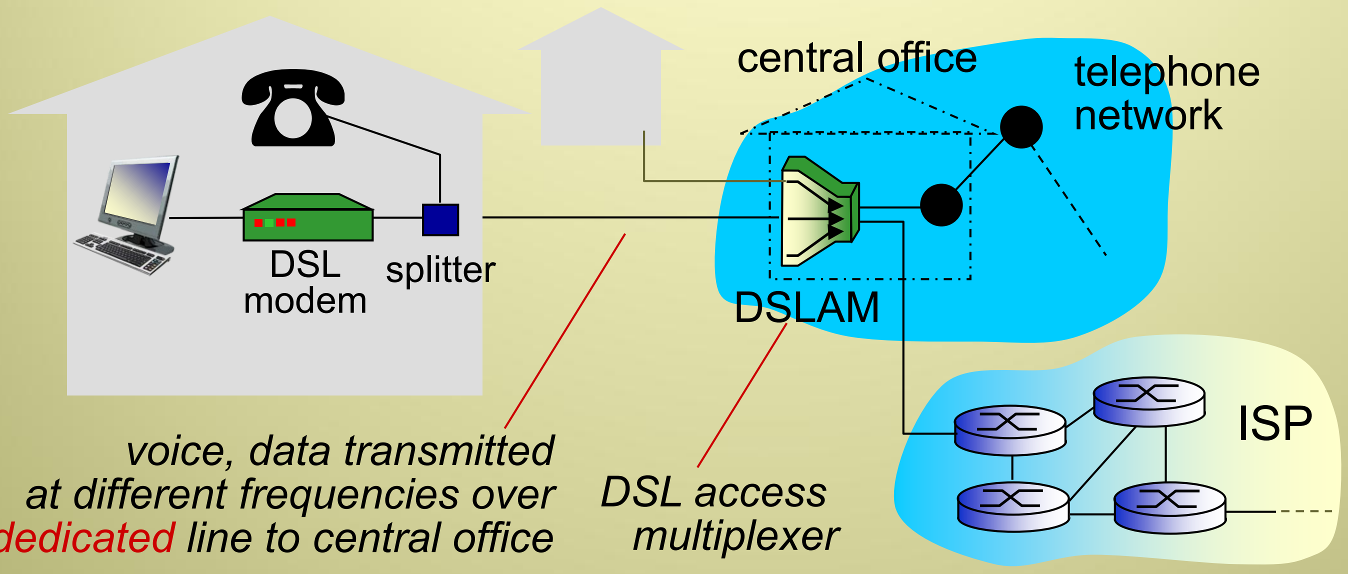


Local Loop - POTS (Plain Old Telephone Service) Configuration



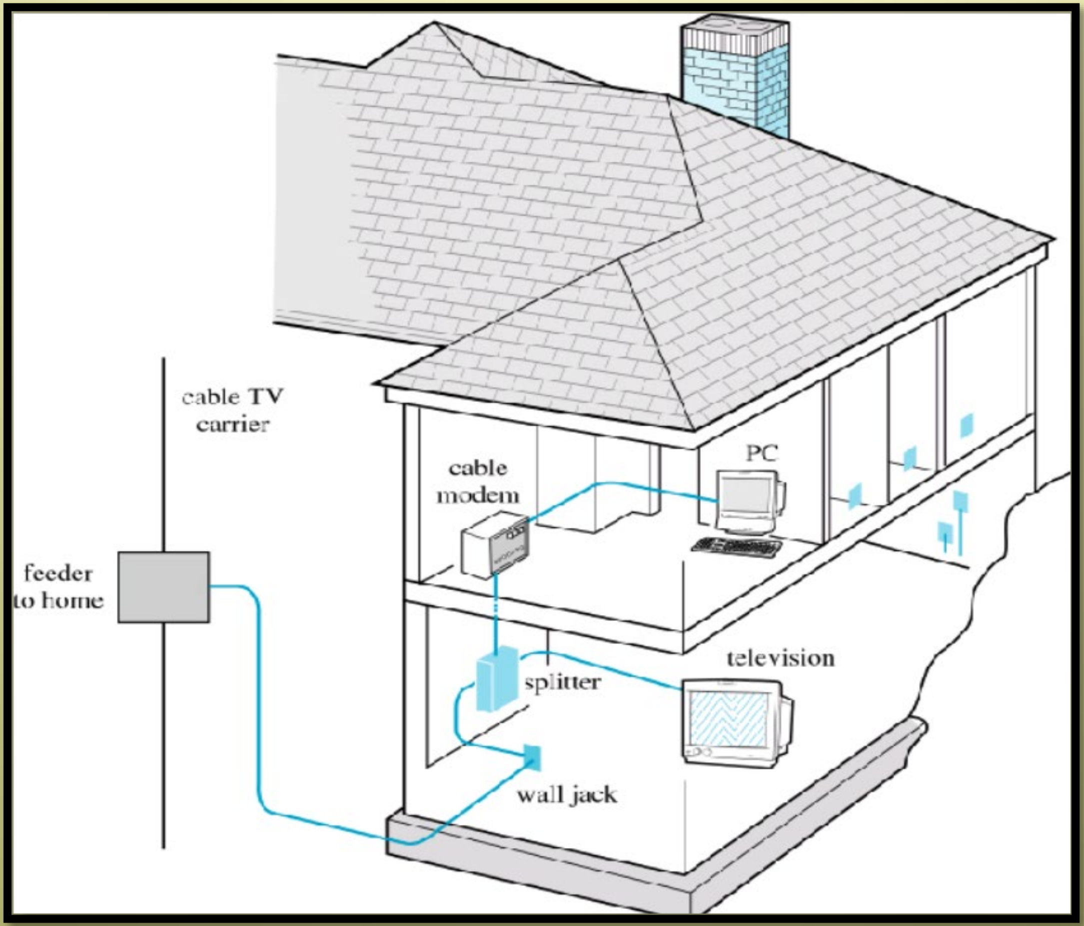
Asymmetric DSL (ADSL) Connection

Access net: digital subscriber line (DSL)



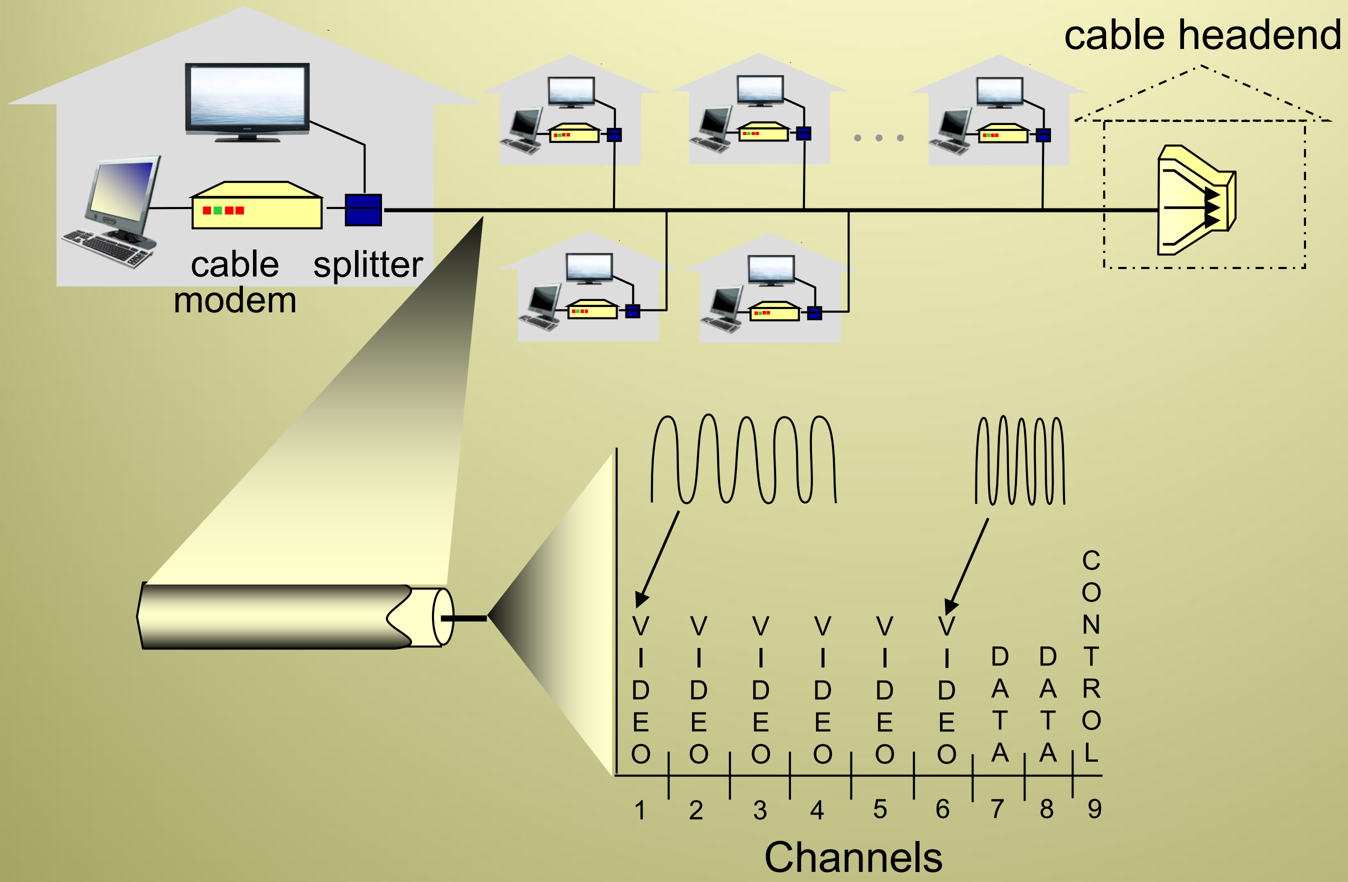
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access net: cable network



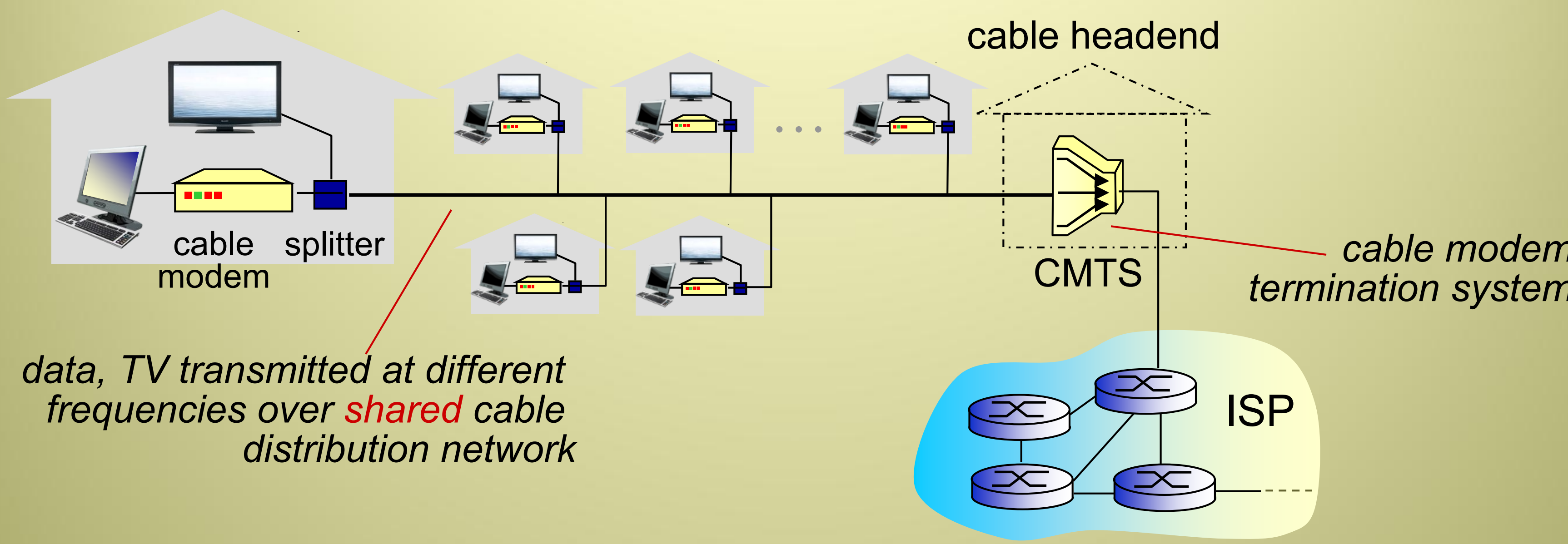
Cable Internet Access

Access net: cable network



frequency division multiplexing: different channels transmitted in different frequency bands

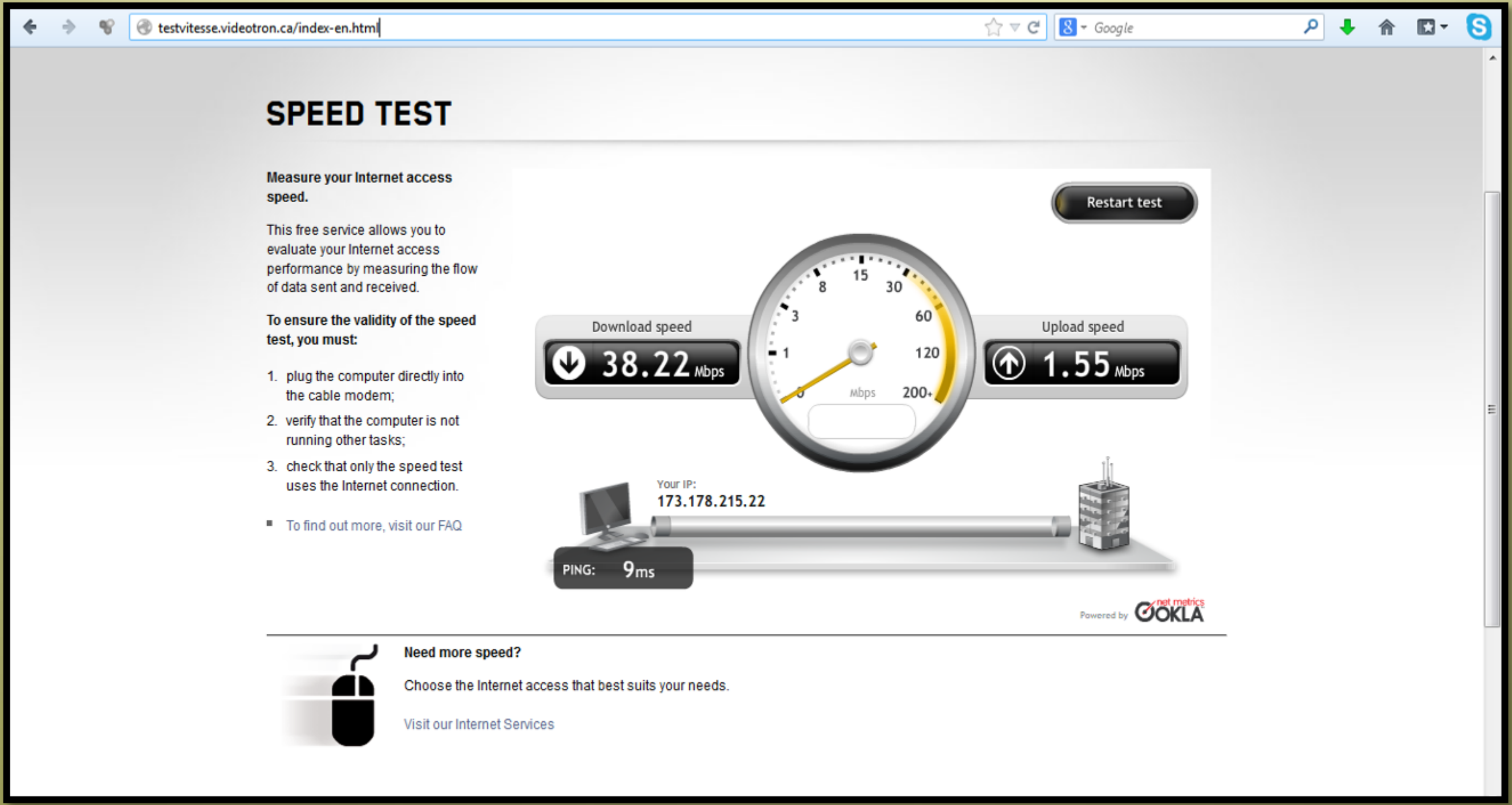
Access net: cable network



- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

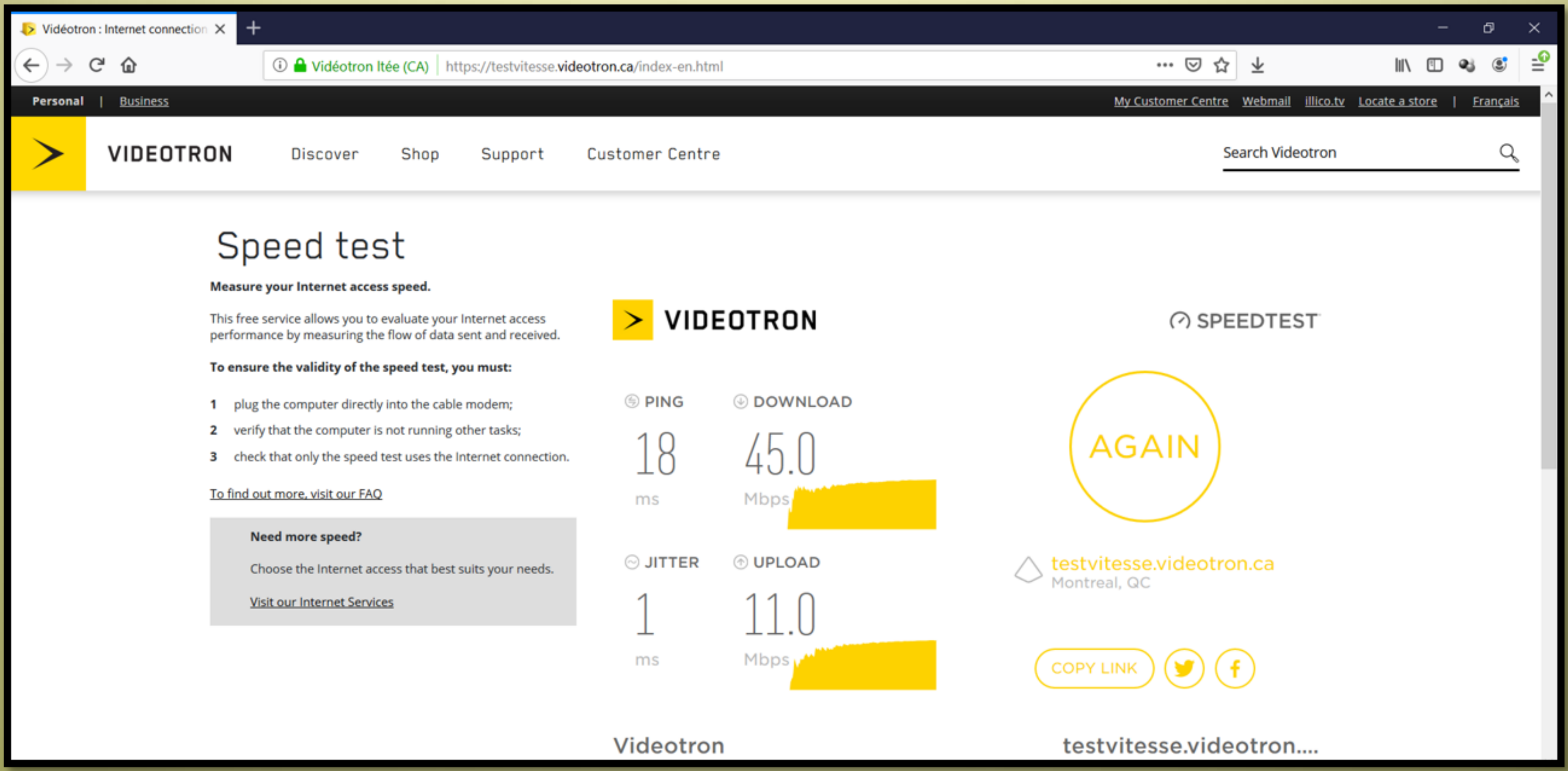
Access net: cable network

- Example: speed testing over a cable Internet access – Mid 2013



Access net: cable network

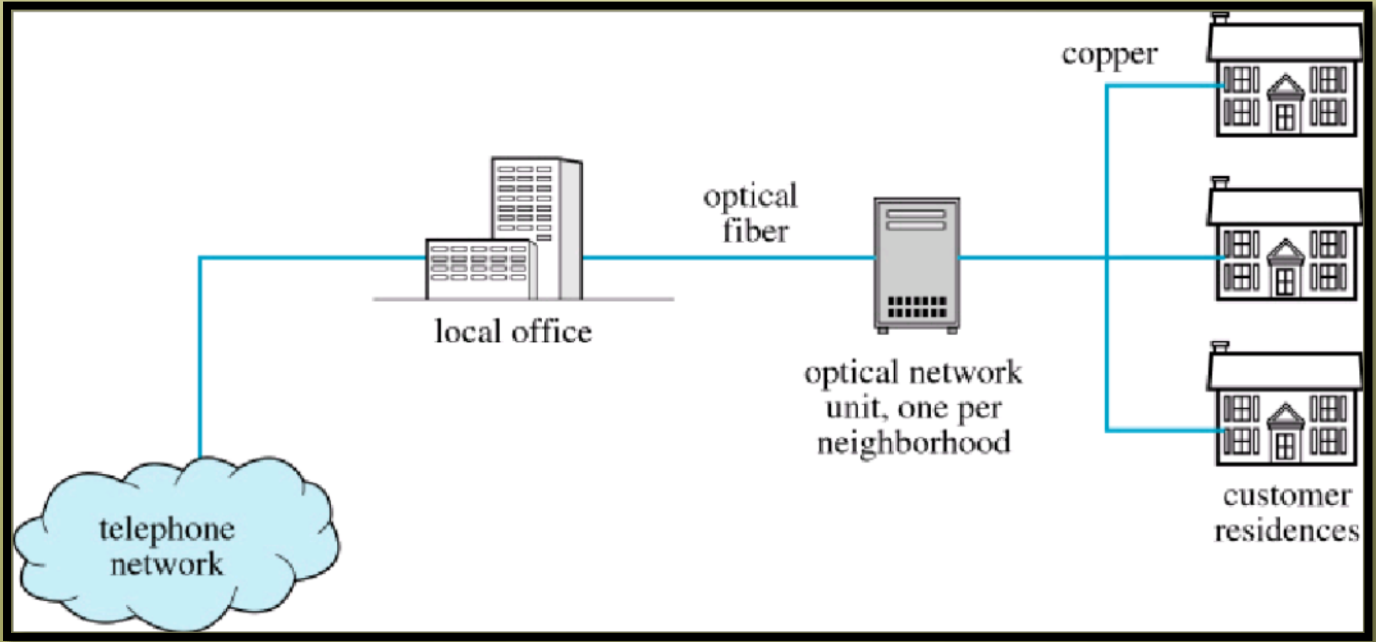
- Example: speed testing over a cable Internet access – September, 2019



Access net: digital subscriber line (DSL)

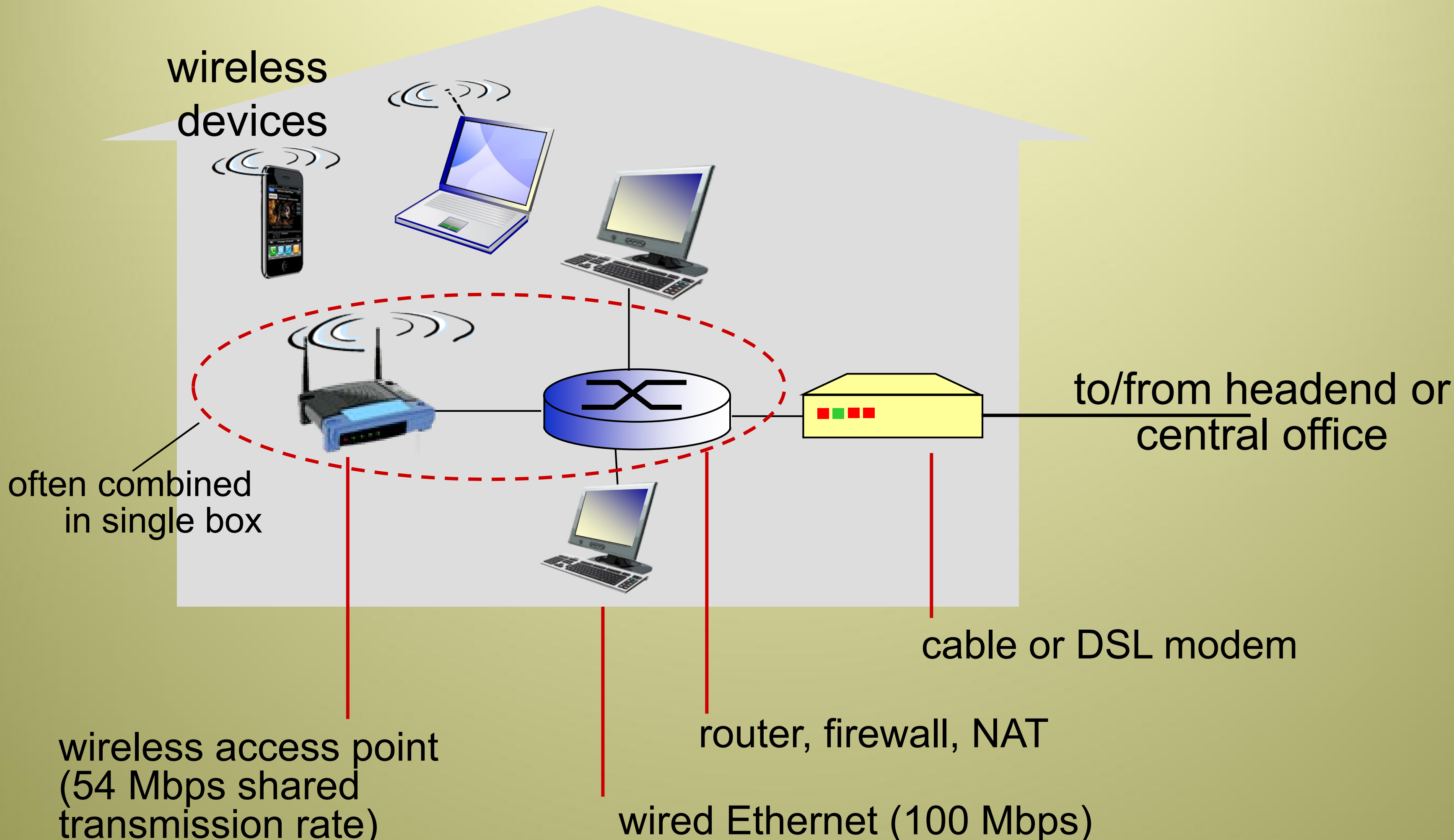
VDSL – Very High Data Rate DSL

- The local loop causes many DSL problems
- Signal degrades over long distance, so DSL is not available if the house is more than 3.5 miles from the local office
- New improved local loop using fiber/copper hybrid is used, which improves quality, reduces the copper length and makes VDSL possible

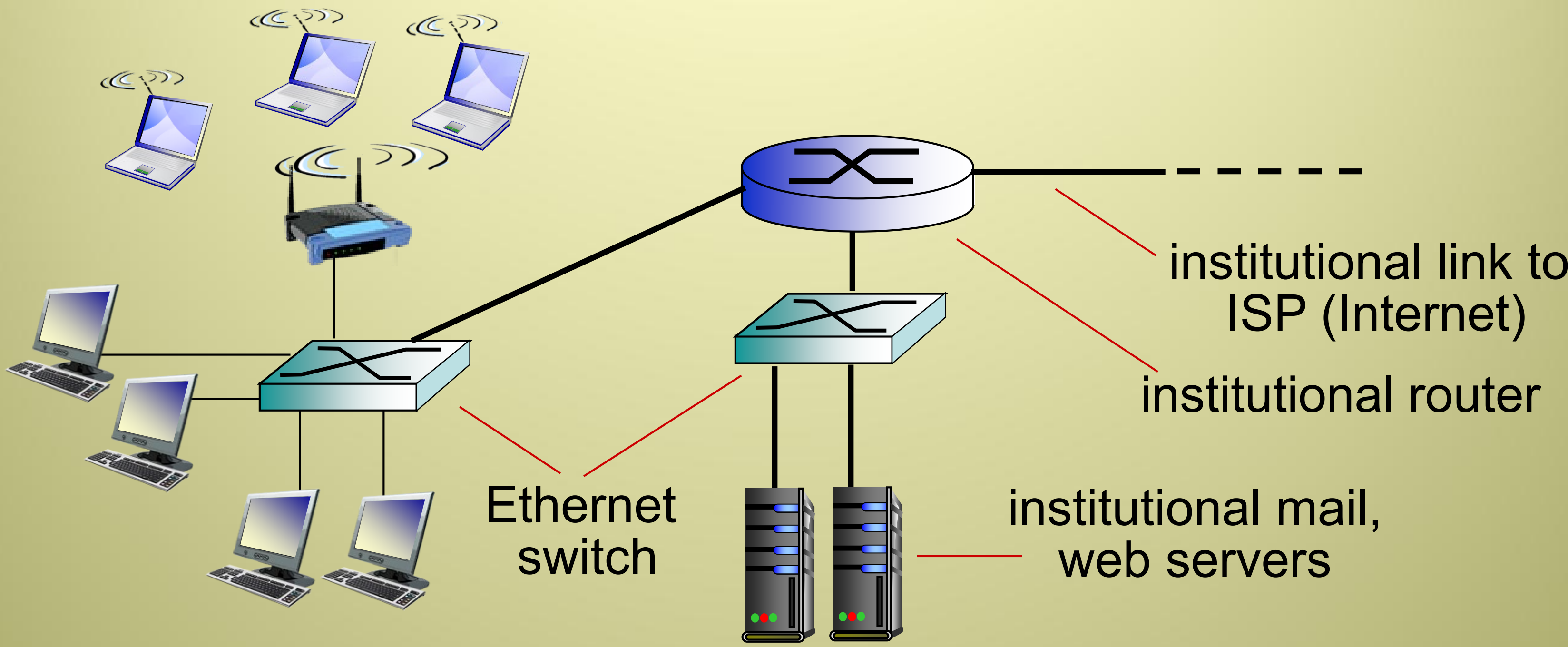


Local Loop: Fiber/Copper Hybrid

Access net: Ethernet & WiFi



Enterprise access networks (Ethernet)



- typically used in companies, universities, etc
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
- today, end systems typically connect into Ethernet switch

Wireless access networks: 3G and LTE

- shared *wireless* access network connects end system to router
  - via base station aka "access point"

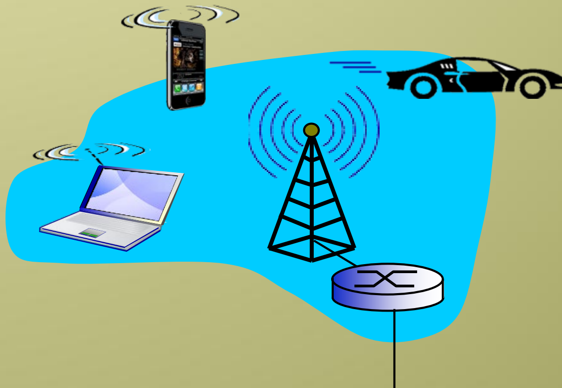
wireless LANs:

- within building (100 ft)
- 802.11b/g (WiFi): 54 Mbps transmission rate

to Internet

wide-area wireless access

- provided by telco (cellular) operator, 10's km
- between 1 and 10 Mbps
- 3G, 4G: LTE



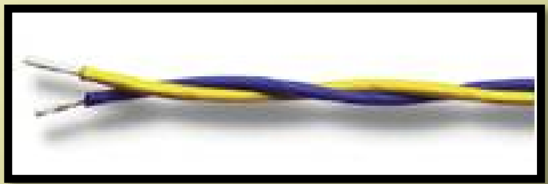
to Internet

Physical media

- bit: propagates between transmitter/receiver 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)

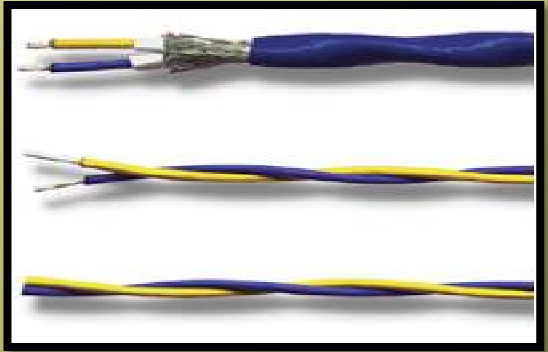
- two insulated copper wires



  - Category 5: 100 Mbps, 1 Gpbs Ethernet
  - Category 6: 10Gbps

Physical media: twisted pairs

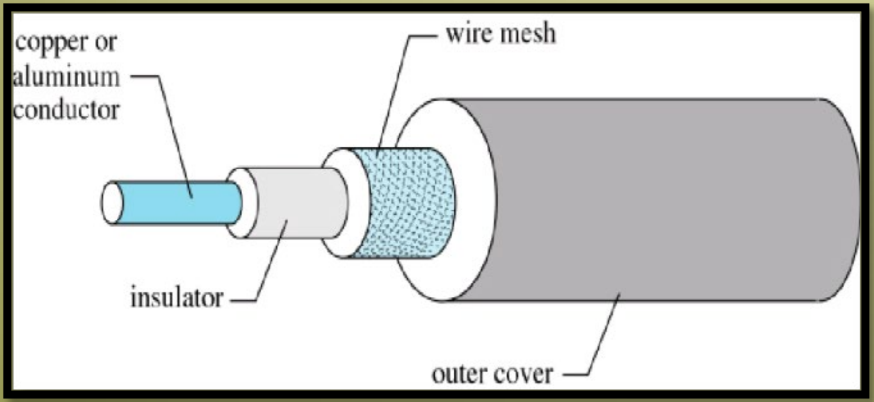
- Copper is usually used due to its less resistance to electricity, as well as high resistance to corrosion
- Twisted wires use balanced signals; 180° out of phase
- More twists reduce ***crosstalk***, the electromagnetic interference between adjacent pairs
  - Although copper has less resistance to electricity, signal will eventually die (***attenuate***)
  - ***Repeaters*** are used to solve this problem
  - Two types of twisted pair wires exist: Unshielded (UTP) & Shielded (STP); they have different cost & quality



Physical media: coax, fiber

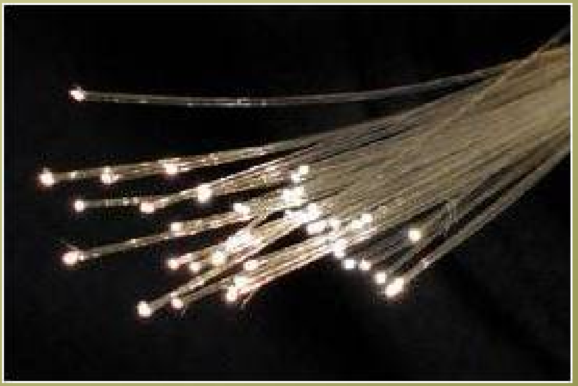
coaxial cable:

- two concentric copper conductors
- Bidirectional
- 10s of Mbps
- 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 Gpbs transmission rate)
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise



Physical media: terrestrial radio

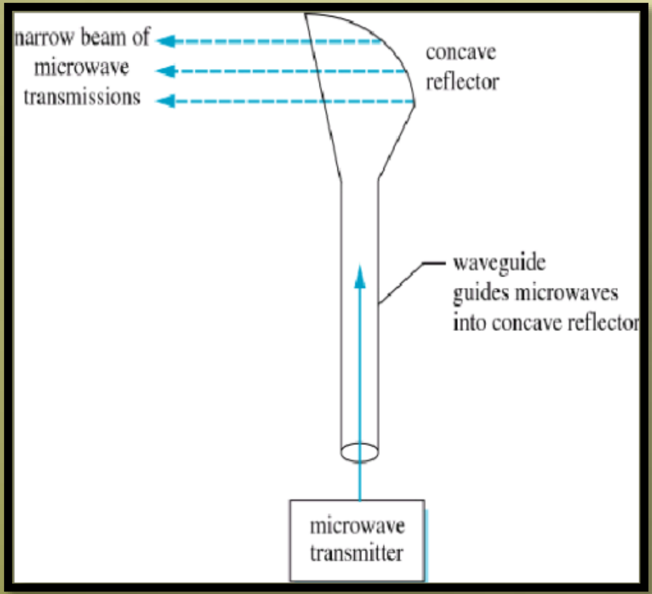
- signal carried in electromagnetic spectrum
- no physical "wire"
- Bidirectional
- propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

radio link types:

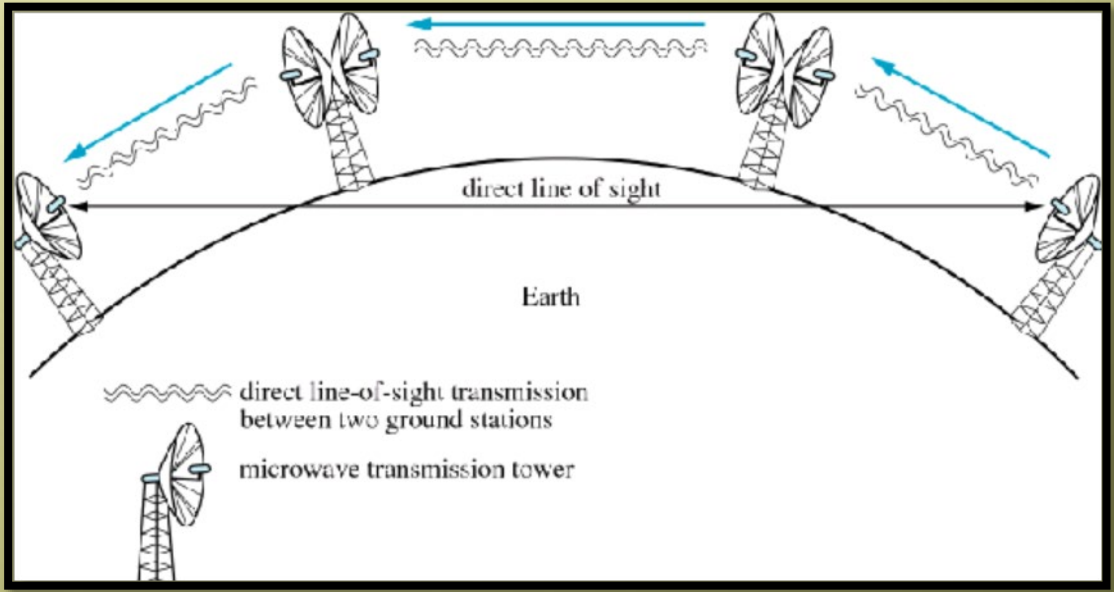
- terrestrial microwave
  - e.g. up to 45 Mbps channels
- LAN (e.g., WiFi)
  - 11Mbps, 54 Mbps
- wide-area (e.g., cellular)
  - 3G cellular: ~ few Mbps

Physical media: terrestrial radio

- Microwave Transmissions
  - Often through Horn Antenna
  - Towers are used as repeaters to solve earth curvature's and signal loss problems

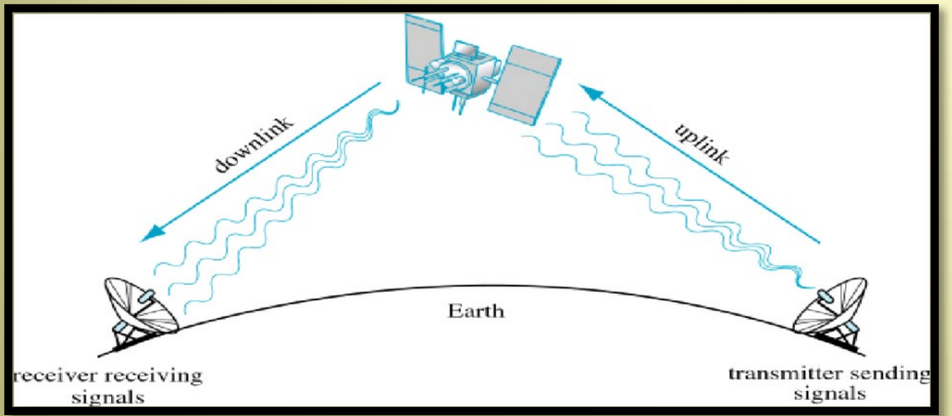


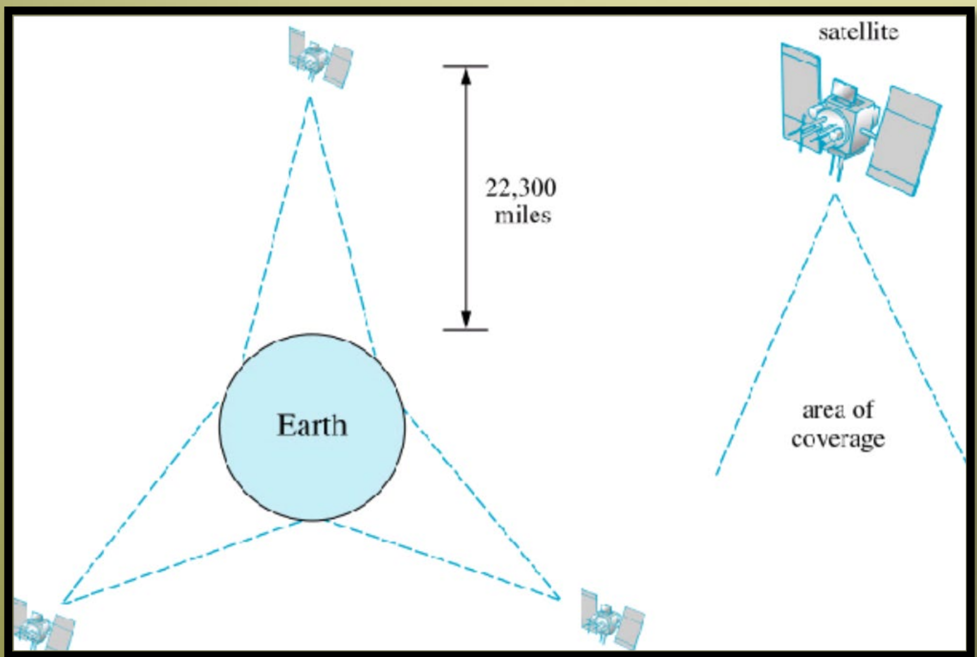
Horn Antenna



Microwave Towers as Repeaters

Physical media: satellite radio

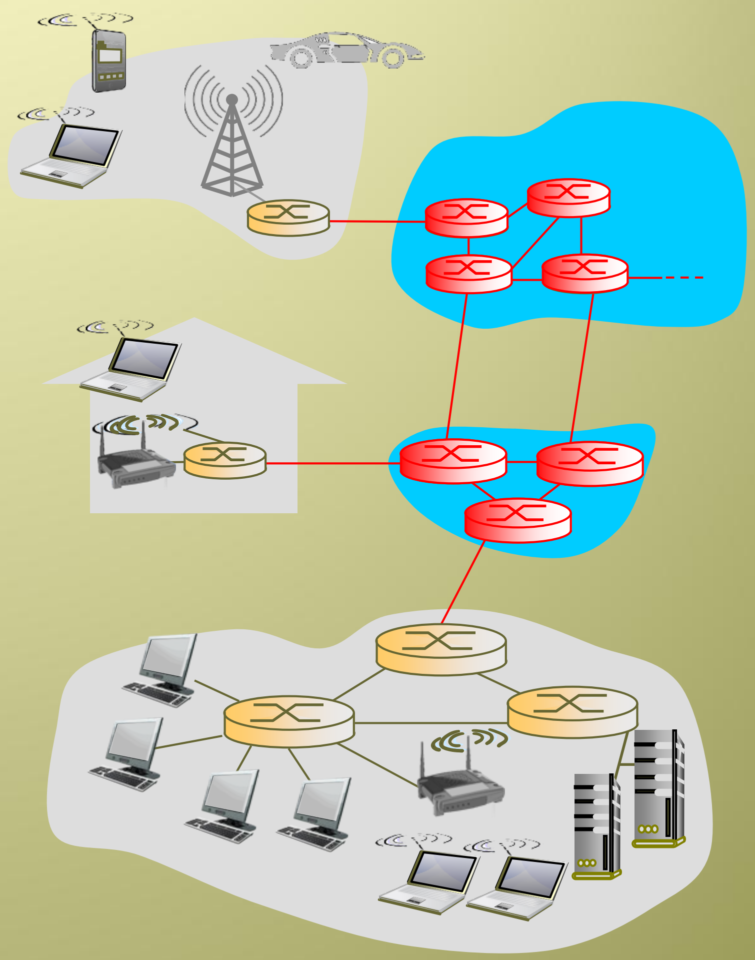




- satellite communications
  - A science fiction in 1945; A common science today!
  - Primarily, it is a microwave transmission in which one of the towers is a satellite
  - In 1957, the Soviet Union launched the Sputnik
  - geosynchronous versus low altitude/low-earth orbit (LEO)
  - Kbps to 45Mbps channel
  - 280 msec end-end delay

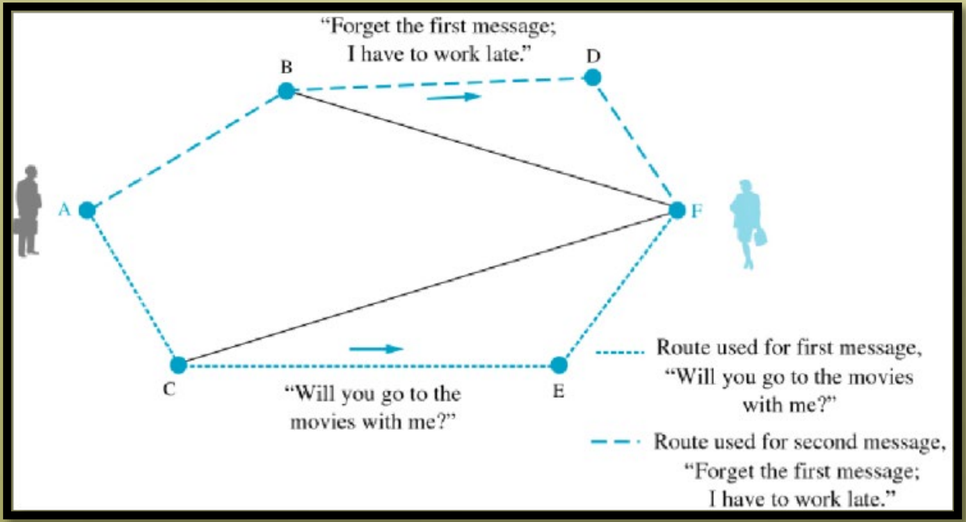
The network core

- mesh of interconnected routers



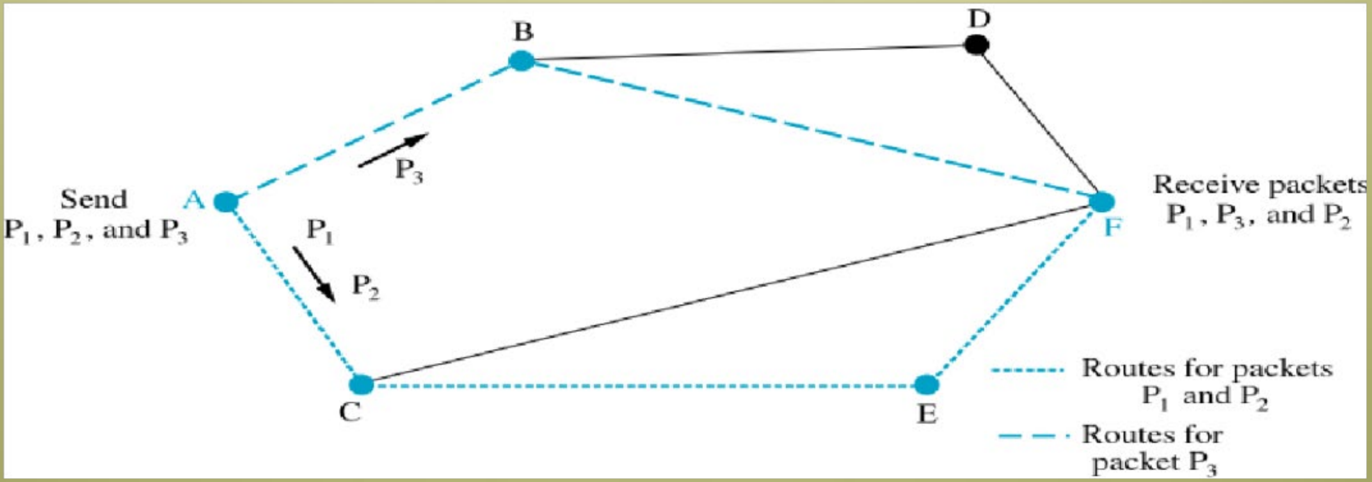
The network core

- message-switching:
  - ***Message***: unit of information
  - A route is established when a message is to be sent
  - A sending node attach the message along with the destination address, chooses a route, then forwards it to the first node in that route
  - The message, in its entirety, is temporarily stored at that node, while logic is working the next node in the following possible route
  - Once the following node is known the message is routed to it
  - This is know as **Store-and-Forward**



The network core

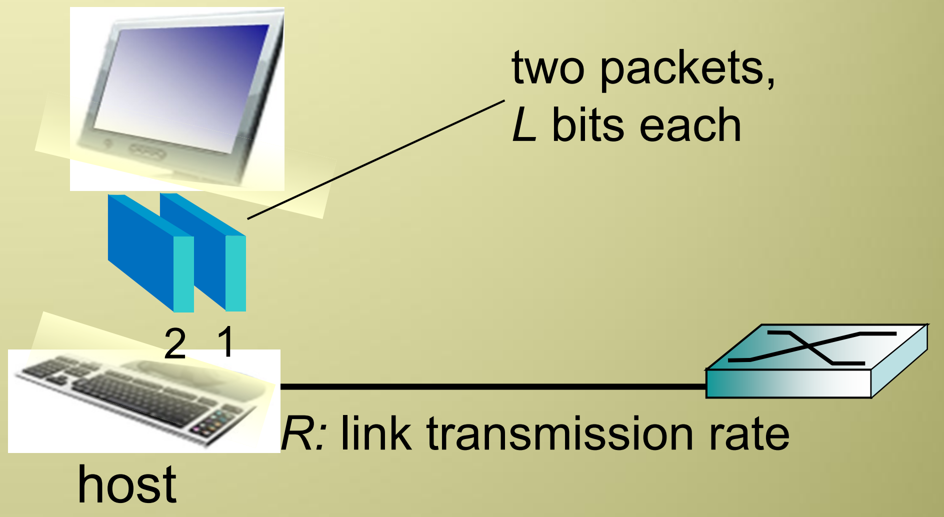
- packet-switching: hosts break application-layer messages into *packets*
  - forward packets from one router to the next, across links on path from source to destination
  - each packet transmitted at full link capacity



Host: sends *packets* of data

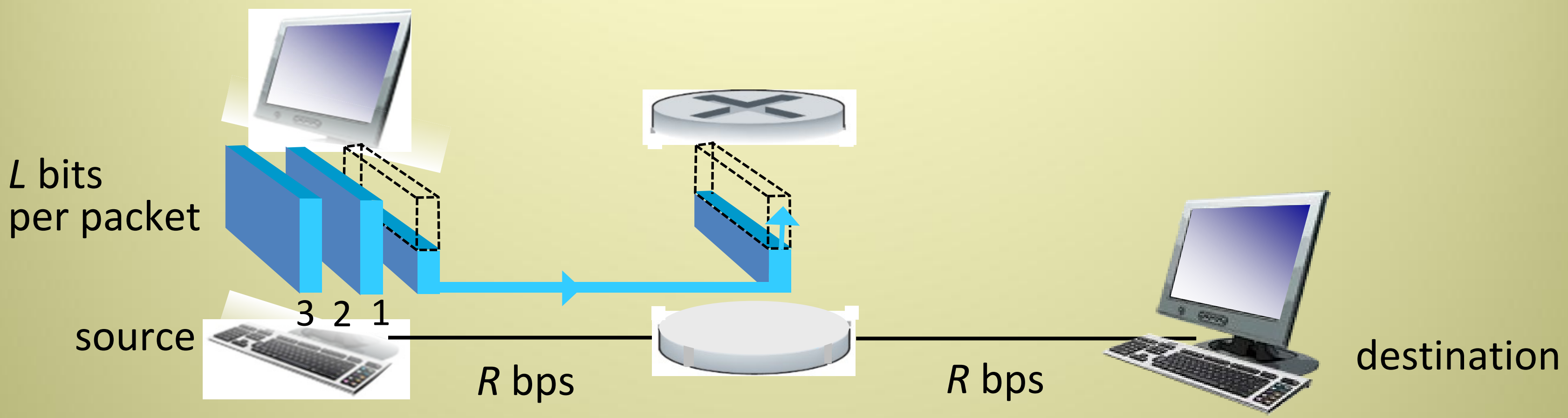
host sending function:

- takes application message
- breaks into smaller chunks, known as *packets*, of length *L* bits
- transmits packet into access network at *transmission rate R*
  - link transmission rate, aka link *capacity, aka link bandwidth*



$$\text{packet transmission delay} = \text{time needed to transmit } L\text{-bit packet into link} = \frac{L \text{ (bits)}}{R \text{ (bits/sec)}}$$

Packet-switching: store-and-forward



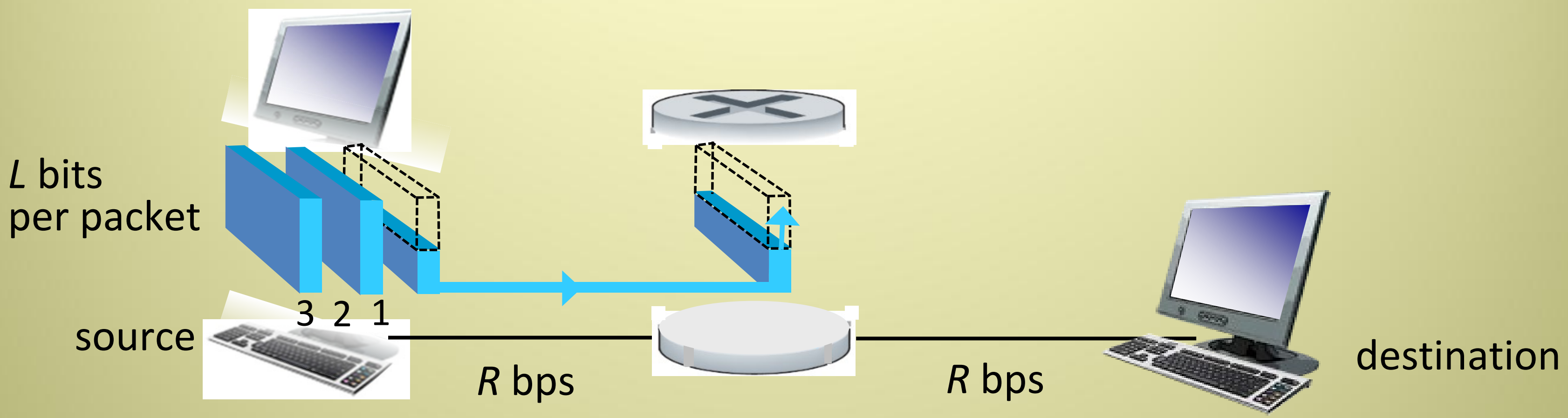
- takes *L/R* seconds to transmit (push out) *L*-bit packet into link at *R* bps
- *store and forward:* entire packet must arrive at router before it can be transmitted on next link
- end-end delay = 2*L/R* (assuming zero propagation delay)

more on delay shortly …

one-hop numerical example:

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

Packet-switching: store-and-forward



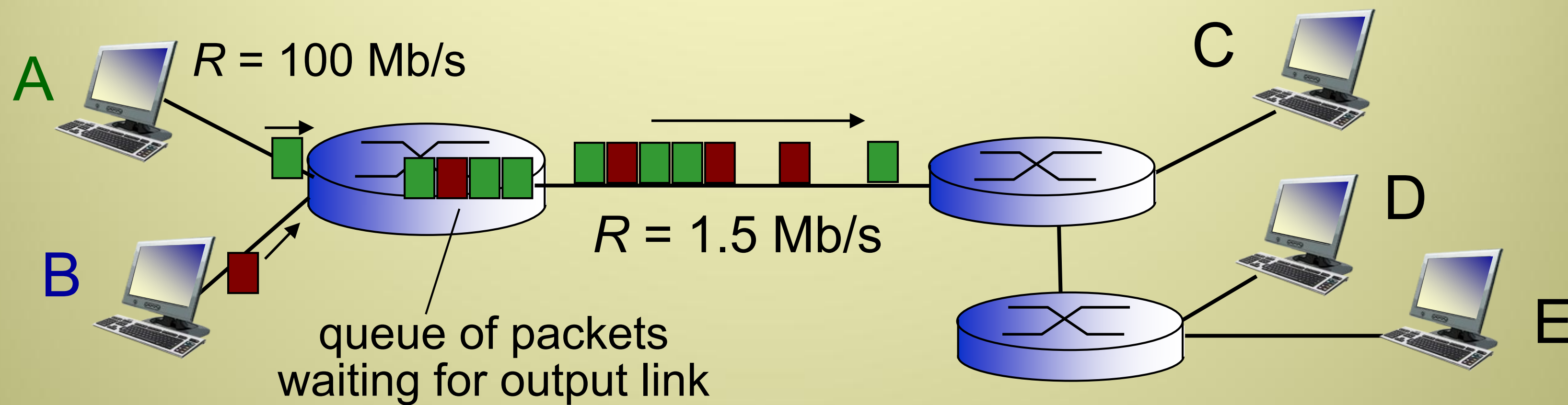
- takes $4L/R$ seconds to receive all 3 packets

- In the general case, sending one packet through N links (N-1 connecting routers) would cost an end-to-end delay as follows:

$$d_{end\text{-}to\text{-}end} = N\ L/R$$

(again, this is assuming zero propagation delay)

Packet Switching: queueing delay, loss



queuing delay and loss:

- If arrival rate (in bits) to link exceeds transmission rate of link for a period of time:
  - packets will queue, wait to be transmitted on link, consequently causing delays
  - packets can be dropped (lost) if memory (buffer) fills up

Packet Switching: Virtual circuit vs Datagram

- Packet switching has two common routing methods
  - **Datagram**
  - **Virtual circuit**

- Sending through different routes is flexible; why?
- However, packets may arrive out of order!

- With virtual circuit, network protocols establish a route (virtual circuit) before sending any packets.
- Consequently, packets are guaranteed to arrive in order

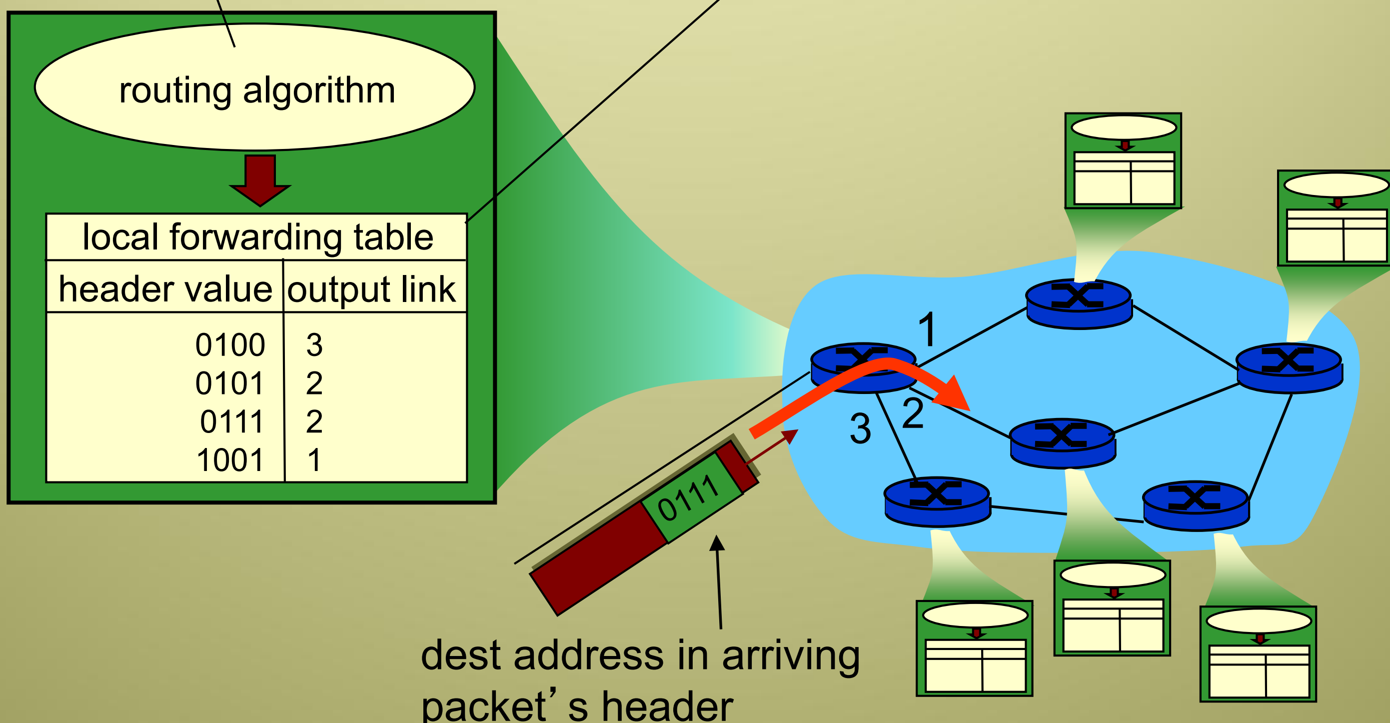
- Important Note: The circuit is not dedicated

Two key network-core functions

routing: determines source-destination route taken by packets

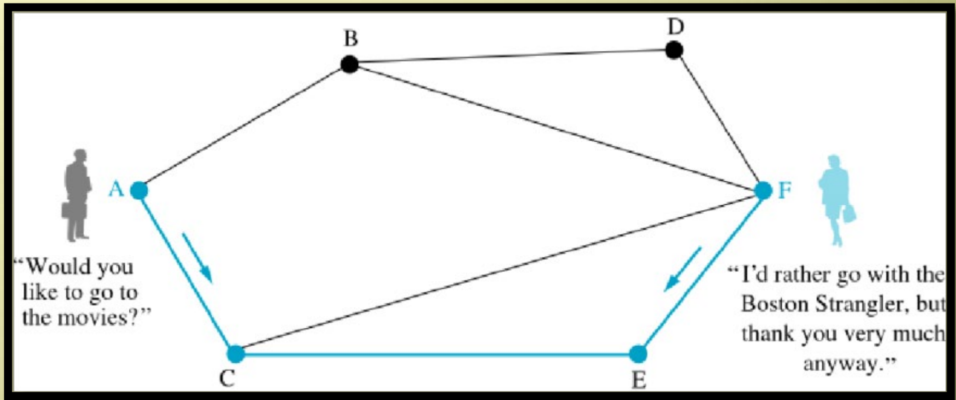
- *routing algorithms*

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

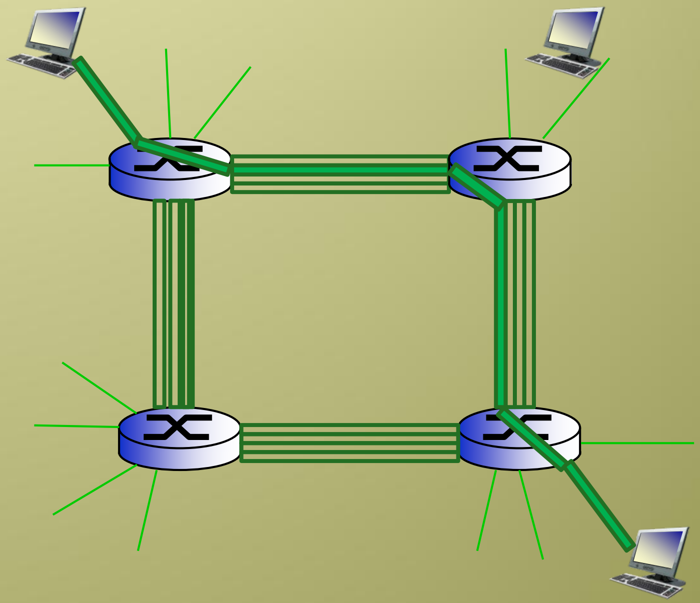


Alternative core: circuit switching

end-end resources allocated to, reserved for, "call" between source & dest:



- In diagram below, each link has four circuits.
  - call gets 2nd circuit in top link and 1st circuit in right link.
- dedicated resources: no sharing
  - circuit-like (guaranteed) performance
- circuit segment idle if not used by call *(no sharing)*
- Commonly used in traditional telephone networks



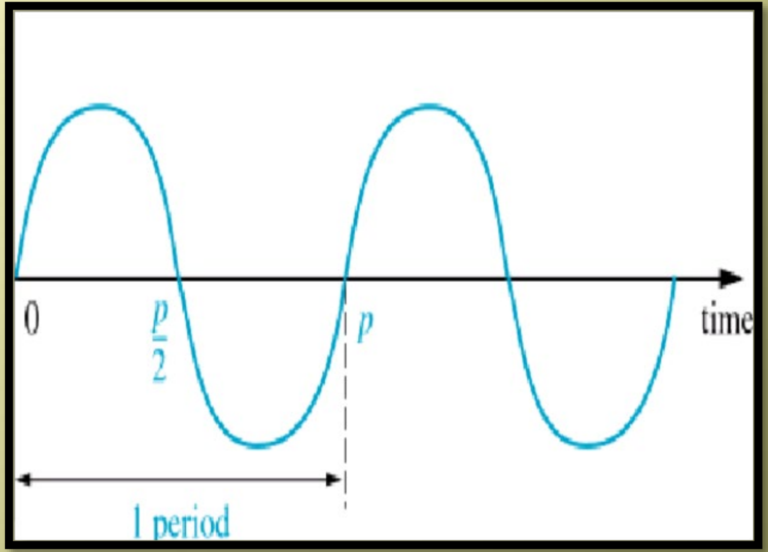
Bit rate & Bandwidth

- **Bit Rate**
  - How many ***bits per second*** (bps) a link can transmit
  - Rates range from 100s bps to billions of bps (gigabits) and now pushing for trillion bps (terabit)

- **Bandwidth**
  - **Period**: Time needed for a signal to complete one cycle
  - **Frequency**: Number of cycles per second, measured in ***Hertz*** (Hz)

$$f = 1 / p$$

  - For example, if p = 0.5 microseconds (μsec) then f = 2 MHz
  - A given medium can accommodate a range of frequency
  - ***Bandwidth*** is the difference between the highest and the lowest possible frequency that can be transmitted
  - For example, telephone signals can handle frequencies between 300 Hz & 3300Hz; the bandwidth is hence 3000 Hz
  - In other words, very high or very low audible sounds cannot pass though the telephone

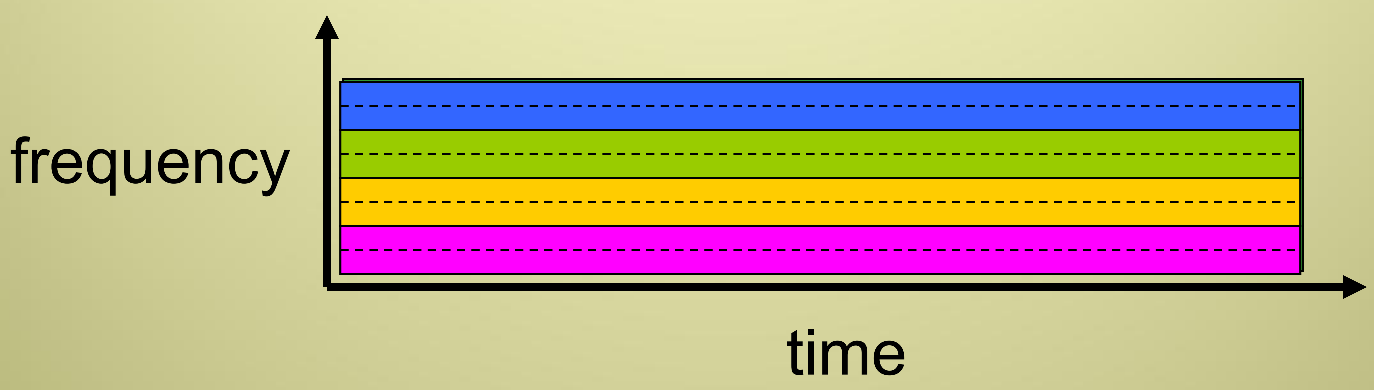


Multiplexing: FDM versus TDM

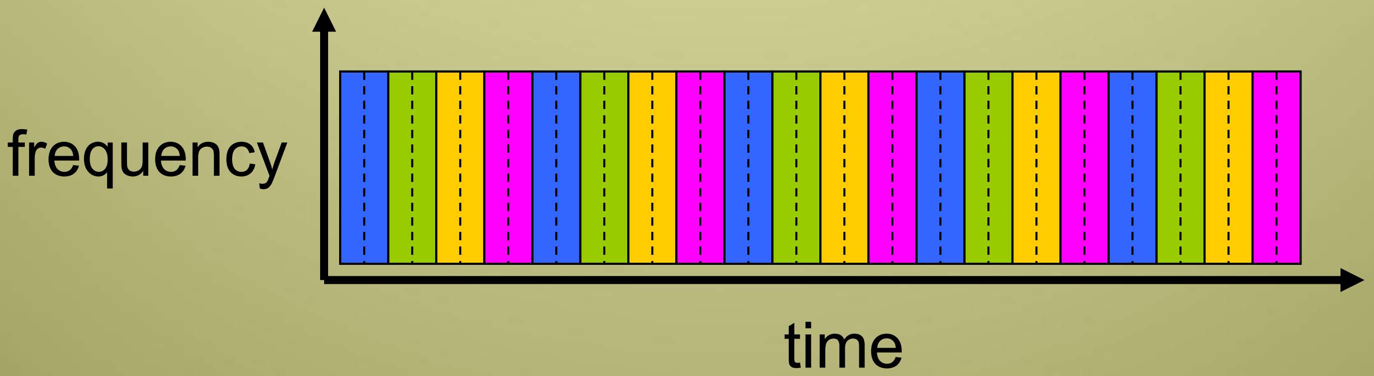
Example:

4 users

FDM

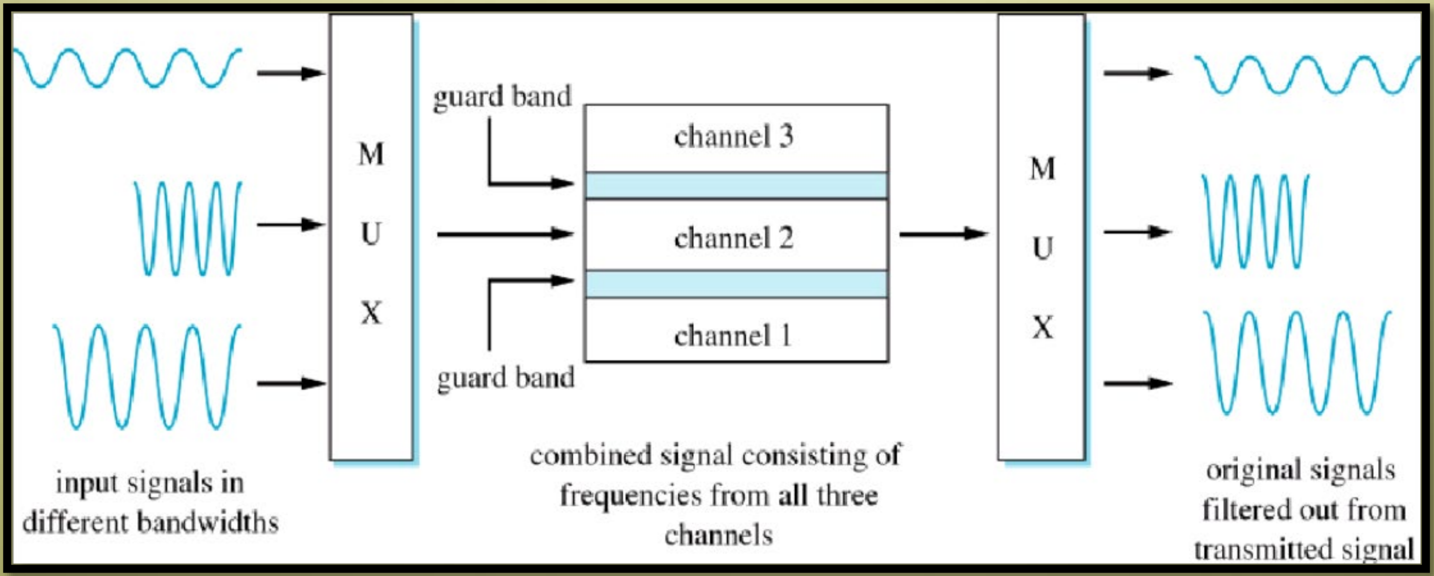


TDM



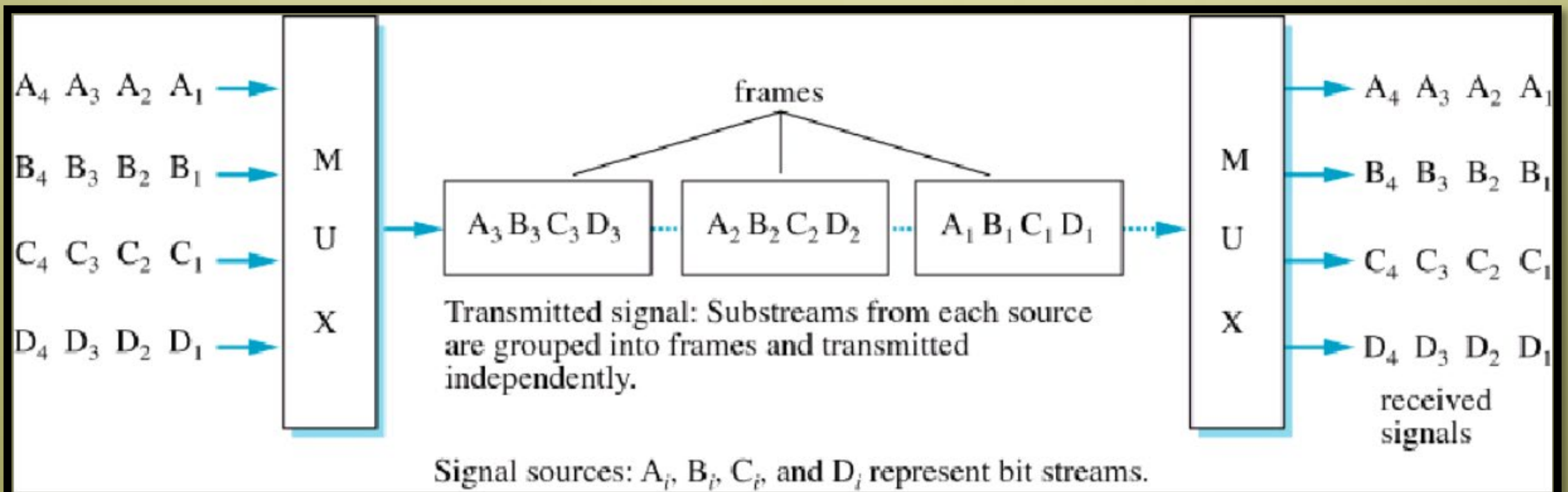
Frequency-Division Multiplexing (FDM)

- The signals from all inputs are combined into as a single, more complex analog signal
- The channels themselves are separated by a **guard band**



Time-Division Multiplexing (TDM)

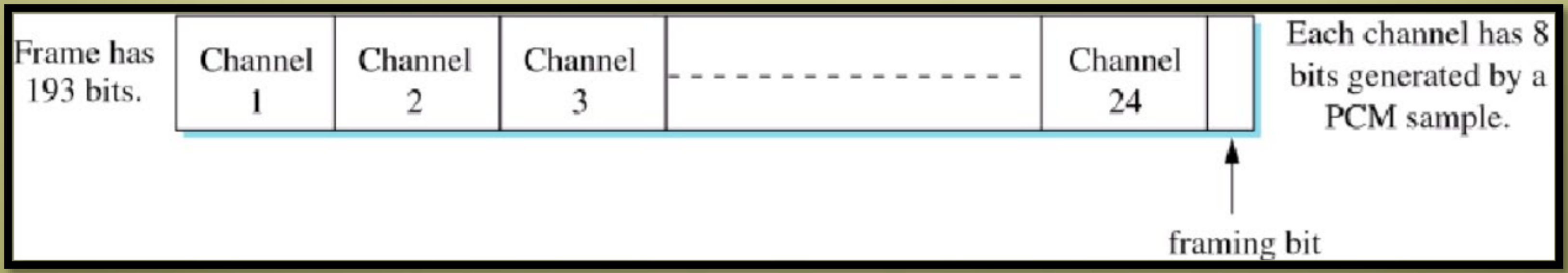
- TDM keeps the signals physically distinct but logically packages them together
- The optimal performance is achieved when the combined input rate is equal to the output rate
- A faster combined input rate would result in signals being dropped and a slower input rate would results in frames that are partially full so the channels are underused



Time-Division Multiplexing (TDM)

T1/DS1 Digital Carrier

- A standard used for long-distance communication
- Uses TDM to combine many voice channels into one Digital Signal 1 (***DS1)*** frame
- *T1* refers to the circuit, *DS1* refers to the signal
- DS1 frame has 24 channels of 8 bits each, and one framing bit for synchronization



DS1 Frame

Time-Division Multiplexing (TDM)

T1/DS1 Digital Carrier

- T1 rate:
  - 8-bit sample * 8000 samples/second ➔ 64 Kbps
  - To support this rate, T1 must transmit a DS1 frame each 1/8000 seconds ➔ must transmit 8000 * 193 bits each second
  - ➔ Date rate of 1.544 Mbps (1.536 Mbps of actual data)
- This rate is considered slow compared to optical fiber capabilities
- That is the reason there are other carriers with more channels and faster bit rate
- T1 is not only used for voice communication; other companies lease phone lines to transfer digital information between computers

Carrier	Digital Signal No.	No. of Channels	Bit Rate, Mbps
T1	DS1	24	1.544
T2	DS2	96	6.312
T3	DS3	672	44.736
T4	DS4	4,032	274.176

Time-Division Multiplexing (TDM)

Example

- Assume a TDM with 24 slots TDM and a bit rate of 1.536 Mbps.
- Assume also that end-to-end circuit establishment requires 500 ms.
- How much time is needed to send a file of size 960 Kbits?

➔ Each circuit is capable of transmitting 1.536 Mbps/24 = **64kbps**

➔ To send 960 kbits it requires: 960 kbits/64 kbps = **15 seconds**

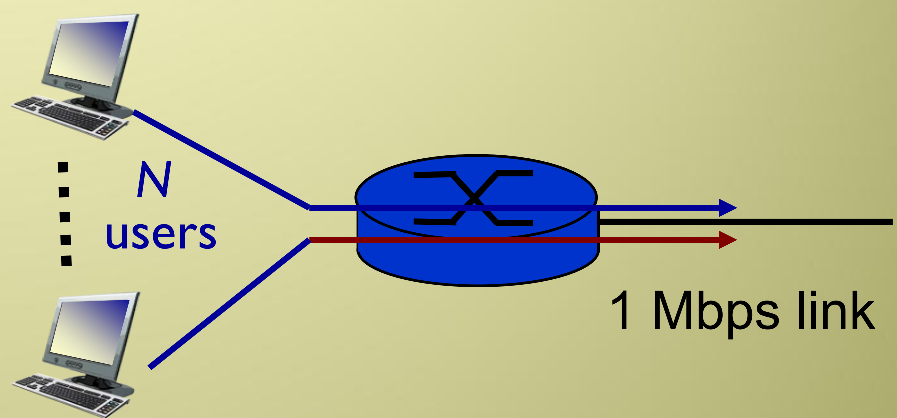
➔ Total time needed to send the file: **15.5 seconds**

Packet switching versus circuit switching

packet switching allows more users to use network!

example:

- 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 found to be less than .0004 *
  - probability of <= 10 active users at the same time is .9996 ➔ packet switching provides essentially the same performance of circuit switching while allowing more than 3 times the number of users

Q: what happens if > 35 users ?

- Proof is irrelevant and beyond the scope of this coverage

Packet switching versus circuit switching

So, is packet switching a "slam dunk winner"?

- great for bursty data
  - resource sharing
  - simpler, no call setup

- excessive congestion possible: 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 (will be discussed later in details)

Internet structure: network of networks

- End systems connect to Internet via access ISPs (Internet Service Providers)
  - Residential, company and university ISPs

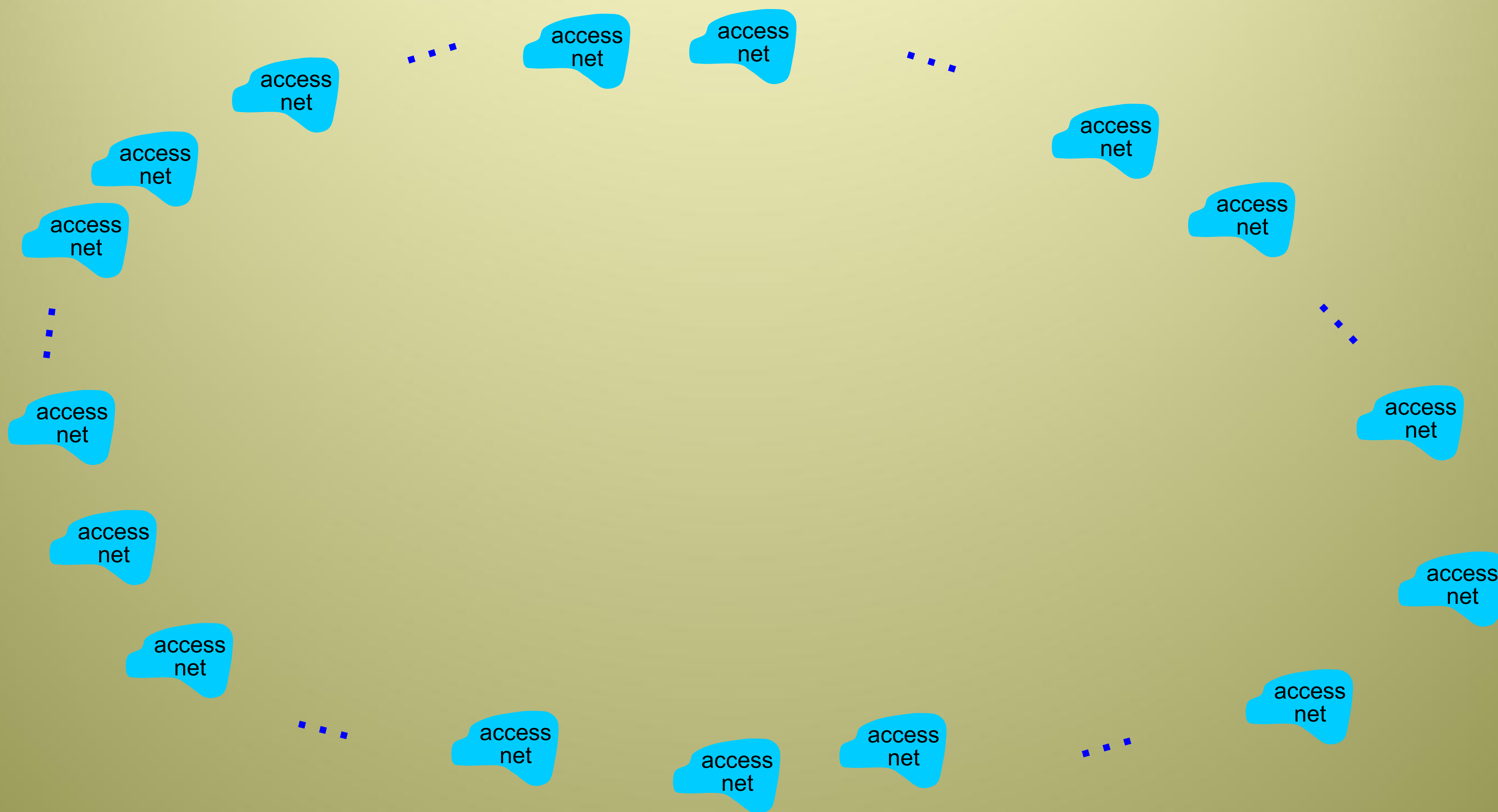
- Access ISPs in turn must be interconnected.
  - So that any two hosts can send packets to each other

- Resulting network of networks is very complex
  - Evolution was driven by economics and national policies

- Let's take a stepwise approach to describe current Internet structure

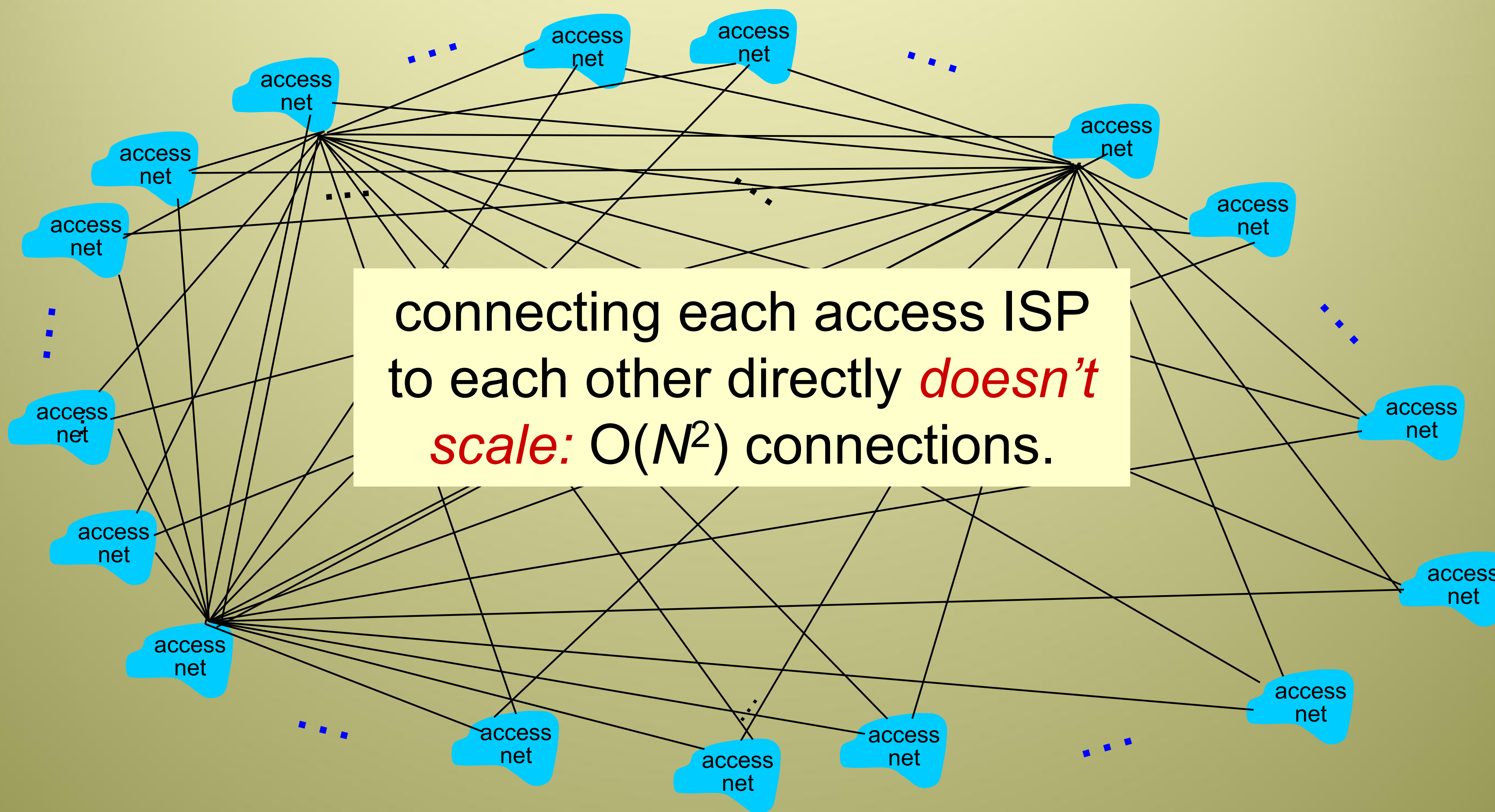
Internet structure: network of networks

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



Internet structure: network of networks

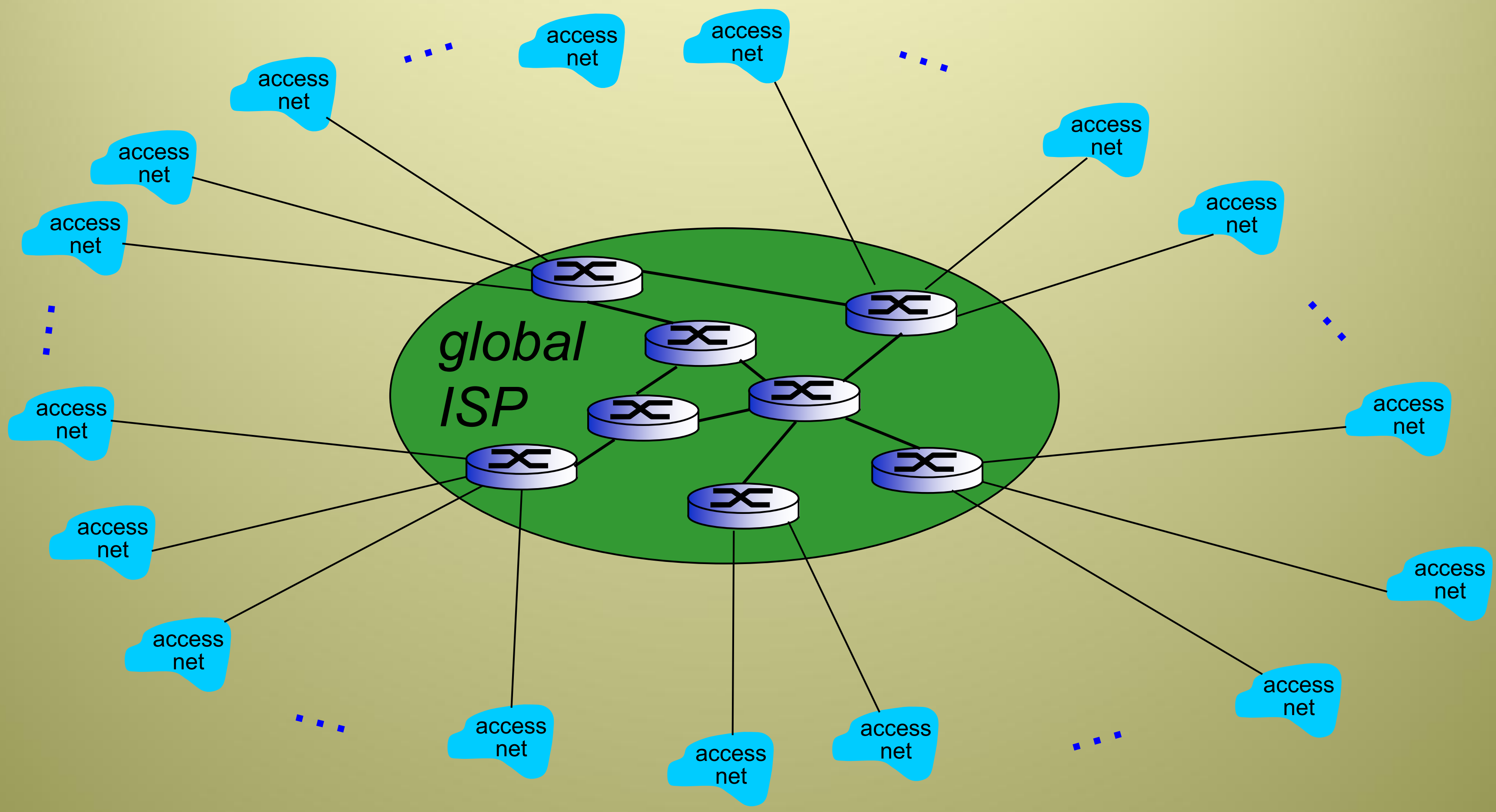
Option: connect each access ISP to every other access ISP?



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

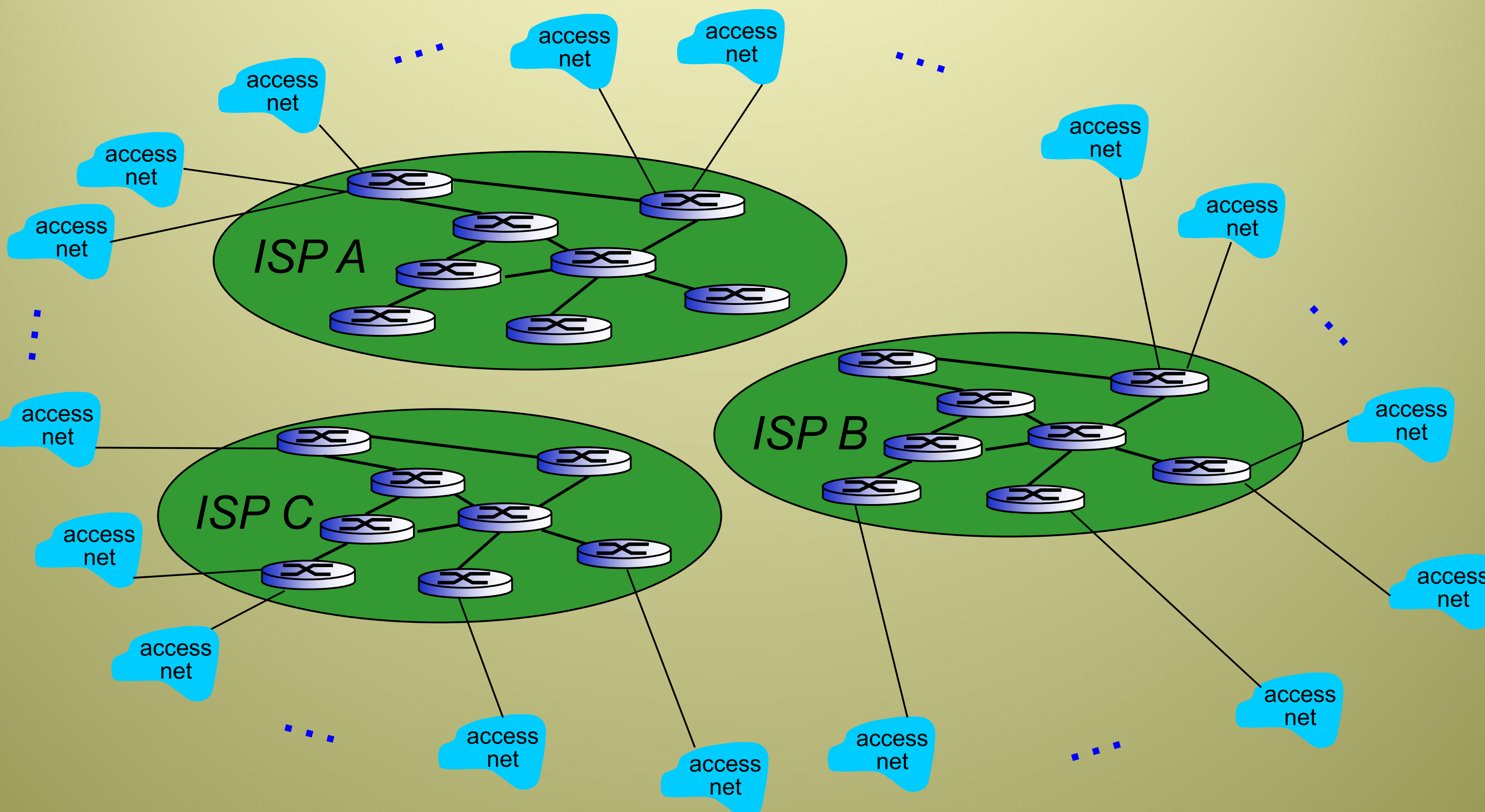
Internet structure: network of networks

Option: connect each access ISP to a global transit ISP? Customer and provider ISPs have economic agreement.



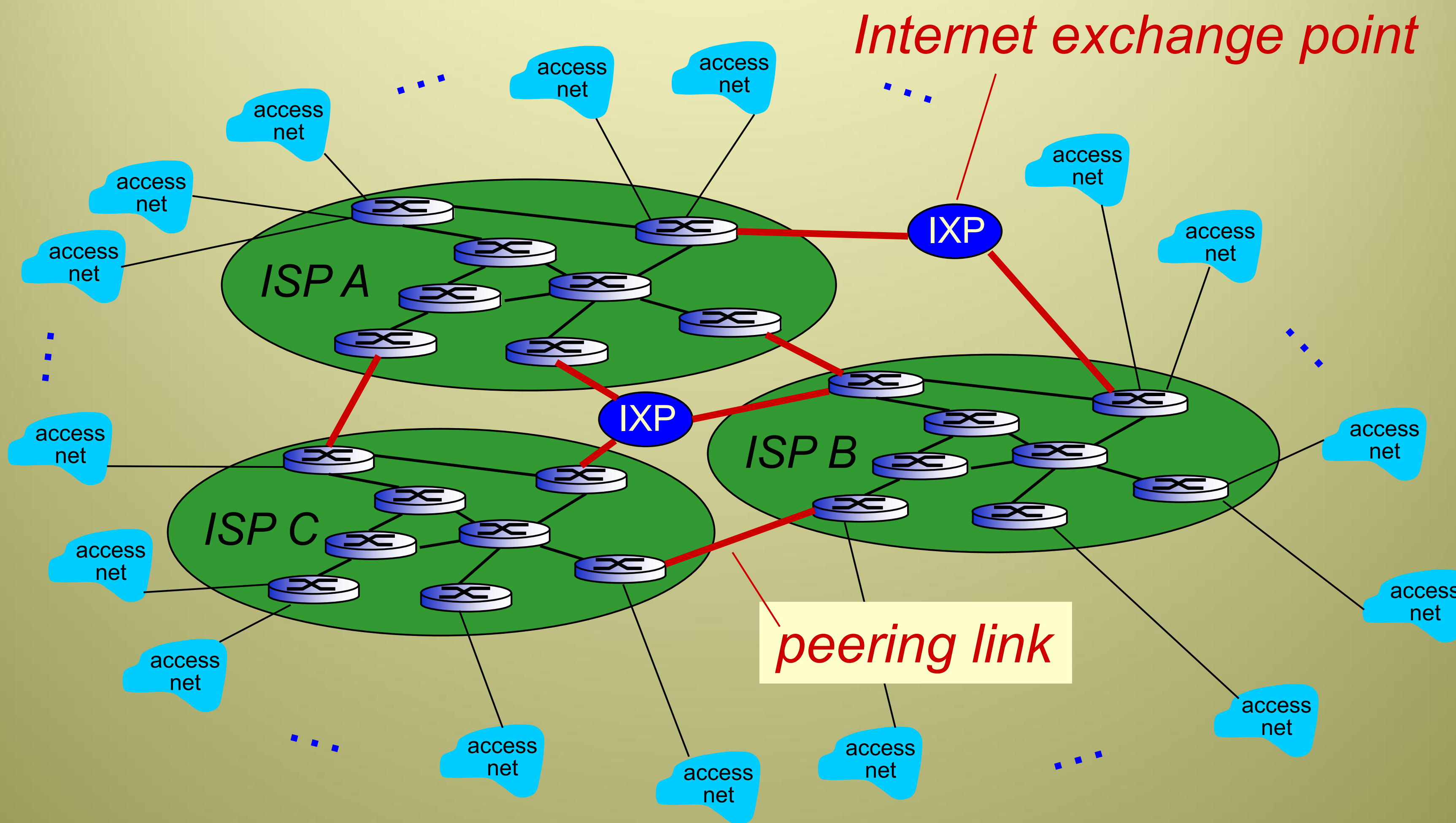
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors ….



Internet structure: network of networks

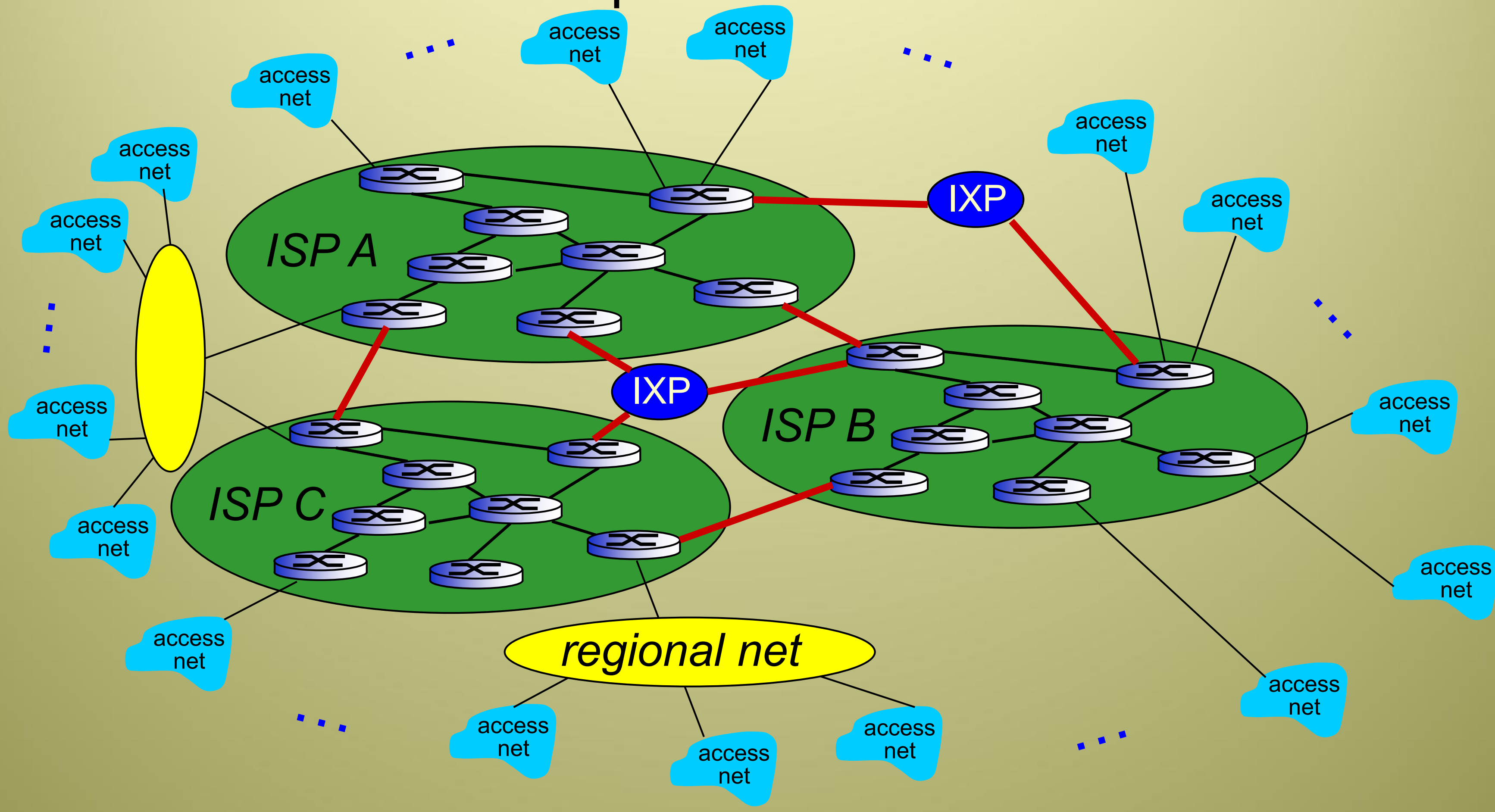
But if one global ISP is viable business, there will be competitors
…. which must be interconnected; leading to a 2-tier hierarchy



Internet structure: network of networks

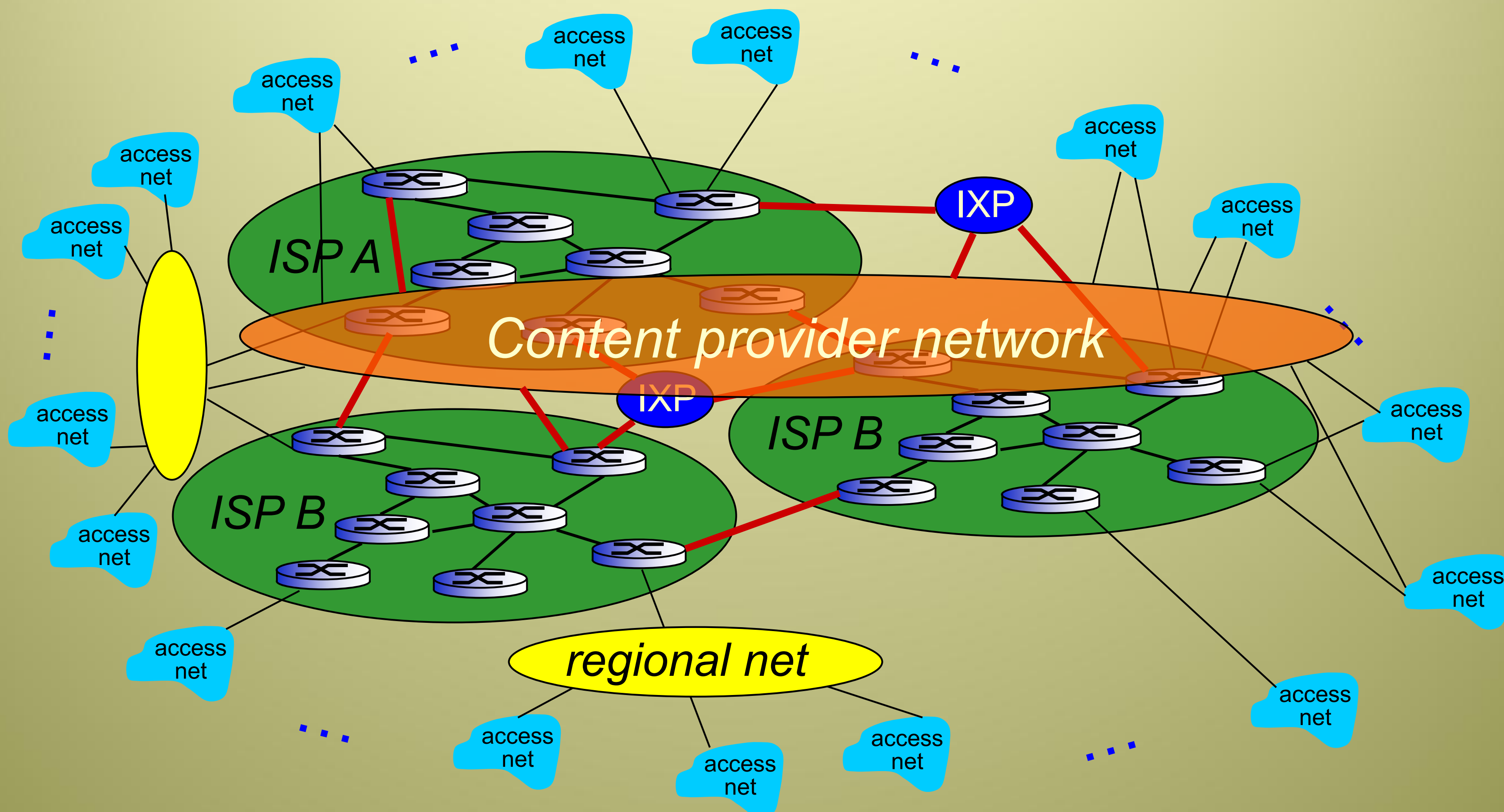
… and regional networks may arise to connect access nets to ISPS

- PoPs and multi-home are possible

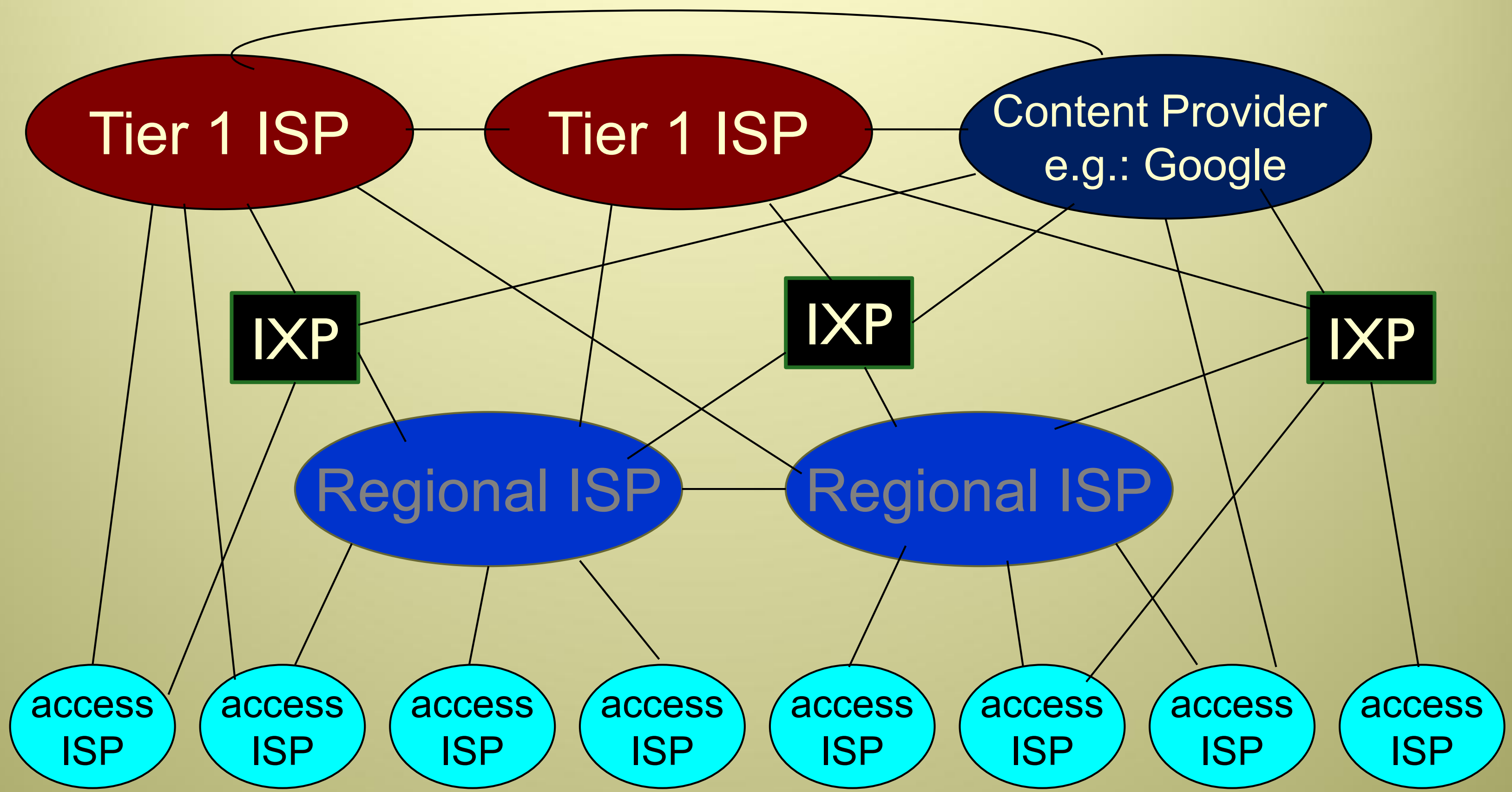


Internet structure: network of networks

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

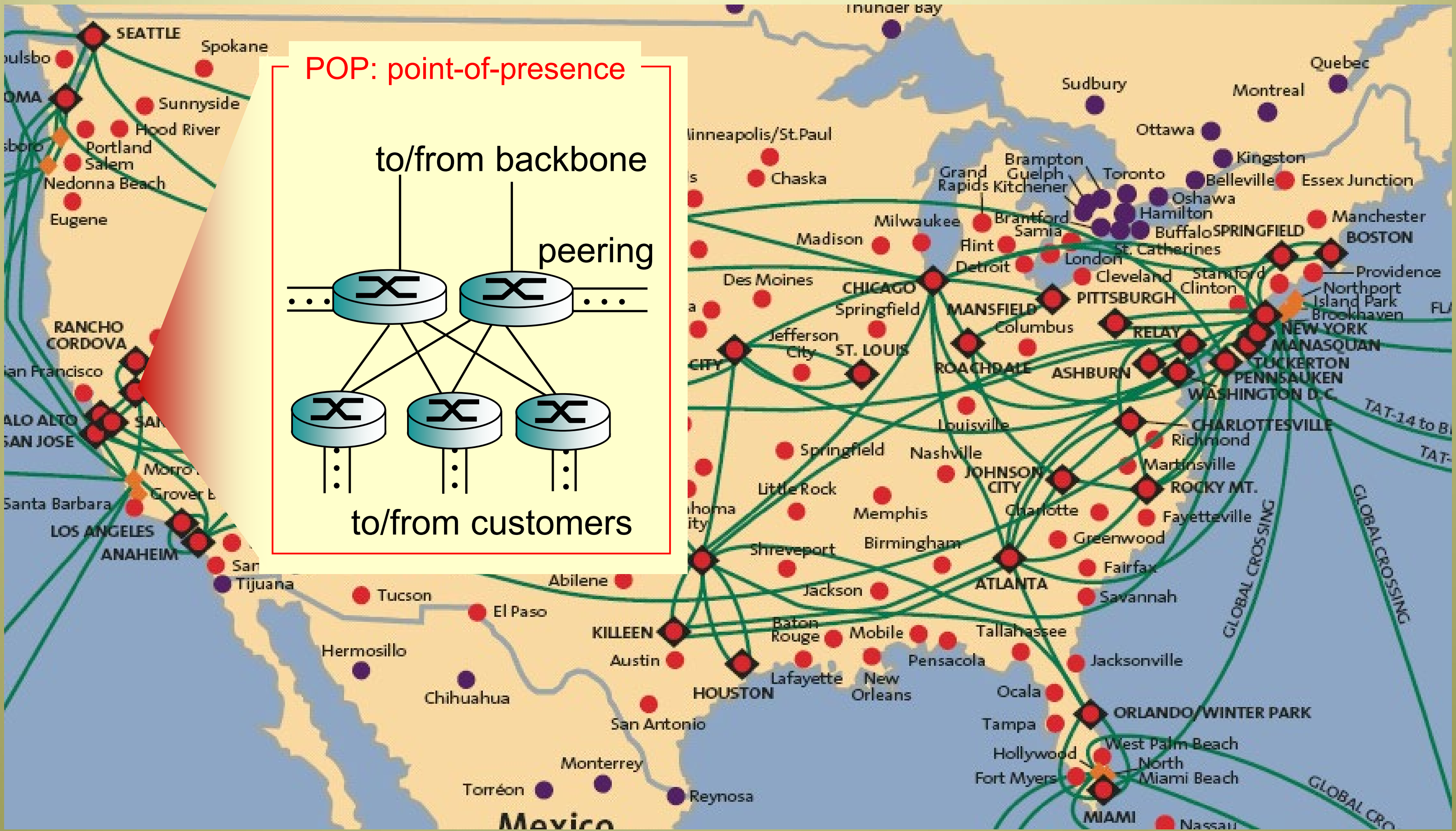


The 2019 Internet structure



- 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 it data centers to Internet, often bypassing tier-1, regional ISPs

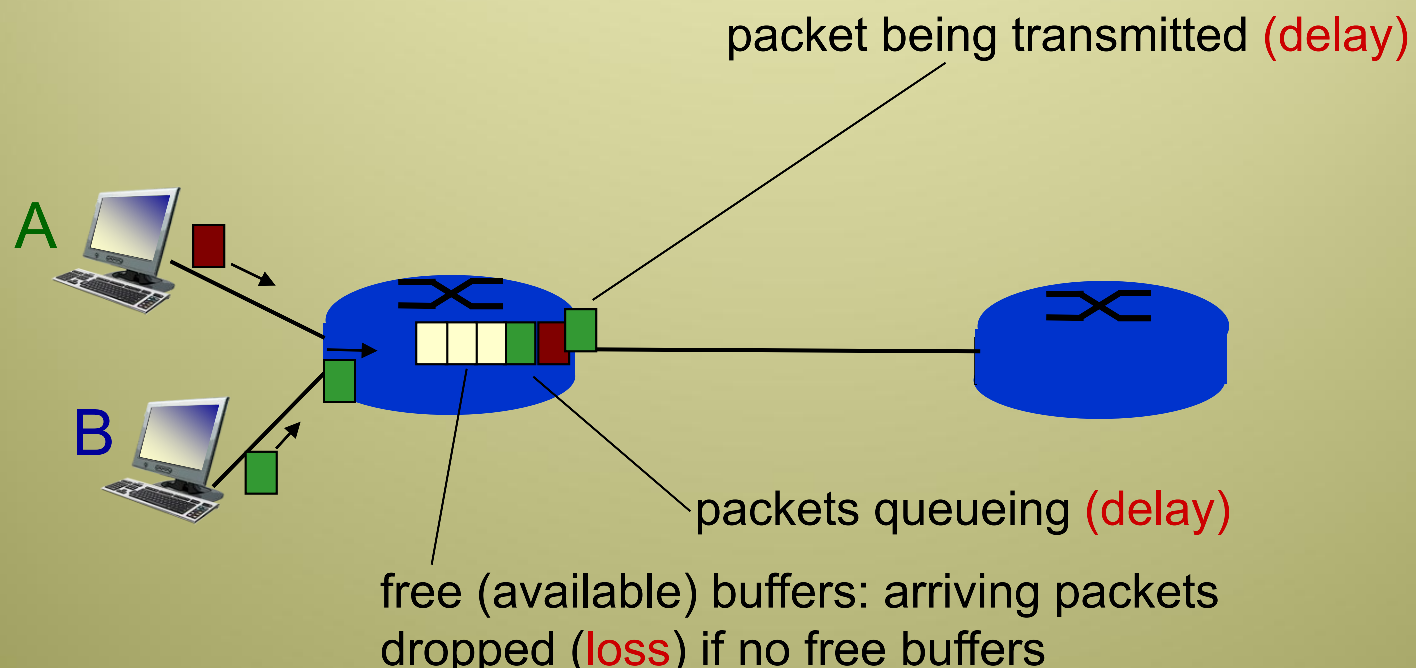
Tier-1 ISP: e.g., Sprint



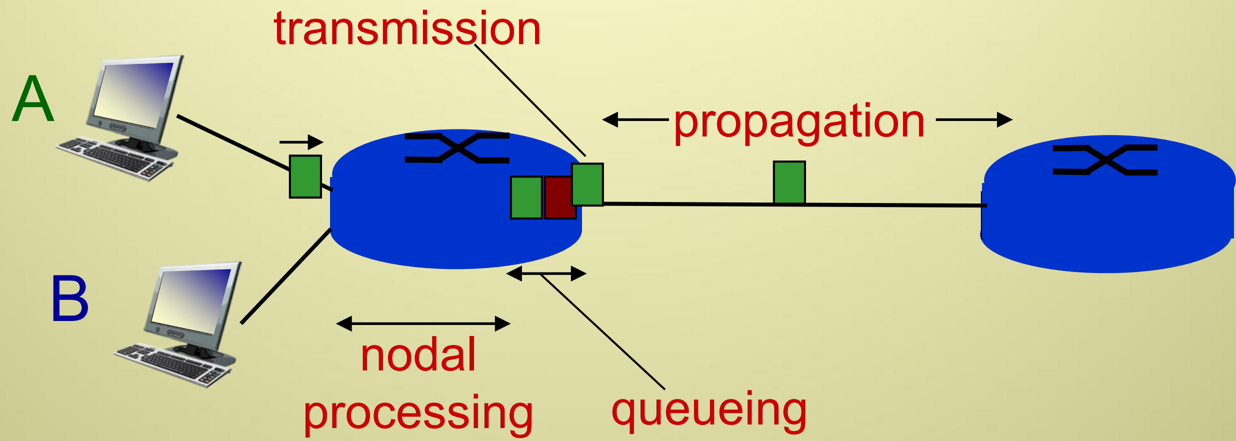
How do loss and delay occur?

packets *queue* in router buffers

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



Four sources of packet delay



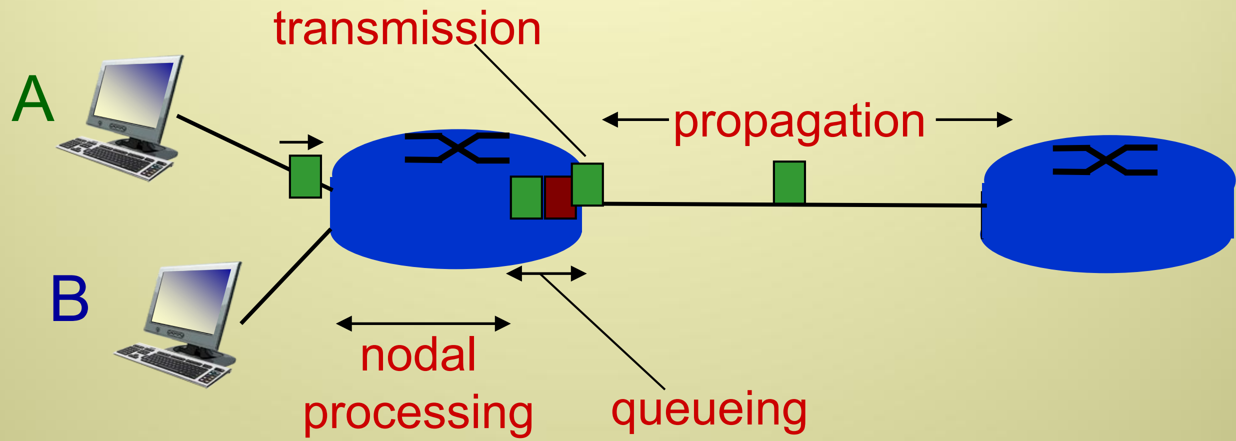
$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

d_{nodal}: total nodal delay

d_{proc}: nodal processing
- check bit errors
- determine output link
- typically < μsec

d_{queue}: queueing delay
- time waiting at output link for transmission
- depends on congestion level of router

Four sources of packet delay



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

d_{trans}: transmission delay:

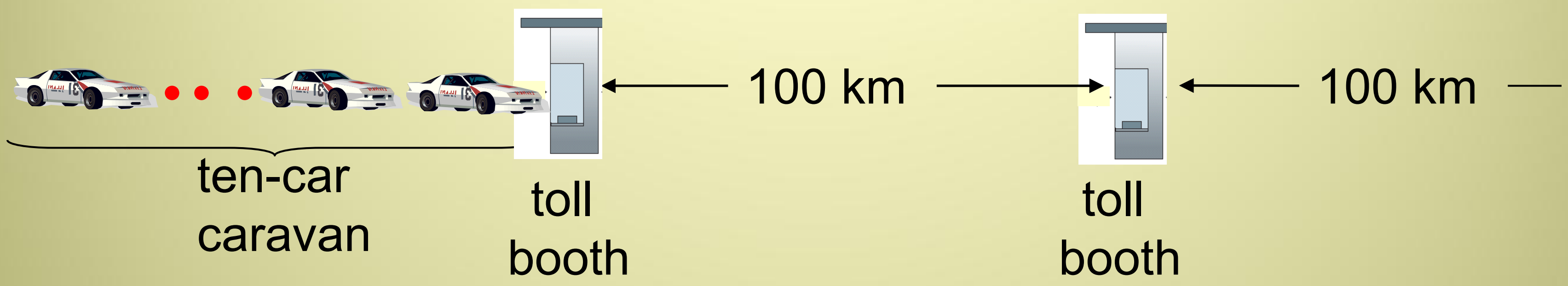
- *L*: packet length (bits)
- *R*: link *bandwidth (bps)*
- $d_{trans} = L/R$

d_{trans} and d_{prop} *very* different

d_{prop}: propagation delay:

- *d*: length of physical link
- *s*: propagation speed in medium ($\sim 2x10^8$ m/sec)
- $d_{prop} = d/s$

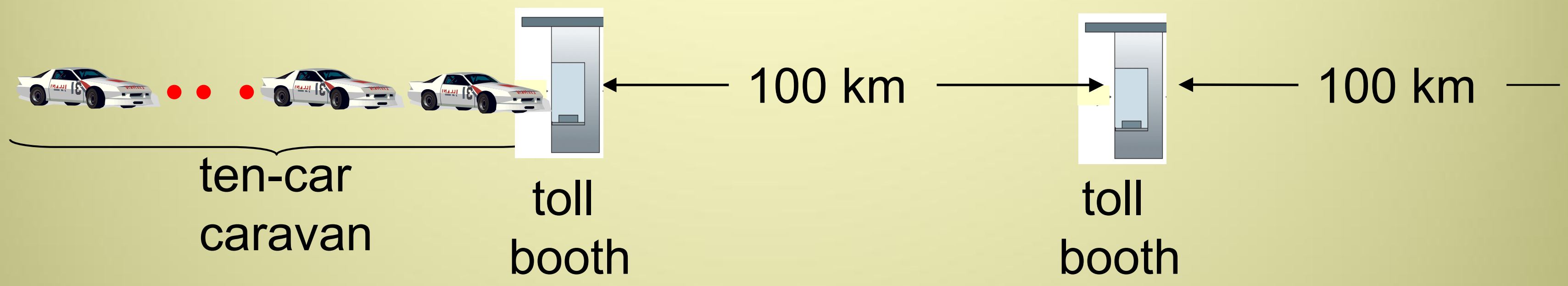
Caravan analogy



- cars "propagate" at 100 km/hr
- toll booth takes 12 sec to service car (bit transmission time)
- car~bit; caravan ~ packet
- *Q*: How long until caravan is lined up before 2nd toll booth?

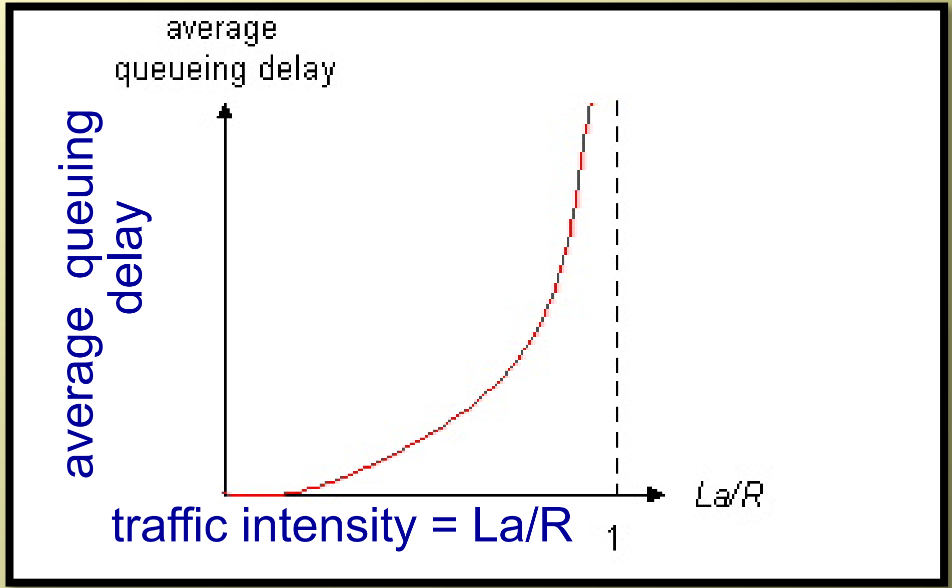
- time to "push" entire caravan through toll booth onto highway = 12*10 = 120 sec
- time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr
- *A:* 62 minutes

Caravan analogy (more)



- suppose cars now "propagate" at 1000 km/hr
- and suppose toll booth now takes 60 seconds to service a car
- *Q:* Will cars arrive to 2nd booth before all cars serviced at first booth?
  - *A: Yes!* after 7 min, 1st car arrives at second booth; three cars still at 1st booth.

Queueing delay (revisited)



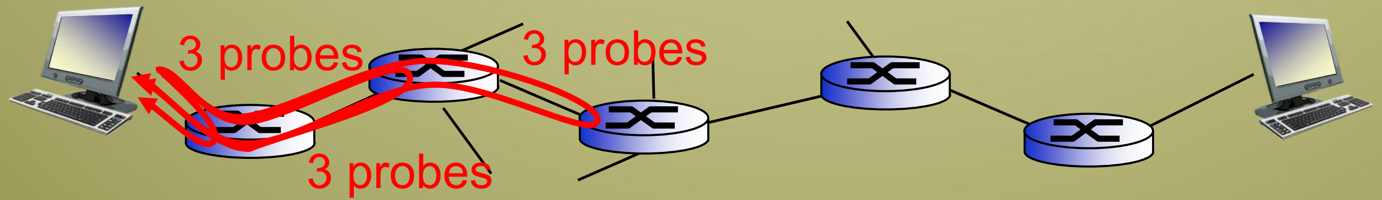
- *R:* link bandwidth (bps)
- *L:* packet length (bits)
- a: average packet arrival rate (# of packets/sec)

- **Traffic intensity**: *La/R*

- *La/R* ~ 0: avg. queuing delay small
- *La/R* → 1: avg. queuing delay large
- *La/R* > 1: more "work" arriving than can be serviced, average delay infinite!

"Real" Internet end-to-end delays and routes

- end-to-end delay: total delay between a source and destination
- provides 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.



“Real” Internet delays, routes

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

3 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

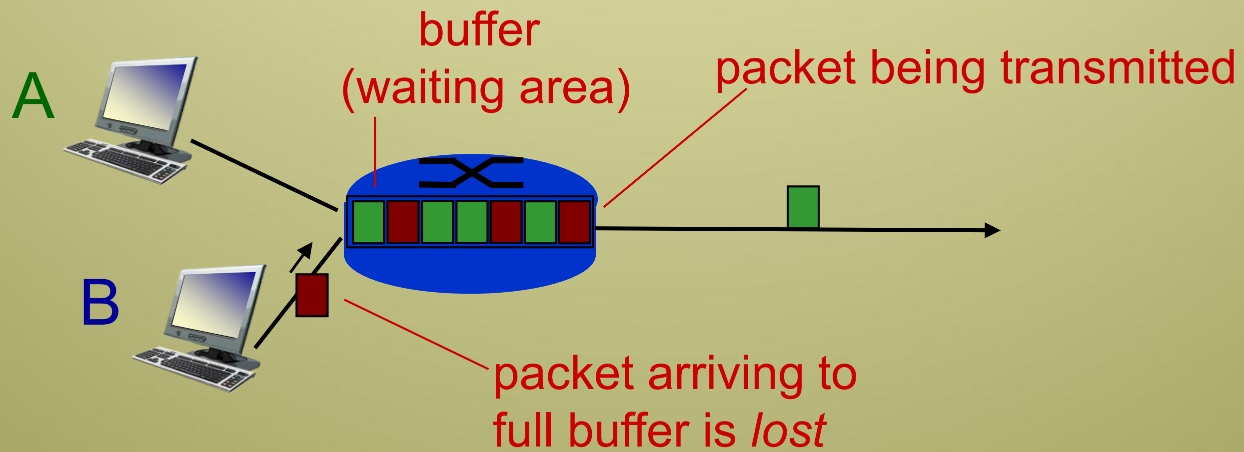
trans-oceanic link

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

* Do some traceroutes from exotic countries at www.traceroute.org

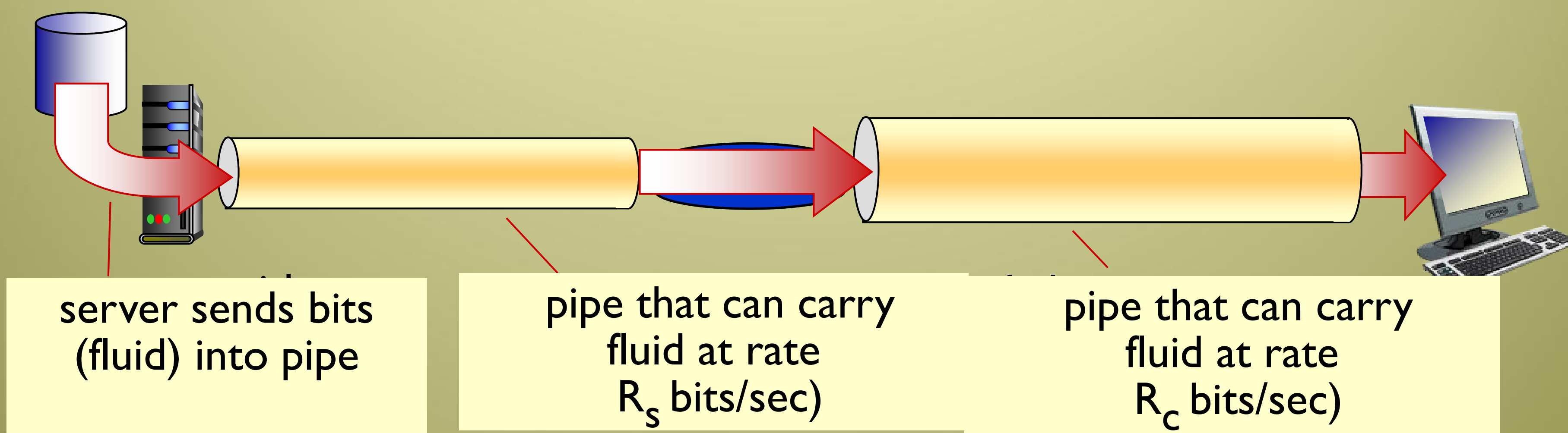
Packet loss

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



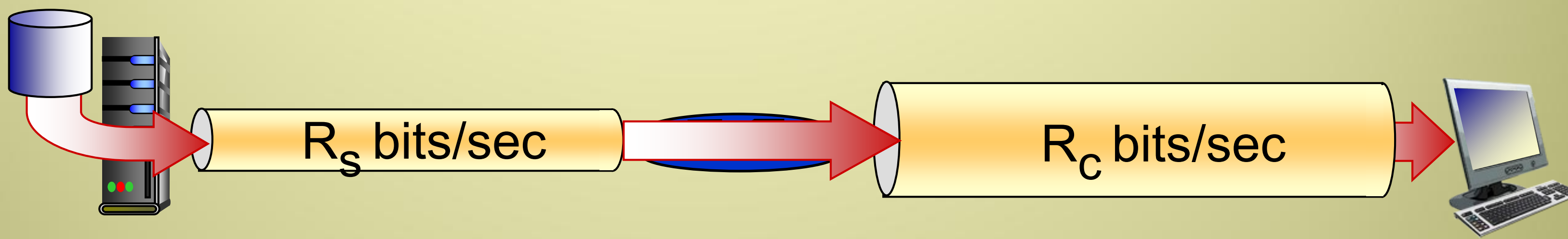
Throughput

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

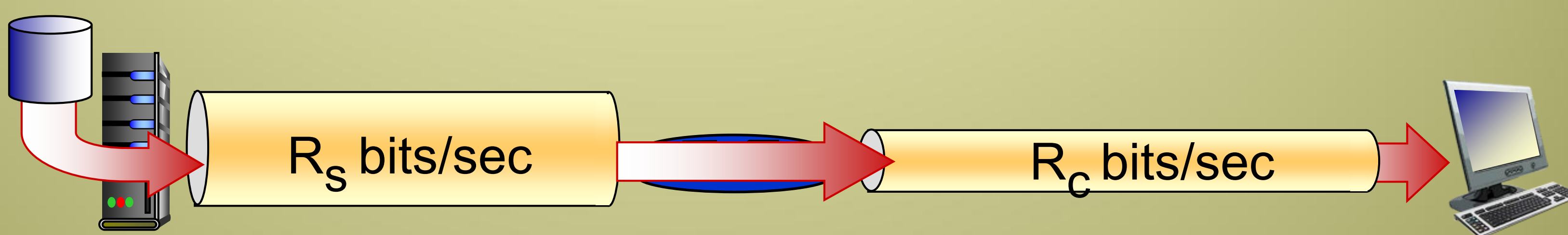


Throughput (more)

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



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

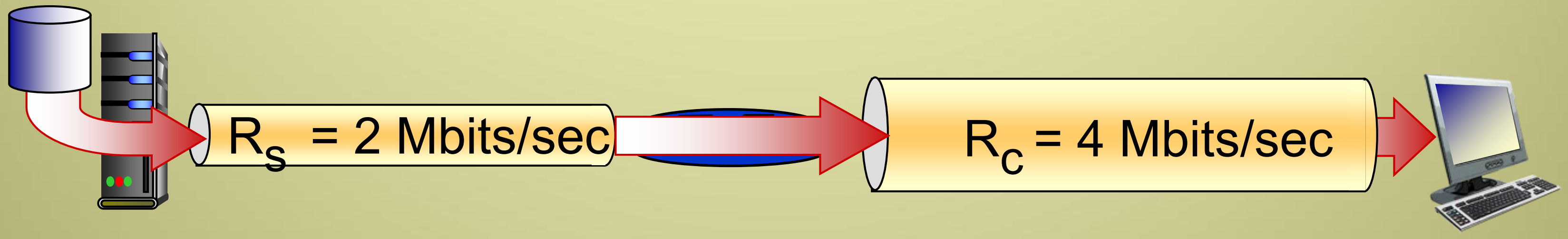


bottleneck link

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

Throughput (more)

- Example: what is the needed **time** to send a music file of size 32Mbit over the following network if R_s = 2Mbps and R_c = 4Mbps?



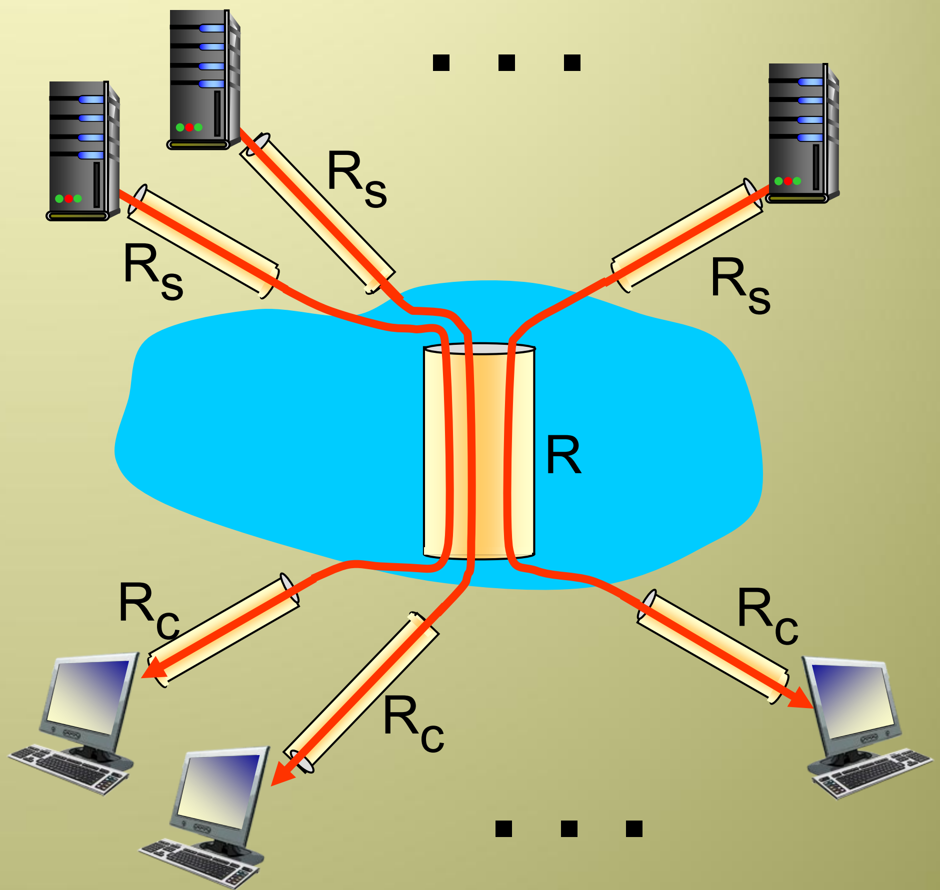
- Time needed = 32M/2Mbps = 16 seconds

Throughput: Internet scenario

- Assume 10 servers and 10 clients are connected to the core of the network

- per-connection end-end throughput: $\min(R_c, R_s, R/10)$

- in practice: R_c or R_s is often bottleneck



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

Protocol "layers" – The ISO OSI Vision

Networks are complex, with 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?

Open Systems & The OSI Model

- *Open system:* A set of protocols that would allow any two different systems to communicate regardless of their underlying architecture

- The **Open System Interconnect** (**OSI**) Model:
  - Introduced by ISO
  - Employs 7 layers, where each layer performs specific functions and communicate with the one above and below it (**service model**)
  - Higher layers deal more with the user applications, services and activities
  - Lower layers deal more with the actual transmission of information
  - Advantages of layered model?

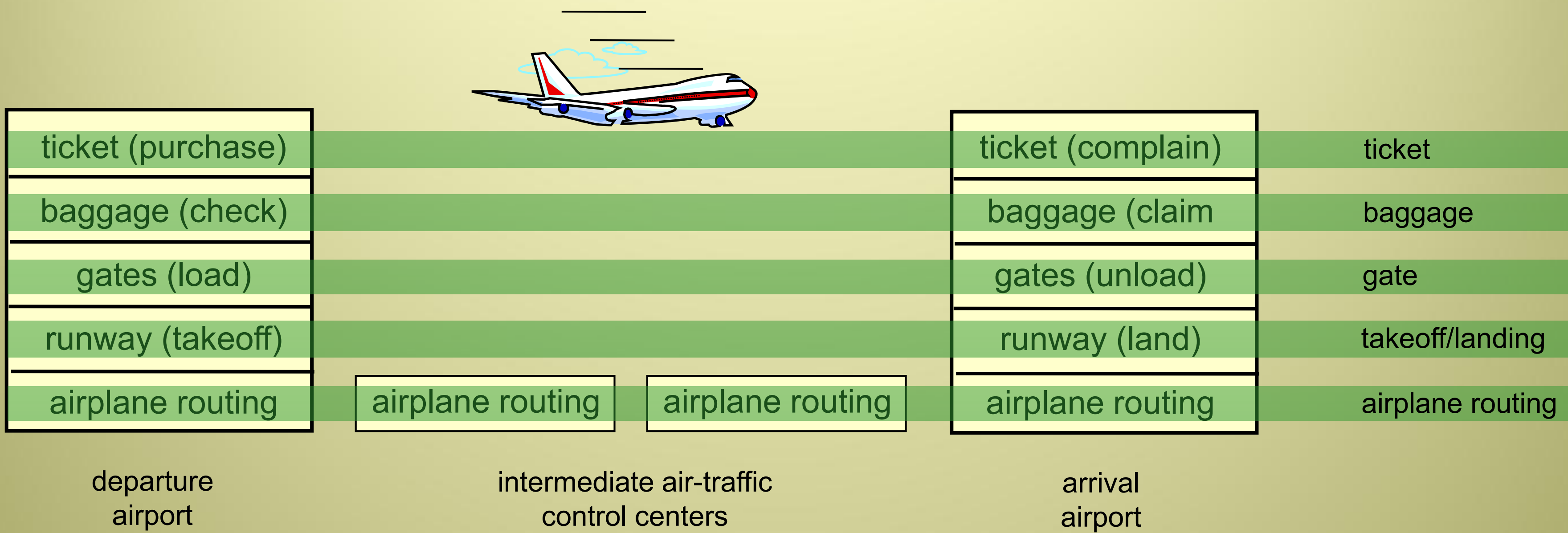
Organization of air travel

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



layers: each layer implements a service

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

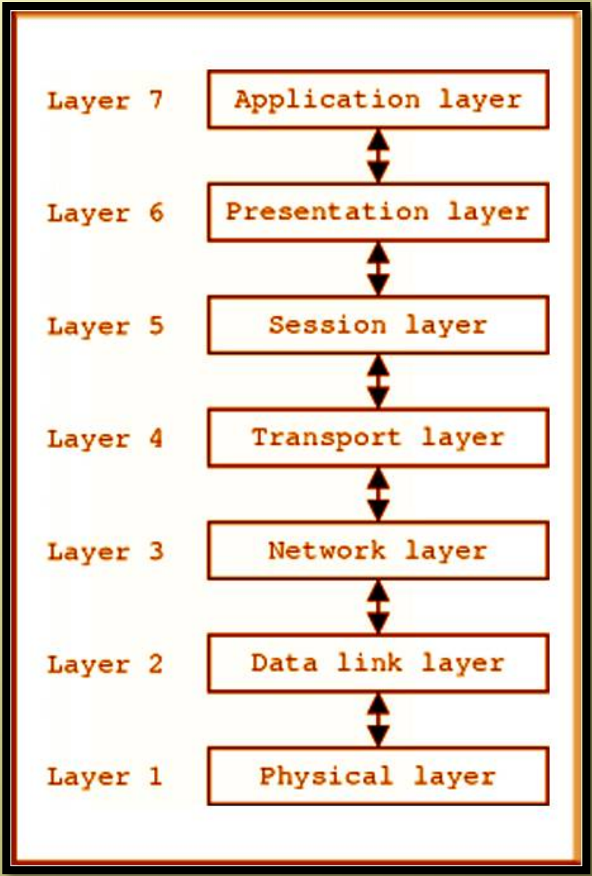
Why layering?

dealing with complex systems:

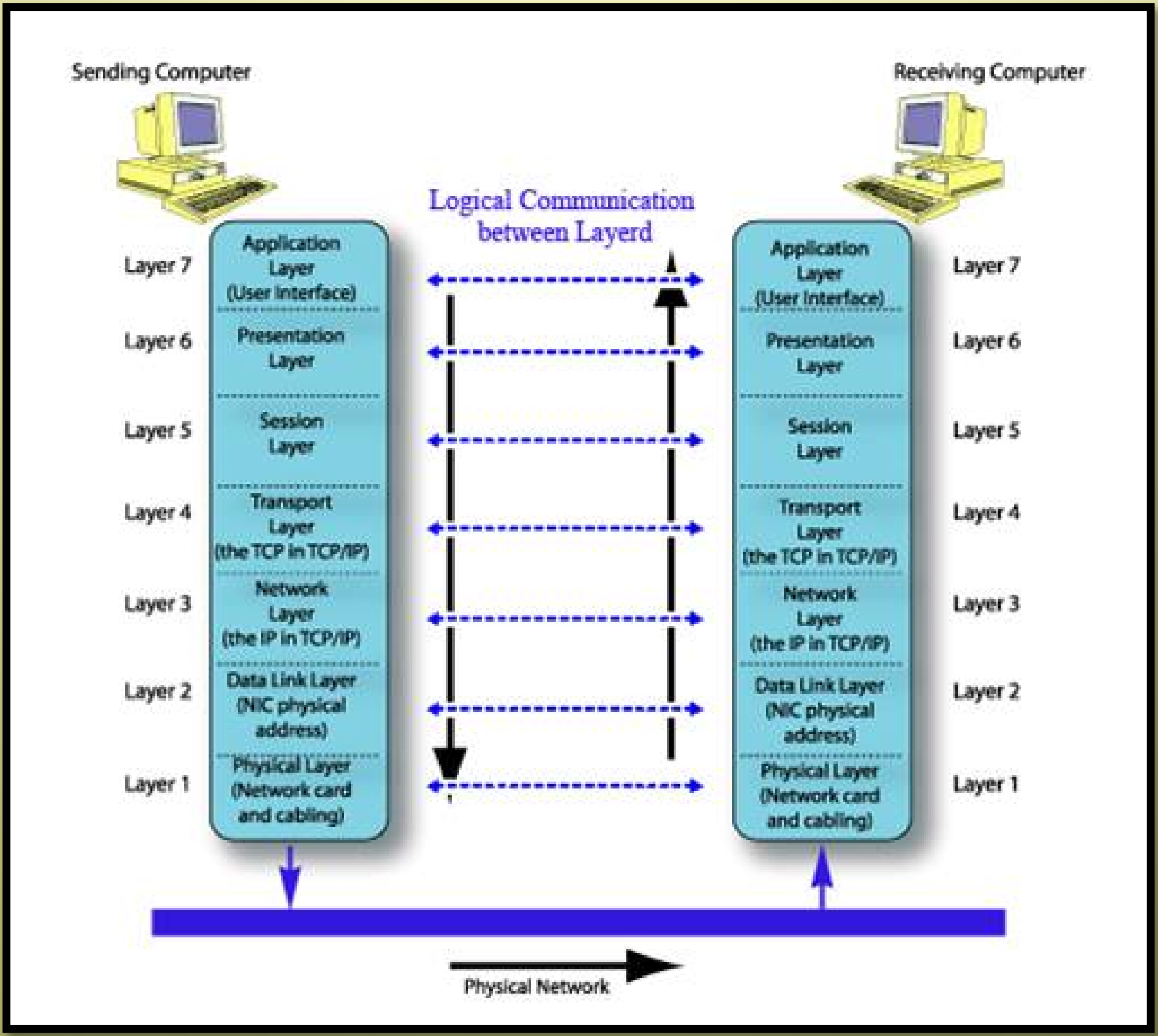
- explicit structure allows identification, relationship of complex system's pieces
  - layered *reference model* for discussion
- modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system
  - e.g., change in gate procedure doesn't affect rest of system
- layering considered harmful?

ISO/OSI reference model

- *application:* supporting network applications
  - FTP, SMTP, HTTP, DNS
- *presentation:* allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- *session:* synchronization, checkpointing, recovery of data exchange
- *transport:* process-process data transfer (**segments**)
  - TCP, UDP
- *network:* routing of **datagrams** from source to destination
  - IP, routing protocols, billings
- *link:* data transfer between neighboring network elements (**frames**)
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits "on the wire"- copper, TP, Fiber, etc.

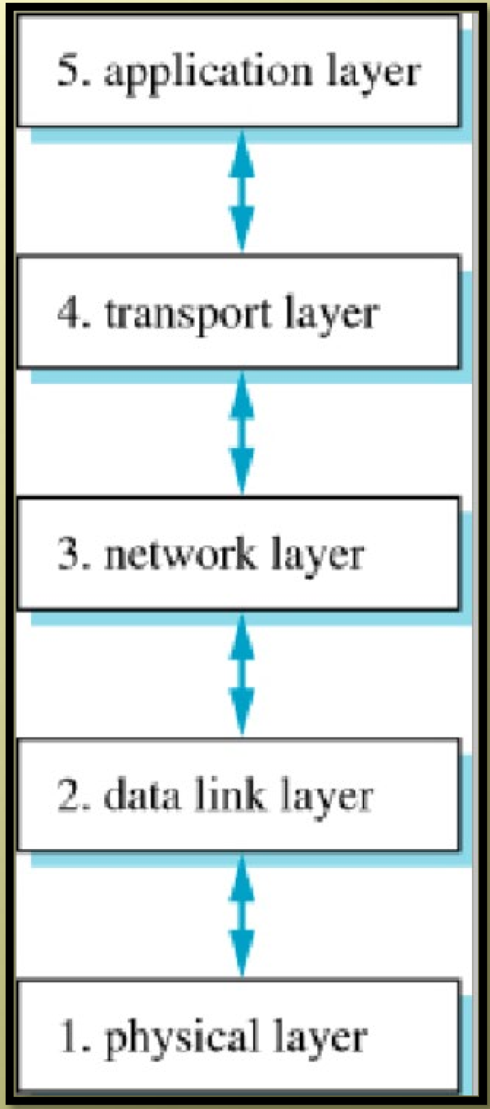


ISO/OSI model

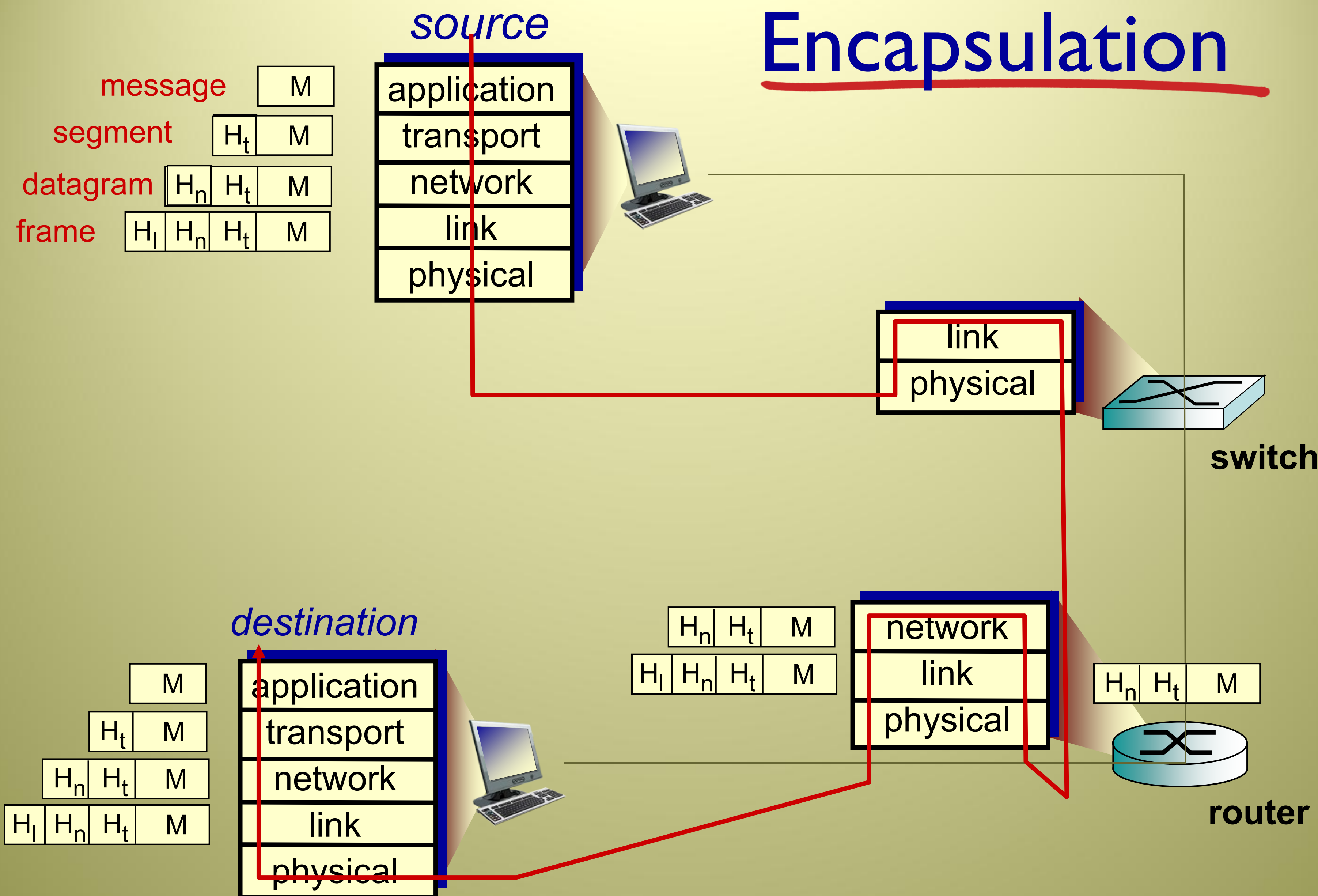


Internet protocol stack

- The Internet has a similar, not identical layers to the ones of the OSI
- The lower 4 layers roughly correspond to the lower 4 layers of OSI
- Functionality of the highest 3 layers of OSI are either omitted, or incorporated in the 5th layer of the Internet
- Layer 4: TCP or UDP
- Layer 5: HTTP, FTP, ..etc



Encapsulation



Network security

- A central topic in the field of computer networking today
- 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!

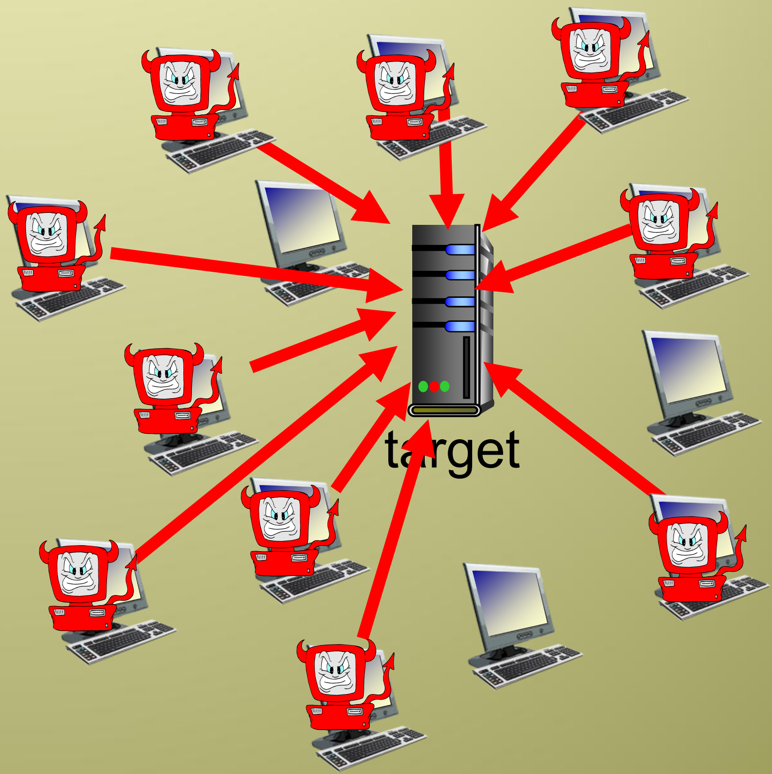
Bad guys: put malware into hosts via Internet

- 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 (i.e. by running a vulnerable network application to which an attacker can send malware without user interventions)
- 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

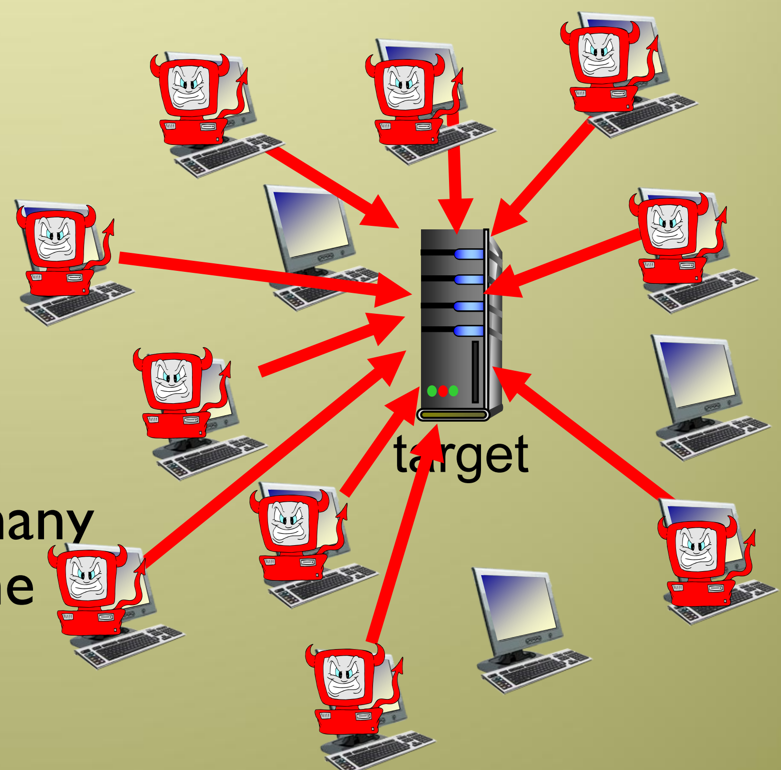
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Bad guys: attack server, network infrastructure

Most DoS attacks fall in one of three categories:

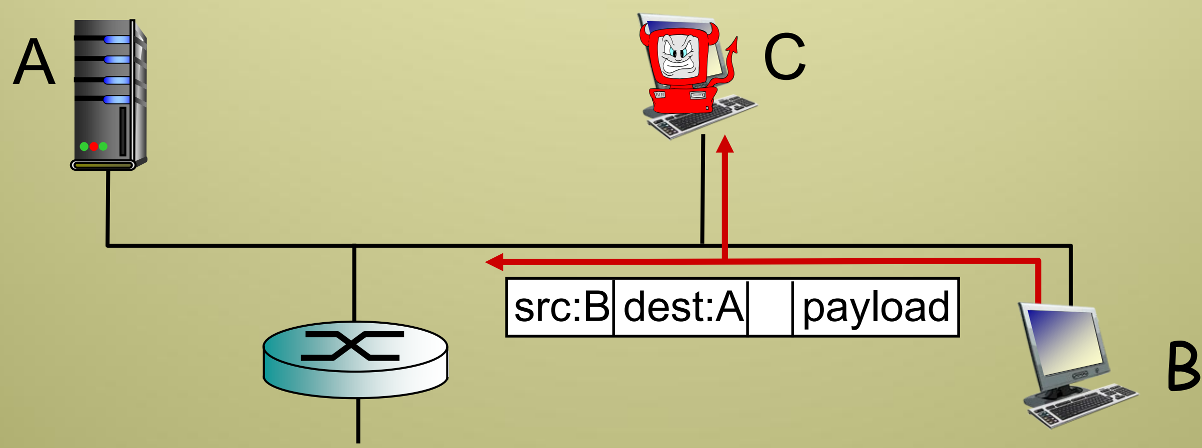
- *Vulnerability attack*: sending well-crafted messages to the vulnerable application resulting in it being stopped or crashed
- *Bandwidth flooding*: send too many packets that the access link to the server becomes clogged, preventing other packets from reaching the server
- *Connection flooding*: establish many open TCP connections that the server stops accepting any further connections



Bad guys can sniff packets

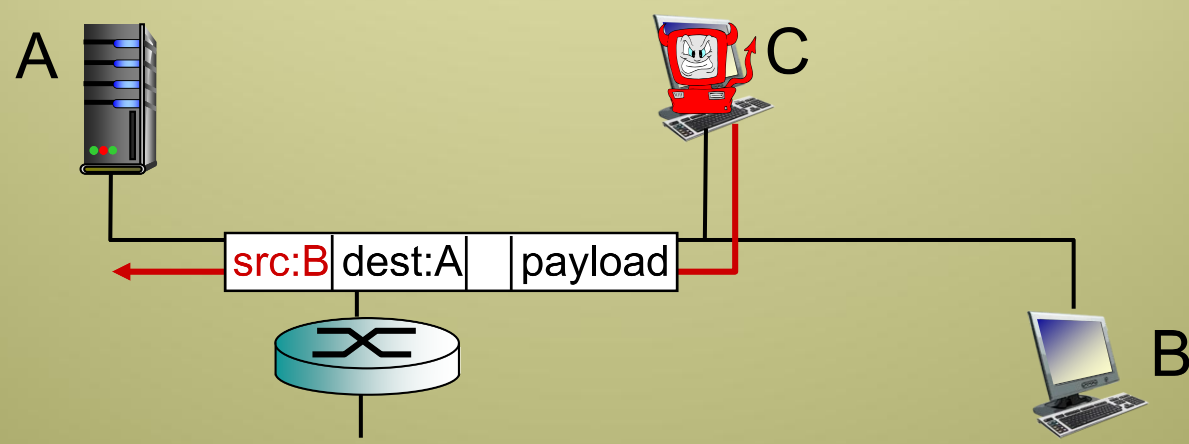
packet "sniffing":

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



Bad guys can use fake addresses

IP spoofing: send packet with false source address, hence fooling the receiver as if the message was from a trusted sender



… *lots more on security to come*