CHALMERS UNIVERSITY OF TECHNOLOGY | UNIVERSITY OF GOTHENBURG

Course on Computer Communication and Networks

Lecture 1 & part of lecture 2
Chapter 1: Introduction

EDA344/DIT 420, CTH/GU

Based on the book Computer Networking: A Top Down Approach, Jim Kurose, Keith Ross, Addison-Wesley.

Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

the Internet: "nuts and bolts" view (1)

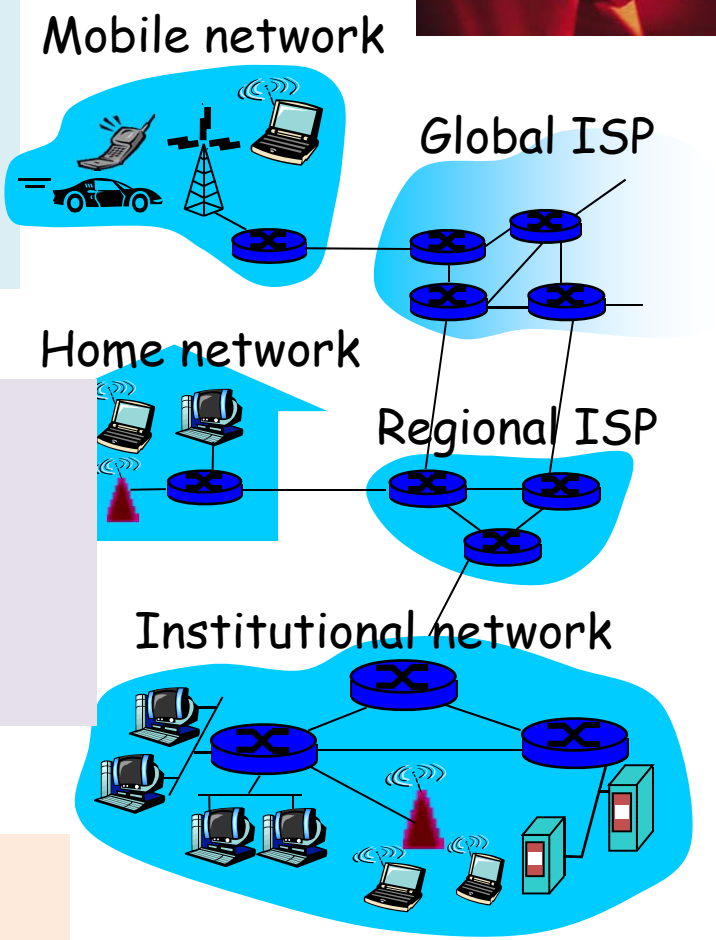
- millions of connected computing devices: *hosts = end systems*
  - running *network apps*

PC

server

wireless laptop

cellular handheld



access points

wired links

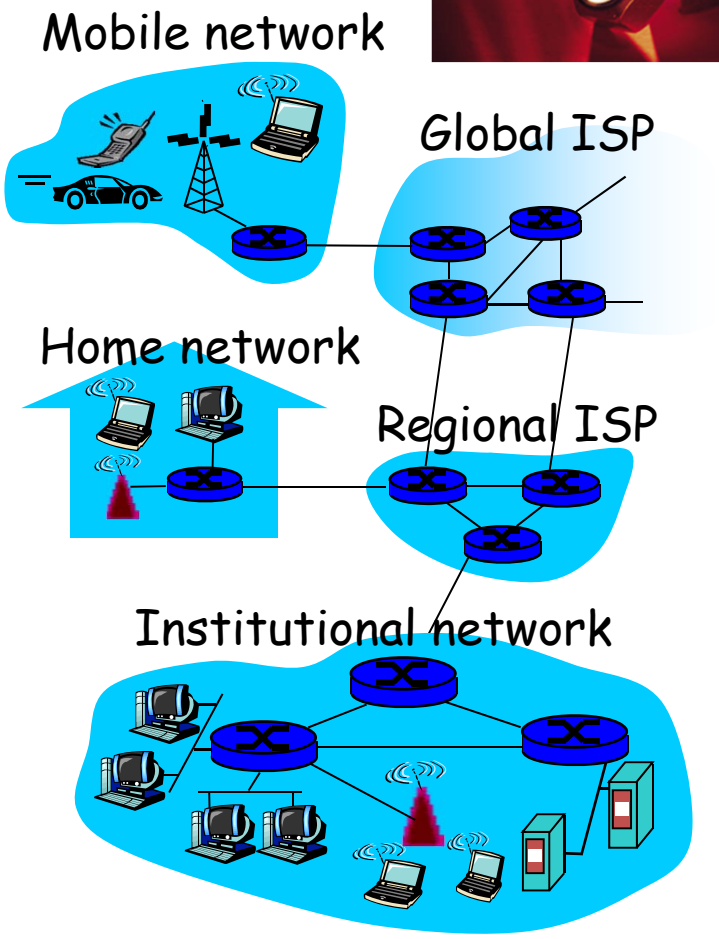
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = *bandwidth*

router

- *routers:* forward packets (chunks of data)

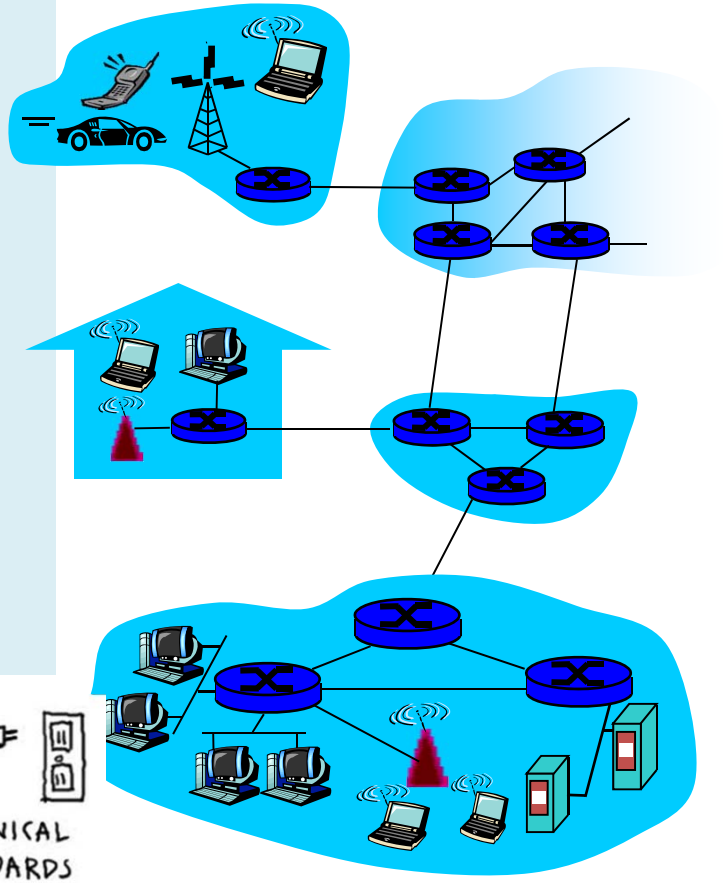
the Internet: "nuts and bolts" view (2)

- *protocols* control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, Skype, Ethernet
- *Internet:* "network of networks"
  - loosely hierarchical
  - public Internet versus private intranet



the Internet: 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



Internet standards

- RFC: Request for comments
- IETF: Internet Engineering Task Force

Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

Networks are complex

- many “pieces”:
  - hosts
  - routers
  - links of various media
  - applications
  - hardware, software

Question:

Is there any hope of *organizing* structure, study, development of networks?

Layers of abstraction

Dealing with complex systems:

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

Terminology: Protocols, Interfaces

- Each layer offers **services** to the upper layers (shielding from the implementation details)
  - **service interface**: across layers in same host
- Layer *n* on a host carries a conversation with layer *n* on another host
  - **host-to-host interface**: defines messages exchanged with peer entity
- Network architecture (set of layers, interfaces) vs **protocol** stack (protocol implementation)

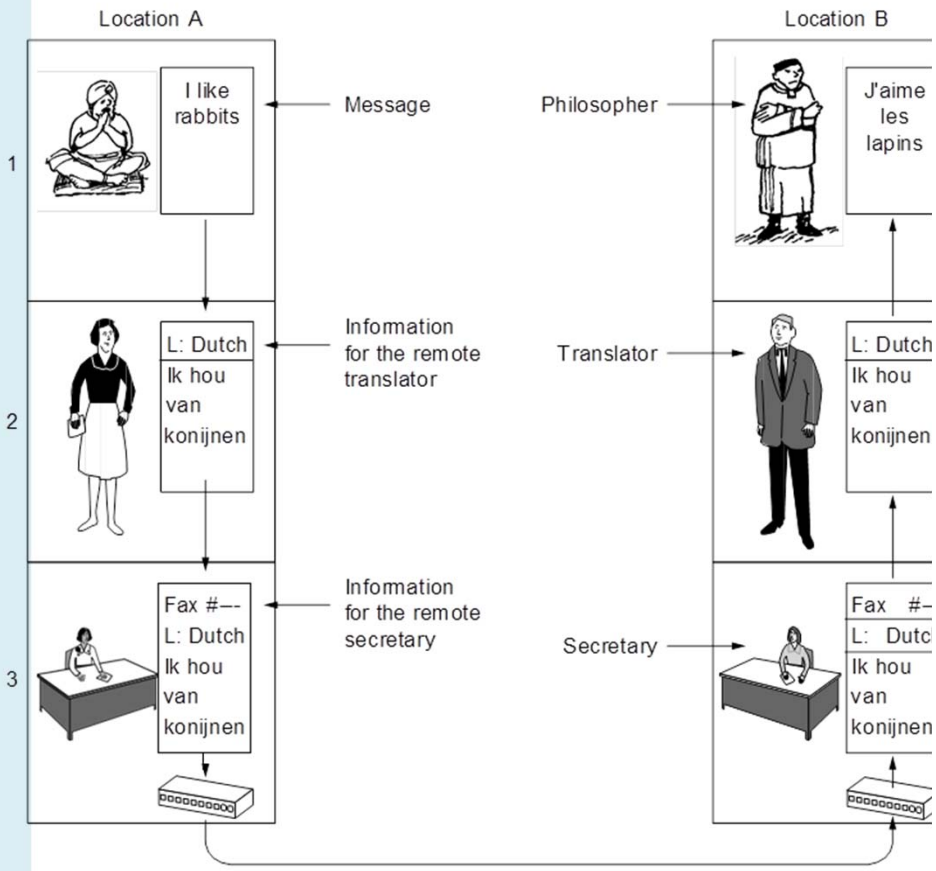
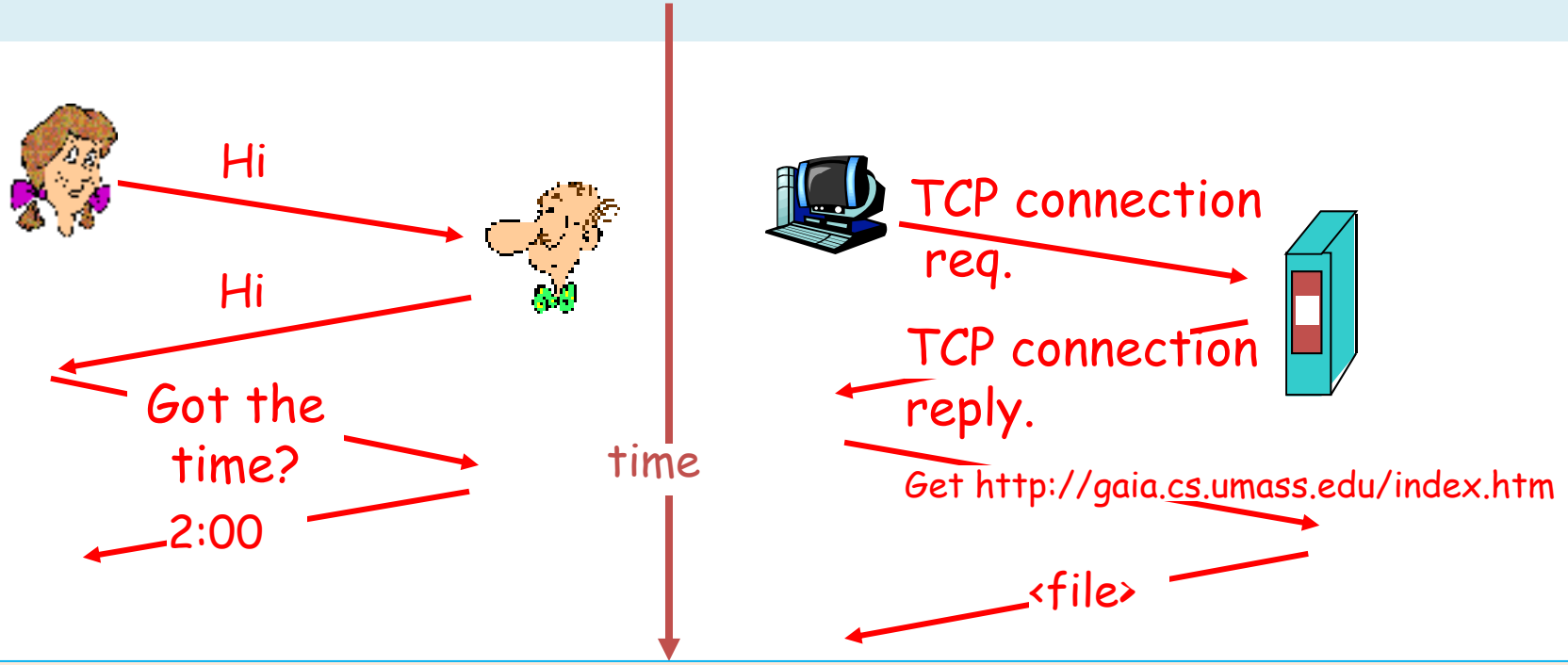


Fig. 1-10. The philosopher-translator-secretary architecture.

What's a protocol?

a human protocol and a computer network protocol:



host-to-host interface: defines

- messages exchanged with peer entity: *format, order of msgs sent and received among network entities*
- *actions taken on msg transmission, receipt*

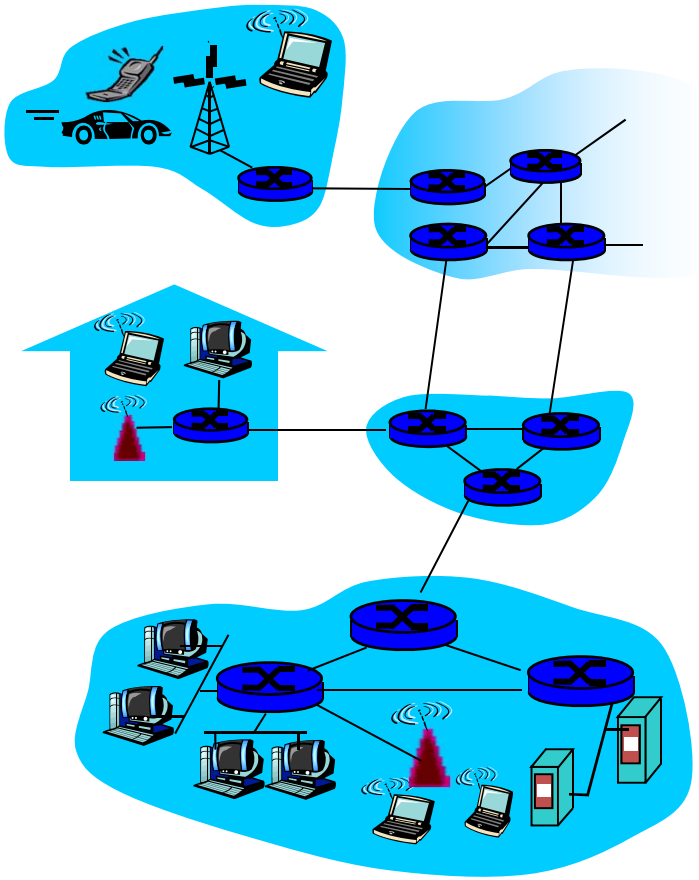
Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

A closer look at (any big) network's structure:

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

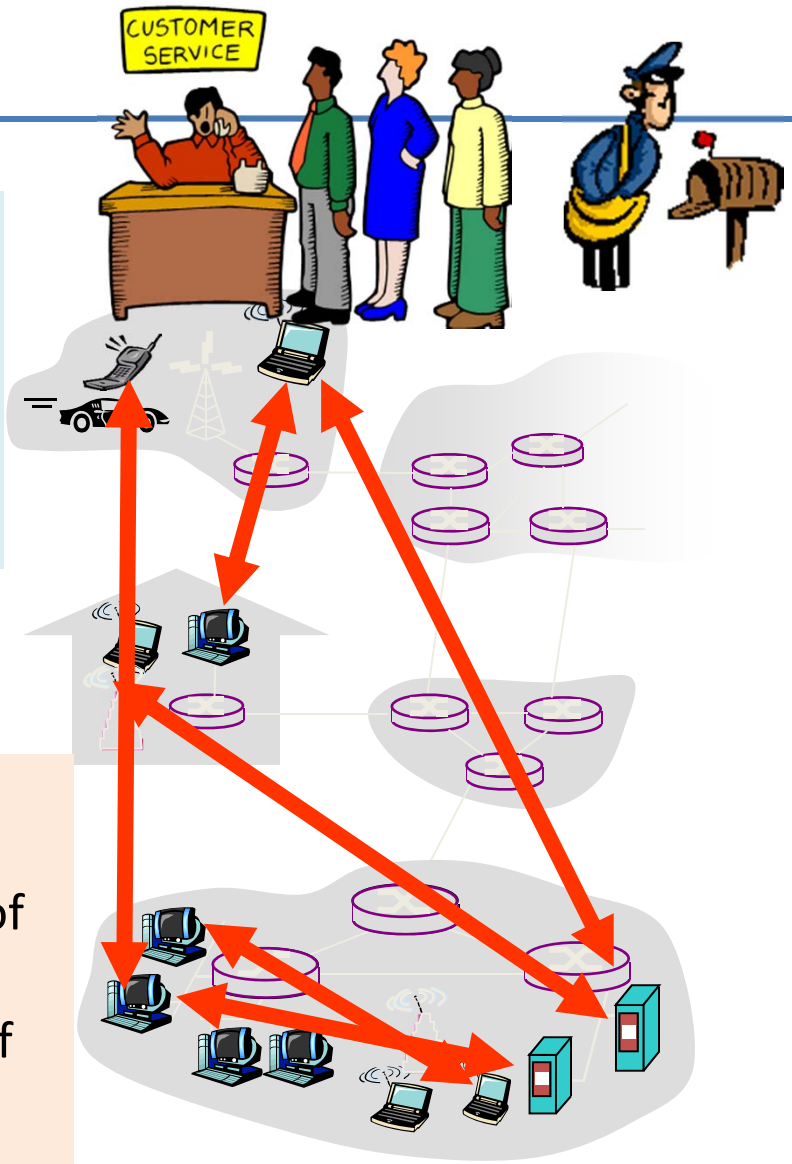
- network core:
  - interconnected routers
  - network of networks



The network edge:

end systems (hosts):

- run application programs e.g. in Internet Web, email, …
- … based on network services available at the edge



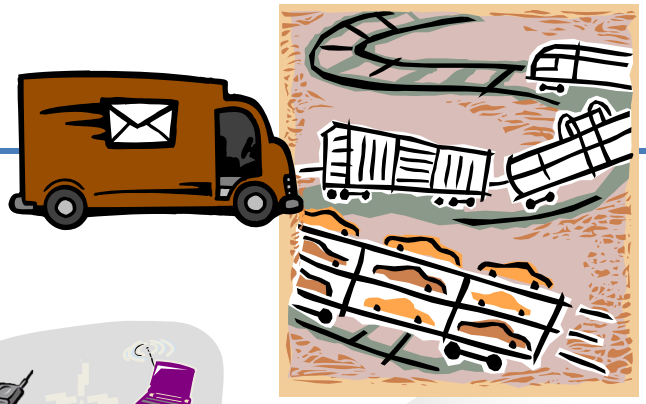
Basic types of service offered by the network to applications:

connection-oriented: reliable delivery of the data in the order they are sent

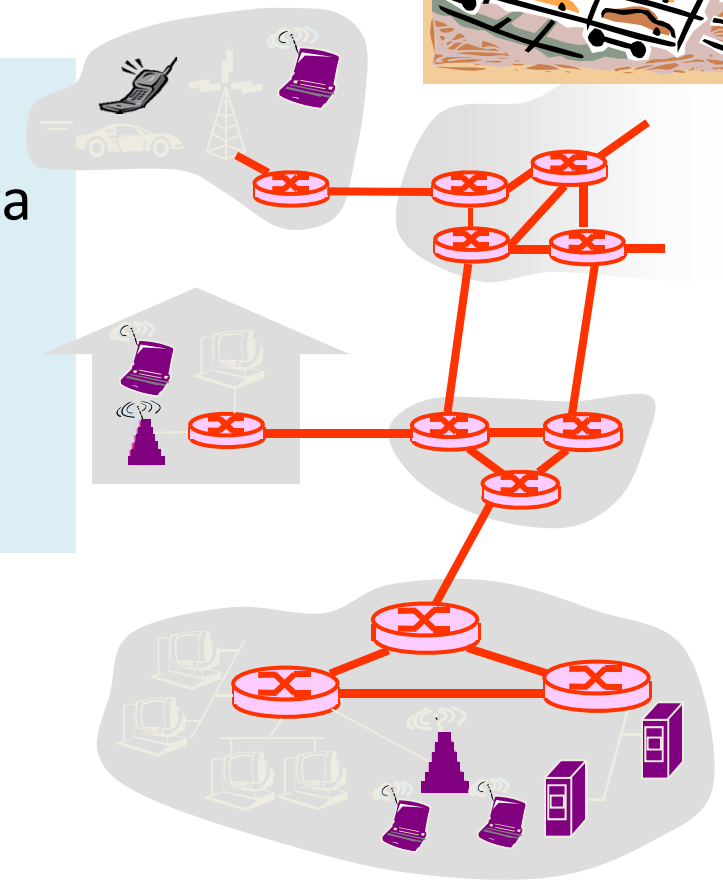
connectionless: "best effort" delivery of the data in arbitrary order

Q: can we think of more types of service?

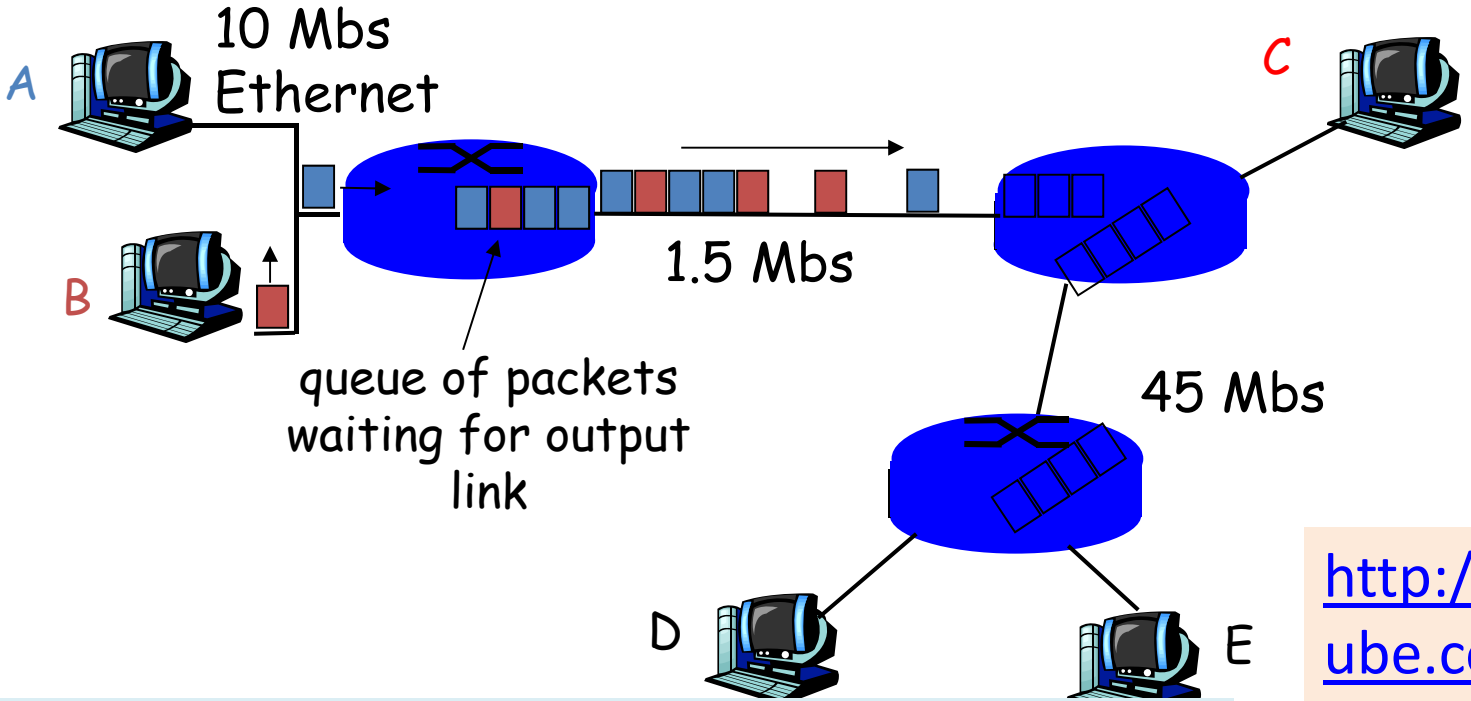
The Network Core



- mesh of interconnected routers
- fundamental question: how is data transferred through net?
- packet-switching: data sent thru net in discrete “chunks”



Network Core: Packet Switching



each end-end data stream divided into *packets*

- packets *share* network resources
- resources used *as needed*

store and forward:

- packets move one hop at a time
  - transmit over link; wait turn at next link

http://www.youtube.com/watch?v=O7CuFlM4V54

nice animation; note some of the terms in narration are not accurate (wrt protocol specifications)

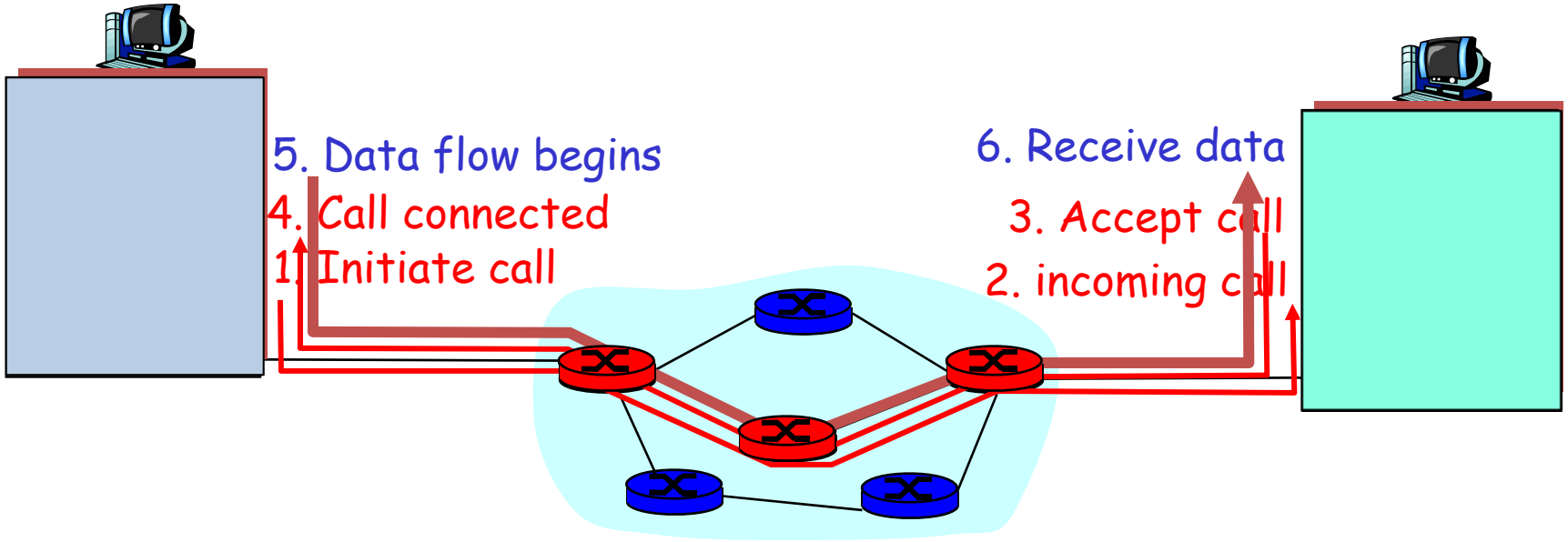
Packet-switched networks: routing

- *What is routing's goal?* find routes from source to destination
  - (Challenge 1) path selection algorithms
  - (Challenge2) Important design issue/type of service offered:
    - **datagram network**:
      - *destination address* determines next hop
      - routes may change during session
    - **virtual circuit network:**
      - fixed path determined at *call setup time*, remains fixed thru session
      - routers maintain per-call state

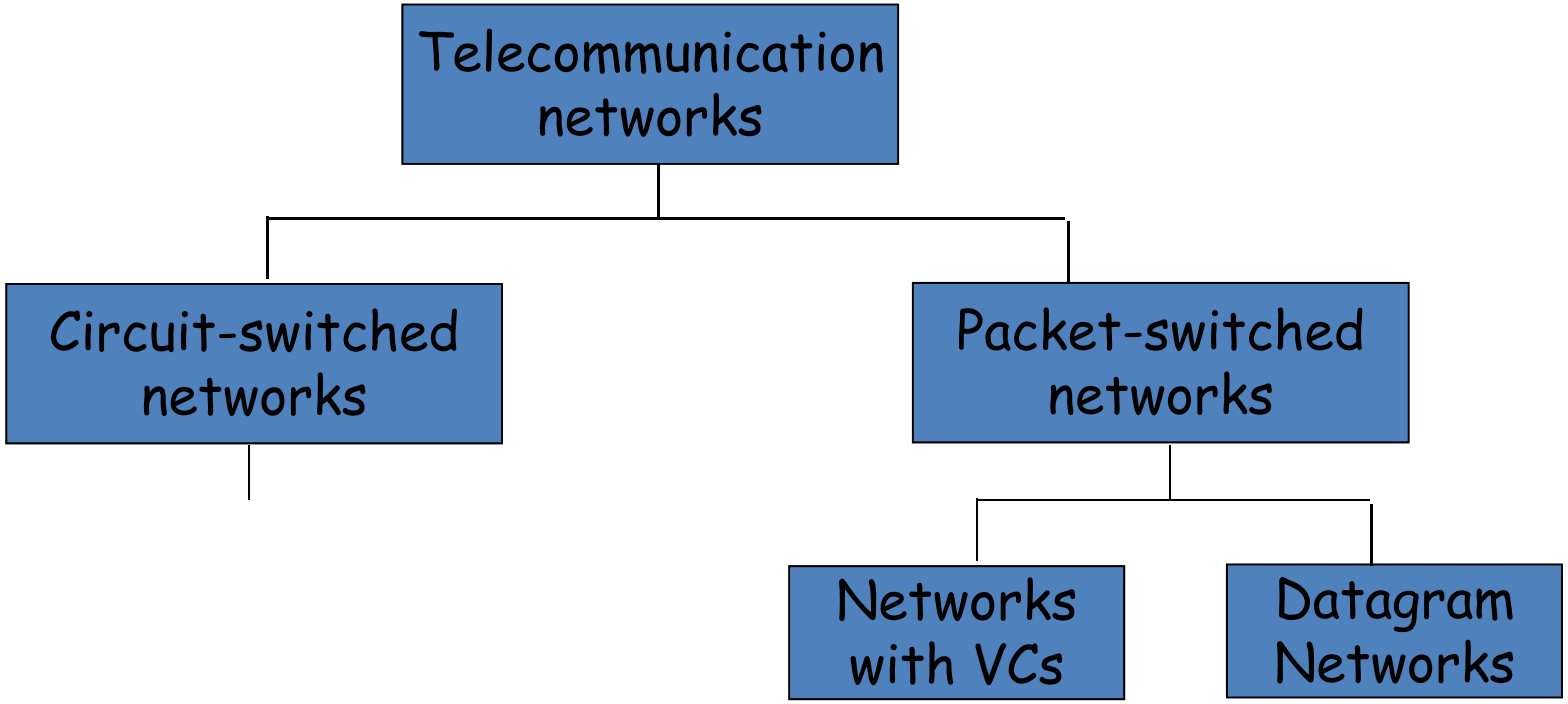
Virtual circuits:

"source-to-dest path behaves almost like a physical circuit"

- call setup, teardown for each call *before* data can flow
  - signaling protocols to setup, maintain, teardown VC
- *every* router maintains "state" for each passing connection
- resources (bandwidth, buffers) may be *allocated* to VC



Network Taxonomy



• Datagram network (eg Internet) cannot be characterized either connection-oriented or connectionless.

• Internet provides both connection-oriented (TCP) and connectionless services (UDP), at the network edge, to apps.

Roadmap

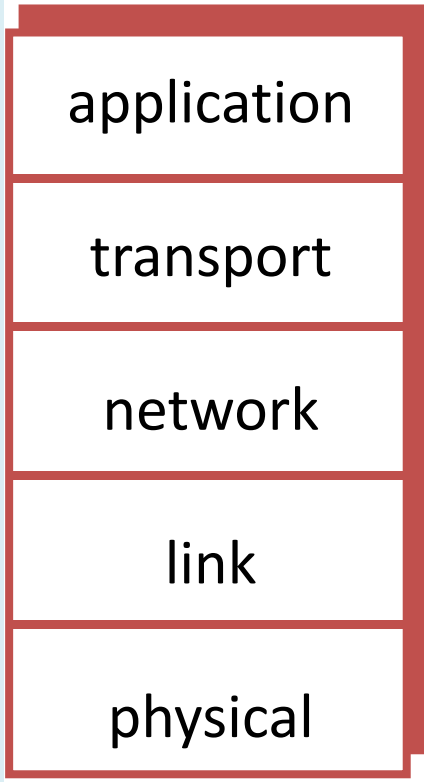
- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

Layering – Some “histrory”:
The OSI Reference Model

- ISO (International Standards Organization) defined the OSI (Open Systems Inerconnect) model to help vendors create interoperable network implementation
- Reduced the problem into smaller and more manageable problems: 7 layers
  - a layer should be created where a different level of abstraction is needed; each layer should perform a well defined function)
  - The function of each layer should be chosen with an eye toward defining internationally standardized protocols
- ``X dot" series (X.25, X. 400, X.500) OSI model implementation (protocol stack)
- Did not really “fly”…

Internet protocol stack

- application: ftp, smtp, http, etc
- transport:
  - connection-oriented, reliable data delivery from source to destination (TCP);
  - connectionless, “best effort” (unreliable) data delivery (UDP)
- network: routing of datagrams from source to destination; best effort service
  - IP, routing protocols
- link: data transfer between neighboring network elements
  - Ethernet, WiFi, …
- physical: bits “on the physical medium”



Internet protocol stack

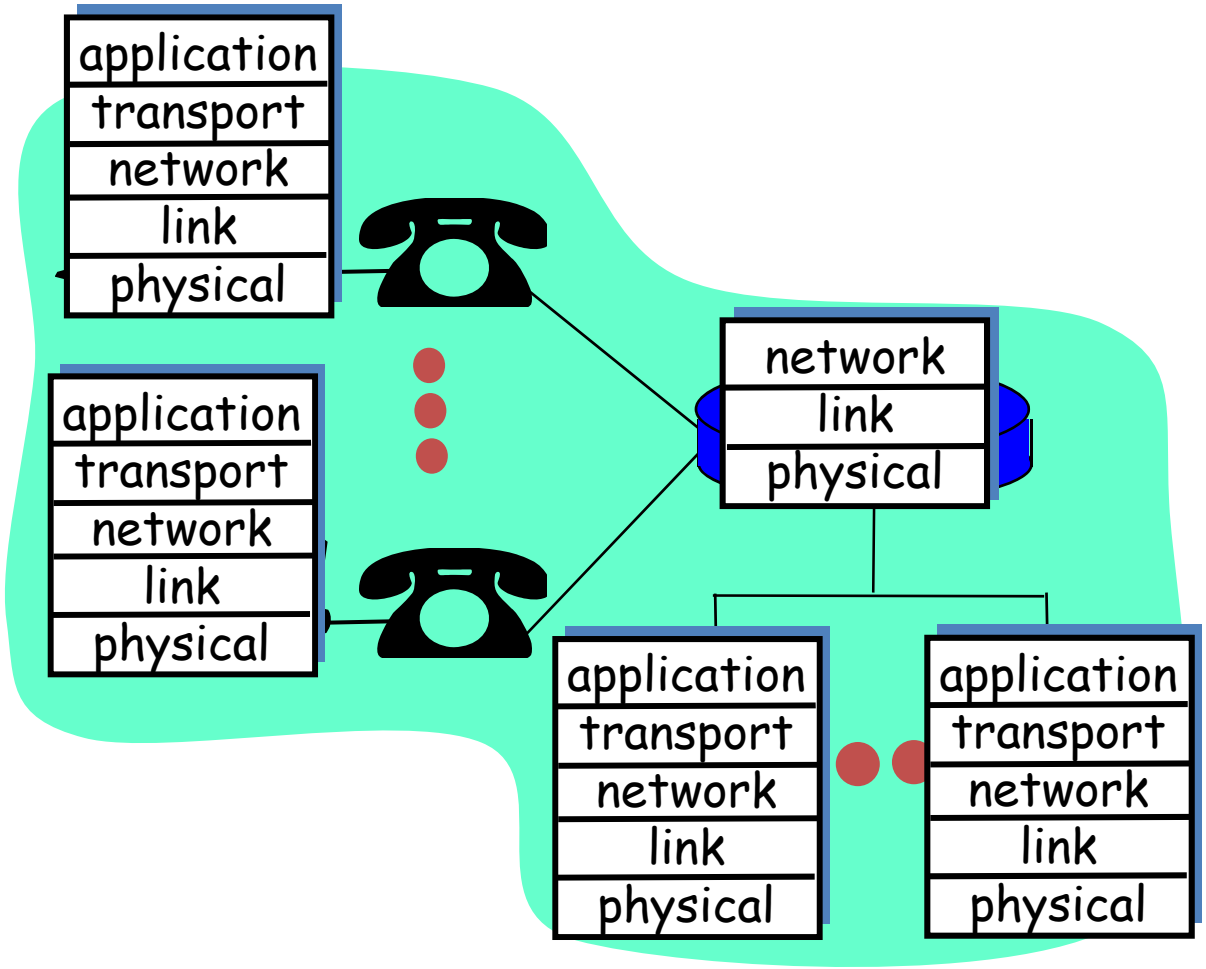
- Architecture simple but not as thoroughly thought as OSI's
  - no clear distinction between interface-design and implementations;
  - hard to re-implement certain layers

- Successful protocol suite (de-facto standard)
  - was there when needed (OSI implementations were too complicated)
  - freely distributed with UNIX

Layering: logical communication

Each layer:

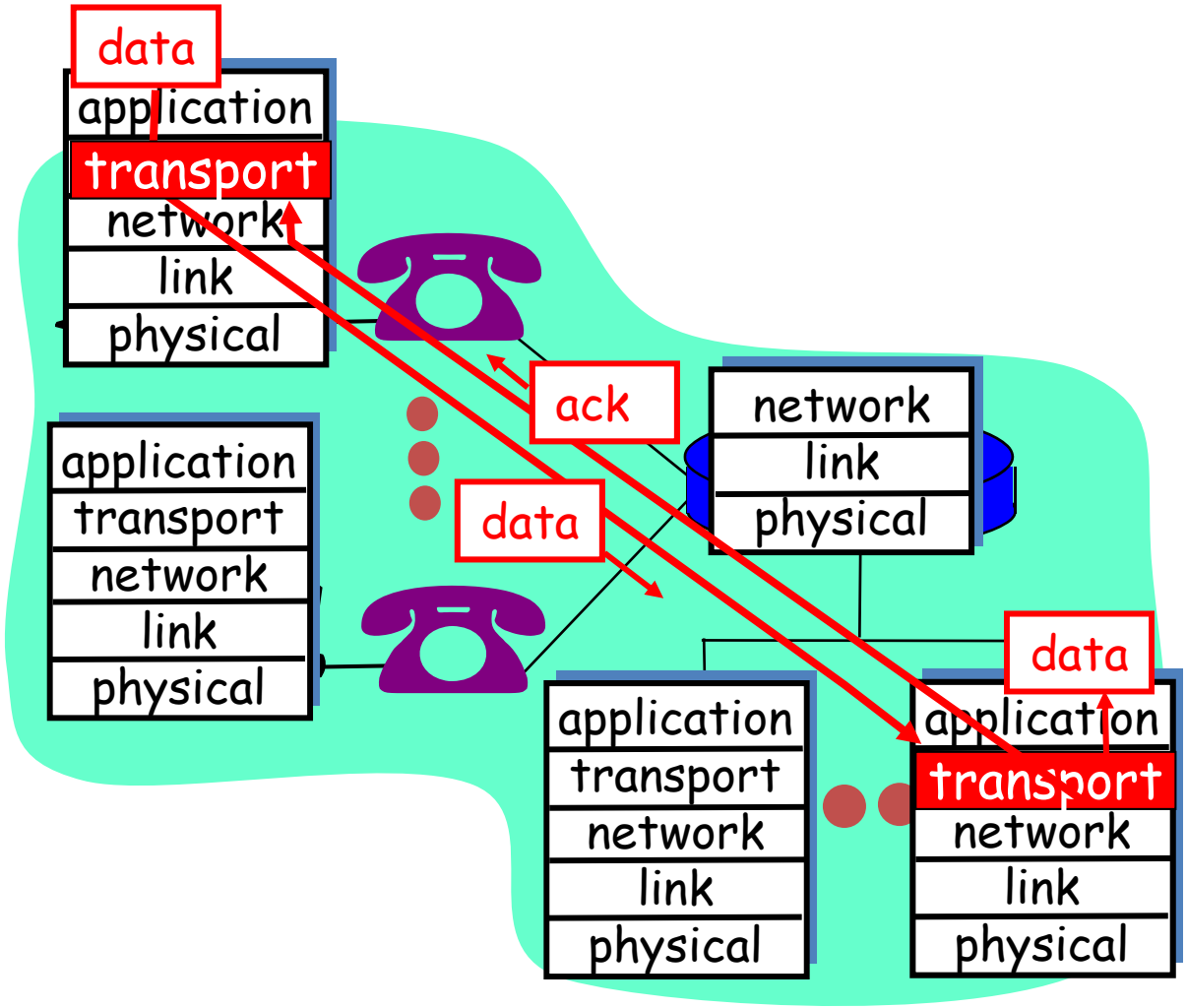
- distributed
- "entities" implement layer functions at each node
- entities perform actions, exchange messages with peers



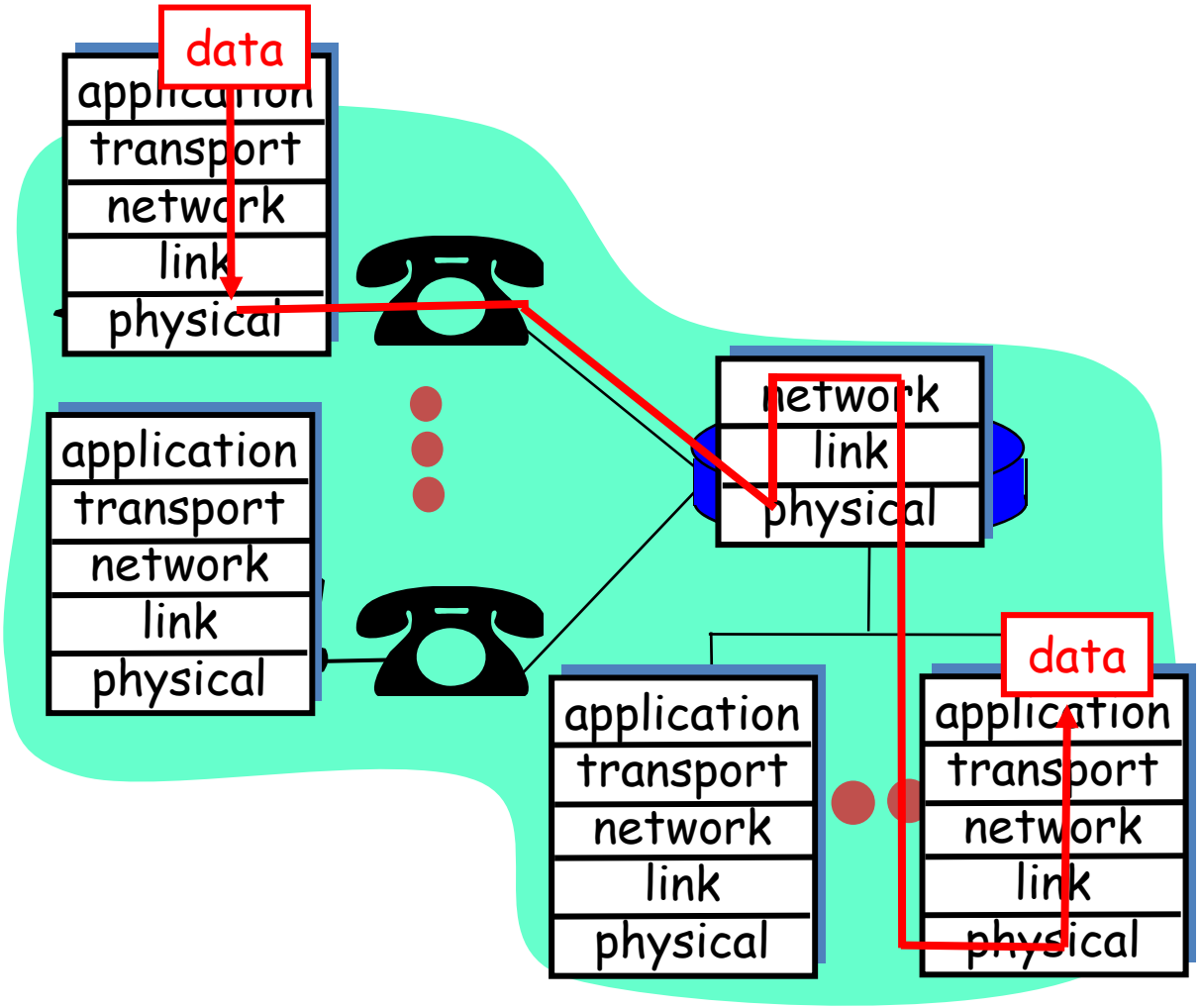
Layering: *logical* communication

E.g.: transport

- take data from app
- add addressing, form “datagram”
- send datagram to peer
- (possibly wait for peer to ack receipt)



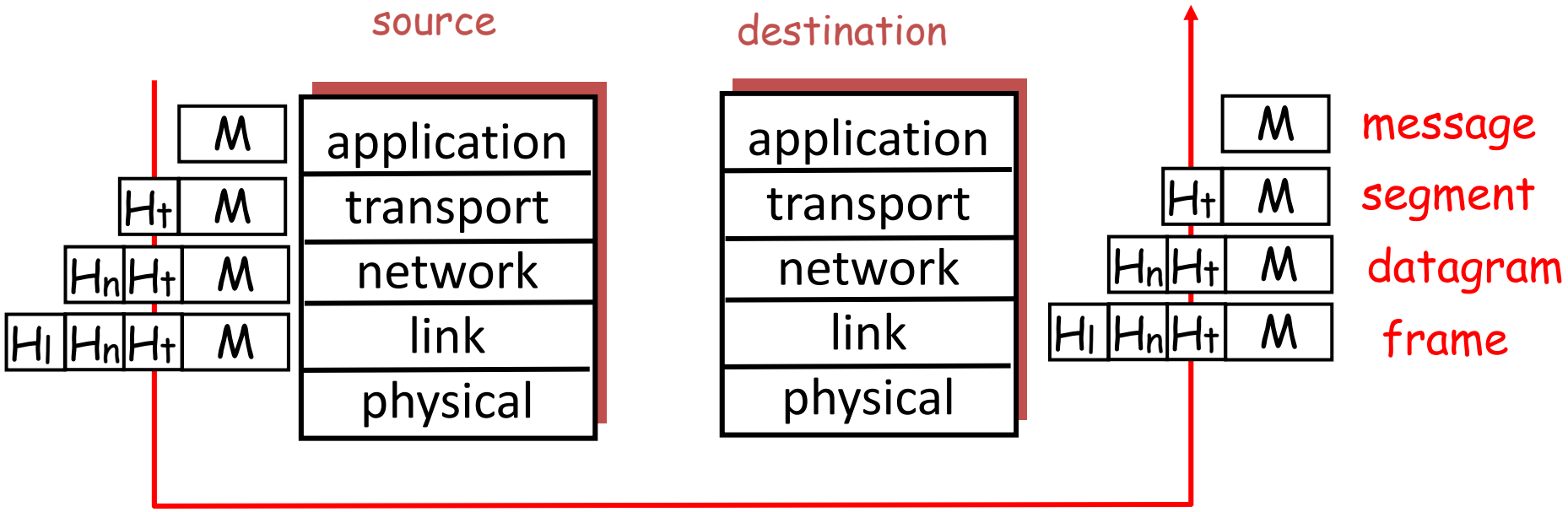
Layering: physical communication



Protocol layering and data

Each layer takes data from above

- adds header information to create new data unit
- passes new data unit to layer below



Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

Delay in packet-switched networks

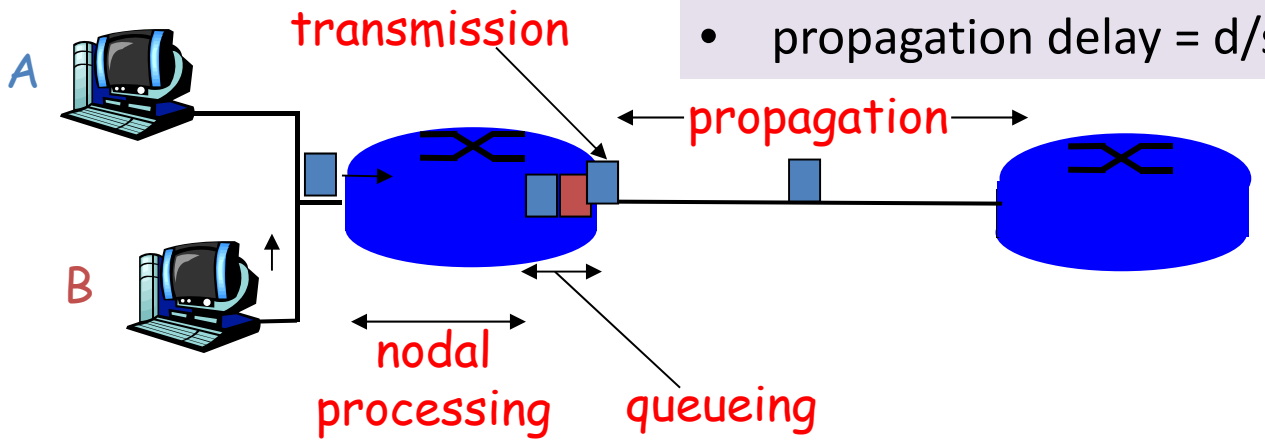
- 1. nodal processing:
  - check bit errors
  - determine output link
- 2. queuing
  - time waiting at output link for transmission
  - depends on congestion level of router

3. Transmission delay:

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

4. Propagation delay:

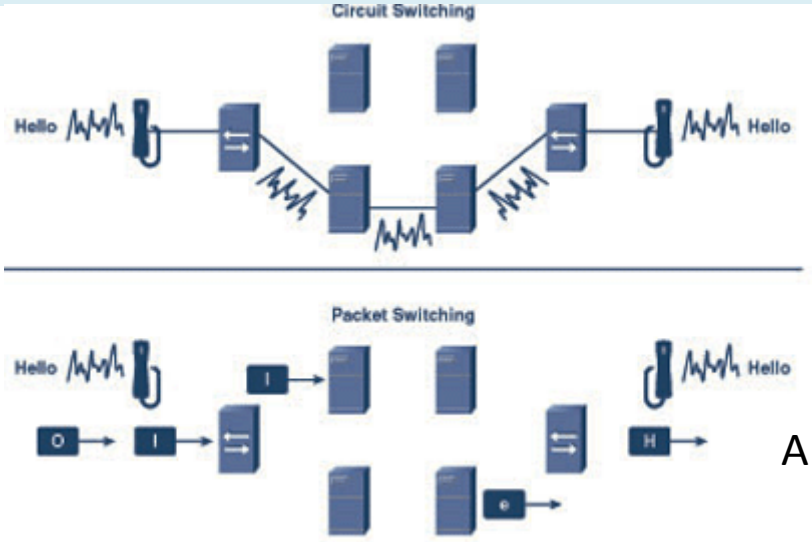
- d = length of physical link
- s = propagation speed in medium (~2×10^8 m/sec)
- propagation delay = d/s

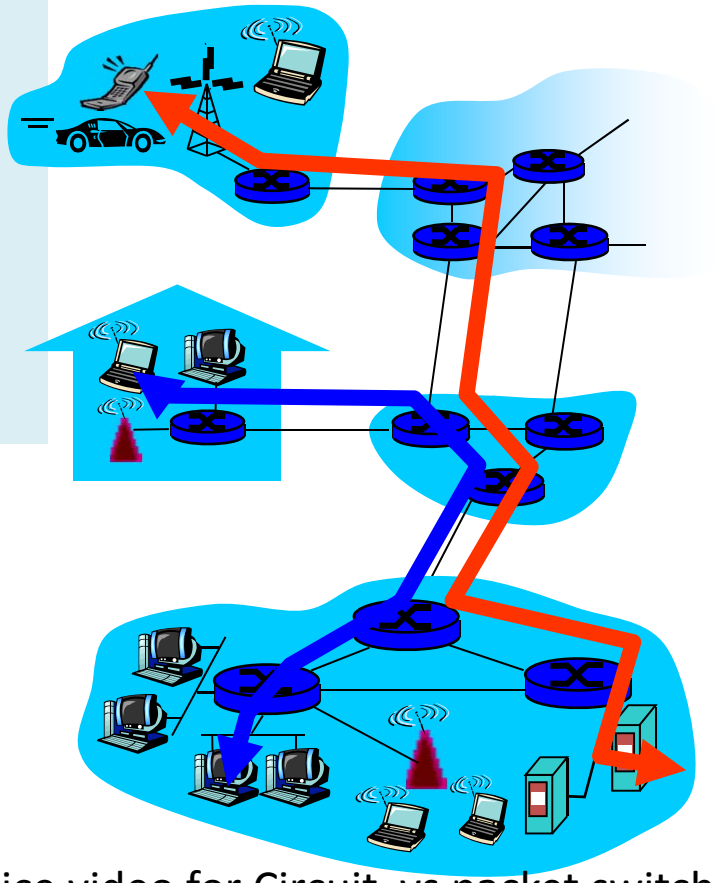


Network Core: Circuit Switching

End-end resources
reserved/dedicated for “call”
(analogue telephony)

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





A nice video for Circuit vs packet switching
http://www.youtube.com/watch?v=Dq1zpiDN9k4&feature=related

Visualize delays: Circuit, message, packet switching

- store and forwar behavior + other delays' visualization *(fig. from "Computer Networks" by A. Tanenbaum,)*

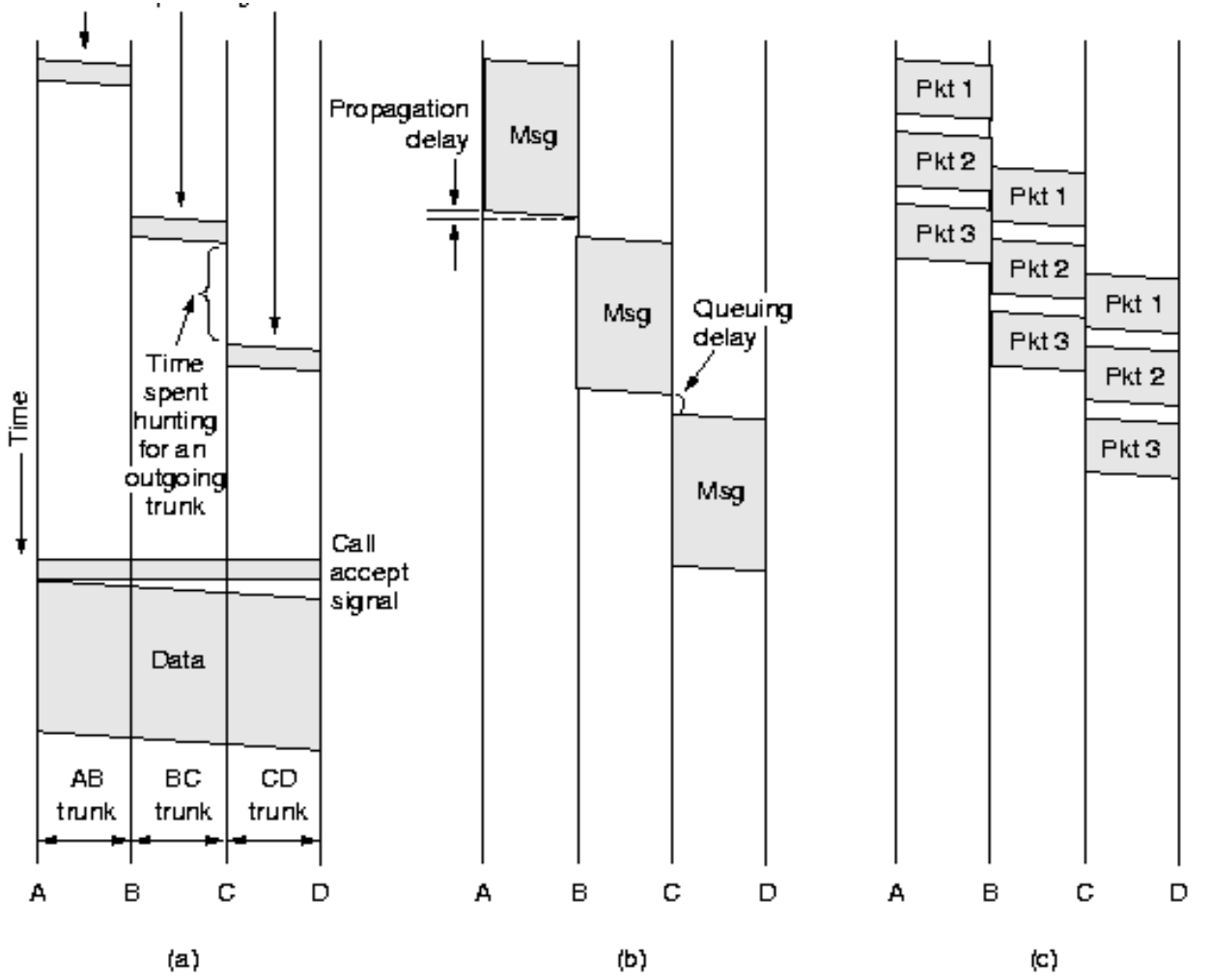
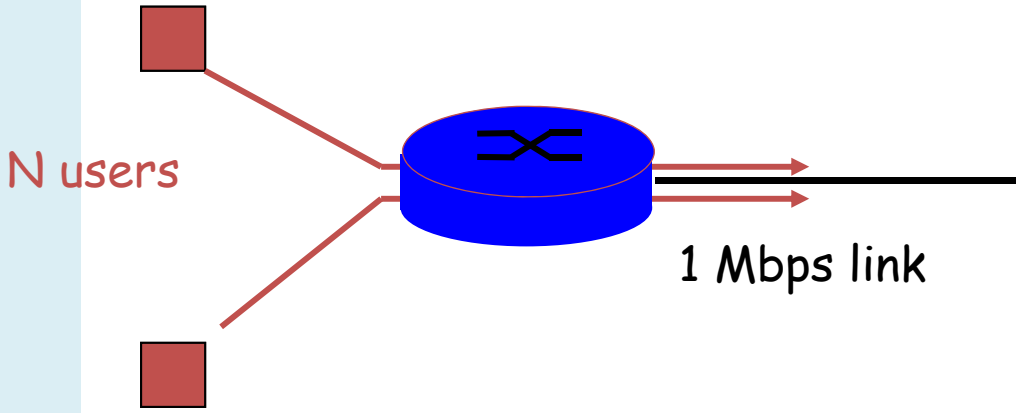


Fig. 2-35. Timing of events in (a) circuit switching, (b) message switching, (c) packet switching.

Packet switching versus classical circuit switching

Packet switching allows more users to use the network!

- 1 Mbit link
- each user/connection:
  - 100Kbps when “active”
  - active 10% of time (bursty behaviour)
- circuit-switching how many users/connections?:
  - 10
- packet switching:
  - with 35 users, probability > 10 active less than 0.0004 ($\Rightarrow$ almost all of the time, same the queuing behaviour is as in circuit switching)



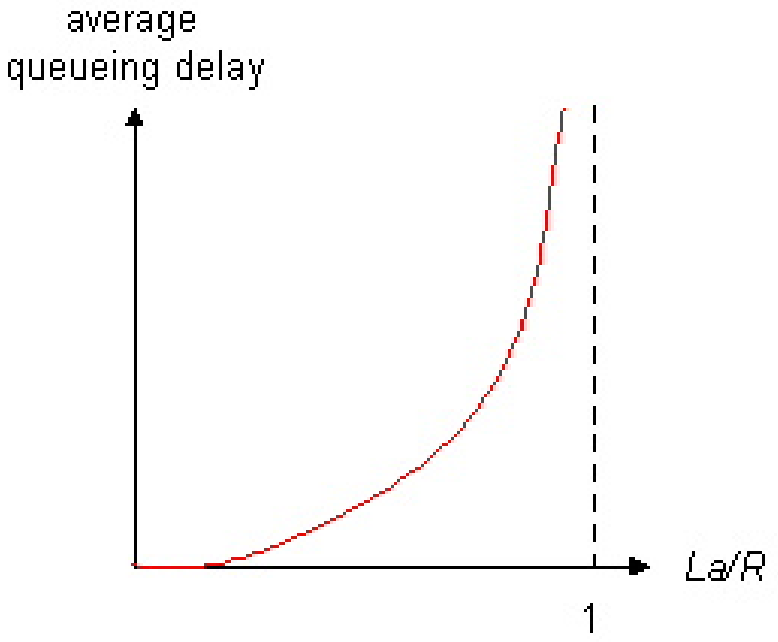
Hint: The probability of *k* out of *n* users active (p=0.1 in our example)

$$f(k;n,p) = \Pr(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Queueing delay (revisited) …

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

traffic intensity = La/R



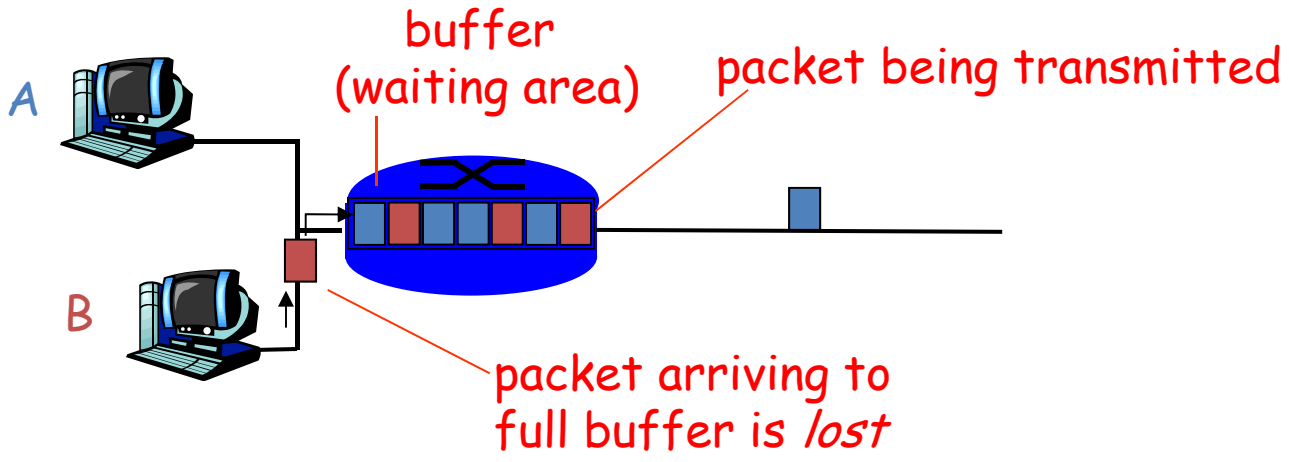
- La/R ~ 0: average queueing delay small
- La/R -> 1: delays become large
- La/R > 1: more "work" arriving than can be serviced, average delay infinite! Queues may grow unlimited, packets can be lost

Related with delays…

- packet loss
- throughput

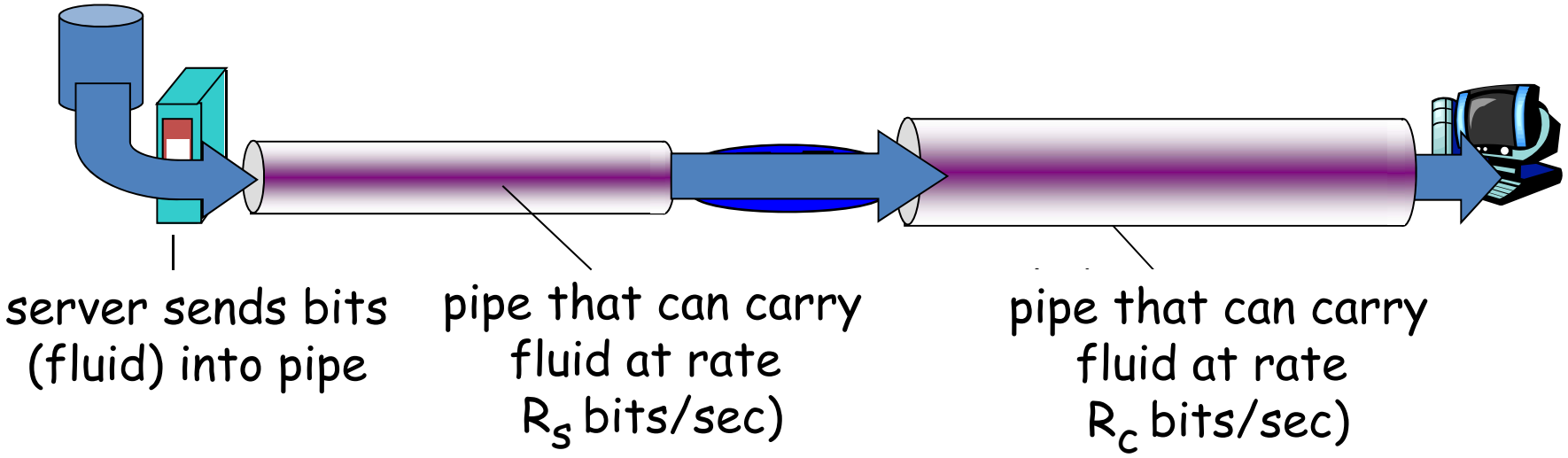
Packet loss

- queue (aka buffer) preceding link 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



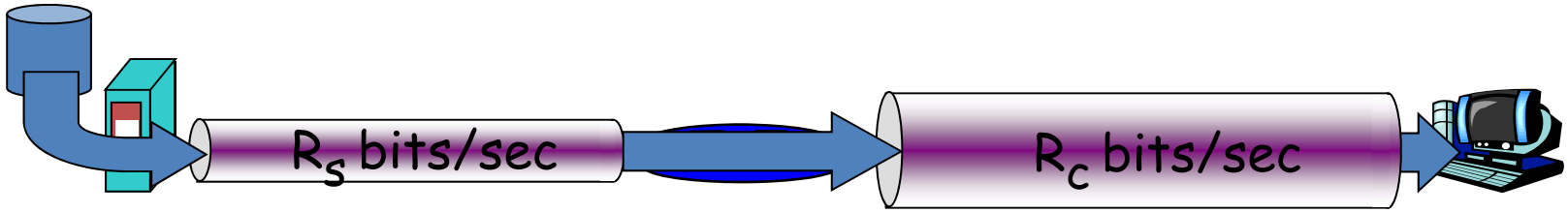
Throughput

- *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

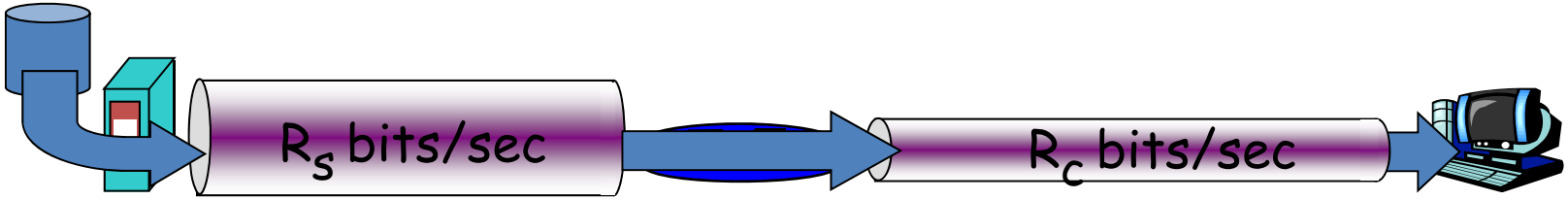


Throughput (more)

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



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

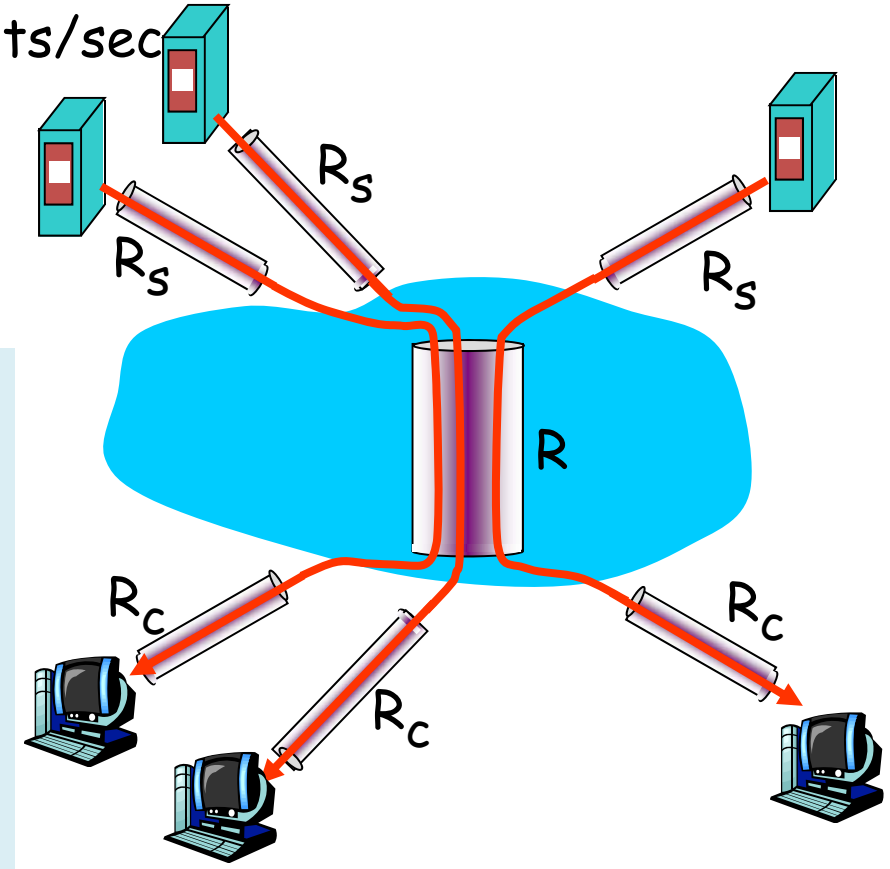


bottleneck link

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

Throughput: Internet scenario

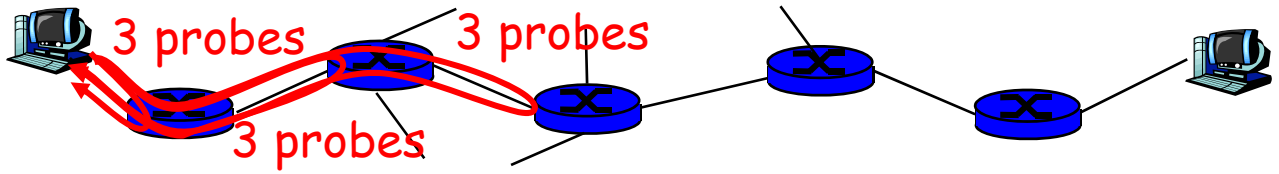
10 connections (fairly) share
backbone bottleneck link of R bits/sec



- per-connection end-end throughput: min(R_c,R_s,R/10 (if fair))
- in practice: R_c or R_s is often bottleneck

… "Real" Internet delays and routes (1)…

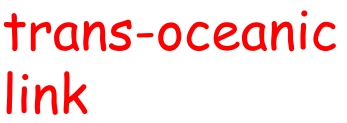
- What do "real" Internet delay & loss look like?
- Traceroute program: provides delay measurement from source to router along end-end Internet path towards destination. For all *i:*
  - sends three packets that will reach router *i* on path towards destination
  - router *i* will return packets to sender
  - sender times interval between transmission and reply.

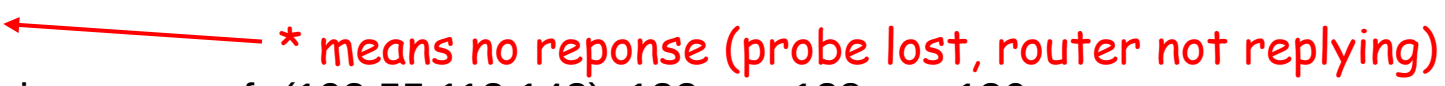


…"Real" Internet delays and routes (2)…

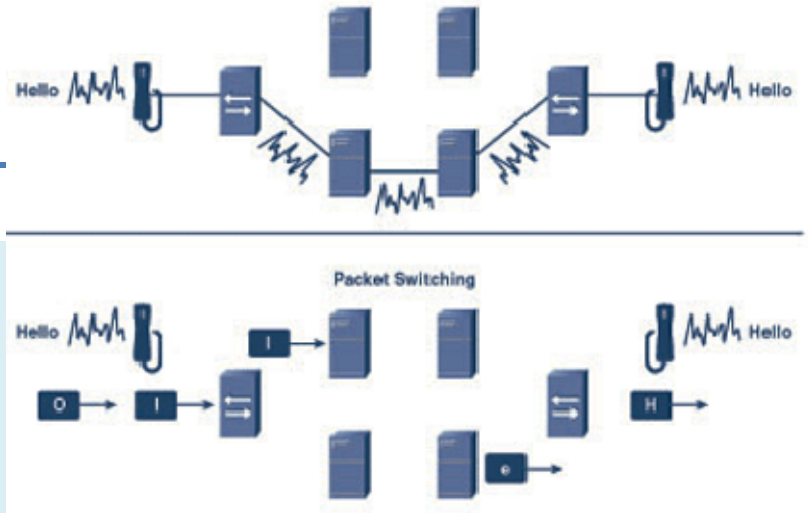
traceroute: gaia.cs.umass.edu to www.eurecom.fr


```
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
```





Packet switching properties



- PS: Good: Great for bursty data
  - resource sharing
  - no call setup
- PS: Not so good? Excessive congestion: packet delay and loss
  - protocols needed for reliable data transfer, congestion control

- **Q: How to provide circuit-like behavior?**
  - **bandwidth guarantees are needed for some apps**
  - **Some routing policies can help???**
    - **Cf virtual circuit**

Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

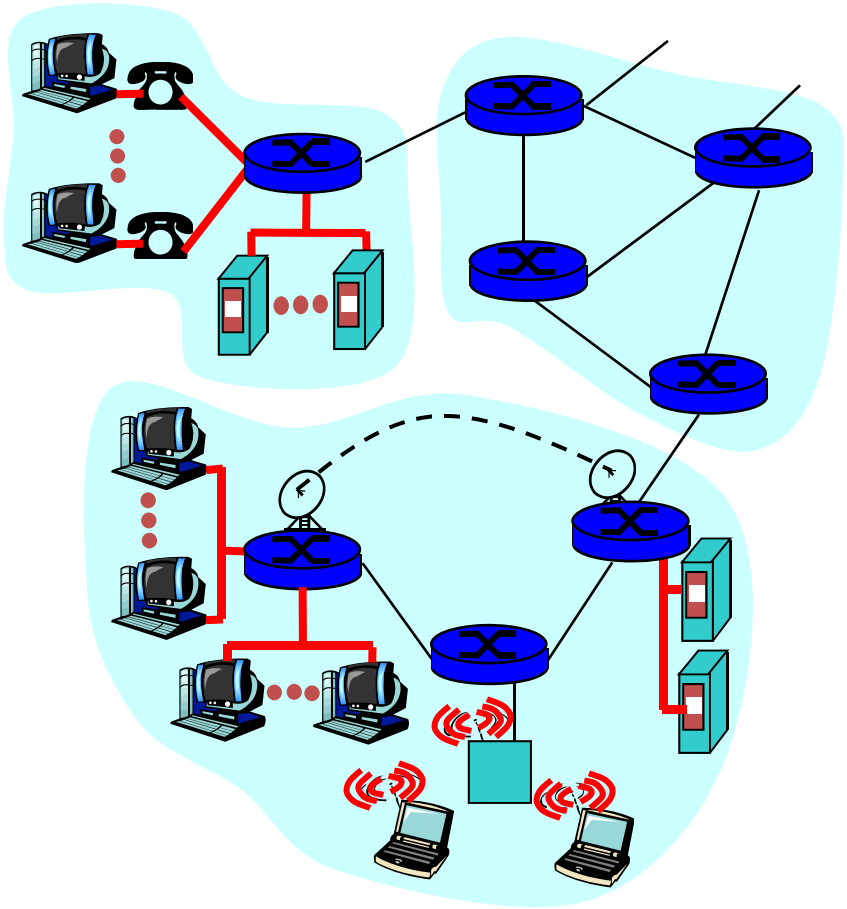
Access networks and physical media

Q: How to connect end systems to edge router?

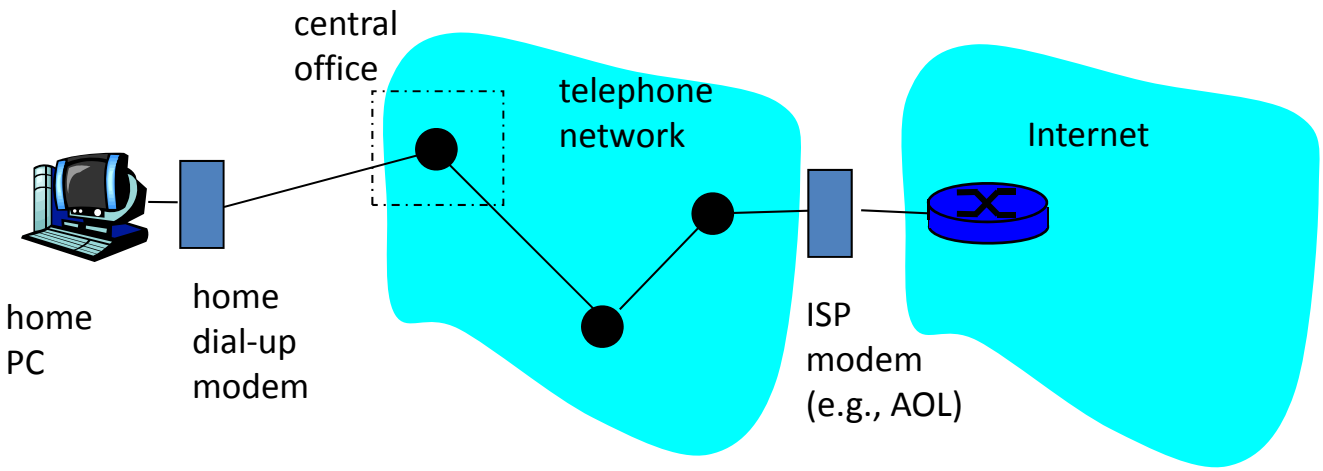
- residential access nets
- institutional access networks (school, company)
- mobile access networks

Considerations:

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

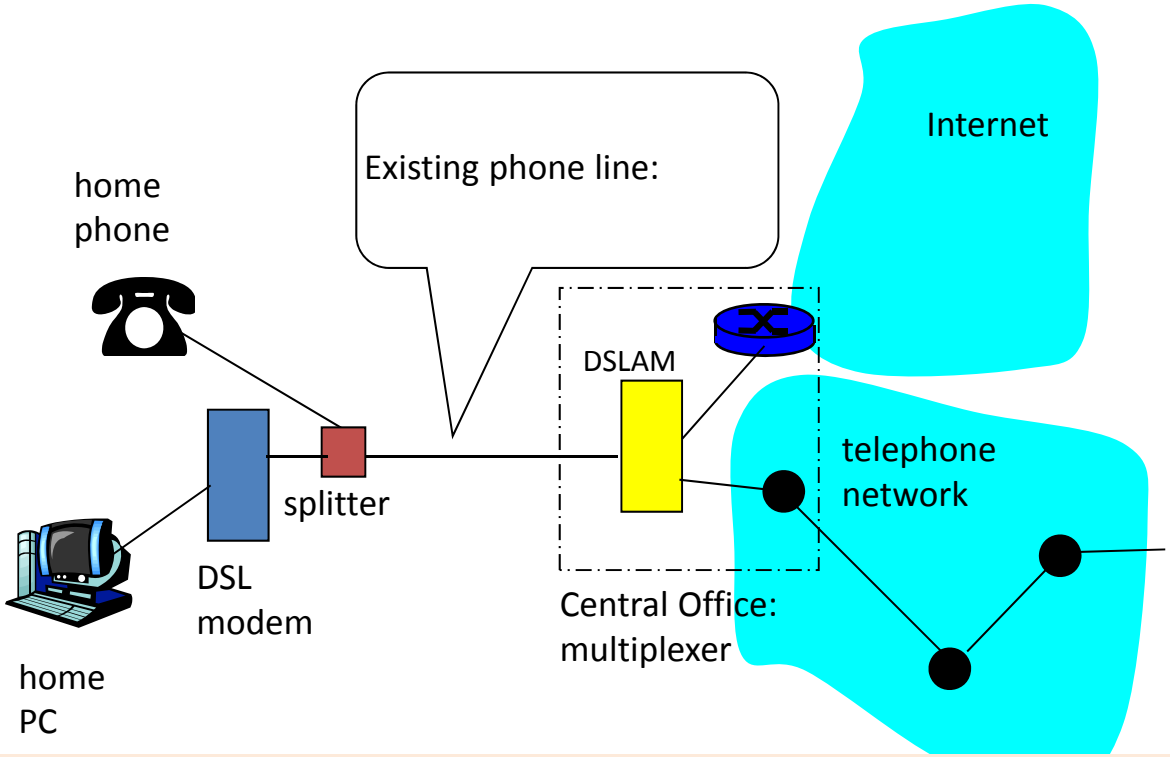


Dial-up Modem



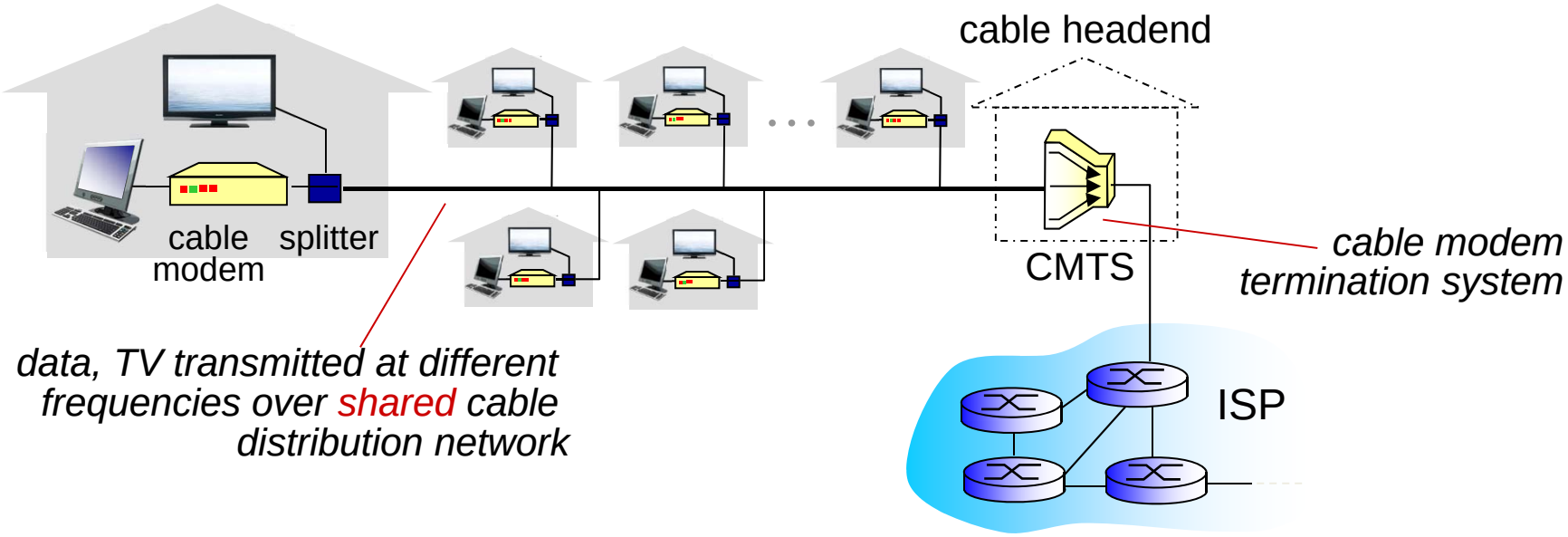
- Uses existing telephony infrastructure
  - Home is connected to central office
- up to 56Kbps direct access to router (often less)
- Can't surf and phone at same time: not "always on"

Digital Subscriber Line (DSL)



- Also uses existing telephone infrastructure
  - dedicated physical line to telephone central office
- Asymmertic: commonly up to 2.5 Mbps upstream; up to 24 Mbps downstream

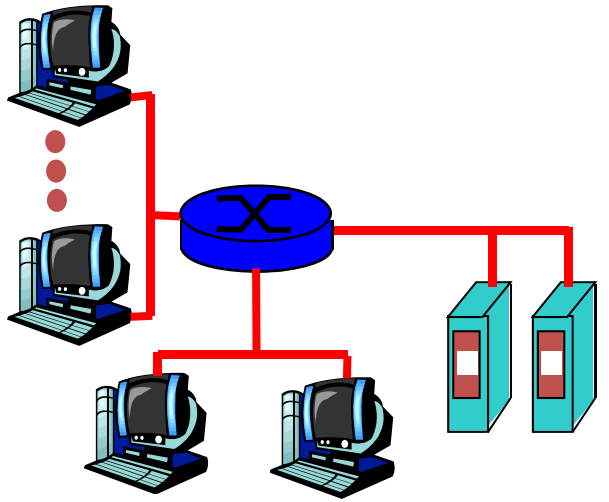
Access net: cable network



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

Institutional access: local area networks

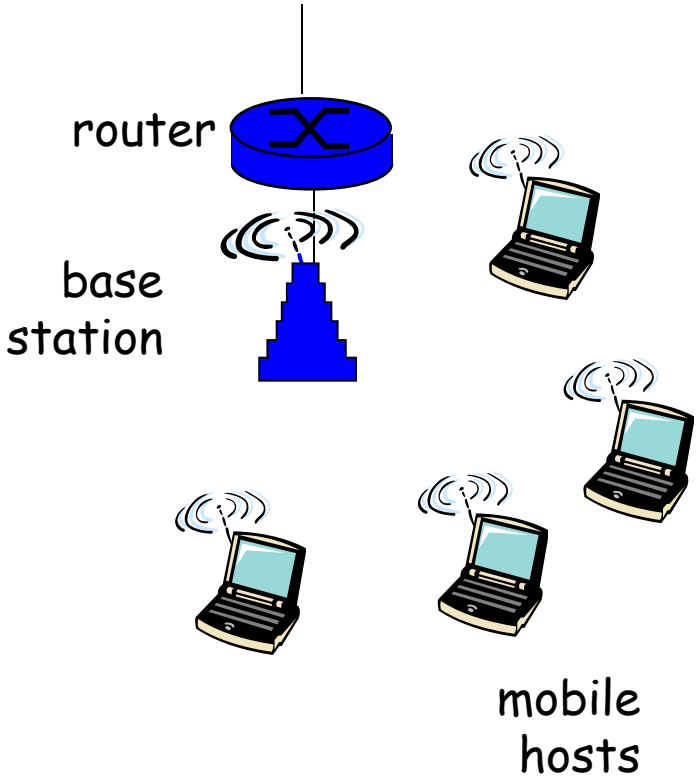
- local area network (LAN) connects end system to edge router
- E.g. Ethernet:
  - 10 Mbs, 100Mbps, Gigabit Ethernet
- deployment: institutions, home LANs



(a lot more on this later in the course)

Wireless access networks

- shared *wireless* access network connects end system to router
  - via base station aka “access point”, or “adhoc”
- wireless LANs:
  - 802.11b/g (WiFi): 11 or 54 Mbps
- wider-area wireless access
  - provided by telco operator
  - ~1Mbps over cellular system
  - WiMAX (10’s Mbps) over wide area

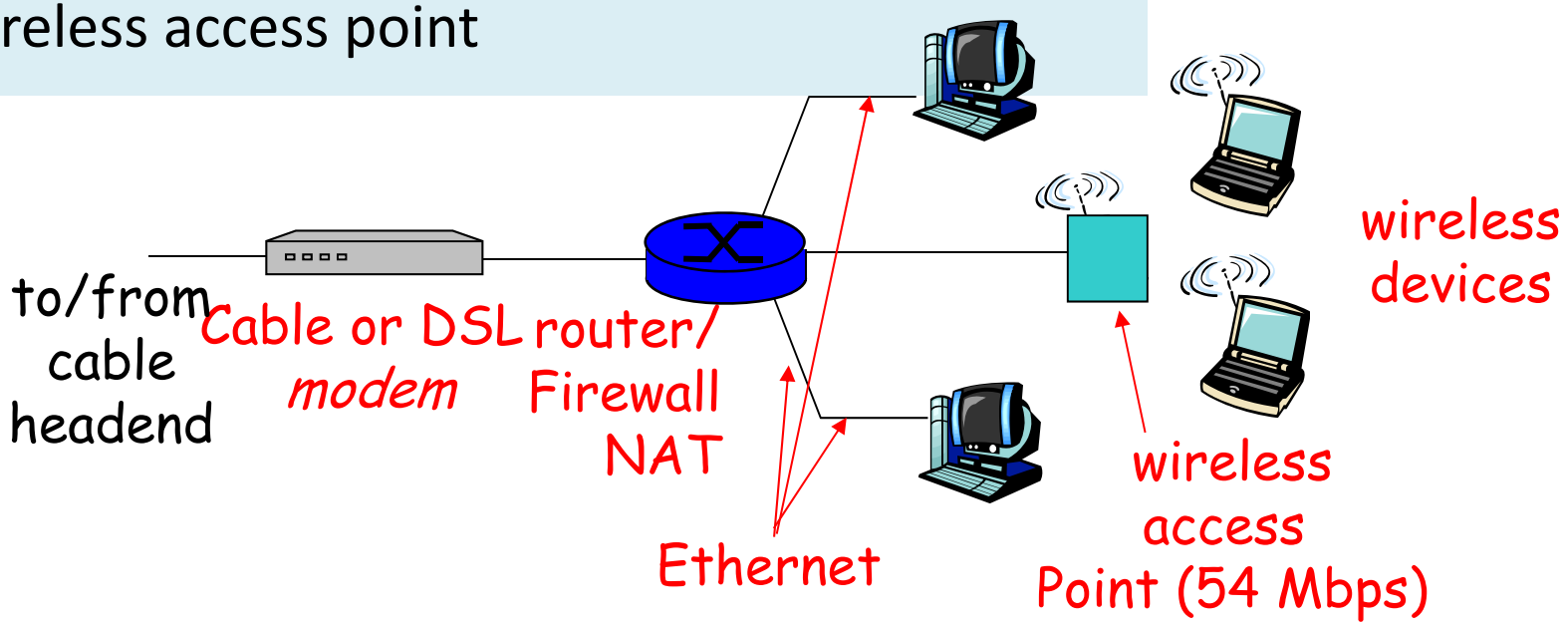


(a lot more on this later in the course)

Home networks

Typical home network components:

- DSL or cable modem or Fiber to the home
- router/firewall/NAT
- Ethernet
- wireless access point



Physical Media

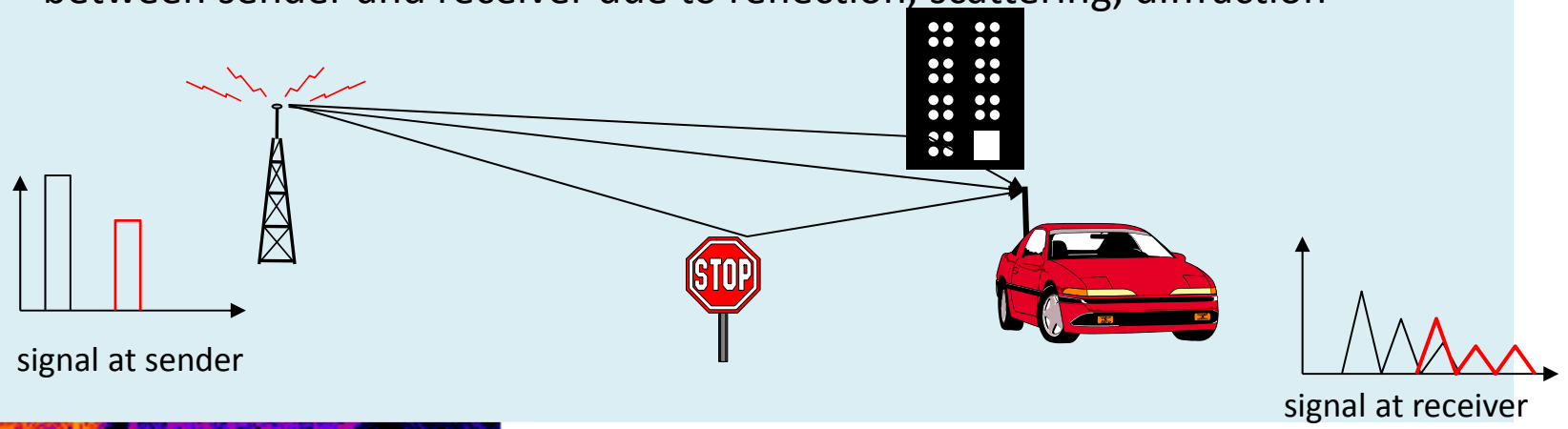
- physical link: transmitted data bit propagates across link
  - guided media:
    - signals propagate in solid media: copper, fiber
  - unguided media:
    - signals propagate freely e.g., radio

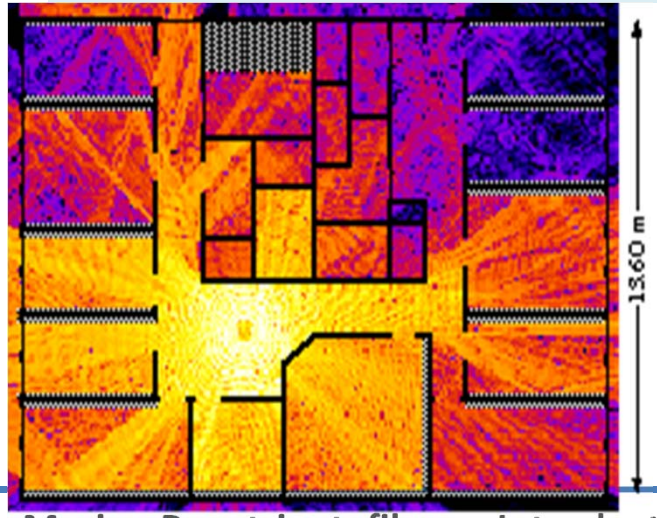
Physical media: wireless

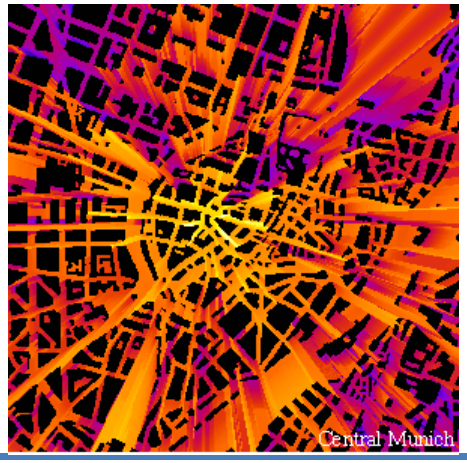
- signal carried in electromagnetic spectrum
- Omnidirectional: signal spreads, can be received by many antennas
- Directional: antennas communicate with focused el-magnetic beams and must be aligned (requires higher frequency ranges)
- propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

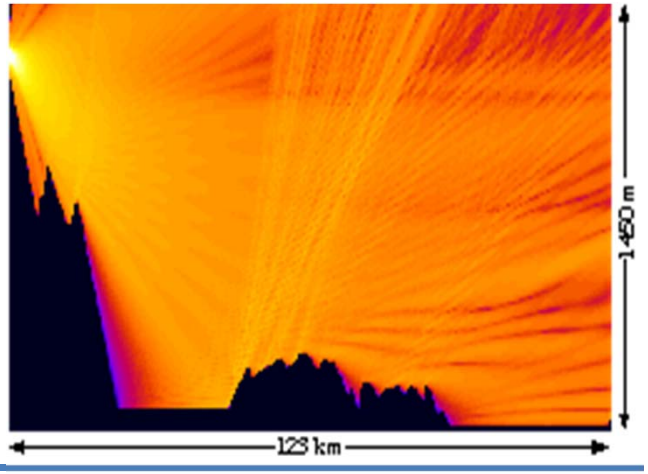
Wireless: properties
Attenuation, Multipath propagation

Signal can fade with distance, can get obstructed, can take many different paths between sender and receiver due to reflection, scattering, diffraction





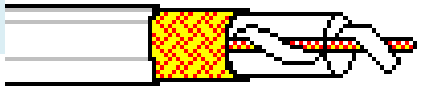




Physical Media: coax, fiber, twisted pair

Coaxial cable:

- wire (signal carrier) within a wire (shield)
  - baseband: single channel on cable (common use in 10Mbs Ethernet)
  - broadband: multiple channels multiplexed on cable(commonly used for cable TV)



Fiber optic cable:

- glass fiber carrying light pulses
- low attenuation
- high-speed operation:
  - 100Mbps Ethernet
  - high-speed point-to-point transmission (e.g., 5 Gps)
- low error rate

Twisted Pair (TP)

- two insulated copper wires

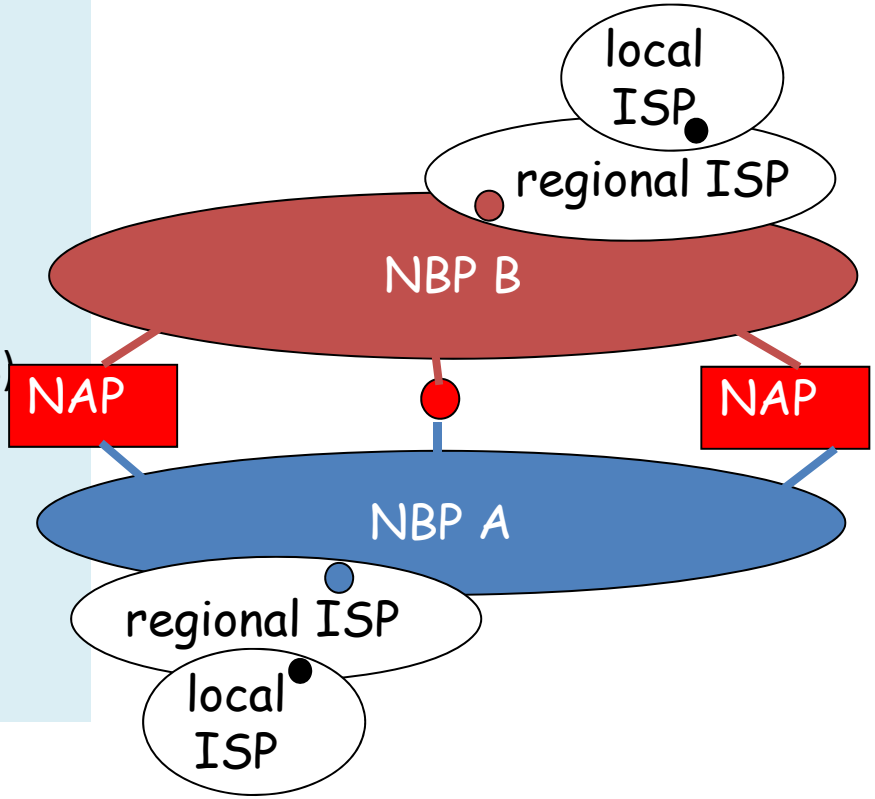
  - Category 3: traditional phone wires, 10 Mbps Ethernet
  - Category 5 TP: more twists, higher insulation: high-speed Ethernet

Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

Internet structure: network of networks

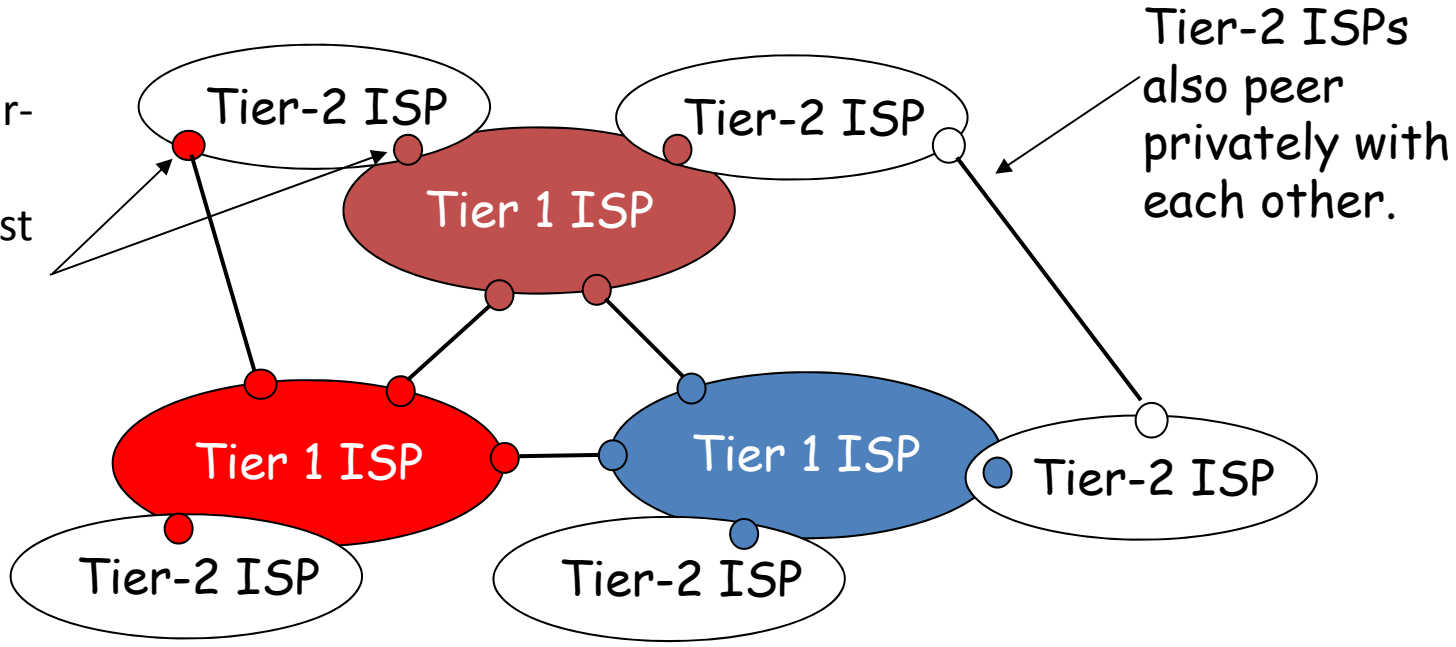
- roughly hierarchical
- national/international backbone providers (NBPs)- tier 1 providers
  - e.g. BBN/GTE, Sprint, AT&T, IBM, UUNet/Verizon, TeliaSonera
  - interconnect (peer) with each other privately, or at public Network Access Point (NAPs: routers or NWs of routers)
- regional ISPs, tier 2 providers
  - connect into NBPs; e.g. Tele2
- local ISP, company
  - connect into regional ISPs



Internet structure: network of networks

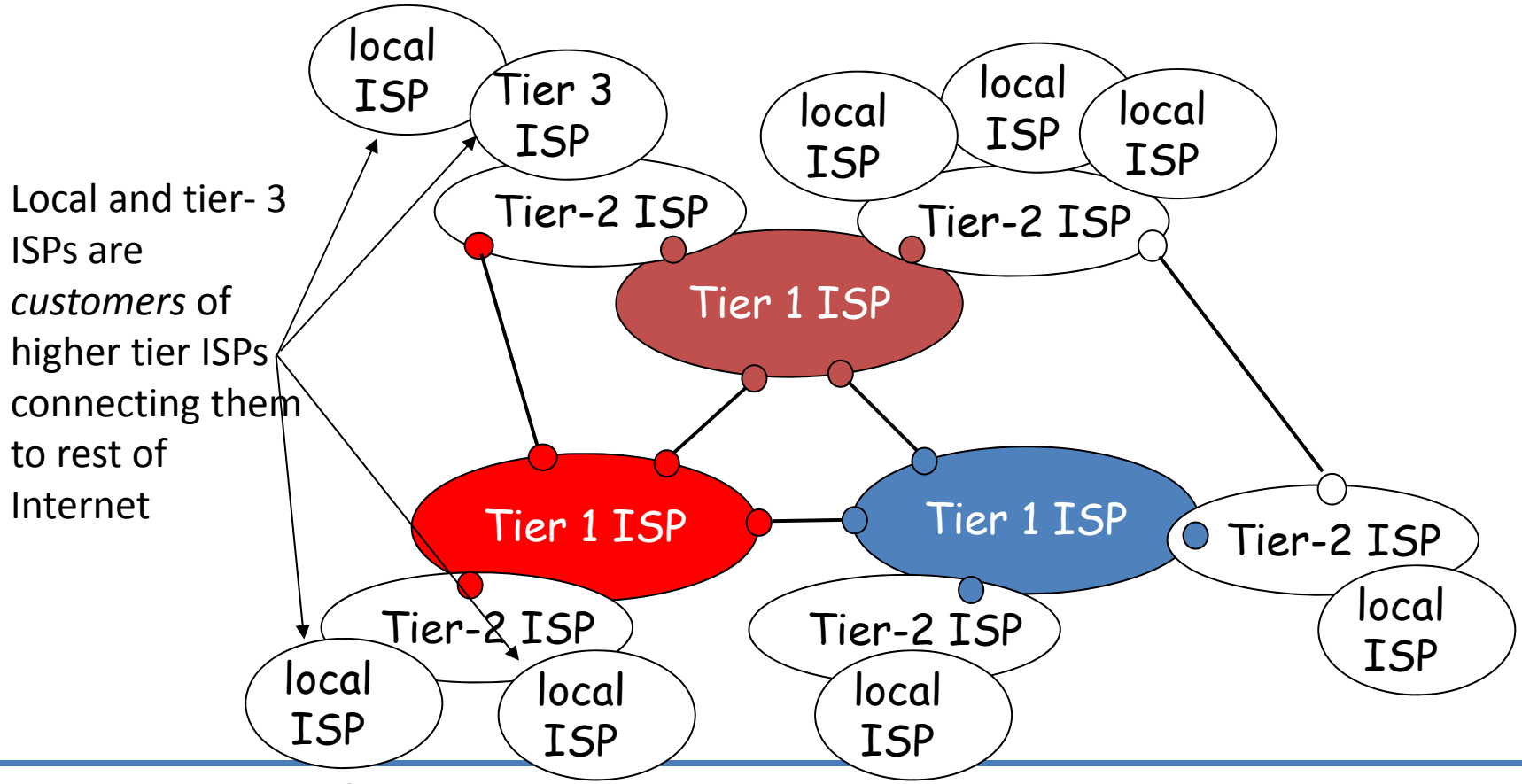
- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

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



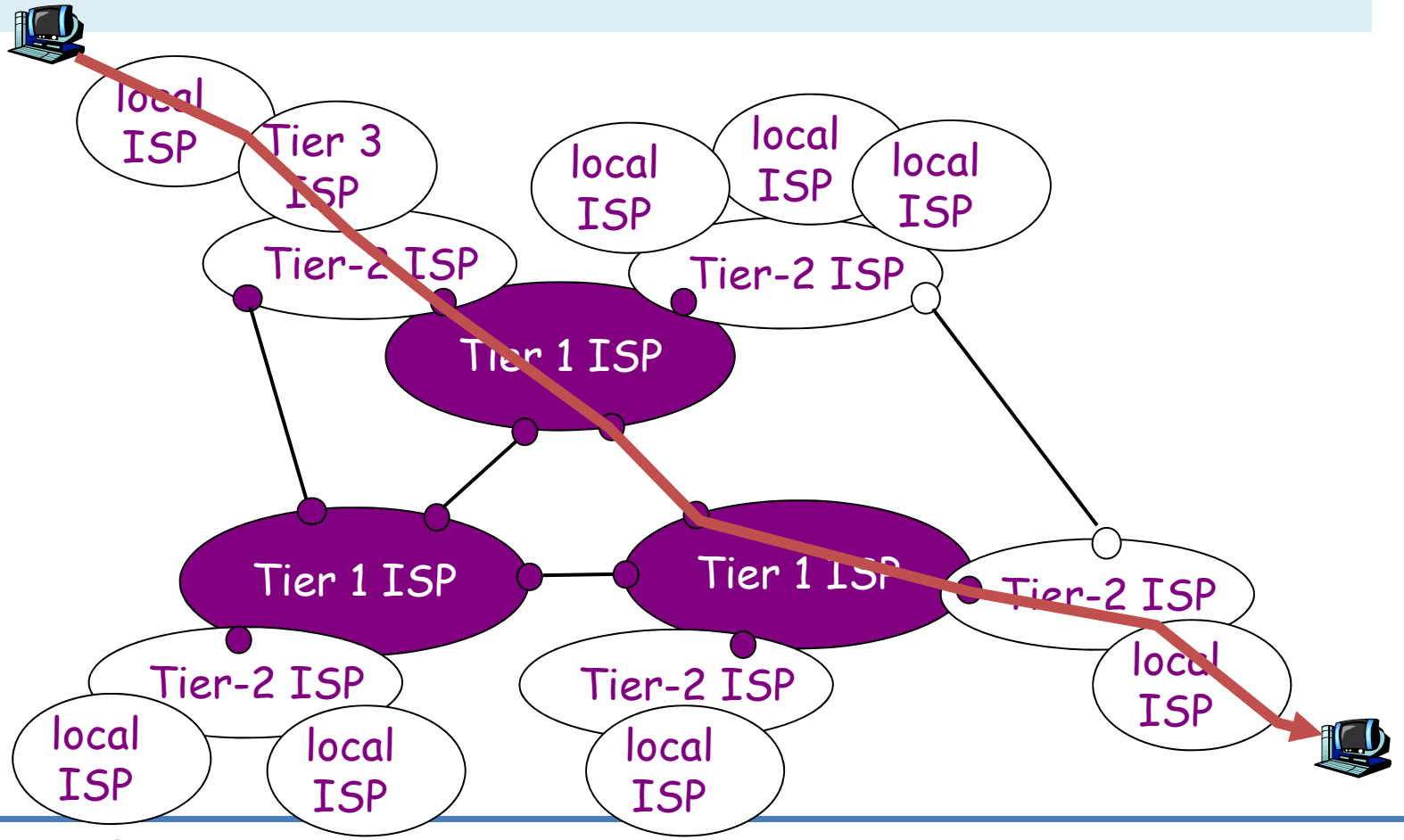
Internet structure: network of networks

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



Internet structure: network of networks

- a packet passes through many networks



Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

Network Security

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

Bad guys can put malware into hosts via Internet

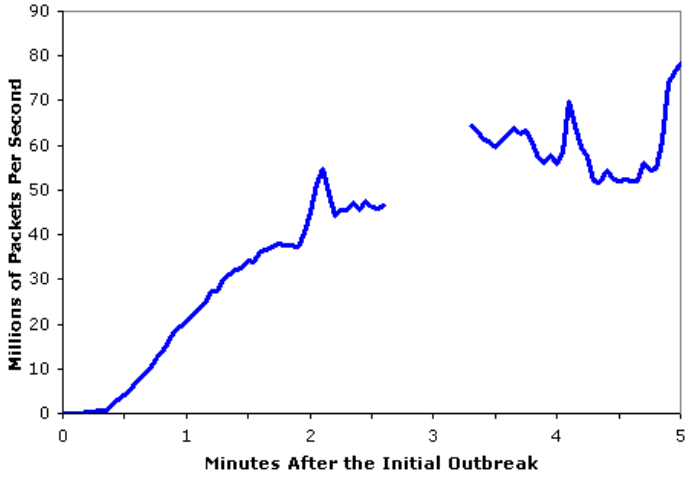
- Malware can get in host from a virus, worm, or trojan horse.
- Spyware malware can record keystrokes, web sites visited, upload info to collection site.
- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.
- Malware is often self-replicating: from an infected host, seeks entry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

Example types of malware

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

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

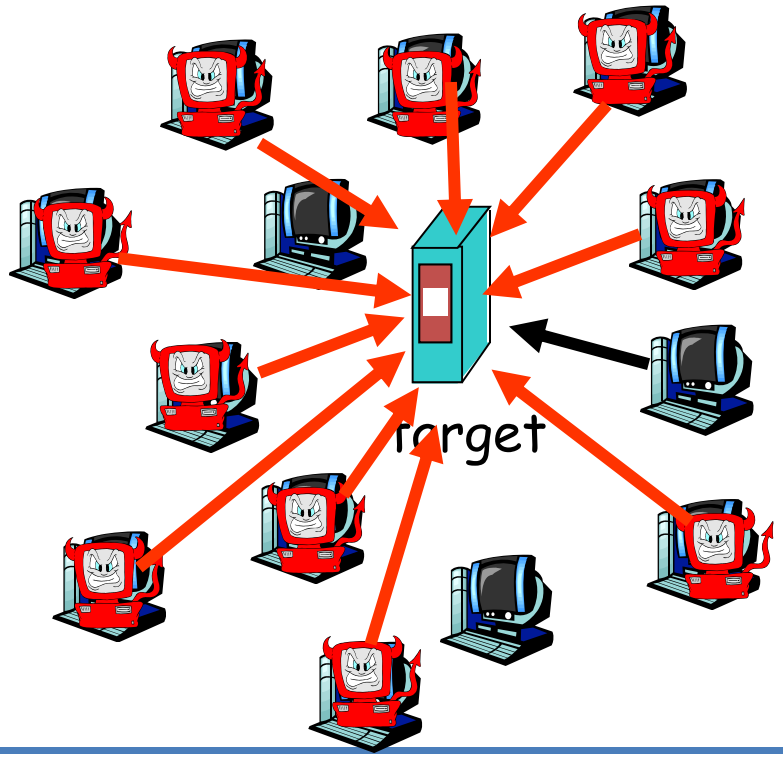
Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)



Bad guys can attack servers and network infrastructure

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

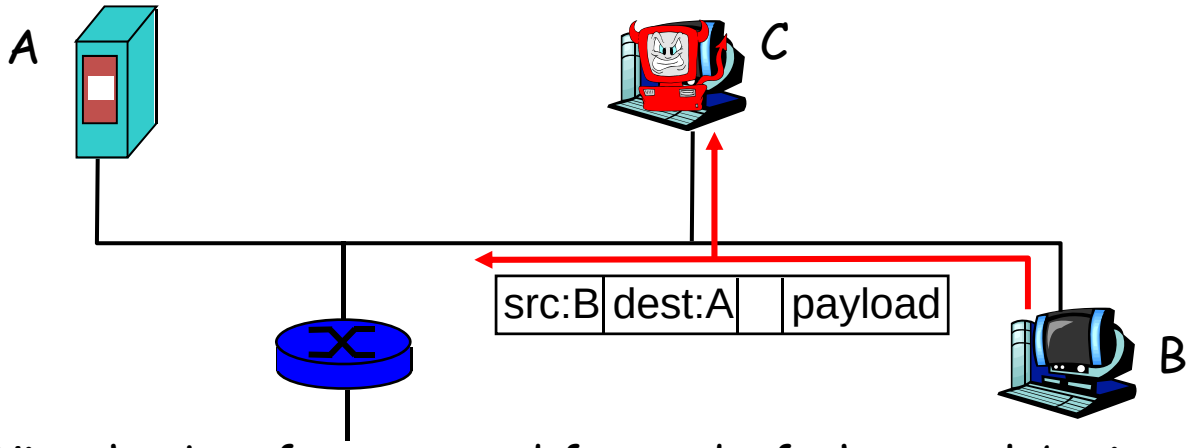
1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts



The bad guys can sniff packets

Packet sniffing:

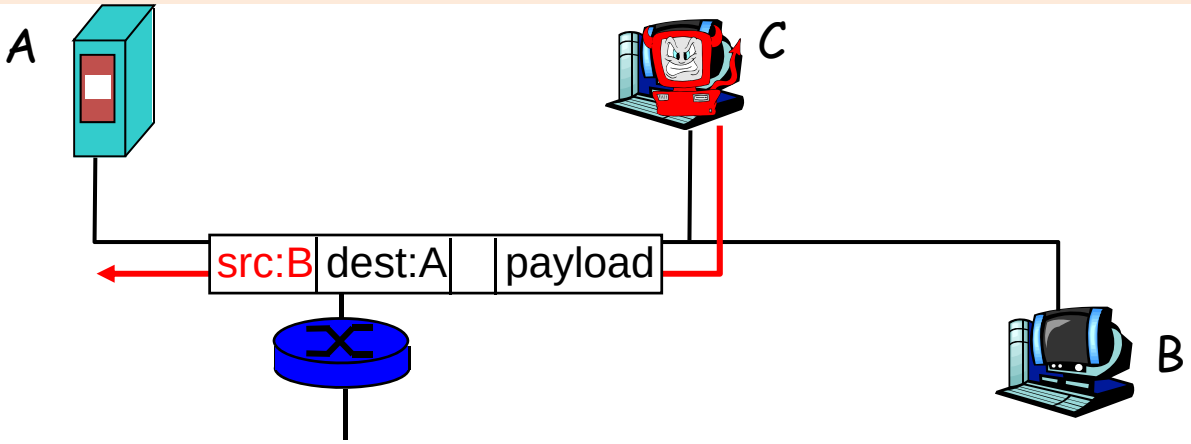
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords) passing by



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

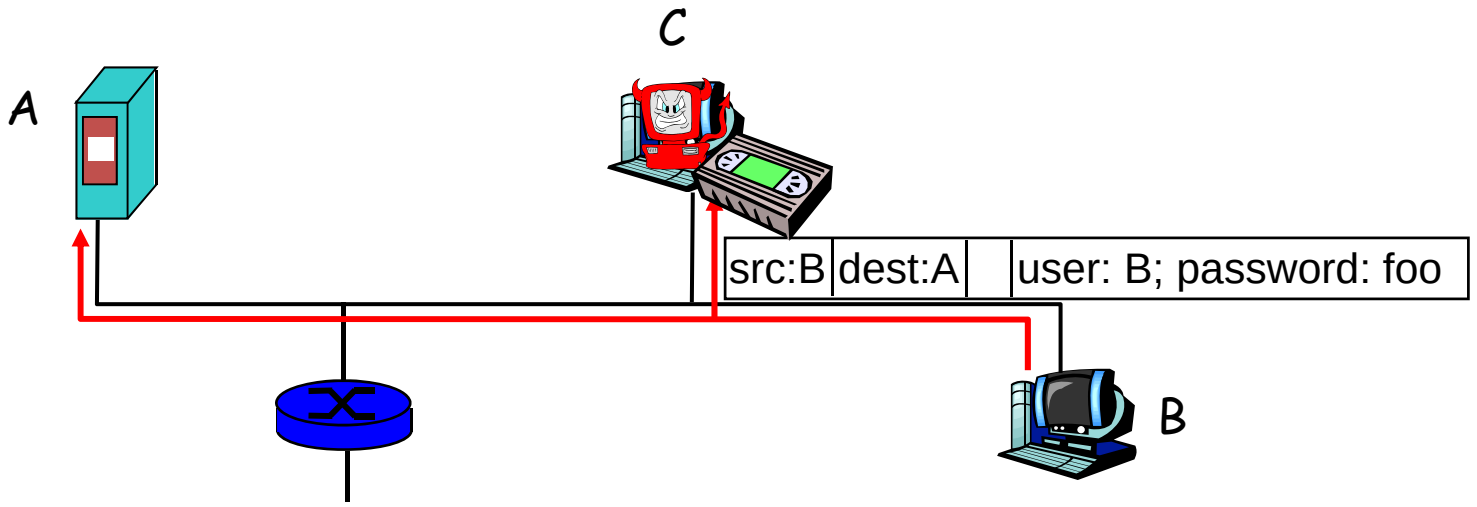
The bad guys can use false source addresses

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



The bad guys can record and playback

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



Roadmap

- what's the Internet
- protocol layers
  - Communication through layers
- edge & core of any big network:
  - types of service, ways of information transfer, routing
- Internet layers & Logical vs physical communication
- Performance:
  - delays, loss
- Network/Internet structure complemented:
  - access net, physical media
  - backbones, NAPs, ISPs
- Security prelude

Chapter 1: Summary

Covered a "ton" of material!

- what's the Internet
- what's a protocol?
- protocol layers, service models
- network edge (types of service)
- network core (ways of transfer, routing)

- performance, delays, loss
- access net, physical media
- backbones, NAPs, ISPs
- Security concerns

- (history: read more corresponding section, interesting & fun ☺)

You now hopefully have:

- context, overview, "feel" of networking
- A point of reference for context in the focused discussions to come

Reading instructions

1. Kurose Ross book

Careful	**Quick**
4/e,5/e,6/e: 1.3, 1.4, 1.5	4/e,5/e,6/e: the rest

Extra Reading (optional)
Computer and Network Organization: An Introduction,
by Maarten van Steen and Henk Sips, Prentice Hall
(very good introductory book for non-CSE students

Review questions

Review questions from Kurose-Ross book, chapter 1 (for basic study)

- R11, R12, R13, R16, 17, R18, R19, R20, R21, R22, R23, R24, R25, R28.

Extra questions, for further study: delay analysis in packet switched networks:

http://www.comm.utoronto.ca/~jorg/teaching/ece466/material/466-SimpleAnalysis.pdf