CPSC441

Chapter 1

- The internet is comprised of billions of connected devices.
  - Hosts are the end systems and they run network apps at Internet's edge.
- Packet Switches: Forward packets (data chunks) → routers, switches
- Communication links: fiber, copper, radio, satellite
- Transmission rate: Bandwidth
- Networks: A collection of devices, routers & links managed by an organization.
- Internet: A network of networks (interconnected ISPs)
- Protocols: They control the sending and receiving of messages.
- Internet Standards:
  - RFC - Request For Comments
  - IETF - Internet Engineering Task Force

Service View:

- The infrastructure that provides services to apps such as web, streaming video, multimedia teleconferencing, email, games, ecommerce, social media, interconnected appliances.
- Provides programming interface to distributed applications:
  - hooks allowing sending/receiving apps to connect to, use Internet transport service.
  - provides service options, analogous to postal service.

Protocols

- Protocols define the format, order of messages sent and received among network entities, and actions taken on message transmission and receipt.

Internet Structure

- Network Edge
  - Hosts → 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 (Wi Fi, 4G/5G)

What to look for:

- Transmission rate (bps) of access network
- Shared or Dedicated access among users?

Cable-based Access

- Frequency Division Multiplexing (FDM): Different channels transmitted in different frequency bands
- Hybrid Fiber Coax (HFC): Asymmetric → up to 40 Mbps - 1.2 Gbs downstream transmission rate, 30 - 100 Mbps upstream transmission rate.
- Network of cable, fiber attaches homes to ISP router
  - Homes share access network to cable headend

Digital Subscriber Line (DSL)

- Use existing telephone line to central office DSLAN
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- 24-52 Mbps dedicated downstream transmission rate
- 3.5-16 Mbps dedicated upstream transmission rate

Home Networks

Wireless devices, wifi access point, wired ethernet, router, firewall NAT, cable or DSL modem

Wireless Access Networks

Shared wireless access network connects end system to router via base station aka access point.

Wireless Local Area Networks (WLANs)

- Typically within 100ft of a building
- 802.11 b/g/n (WiFi): 11, 54, 450 Mbps transmission rate

Wide Area Cellular Access Networks

- provided by mobile, cellular network operator (10 kms)
- 10's Mbps
- 4G cellular networks (5G)

Enterprise Networks

- Companies, universities, etc
- mix of wired, wireless link technologies, connecting a mix of switches and routers
  - Ethernet: wired access at 100Mbps, 1Gbps, 10Gbps
  - WiFi: wireless access point at 11, 54, 450 Mbps

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.
  - Bandwidth → link capacity → link transmission rate

packet transmission delay = time needed to transmit L-bit packet into link = $\frac{L}{R}$

Links: 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 propogate freely
- Twisted pair: category 5 → 100 Mbps, 1 Gbps ethernet, Category 6 → 10 Gbps Ethernet

- Coaxial Cable:
  - two concentric copper conductors
  - bidirectional
  - broadband:
    - multiple frequency channels on cable
    - 100's Mbps per channel

- Fiber Optic Cable:
  - glass fiber carrying light pulses, each pulse a bit
  - high-speed operation → point to point transmission (10's-100's Gbps)
  - low error rate → repeaters spaced far apart, immune to electromagnetic noise
- Wireless radio
  - signal carried in electromagnetic spectrum
  - no physical wire
  - broadcast and half-duplex (sender to receiver)
  - propagation environment effects:
    reflection, obstruction by objects, interference

- Radio link types
  - terrestial microwave → up to 45Mbps/channel
  - wireless LAN (WiFi) → up to 100's Mbps
  - wide area (e.g. cellular) → 4G cellular 10's Mbps
  - satellites → up to 45Mbps per channel, 270msec end-to-end delay, geosynchronous versus low-earth-orbit

The network core

- Mesh of interconnected routers
- 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.

Packet Switching

- Transmission delay: takes L/R seconds to transmit (push out) L-bit packet into link at R bps L=10kbits, R=100Mbps, one-hop transmission delay=0.1msec
- Store and forward: Entire packet must arrive at router before it can be transmitted on next link.
- End-end delay: 2L/R (above), assuming zero propogation delay (more on delay shortly)

Queueing delay, loss

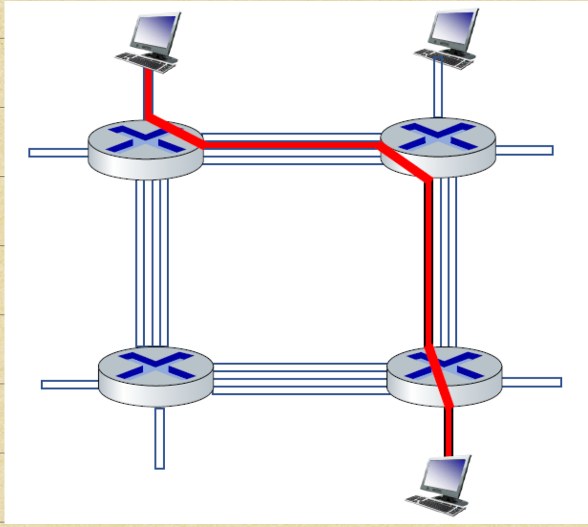
- Packet queueing and loss: If arrival rate (in bps) to link exceeds transmission rate (bps) of link for a period of time:
  - packets will queue, waiting to be transmitted on output link
  - packets can be dropped (lost) if memory (buffer) in router fills up

Two key network-core functions

- Forwarding: local action, move arriving packets from router's input link to appropriate router output link
- Routing: global action, determine source-destination paths taken by packets. (routing algorithms)

Circuit Switching

end-end resources allocated to reserved for "call" between source and destination

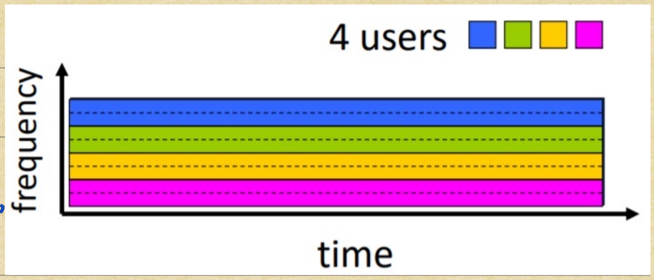


- Each link has 4 circuits. The call gets 2^{nd} circuit in top link and 1^{st} circuit in right link.
- The resources are dedicated. No sharing, guaranteed performance (circuit like
- Segment idle if not used by call (no sharing)

Commonly used in traditional telephone networks

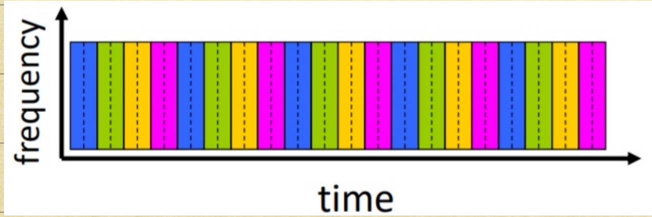
FDM and TDM

Frequency Division Multiplexing:



- optical, electromagnetic frequencies divided into (narrow) frequency bands.
- Each call allocated its own band, can transmit at max rate of that narrow band

Time Division Multiplexing

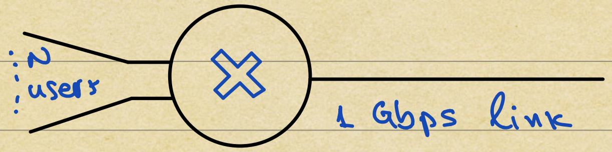


- Time divided into slots
- Each call allocated periodic slot(s), can transmit at maximum rate of (wider) frequency band, but only during its time slot.

Packet Switching vs Circuit Switching

Packet Switching allows more users to use network!

Example:



- 1 Gb/s link
- each user:

→ 100 Mb/s when active

→ active 10% time

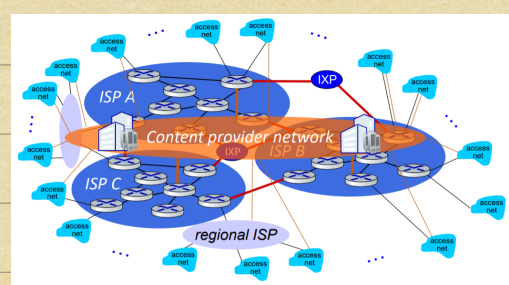
- circuit switching → 10 users
- packet switching → 35 users, probability that we have 10 or greater active users at the same time is less than .0004

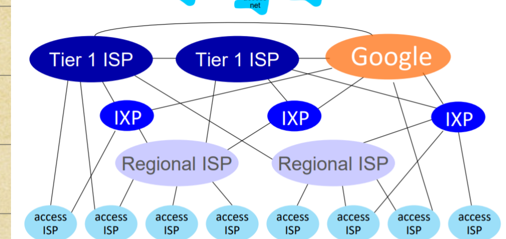
Packet Switching

- Great for bursty data - sometimes has data to send, but sometimes not
  - resource sharing
  - simple, no call setup
- Excessive congestion possible, packet delay/loss due to buffer overflow
  - protocols needed for reliable data transfer & congestion control
- Bandwidth guaranteed usually for audio/video applications

Internet Structure

- Hosts connect to Internet via Internet Service Providers (ISPs)
  - residential, enterprise ISPs
- Access ISPs in turn must be interconnected in order for any 2 hosts to be able to send packets to each other
- Resulting network of networks is very complex
  - economics & national policies drive evolution





At the "center": small # of well connected large networks:

- tier 1 commercial ISPs (Level 3, Sprint, AT&T, NTT), national and international coverage.
- content provider networks (Google, Facebook) private network that connects its data centers to Internet, often bypassing tier-1, regional ISPs.

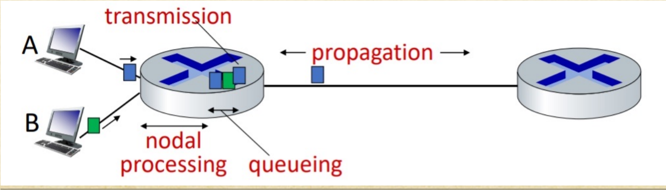
How does packet loss and delay occur?

Packets queue in router buffers

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

So we lose packets at the buffer during arrival

Packet delay: four sources



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

dproc: nodal processing

- check bit errors
- determine output link
- typically < msec

dqueue: queueing delay

- time waiting at output link for transmission
- depends on congestion level of router

dtrans: transmission delay

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

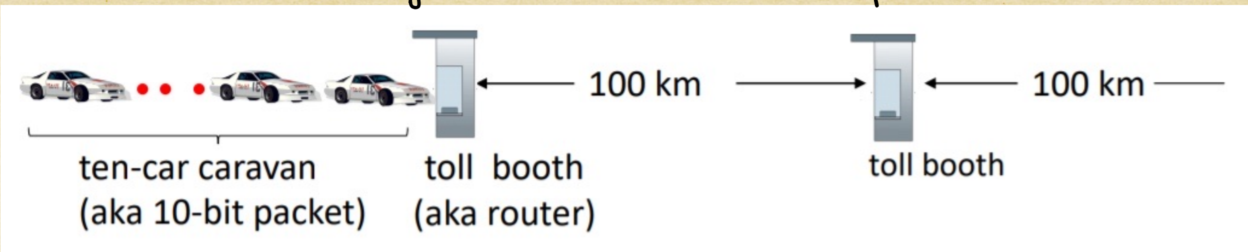
dprop: propagation delay

- d: length of physical link
- s: propagation speed ($\sim 2\times10^8$ m/sec)
- $d_{prop} = d/s$

different

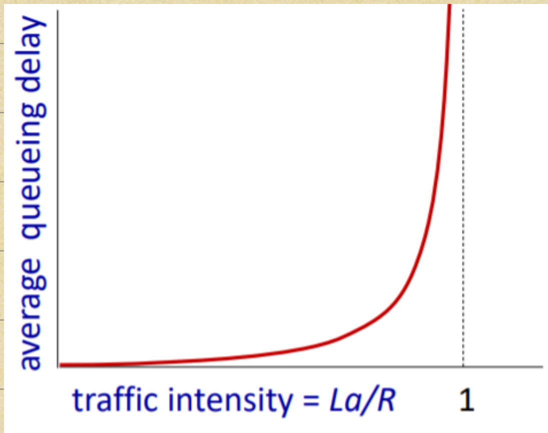
Caravan analogy

- cars "propagate" at 100km/hr
- toll booth takes 12sec to service car(bit transmission time)
- car ~ bit; caravan~packet
- time to "push" entire caravan through toll both onto highway:
  100km/(100km/hr)=1 hr
- A: 62 minutes(How long until caravan is lined up before 2nd toll booth.



If cars propagate at 1000km/h and the tollbooth takes a minute to service a car at a booth. Will cars arrive to 2nd booth before all cars serviced at first booth?
Yes! After 7 min the first car arrives at booth 2, and 3 cars will still be at booth 1.

Packet queueing delay



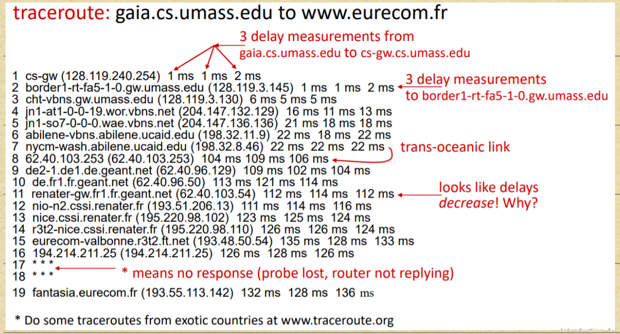
- R: link bandwidth
- L: packet length
- a: average packet arrival rate
- $La/R \sim 0$: avg. queueing delay small
- $La/R \to 1$: avg. queueing delay large
- $La/R > 1$: more "work" arriving is more than can be serviced-avg delay infinite!

Real Internet delays and routes

- **Traceroute program:** provides delay measurement from source to router along end-end Internet path towards destination.

  For all i :

  - sends three packets that will reach router i on path towards destination(with time-to-live field value of i)
  - router i will return packets to sender.
  - sender measures time interval between transmission and reply.



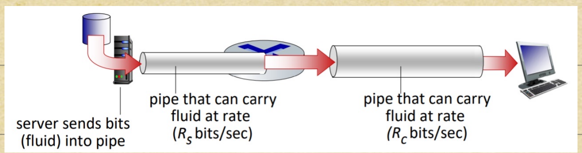
traceroute: gaia.cs.umass.edu to www.eurecom.fr

```
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
```


* 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 (aka lost)
- Lost packet may be retransmitted by previous node, by source end system, or not at all.

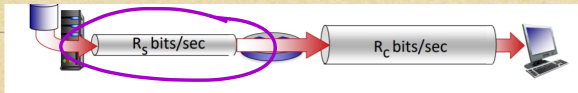


Throughput

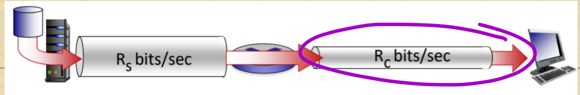
- **throughput:** rate(bits/time unit) at which bits are being sent from sender to receiver.
  - instantaneous → rate at given point in time
  - average → rate over longer period of time

What is average end-end throughput?

$R_s < R_c$

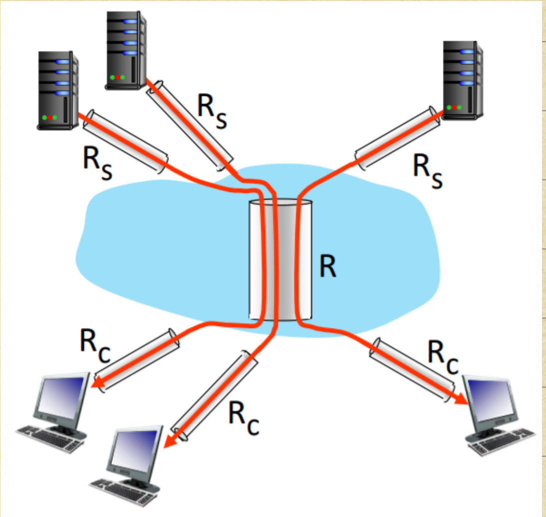


$R_s > R_c$



Bottleneck link: link on end-end path that constraints end-end throughput.

Network Scenario



- 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 bit/sec

Network Security

- field of network security:
  - How bad guys can attack computer networks
  - How we can defend networks against attacks
  - How to design architecture that are immune to attacks

Internet protocol designers are playing catch up

We need to consider security on all layers.

Malware

A host may get a malware from:

- virus: Self-reprecating infection by receiving/executing object (email attachment)
- worm: Self-reprecating infection by passively receiving object that gets itself executed

Spyware malware: Record keystrokes, web sites visited, upload info to collection site.

An infected host can be enrolled in botnet, used for spam or distributed denial of service (DDoS) attacks

Denial of Service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resourse with bogus traffic.

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

Packet interception

packet sniffing:

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

Fake Identity:

IP spoofing: send packet with false source address.

Each layer of the protocols of the Internet implements a service.

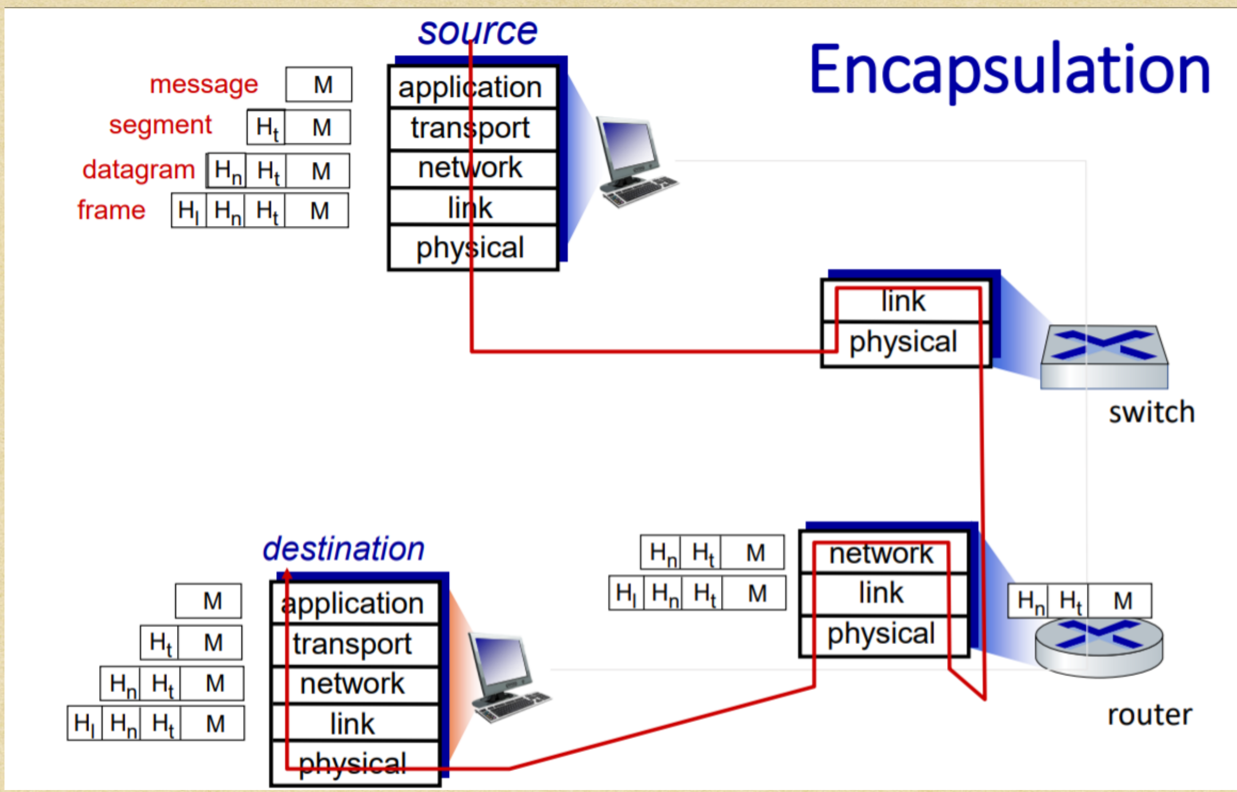
Layering

Allows us to deal 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 in layer's service implementation: transparent to the rest of the system
  - change in gate procedure doesn't affect the rest of the system.
- Is layering considered harmful?
- Layering in other complex systems?

Internet protocol stack

- **Application**: supporting network applications
  - IMAC, SMTP, HTTP
- **Transport**: process-process data transfer
  - TCP, UDP
- **Network**: routing of datagrams from source to destination.
  - IP, routing protocols
- **Link**: data transfer between neighboring network elements
  - Ethernet, 802.11 (WiFi), PPP
- **Physical**: bits on the wire



Internet history

1961-1972: Early packet-switching principles

- 1961: Kleinrock - queueing theory shows effectiveness of packet-switching
- 1964: Baran - packet-switching in military nets
- 1967: ARPAnet conceived by Advanced Research Projects Agency
- 1969: first ARPAnet node operational
- 1972:
  - ARPAnet public demo
  - NCP(Network Control Protocol) first host protocol
  - first e-mail program
  - ARPAnet has 15 nodes

1972-1980:

- 1970: ALOHAnet satellite network in Hawaii
- 1974: Cerf and Kahn - architecture for interconnecting networks
- 1976: Ethernet at Xerox PARC
- late 70's: proprietary architectures: DECnet, SNA, XNA
- late 70s: switching fixed length packets(ATM precursor)
- 1979: ARPAnet has 200 nodes

Cerf and Kahn's internetworking principles:

- Minimalism, autonomy - no internal changes required to interconnect networks
- best-effort service model
- stateless routing
- decentralized control

1980-1990: new protocols, a proliferation of networks

- 1982: smtp e-mail protocol defined
- 1983: deployment of TCP/IP
- 1983: DNS defined for name-to-IP-address translation
- 1985: ftp protocol defined
- 1988: TCP congestion control
- new national networks: CSnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks

1990, 2000s: commercialization, the Web, new applications

- early 1990s: ARPAnet decommissioned
- 1991: NSF lifts restrictions on commercial use of NSFnet
- early 1990s: Web
  - hypertext
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, later Netscape
  - late 1990s: commercialization of the Web

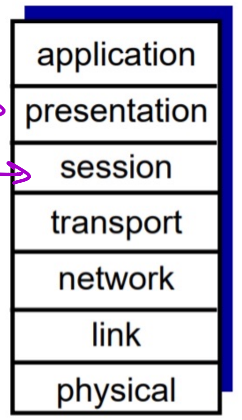
Late 1990s-2000s:

- more killer apps: instant messaging, P2P file sharing
- network security to forefront
- est. 50 million host, 100 million+ users
- backbone links running at Gbps

2005-present: more new applications, Internet is "everywhere"

- 18B devices attached to Internet
- aggressive deployment of broadband
- increasing ubiquity of high-speed wireless access: 4G/5G, WiFi
- emergence of online social networks
- Service Providers create their own networks
  - bypass commercial Internet to connect "close" to end user, providing "instantaneous" access to search, video content
- enterprises run their services in "cloud"

ISO/OSI reference model

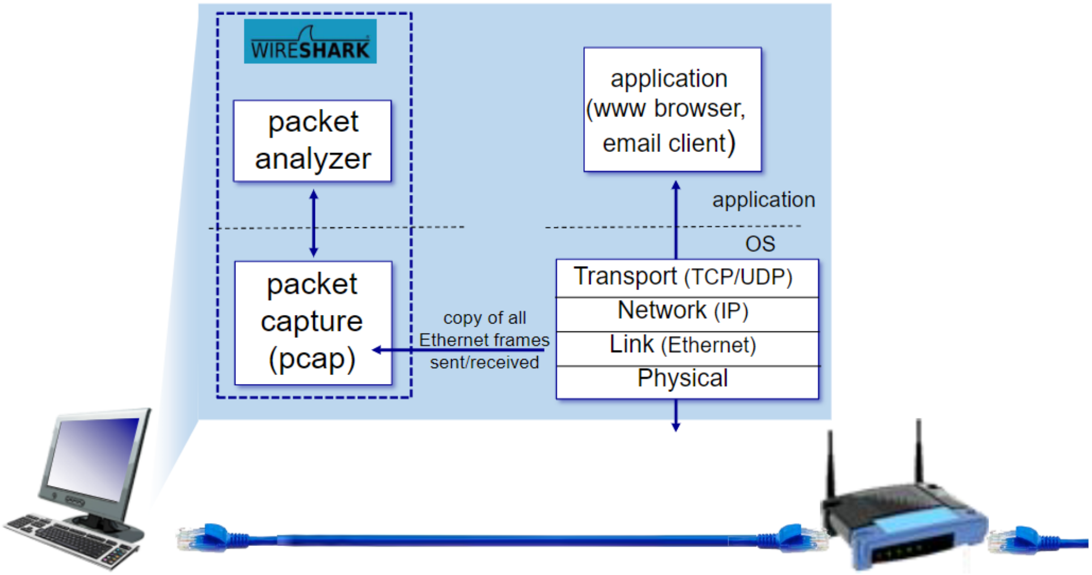


The seven layer OSI/ISO reference model

Two layers not found in the Internet Protocol stack

- Presentation: Allow applications to interpret meaning of data, e.g, encryption, compression, machine specific conventions.
- Session: Synchronization, checkpointing recovery of data exchange
- These services if needed must be implemented in application.

Wireshark



WIRESHARK
packet analyzer
packet capture (pcap)
copy of all Ethernet frames sent/received
application (www browser, email client)
application
OS
Transport (TCP/UDP)
Network (IP)
Link (Ethernet)
Physical