Course on Computer Communication and Networks

Lecture 2
Chapter 1: Introduction:
Part B: Network structure, performance, security prelude

CTH EDA344/GU DIT 420

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

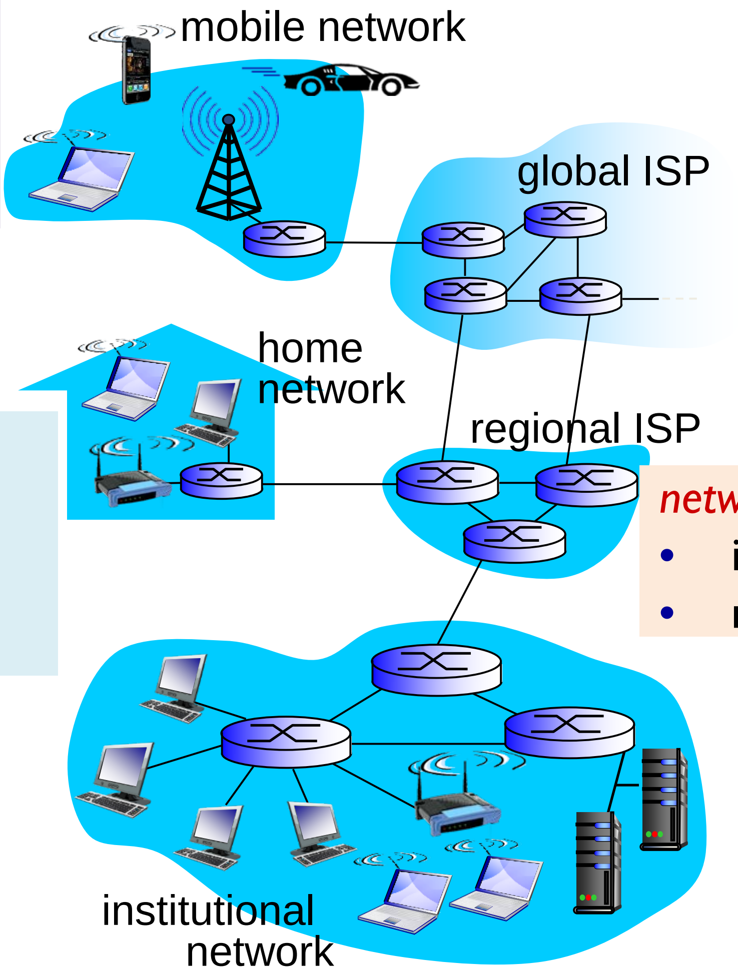
A closer look at network structure:

network edge: hosts:

- run application programs e.g. Web, email, …
- … based on network services available

access networks:

- *connect end-hosts to the Internet (edge routers)*
- *through physical media:* wired, wireless links



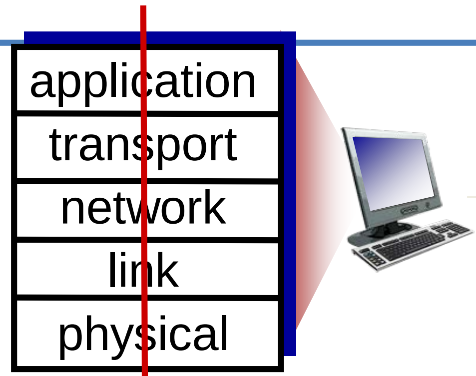
network core:

- interconnected routers
- network of networks

A closer look at network structure:

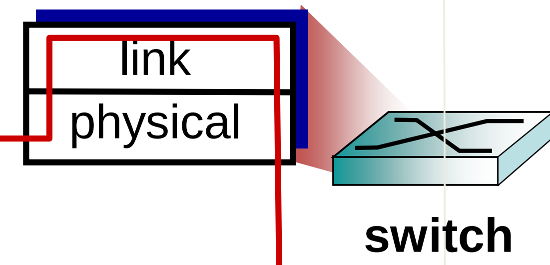
network edge: hosts:

- run application programs e.g. Web, email, …
- … based on network services available



access networks:

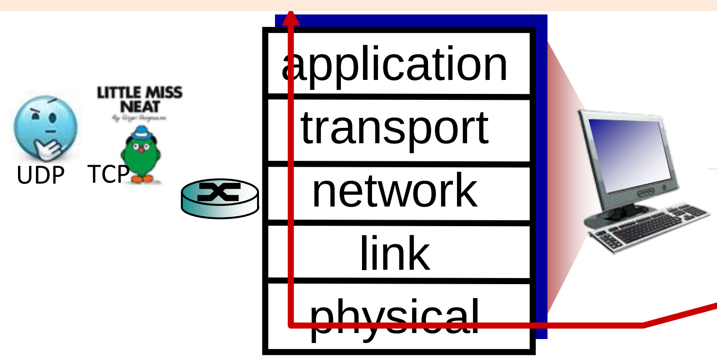
- *connect end-hosts to the Internet (edge routers)*
- *through physical media:* wired, wireless links

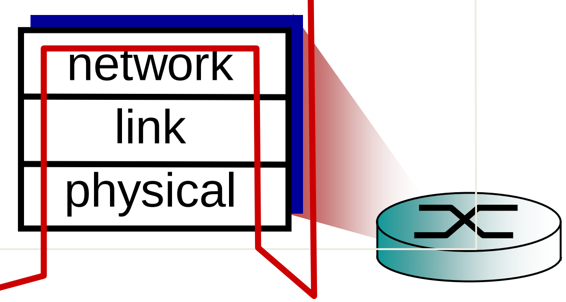


Types of communication service available by the transport layer @ Internet:

- **connection-oriented**: reliable, in-order data delivery (TCP)
- **connectionless**: "best effort", arbitrary order data-delivery (UDP)

Q: How & based on what "core" functionality?
(…main Q for the course….)

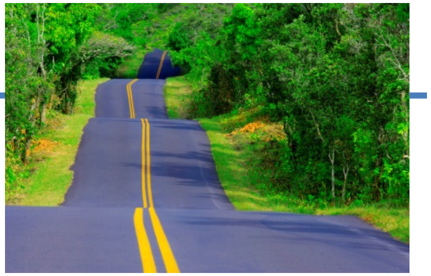




network core:

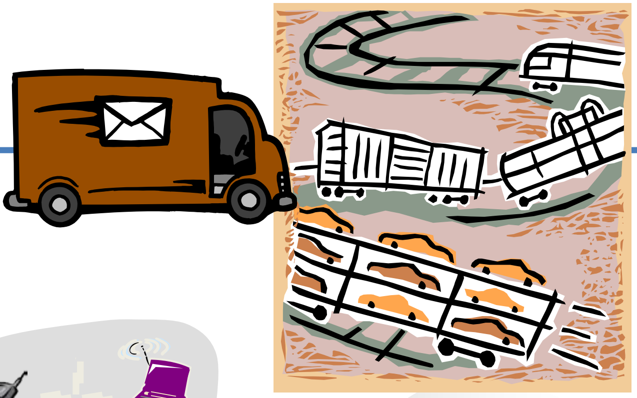
- interconnected routers
- network of networks

Roadmap

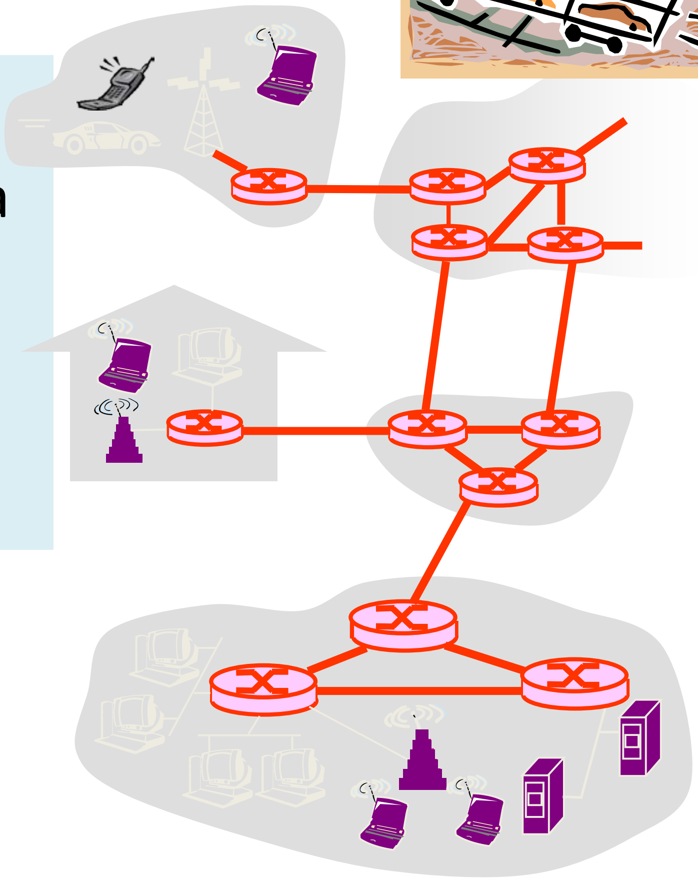


1. Zooming into core
   – Ways of data transfer
   – Routing
   – Performance: delays (& loss)
   – …. throughput
2. Network/Internet structure complemented:
   – access net, physical media
   – backbones, NAPs, ISPs
3. Security prelude

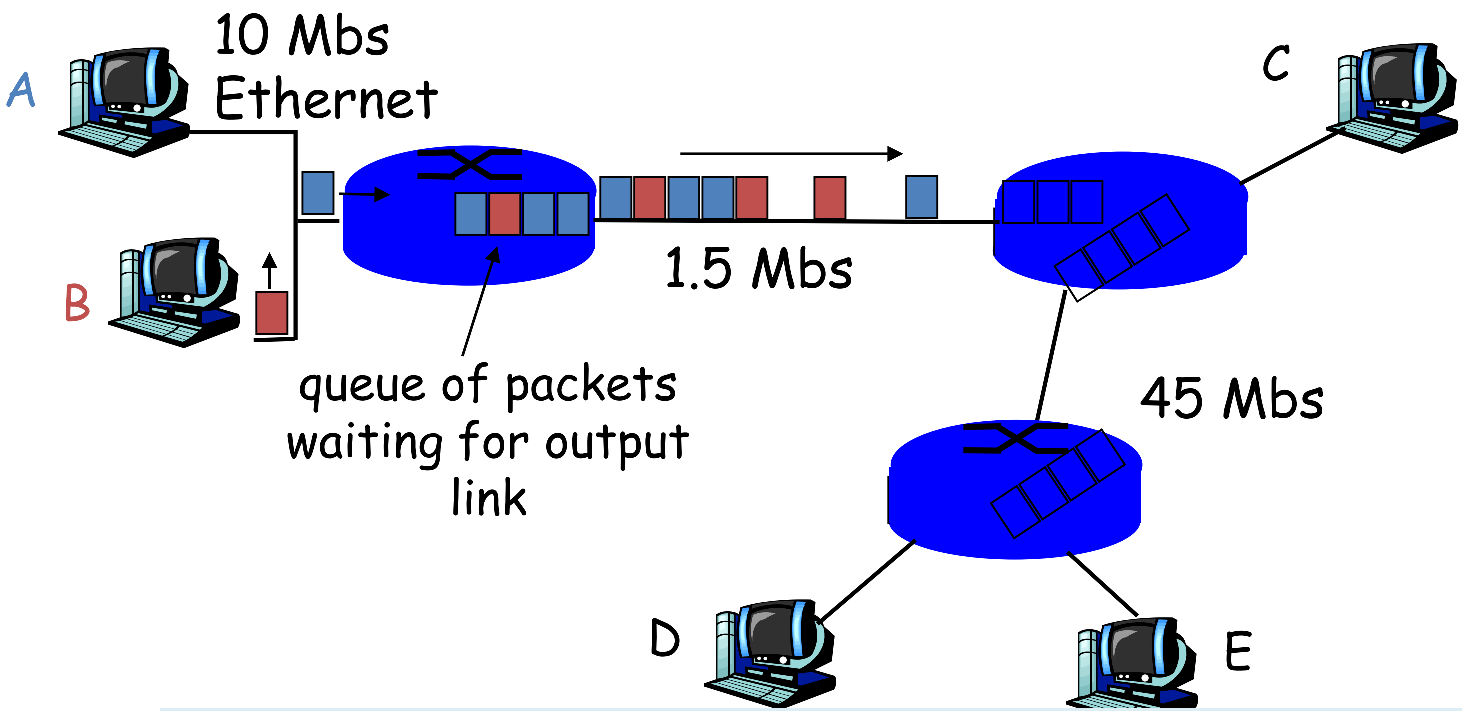
The Network Core



- 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



Application messages divided into *packets*

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

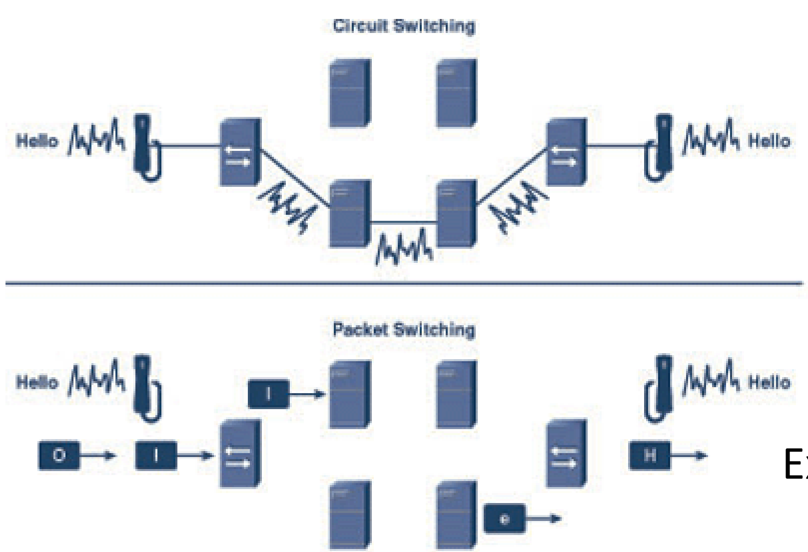
store and forward:

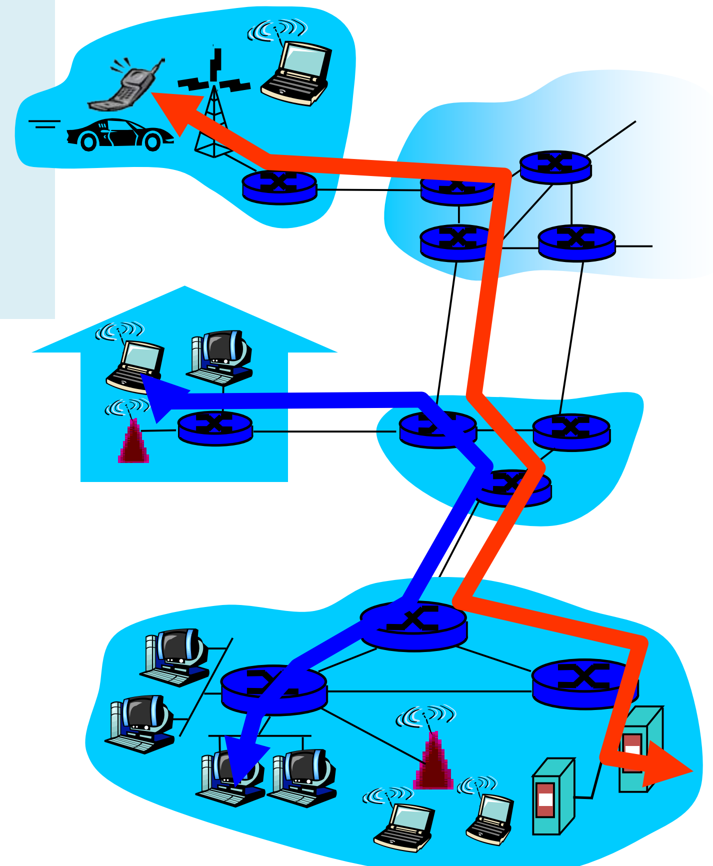
- packets move one hop at a time
  - transmit over link; wait turn at next link

Alternative Core: Circuit Switching
(analogue telephony)

End-end resources dedicated for "call"

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





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

Packet switching versus circuit switching

Packet switching allows more users to use the network!

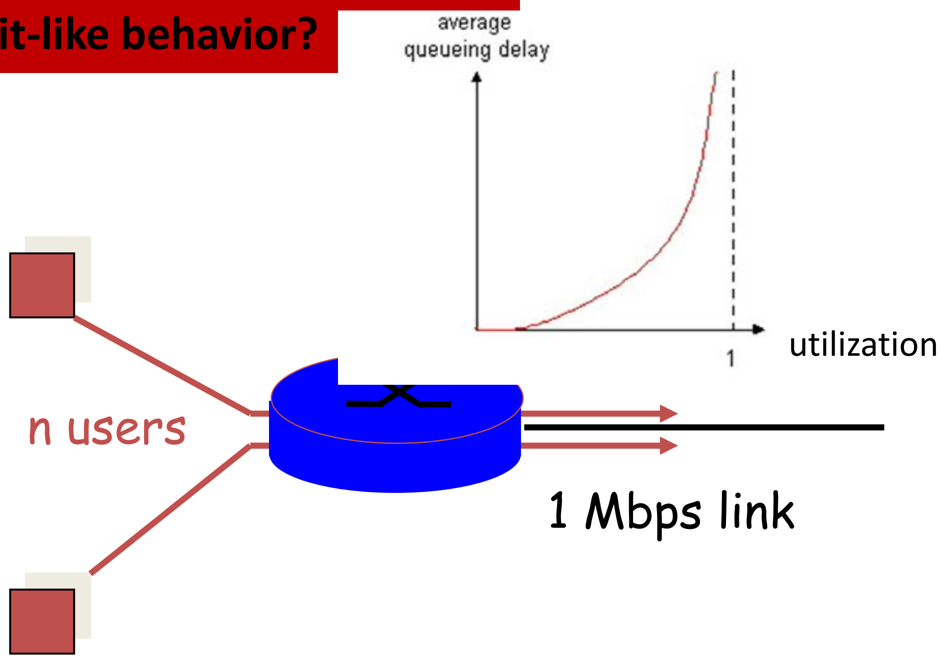
- 1 Mbit link
- each user/connection:
  - 100Kbps when “active”
  - active 10% of time (bursty behaviour)
- **circuit-switching** how many users/connections?:
  - 10
- **packet switching**

  with n= 35 users:

  P(k > 10 active) < 0.0004

  ⇒ almost all of the time, same queuing behaviour as in circuit switching)

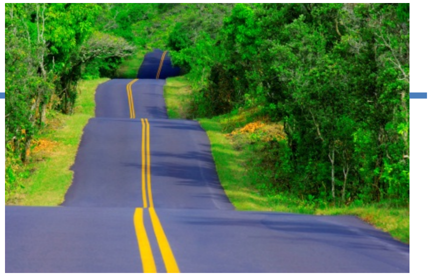
Q: what happens with > 35 users?
Still circuit-like behavior?



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

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

Roadmap



1. Zooming into core
   – Ways of data transfer
   – Routing
   – Performance: delays, (& loss) …
   – …. throughput
2. Network/Internet structure complemented:
   – access net, physical media
   – backbones, NAPs, ISPs
3. Security prelude

(Can we combine the benefits of CS & PS?)

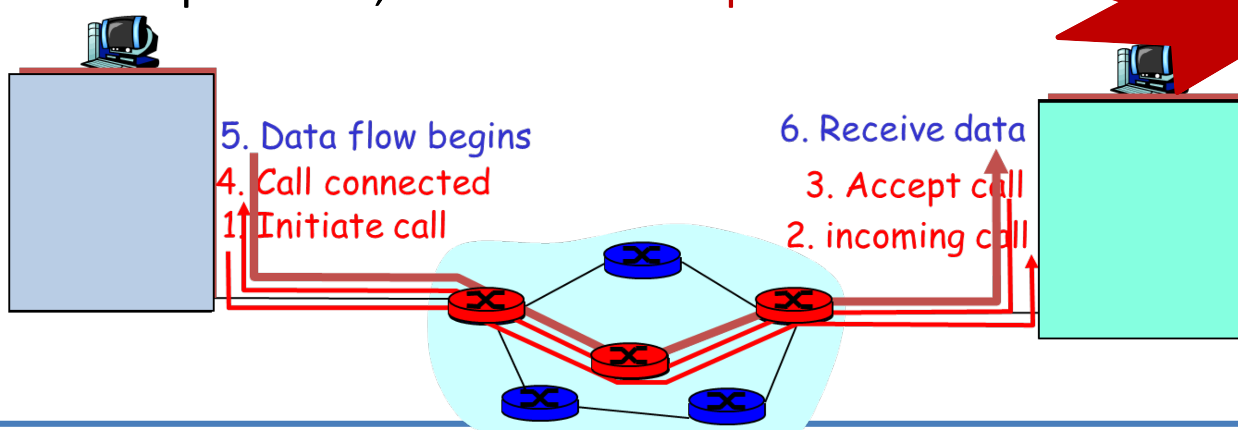
Routing and network-core main design issue

What is routing's role? find routes from source to destination

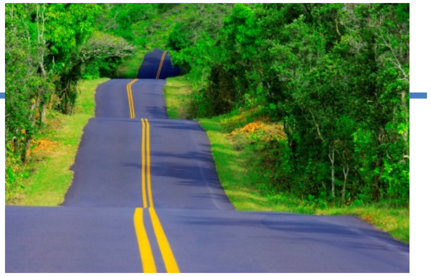
1. path selection algorithms
2. Important design issue/type of service offered at network layer:
   - **datagram network**:
     - *destination address* determines next hop
     - routes may change during session
   - **virtual circuit network:**
     - path determined at *call setup*, remains fixed thru session
     - *"bridging" packet-switching with circuit switching*
     - routers can prioritize, must maintain per-session state

Simple to implement & maintain (Internet approach)

Expensive, but better to build reliability



Roadmap



1. Zooming into core
   – Ways of data transfer
   – Routing
   – Performance: delays, (& loss) …
   – …. throughput
2. Network/Internet structure complemented:
   – access net, physical media
   – backbones, NAPs, ISPs
3. Security prelude

Delay in packet-switched networks

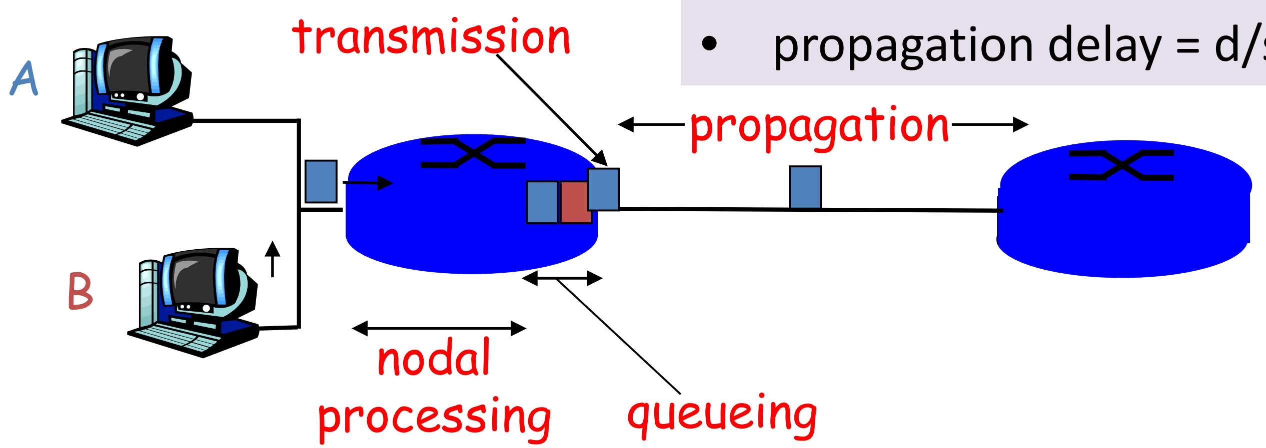
- 1. nodal processing:
  - check bit errors
  - determine output link
- 2. queuing
  - time waiting at output link for transmission
  - depends on congestion level of router

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



Visualize delays: Circuit, packet switching

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

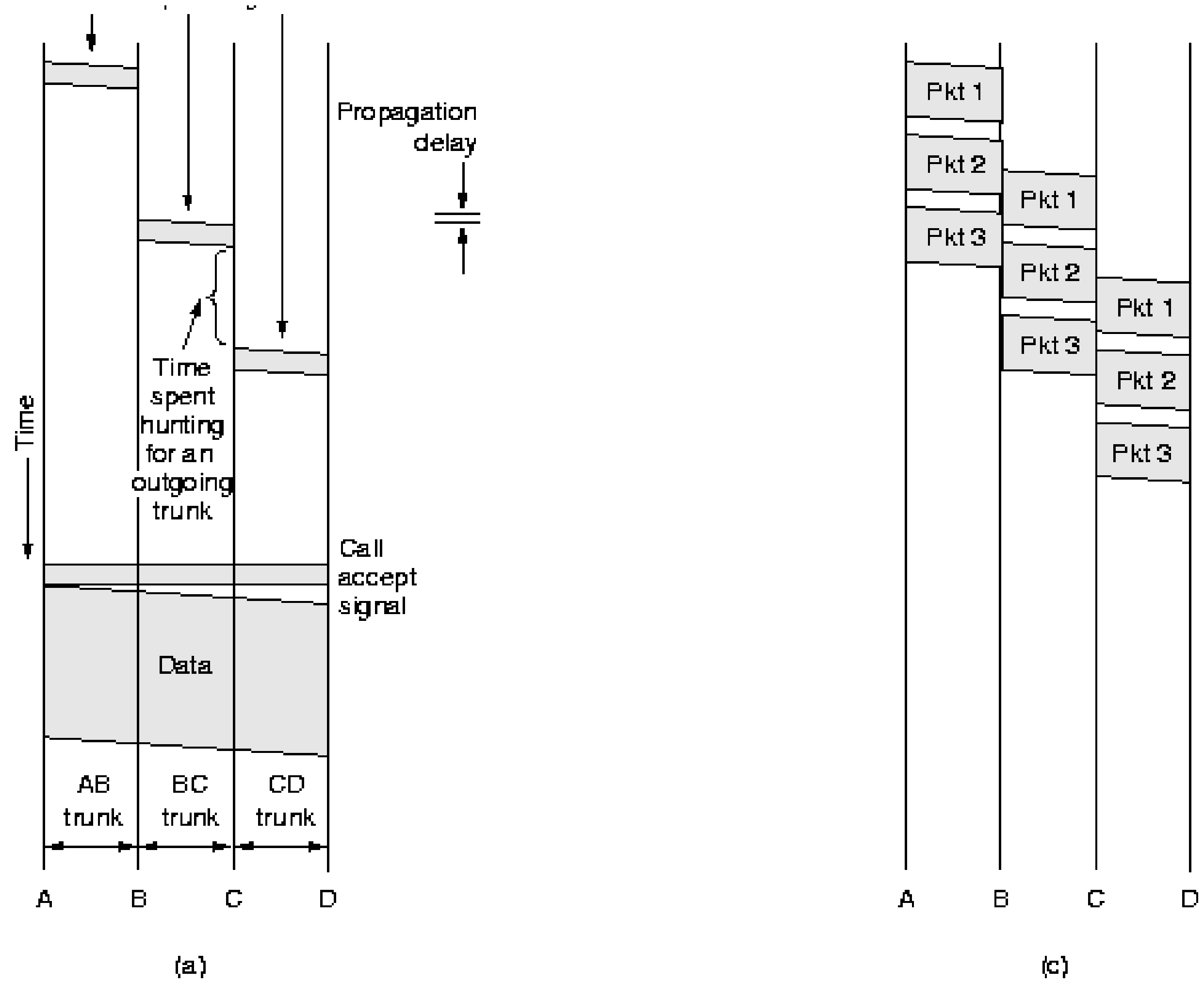
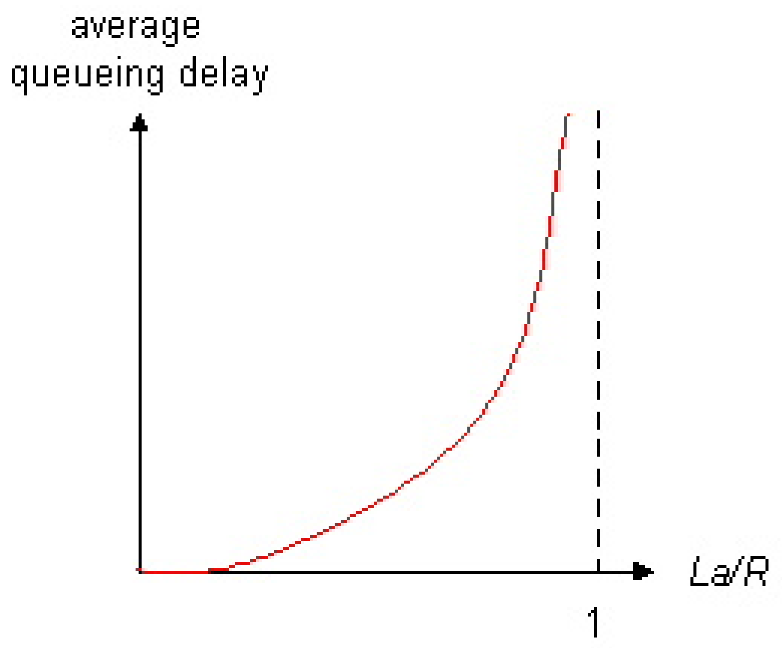


Fig. 2-35. Timing of events in (a) circuit switching, (c) packet switching.

Queueing delay (revisited) …

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

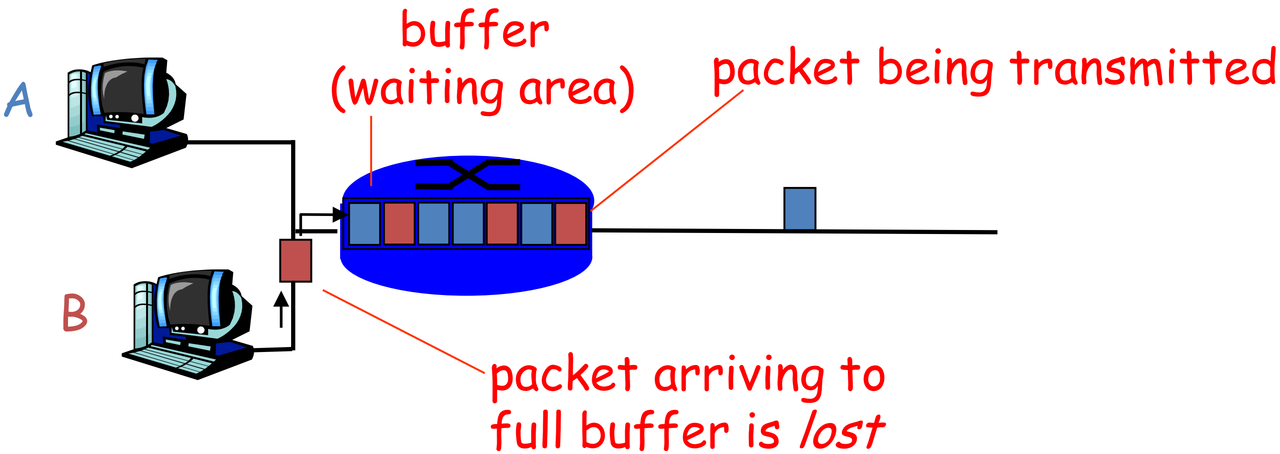
traffic intensity = La/R



- 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

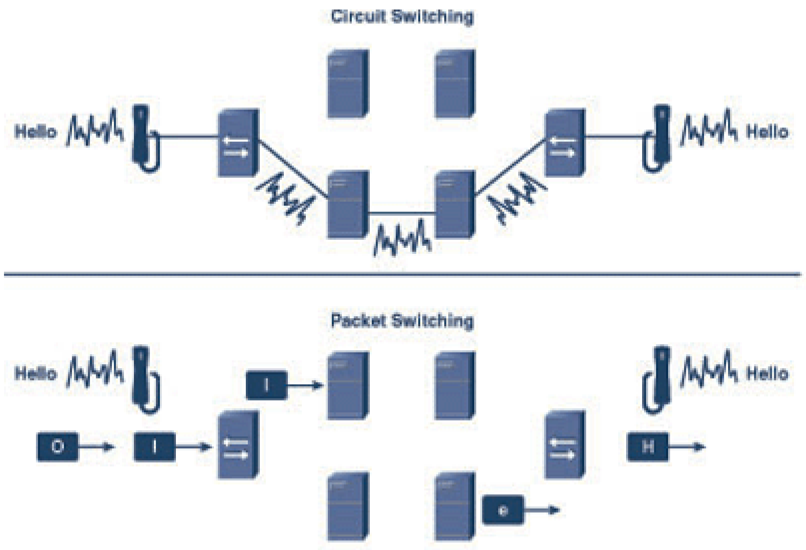
Delays and packet loss

- Link queue (aka buffer) has finite capacity
- packet arriving to full queue dropped (aka lost)



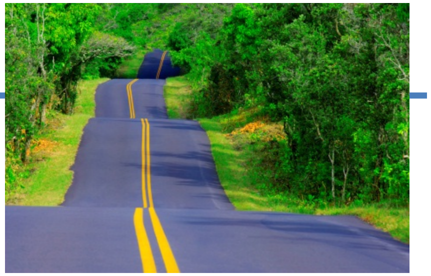
Connecting to *"Packet switching vs Circuit switching"*

- 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 <u>circuit-like</u> behavior?**
  - **bandwidth guarantees are needed for some apps**
  - **Some routing policy can help???**
    - **Cf virtual circuit**

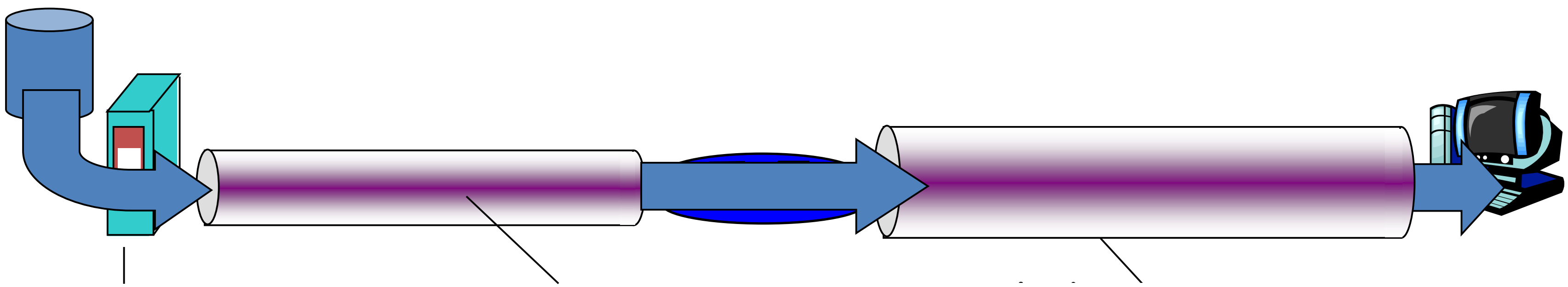
Roadmap



1. Zooming into core
   - Ways of data transfer
   - Routing
   - Performance: delays, (& loss)…
   - …. throughput
2. Network/Internet structure complemented:
   - access net, physical media
   - backbones, NAPs, ISPs
3. Security prelude

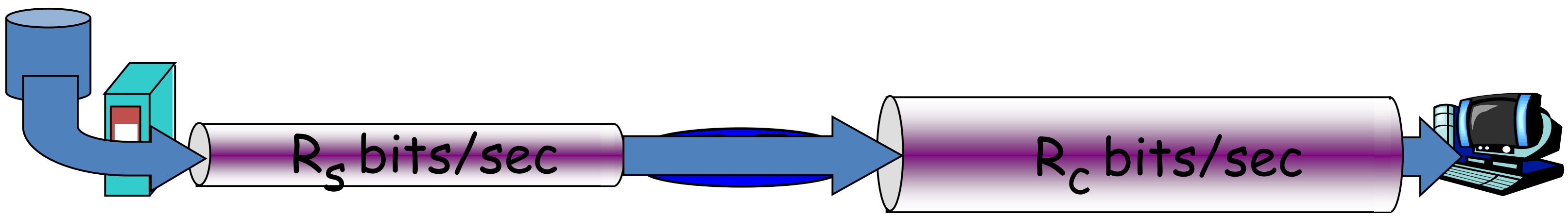
Throughput

- *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

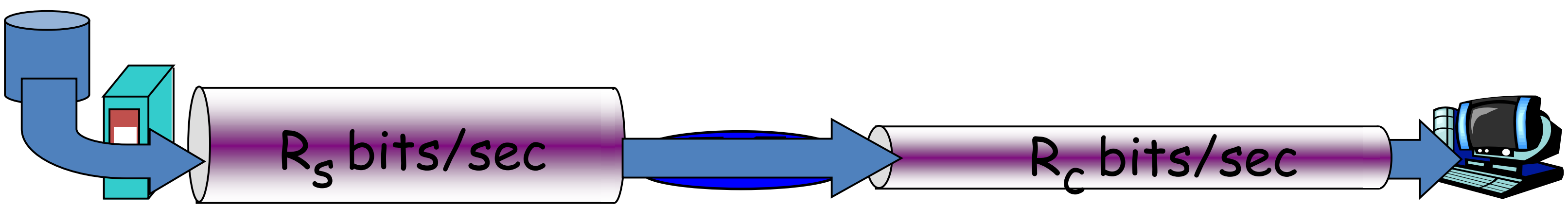


Throughput (more)

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



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

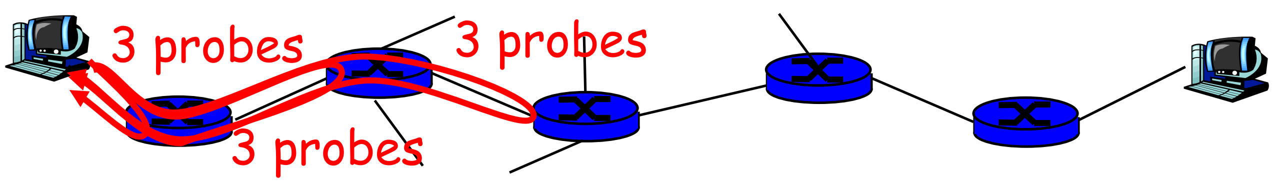


bottleneck link

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

… "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

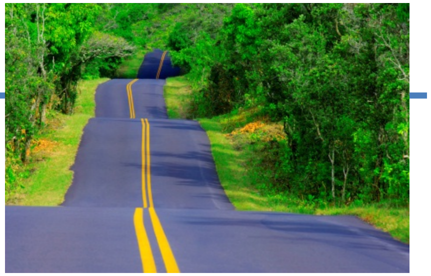
Three delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

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 reponse (probe lost, router not replying)

Roadmap



1. Zooming into core
   – Ways of data transfer
   – Routing
   – Performance: delays, (& loss) …
   – …. throughput
2. Network/Internet structure complemented:
   – access net, physical media
   – backbones, NAPs, ISPs
3. Security prelude

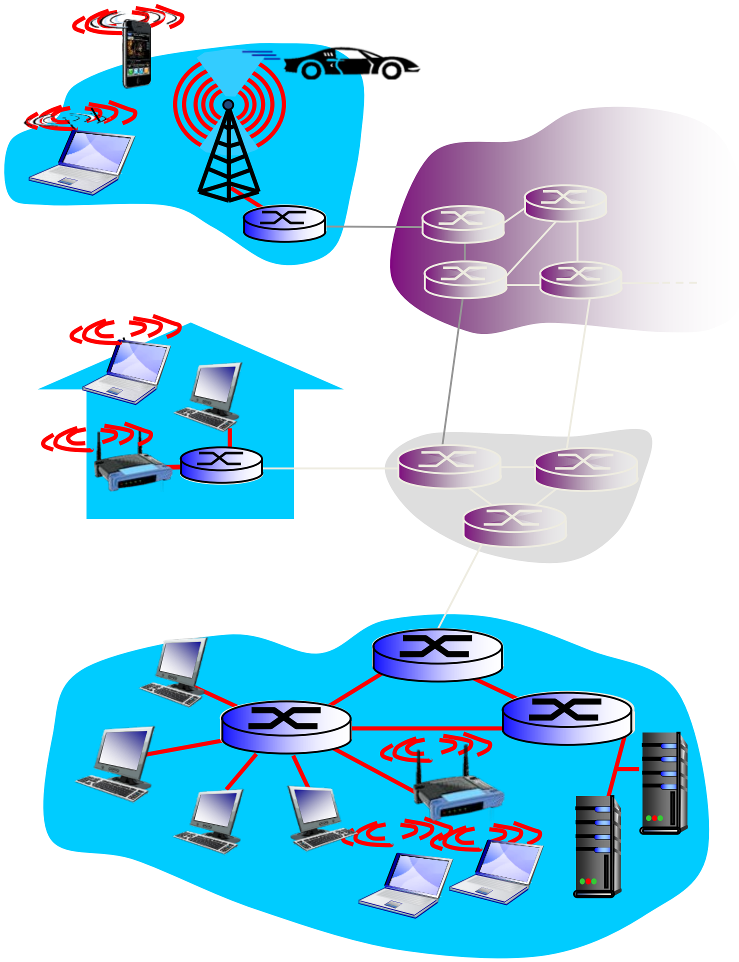
Access networks and physical media

Q: How to connect end systems to edge router?

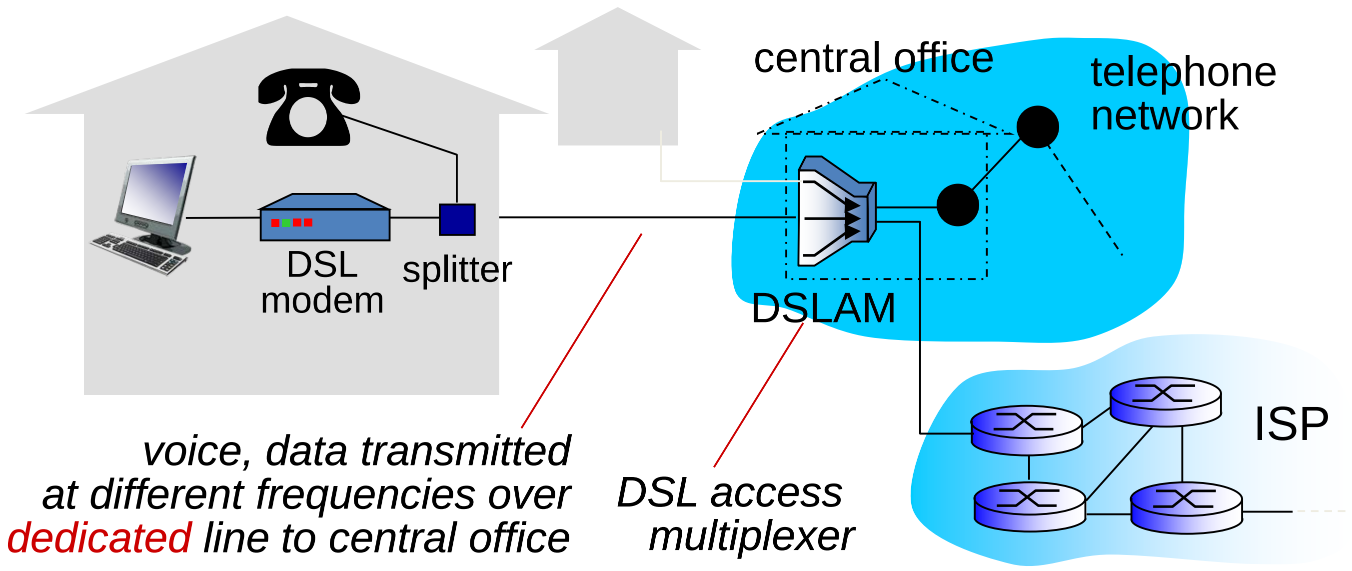
- residential access nets
- institutional access networks (school, company)
- mobile access networks

keep in mind:

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

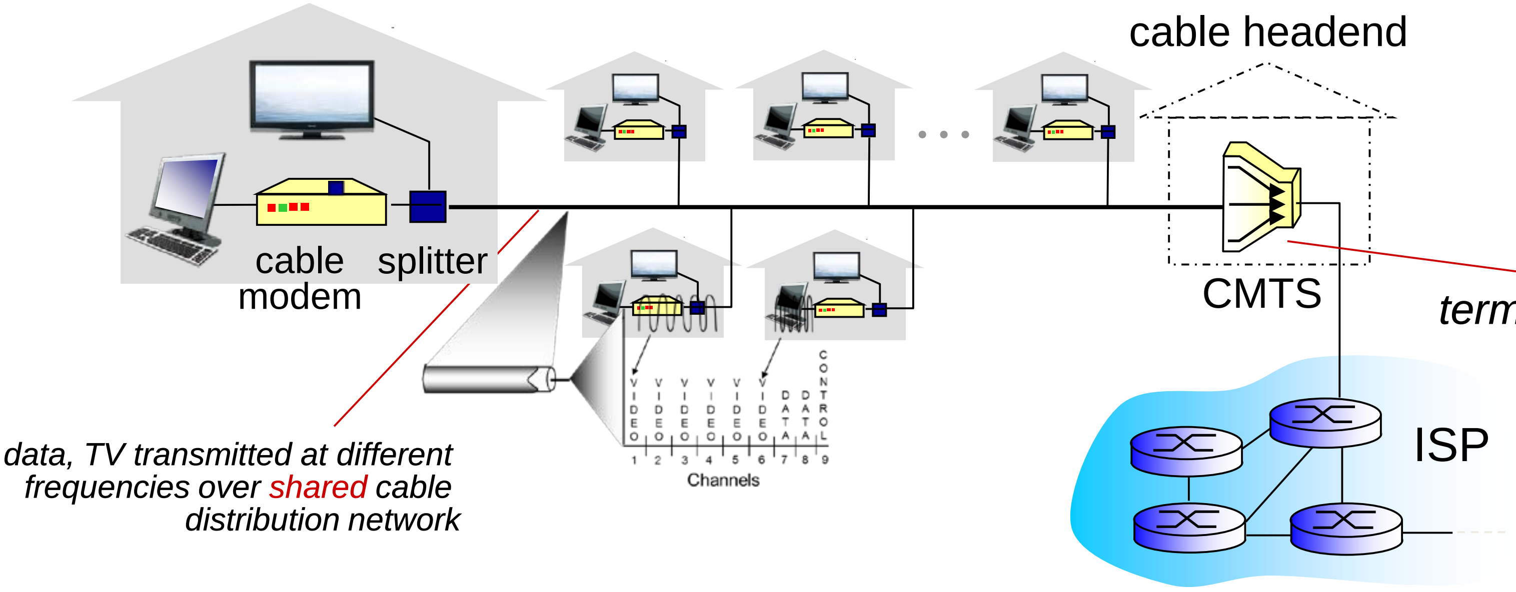


Access net: digital subscriber line (DSL)



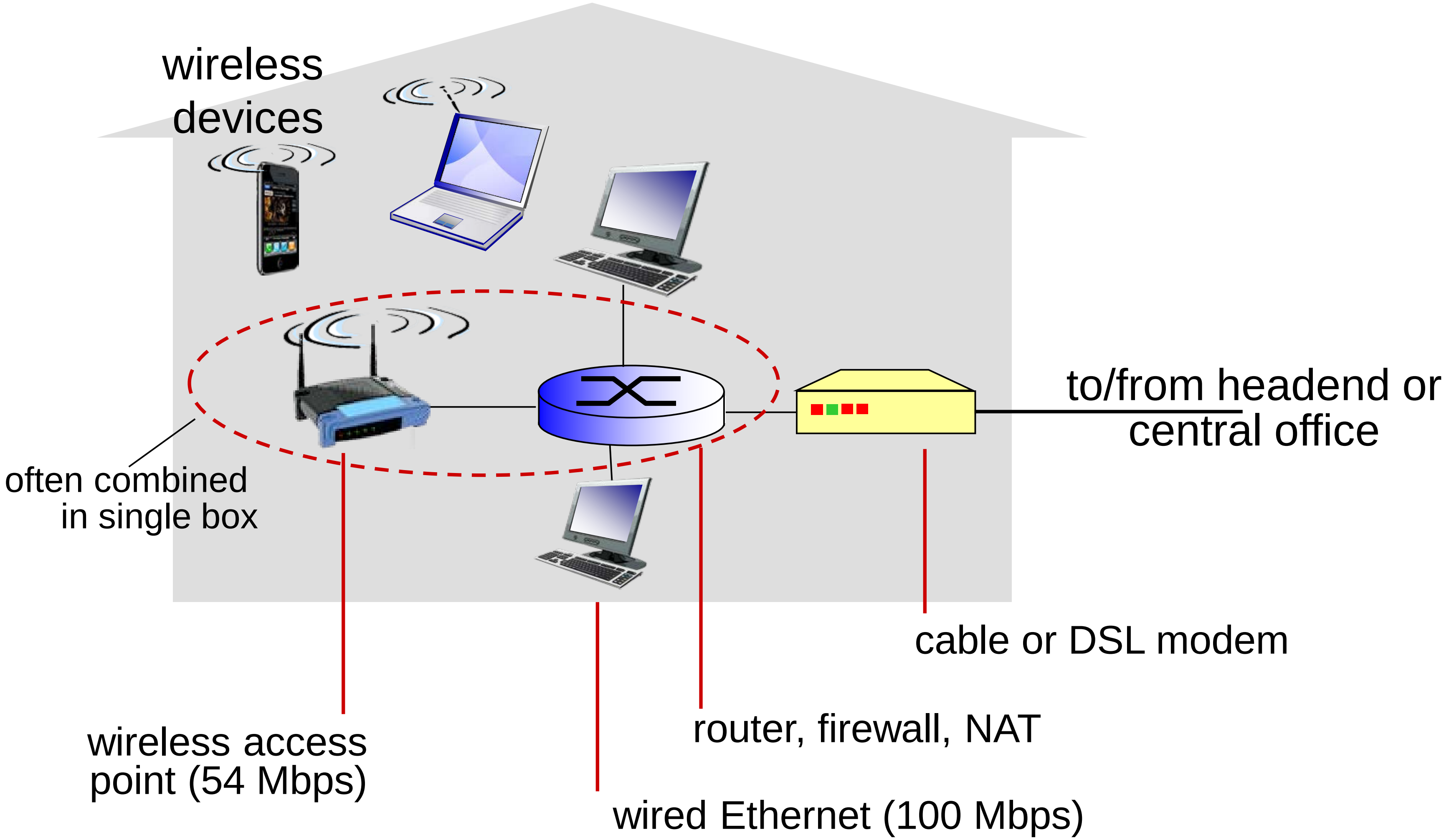
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access net: cable network

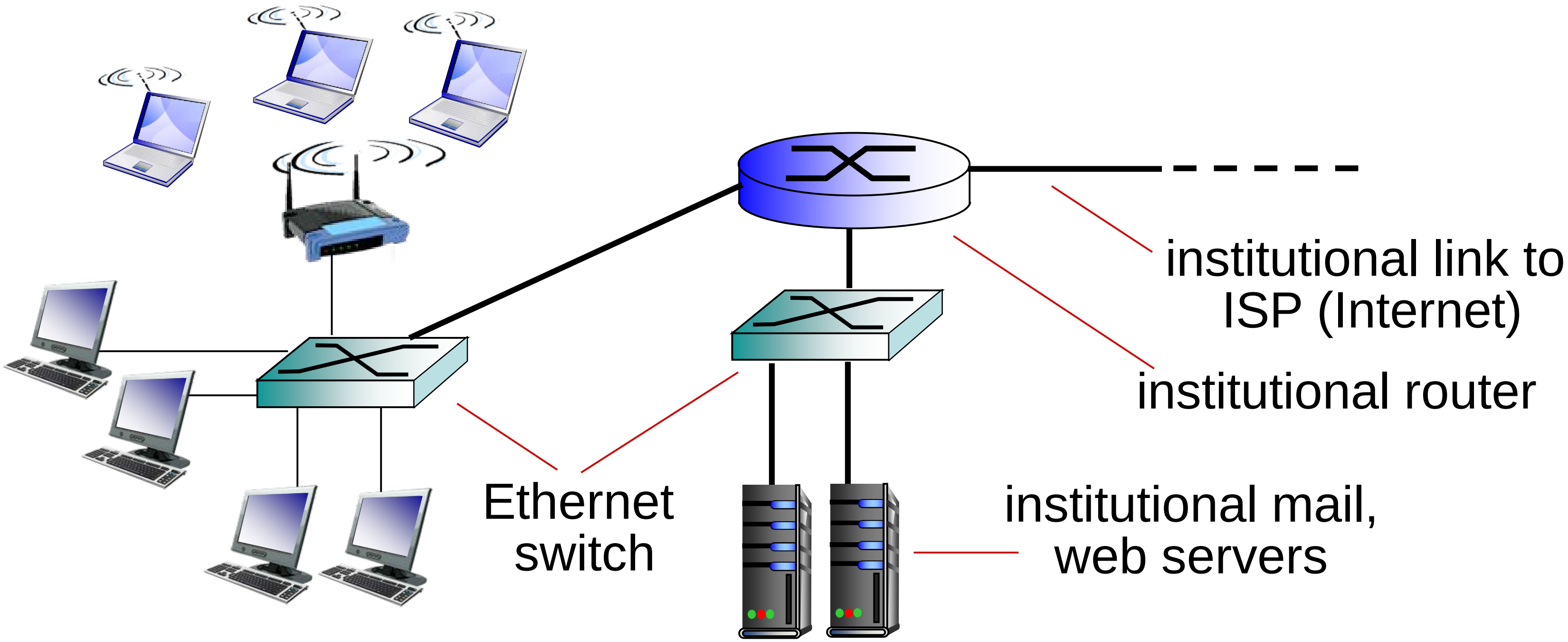


- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cables, attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

Access net: home network



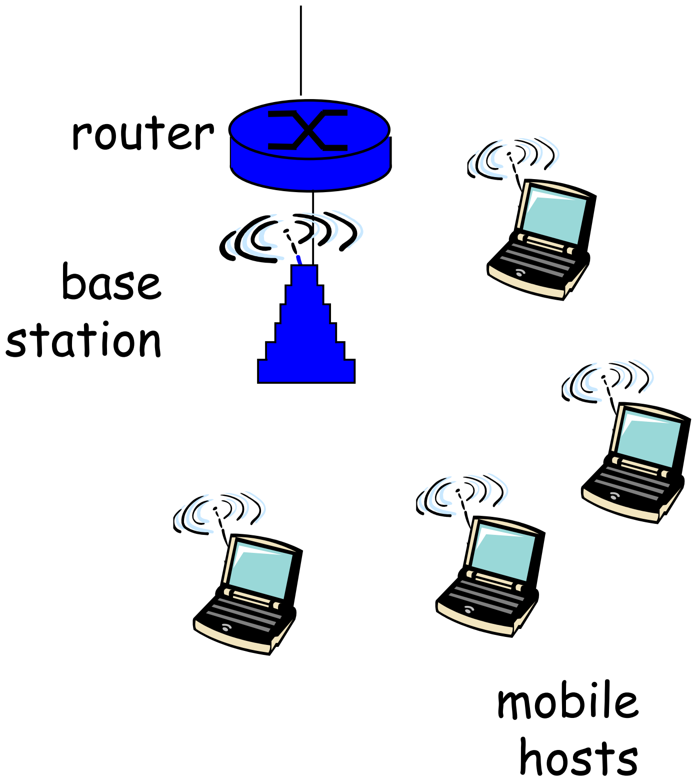
Enterprise access networks (Ethernet)



- typically used in companies, universities, etc
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates

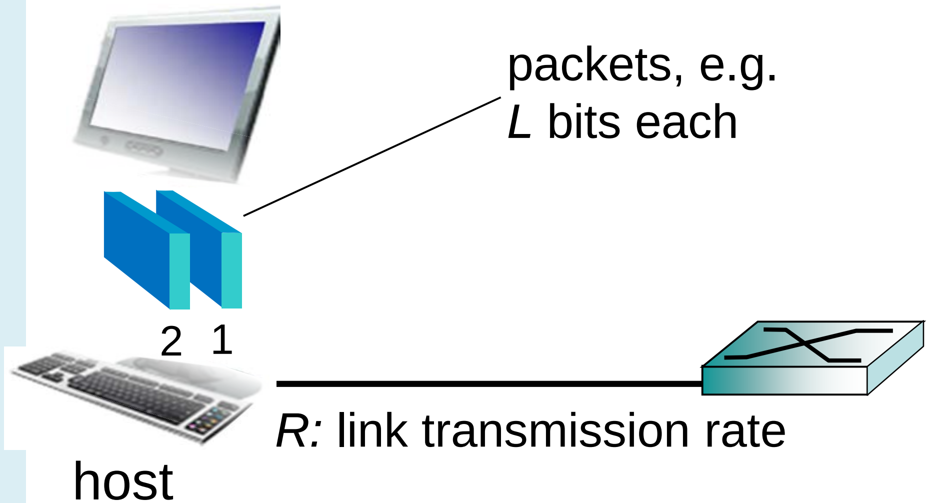
Wireless access networks

- shared *wireless* access network connects end system to router
  - “adhoc” or via base station aka “access point”
- wireless LANs (10’s m)
  - 802.11b/g (WiFi): 11 or 54 Mbps
- wider-area wireless access (10’s km)
  - provided by telco operator
  - ~1-10 Mbps over cellular system
  - 3G, 4G: LTE



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

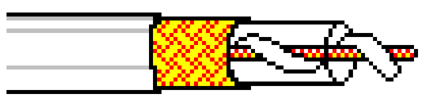


aka link *capacity,*
aka link bandwidth

Guided physical Media: coax, fiber, twisted pair

Coaxial cable:

- wire (signal carrier) within a wire (shield)
- broadband: multiple channels multiplexed on cable (HFC, cable TV)



Fiber optic cable:

- low attenuation: fewer repeaters
- low error rate: light pulses immune to electromagnetic noise
- high-speed operation: e.g., 10-100 Gps

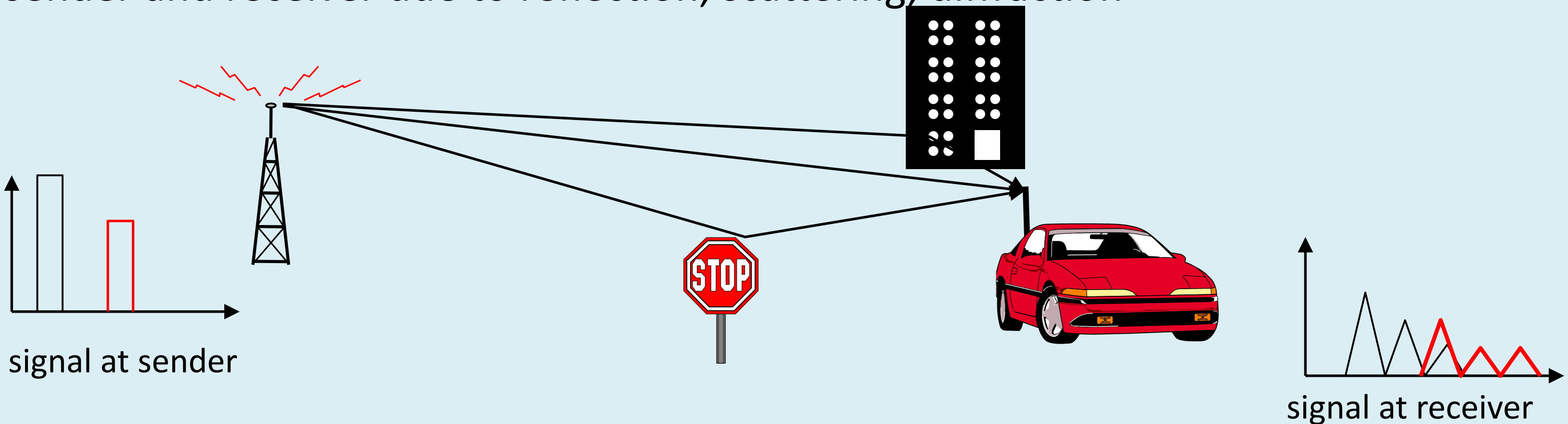
Twisted Pair (TP)

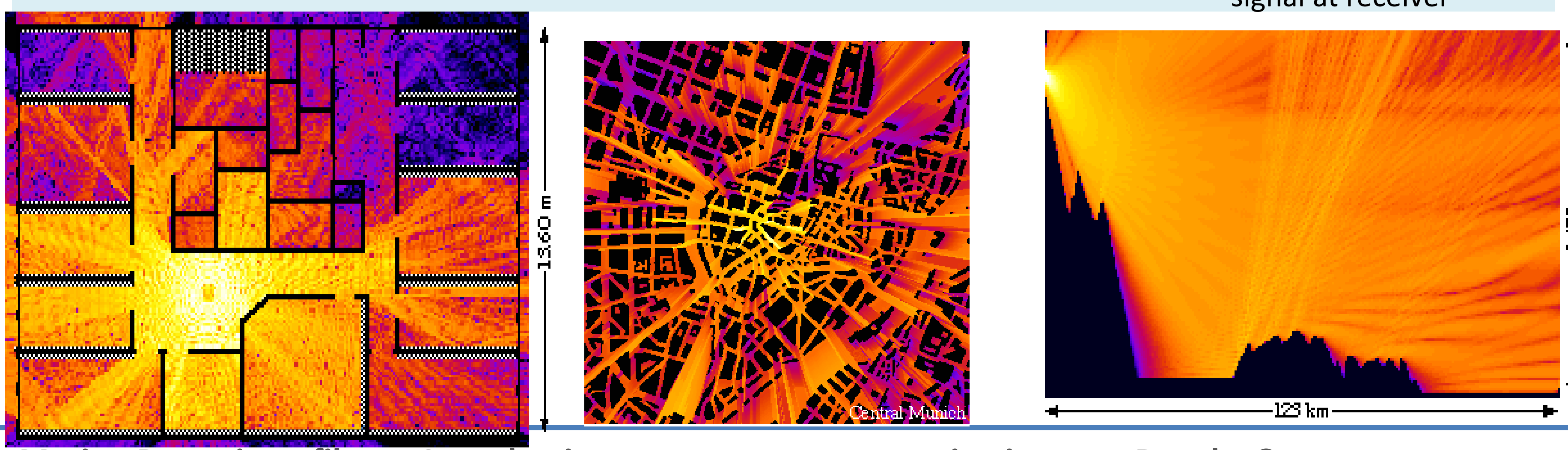
- two insulated copper wires
  - Category 3: traditional phone
  - Category 5/6: more twists, higher insulation: 100-1000 Mbps, Gbps

Unguided Physical media: Radio
Properties: Attenuation, Multipath propagation

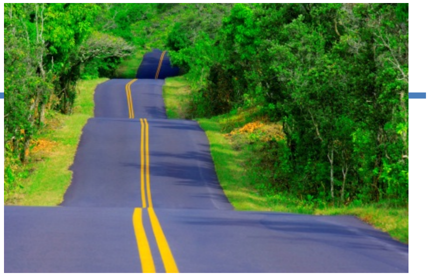
radio links (Mbps): terrestrial microwave, LAN/WiFi, wide-area/cellular, satellite

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





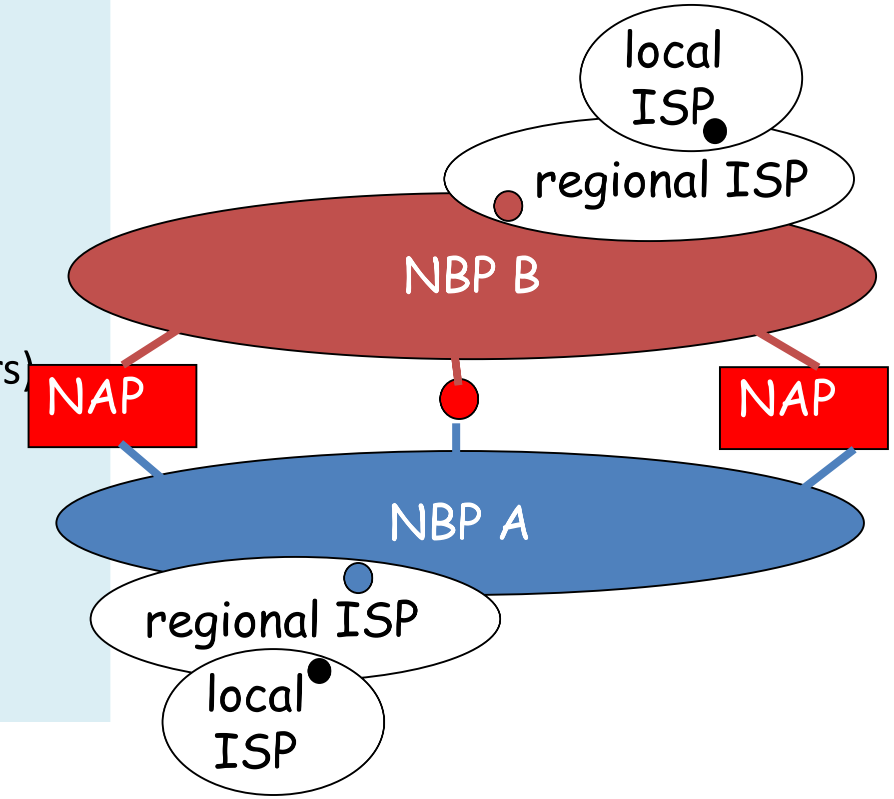
Roadmap



1. Zooming into core
   – Ways of data transfer
   – Routing
   – Performance: delays, (& loss)…
   – …. throughput
2. Network/Internet structure complemented:
   – access net, physical media
   – backbones, NAPs, ISPs
3. Security prelude

Internet structure: network of networks

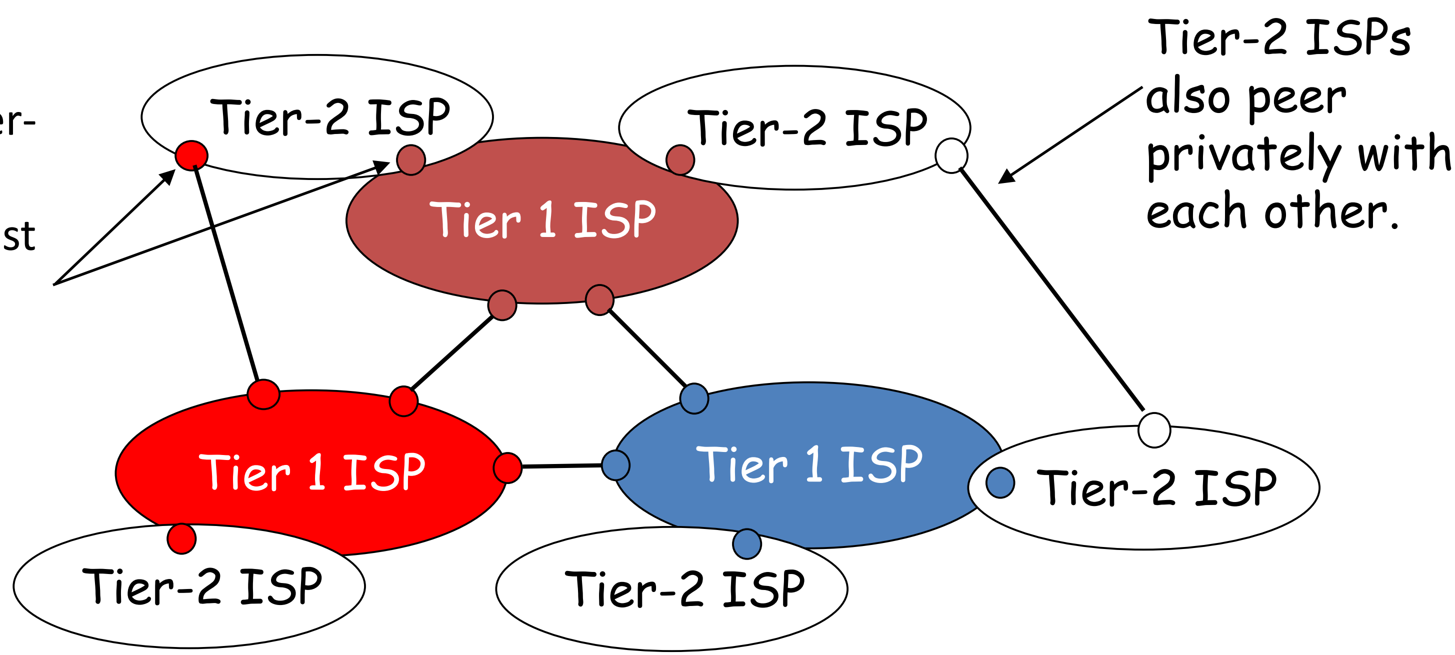
- roughly hierarchical
- national/international backbone providers (NBPs)- tier 1 providers
  - e.g. BBN/GTE, Sprint, AT&T, IBM, UUNet/Verizon, TeliaSonera
  - interconnect (peer) with each other privately, or at public Network Access Point (NAPs: routers or NWs of routers)
- regional ISPs, tier 2 providers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

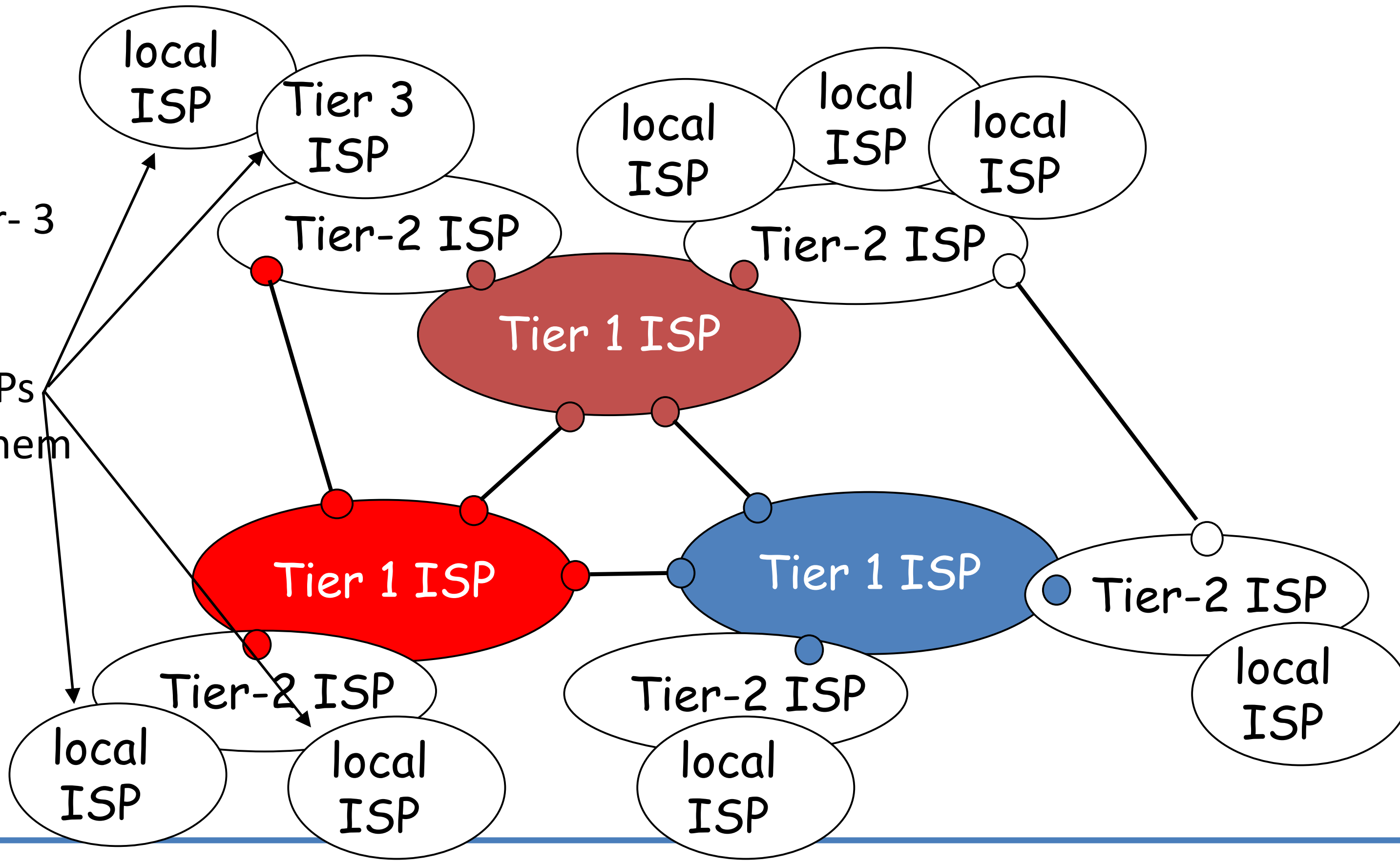
Tier-2 ISP pays tier-1 ISP for connectivity to rest of Internet
- tier-2 ISP is *customer* of tier-1 provider



Internet structure: network of networks

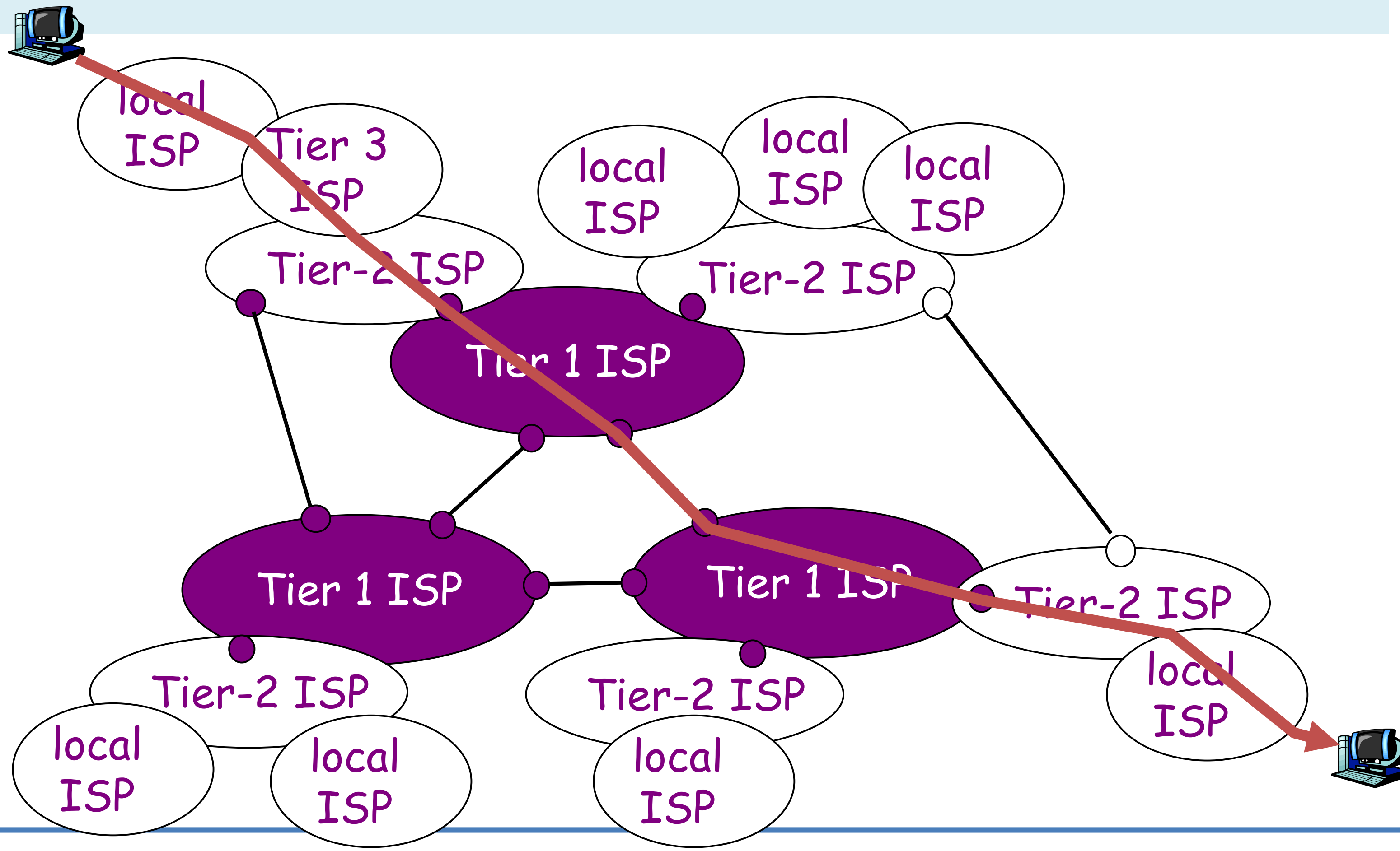
- "Tier-3" ISPs and local ISPs
  - last hop ("access") network (closest to end systems)

Local and tier- 3 ISPs are *customers* of higher tier ISPs connecting them to rest of Internet

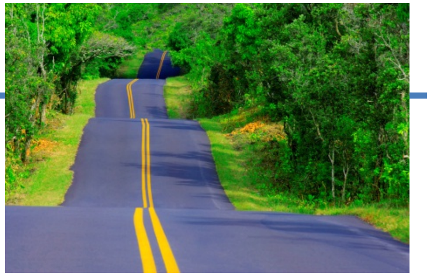


Internet structure: network of networks

- a packet passes through many networks



Roadmap



1. Zooming into core
   – Ways of data transfer
   – Routing
   – Performance: delays, …
   – …. throughput, loss
2. Network/Internet structure complemented:
   – access net, physical media
   – backbones, NAPs, ISPs
3. Security prelude

Network Security Prelude

- 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!

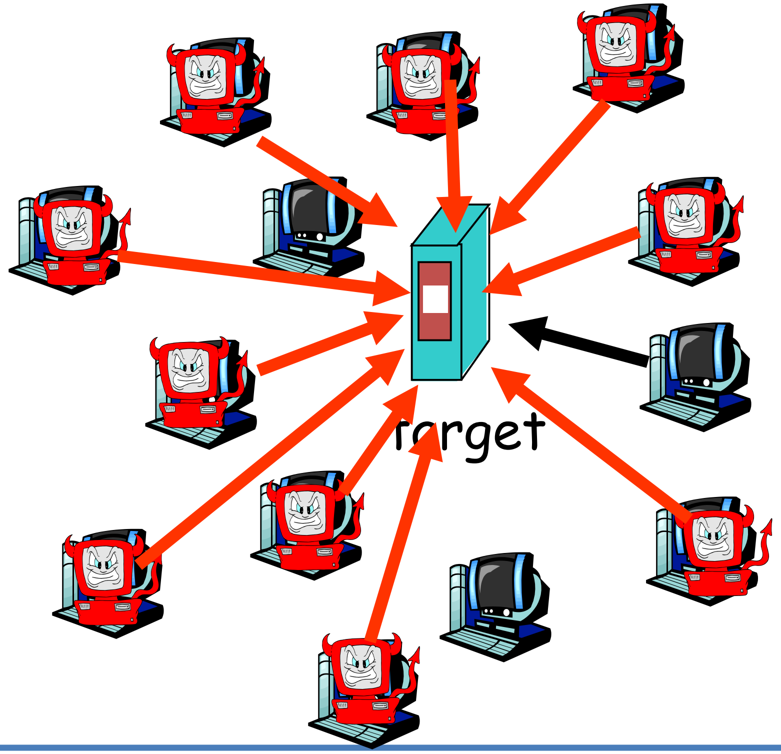
Bad guys can put malware into hosts via Internet

- 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

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

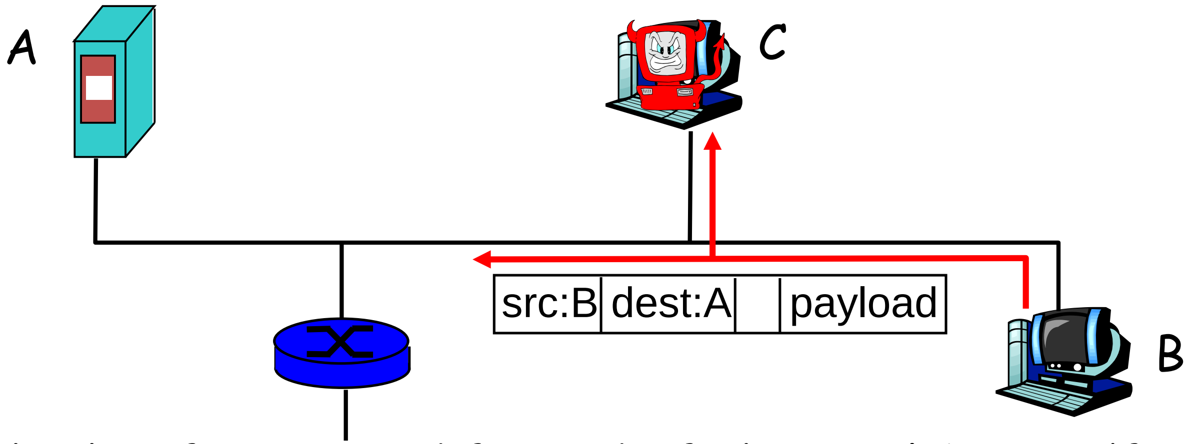
1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts



The bad guys can sniff packets

Packet sniffing:

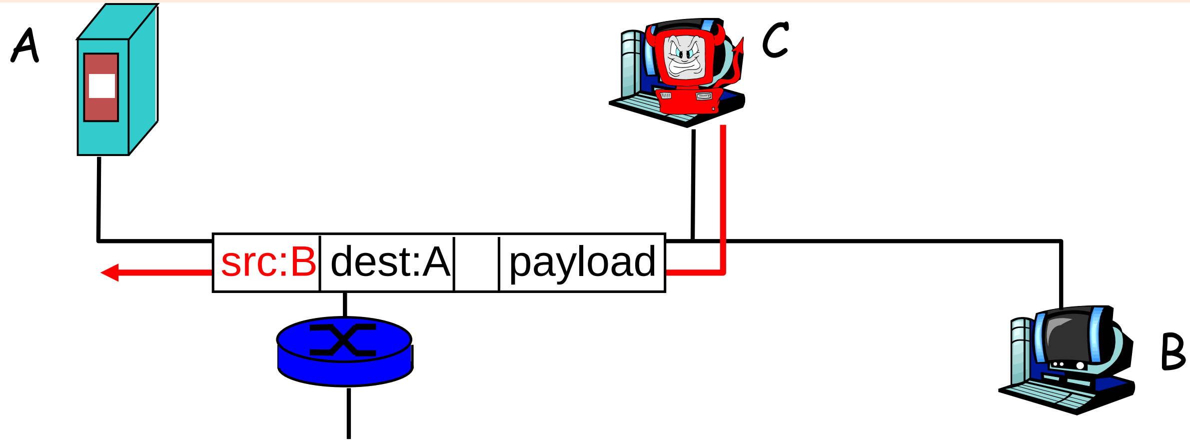
- Shared/broadcast medium (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets passing by



- Wireshark software used for end-of-chapter labs is a (free) packet-sniffer
- NOTE: be aware that it is inappropriate to use outside the lab

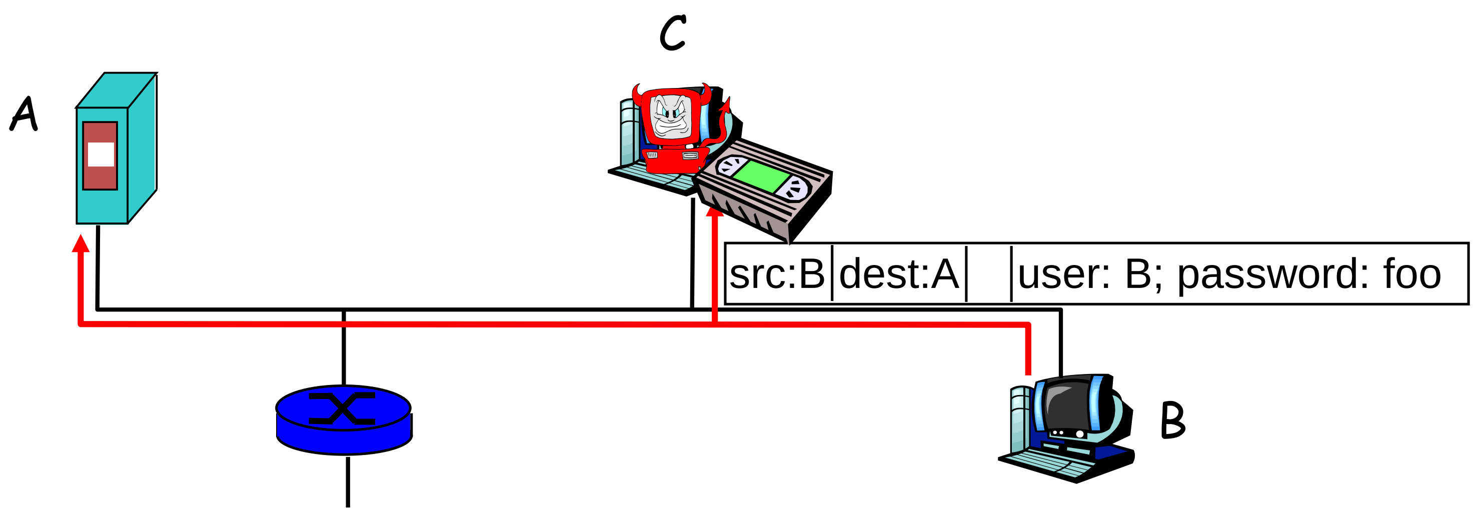
The bad guys can use false source addresses

- *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



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 ☺)

In order to 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

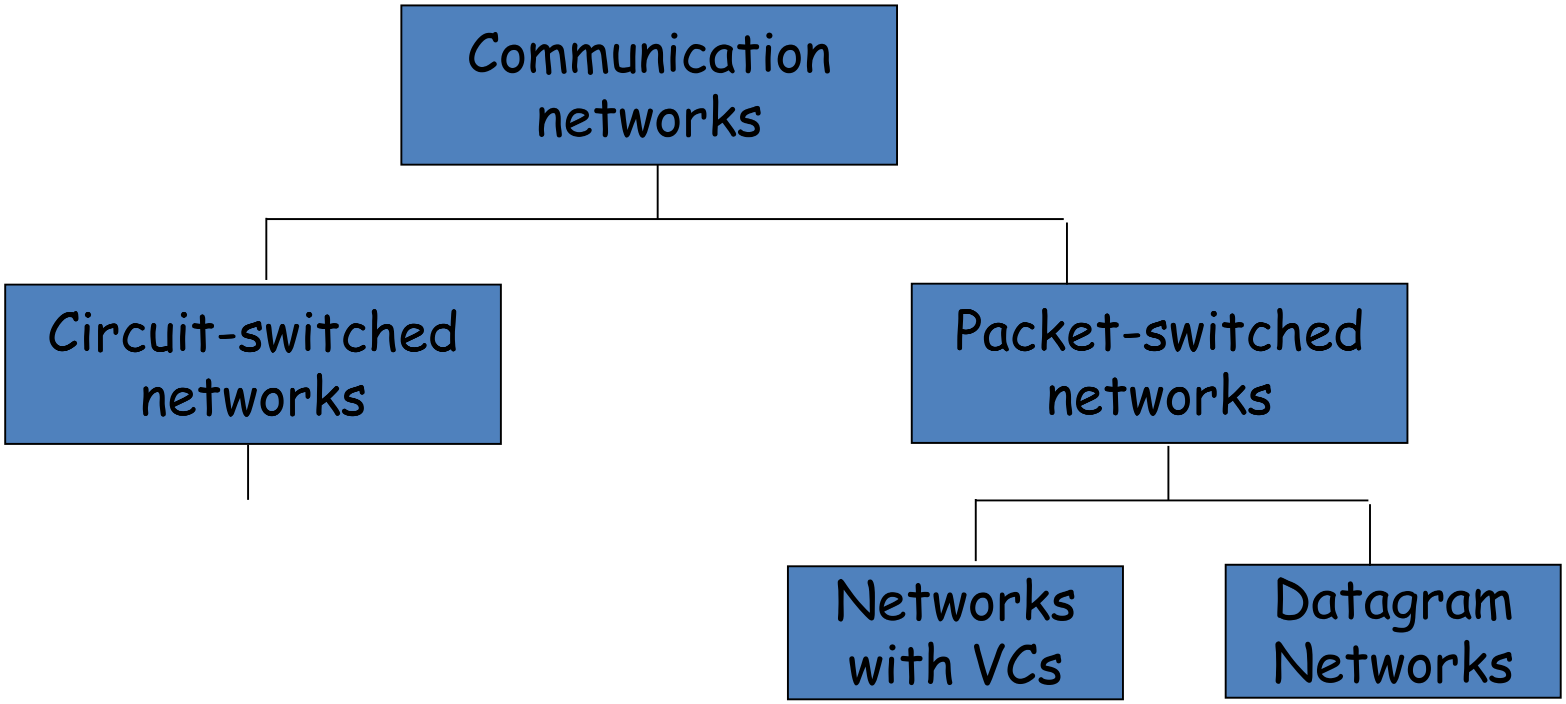
Review questions from Kurose-Ross book, chapter 1 (for basic study)

- 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

Review: Network Taxonomy



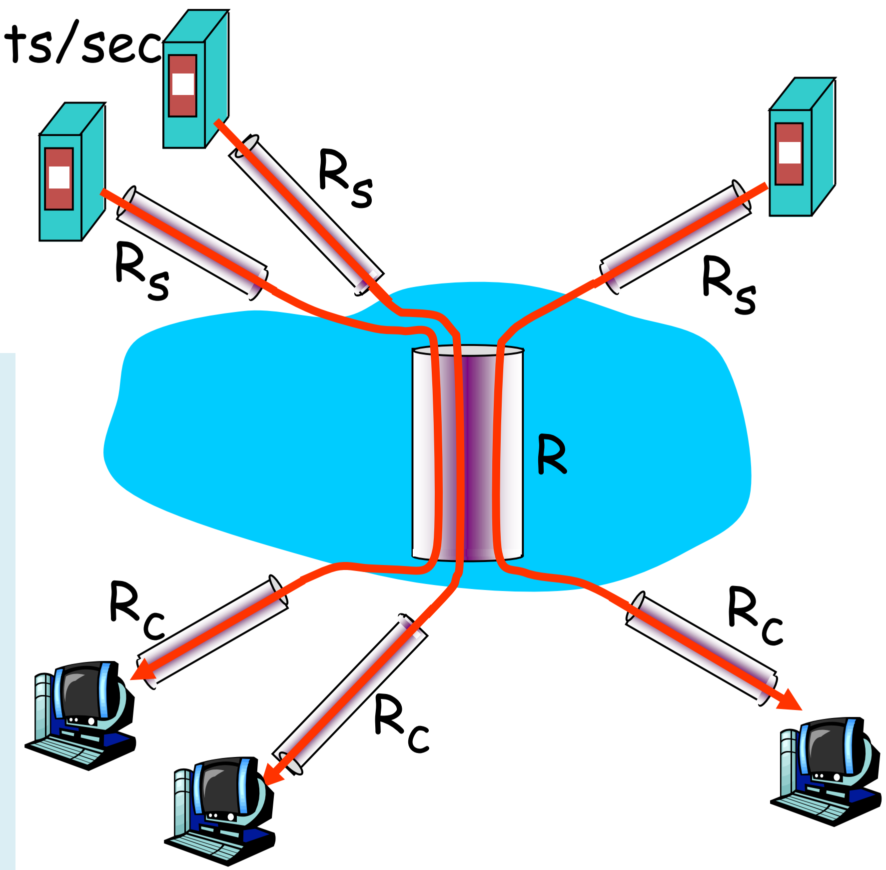
Datagram network (eg Internet) cannot be characterized either connection-oriented or connectionless.

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

Review questions:

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

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)