University of Duisburg-Essen
Networked Embedded Systems Group
Institute for Computer Science and
Business Information Systems (ICB)
Schützenbahn 70
D-45127 Essen, Germany

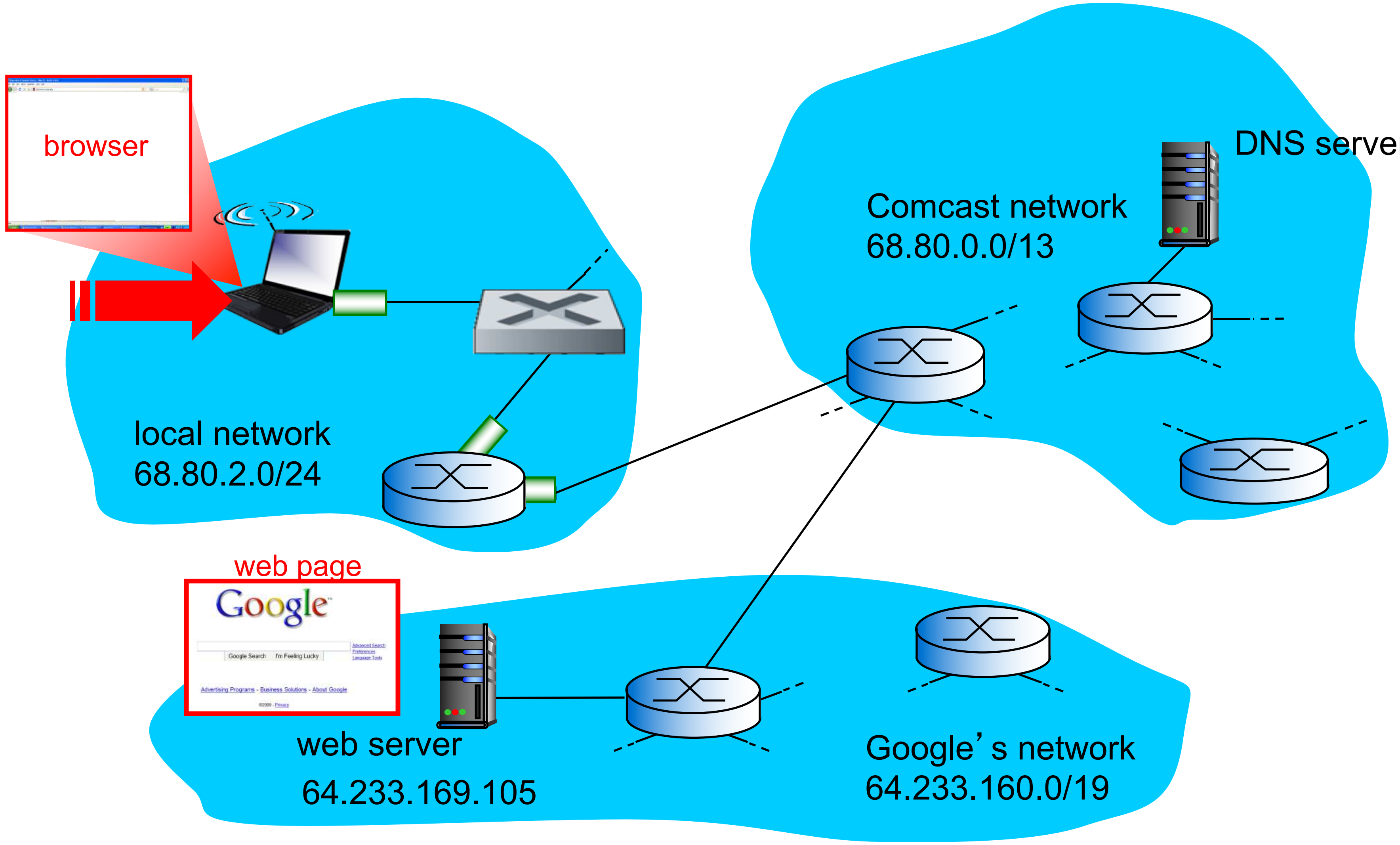
Kommunikationsnetze 2
1 – Introduction

Prof. Dr. Pedro José Marrón

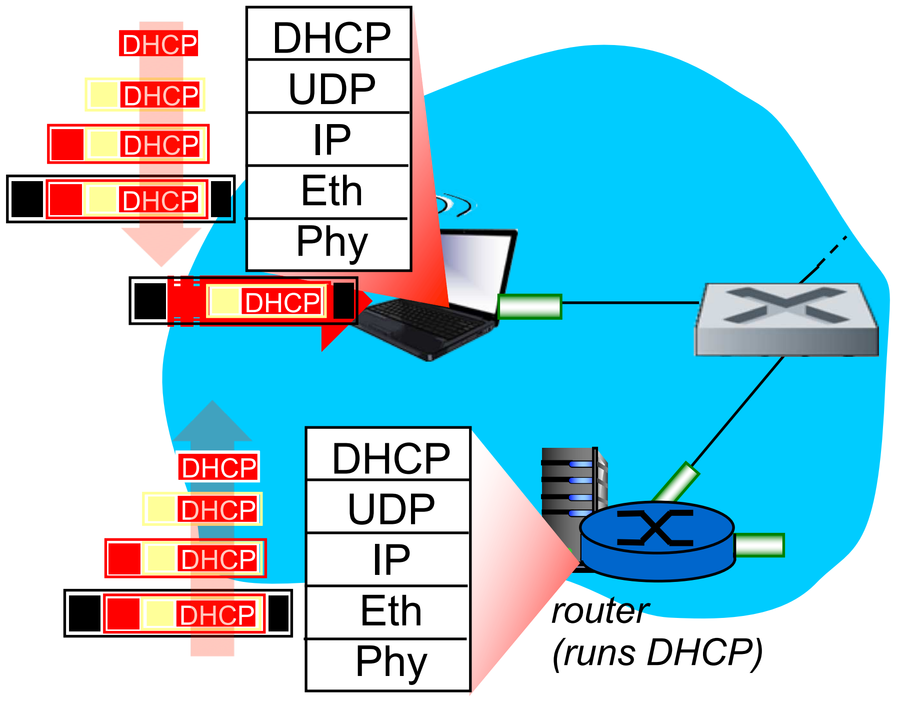
A Day in the Life of a Web Request

What happens when you connect your laptop to a network and request a web page?

A Web Request: Scenario

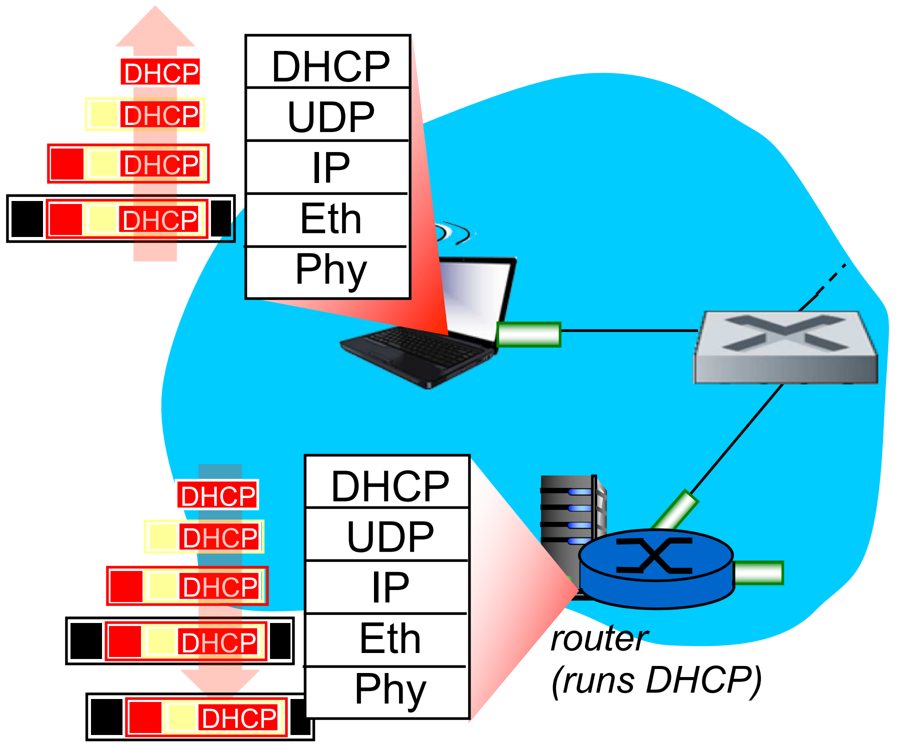


A Web Request: Connecting to the Internet



- Laptop needs to get its own IP address, the address of first-hop router, the address of DNS server: use *DHCP*
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.3 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demuxed to IP demuxed to UDP demuxed to DHCP

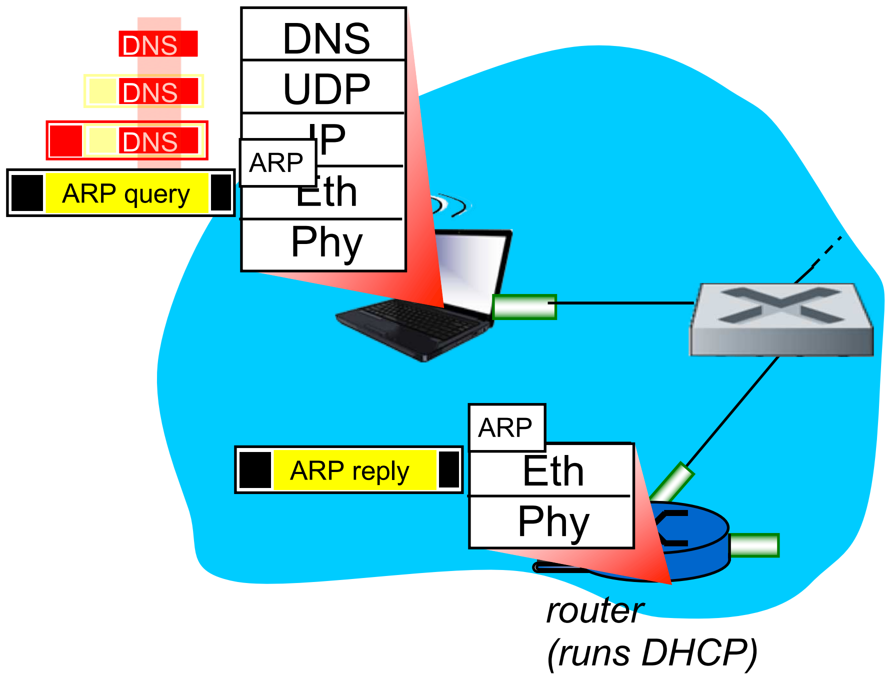
A Web Request: Connecting to the Internet



- DHCP server formulates *DHCP ACK* containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- Encapsulation at DHCP server, frame forwarded (switch learning) through LAN, demultiplexing at client
- DHCP client receives DHCP ACK reply

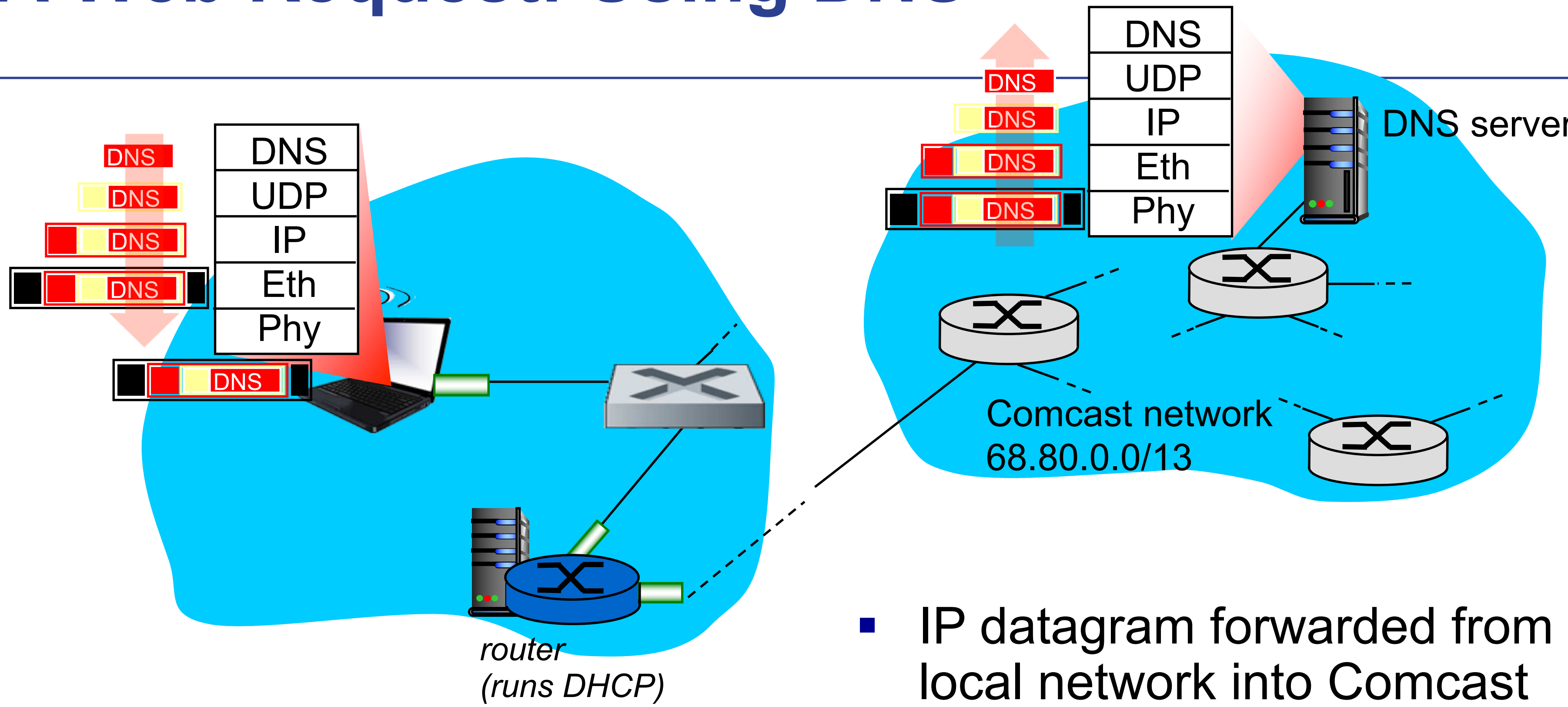
Client now has IP address, knows name & address of DNS server, IP address of its first-hop router

A Web Request: ARP (before DNS, before HTTP)



- Before sending *HTTP* request, the IP address of www.google.com is needed: *DNS*
- DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, MAC address of router interface is needed: ARP
- ARP query is broadcasted, received by router, which replies with ARP reply giving MAC address of router interface
- Client now knows MAC address of first hop router, so can now send frame containing DNS query

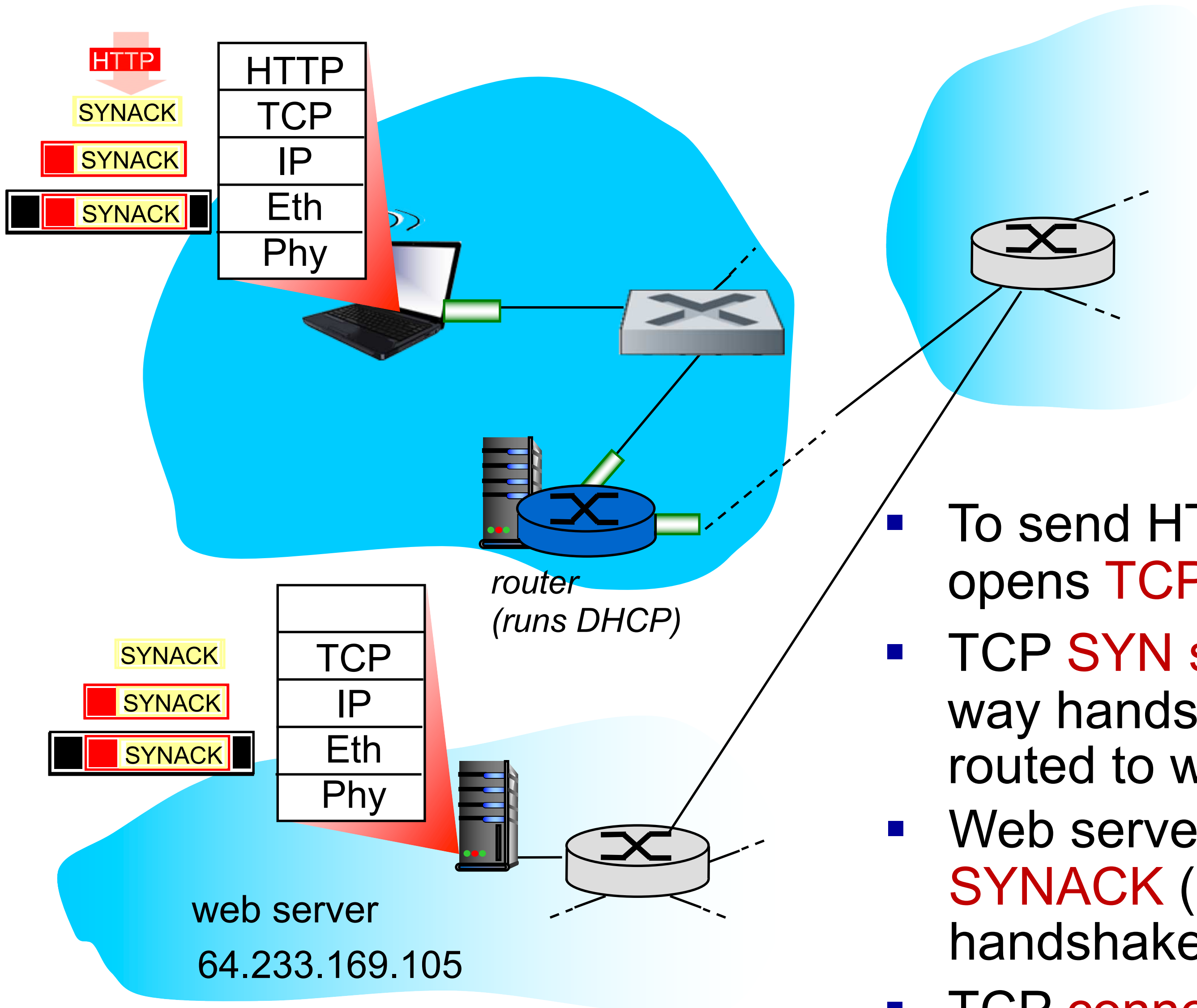
A Web Request: Using DNS



- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router

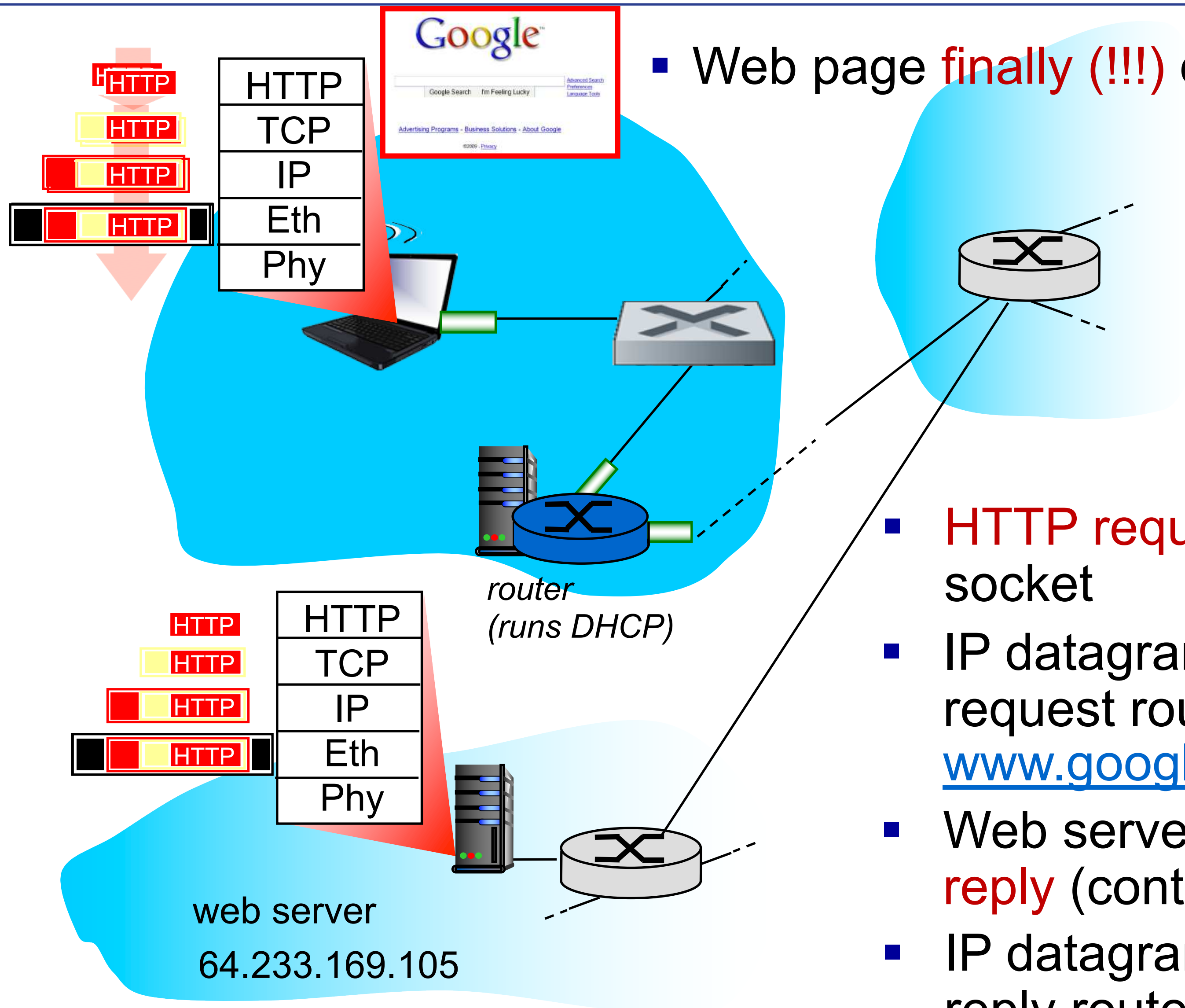
- IP datagram forwarded from local network into Comcast network, routed (tables created by RIP, OSPF, IS-IS and/or BGP routing protocols) to DNS server
- Demuxed to DNS server
- DNS server replies to client with IP address of www.google.com

A Web Request: TCP Connection Carrying HTTP



- To send HTTP request, client first opens TCP socket to web server
- TCP SYN segment (step 1 in 3-way handshake) inter-domain routed to web server
- Web server responds with TCP SYNACK (step 2 in 3-way handshake)
- TCP connection established!

A Web Request: HTTP Request/Reply



- Web page finally (!!!) displayed

- HTTP request sent into TCP socket
- IP datagram containing HTTP request routed to www.google.com
- Web server responds with HTTP reply (containing web page)
- IP datagram containing HTTP reply routed back to client

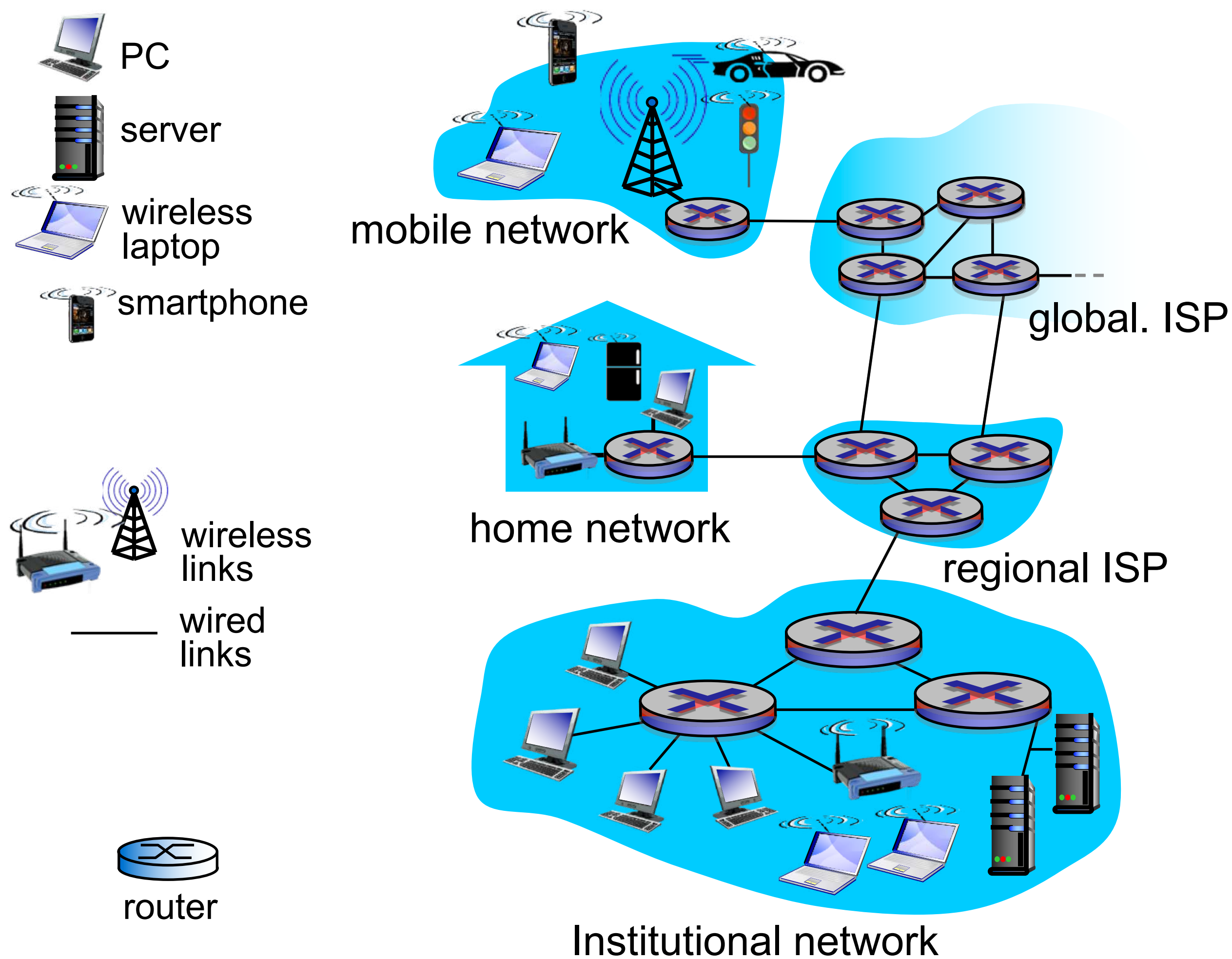
From KN1 to KN2

- In Kommunikationsnetze 2
  - More detailed discussion of concepts introduced in KN1
    - IPv6
    - Routing and Transport Layers
    - Infrastructure Services
  - As well as new concepts
    - Security
    - Wireless
  - And state-of-the-art communication technologies
    - Internet of Things

Let’s start!

What’s the Internet: Devices and Connections

- Billions of connected computing devices
  - hosts = end systems
  - running network apps
- Communication links
  - fiber, copper, radio, satellite
  - transmission rate: bandwidth
- Packet switches forward packets (chunks of data)
  - routers and switches



The Internet of Connected Devices

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

Web-enabled toaster +
weather forecaster

Tweet-a-watt:
monitor energy use

Slingbox: watch,
control cable TV remotely

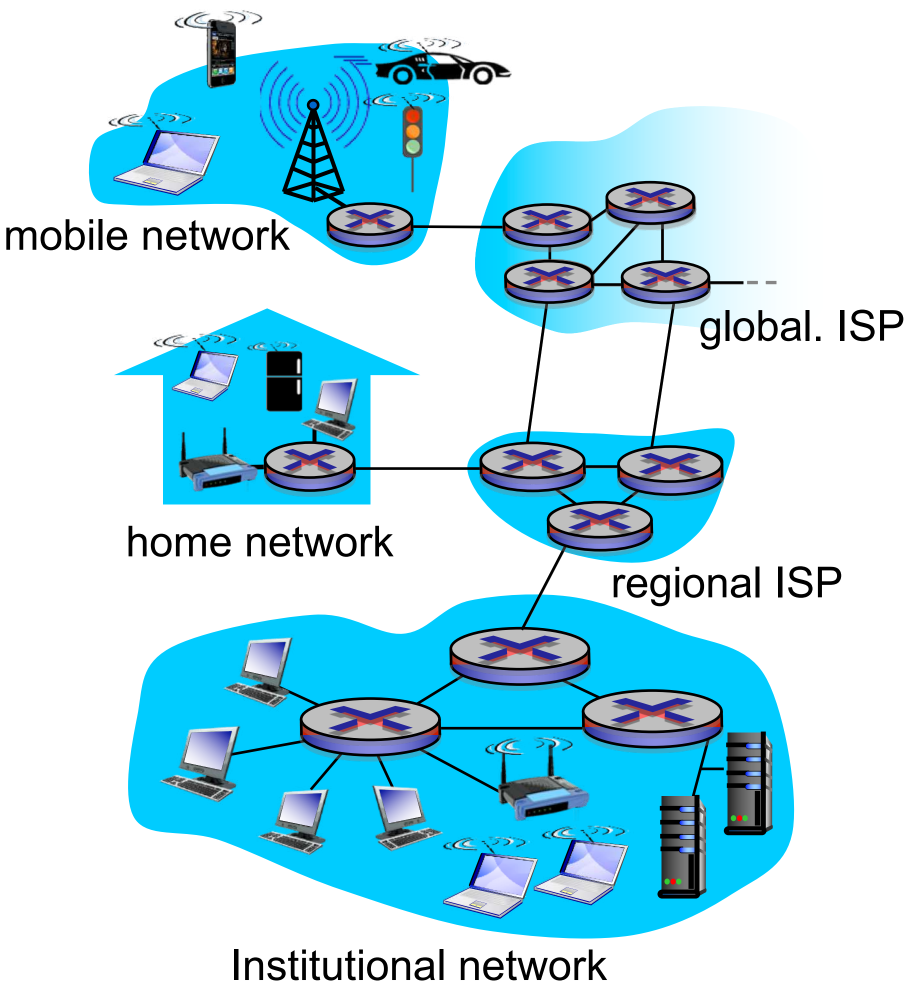
Internet
refrigerator

sensorized,
bed
mattress

Internet phones

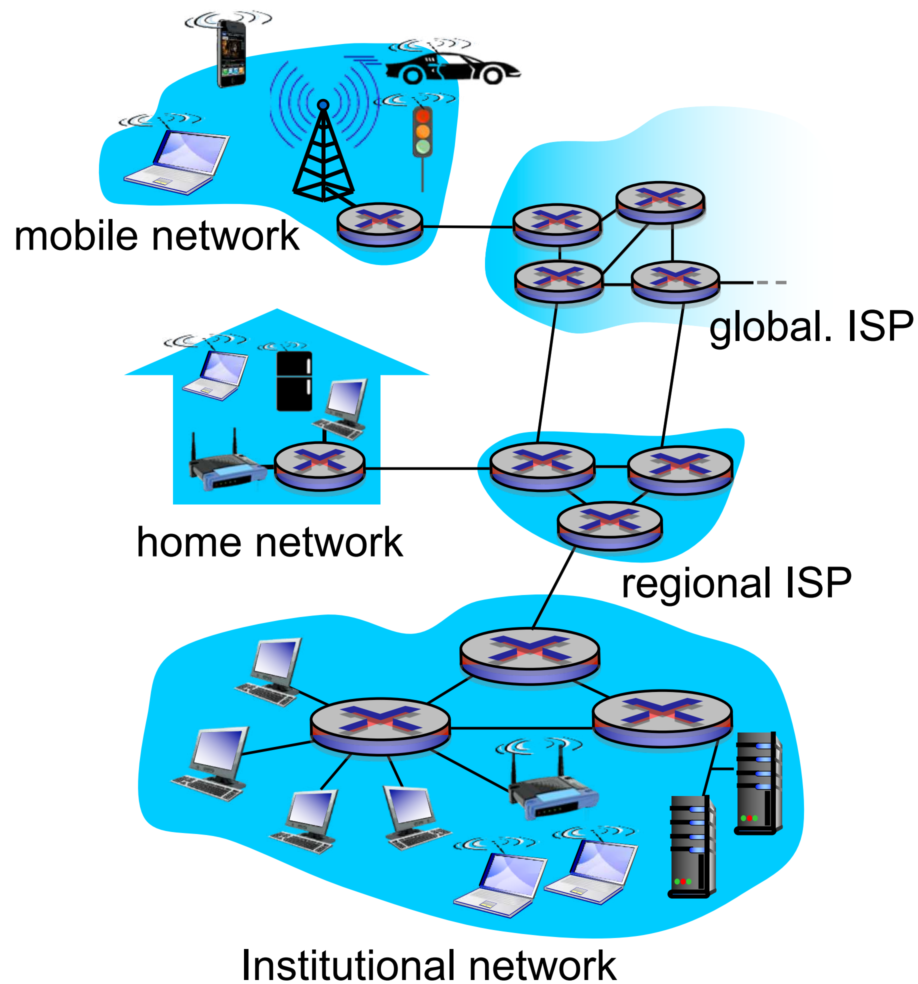
What's the Internet: Networks and Protocols

- Internet: “network of networks”
  - Interconnected ISPs
- Protocols control sending, receiving of messages
  - E.g., TCP, IP, HTTP, Skype, 802.11
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force



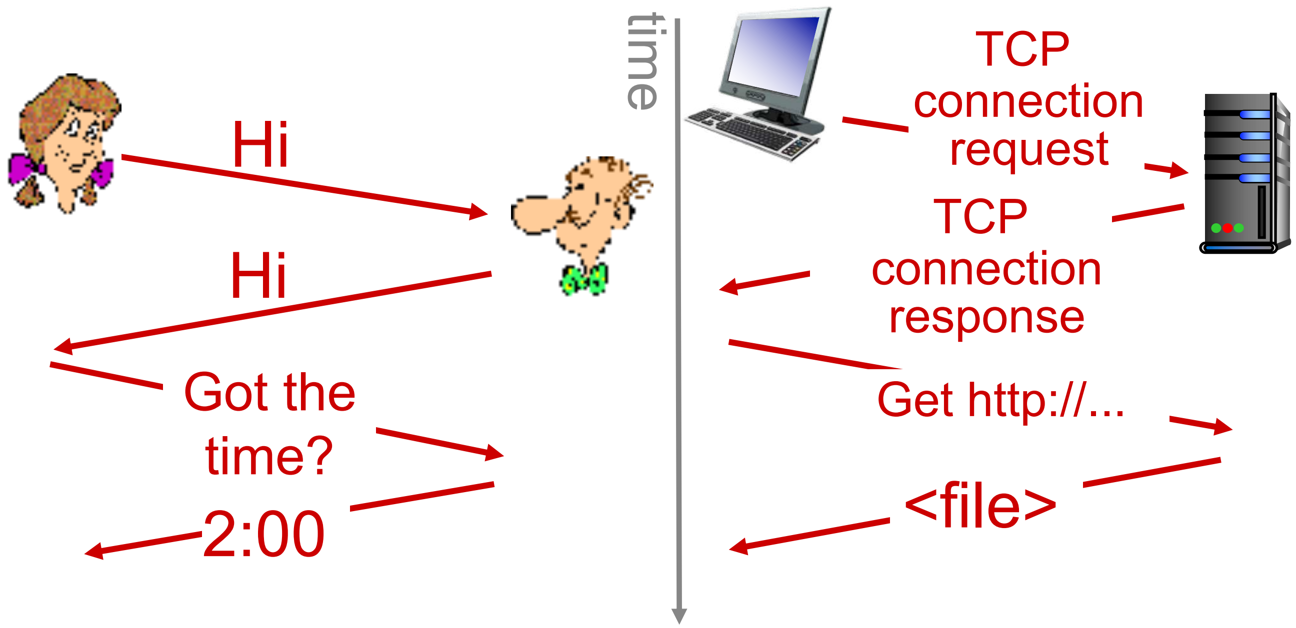
What’s the Internet: Services

- Infrastructure that provides services to applications
  - Web, VoIP, email, games, e-commerce, social networks
- Provides programming interface to applications
  - Hooks that allow sensing and receiving application programs to “connect” to the Internet
  - Service options, analogous to postal service



What’s a Protocol?

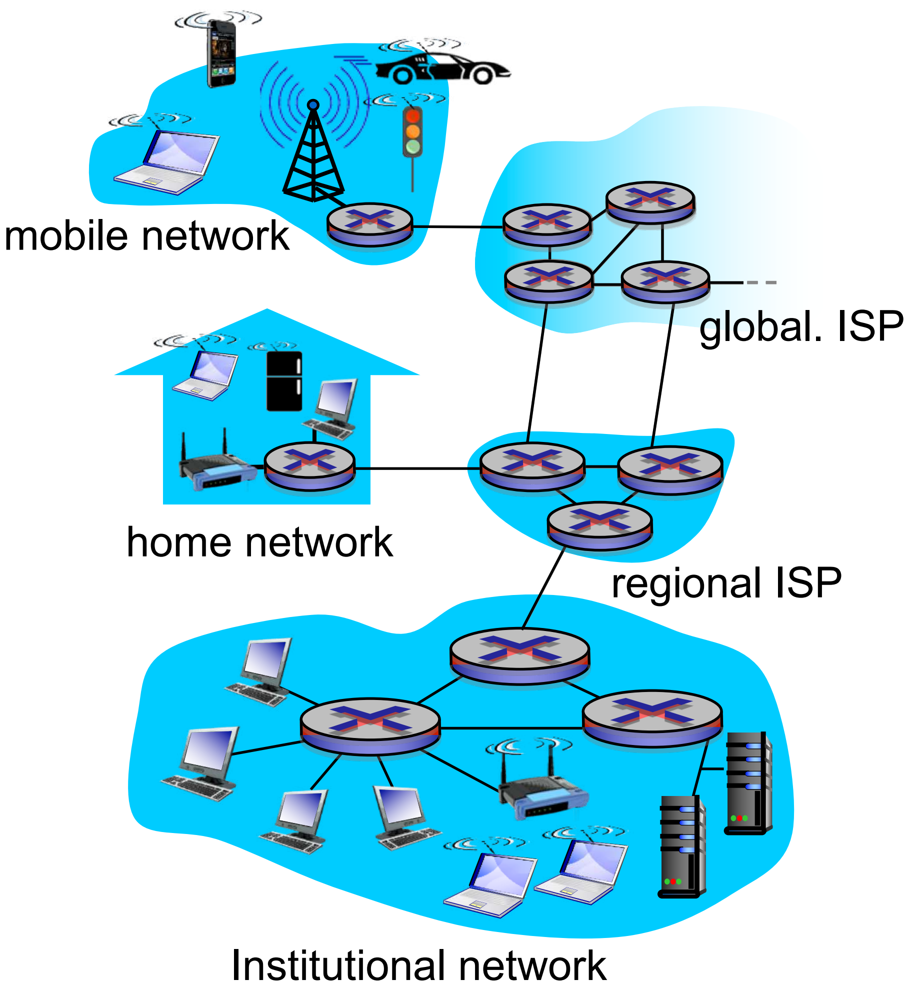
- Human protocols
  - “what’s the time?”
  - “I have a question”
  - Introductions
- Specific messages sent
- Specific actions taken



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

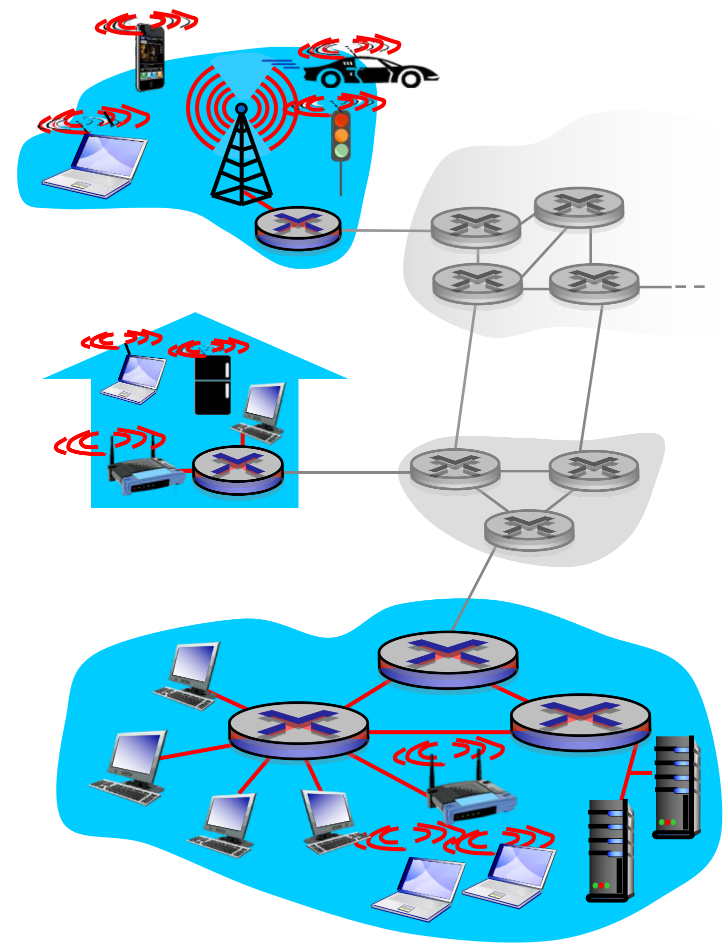
A Closer Look at Network Structure

- Network edge
  - Hosts: clients and servers
  - Servers often in data centers
- Access networks and physical media
  - Wired, wireless communication links
- Network core
  - Interconnected routers
  - Network of networks

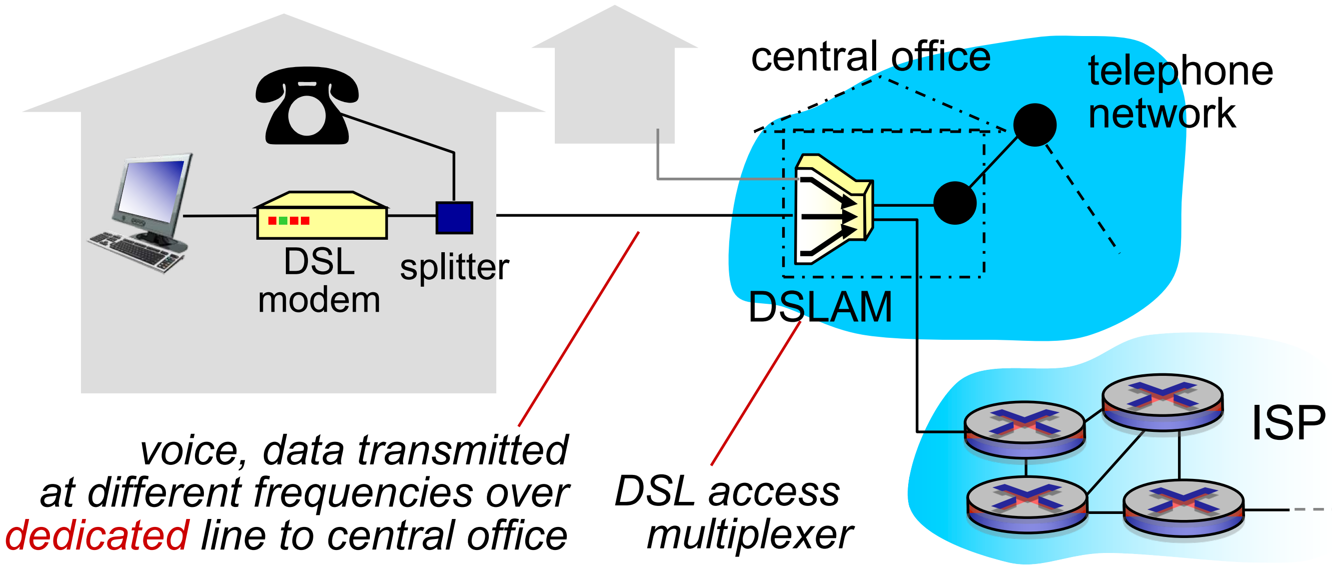


Access Networks and Physical Media

- How to connect end systems to edge routers?
  - Residential access networks
  - Institutional access networks (school, company)
  - Mobile access networks
- Keep in mind
  - Bandwidth (bits per second) of access network?
  - Shared or dedicated?

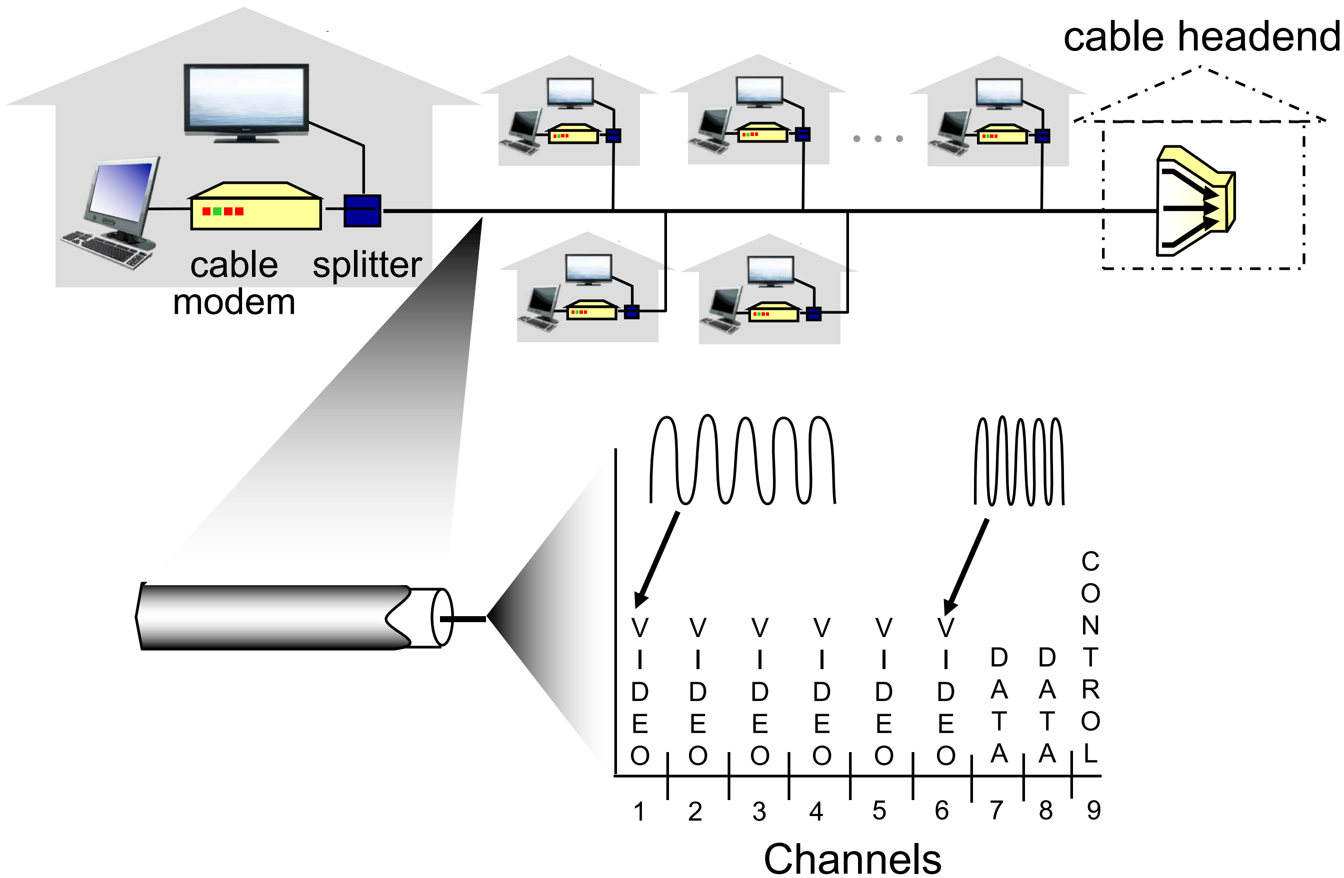


Access Network: Digital Subscriber Line (DSL)



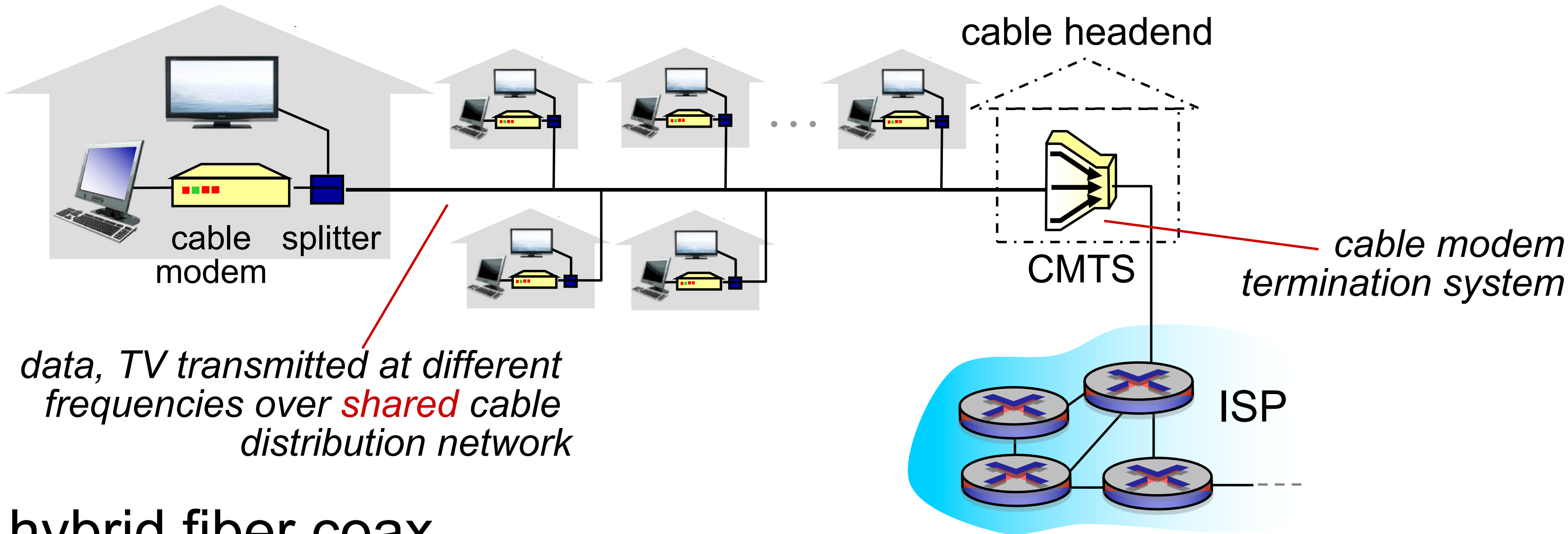
- Use existing telephone line to central office DSLAM
  - Data over DSL phone line goes to Internet
  - Voice over DSL phone line goes to telephone network
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access Network: Cable Network



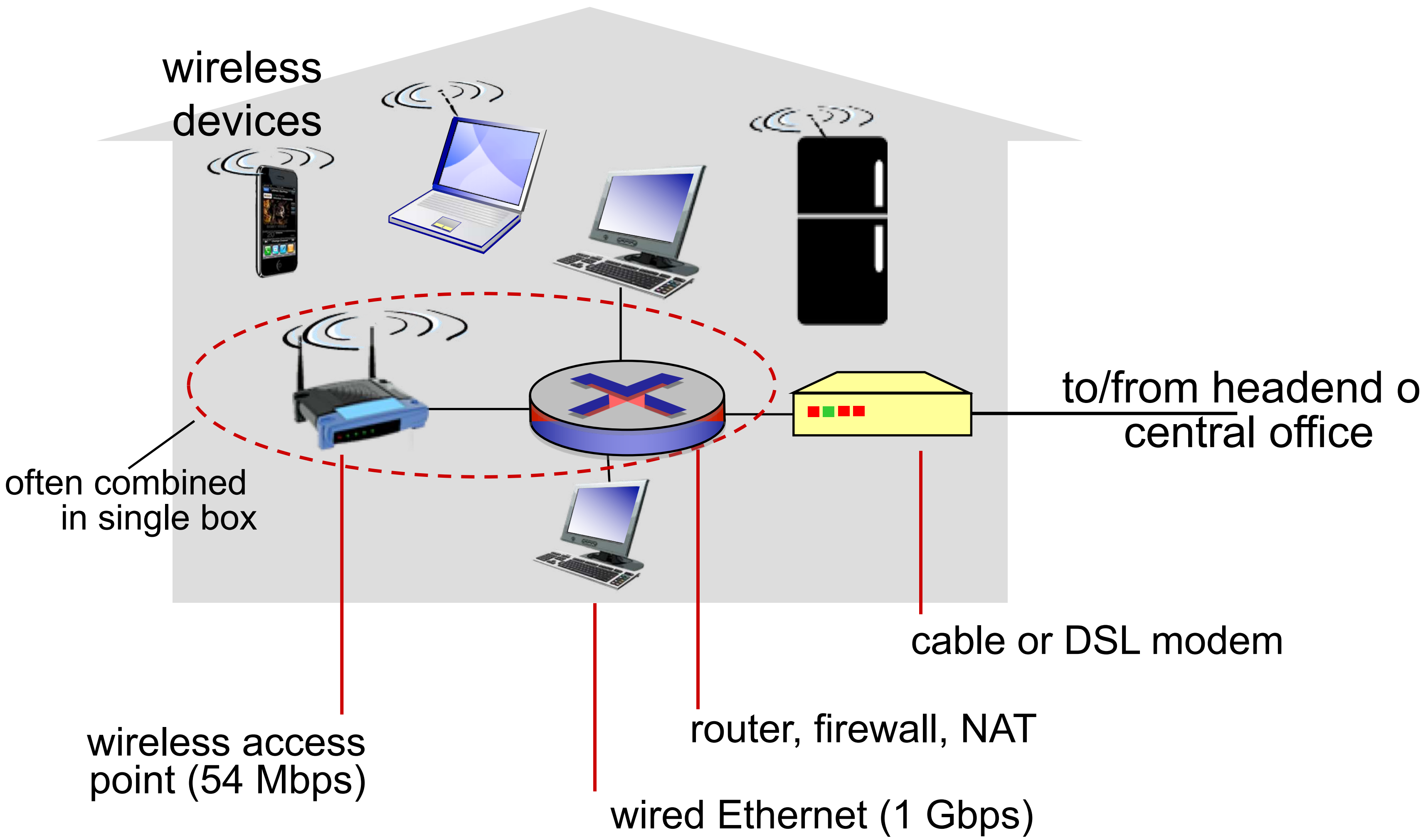
- Frequency division multiplexing
  - Different channels transmitted in different frequency bands

Access Network: Cable Network

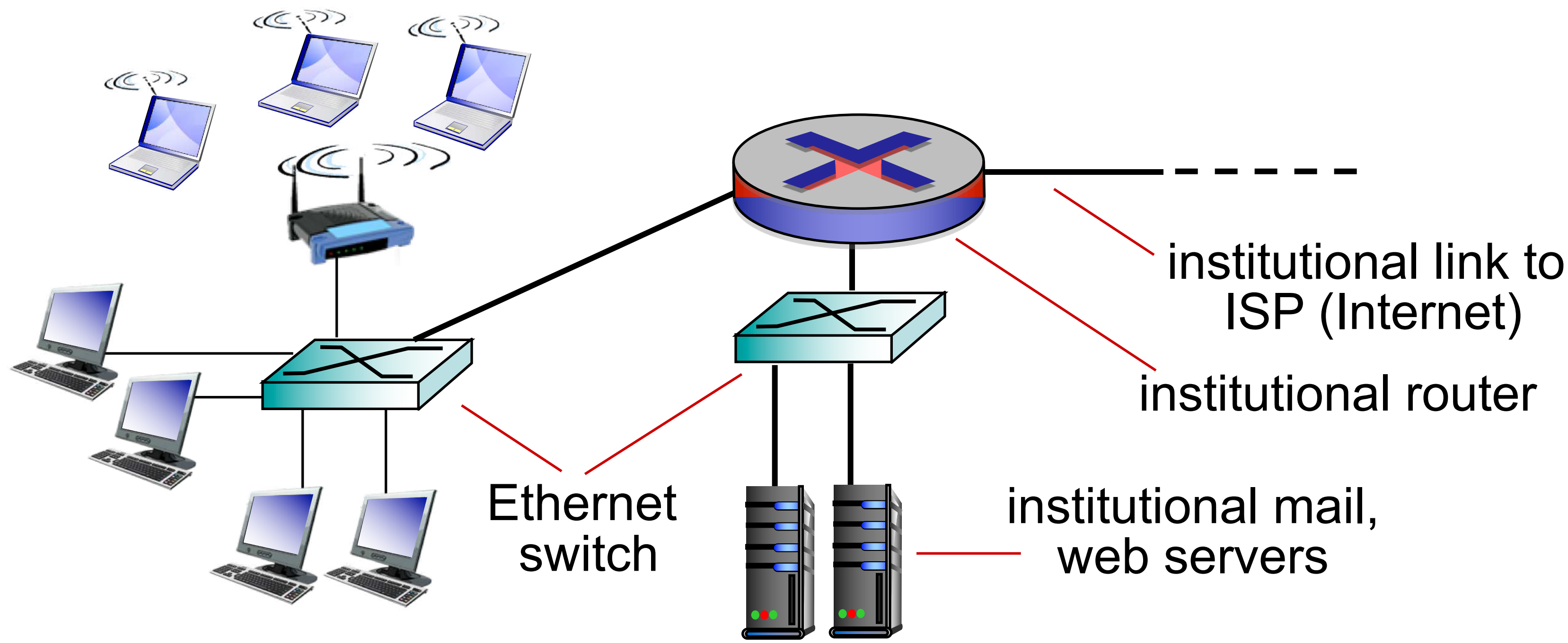


- HFC: hybrid fiber coax
  - Asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- Network of cable, fiber attaches homes to ISP router
  - Homes share access network to cable headend
  - Unlike DSL, which has dedicated access to central office

Access Network: Home Networks



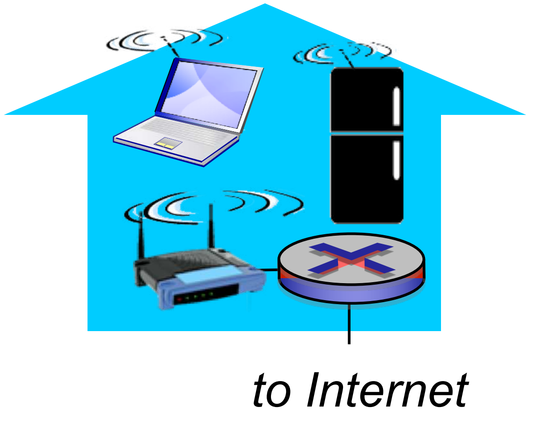
Access Network: Enterprise Networks

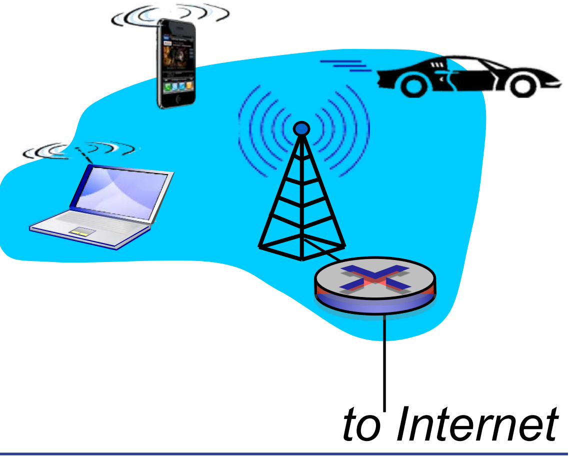


- Typically used in companies, universities, etc.
- 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps transmission rates

Wireless Access Networks

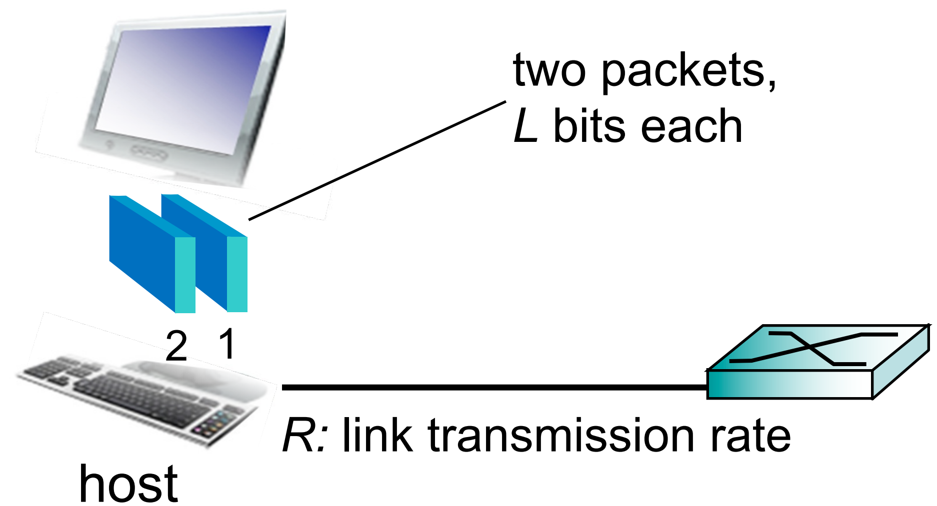
- Shared wireless access network connects end system to router
  - Via base stations/access points
- Wireless LANs
  - Within building (100s m)
  - 802.11 b/g/n (WiFi): 11, 54, 450 Mbps transmission rates
- Wide-area wireless access
  - By telecommunication operators (10s km)
  - 3G, 4G (LTE): between 1 and 10 Mbps





Sending Data Packets

- Host sending function:
  - Take application message
  - Break into chunks (packets) of length L bits
  - Transmit packet into access network at transmission rate R
    - Link transmission rate/capacity/bandwidth



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

Physical Media

- A bit propagates between transmitter/receiver pairs
- A physical link lies between transmitter and receiver
- Guided media
  - Signals propagate in solid media: copper, fiber, coax
- Unguided media
  - Signals propagate freely, e.g., radio

- Twisted Pair
  - Two insulated copper wires
    - CAT5: 100 Mbps, 1 Gbps Ethernet
    - CAT6: 10 Gbps

Physical Media: Coax, Fiber

- Coaxial cable
  - Two concentric copper conductors
  - Bidirectional
  - Broadband
    - Multiple channels on cable
    - HFC

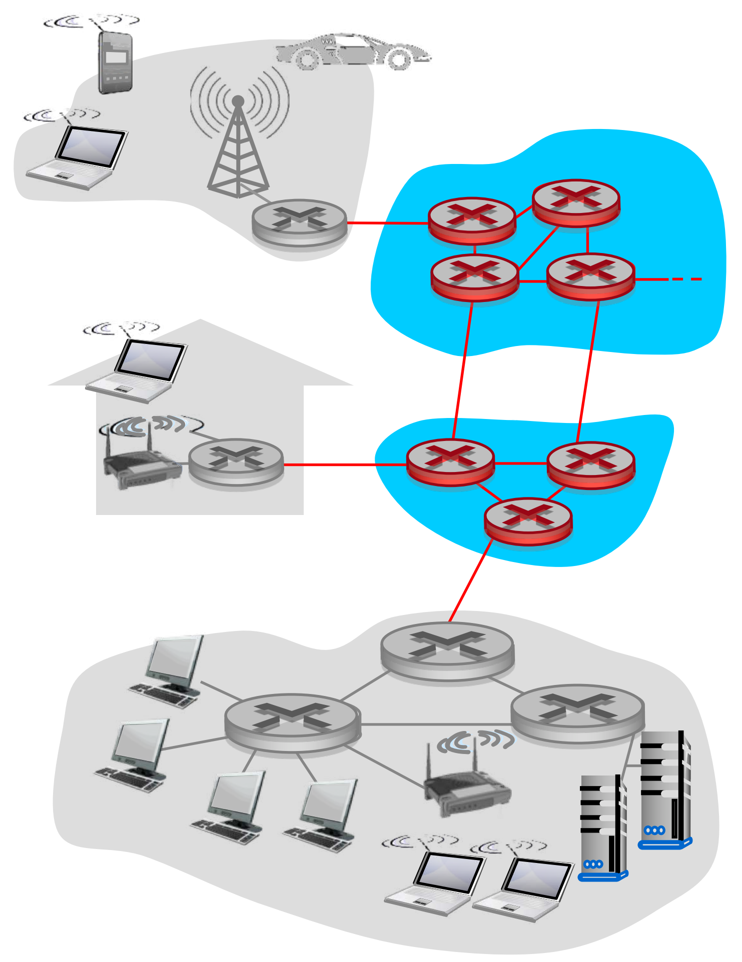
- Fiber Optic Cable
  - Glass fiber carrying light pulses, each pulse a bit
  - High speed operation
    - E.g., 10s-100s Gbps transmission rate
  - Low error rate
    - Repeaters spaced far apart
    - Immune to electromagnetic noise

Physical Media: Radio

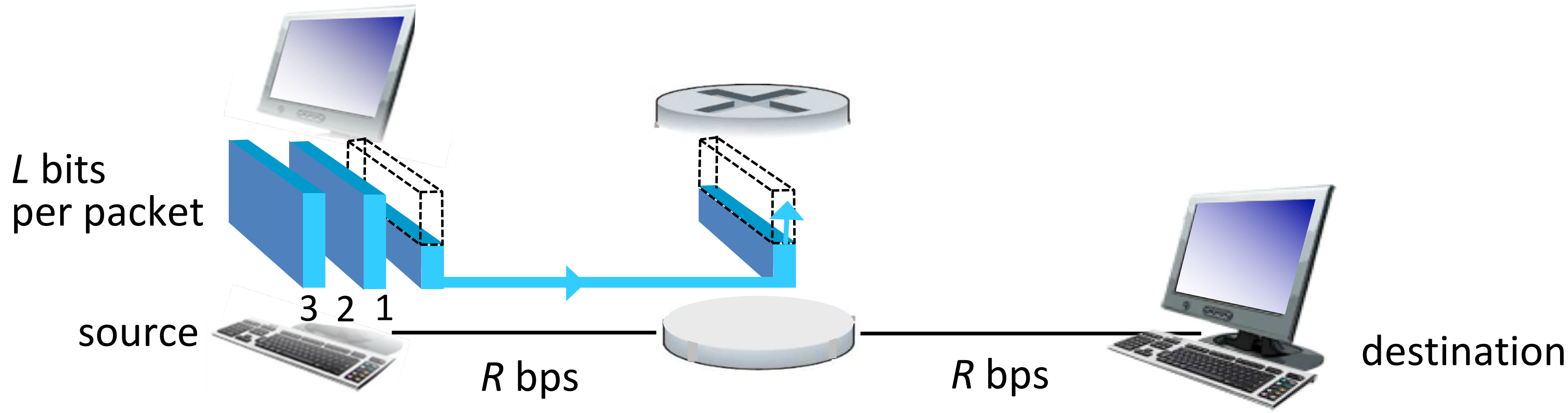
- Signal carried in electromagnetic spectrum
- No physical “wire”
- Bidirectional
- Propagation environment effects:
  - Reflection, obstruction by objects, interference
- Radio link types
  - Terrestrial microwave: e.g., up to 45 Mbps channels
  - LAN (e.g., WiFi): 54 Mbps
  - Wide-area (e.g., cellular): 4G cellular ~ 10 Mbps
  - Satellite: Kbps to 45Mbps channel (or multiple smaller channels) with 270 msec end-end delay

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

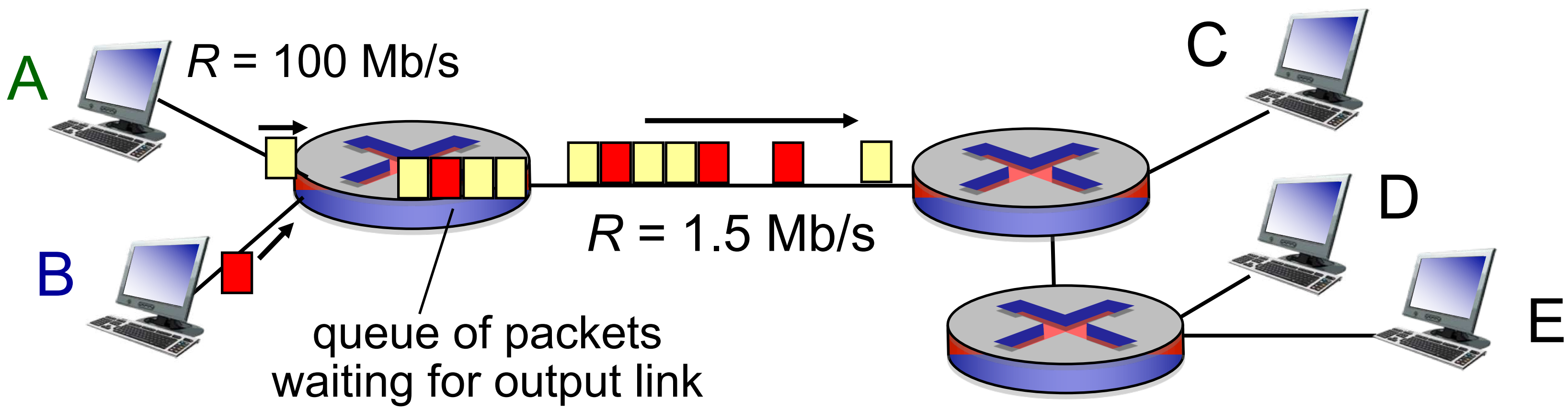


Packet-Switching: Store-and-Forward



- Takes L/R seconds to transmit (push out) L-bit packet into link at R bps
- Store and forward: entire packet must arrive at router before it can be transmitted on next link
- End-end delay = 2L/R (assuming zero propagation delay)
- One-hop numerical example:
  - L = 7.5 Mbits, R = 1.5 Mbps, one-hop delay = 5 sec

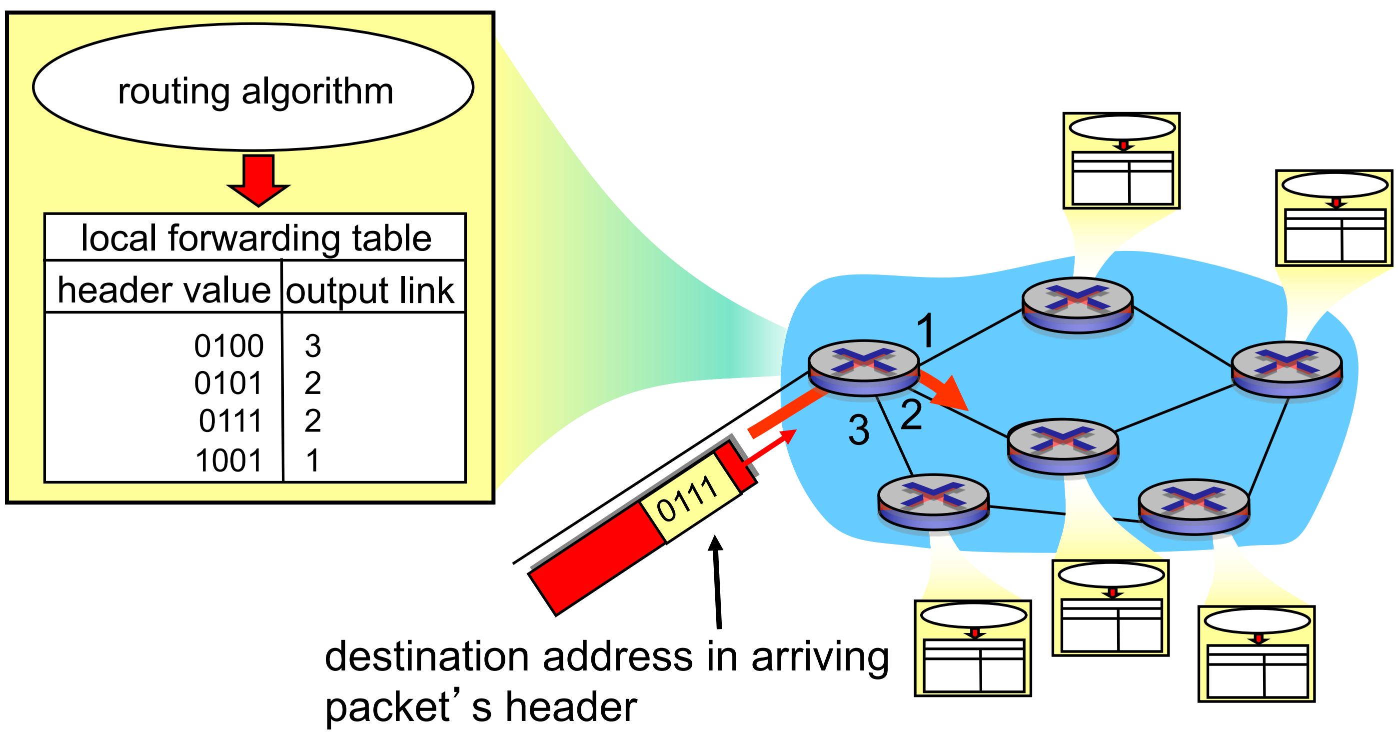
Packet Switching: Queuing Delay and Loss



- Queuing and loss
  - If arrival rate (in bits) to link exceeds transmission rate of link for a period of time
    - Packets will queue and wait to be transmitted on link
    - Packets can be dropped (lost) if memory (buffer) fills up

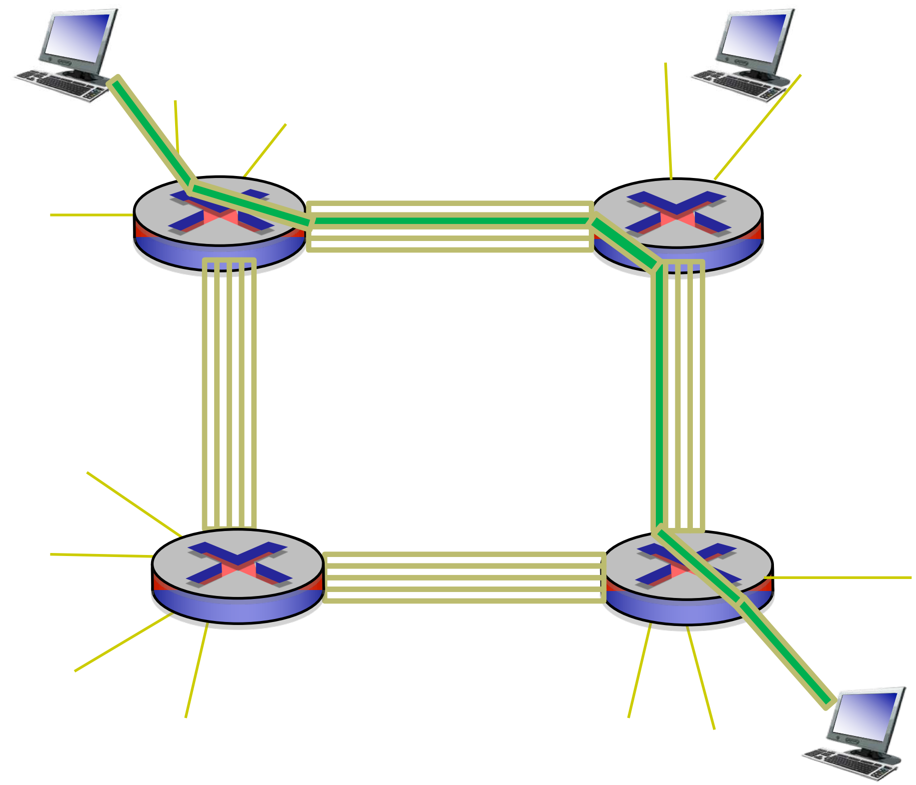
Two Key Network-Core Functions

- Routing: determines source-destination route taken by packets
- Forwarding: move packets from router's input to appropriate router's output



Alternative: Circuit Switching

- End-end resources allocated to, reserved for "call" between source and destination
  - Dedicated resources: no sharing
    - Circuit-like (guaranteed) performance
  - Circuit segment idle if not used by call (no sharing)
  - Commonly used in traditional telephone networks

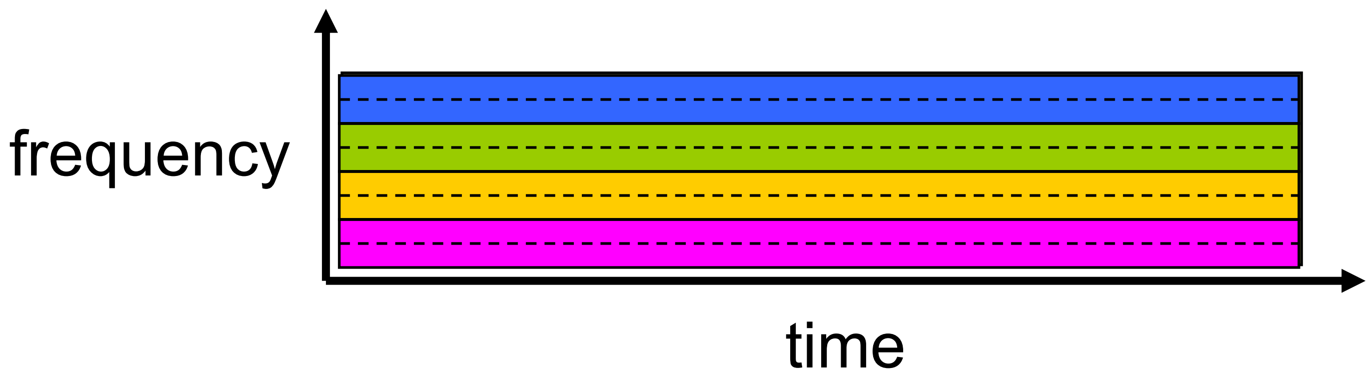


Circuit Switching: FDM versus TDM

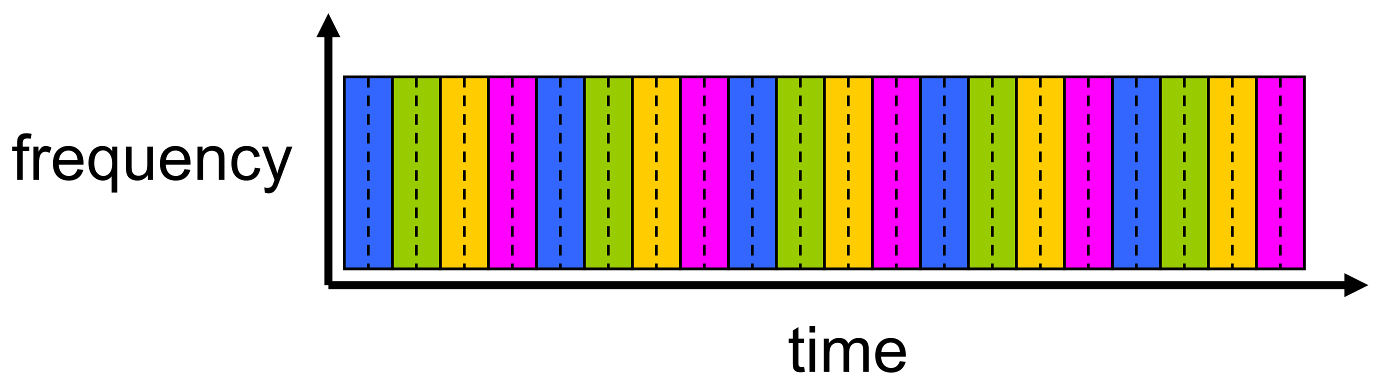
Example:

4 users

FDM

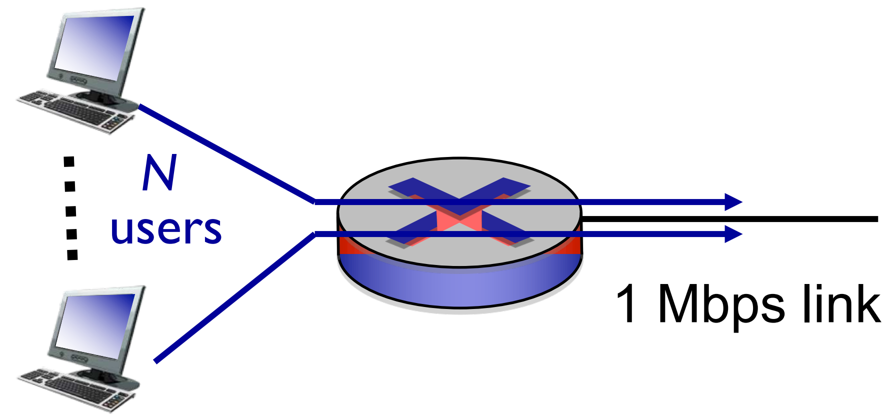


TDM



Packet Switching versus Circuit Switching

- Packet switching allows more users to use network!
- Example
  - 1 Mb/s link
  - User 100 kb/s when “active”
    - Active 10% of time
  - Circuit switching:
    - 10 users
  - Packet switching:
    - With 35 users, probability > 10 users active at same time is less than .0004



Packet Switching versus Circuit Switching

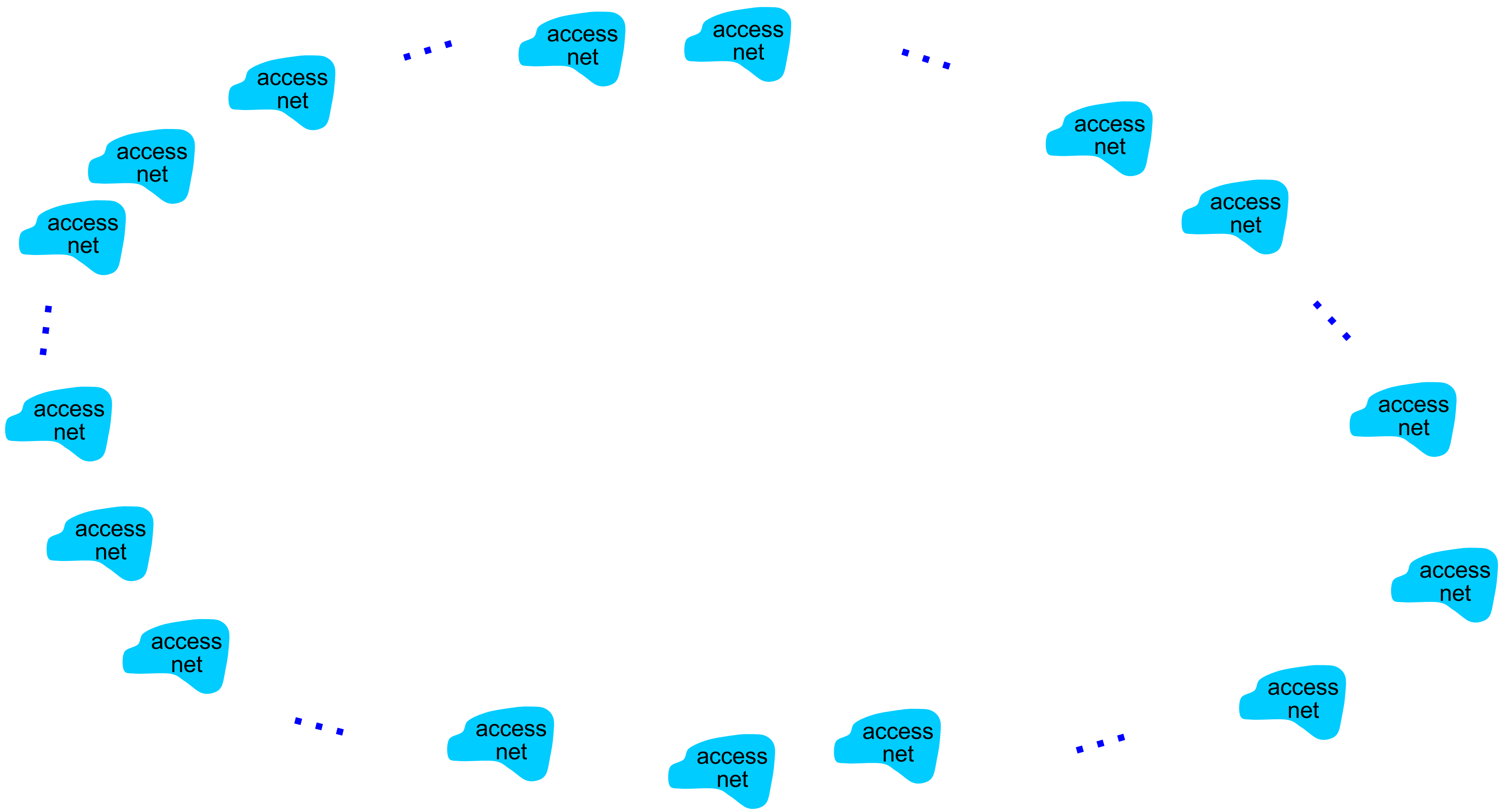
- Packet Switching works for bursty data
  - Resource sharing
  - Simpler, no call setup
- However, excessive congestion possible
  - Packet delay and loss
  - Protocols needed for reliable data transfer and congestion control
- How to provide circuit-like behaviour?
  - E.g., for audio/video apps

Internet Structure: Network of Networks

- End systems connect to Internet via access ISPs (Internet Service Providers)
  - Residential, company and university ISPs
- Access ISPs in turn must be interconnected
  - So that any two hosts can send packets to each other
- Resulting network of networks is very complex
  - Evolution was driven by economics and national policies

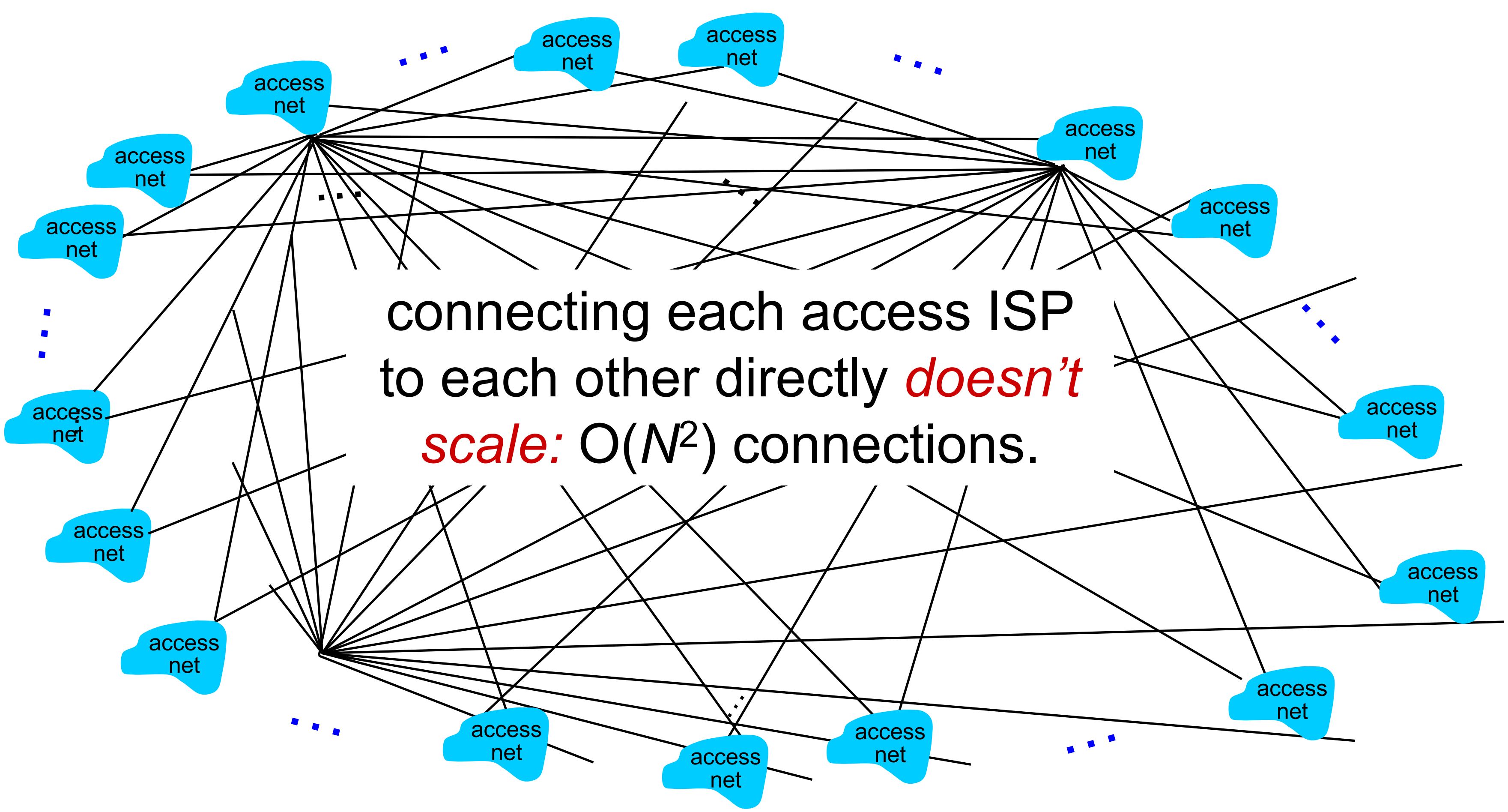
Internet Structure: Network of Networks

- Given millions of access ISPs, how to connect them together?



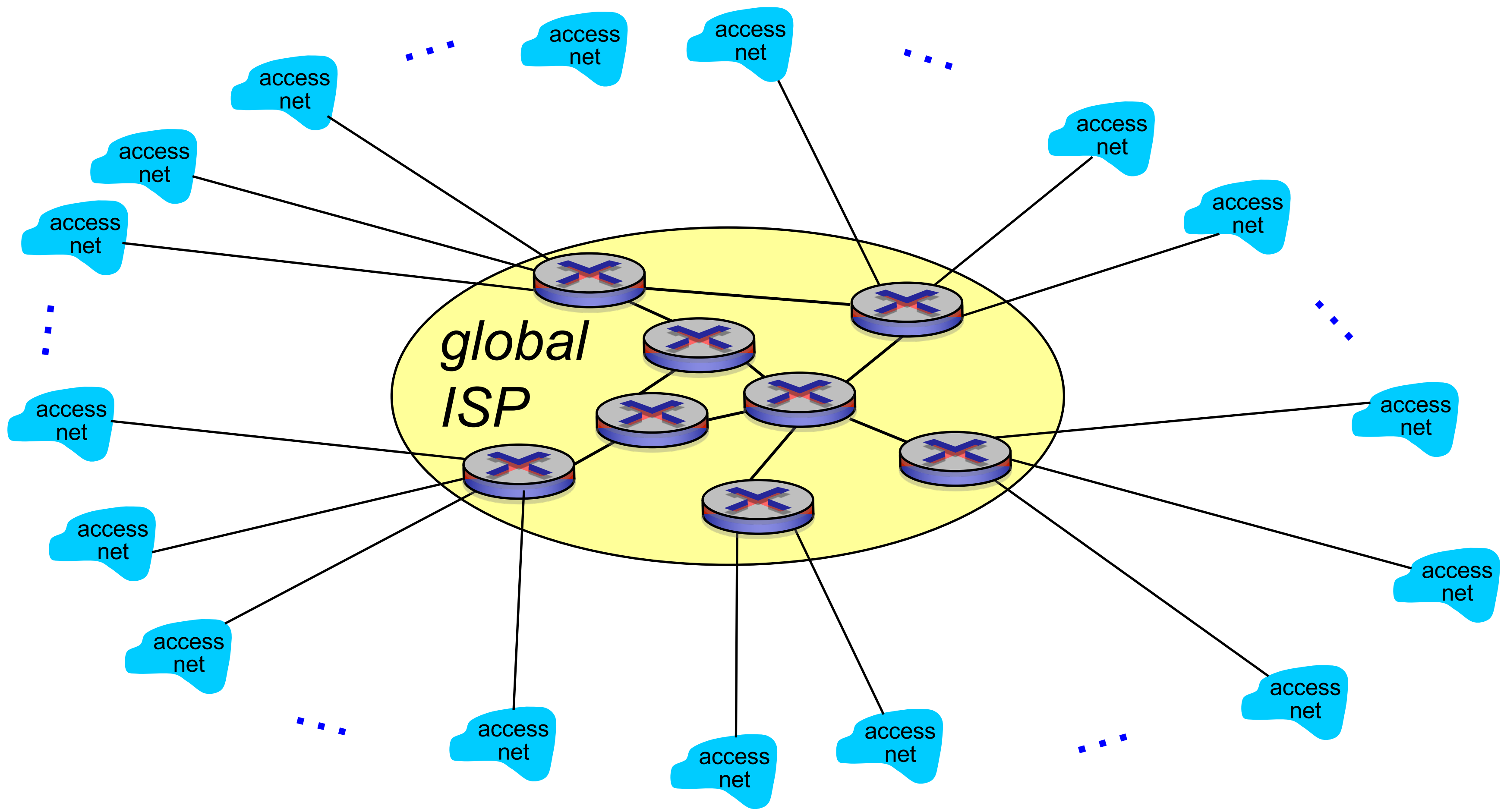
Internet Structure: Network of Networks

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



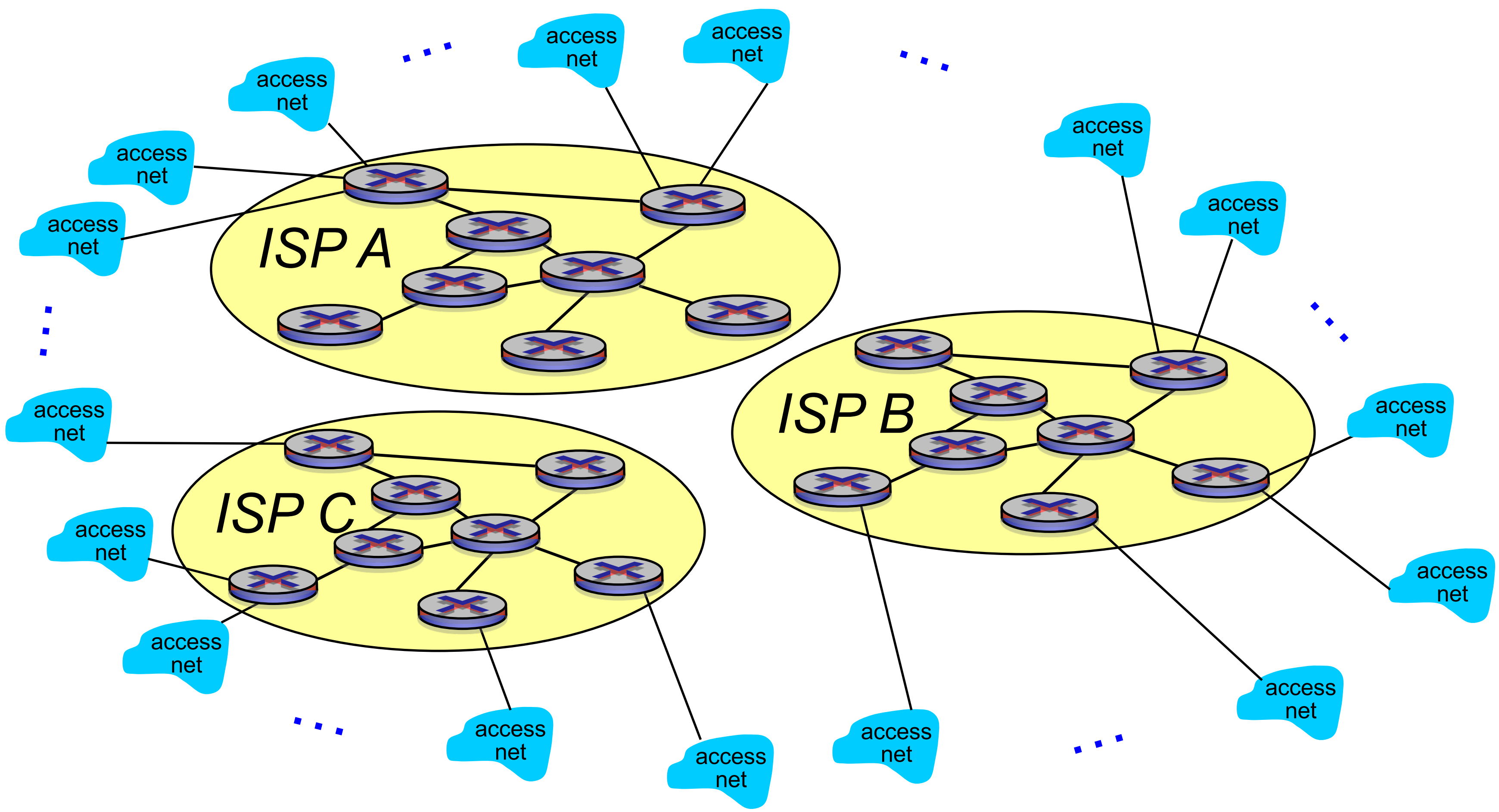
Internet Structure: Network of Networks

- Option: connect each access ISP to one global transit ISP?



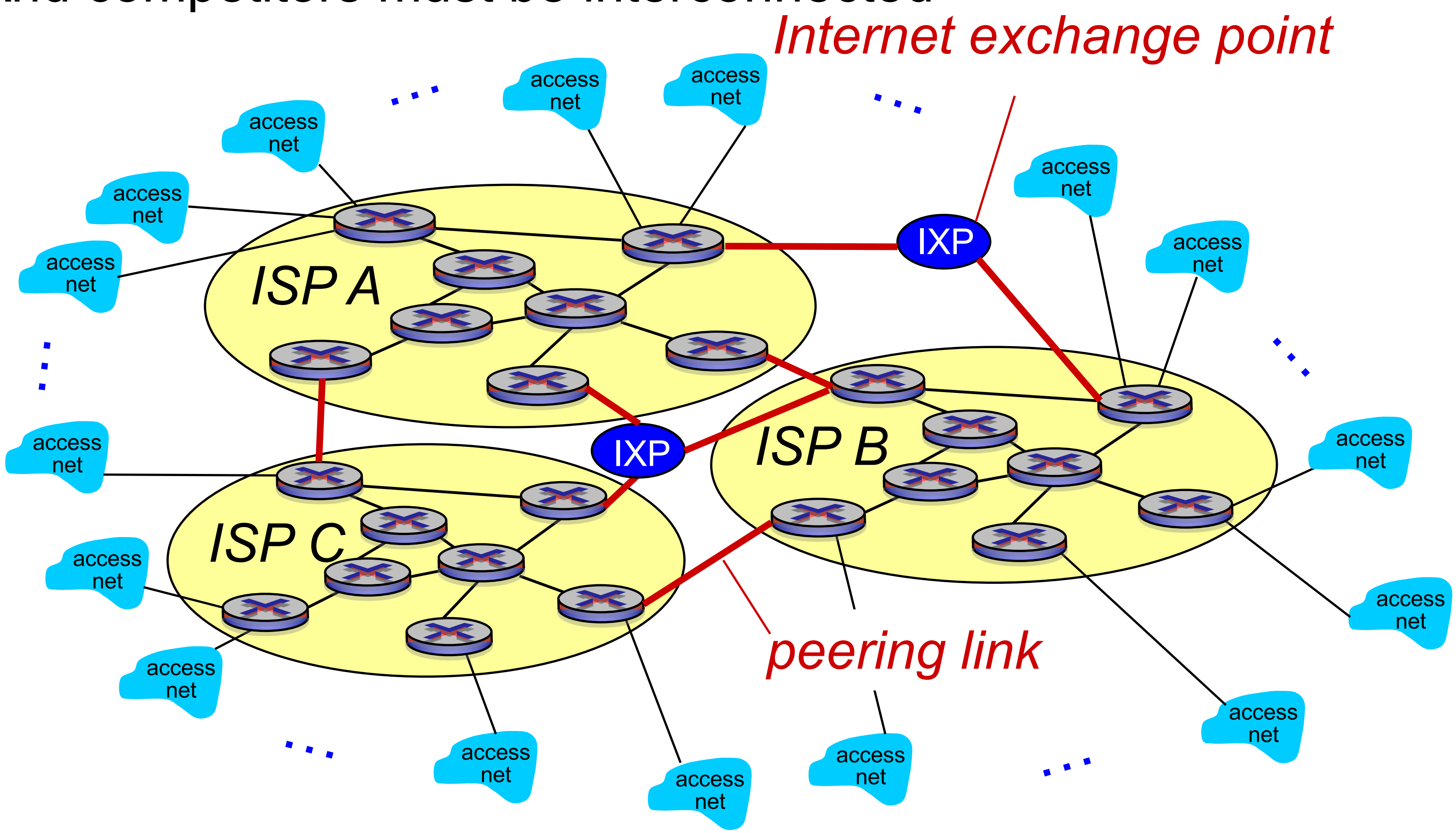
Internet Structure: Network of Networks

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



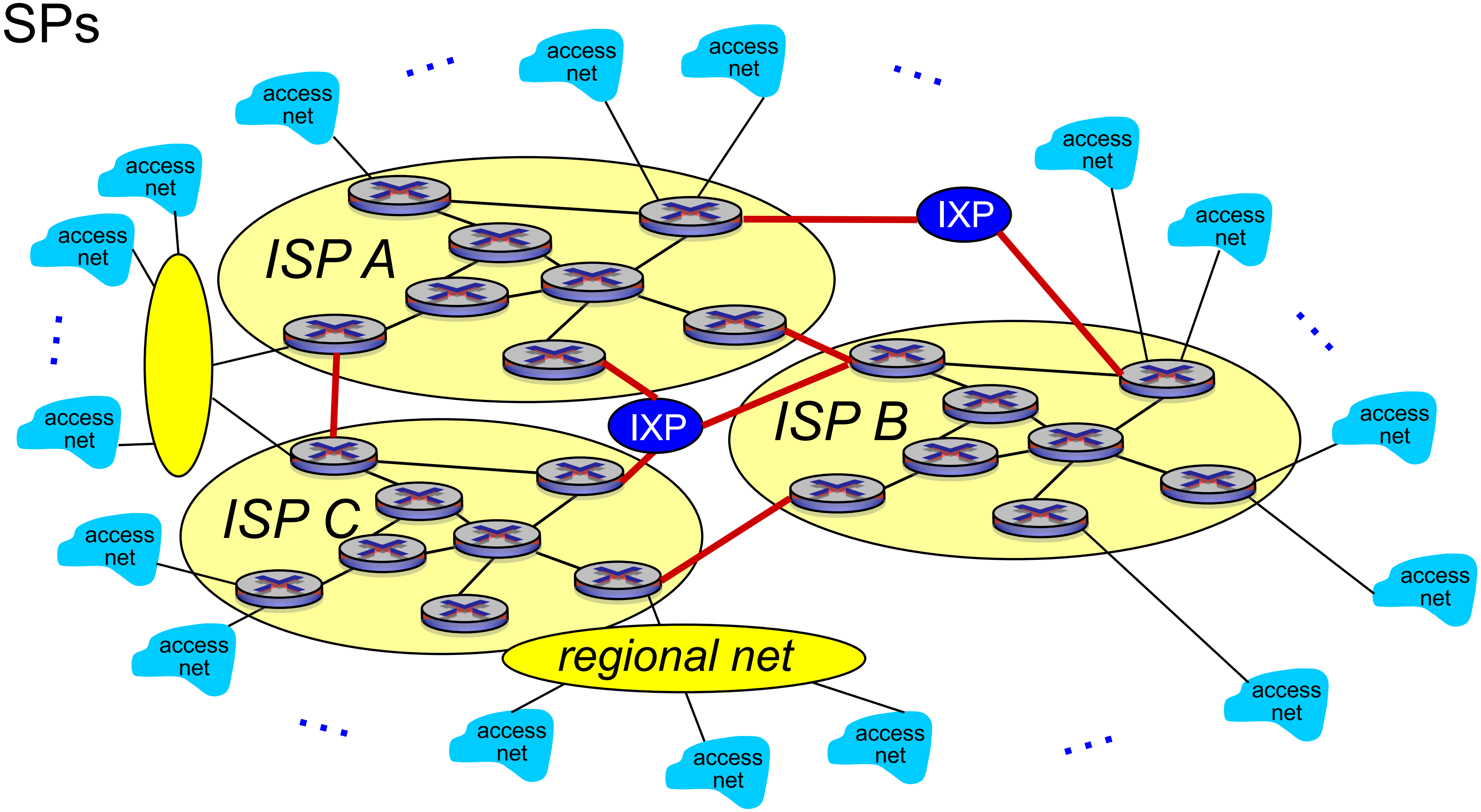
Internet Structure: Network of Networks

- And competitors must be interconnected



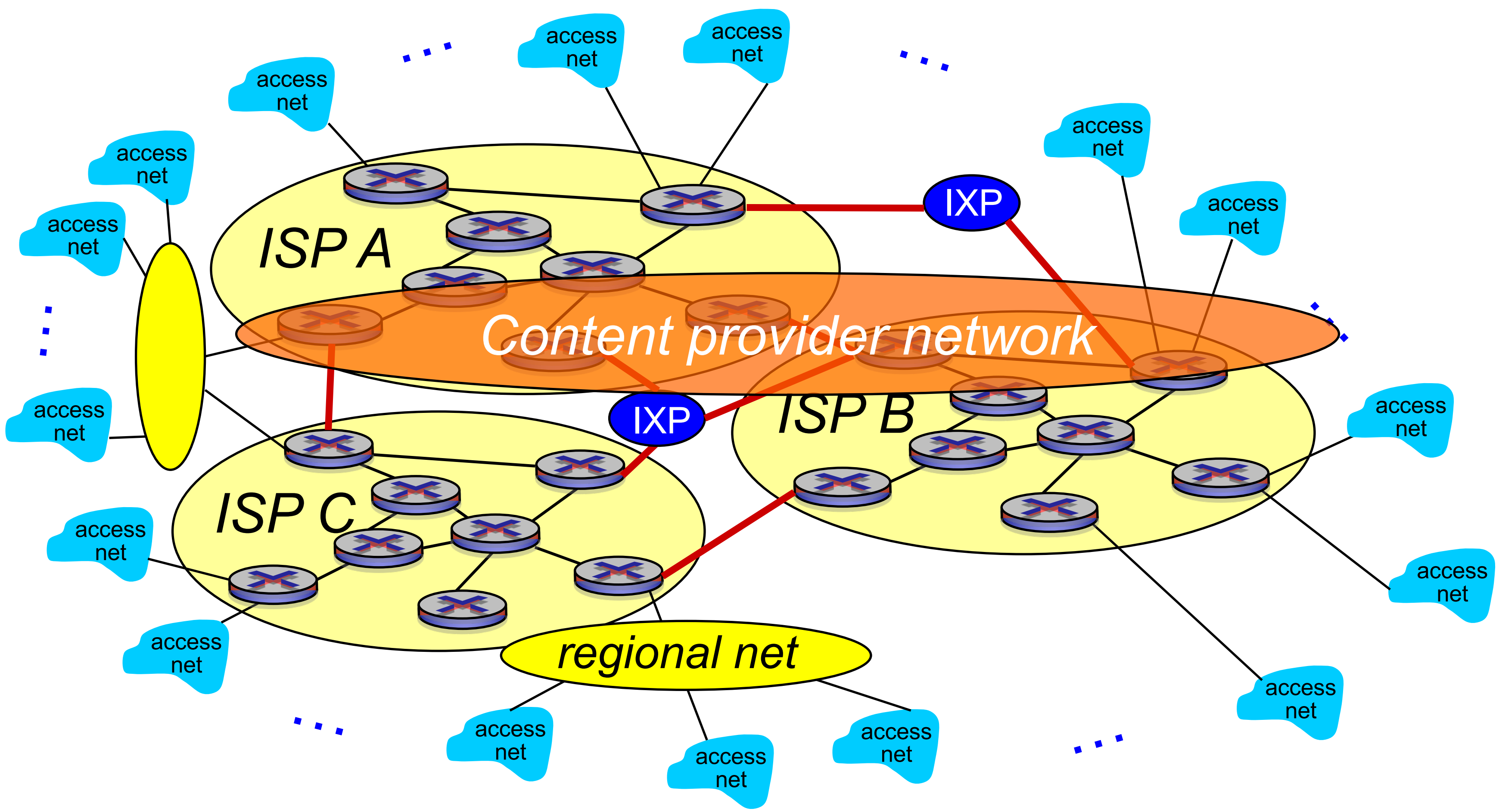
Internet Structure: Network of Networks

- And regional networks may arise to connect access networks to ISPs



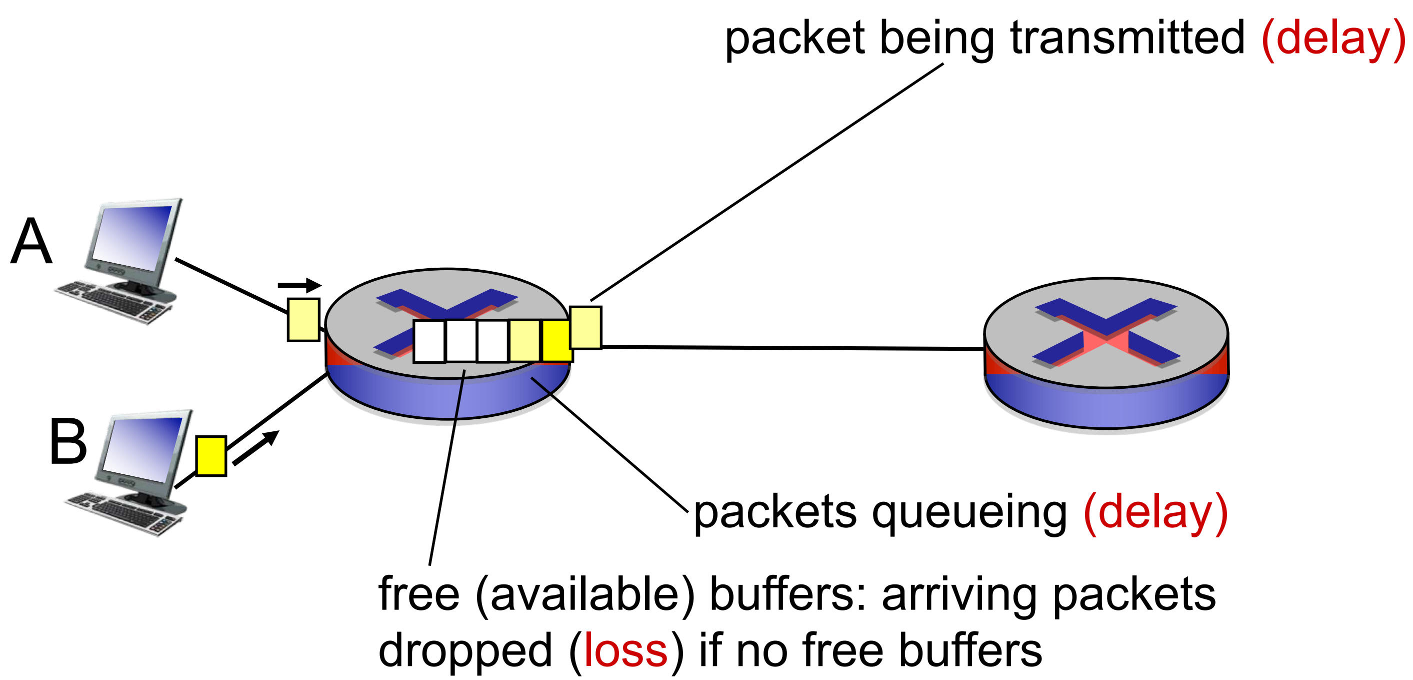
Internet Structure: Network of Networks

- And content provider networks may run their own network

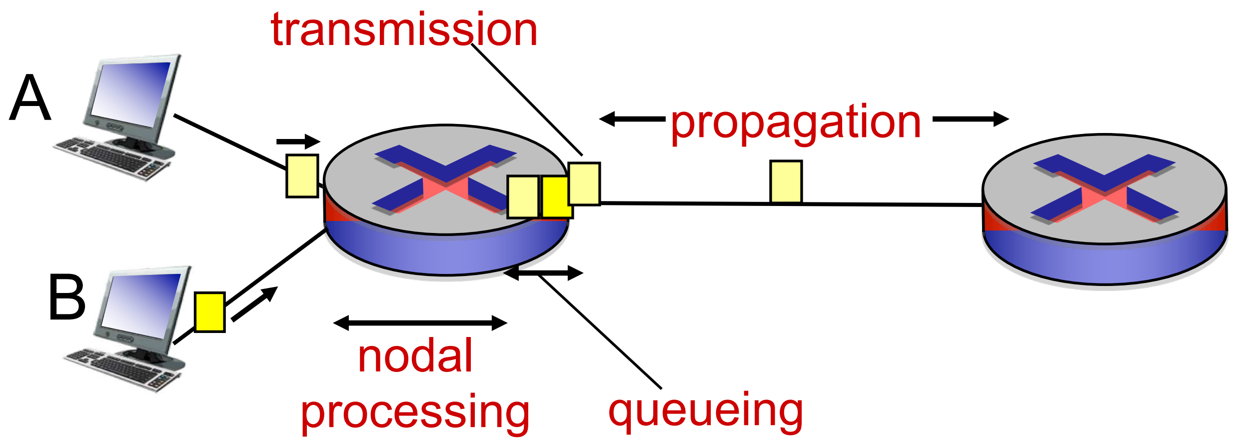


How Do Loss and Delay Occur?

- Packets queue in router buffers
  - Packet arrival rate to link (temporarily) exceeds output link capacity
  - Packets queue, wait for turn



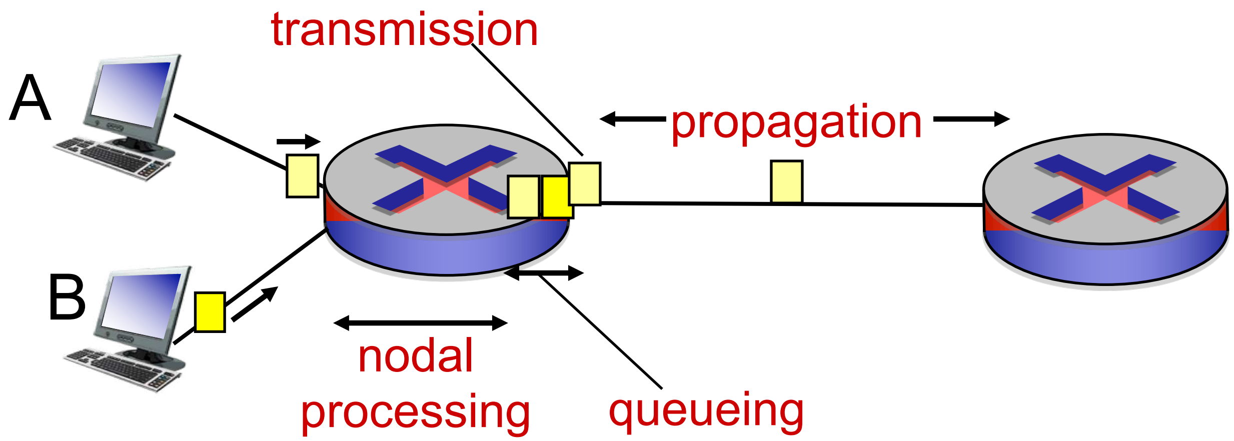
Four Sources of Packet Delay



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

- d_{proc} nodal processing
  - Check bit errors
  - Determine output link
  - Typically < msec
- d_{queue} queueing delay
  - Time waiting at output link for transmission
  - Depends on congestion level of router

Four Sources of Packet Delay

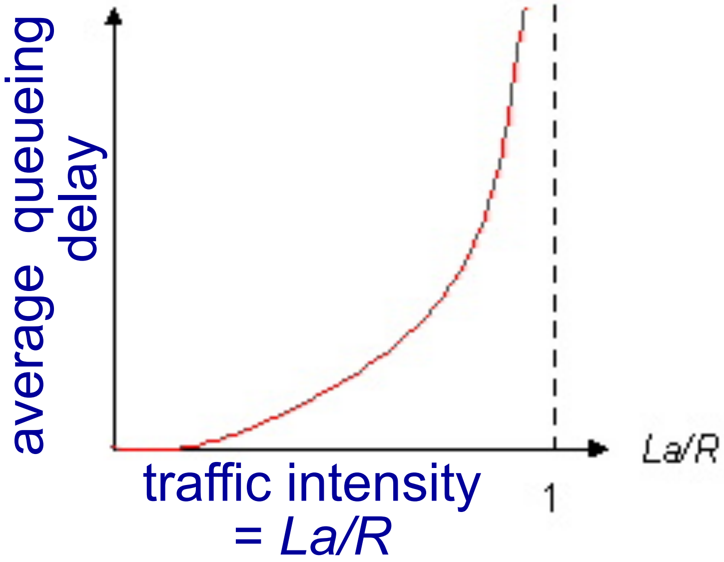


$$\boxed{d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}}$$

- d_{trans} transmission delay
  - L: packet length (bits)
  - R: link bandwidth (bps)
  - $d_{trans} = L/R$
- d_{prop} propagation delay
  - d: length of physical link
  - s: propagation speed (~2×10^8 m/sec)
  - $d_{prop} = d/s$

Queueing delay

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



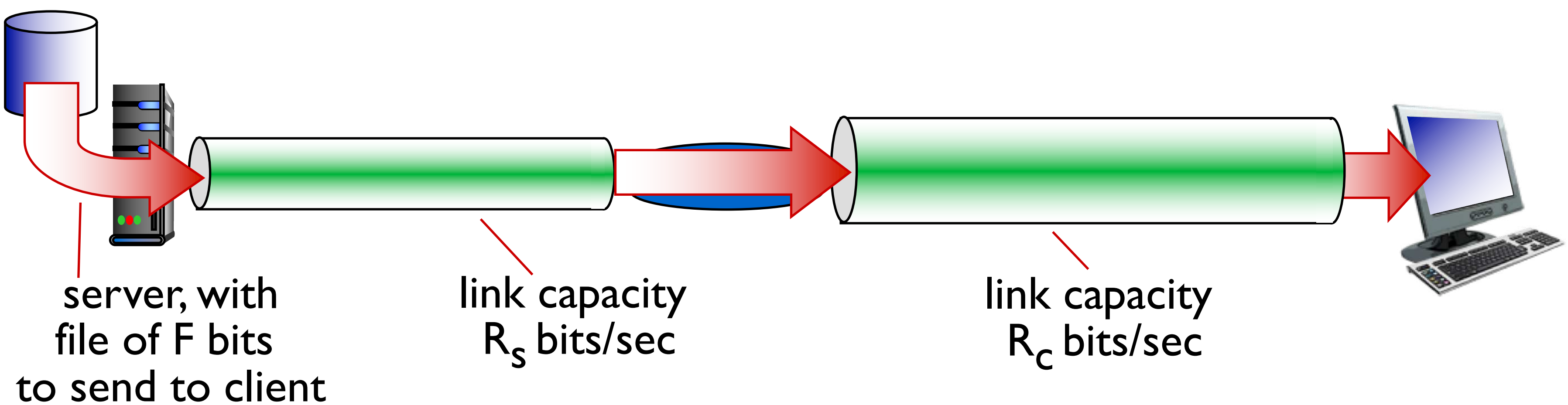
- La/R ~ 0: avg. queueing delay small
- La/R -> 1: avg. queuing delay large
- La/R > 1: more “work” arriving that can be served, average delay infinite!


La/R ~ 0


La/R -> 1

Throughput

- Throughput: rate (bits/time unit) at which bits are transferred between sender and receiver
  - Instantaneous: rate at given point in time
  - Average: rate over longer period of time

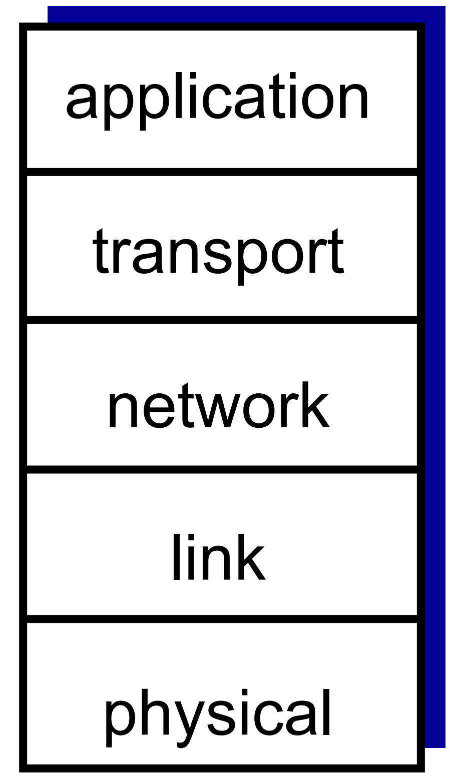


Why Layering?

- Networks are complex and made of many and different pieces
  - Hosts, routers, heterogeneous links, applications, …
- Explicit structure allows identification of complex system's pieces
- Modularization eases maintenance and updating of systems
  - Change of implementation of a layer's service transparent to rest of system
- Can layering be considered harmful?

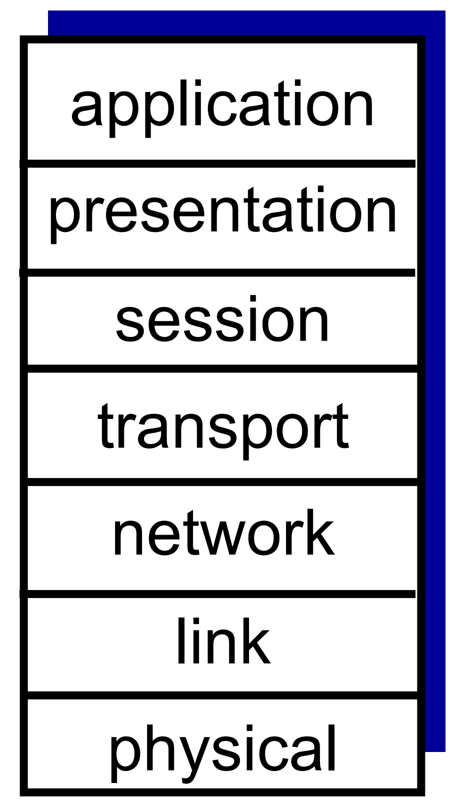
Internet Protocol Stack

- 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 neighbouring network elements
  - Ethernet, 802.11 (WiFi)
- Physical: bits “on the wire”

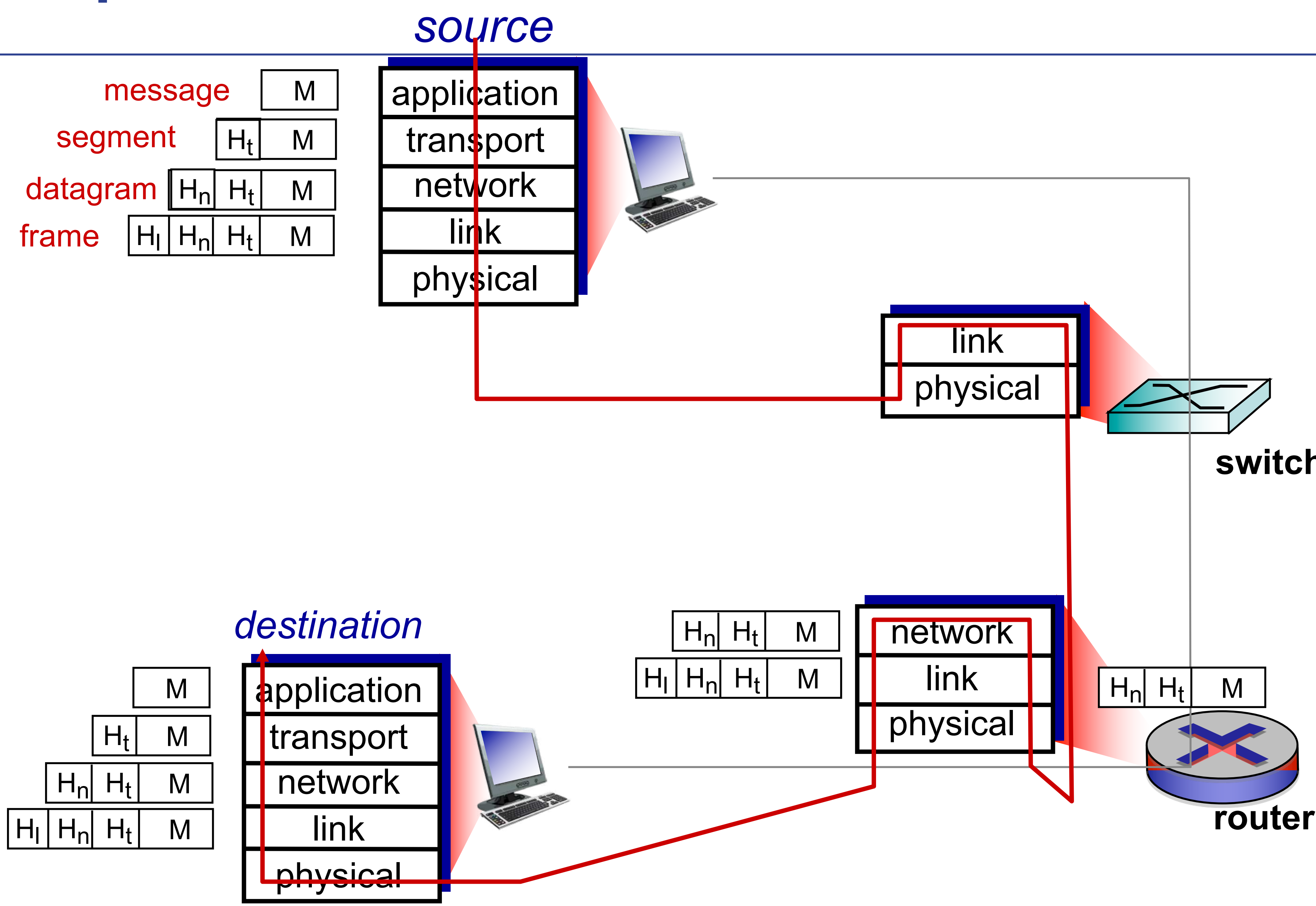


ISO/OSI Reference Model

- Presentation: allow applications to interpret meaning of data
  - Encryption, compression, machine-specific conventions
- Session: synchronization, checkpointing, recovery of data exchange
- Internet stack “missing” these layers!



Encapsulation



Network Security

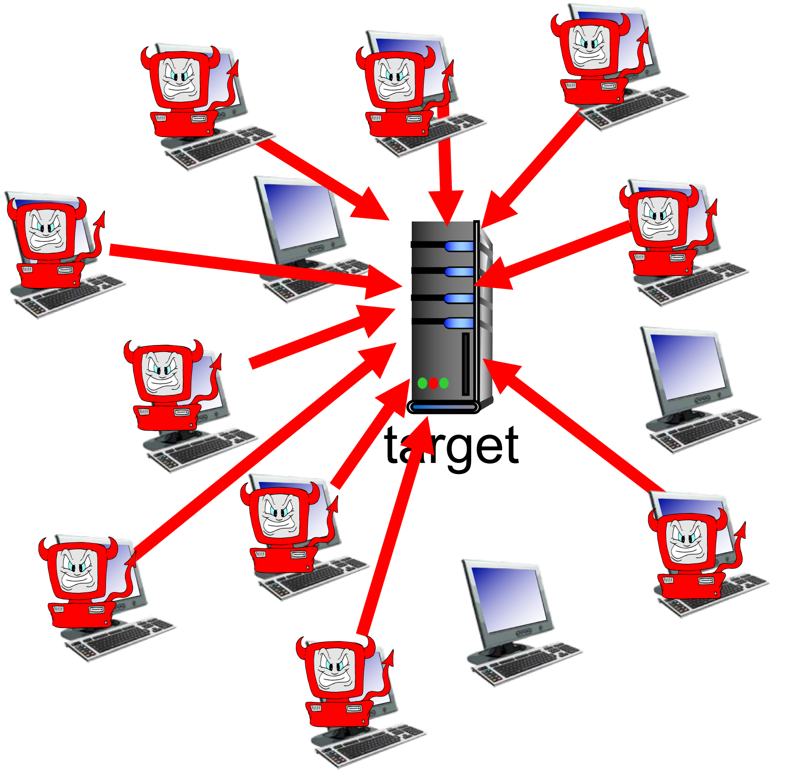
- Network security questions
  - How can computer networks be attacked?
  - How can computer networks be defended against attacks?
  - How can network architectures be designed to be immune to attacks?
- Internet not originally designed with (much) security in mind
  - Original vision: “a group of mutually trusting users attached to a transparent network”

Malware into Hosts

- Malware can reach a host through:
  - Virus: self-replicating infection by receiving/executing object
  - Worm: self-replicating infection by passively receiving object that gets itself executed
- Spyware can record keystrokes, web sites visited, upload info to collection site
- Infected host can be enrolled in botnet, used for spam and DDoS attacks

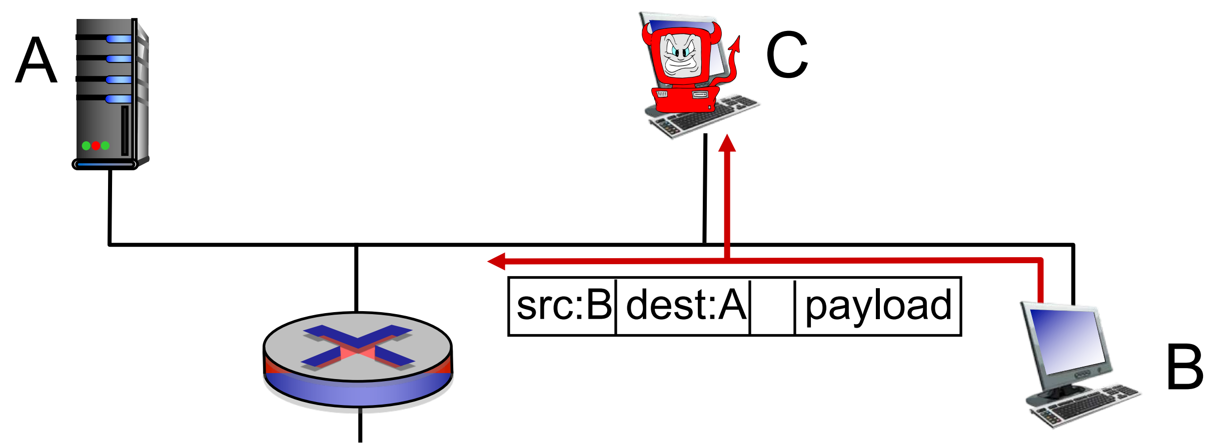
Denial of Service

- Denial of Service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic
- Example:
  1. Select target
  2. Break into hosts around the network (see botnet)
  3. Send packets to target from compromised hosts



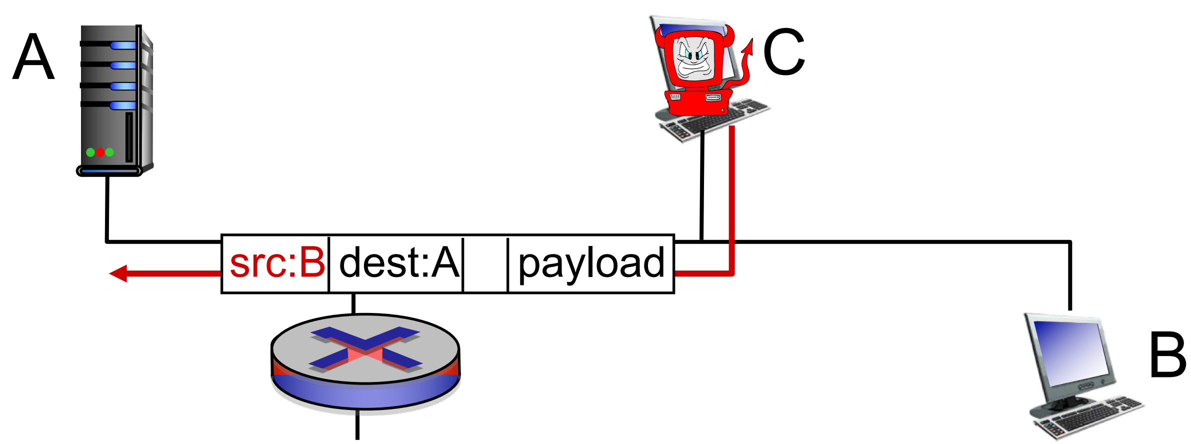
Packet Sniffing

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



Fake Addresses

- IP spoofing: send packet with false source address



More on security later…

Internet History

1961 – 1972: Early packet-switching principles

- 1961: queueing theory shows effectiveness of packet-switching
- 1964: packet-switching in military networks
- 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
  - ARPAnet has 15 nodes

Internet History

1972 – 1980: Internetworking, new and proprietary networks

- 1970: ALOHAnet satellite network in Hawaii
- 1974: Cerf and Kahn – architecture for interconnecting networks
  - Defining Principles: best effort service model, stateless routers, decentralized control
- 1976: Ethernet at Xerox PARC
- Late 70's: proprietary architectures: DECnet, SNA, XNA
- Late 70's: switching fixed length packets (ATM precursor)
- 1979: ARPAnet has 200 nodes

Internet History

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
- 100,000 hosts connected to confederation of networks

Internet History

1990 – 2000: Commercialization, the Web, apps

- Early 90’s: ARPAnet decommissioned
- Early 90’s: Web
  - Hypertext, HTML, HTTP, Netscape, …
- Late 90’s
  - Instant messaging, P2P
  - Network security
  - Estimated 50 million hosts, 100 million users
  - Backbone links running at Gbps

Internet History

- 2000 – present
- 2016: ~5B devices attached to Internet
- Deployment of broadband access
- Ubiquity of wireless access
- Online social networks
- Service providers (Google, Microsoft) create their own networks
- E-commerce, universities, enterprise services running in the “cloud” (e.g., Amazon EC2)

Additional Material

- Watch what it takes to lay Google's super-fast submarine Internet cable
  - https://www.youtube.com/watch?v=0TZwiUwZwIE
- Inside a Google Data Center
  - https://www.youtube.com/watch?v=XZmGGAbHqa0