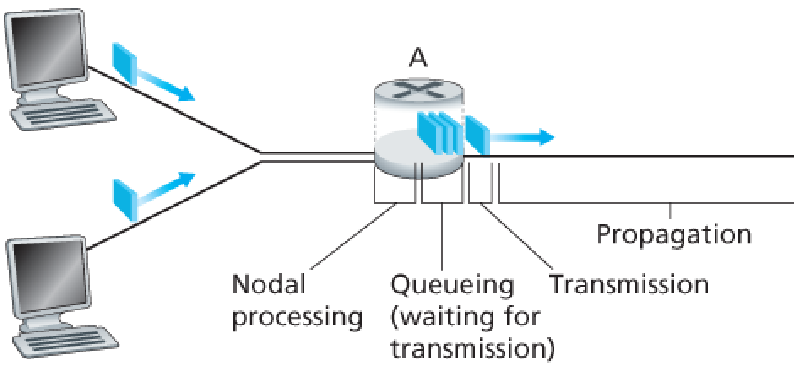
Protocol layers and service models
Internet and security

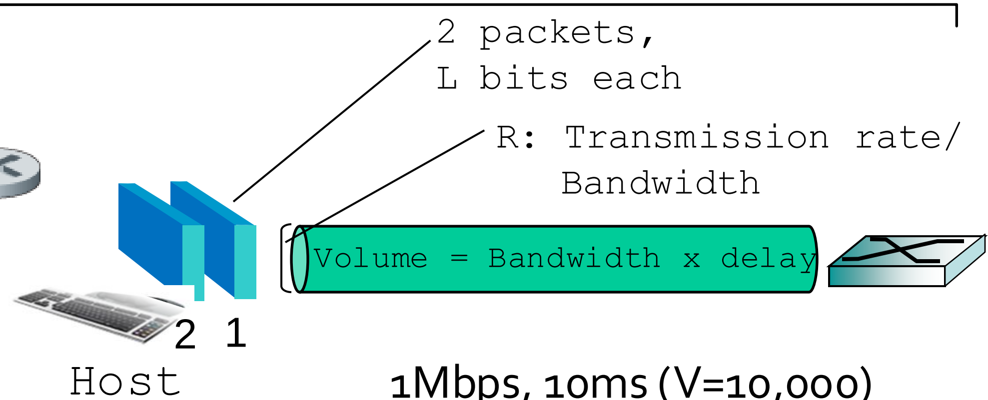
CE 352, Computer Networks

Salem Al-Agtash

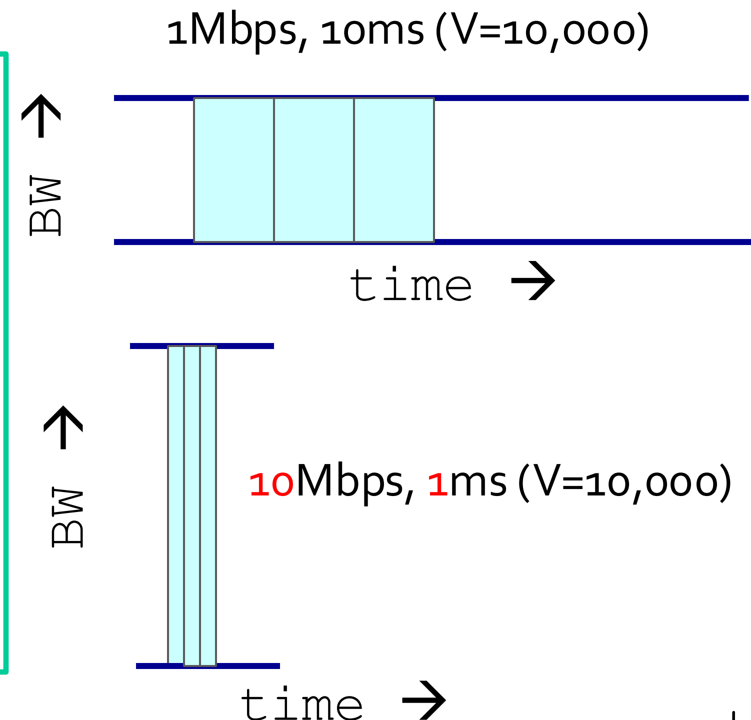
Lecture 3

Recap (Packet delay and volume)

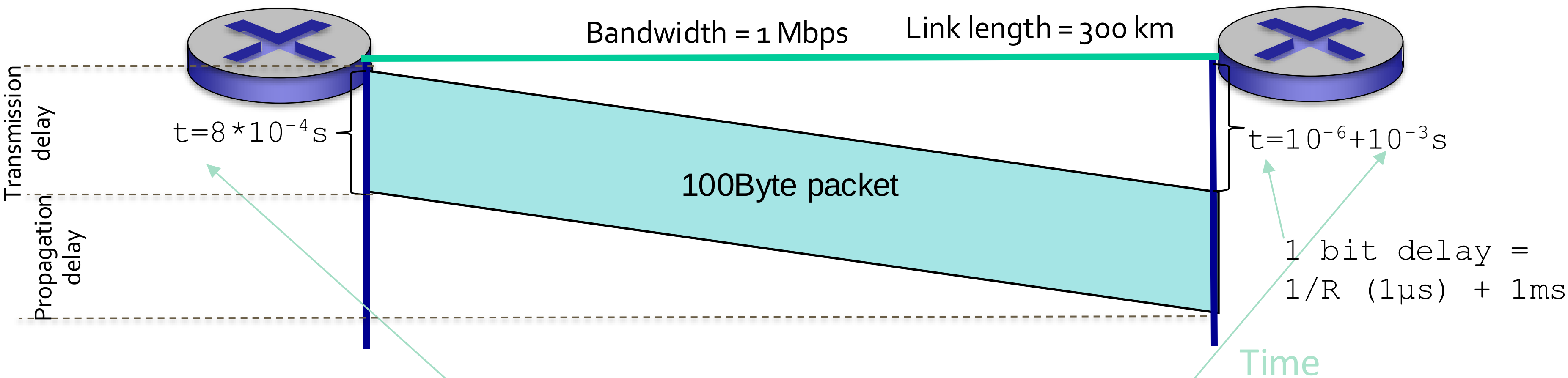




- **Nodal Processing Delay**: The time required to examine the packet's header and determine where to direct the packet
- **Queuing Delay**: The time a packet waits to be transmitted onto the link
- **Transmission Delay**: This time required to push (that is, transmit) all of the packet's bits into the link, L (packet size)/R (bandwidth)
- **Propagation Delay**: The time required to propagate from the beginning to the end of the link.



Recap (Transmission/ propagation Delay)



- Transmission Delay: This time required to push (that is, transmit) all of the packet's bits into the link
  - = L (packet size)/R (bandwidth) --> 100 bytes * (8 bits/1 byte)/ 1 Mbps
    --> 800 bits/ 1 x 10^6 bits/second = $8x10^{-4}$ seconds
    --> 0.8 ms
- Propagation Delay: The time required to propagate from the beginning to the end of the link, bits travel at the speed of light
  - = distance / speed of light --> 300 km/$3x10^8$m/second --> $3x10^5$/$3x10^8$m/s = $1x10^{-3}$ s
    --> 1 ms

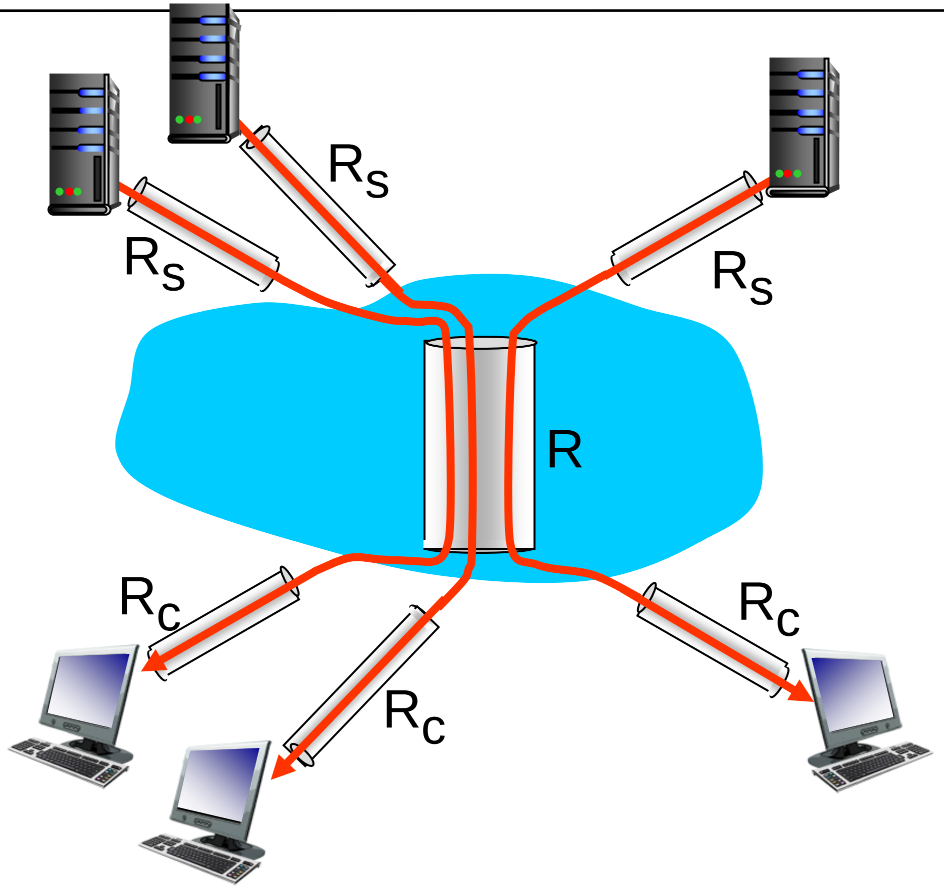
Recap (Throughput: Internet scenario)

per-connection end-end throughput:

- *min(R_c, R_s, R/10)*

in practice:

- R_c or R_s is often bottleneck

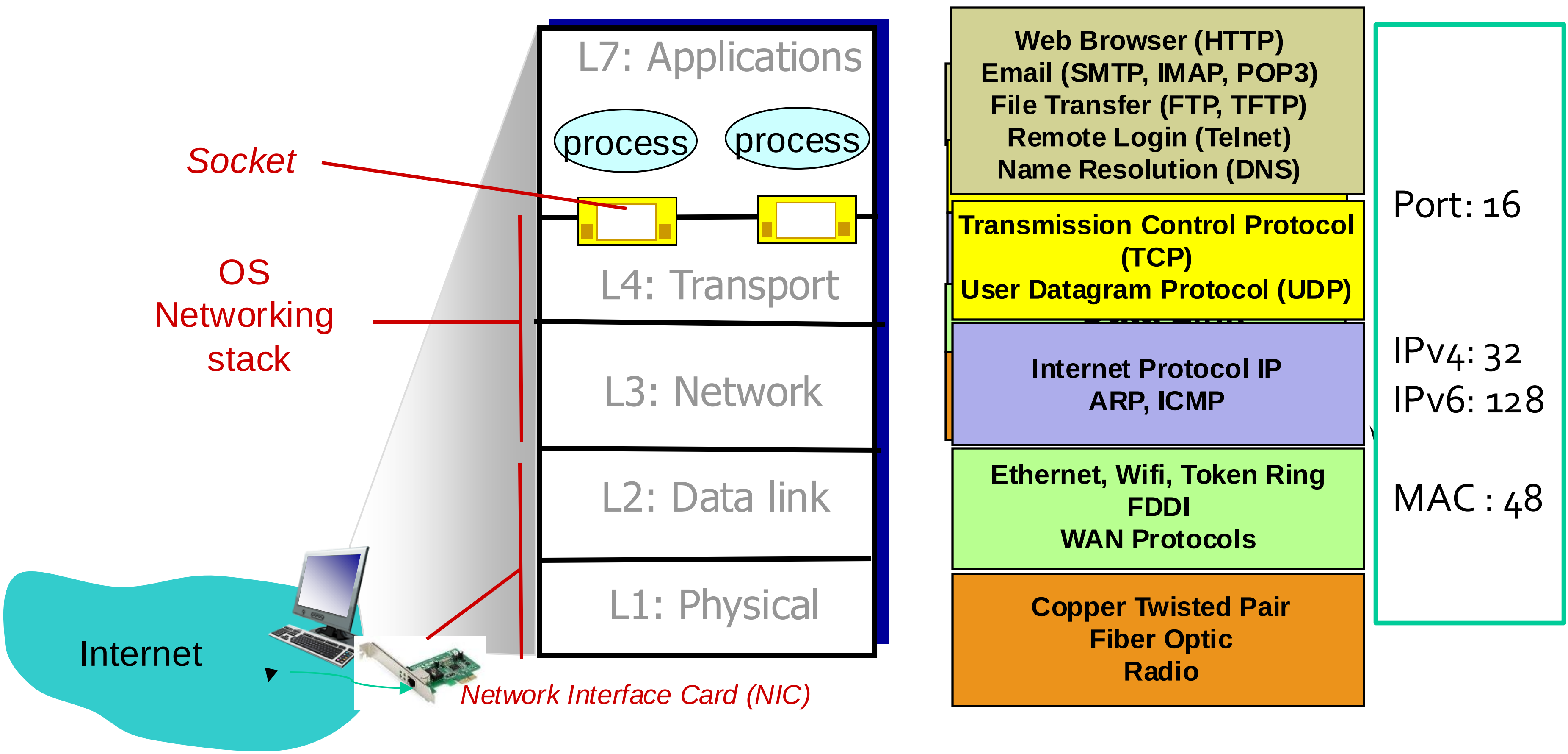


10 connections (fairly) share backbone bottleneck link *R* bits/sec

Topics of today

- The Internet layers and protocol stack
- TCP/IP hybrid model vs OSI reference model
- Layers, services, encapsulation
- Port number (16 bits), IP address (IPv4: 32 or IPv6: 128 bits), and MAC address (48 bits)
- The Internet structure
- The Internet history
- Security concerns

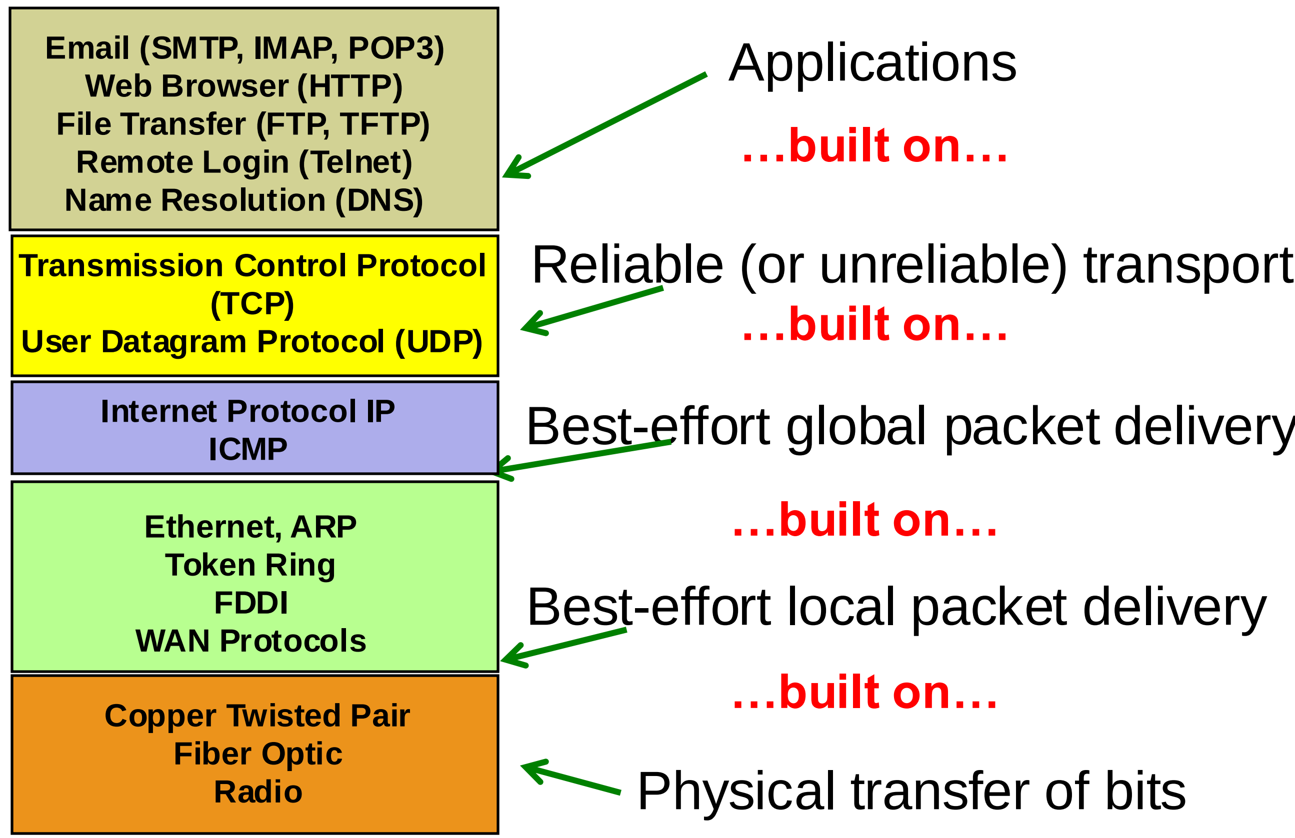
Protocol "Layers" - details



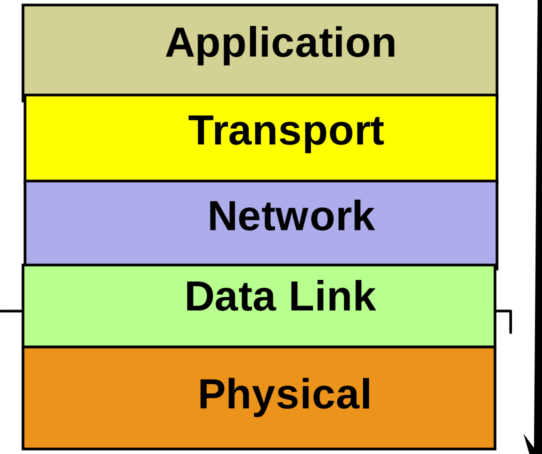
Protocol "layers"

Networks are complex, with many "pieces":

- Applications
- Hosts
- Protocols
- Switches and routers
- Links of various types

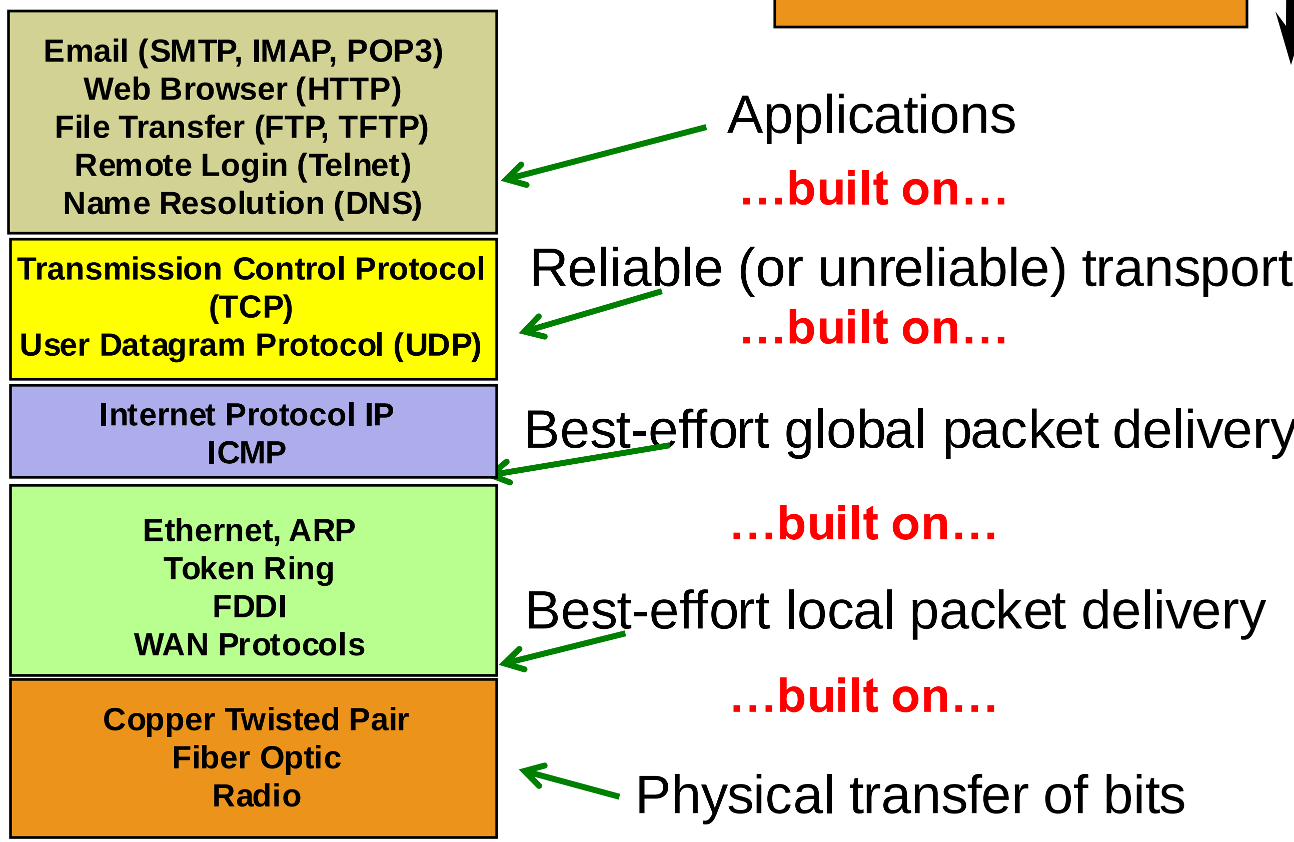


Protocol "layers"



Networks are complex, with many "pieces":

- Applications
- Hosts
- Protocols
- Switches and routers
- Links of various types



Observations

Each layer:

- Depends on layer below
- Supports layer above
- Independent of others

Multiple versions in layer

- Interfaces differ somewhat
- Components pick which lower-level protocol to use

Layering is crucial to Internet's success

- Reuse
- Hides underlying details
- Innovation at each level can proceed in parallel
- Pursued by very different communities

Layers are simple if only on a single machine

- Just stack of modules interacting with those above/below

Need to implement layers across machines

- Host devices (computers, ..) (? layers)
- Routers (? layers), switches (? layers)

Observations

Each layer:

- Depends on layer below
- Supports layer above
- Independent of others

Multiple versions in layer

- Interfaces differ somewhat
- Components pick which lower-level protocol to use

Layering is crucial to Internet's success

- Reuse
- Hides underlying details
- Innovation at each level can proceed in parallel
- Pursued by very different communities

Layers are simple if only on a single machine

- Just stack of modules interacting with those above/below

Need to implement layers across machines

- Hosts (all layers)
- Routers (3 layers), switches (2 layers)

Internet protocol stack

application: protocols to support network applications

- ?

transport: protocols for process-process data transfer

- ?

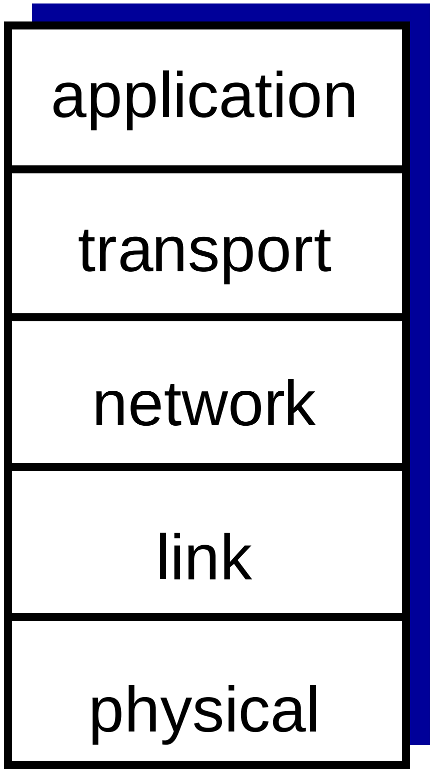
network: routing of datagrams from source to destination

- ?

link: data transfer between neighboring network elements

- ?

physical: bits "on the wire on the air"



Internet protocol stack

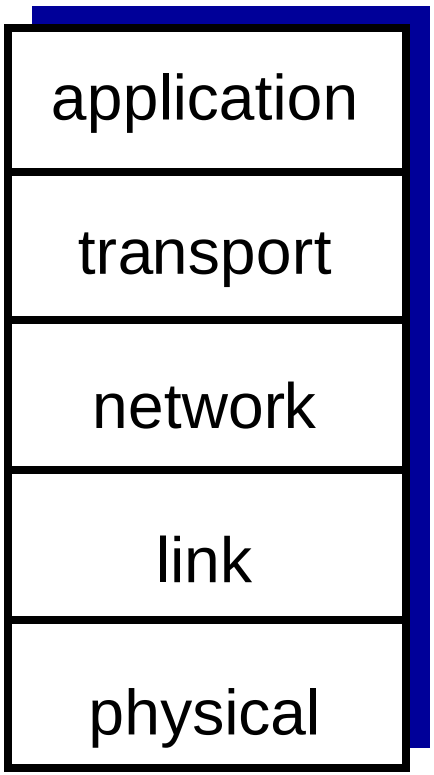
application: supporting network applications
- FTP, SMTP, HTTP

transport: process-process data transfer
- TCP, UDP

network: routing of datagrams from source to destination
- IP, routing protocols

link: data transfer between neighboring network elements
- Ethernet, 802.11 (WiFi)

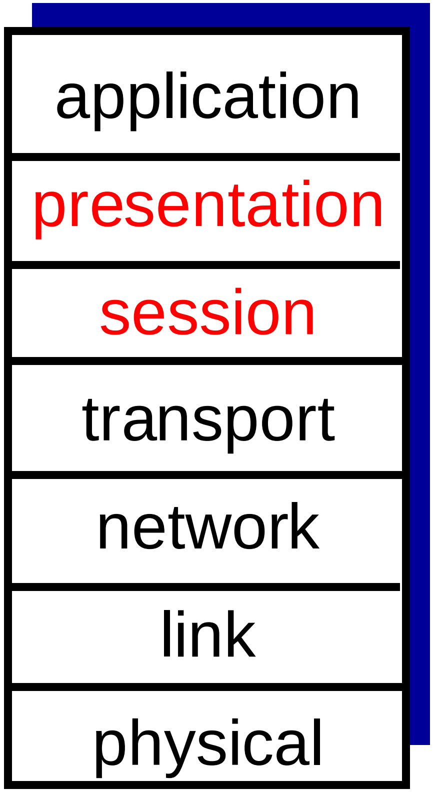
physical: bits “on the wire on the air”



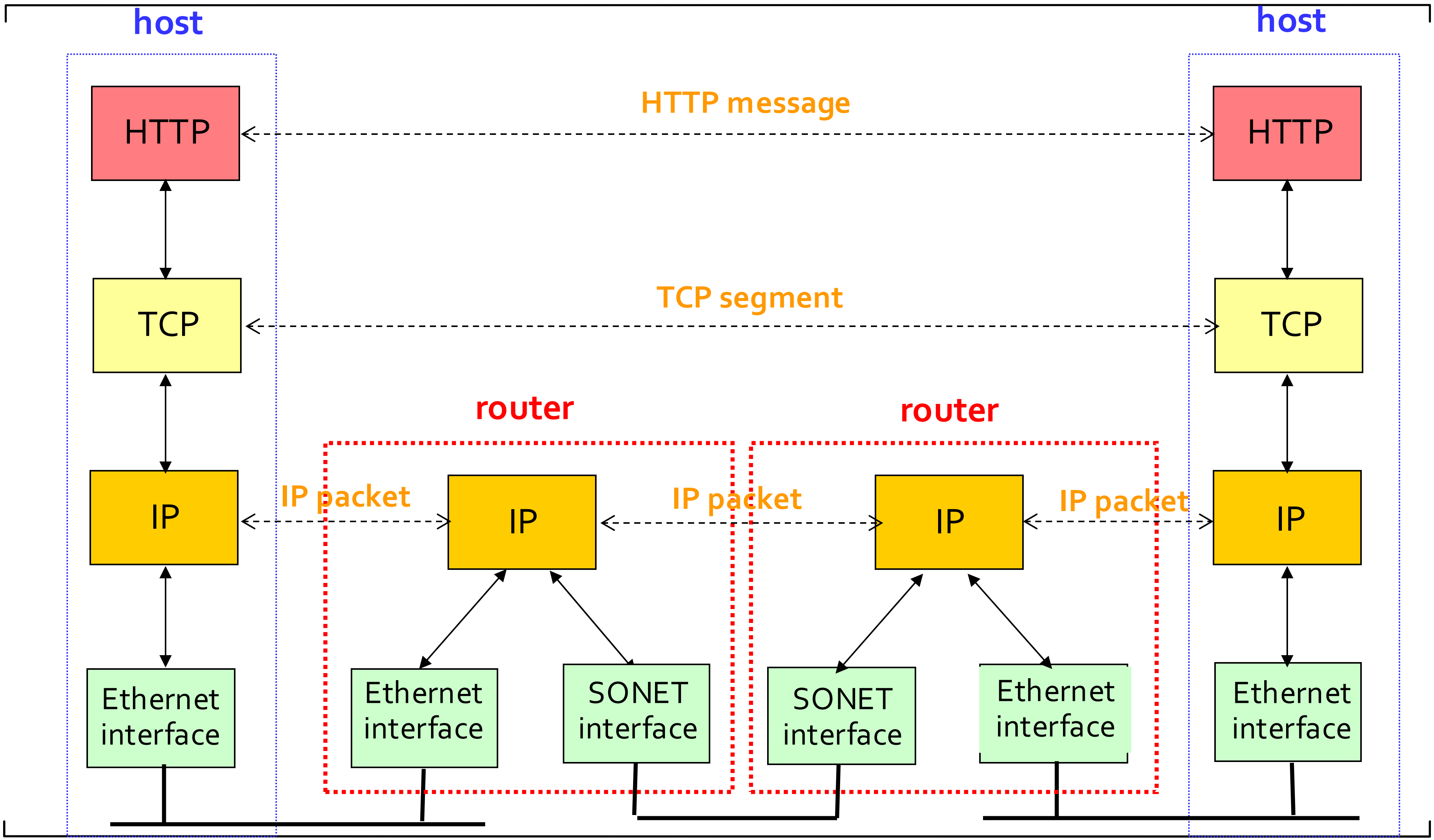
OSI reference model

presentation: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions

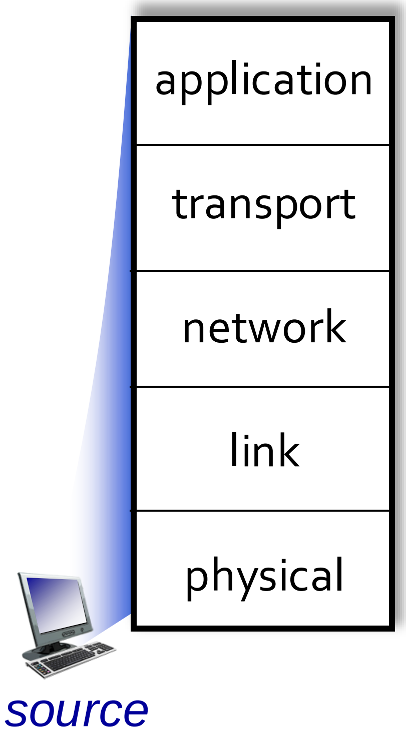
session: synchronization, checkpointing, recovery of data exchange



Network diagram



Services, Layering and Encapsulation



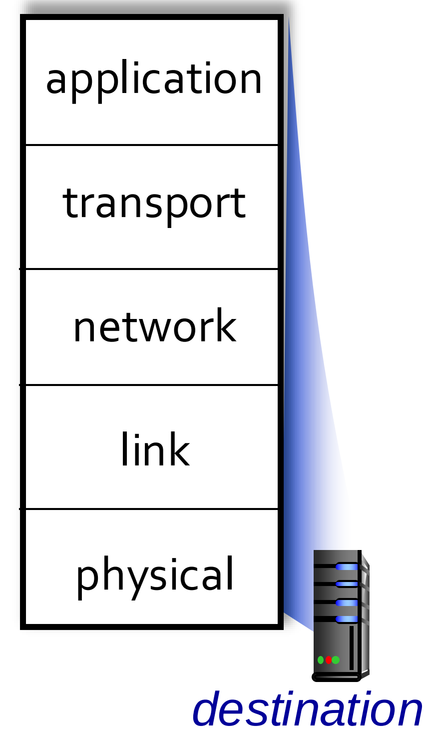
M

Application exchanges .... to implement some application service using *services* of transport layer

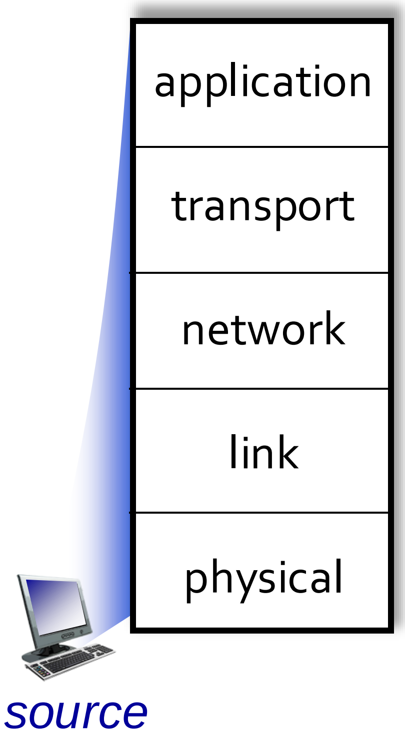
H_t M

Transport-layer protocol transfers M (e.g., reliably) from one *process* to another, using services of network layer

- transport-layer protocol encapsulates application-layer message, M, with *transport* layer-layer header H_t to create a transport-layer ....
  - H_t used by transport layer protocol to implement its service



Services, Layering and Encapsulation



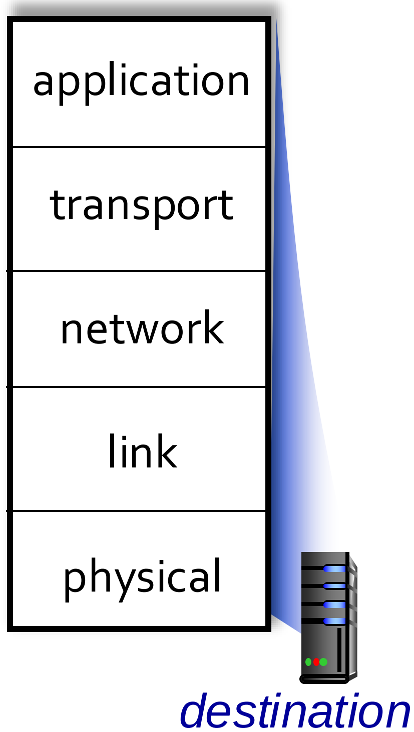
M

Application exchanges messages to implement some application service using *services* of transport layer

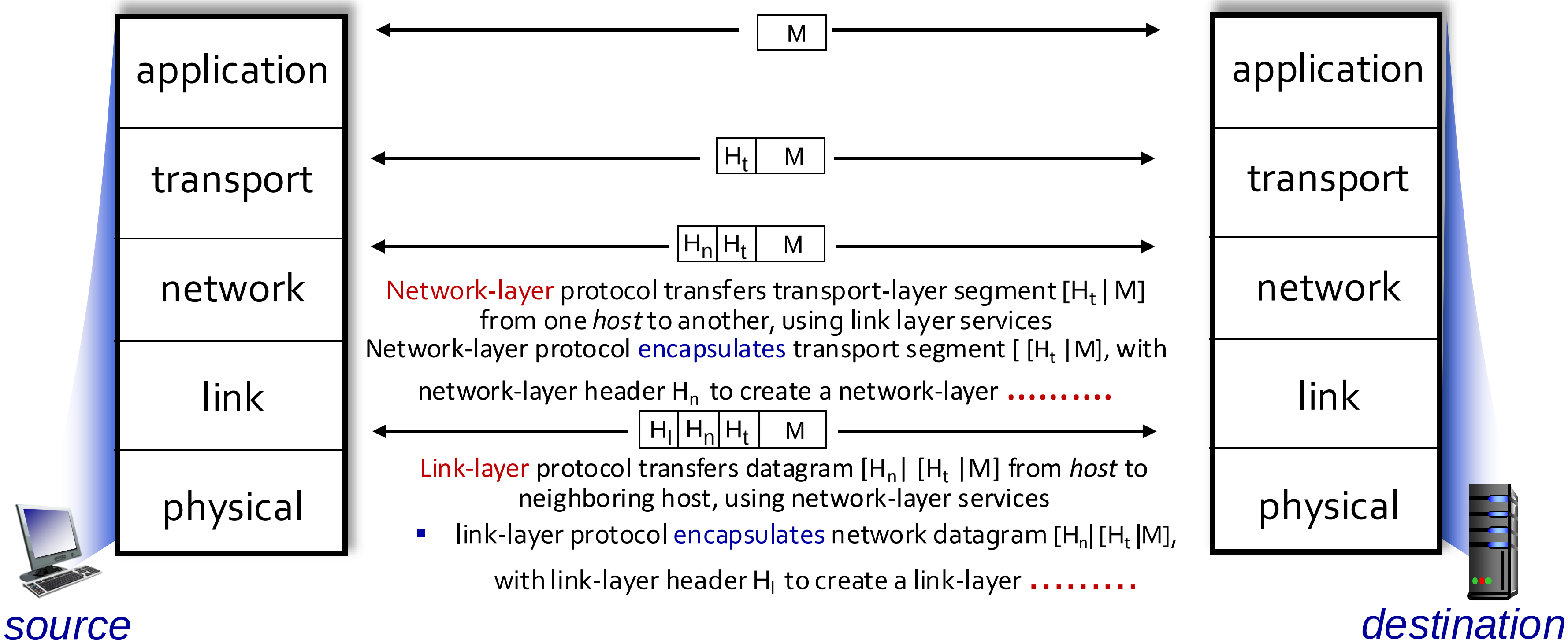
H_t M

Transport-layer protocol transfers M (e.g., reliably) from one *process* to another, using services of network layer

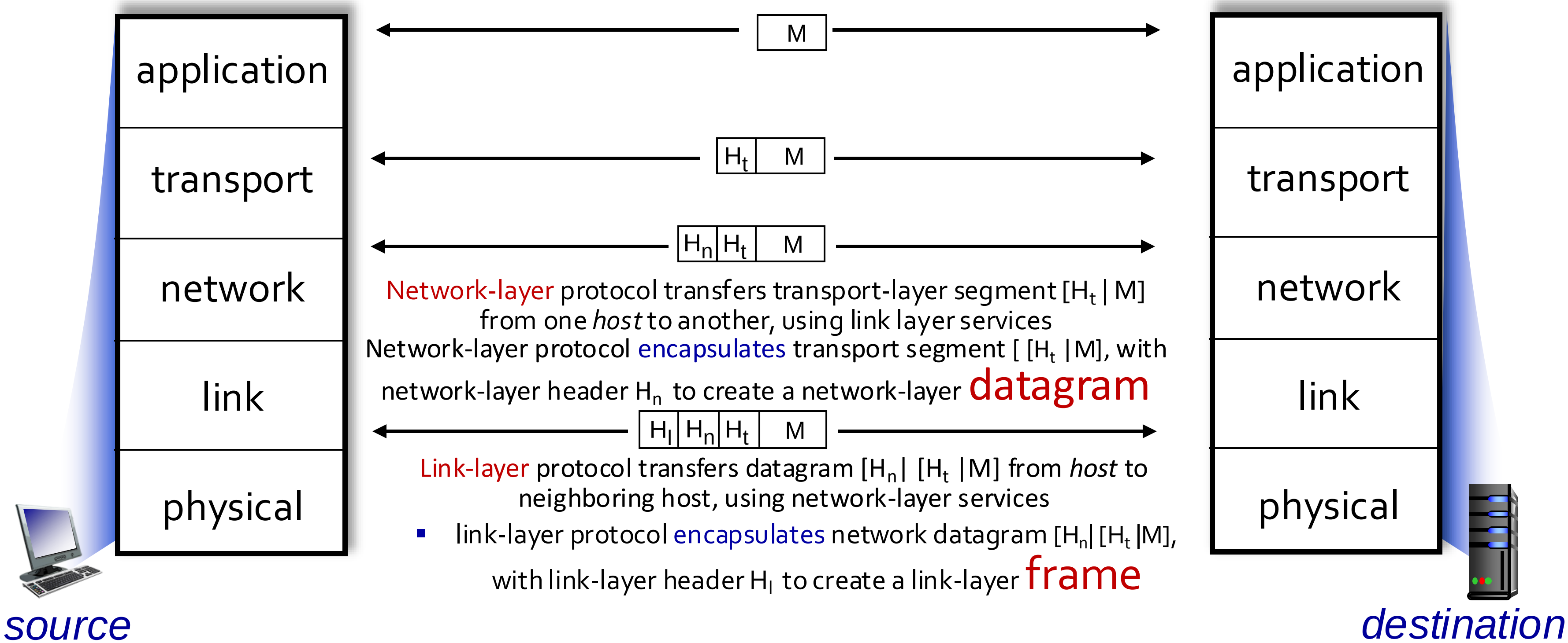
- transport-layer protocol encapsulates application-layer message, M, with *transport* layer-layer header H_t to create a transport-layer segment
  - H_t used by transport layer protocol to implement its service



Services, Layering and Encapsulation



Services, Layering and Encapsulation



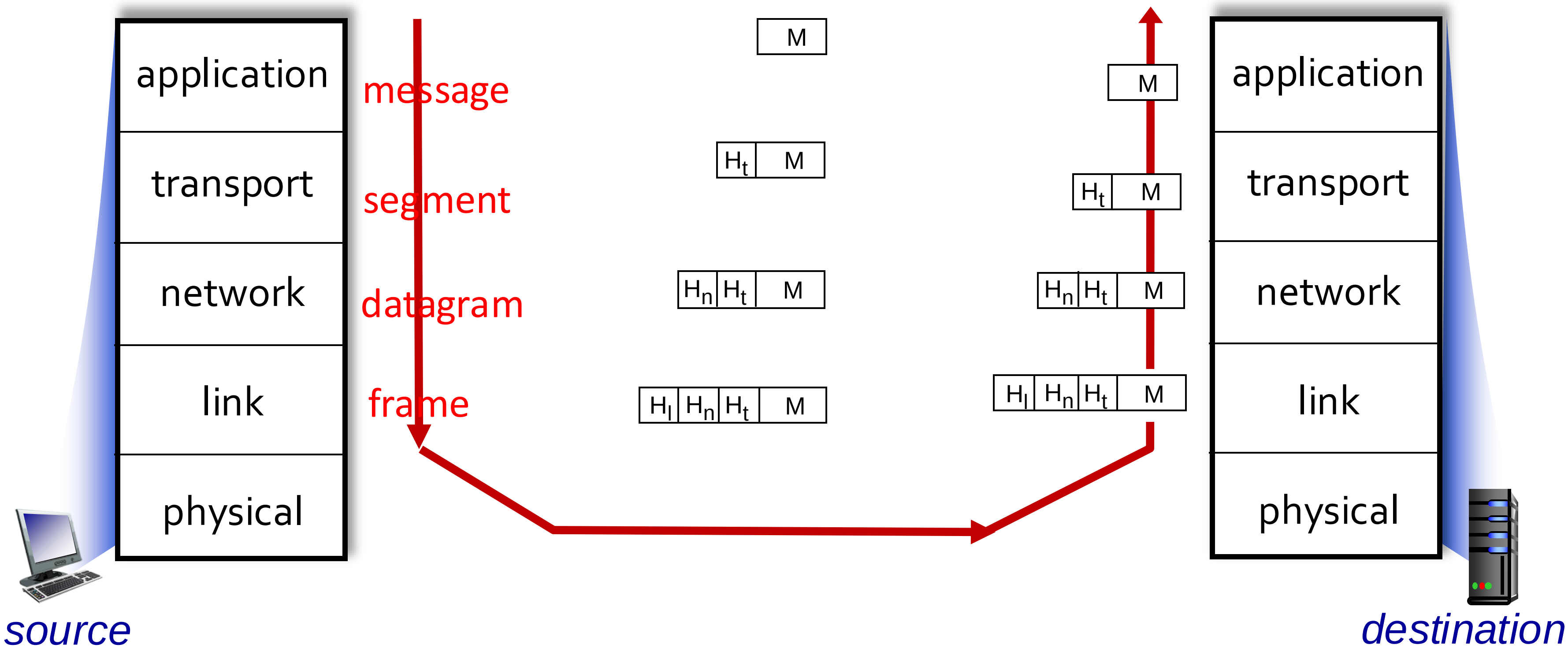
Network-layer protocol transfers transport-layer segment [H_t | M] from one *host* to another, using link layer services

Network-layer protocol encapsulates transport segment [[H_t |M], with network-layer header H_n to create a network-layer **datagram**

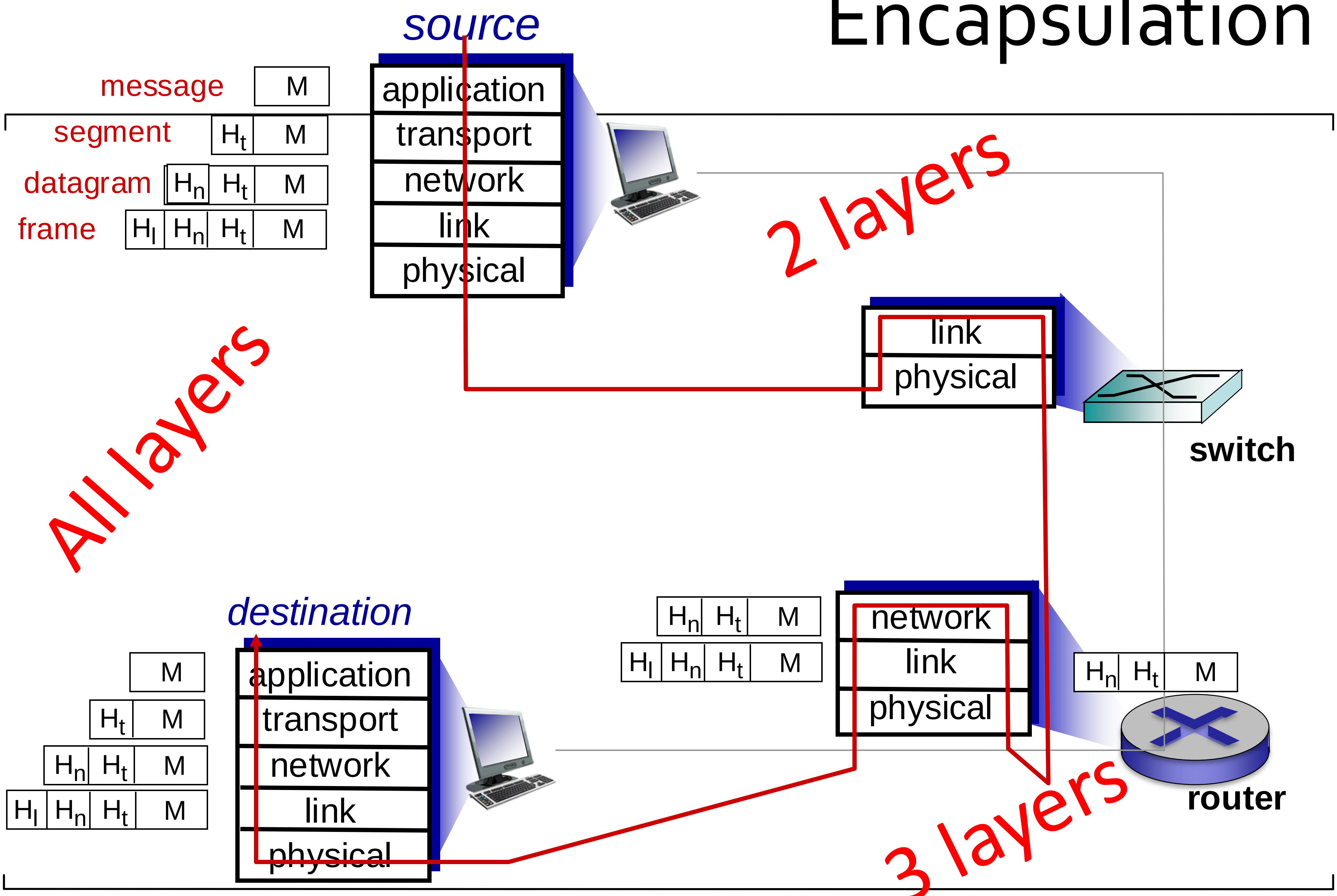
Link-layer protocol transfers datagram [H_n| [H_t |M] from *host* to neighboring host, using network-layer services

- link-layer protocol encapsulates network datagram [H_n| [H_t |M], with link-layer header H_l to create a link-layer **frame**

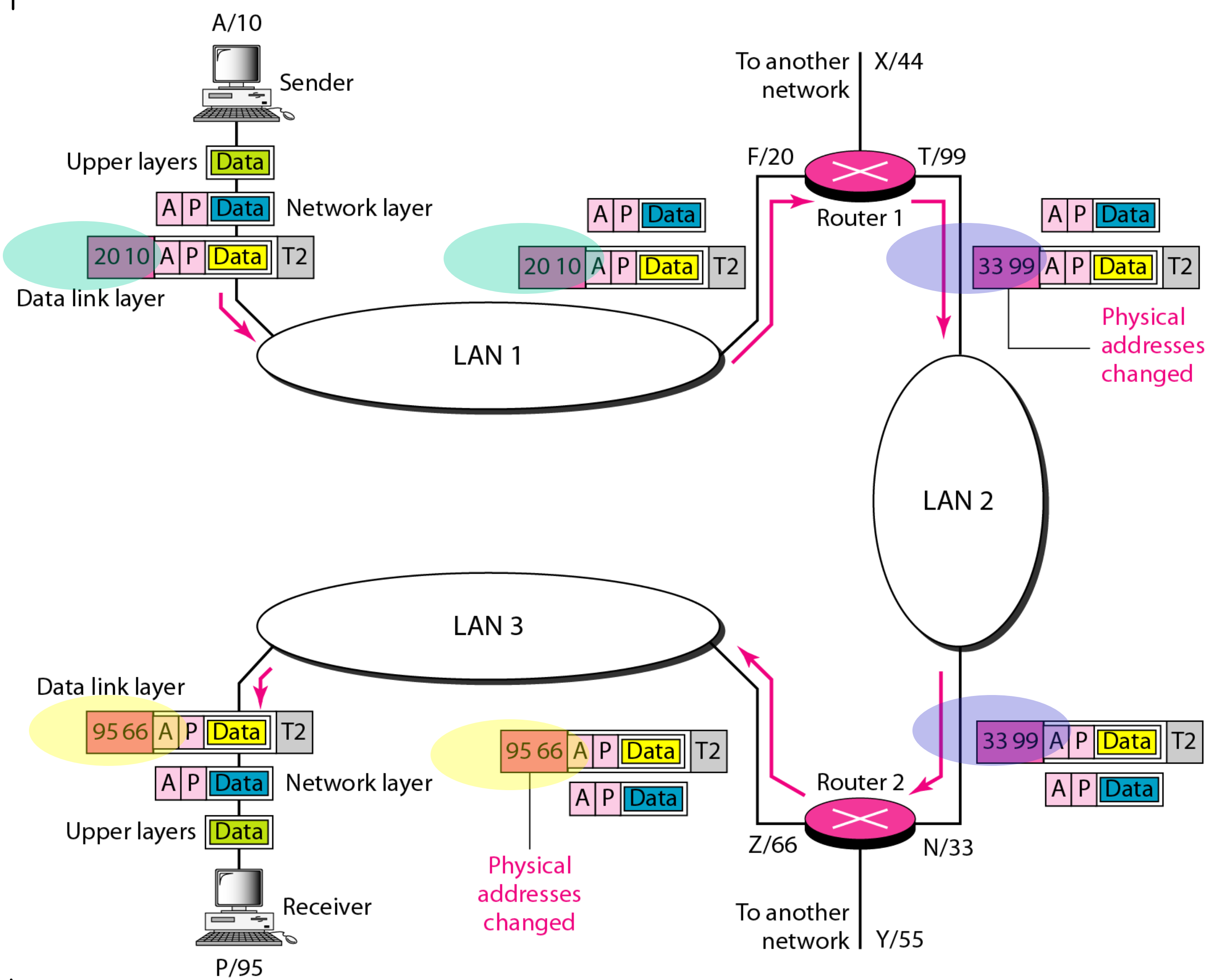
Services, Layering and Encapsulation



Encapsulation



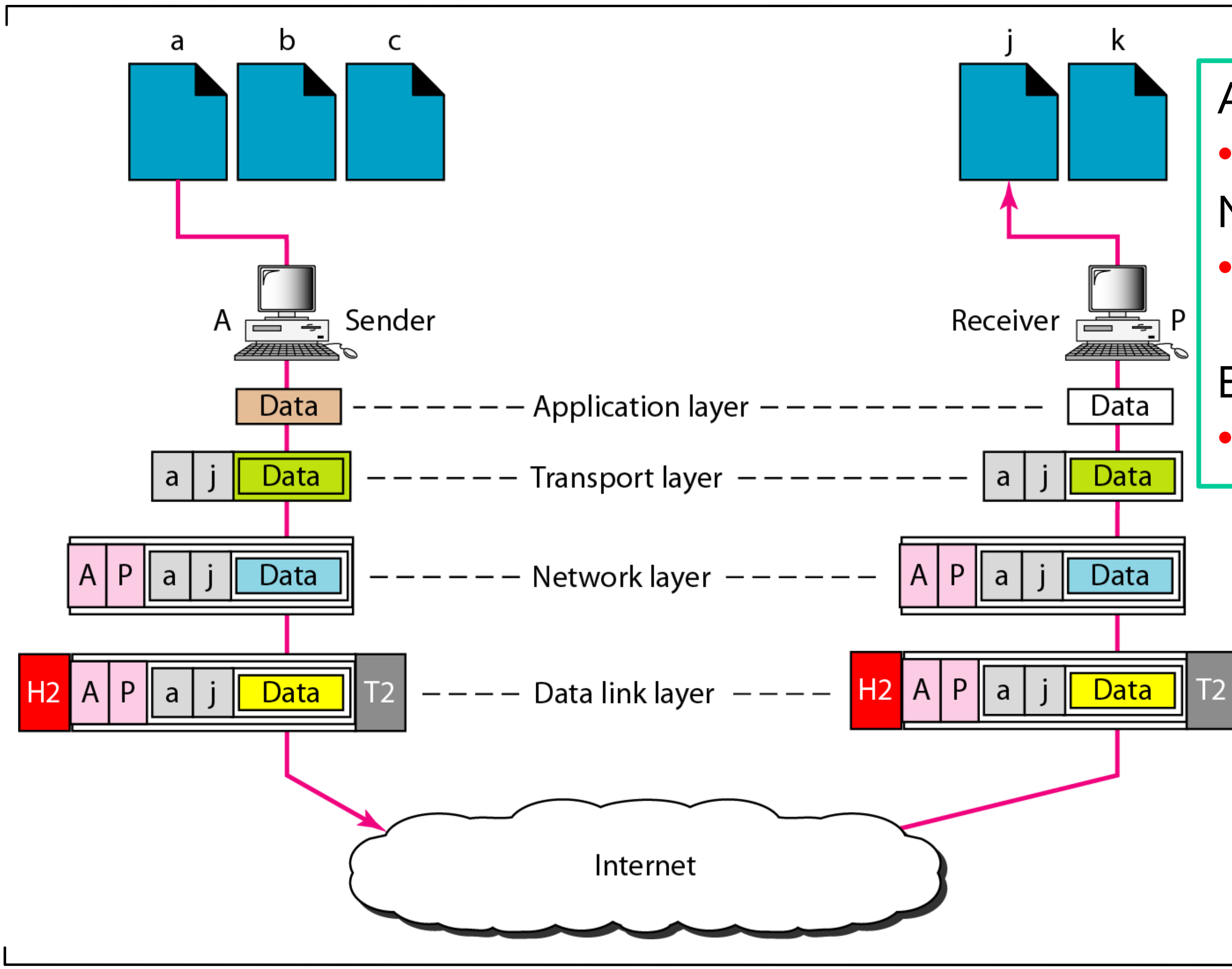
IP addresses



Communication:

- Between nodes
- Segment, Datagram, and Frame units
- Port, IP, and MAC addresses
- Encryption, Data flow, and Error control

Port, IP, and MAC addresses



Application:
- Port: 16 bits

Network
- IP: 32 (IPv4) or 128 (IPv6) - bits

Ethernet or Wifi:
- MAC : 48 bit

Internet structure

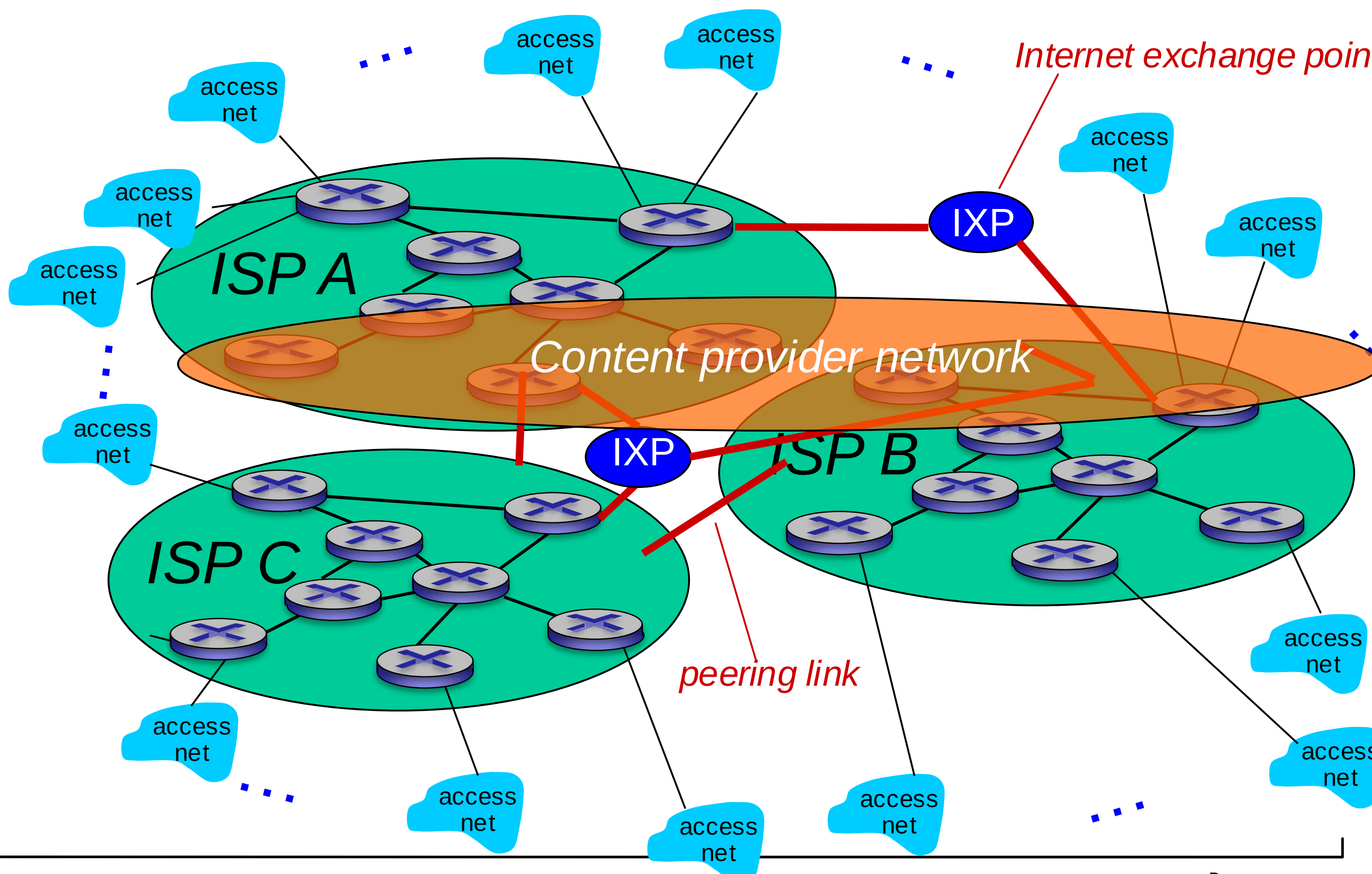
hosts connect to Internet via access Internet Service Providers (ISPs)

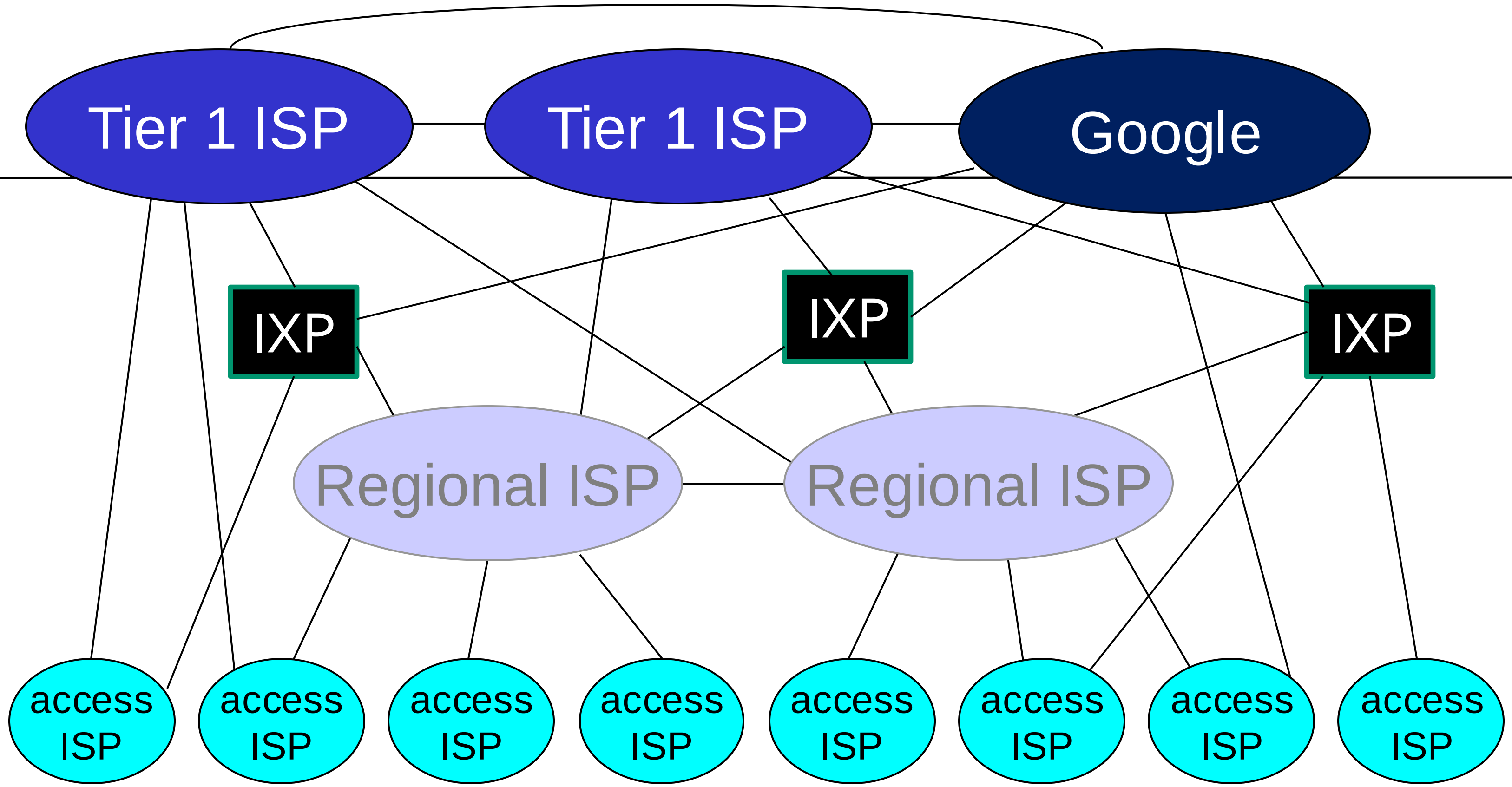
access ISPs interconnected

so that *any* two hosts *(anywhere!)* can send packets to each other

resulting network of networks is very complex

evolution driven by economics, national policies

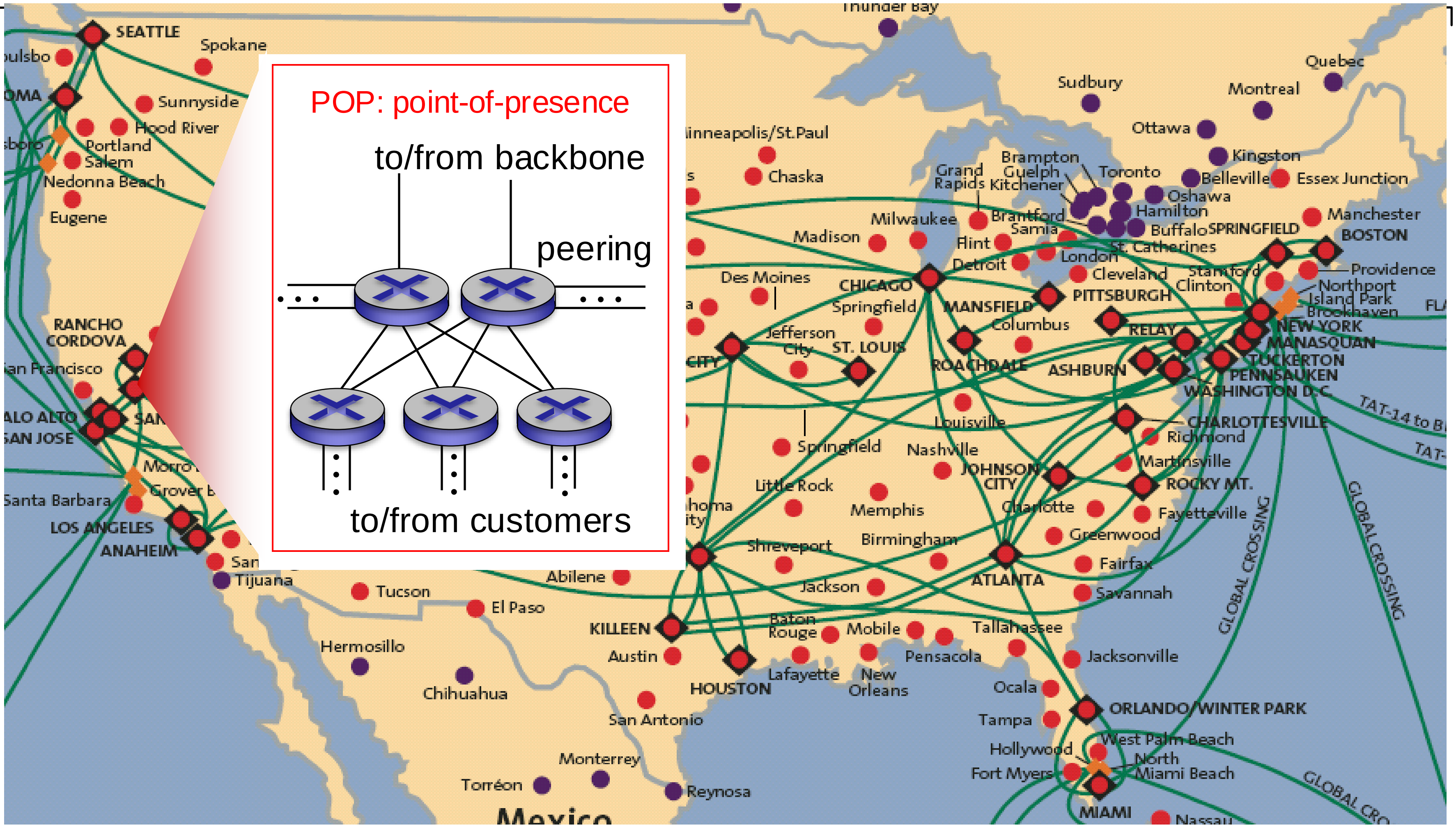




at center: small # of well-connected large networks

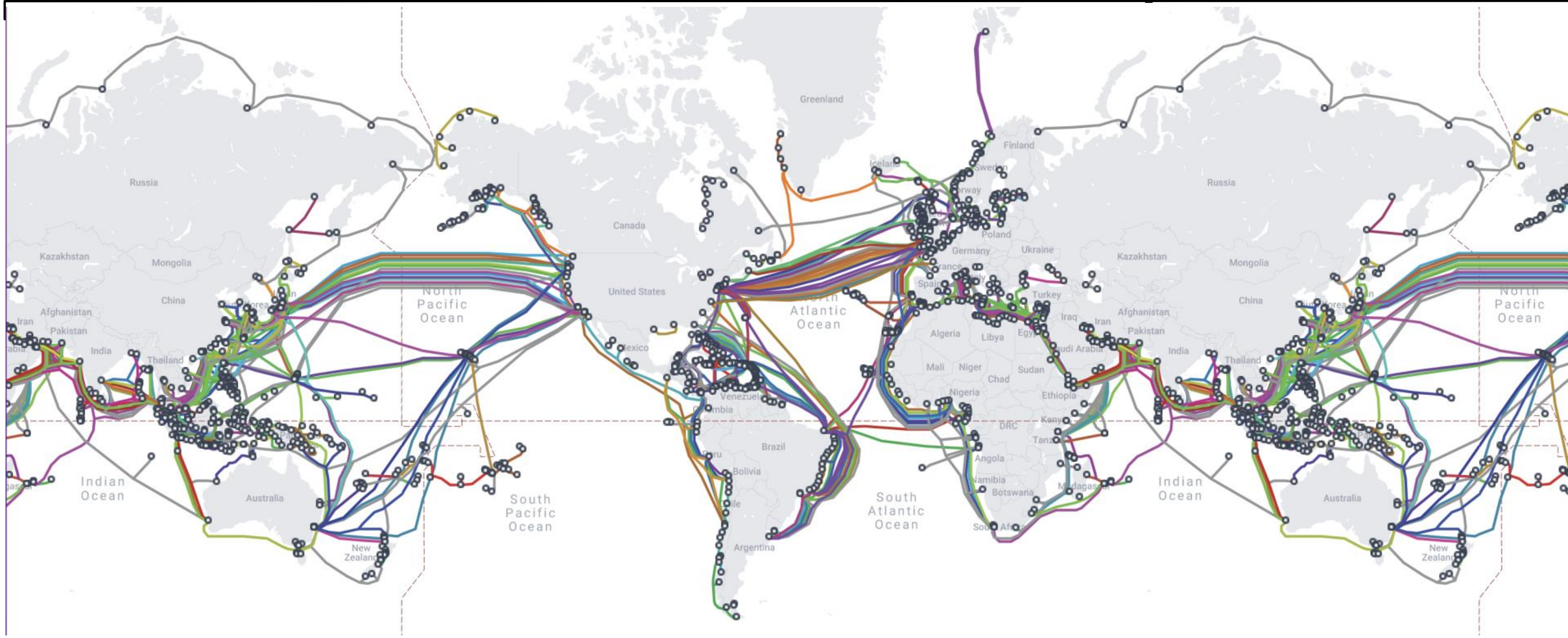
- "tier-1" commercial ISPs (e.g. Sprint, AT&T), national & international coverage
- content provider network (e.g., Google): private network that connects it data centers to Internet, often bypassing tier-1, regional ISPs

Tier – 1 ISP: e.g. Sprint



https://www.youtube.com/watch?v=kHA-Mtkuzno

World Submarine Cable Map



https://www.submarinecablemap.com

https://www.internetexchangemap.com

https://www.amlight.net/?p=119#

Internet history

1961-1972: Early packet-switching principles

1961: Kleinrock - queueing theory shows effectiveness of packet-switching

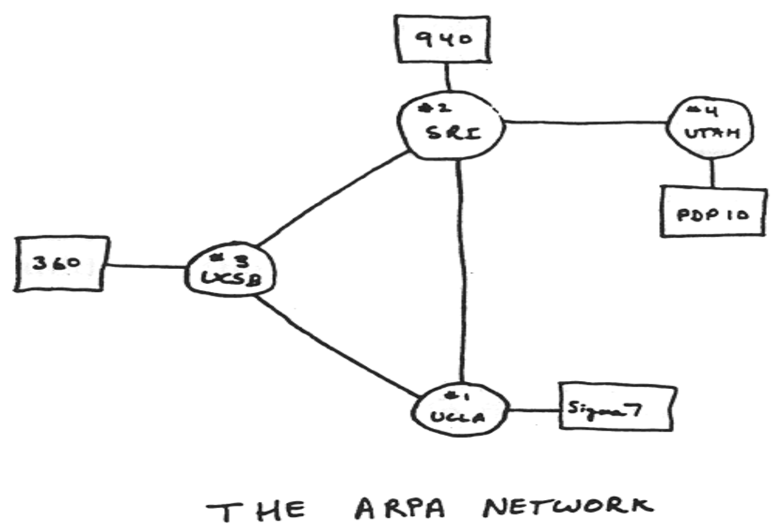
1964: Baran - packet-switching in military nets

1967: ARPAnet conceived by Advanced Research Projects Agency

1969: first ARPAnet node operational

1972:

- ARPAnet public demo
- NCP (Network Control Protocol) first host-host protocol
- first e-mail program



Internet history

1972-1980: Internetworking, new and proprietary nets

1970: ALOHAnet satellite network in Hawaii

1974: Cerf and Kahn - architecture for interconnecting networks

1976: Ethernet at Xerox PARC

late70's: proprietary architectures: DECnet, SNA, XNA

late 70's: switching fixed length packets (ATM precursor)

1979: ARPAnet has 200 nodes

Cerf and Kahn's internetworking principles:

- autonomy - no internal changes required to interconnect networks
- best effort service model
- decentralized control

define today's Internet architecture

Internet history

1980-2000: new protocols, a proliferation of networks, the web

1983: deployment of TCP/IP

1982: smtp e-mail protocol defined

1983: DNS defined for name-to-IP-address translation

1985: ftp protocol defined

1988: TCP congestion control

early 1990's: ARPAnet decommissioned

1991: NSF lifts restrictions on commercial use of NSFnet (decommissioned, 1995)

early 1990s: Web

- hypertext [Bush 1945, Nelson 1960's]
- HTML, HTTP: Berners-Lee
- 1994: Mosaic, later Netscape
- late 1990's: commercialization of the Web

late 1990's – 2000's:

- instant messaging, P2P file sharing
- network security to forefront
- ~ 50 million host, 100 million+ users
- backbone links running at Gbps

Internet history

2005-present

~5B devices attached to Internet (2016)

- smartphones and tablets

aggressive deployment of broadband access

increasing ubiquity of high-speed wireless access

emergence of online social networks:

- Facebook

service providers (Google, Microsoft) create their own networks

- bypass Internet, providing "instantaneous" access to search, video content, email, etc.

e-commerce, universities, enterprises running their services in "cloud" (e.g., Amazon)

Big concern: security

field of network security:

- possible to attack computer networks
- how to design architectures that are immune to attacks

Internet not originally designed with (much) security in mind

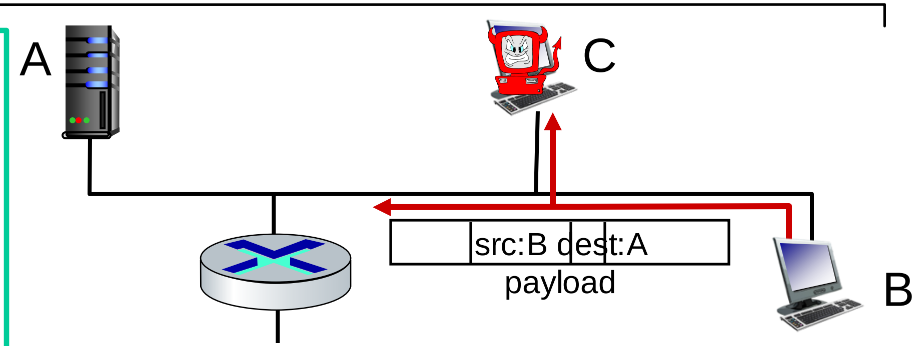
- *original vision:* "a group of mutually trusting users attached to a transparent network" ☺

We now need to think about:

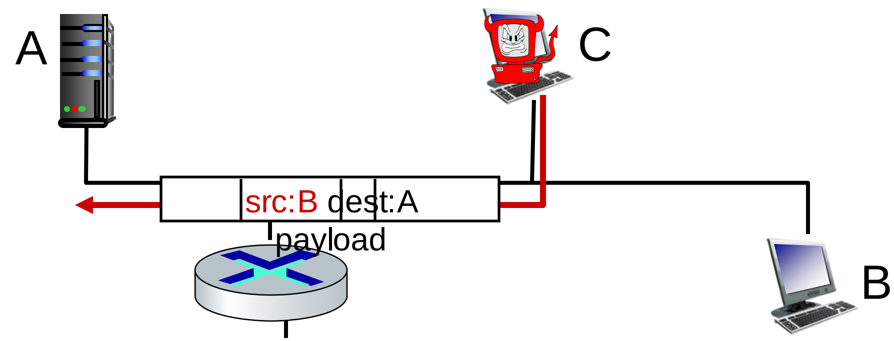
- how bad guys can attack computer networks
- how we can defend networks against attacks
- how to design architectures that are immune to attacks

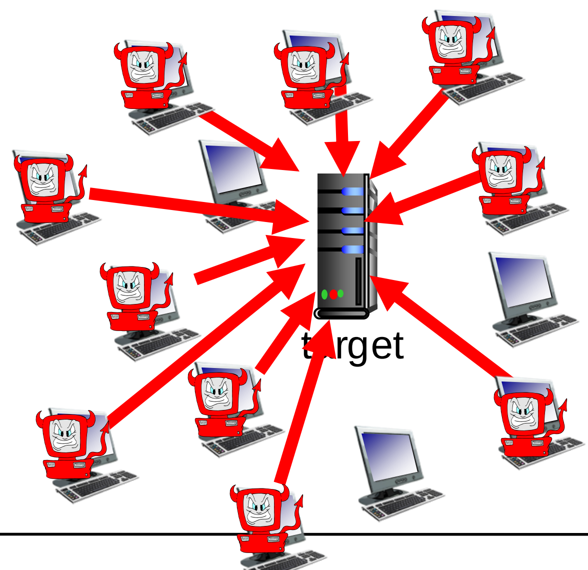
Packet interception, Fake identity, DOS

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



IP spoofing: injection of packet with false source address





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

Lines of defense:

- authentication: proving you are who you say you are
  - cellular networks provides hardware identity via SIM card; no such hardware assist in traditional Internet
- confidentiality: via encryption
- integrity checks: digital signatures prevent/detect tampering
- access restrictions: password-protected VPNs
- firewalls: specialized “middleboxes” in access and core networks:
  - off-by-default: filter incoming packets to restrict senders, receivers, applications
  - detecting/reacting to DOS attacks

Summary

Today:

- Protocol layers
- Internet protocol stack: TCP/IP and OSI service models
- Network diagram, IP addresses, Port addresses
- The Internet structure and history
- Security, a big concern

Camino discussion:

- Reflection
- Exit ticket

Next time:

- read 2.1 and 2.2 of K&R (Application layer, the Web)
- follow on Camino! material and announcements

Any questions?