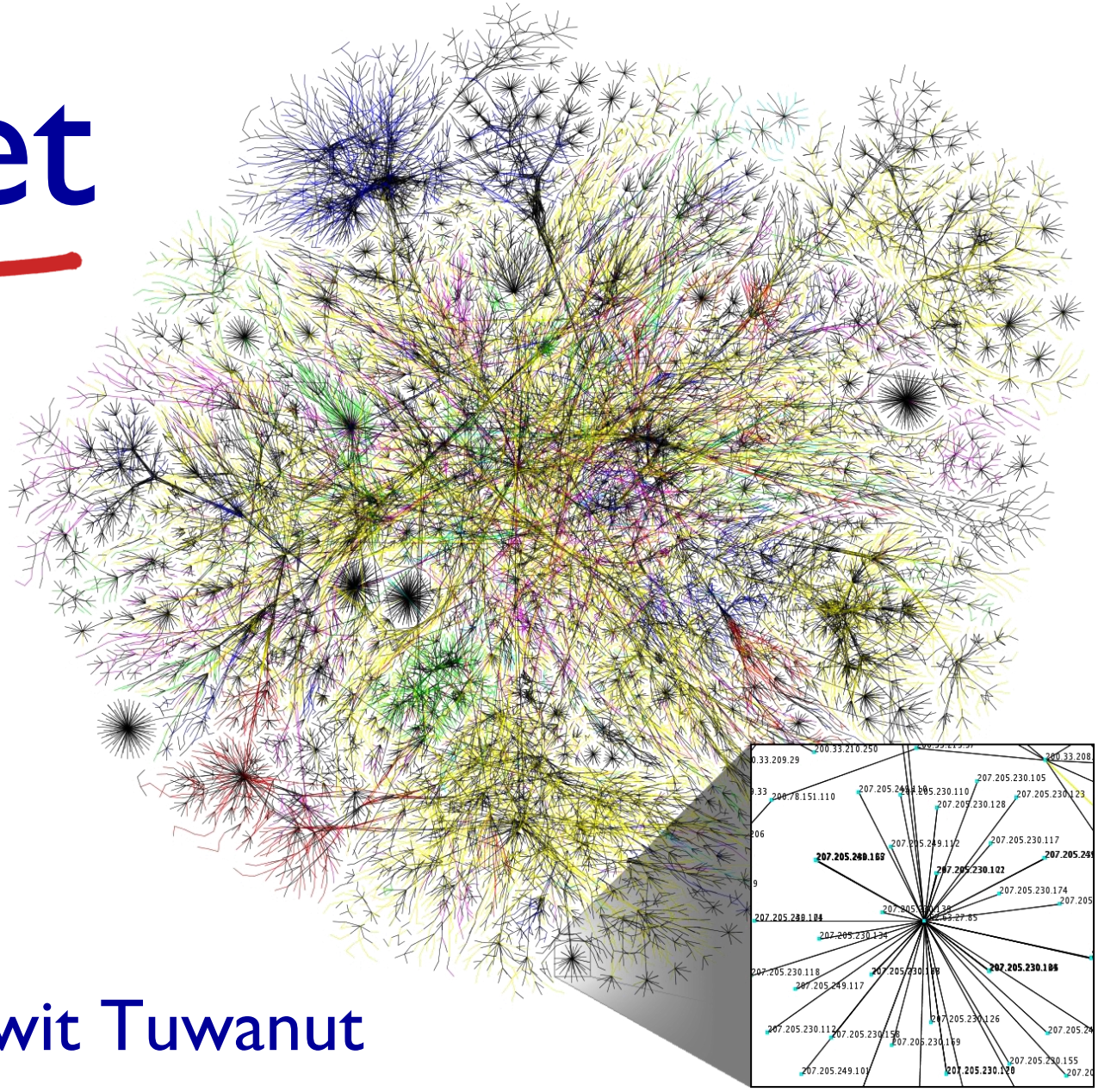
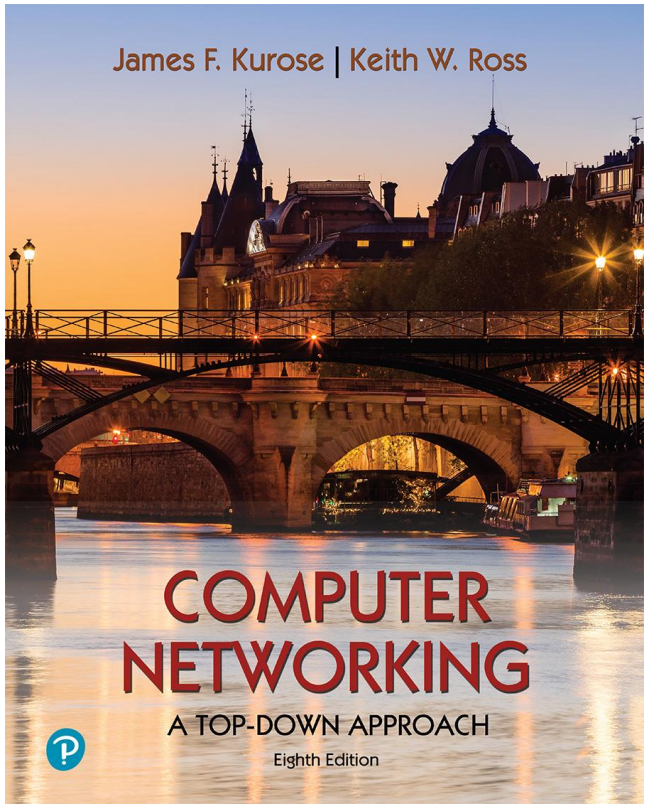
Internet



Assoc.Prof. Panwit Tuwanut

Reference



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Chapter 1. Introduction

1. What *is* the Internet?

- There are a couple of ways to answer this question.
- First, we can describe the nuts and bolts of the Internet, that is, the basic hardware and software components that make up the Internet.
- Second, we can describe the Internet in terms of a networking infrastructure that provides services to distributed applications.

nuts and bolts เป็น สำนวน แปลว่า หลักปฏิบัติขั้นพื้นฐาน

What's the Internet: "nuts and bolts" view

- The Internet is a computer network that interconnects billions of computing devices throughout the world.
- Not too long ago, these computing devices were primarily traditional desktop PCs, Linux workstations, and so-called servers that store and transmit information such as Web pages and e-mail messages.
- Increasingly, however, nontraditional Internet end systems such as laptops, smart phones, tablets, TVs, gaming consoles, Web cams, automobiles, environmental sensing devices, picture frames, and home electrical and security systems are being connected to the Internet.

“Fun” Internet-connected devices

Amazon Echo

Internet refrigerator

IP picture frame

Pacemaker & Monitor

Tweet-a-watt: monitor energy use

bikes

cars

scooters

Security Camera

Slingbox: remote control cable TV

Web-enabled toaster + weather forecaster

AR devices

Fitbit

Internet phones

Gaming devices

sensorized bed mattress

diapers

Others?

What's the Internet: "nuts and bolts" view

Indeed, the term *computer network* is beginning to sound a bit dated, given the many nontraditional devices that are being hooked up to the Internet.

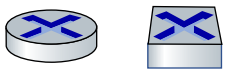
- In Internet jargon, all of these devices are called **hosts** or **end systems**. As of Sep 2021, there were billions of end systems attached to the Internet, not counting smart phones, laptops, and other devices that are only intermittently connected to the Internet. Overall, more there are an estimated 2 billion Internet users.

Jargon แปลว่า ศัพท์เฉพาะ

What's the Internet: "nuts and bolts" view

Billions of connected computing *devices*:

- *hosts* = *end systems*
- running *network apps* at Internet's "edge"



Packet switches: forward packets (chunks of data)

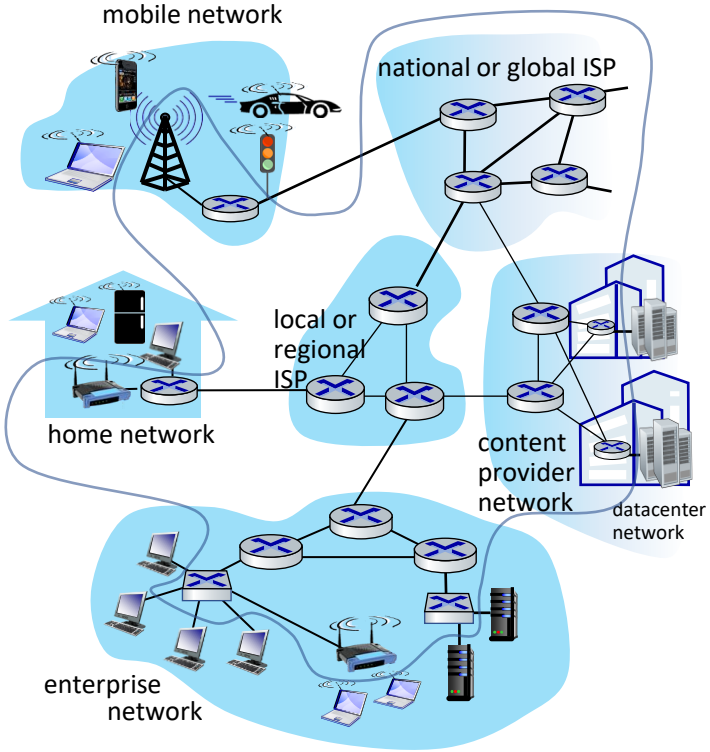
- *routers, switches*

Communication links

- fiber, copper, radio, satellite
- transmission rate: *bandwidth*

Networks

- collection of devices, routers, links: managed by an organization



What's the Internet: "nuts and bolts" view

- End systems are connected together by a network of **communication links** and **packet switches**. that there are many types of communication links, which are made up of different types of physical media, including coaxial cable, copper wire, optical fiber, and radio spectrum.

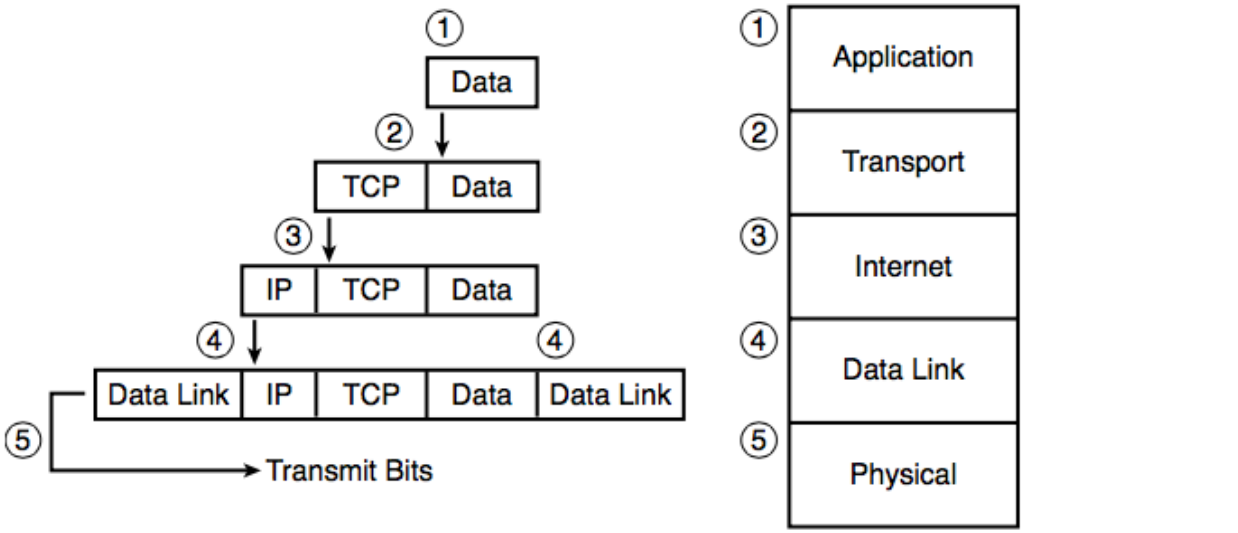
- Different links can transmit data at different rates, with the **transmission rate** of a link measured in bits/second.

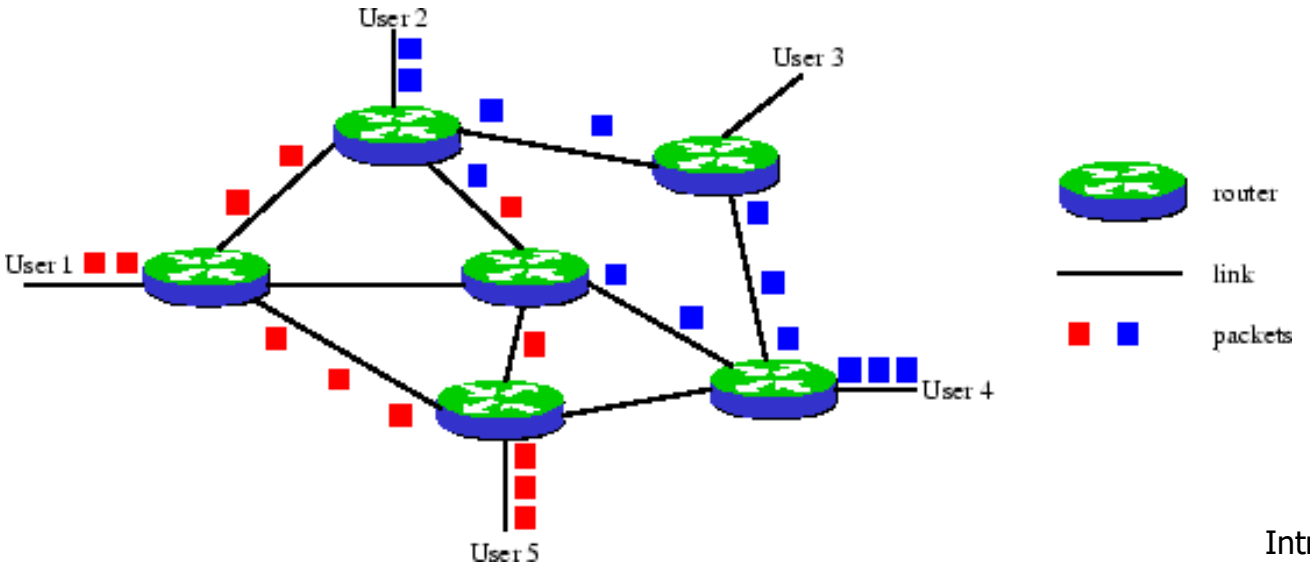
What's the Internet: "nuts and bolts" view

- When one end system has data to send to another end system, the sending end system segments the data and adds header bytes to each segment.

- The resulting packages of information, known as **packets** in the jargon of computer networks, are then sent through the network to the destination end system, where they are reassembled into the original data.

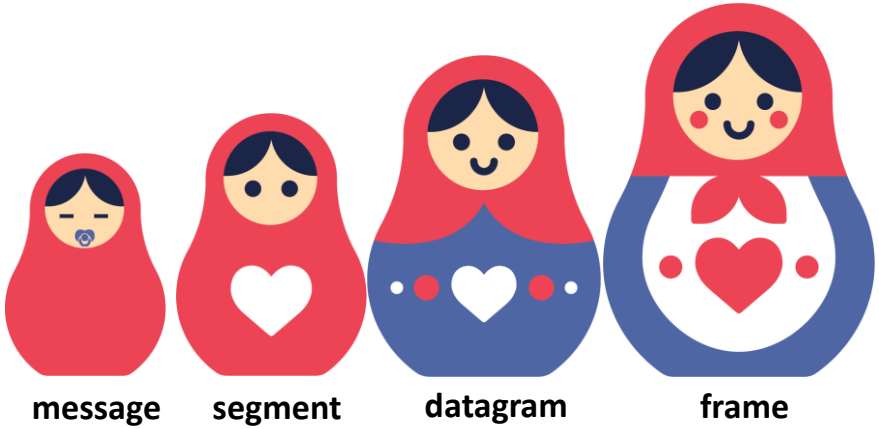
Encapsulation





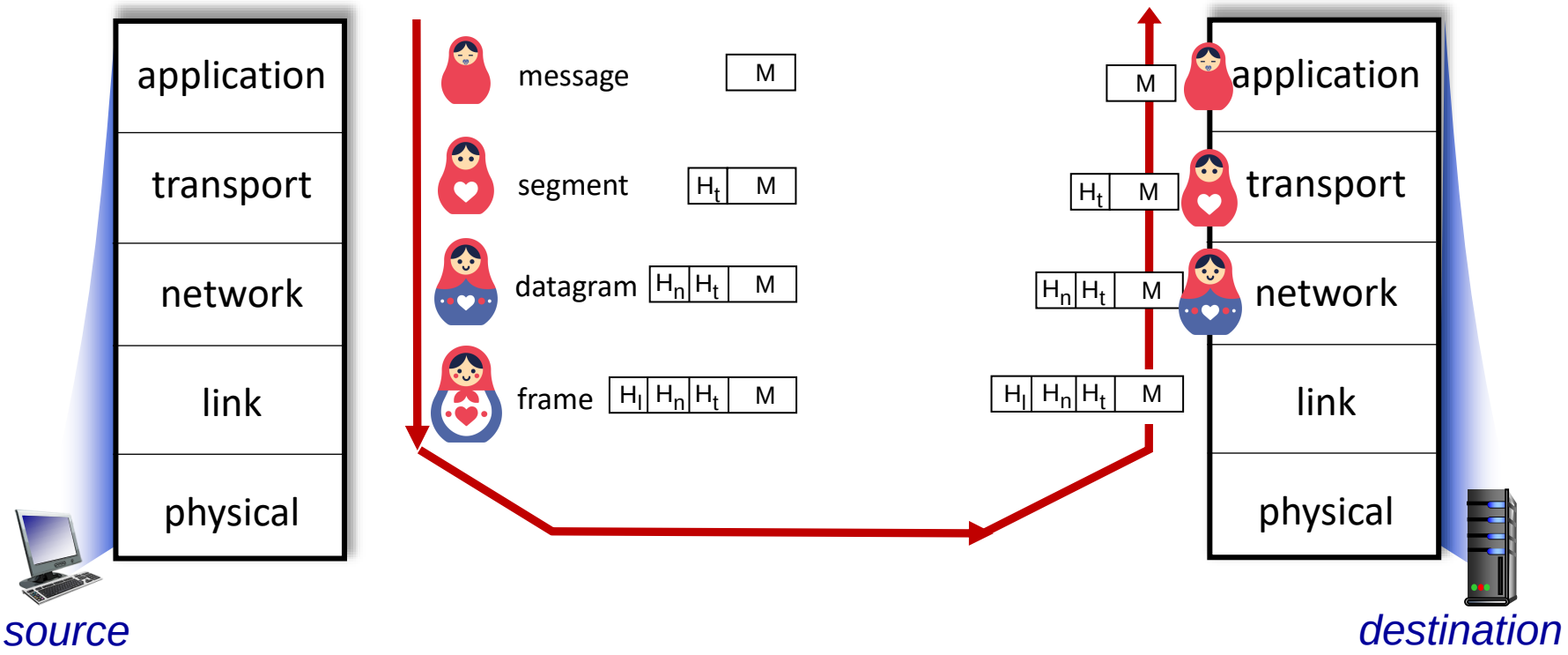
Encapsulation

Matryoshka dolls (stacking dolls)



Credit: https://dribbble.com/shots/7182188-Babushka-Boi

Services, Layering and Encapsulation



What's the Internet: "nuts and bolts" view

A packet switch takes a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links.

Packet switches come in many shapes and flavors, but the two most prominent types in today's Internet are **routers** and **link-layer switches**.

- Both types of switches forward packets toward their ultimate destinations. Link-layer switches are typically used in **access networks**, while routers are typically used in the **network core**. **

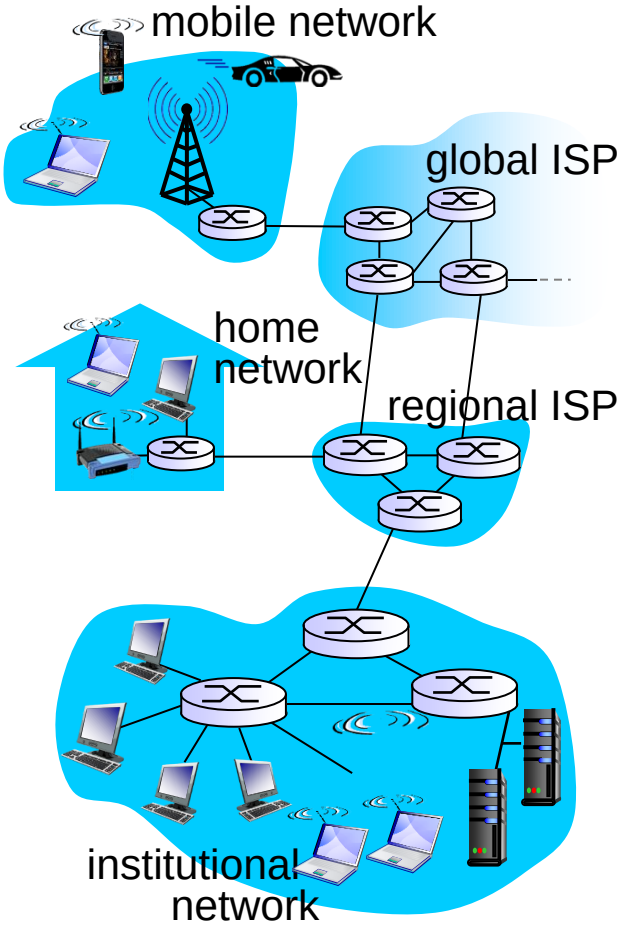
What's the Internet: "nuts and bolts" view

The sequence of communication links and packet switches traversed by a packet from the sending end system to the receiving end system is known as a **route** or **path** through the network.

- End systems access the Internet through **Internet Service Providers (ISPs)**, including residential ISPs such as local cable or telephone companies; Corporate ISPs; university ISPs; and ISPs that provide WiFi access in airports, hotels, coffee shops, and other public places.

What's the Internet: "nuts and bolts" view

Each ISP is in itself a network of packet switches and communication links. ISPs provide a variety of types of network access to the end systems, including residential broadband access such as cable modem or DSL, high-speed local area network access, wireless access, and 56 kbps dial-up modem access.

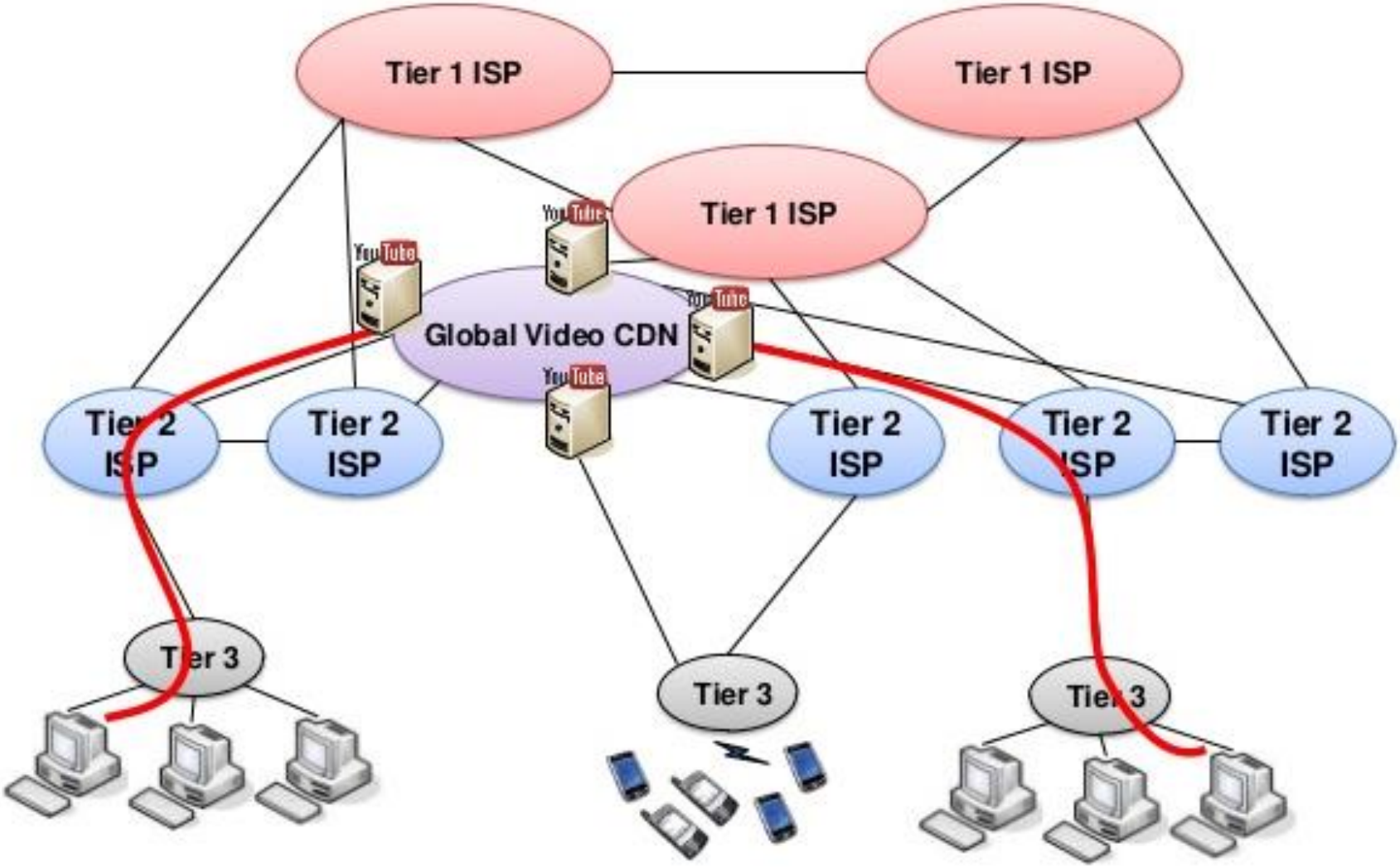


- ISPs also provide Internet access to **content providers**, connecting Web sites directly to the Internet. The Internet is all about connecting end systems to each other, so the ISPs that provide access to end systems must also be interconnected.

What's the Internet: "nuts and bolts" view

- These lower-tier ISPs are interconnected through national and international upper-tier ISPs such as Level 3 Communications (USA), AT&T (USA), Sprint (USA), and NTT(Japan).

- An upper-tier ISP consists of high-speed routers interconnected with high-speed fiber-optic links. Each ISP network, whether upper-tier or lower-tier, is managed independently, runs the **IP protocol**, and conforms to certain naming and address conventions.

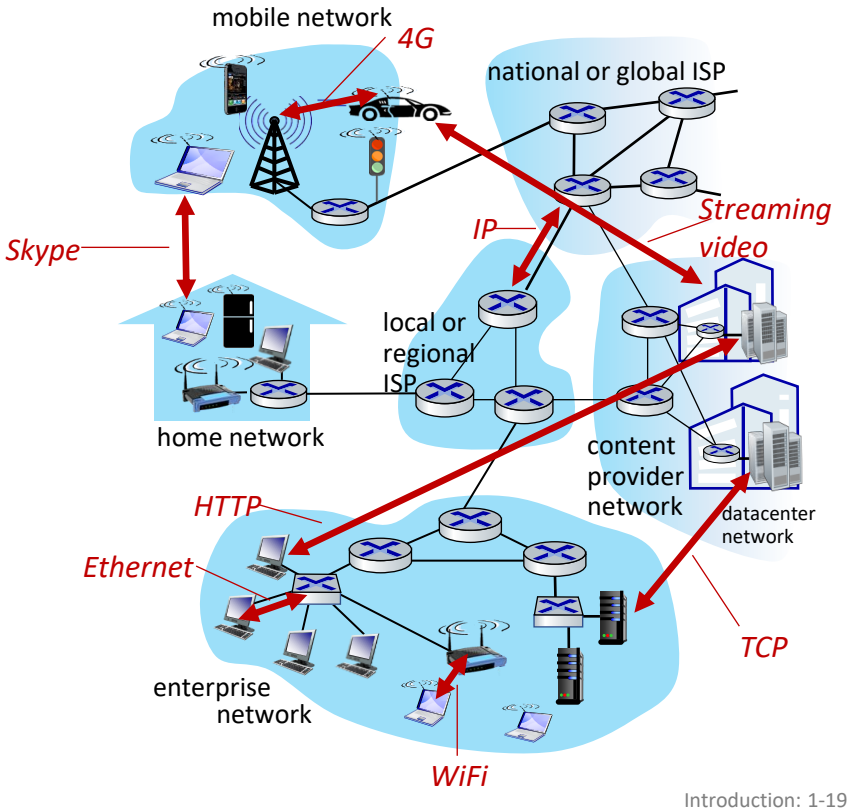

Tier 1 ISP
Tier 1 ISP
Tier 1 ISP
Global Video CDN
Tier 2 ISP
Tier 2 ISP
Tier 2 ISP
Tier 2 ISP
Tier 2 ISP
Tier 3
Tier 3
Tier 3

List of Tier 1 networks

Name	Headquarters	AS number	CAIDA AS rank[10]	Fiber route (km)	Peering policy
AT&T[11]	United States	7018	26	660,000[12]	AT&T Peering policy
Comcast[13]	United States	7922	31	150,000[14]	Comcast Interconnection Policy
Deutsche Telekom Global Carrier[15]	Germany	3320	19	250,000[16]	DTAG Peering Details
GTT Communications	United States	3257	7	232,934[17][18]	GTT Peering Policy
Liberty Global[19][20]	The Netherlands[21]	6830	21	800,000[22]	Peering Principles
Lumen Technologies (formerly CenturyLink, formerly Level 3)[23][24][25]	United States	3356	1	885,139[26][27]	Lumen Peering Policy
NTT Communications (formerly Verio)[28]	Japan	2914	6	?	Global Peering Policy
Orange[29]	France	5511	13	495,000 [30]	OTI peering policy
PCCW Global	Hong Kong	3491	10	?	Peering policy
T-Mobile US (formerly Sprint)[31]	United States	1239	20	30,000[32]	Peering policy
Tata Communications (formerly Teleglobe)[33]	India	6453	9	700,000[34]	Peering Policy
Telecom Italia Sparkle (Seabone)[35]	Italy	6762	5	560,000	Peering Policy
Arelion (formerly Telia Carrier)[36]	Sweden	1299	2	70,000[37]	Arelion's IP Network Peering Policy
Telxius (Subsidiary of Telefónica)[38]	Spain	12956	15	65,000[39]	Peering Policy
Verizon Enterprise Solutions (formerly UUNET)[44]	United States	701	24	805,000[45]	Verizon UUNET Peering policy 701, 702, 703
Zayo Group (formerly AboveNet)[46]	United States	6461	8	196,339[47]	Zayo Peering Policy

What's the Internet: "nuts and bolts" view

- *Internet:* "network of networks"
  - Interconnected ISPs
- *protocols* are *everywhere*
  - control sending, receiving of messages
  - e.g., HTTP (Web), streaming video, Skype, TCP, IP, WiFi, 4/5G, Ethernet
- *Internet standards*
  - RFC: Request for Comments
  - IETF: Internet Engineering Task Force



What's the Internet: "nuts and bolts" view

- End systems, packet switches, and other pieces of the Internet run **protocols** that *control the sending and receiving of information within the Internet*. The **Transmission Control Protocol (TCP)** and the **Internet Protocol (IP)** are two of the most important protocols in the Internet.

- The IP protocol *specifies the format of the packets that are sent and received among routers and end systems*.

- The Internet's principal protocols are collectively known as **TCP/IP**.

What's the Internet: "nuts and bolts" view

- **Internet standards** are developed by the **Internet Engineering Task Force** (IETF)[IETF 2012].

- The IETF standards documents are called **requests for comments (RFCs)**. RFCs started out as general requests for comments (hence the name) to resolve network and protocol design problems that faced the precursor to the Internet [Allman 2011].

- RFCs tend to be quite technical and detailed. They define protocols such as TCP, IP, HTTP (for the Web), and SMTP (for e-mail). There are currently more than 6,000 RFCs.

Review

- อุปกรณ์ใดไม่ถือว่าเป็น End systems

  Desktop Workstation Web Server Environmental sensing devices Link-Layer Switch

- ข้อใดไม่ใช่ Communication Link

  Coaxial cable Copper wire Optical fiber Router Radio wave

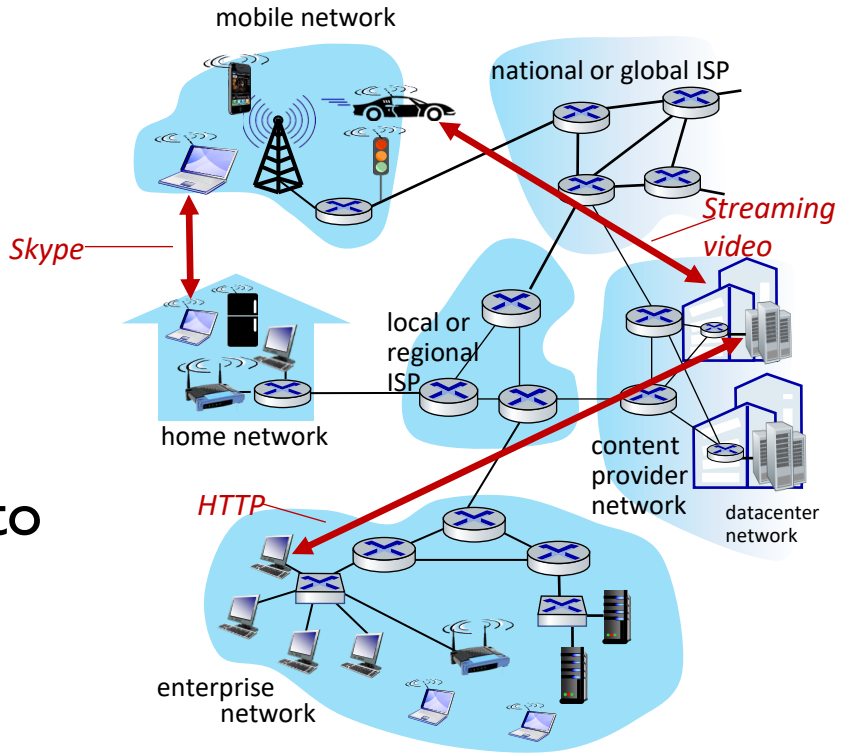
- เอกสาร Requests for comments ออกโดยหน่วยงานใด

  IEEE ITU IETF IFET ANSI

- จงยกตัวอย่าง Content Provider
- What is the difference between a host and an end system?
- List several different types of end systems.
- Is a Web server an end system?

What's the Internet: a service view

- *Infrastructure* that provides services to applications:
  - Web, streaming video, multimedia teleconferencing, email, games, e-commerce, social media, inter-connected 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



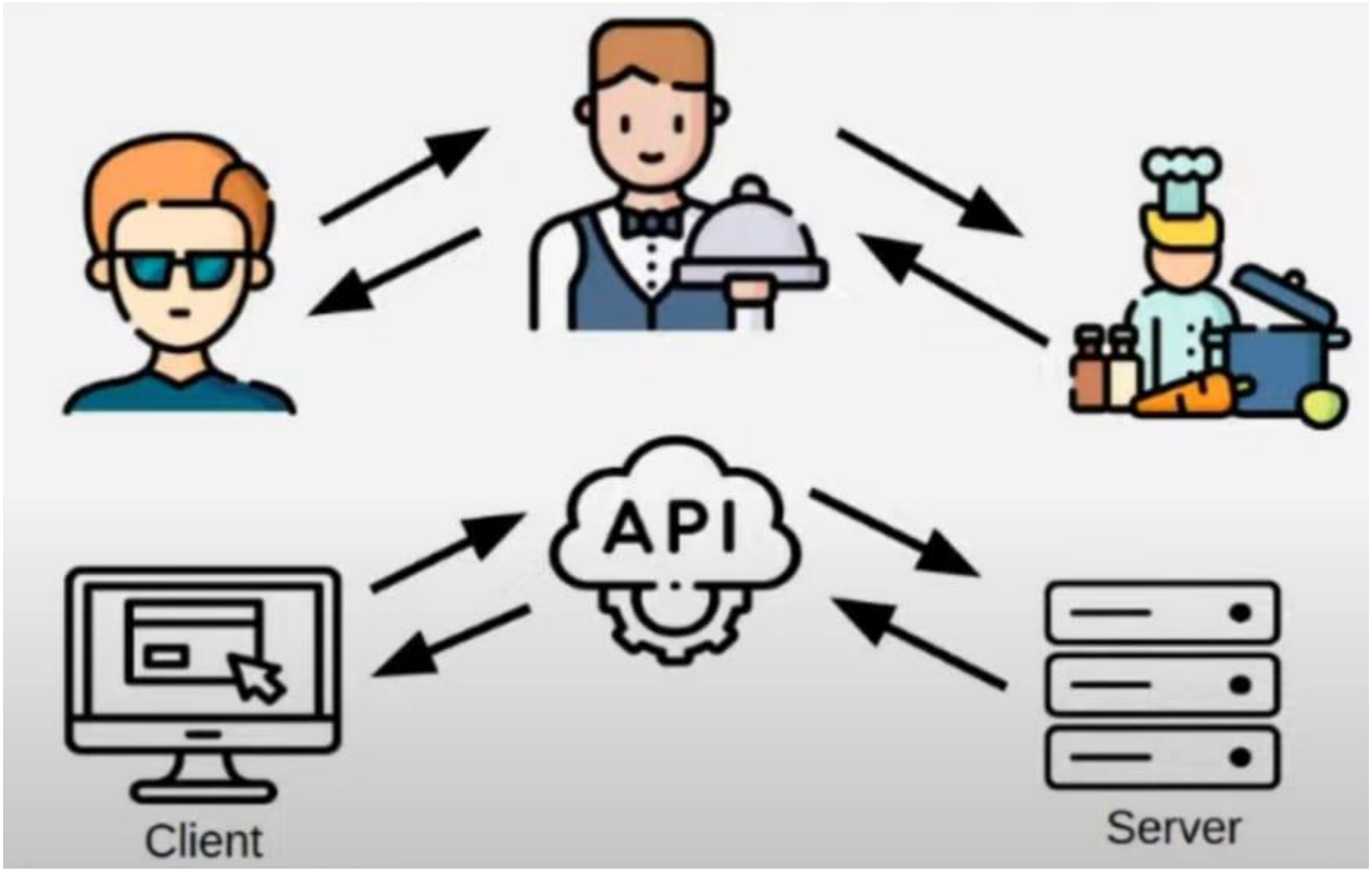
What's the Internet: a service view

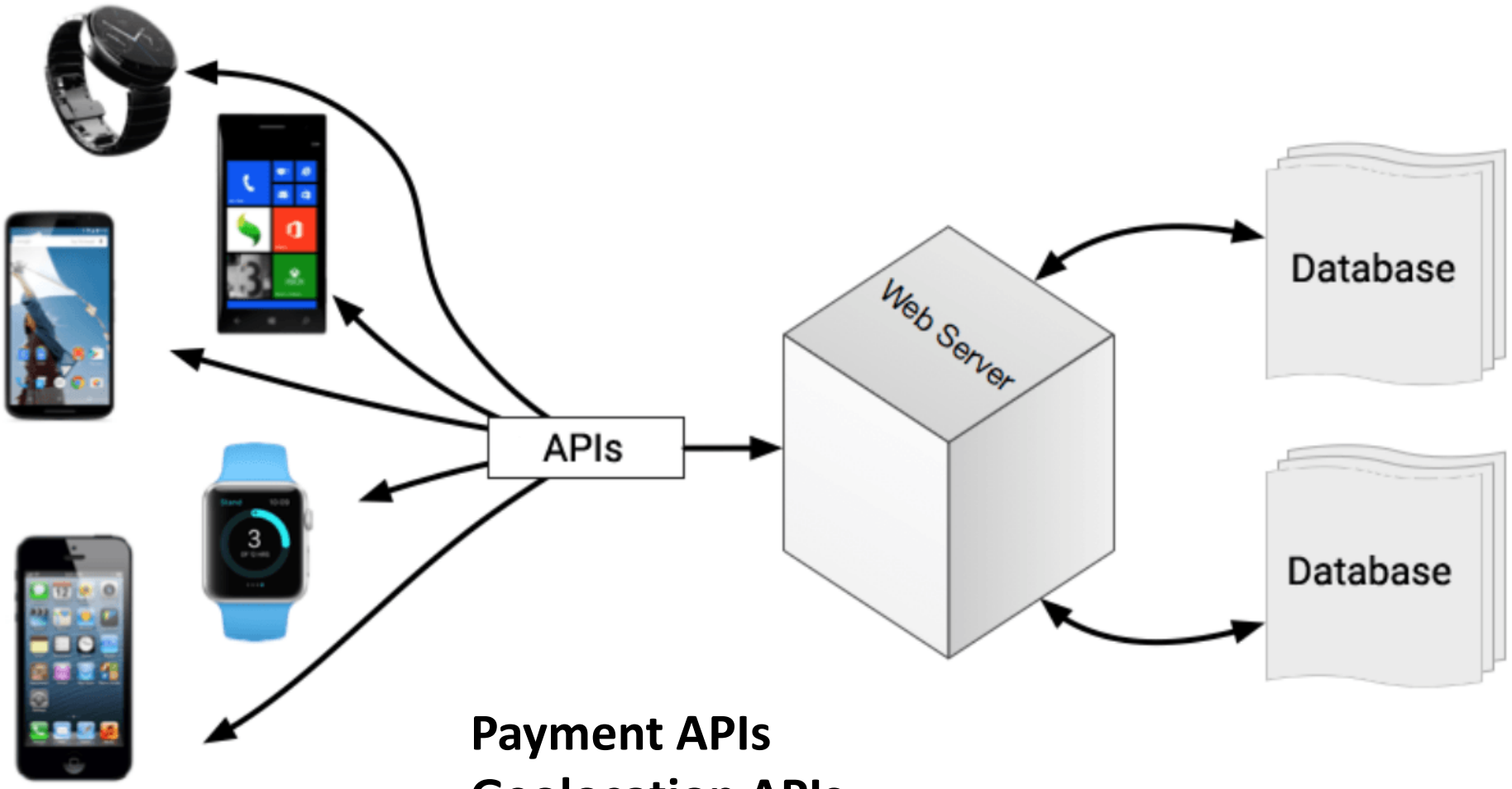
- The applications are said to be **distributed applications**, since they involve multiple end systems that exchange data with each other. Importantly, Internet applications run on end systems—they do not run in the packet switches in the network core.

- End systems attached to the Internet provide an **Application Programming Interface (API)** that specifies how a program running on one end system asks the Internet infrastructure to deliver data to a specific destination program running on another end system.

- Example: Alice wants to send a letter to Bob using the postal service. drop the envelope into an official postal service mailbox

  Thus, the postal service has its own "postal service API," or set of rules, that Alice must follow to have the postal service deliver her letter to Bob.


API
Client
Server



Payment APIs
Geolocation APIs
Chat APIs
…

2. What's a protocol?

human protocols:

- "what's the time?"
- "I have a question"
- introductions

… specific msgs sent

… specific actions taken when msgs received, or other events

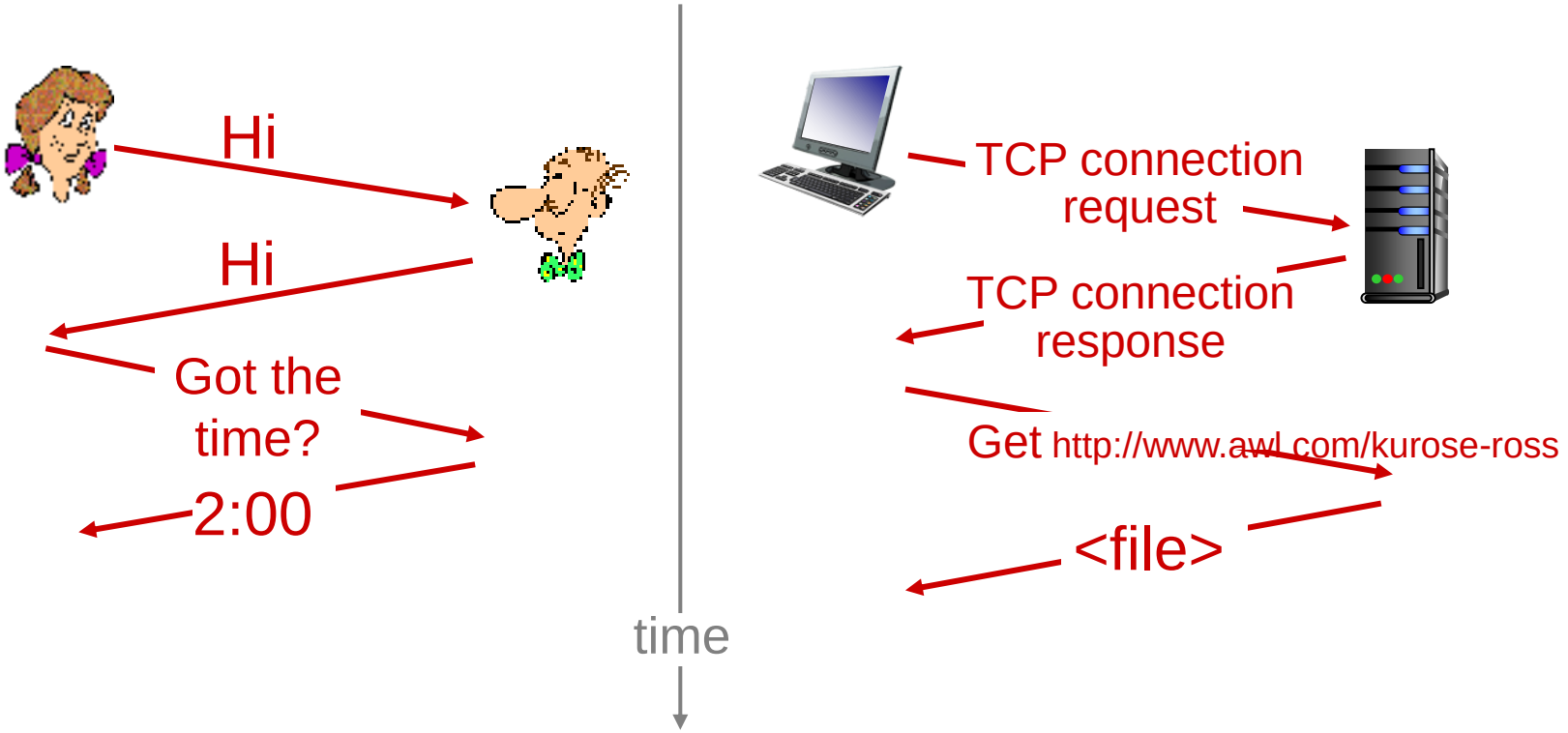
network protocols:

- machines rather than humans
- all communication activity in Internet governed by protocols

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

What's a protocol?

a human protocol and a computer network protocol:



Q: other human protocols?

3. Network Edge

- We begin in this section at the edge of a network and look at the components with which we are most familiar—namely, the computers, smartphones and other devices that we use on a daily basis.

- Furthermore, an increasing number **of non-traditional devices** are being attached to the Internet as end systems

- IP-enabled phones with GPS capabilities put location-dependent services (maps, information about nearby services or people) at your fingertips. Networked sensors embedded into the physical environment allow monitoring of buildings, bridges, seismic activity, wildlife habitats, river estuaries, and the weather. Biomedical devices can be embedded and networked in a body-area network. With so many diverse devices being networked together, the Internet is indeed becoming an "**Internet of things**" [ITU 2005b].

- In the next section we'll move from the network edge to the network core and examine switching and routing in computer networks.

Network Edge

- End systems are also referred to as *hosts* because they host (that is, run) application programs such as a Web browser program, a Web server program, an e-mail client program, or an e-mail server program. Throughout this book we will use the terms hosts and end systems interchangeably; that is, *host = end system*.

- Hosts are sometimes further divided into two categories: **clients** and **servers**. Informally, clients tend to be desktop and mobile PCs, smart phones, and so on, whereas servers tend to be more powerful machines that store and distribute Web pages, stream video, relay e-mail, and so on.

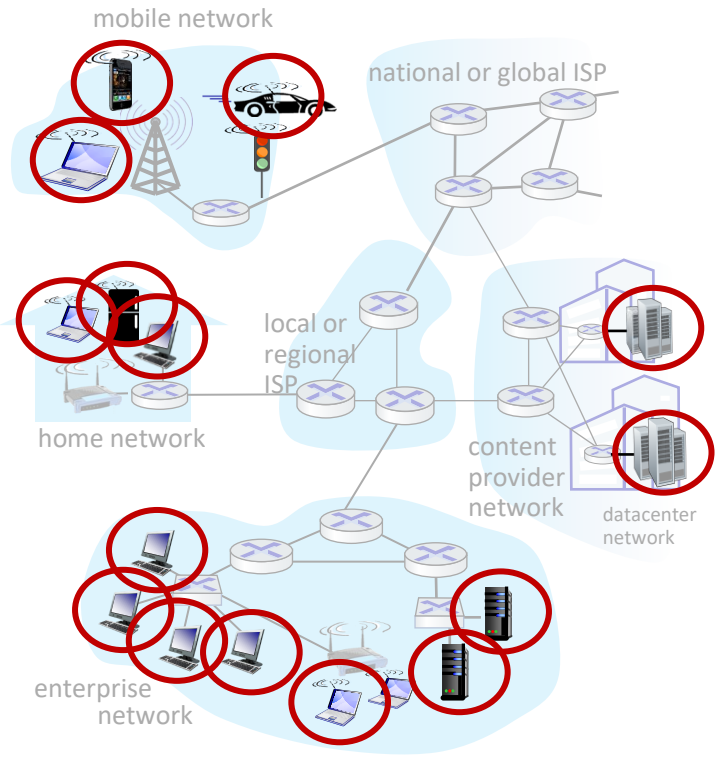
- Today, most of the servers from which we receive search results, e-mail, Web pages, and videos reside in large **data centers**. For example, Google has 30–50 data centers, with many having more than one hundred thousand servers.

Google data centers

A closer look at Internet structure

Network edge:

- hosts: clients and servers
- servers often in data centers



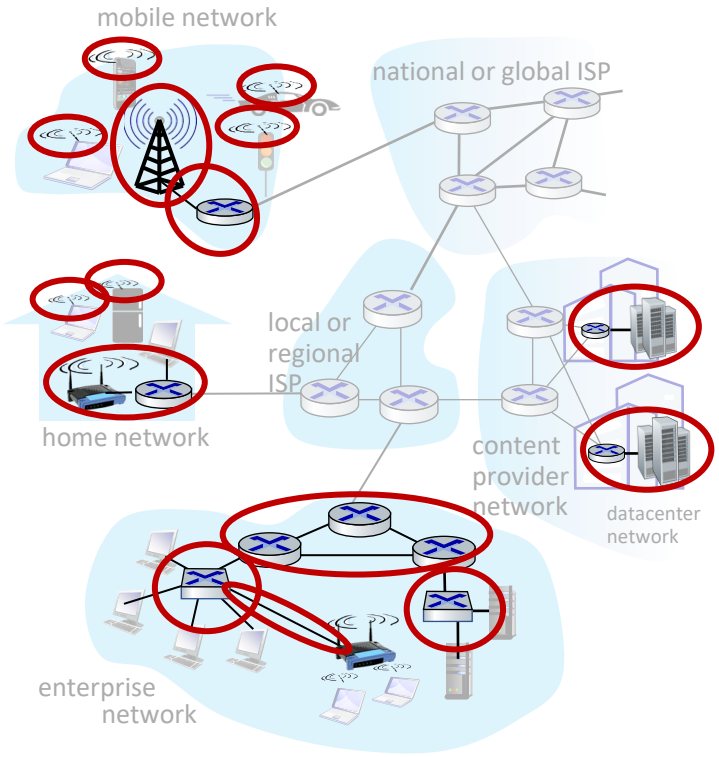
A closer look at Internet structure

Network edge:

- hosts: clients and servers
- servers often in data centers

Access networks, physical media:

- wired, wireless communication links



A closer look at Internet structure

Network edge:

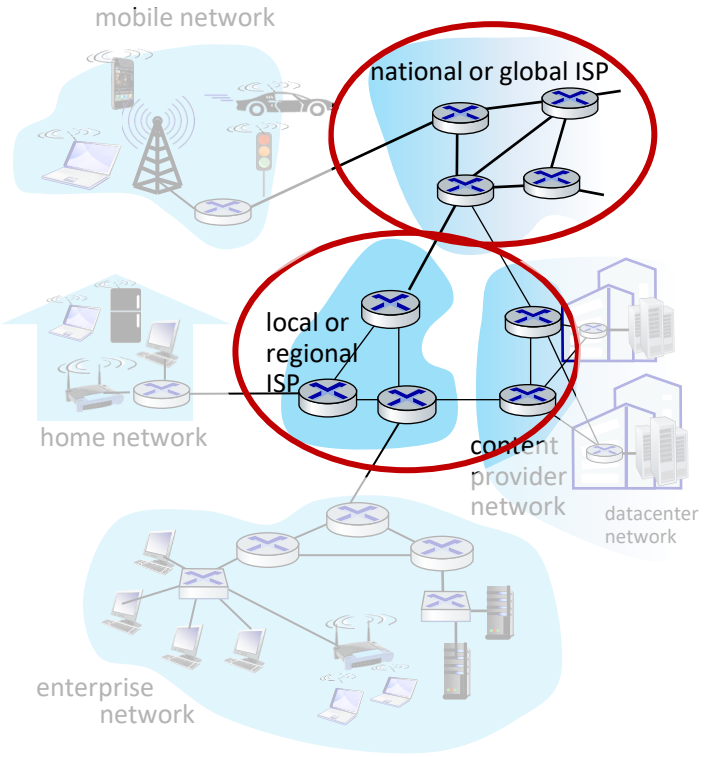
- hosts: clients and servers
- servers often in data centers

Access networks, physical media:

- wired, wireless communication links

Network core:

- interconnected routers
- network of networks



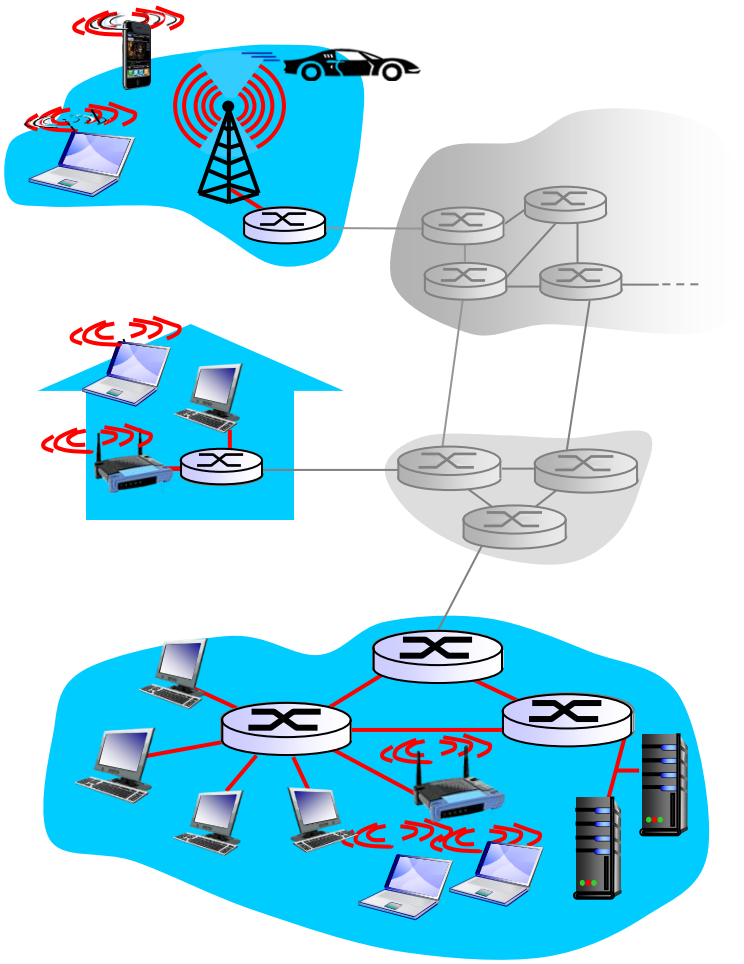
4. Access networks and physical media

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 networks and physical media

- **Access Network**
  - Home Access: DSL, Cable, FTTH, Dial-Up, and Satellite
  - Access in the Enterprise (and the Home): Ethernet and WiFi
  - Wide-Area Wireless Access: 3G and LTE

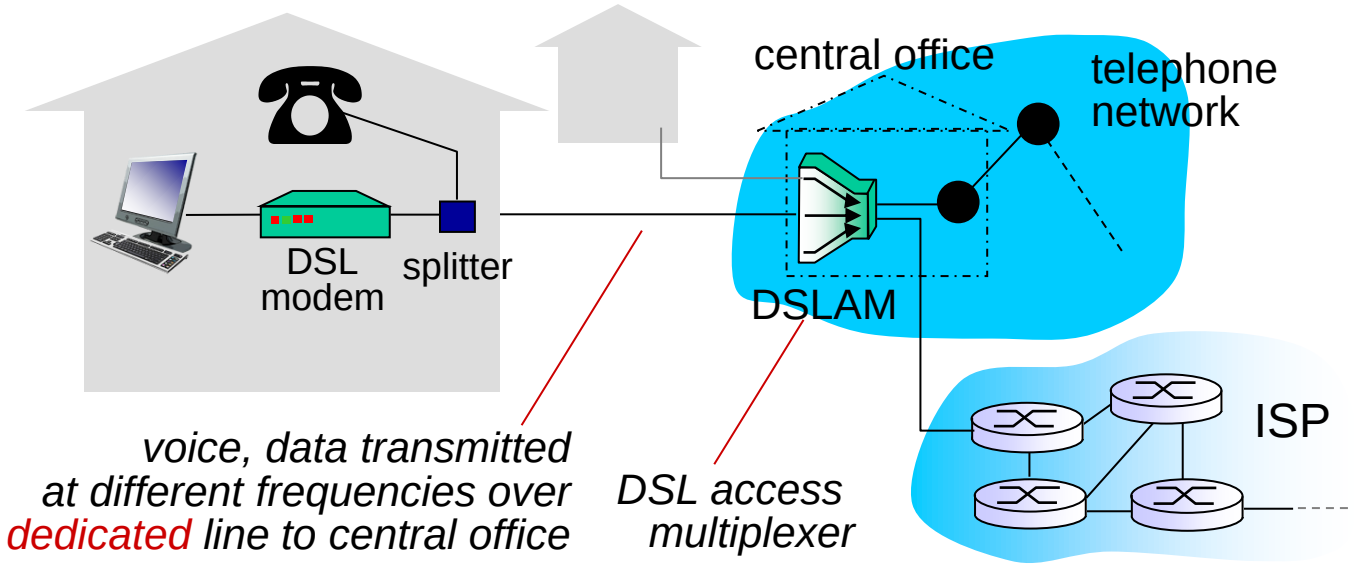
- **Physical Media**

  Physical media fall into two categories:

  guided media

  unguided media

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
- 3.5-16 Mbps upstream transmission rate
- 24- 52 Mbps downstream transmission rate

Access net: digital subscriber line (DSL)

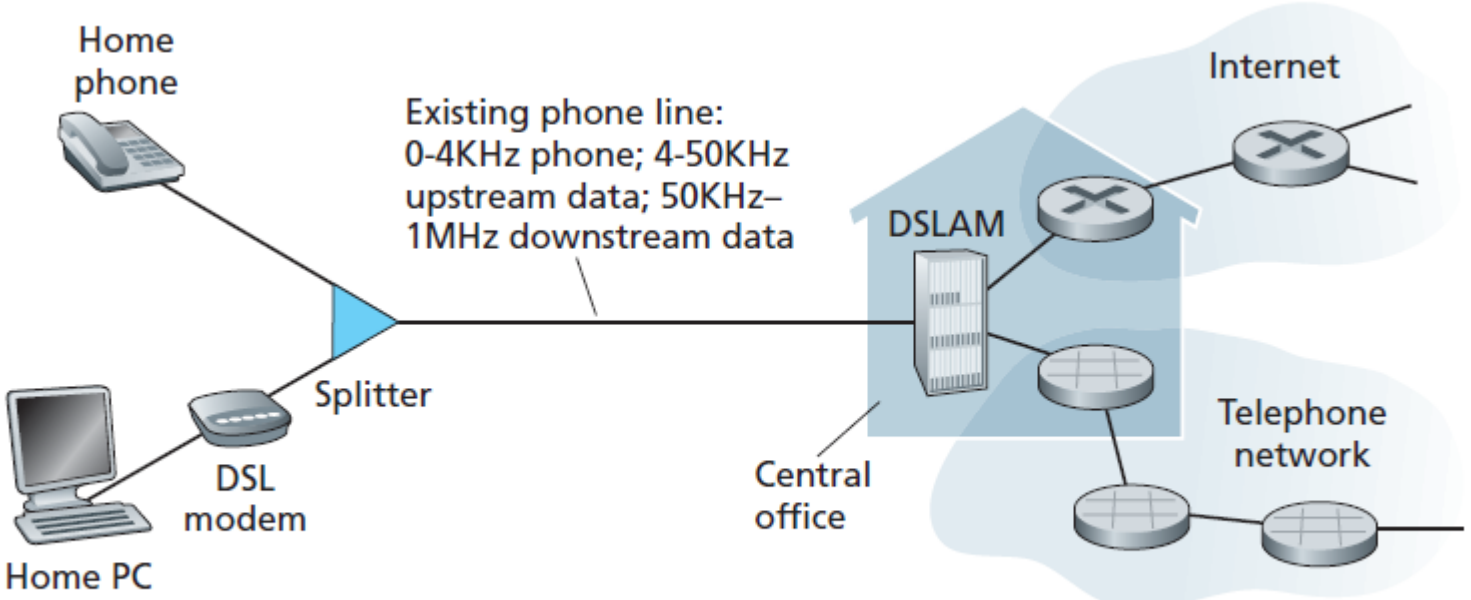
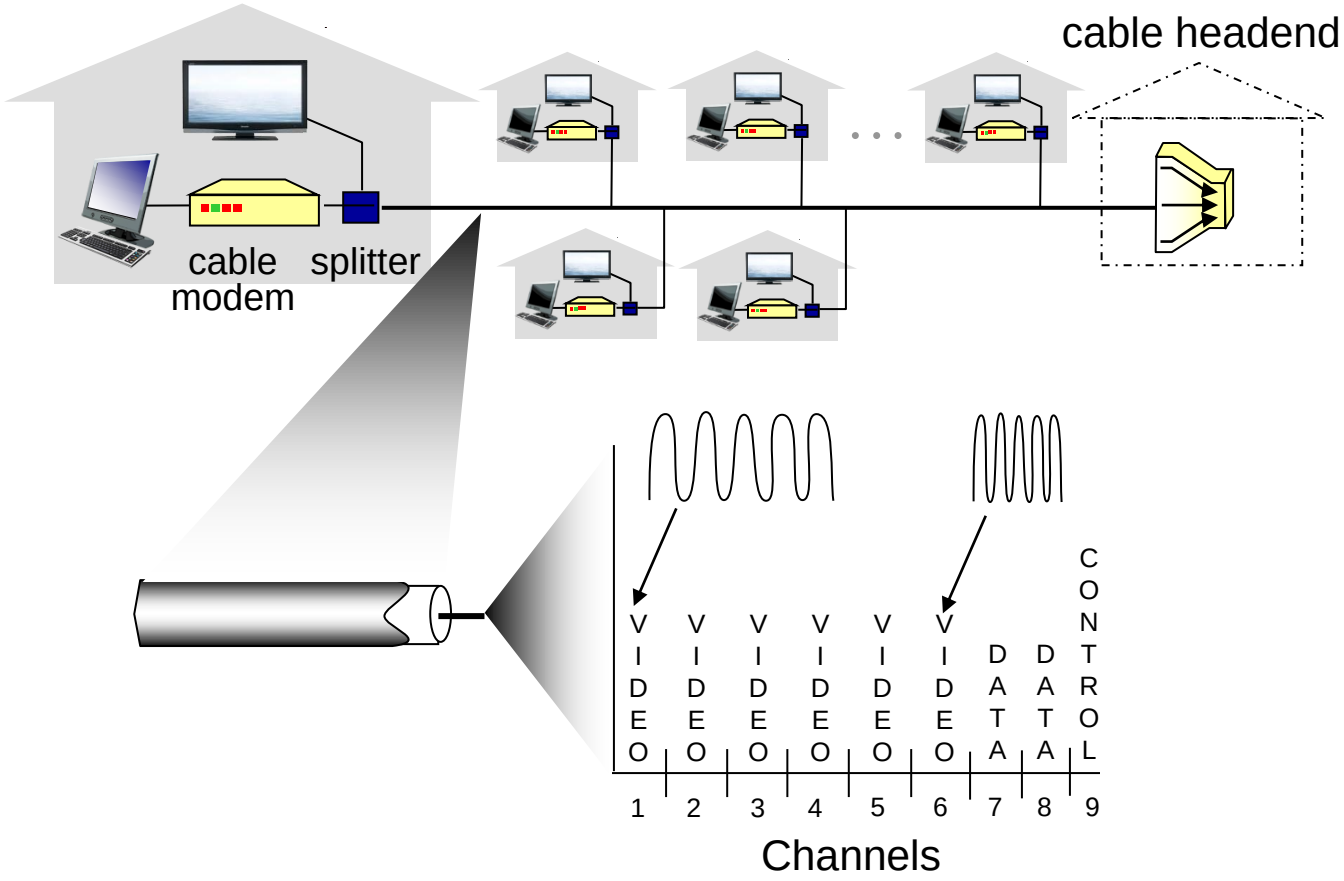


Figure 1.5 ♦ DSL Internet access

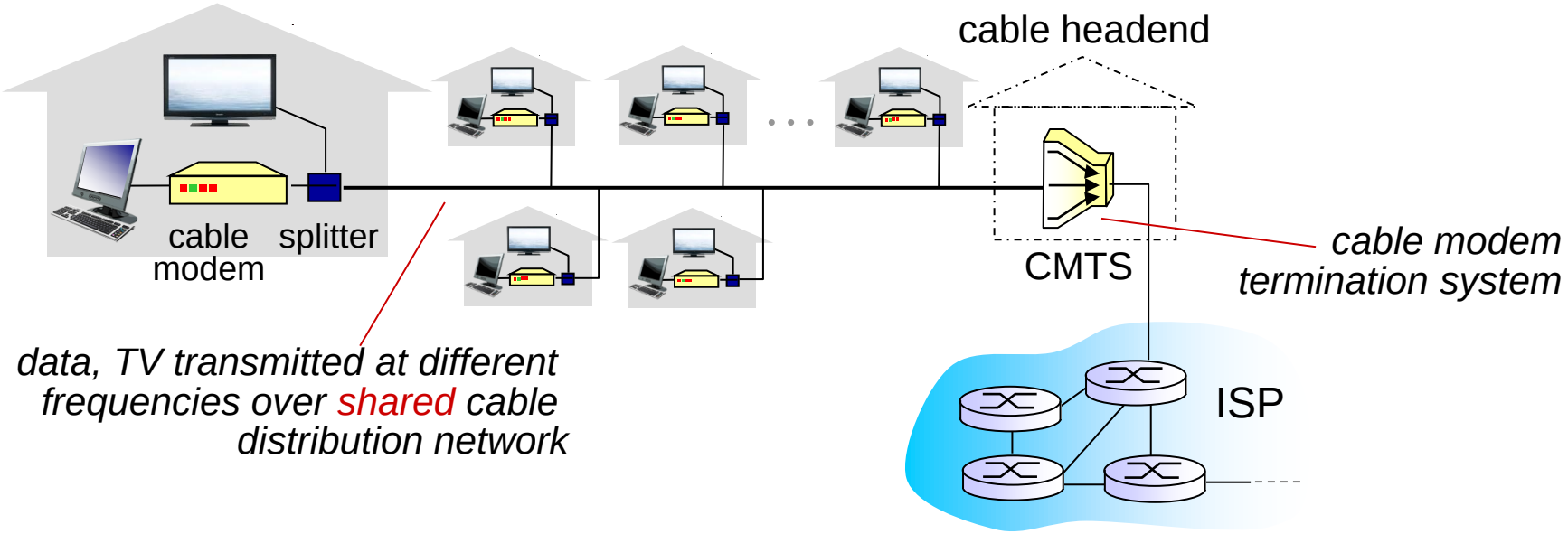
DSLAM separates the data and phone signals and sends the data into the Internet

Access net: cable network



frequency division multiplexing: different channels transmitted in different frequency bands

Access net: cable network



- HFC: hybrid fiber coax
  - asymmetric: up to 40 Mbps -1.2Gbps 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
  - unlike DSL, which has dedicated access to central office

Access net: cable network HFC

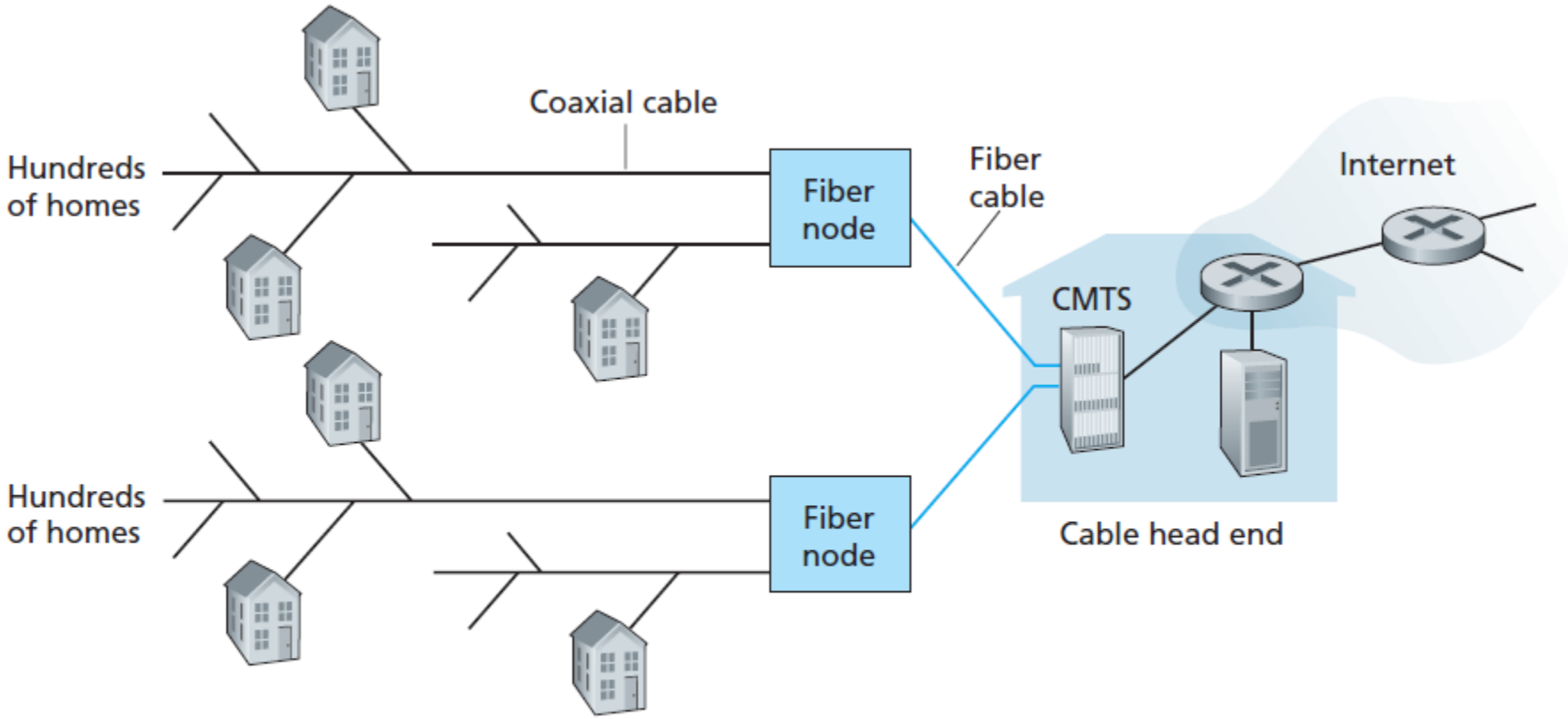


Figure 1.6 ♦ A hybrid fiber-coaxial access network

FTTH (Fiber to the home) Internet access

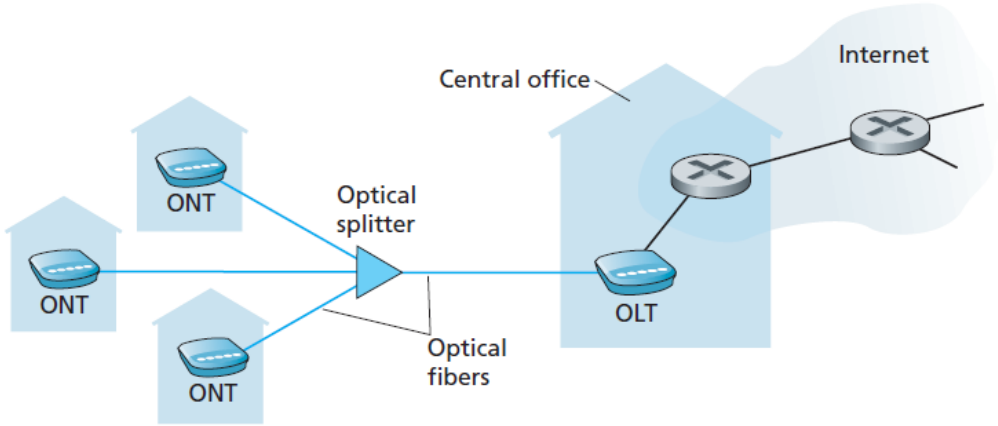


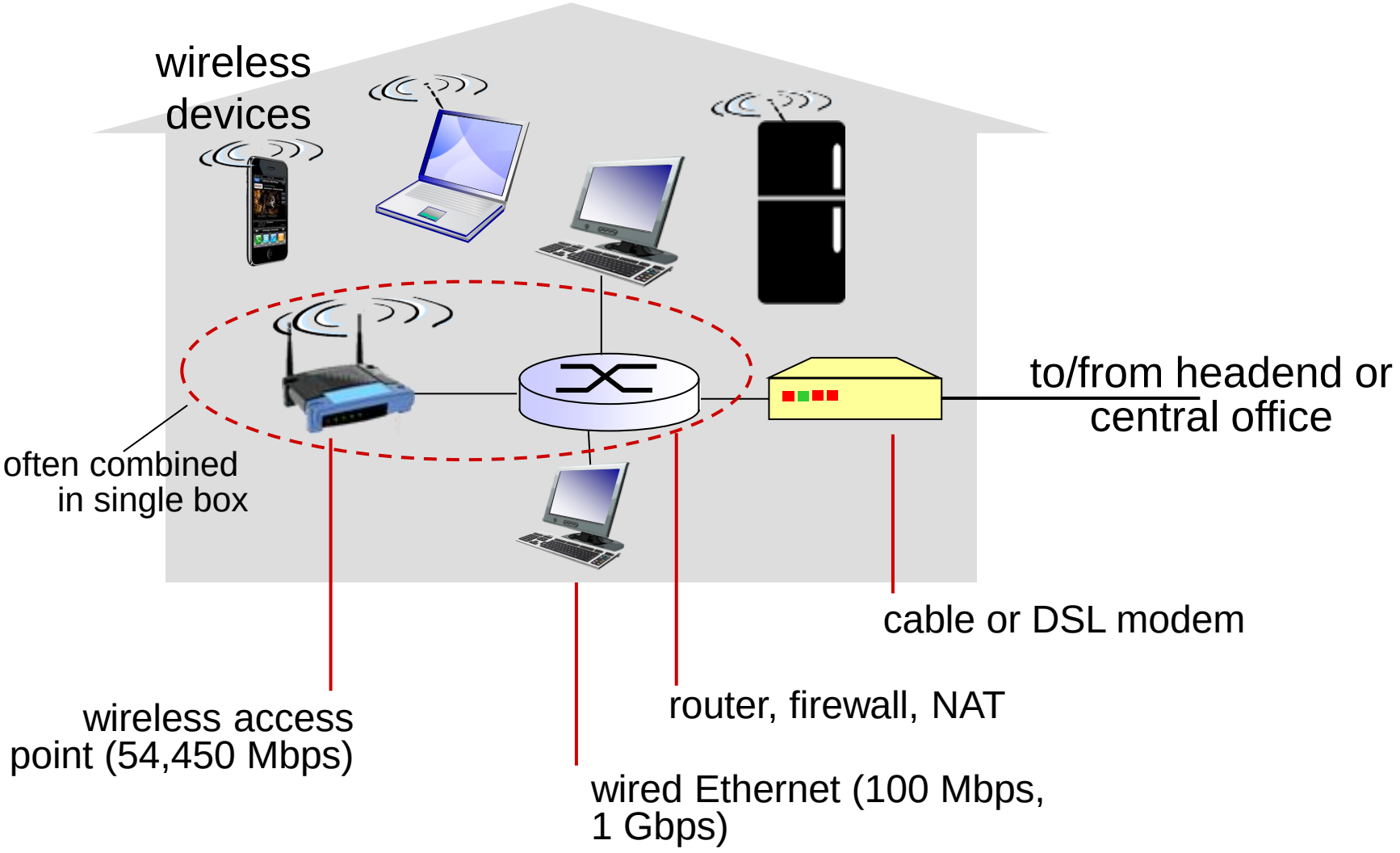
Figure 1.7 ♦ FTTH Internet access

Two other access network technologies are also used to provide Internet access to the home. In locations where DSL, cable, and FTTH are not available (e.g., in some rural settings),

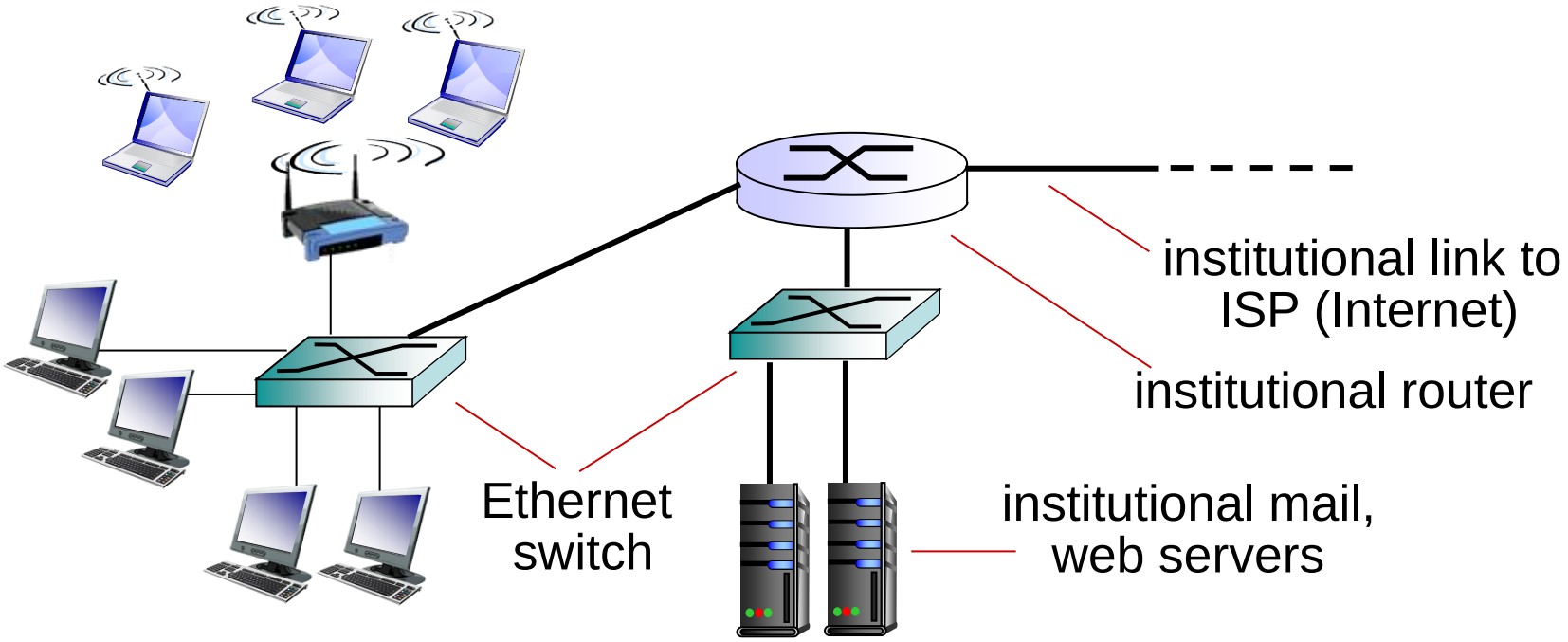
a satellite link can be used to connect a residence to the Internet at speeds of more than 1 Mbps; StarBand and HughesNet are two such satellite access providers.

Dial-up access over traditional phone lines is based on the same model as DSL

Access net: home network



Enterprise access networks (Ethernet)



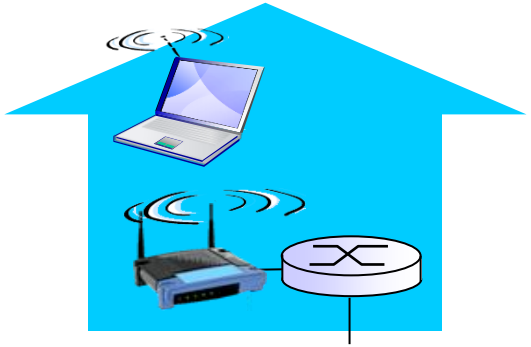
- typically used in companies, universities, etc
- mix of wired, wireless link technologies, connecting a mix of switches and routers (we'll cover differences shortly)
  - 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
  - WiFi: wireless access points at 11, 54, 450 Mbps

Wireless access networks

- shared *wireless* access network connects end system to router
  - via base station aka "access point"

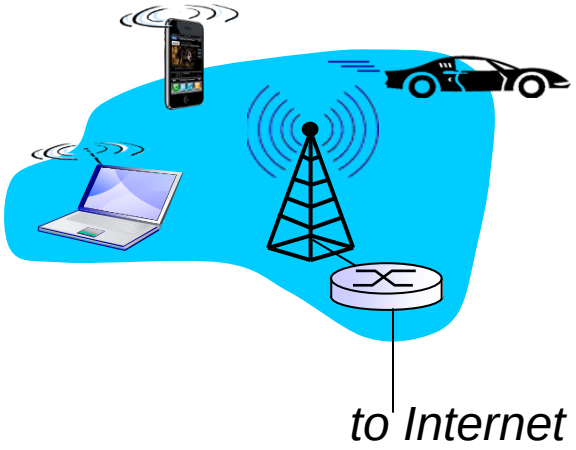
wireless LANs:

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



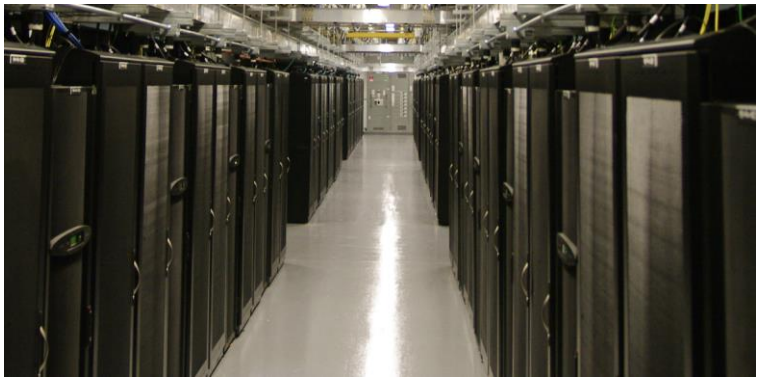
wide-area wireless access

- provided by telco (cellular) operator, 10's km
- 10 Mbps
- 4G,5G Cellular networks

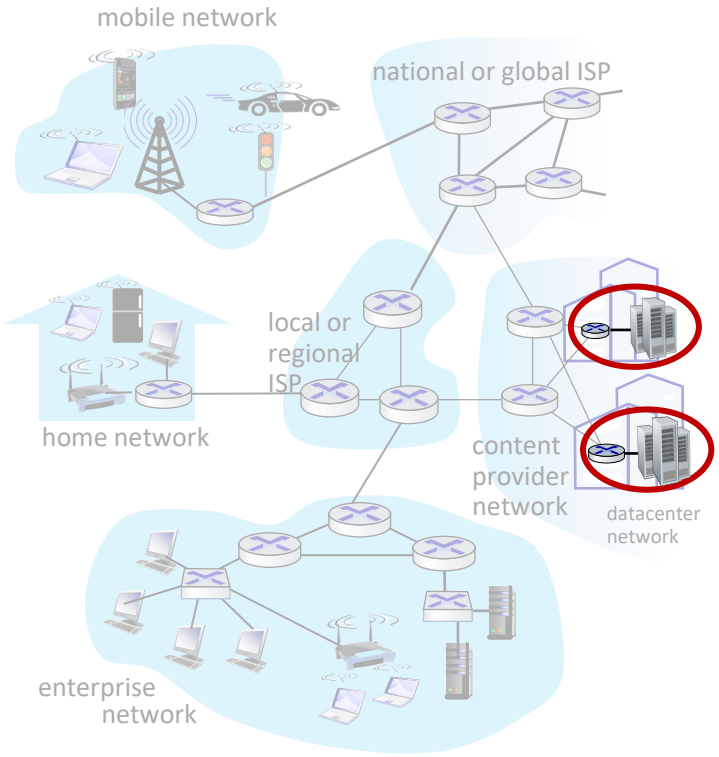


Access networks: data center networks

- high-bandwidth links (10s to 100s Gbps) connect hundreds to thousands of servers together, and to Internet



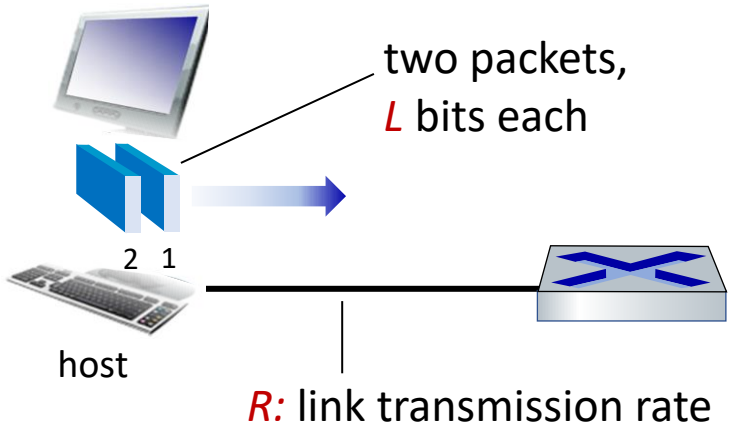
Courtesy: Massachusetts Green High Performance Computing Center (mghpcc.org)



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*
  - link transmission rate, aka link *capacity, aka link 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

- 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 propagate freely, e.g., radio

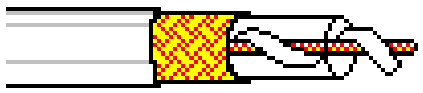
twisted pair (TP)

- two insulated copper wires
  - Category 5: 100 Mbps, 1 Gpbs Ethernet
  - Category 6: 10Gbps

Physical media: coax, fiber

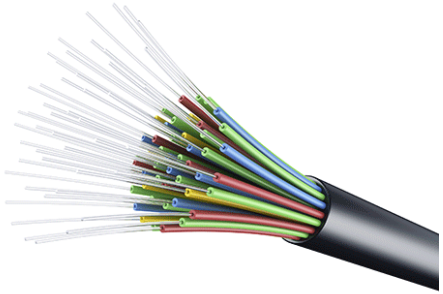
coaxial cable:

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



fiber optic cable:

- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10' s-100' s Gpbs transmission rate)
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise



Physical media: radio

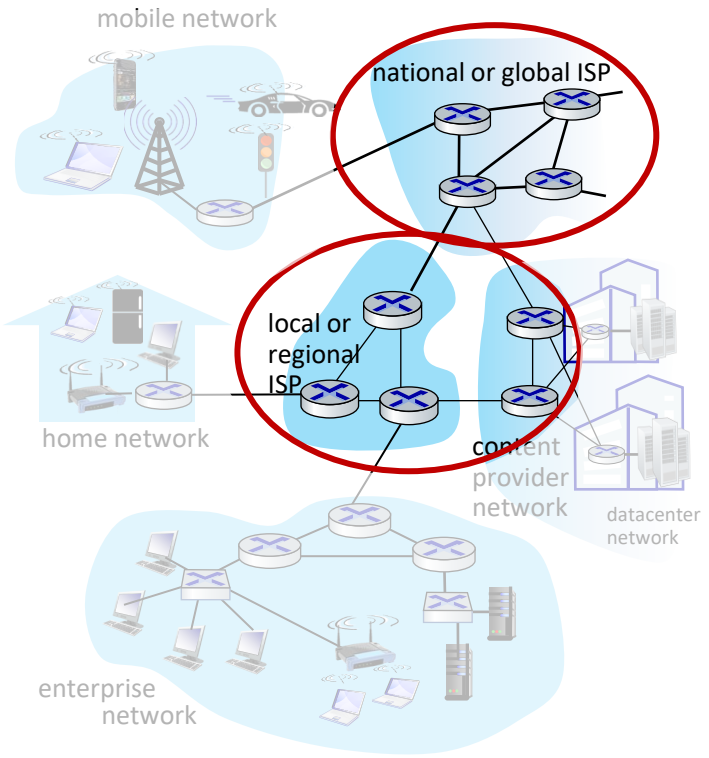
- signal carried in various band in electromagnetic spectrum
- no physical "wire"
- broadcast, "half-duplex" (sender to receiver)
- propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

radio link types:

- terrestrial microwave
  - point-to-point; 45 Mbps channels
- Wireless LAN (WiFi)
  - 10-100's Mbps; 10's of meters
- wide-area (e.g., 4G/5G cellular)
  - 10's Mbps (4G) over ~10 Km
- Bluetooth: cable replacement
  - short distances, limited rates
- satellite
  - up to < 100 Mbps (Starlink) downlink
  - 270 msec end-end delay
  - geosynchronous versus low altitude

5. The network core

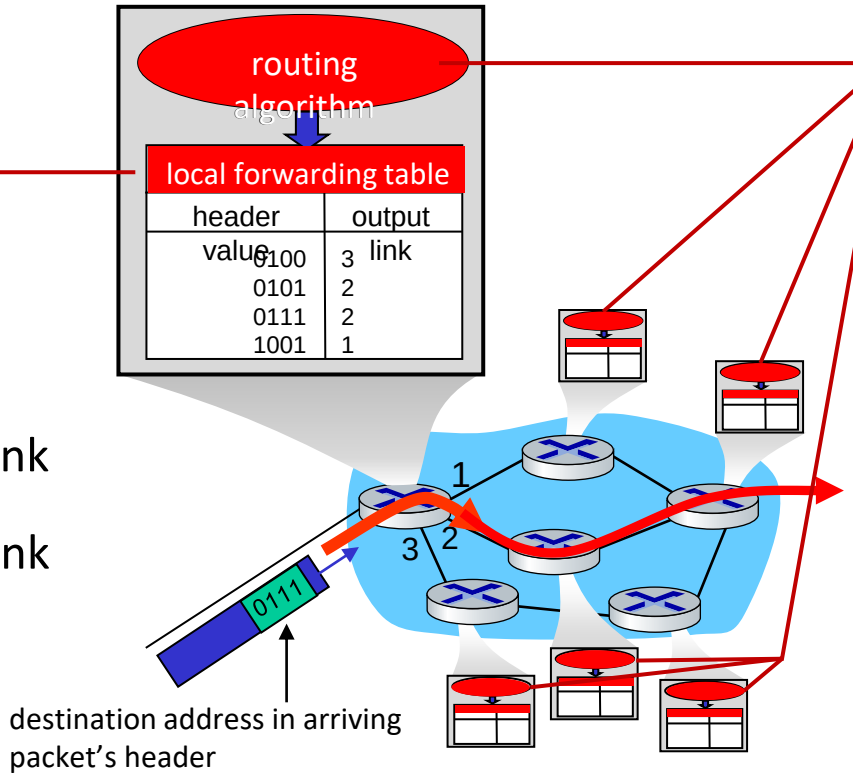
- mesh of interconnected routers
- packet-switching: hosts break application-layer messages into *packets*
  - network forwards packets from one router to the next, across links on path from source to destination



Two key network-core functions

Forwarding:

- aka "switching"
- *local* action: move arriving packets from router's input link to appropriate router output link



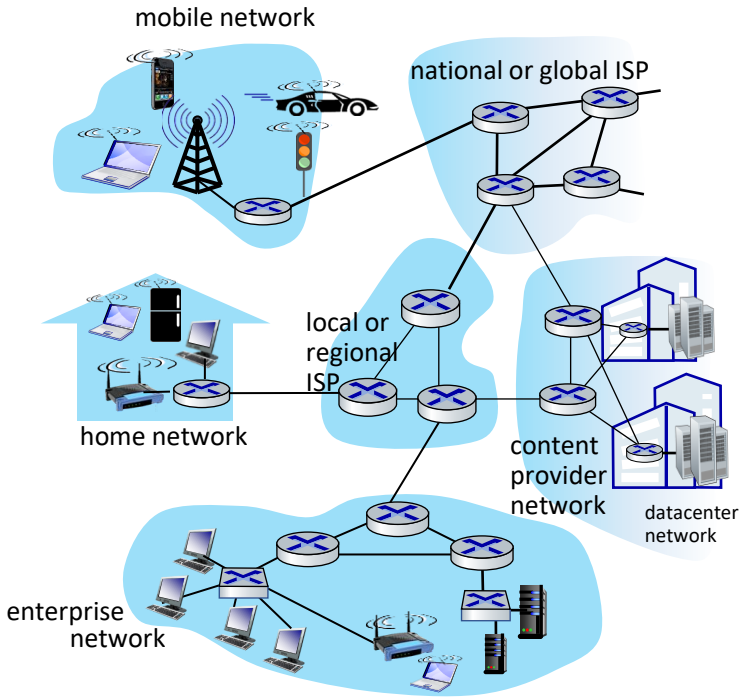
Routing:

- *global* action: determine source-destination paths taken by packets
- routing algorithms


routing
45 h
3,053 miles
48 h
3,309 miles
United States
San Jose
Northampton
Victoria
Seattle
Portland
Minneapolis
Chicago
Detroit
Toronto
Ottawa
Montreal
Quebec City
New York
Philadelphia
Indianapolis
Kansas City
Nashville
Atlanta
Charlotte
Dallas
Houston
Austin
San Antonio
New Orleans
Jacksonville
Orlando
Tampa
Las Vegas
Los Angeles
San Diego
Phoenix
Tucson
El Paso
WASHINGTON
OREGON
CALIFORNIA
NEVADA
IDAHO
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
SOUTH CAROLINA
NORTH CAROLINA
VIRGINIA
WEST VIRGINIA
PENNSYLVANIA
MARYLAND
DE
NJ
CT
RI
VERMONT
NEW HAMPSHIRE
MAINE
BAJA CALIFORNIA
SONORA
CHIHUAHUA
COAHUILA

6. Internet structure: a "network of networks"

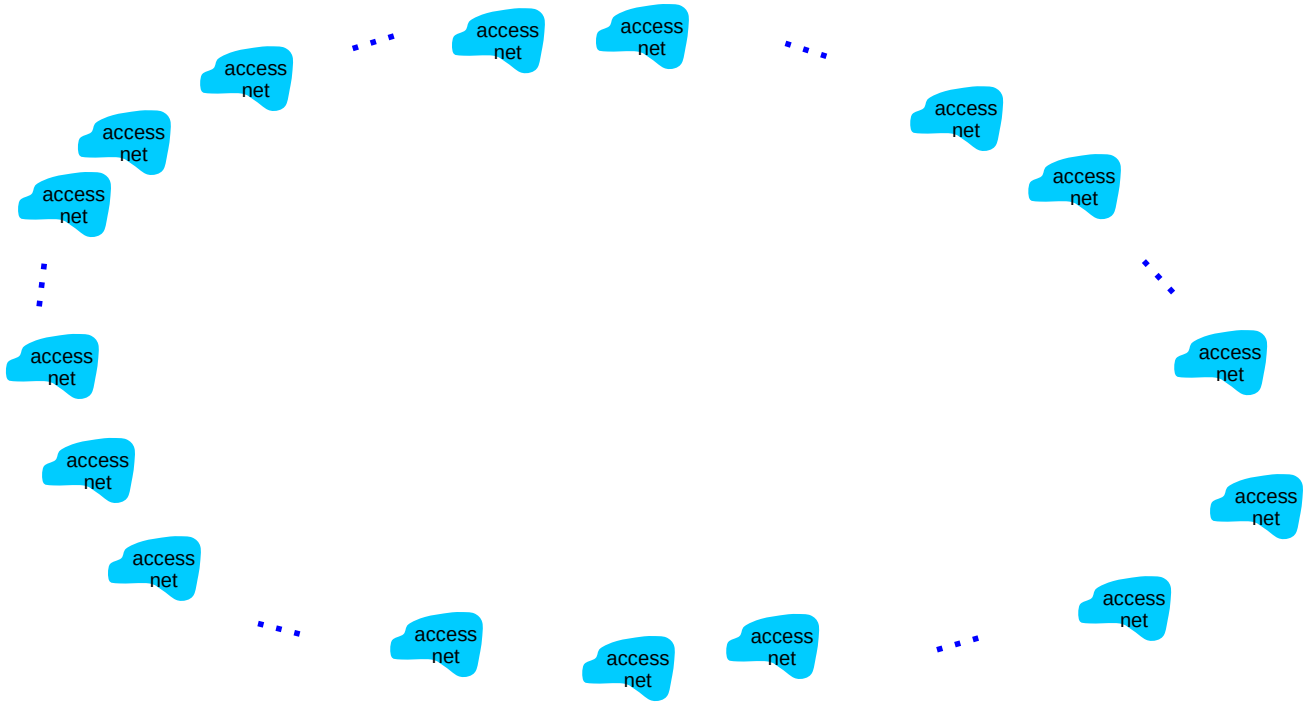
- hosts connect to Internet via access Internet Service Providers (ISPs)
- access ISPs in turn must be interconnected
  - so that *any* two hosts *(anywhere!)* can send packets to each other
- resulting network of networks is very complex
  - evolution driven by economics, national policies



Let's take a stepwise approach to describe current Internet structure

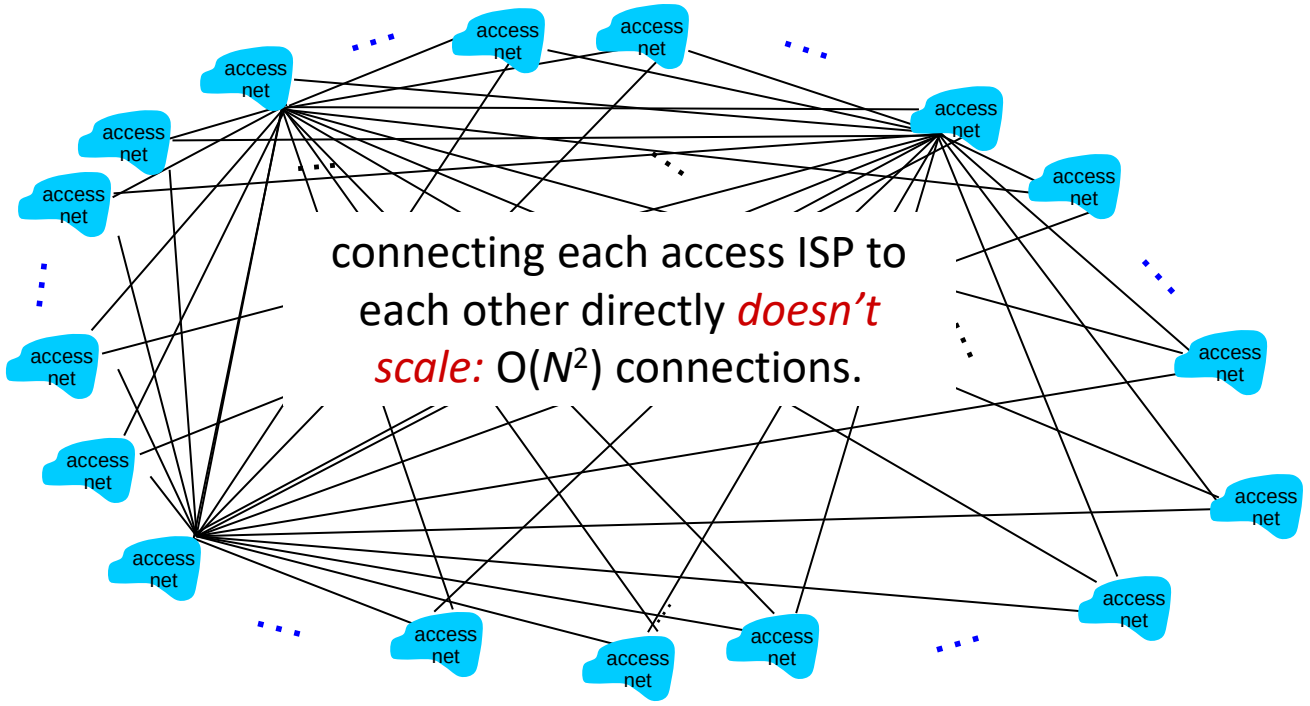
Internet structure: a "network of networks"

Question: given *millions* of access ISPs, how to connect them together?



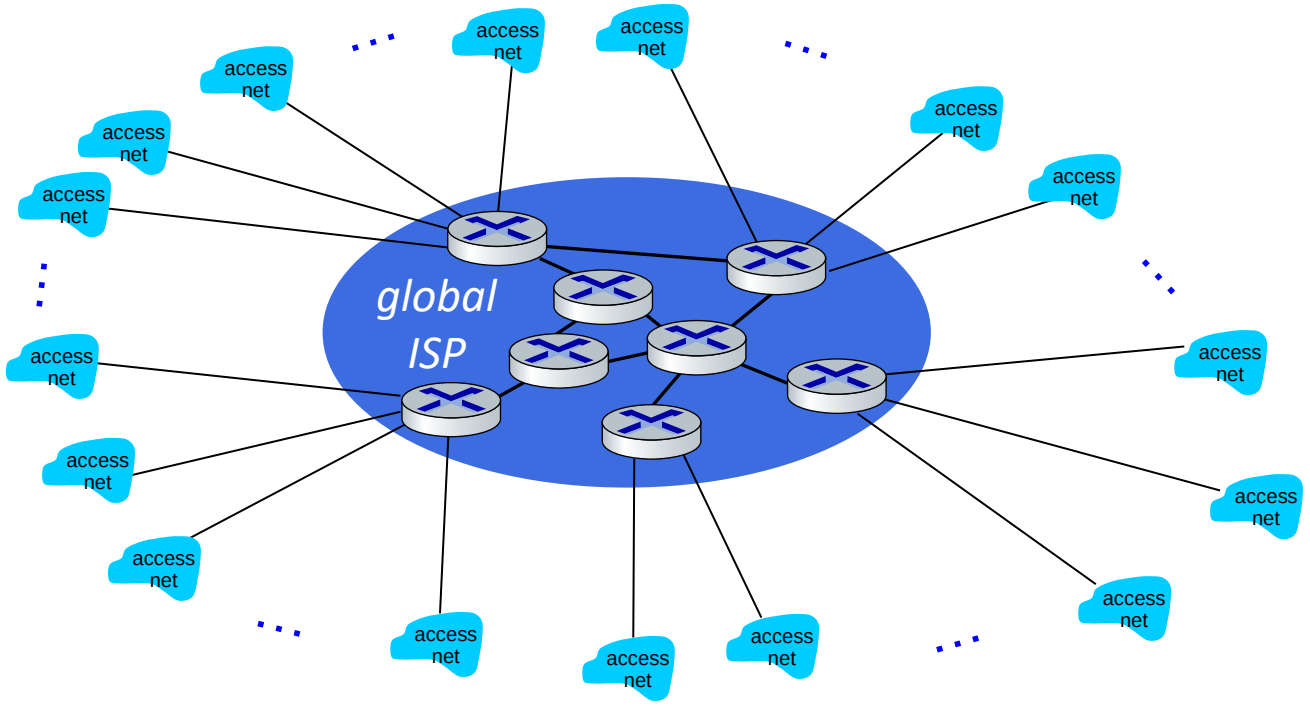
Internet structure: a "network of networks"

Question: given *millions* of access ISPs, how to connect them together?



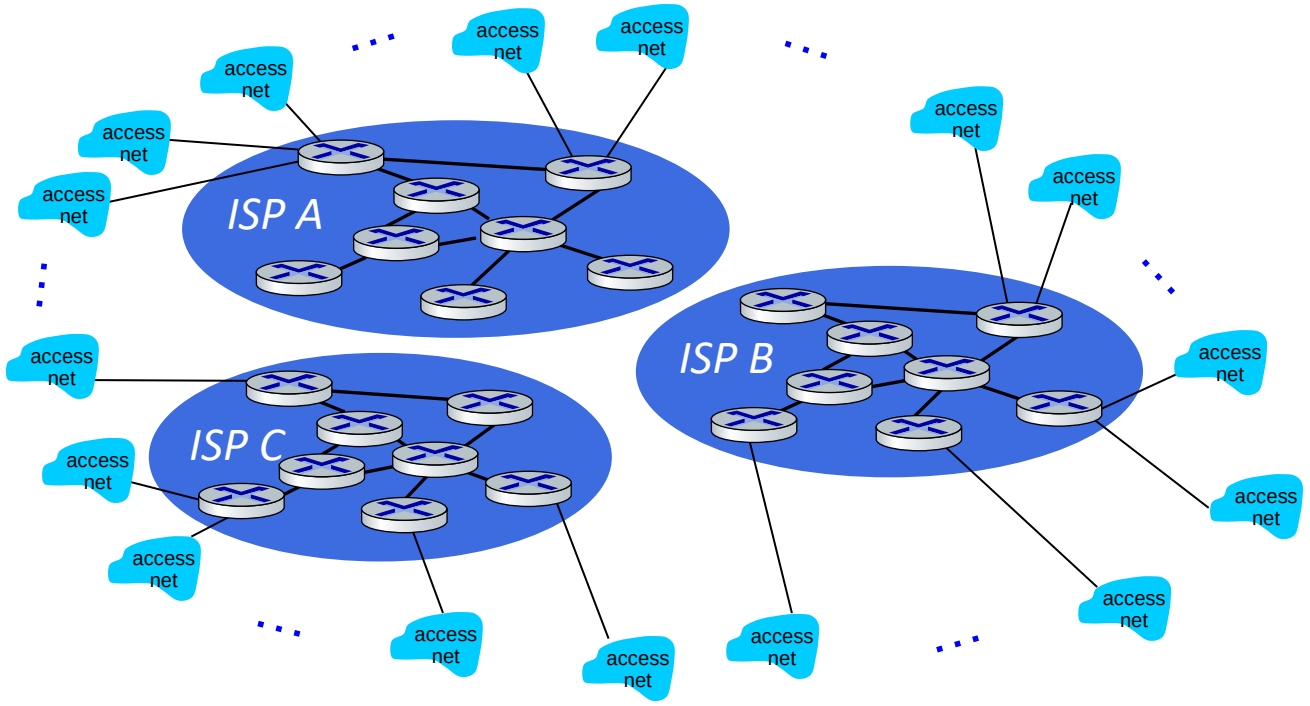
Internet structure: a "network of networks"

Option: connect each access ISP to one global transit ISP?
Customer and provider ISPs have economic agreement.



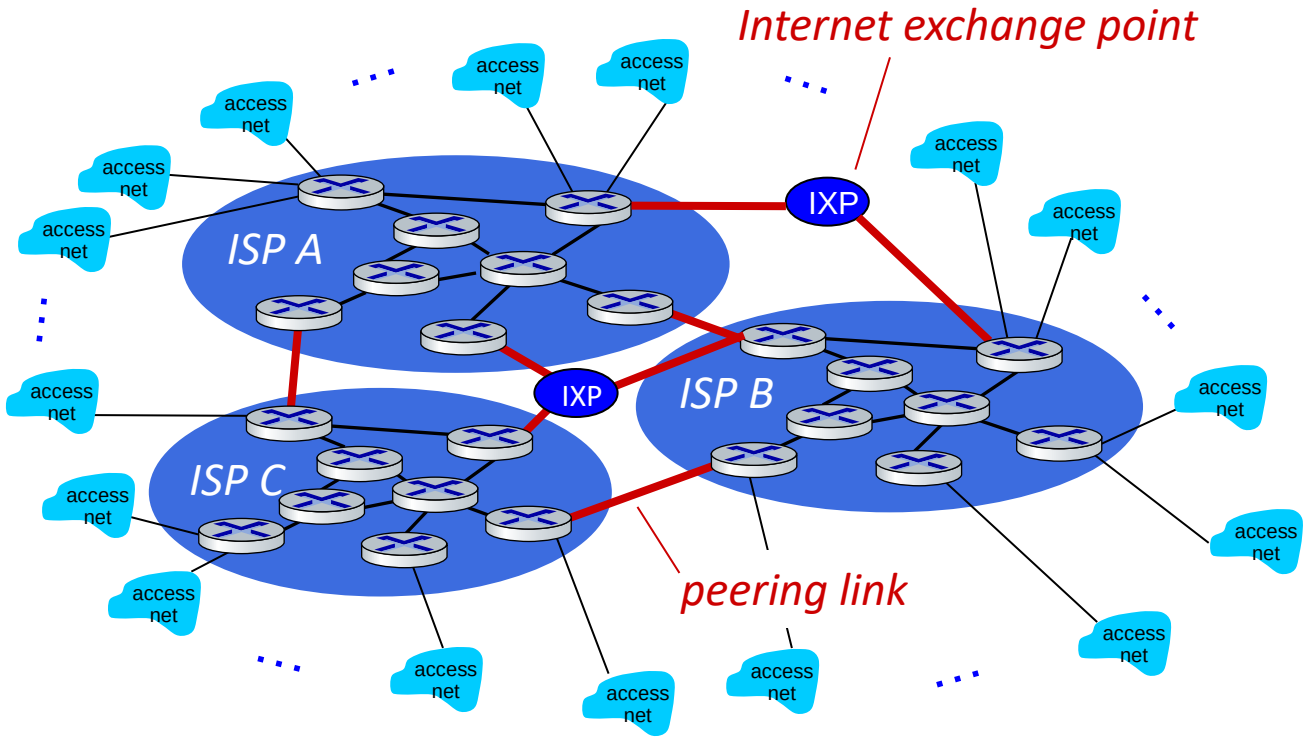
Internet structure: a "network of networks"

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



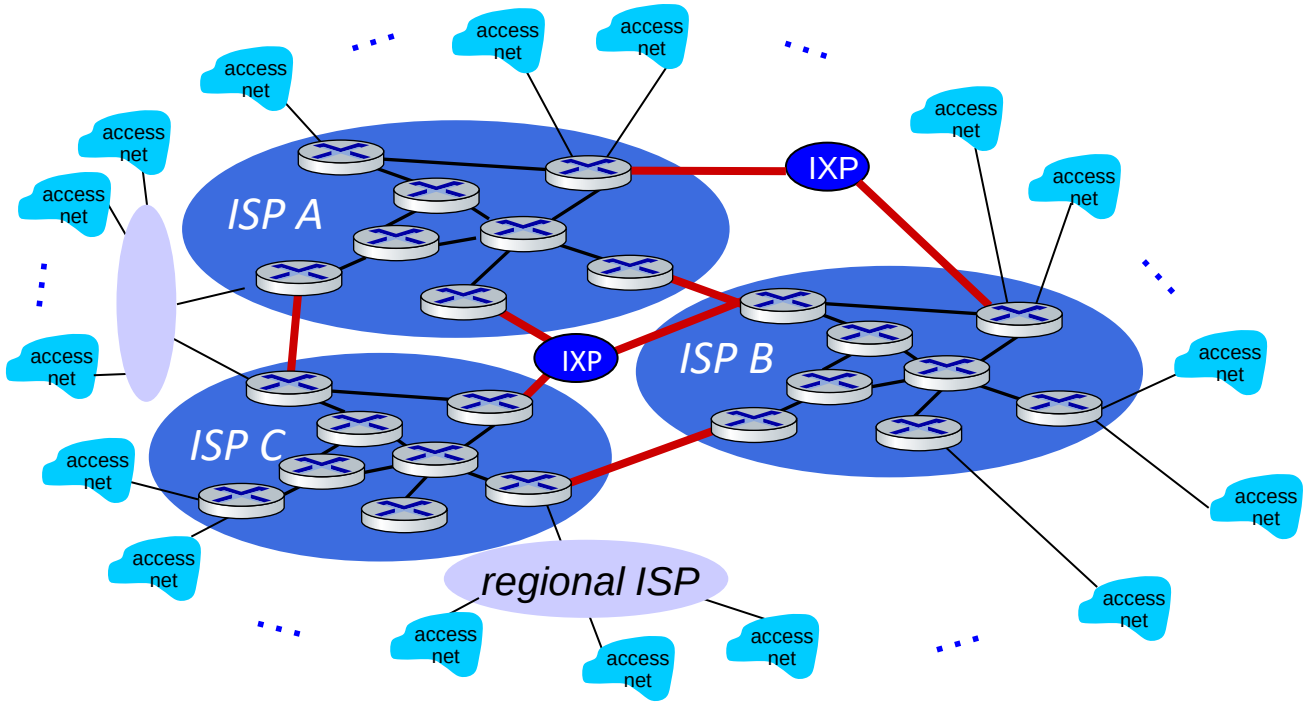
Internet structure: a "network of networks"

But if one global ISP is viable business, there will be competitors …. who will want to be connected



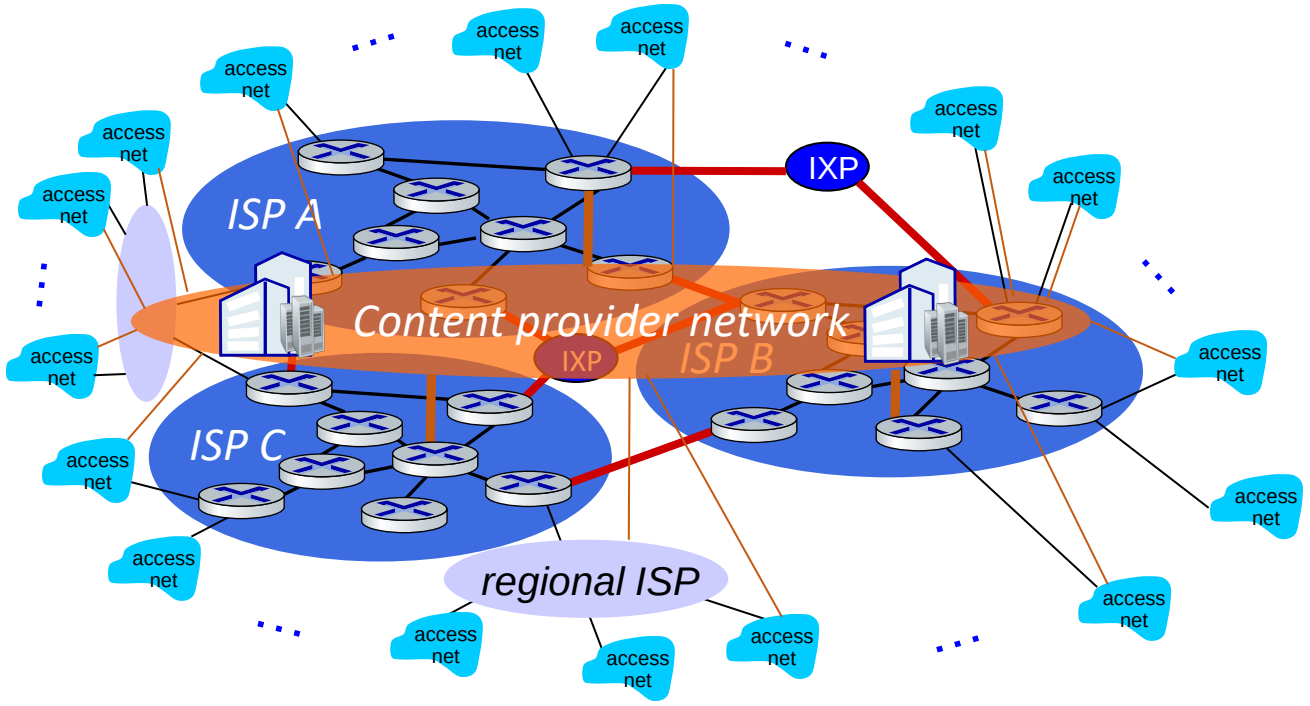
Internet structure: a "network of networks"

… and regional networks may arise to connect access nets to ISPs

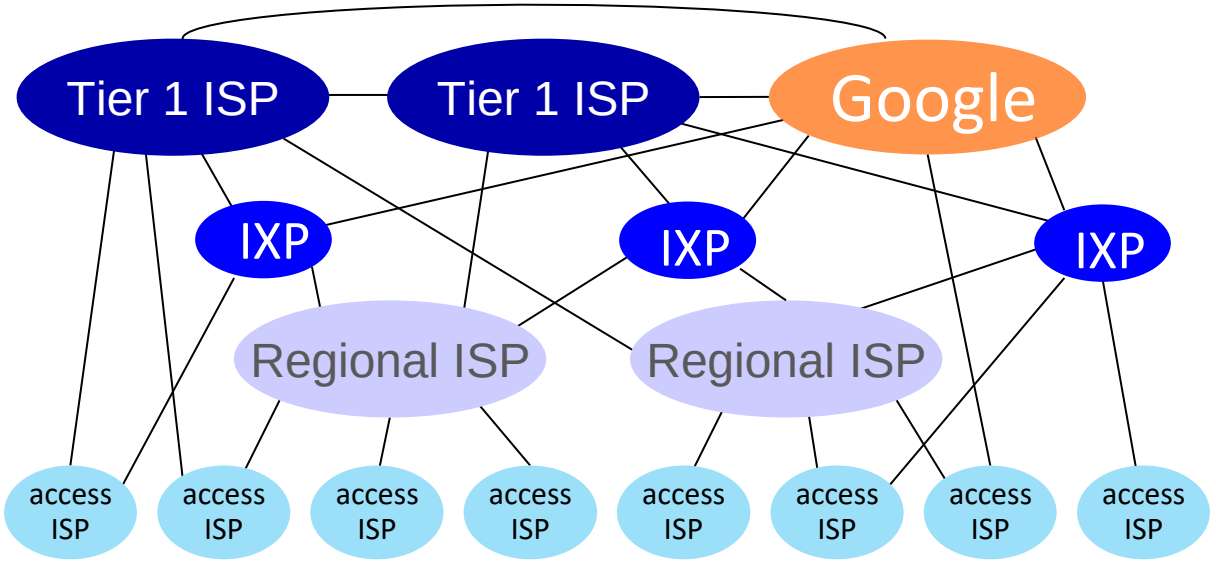


Internet structure: a "network of networks"

… and content provider networks (e.g., Google, Microsoft, Akamai) may run their own network, to bring services, content close to end users



Internet structure: a "network of networks"



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

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

7. Network security

- 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!
- 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

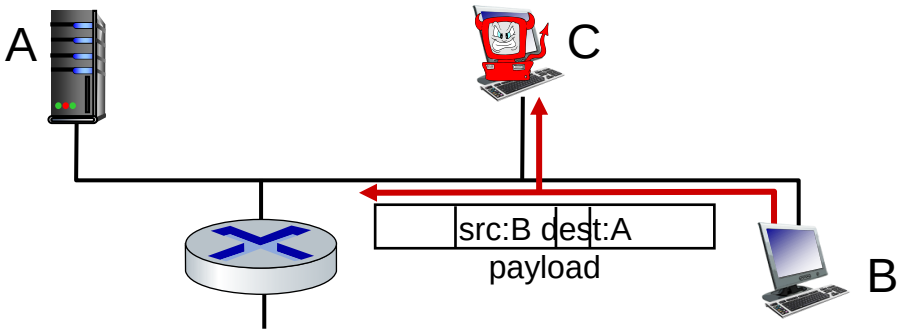
Network security

- 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!
- 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

Bad guys: packet interception

packet "sniffing":

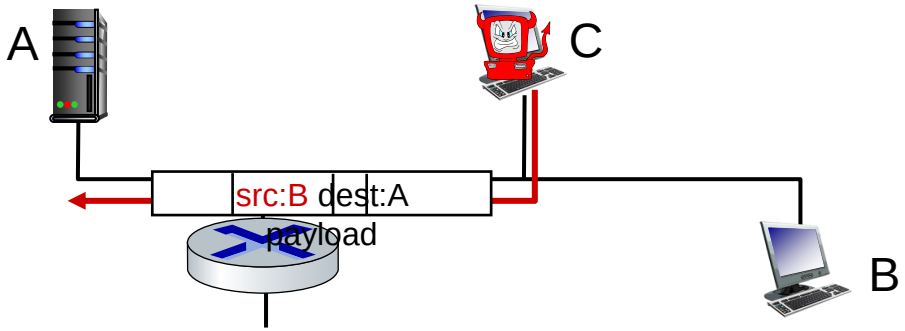
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



Wireshark software used for packet-sniffer

Bad guys: fake identity

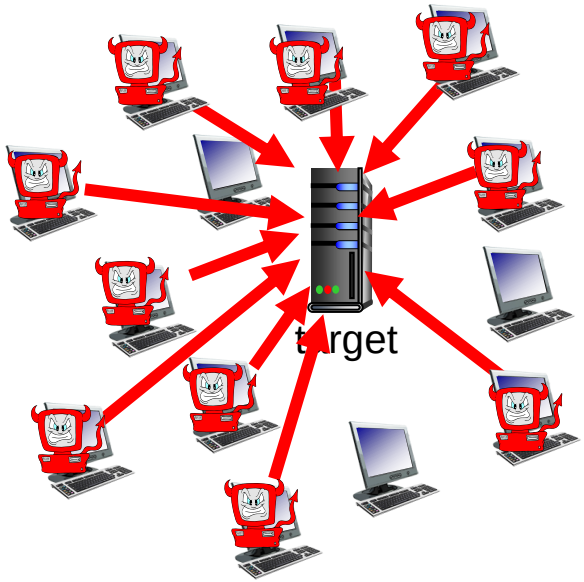
IP spoofing: injection of packet with false source address



Bad guys: denial of service

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 to target from compromised hosts



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


Any Questions