

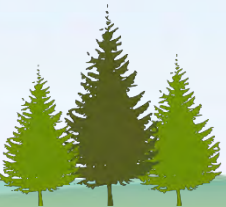
Networking and DDoS



Xinwen Fu., Ph.D

Professor

Department of Computer Science
University of Massachusetts Lowell

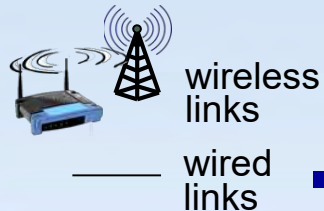


Outline

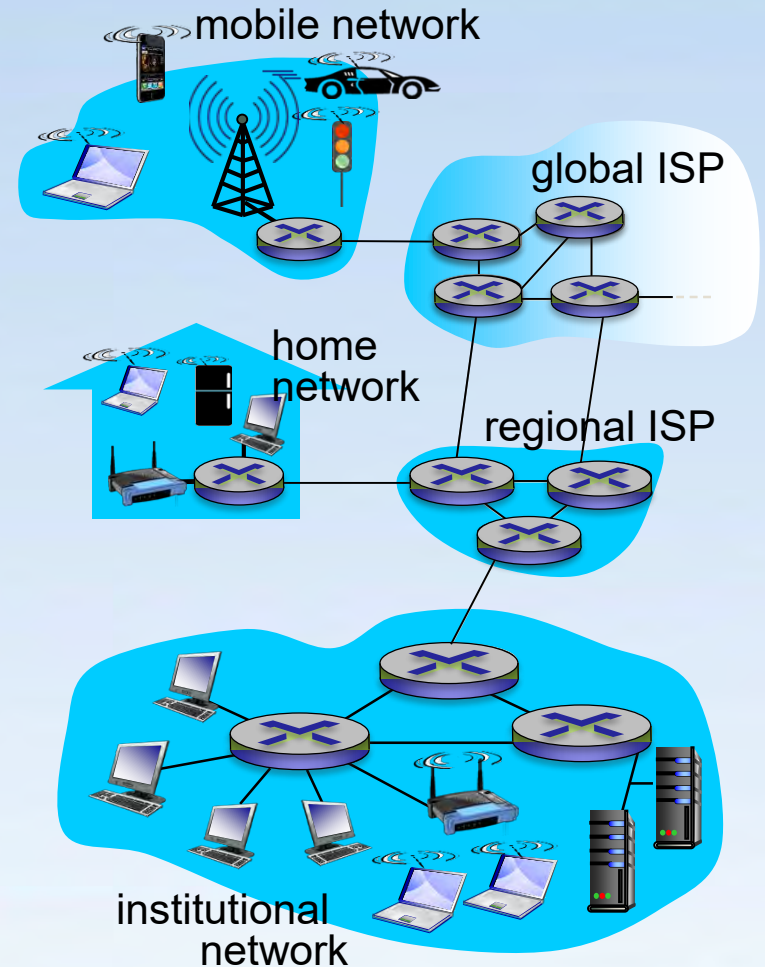
1. *what is the Internet?*
2. network edge
 - end systems, access networks, links
3. network core
 - packet switching, circuit switching, network structure
4. protocol layers, service models
5. networks under attack: security
6. history
7. Hand-on lab



What's the Internet: “nuts and bolts” view



- 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*



“Fun” Internet-connected devices



IP picture frame

<http://www.ceiva.com/>



Web-enabled toaster +
weather forecaster



Tweet-a-watt:
monitor energy use



Internet
refrigerator



Slingbox: watch,
control cable TV remotely



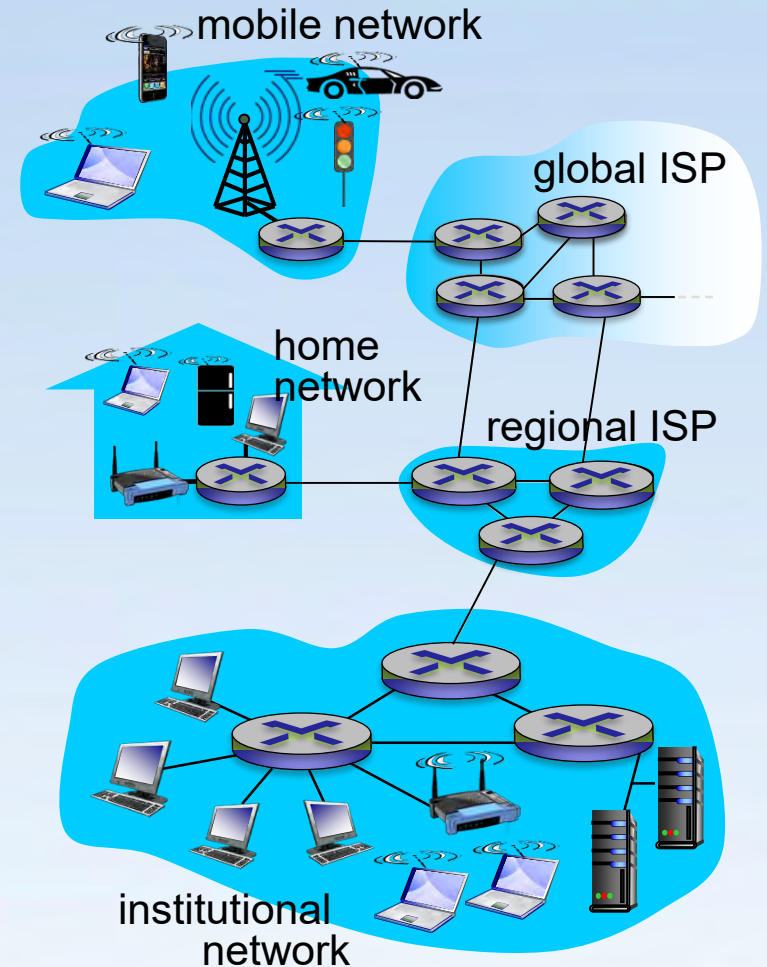
sensorized,
bed
mattress



Internet phones

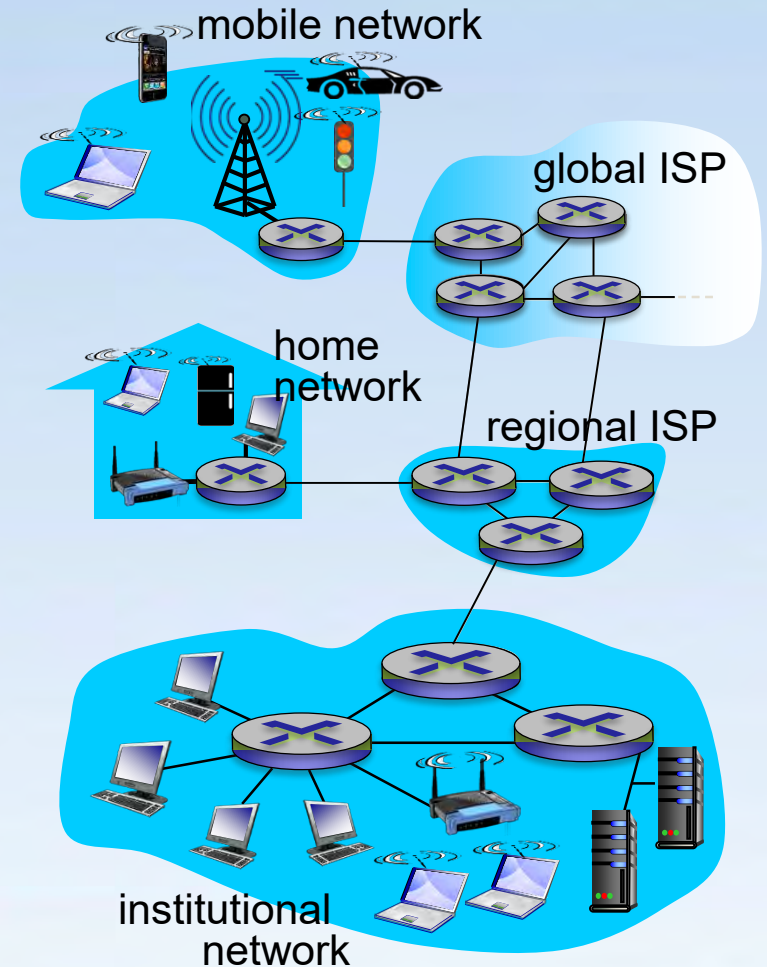
What's the Internet: "nuts and bolts" view

- *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: a service view

- *infrastructure that provides services to applications:*
 - Web, VoIP, email, games, e-commerce, social nets, ...
- *provides programming interface to apps*
 - hooks that allow sending and receiving app programs to “connect” to Internet
 - provides 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 when messages received, or other events

network protocols:

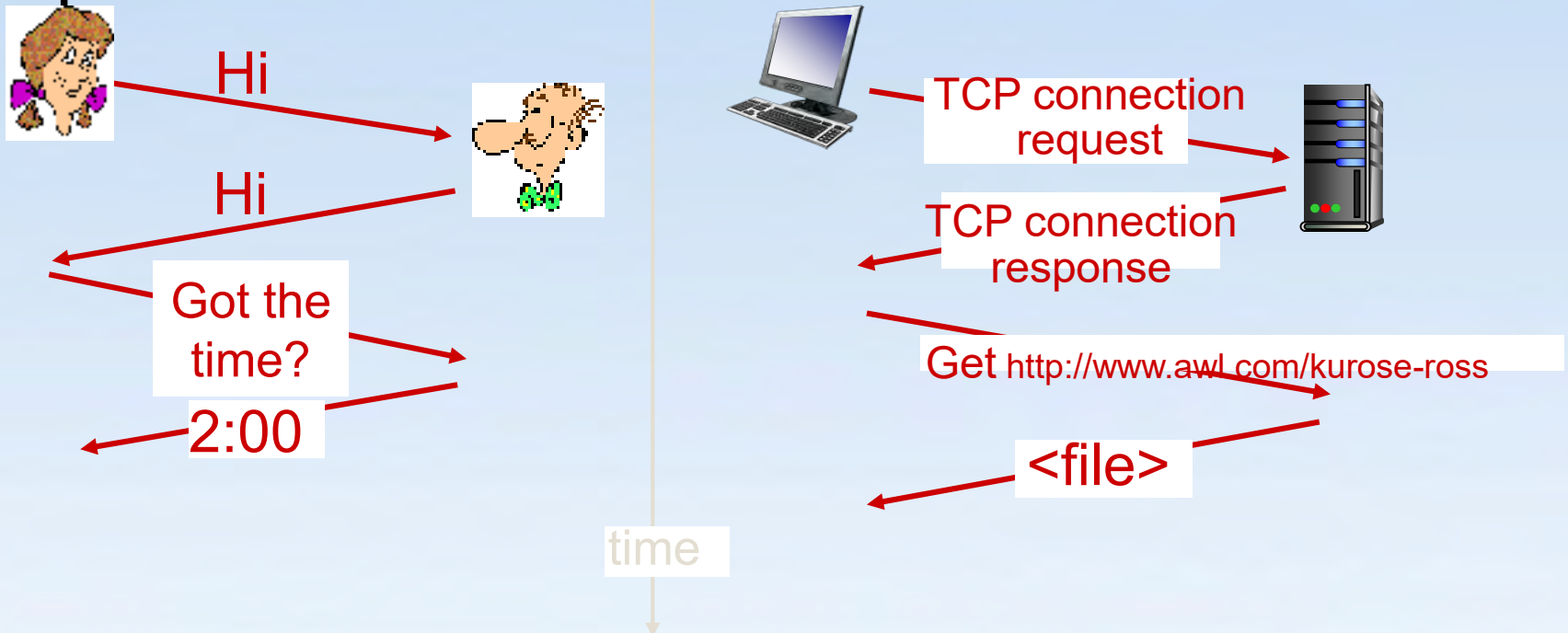
- machines rather than humans
- all communication activity in Internet governed by protocols

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



What's a protocol?

a human protocol and a computer network protocol:



Q: other human protocols?

Chapter 1: roadmap

1. what *is* the Internet?

2. network edge

- end systems, access networks, links

3. network core

packet switching, circuit switching, network structure

4. protocol layers, service models

5. networks under attack: security

6. history

7. Hand-on lab



A closer look at network structure:

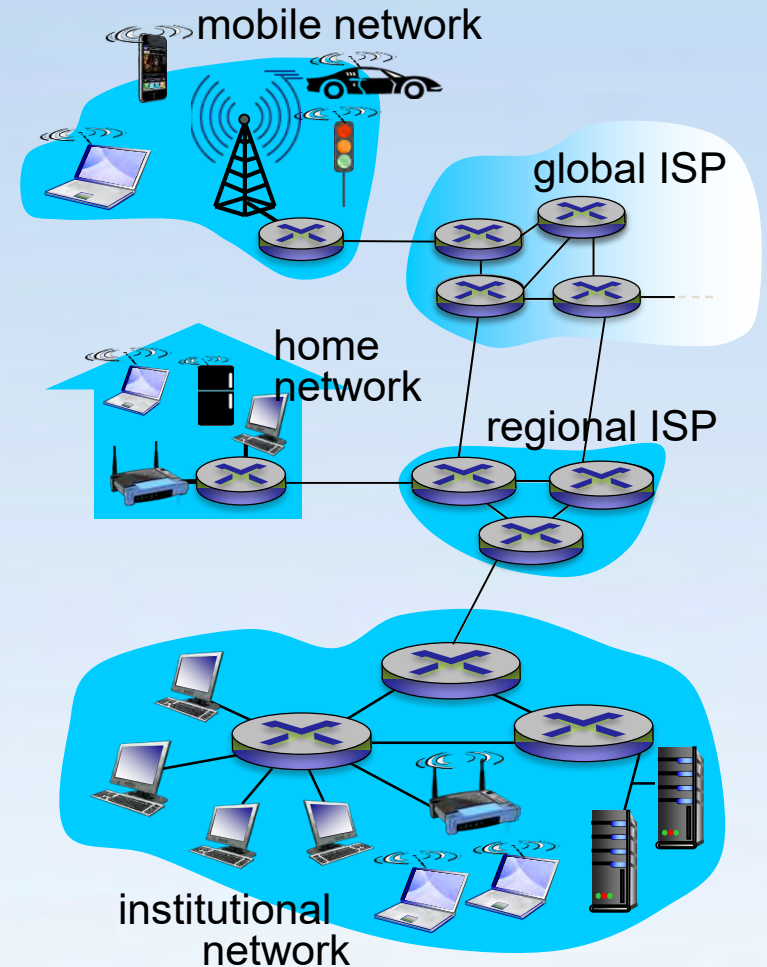
■ *network edge:*

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

■ *access networks, physical media:* wired, wireless communication links

■ *network core:*

- interconnected routers
- network of networks



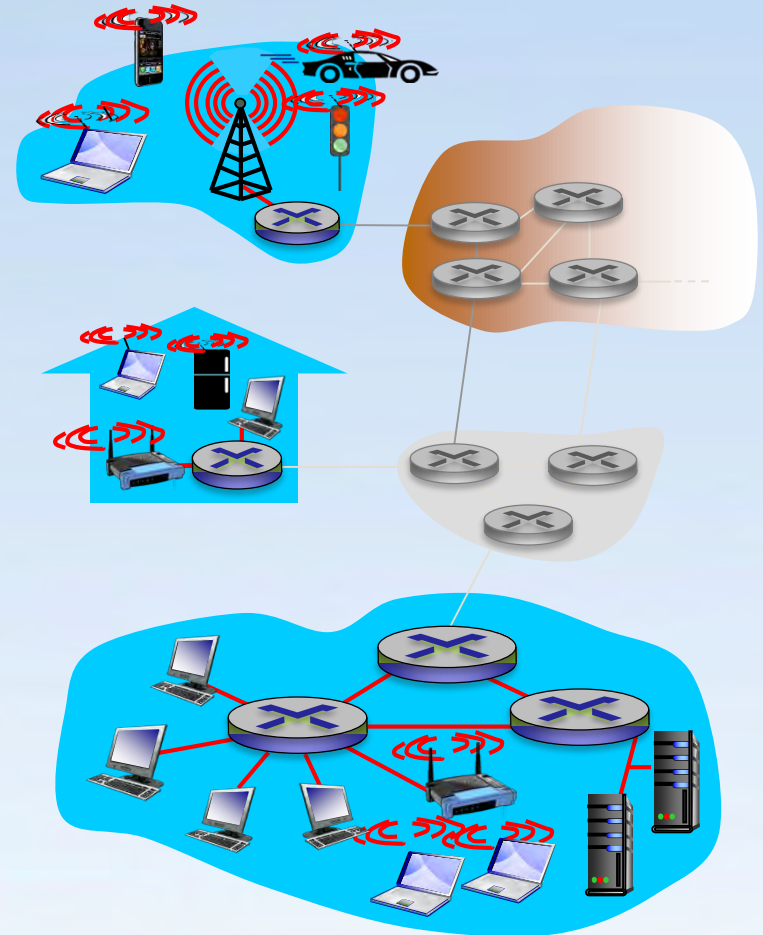
Access networks and physical media

Q: How to connect end systems to edge router?

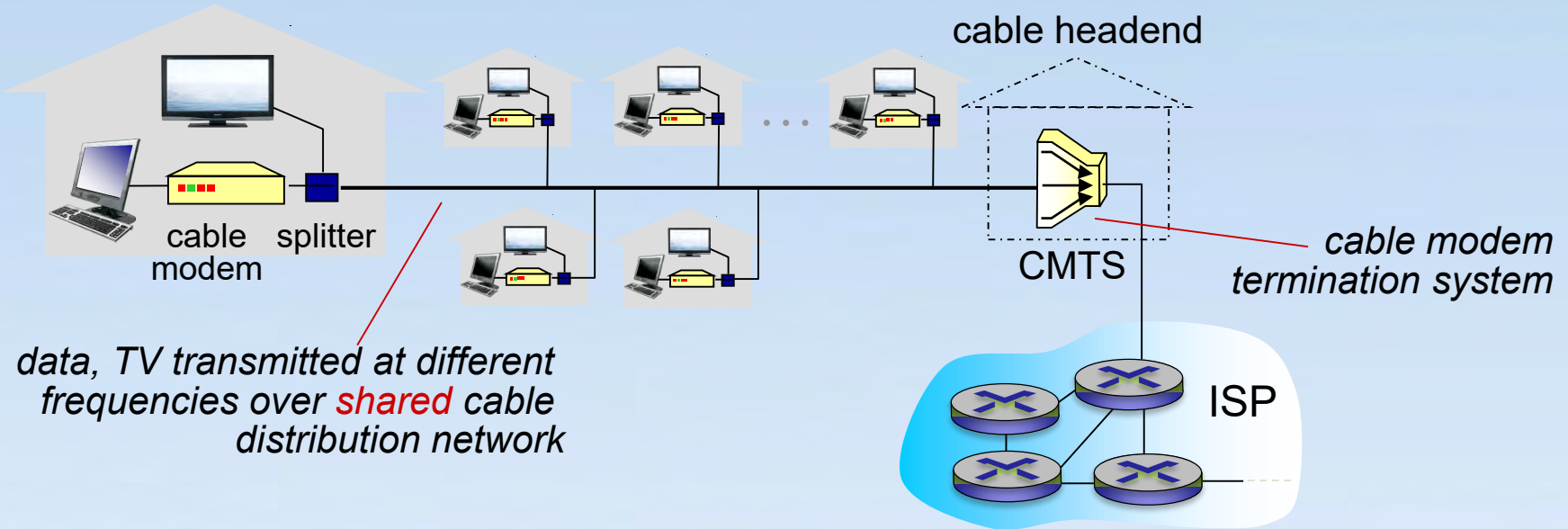
- residential access nets
- institutional access networks (school, company)
- mobile access networks

keep in mind:

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



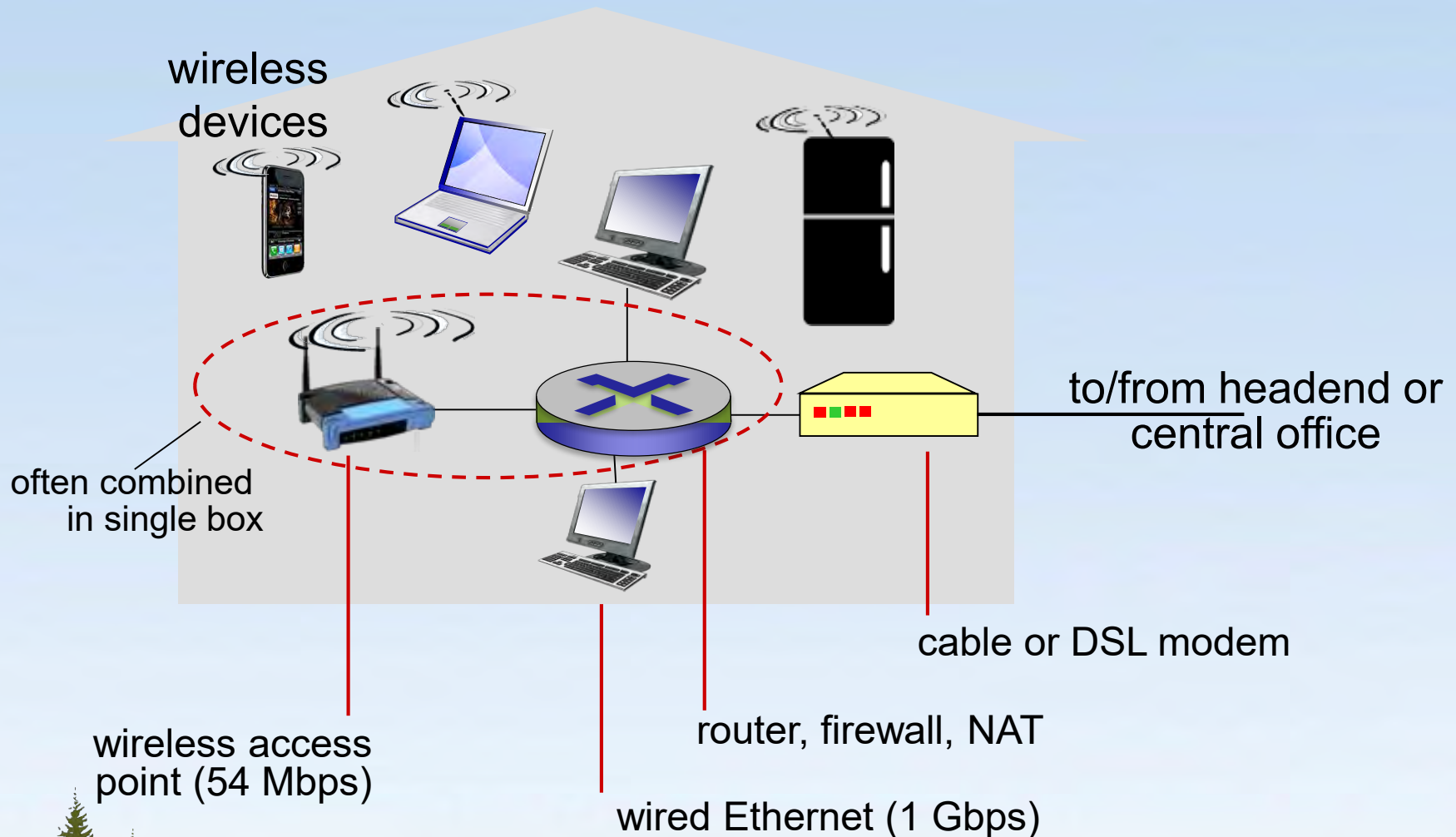
Access network: cable network



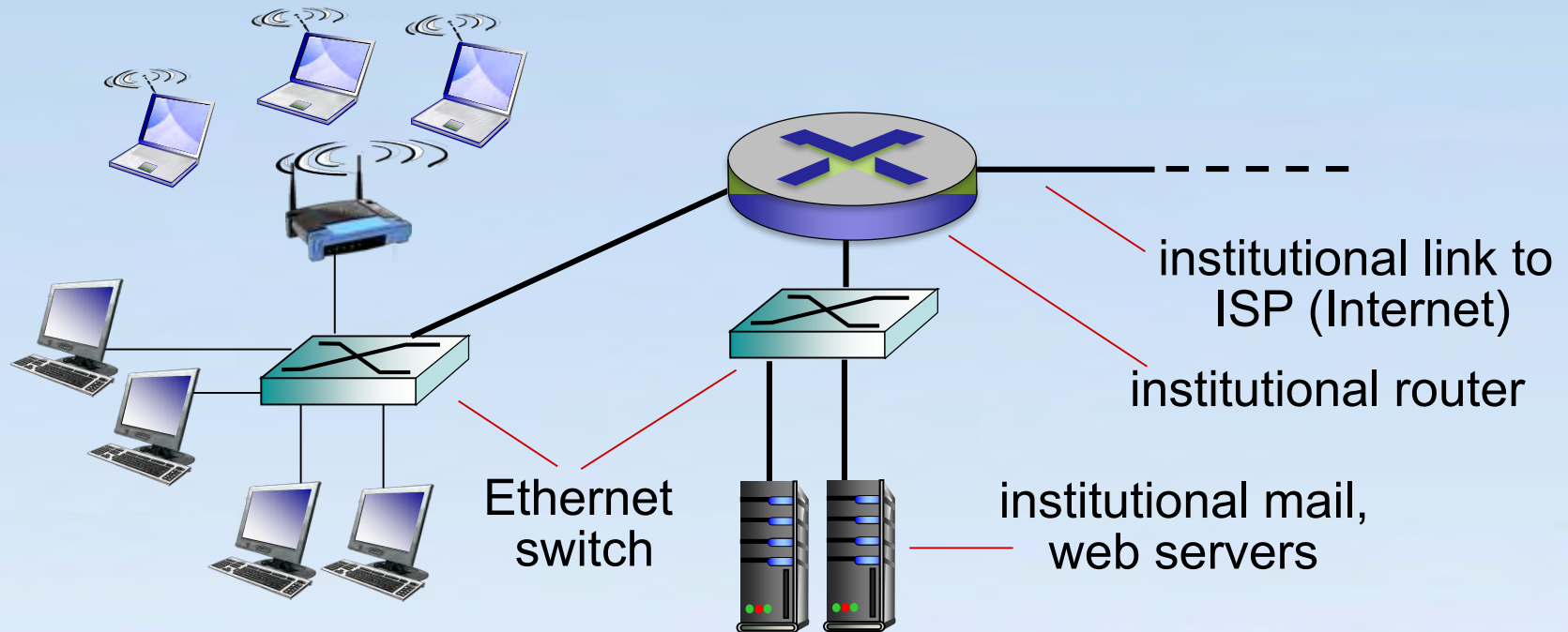
■ HFC: hybrid fiber coax

- 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 network



Enterprise access networks (Ethernet)



- typically used in companies, universities, etc.
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
- today, end systems typically connect into Ethernet switch

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/n (WiFi): 11, 54, 450 Mbps transmission rate



to Internet

wide-area wireless access

- provided by telco (cellular) operator, 10's km
- between 1 and 10 Mbps
- 3G, 4G: LTE



to Internet

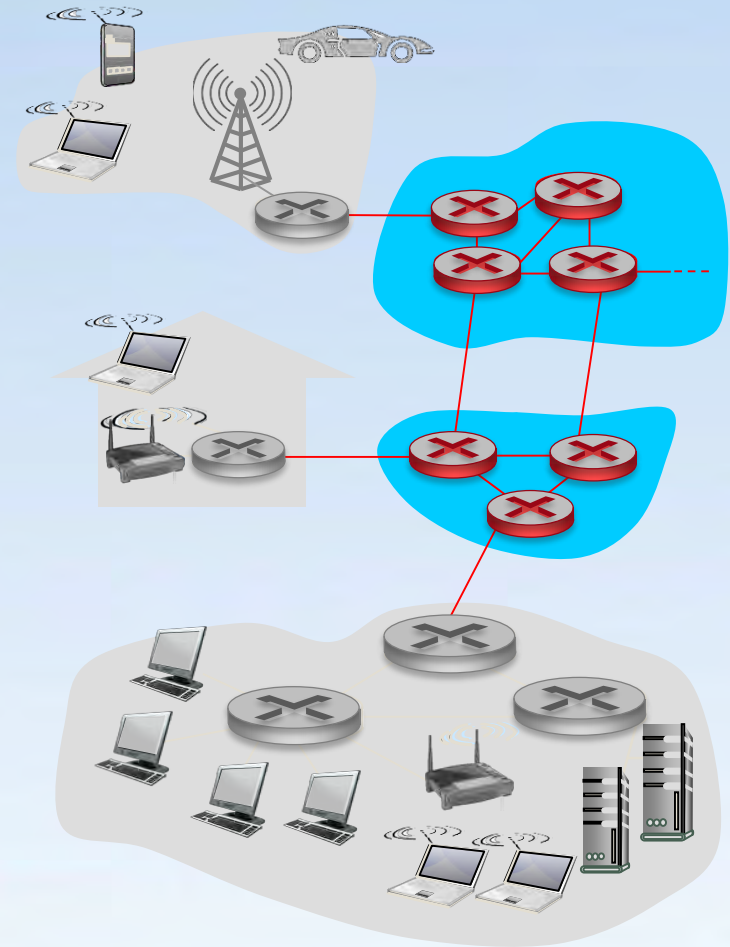
Outline

1. what *is* the Internet?
2. network edge
 - end systems, access networks, links
3. network core
 - packet switching, circuit switching, network structure
4. protocol layers, service models
5. networks under attack: security
6. history
7. Hand-on lab



The network core

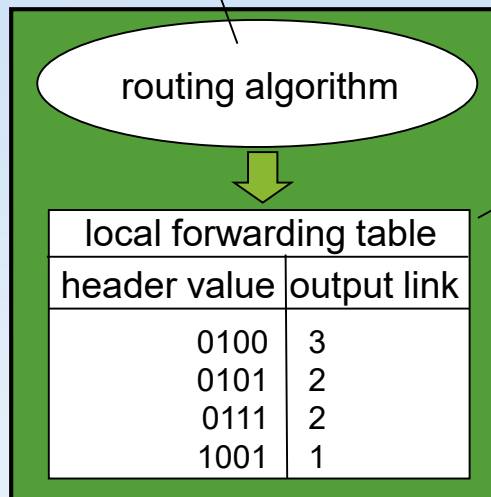
- mesh of interconnected routers
- packet-switching: hosts break application-layer messages into *packets*
 - forward packets from one router to the next, across links on path from source to destination
 - each packet transmitted at full link capacity



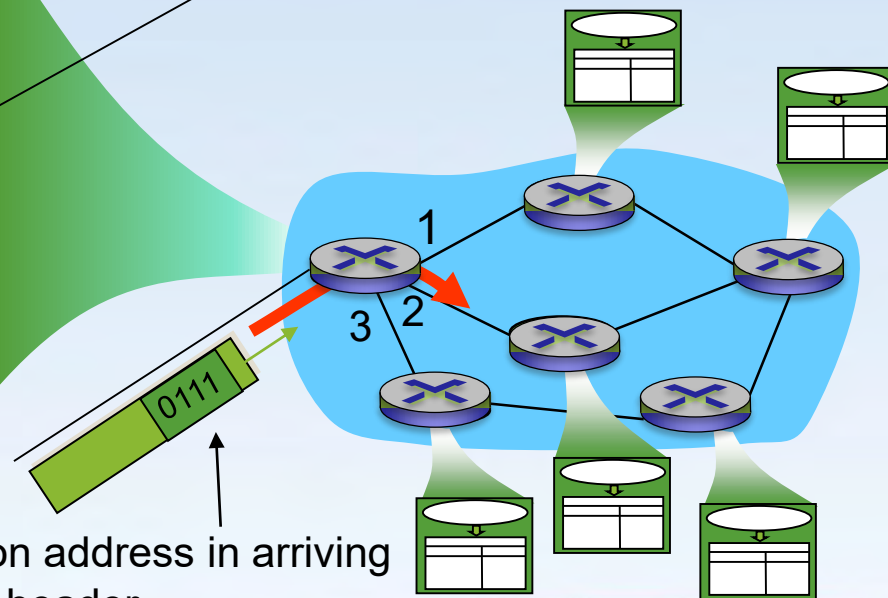
Two key network-core functions

routing: determines source-destination route taken by packets

- *routing algorithms*



forwarding: move packets from router's input to appropriate router output

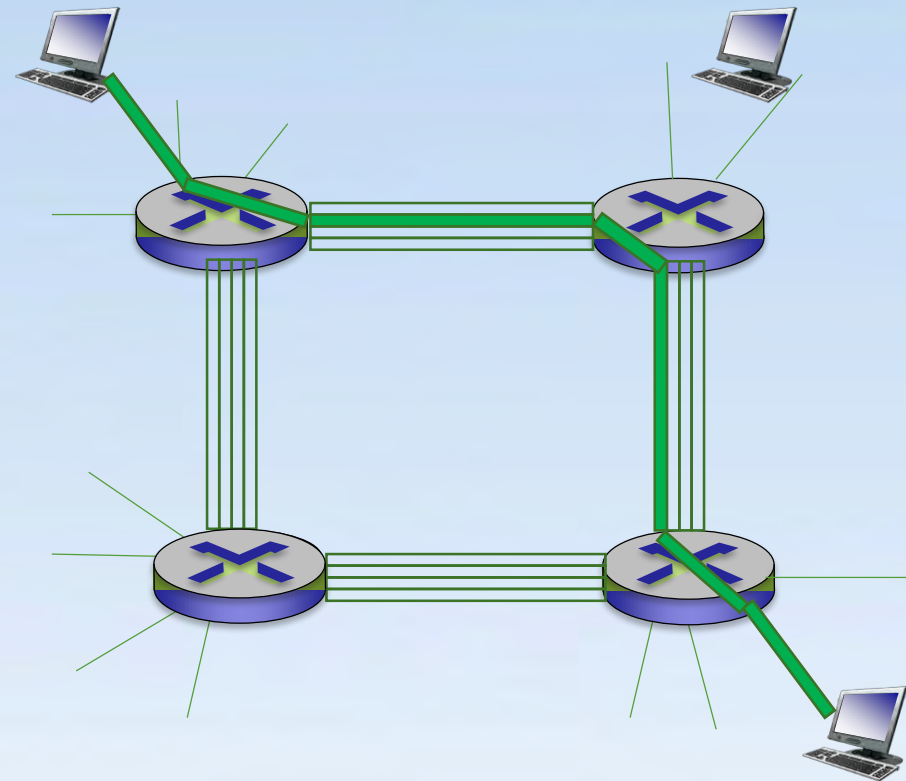


destination address in arriving packet's header

Alternative core: circuit switching

end-end resources
allocated to, reserved
for “call” between
source & dest:

- circuit-like (guaranteed) performance
- circuit segment idle if not used by call (*no sharing*)
- commonly used in traditional telephone networks



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



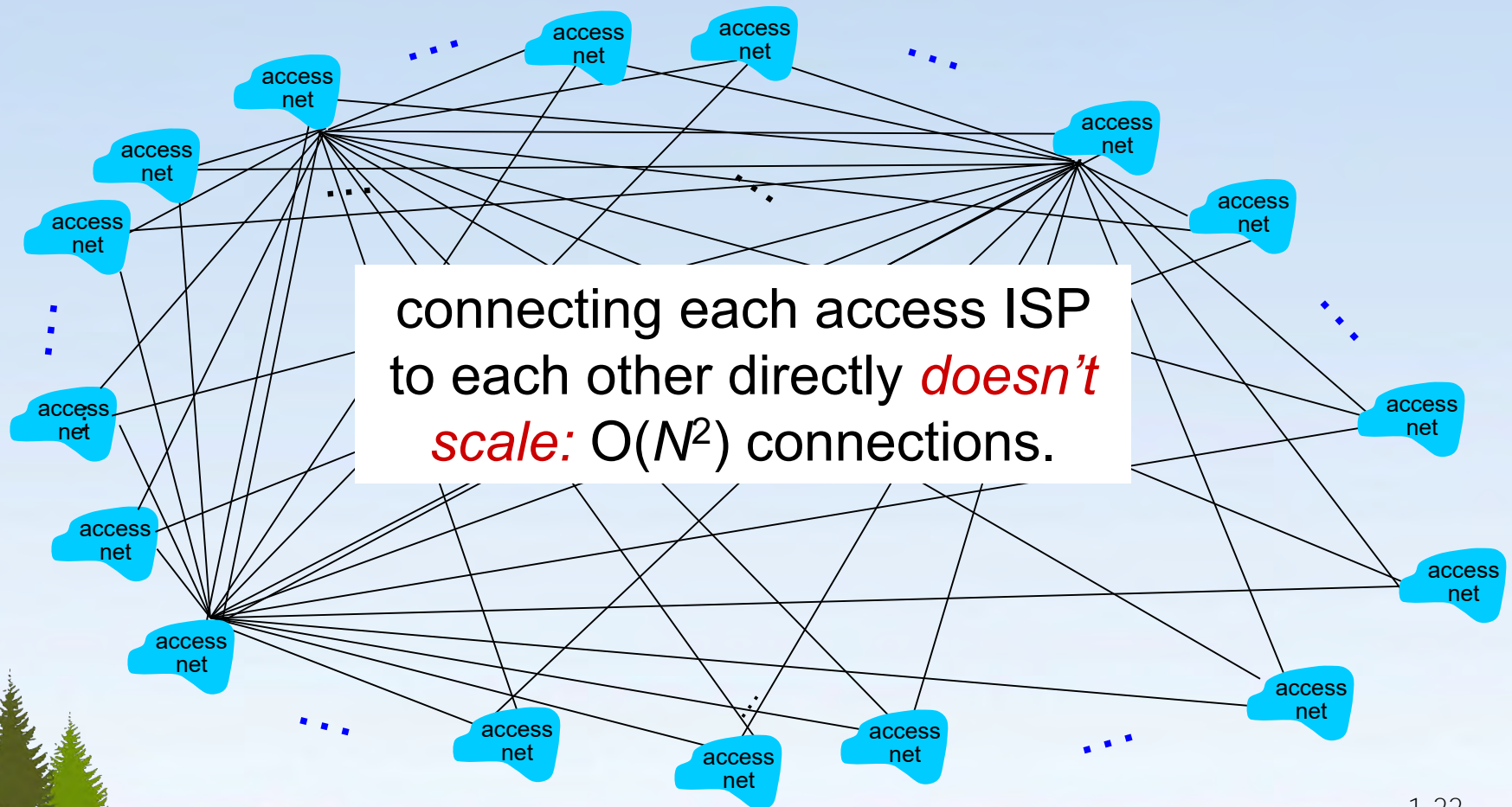
Internet structure: network of networks

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



Internet structure: network of networks

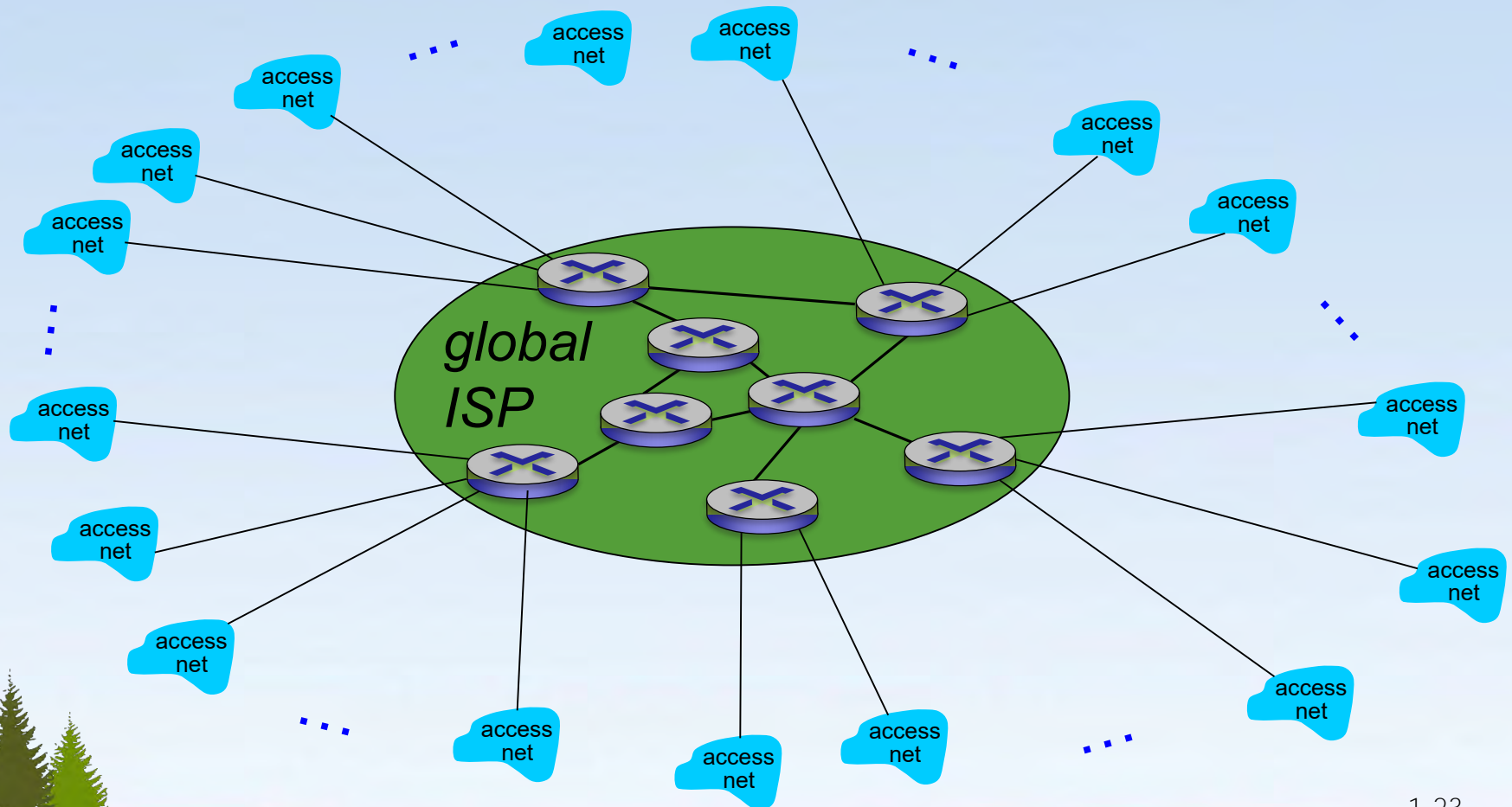
Option: connect each access ISP to every other access ISP?



Internet structure: network of networks

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

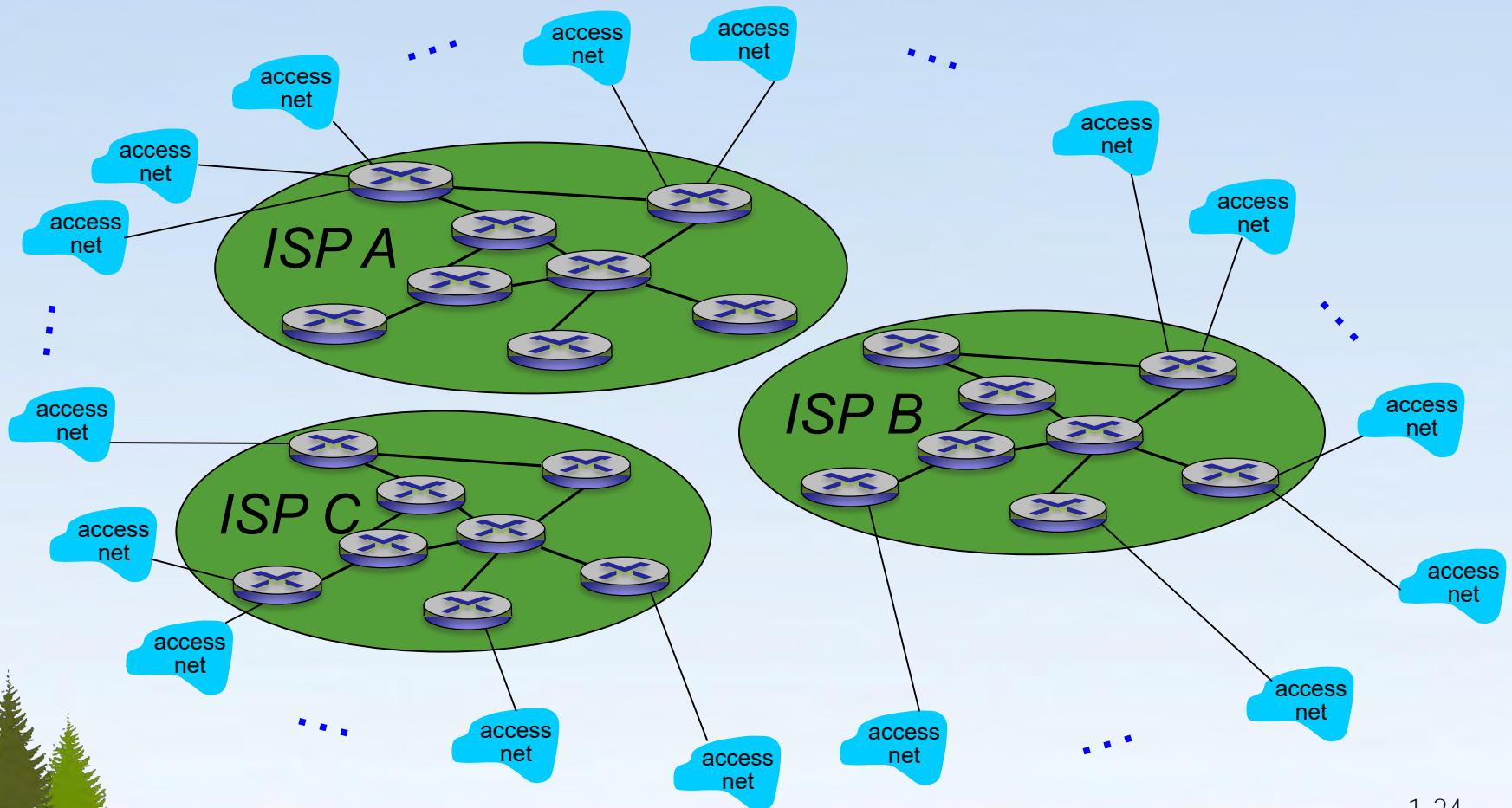
Customer and provider ISPs have economic agreement.



Internet structure: network of networks

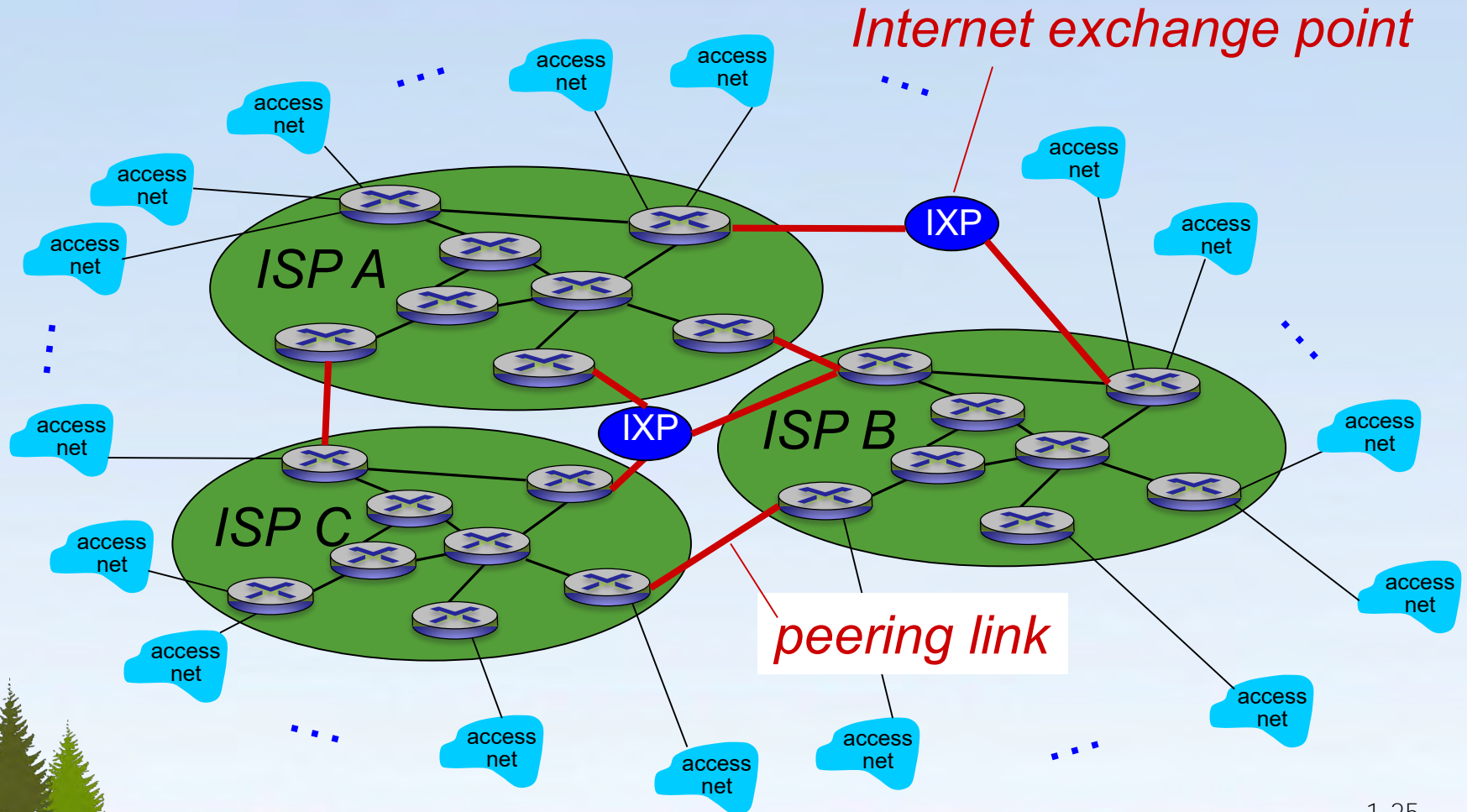
But if one global ISP is viable business, there will be competitors

....



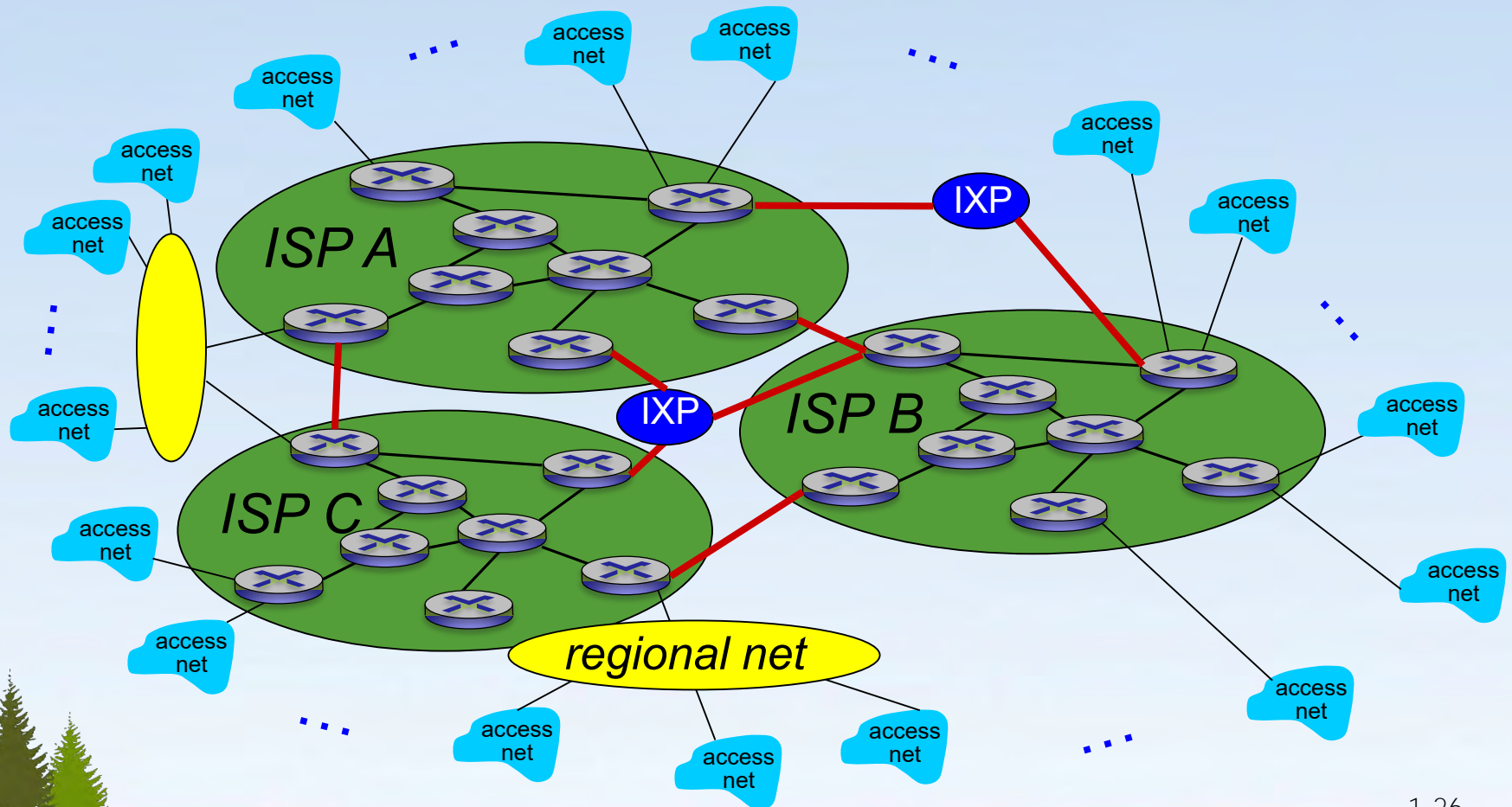
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors
.... which must be interconnected



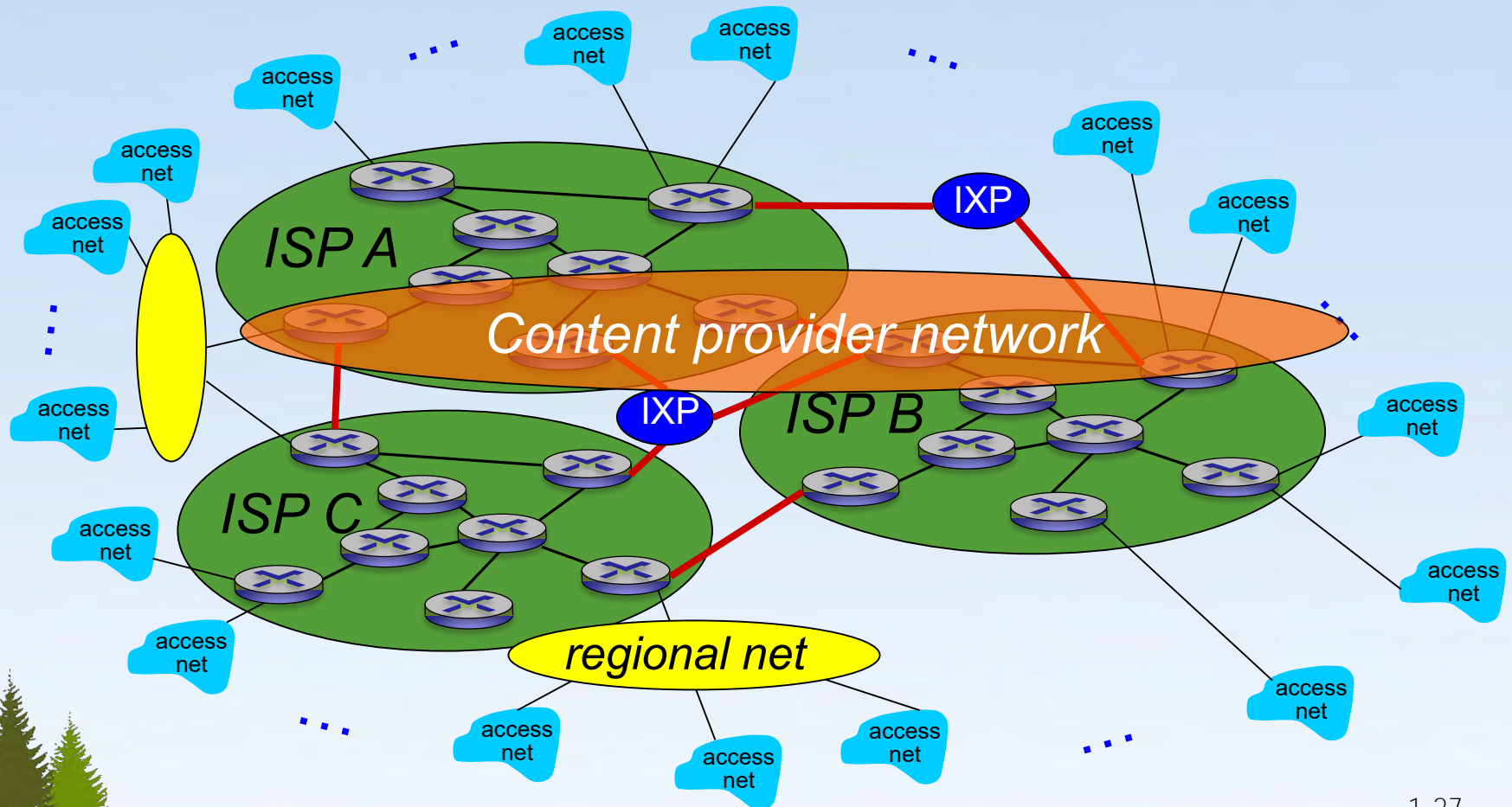
Internet structure: network of networks

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

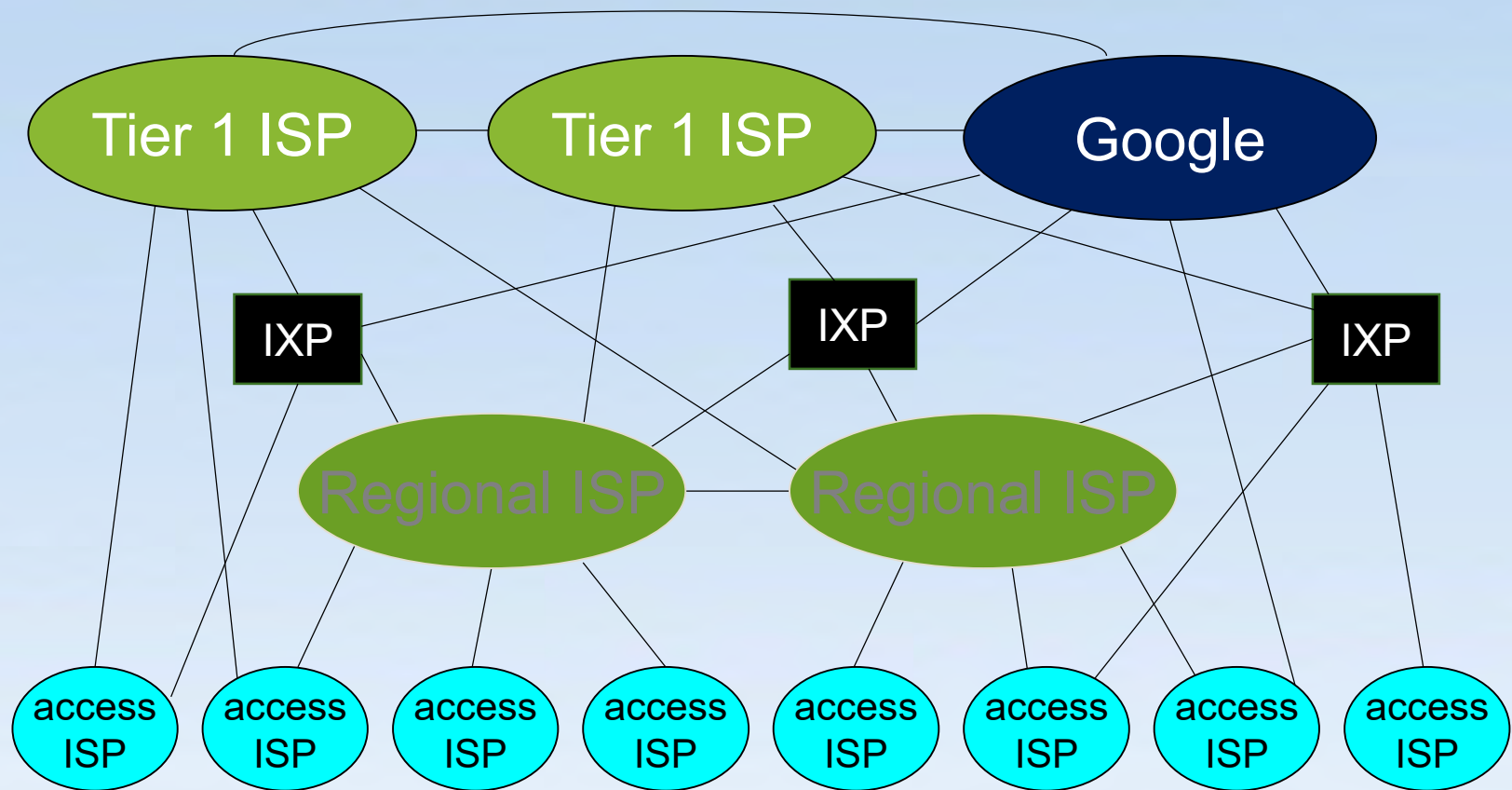


Internet structure: network of networks

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

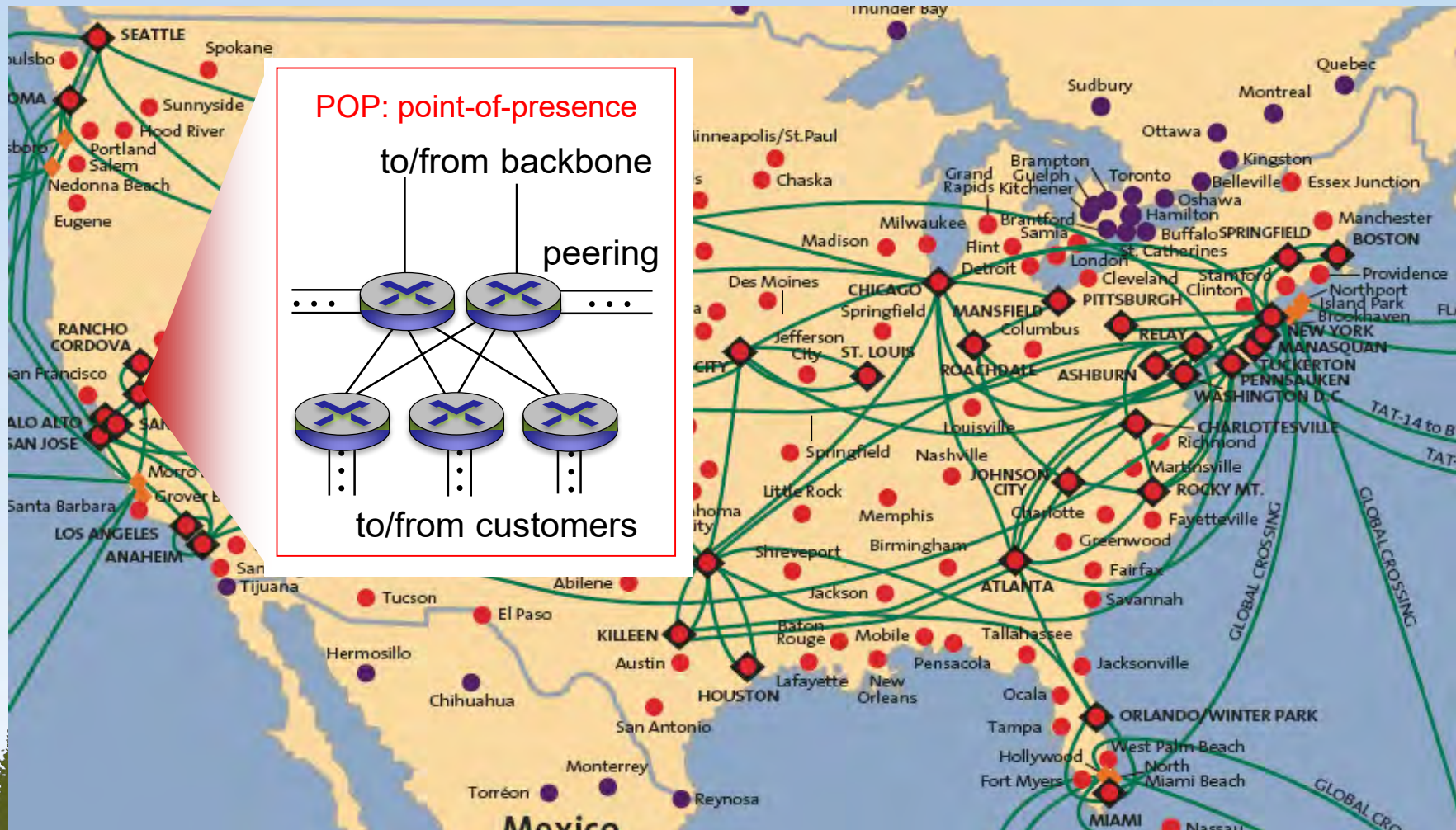


Internet structure: network of networks



- 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 network (e.g., Google): private network that connects its data centers to Internet, often bypassing tier-1, regional ISPs

Tier-1 ISP: e.g., Sprint



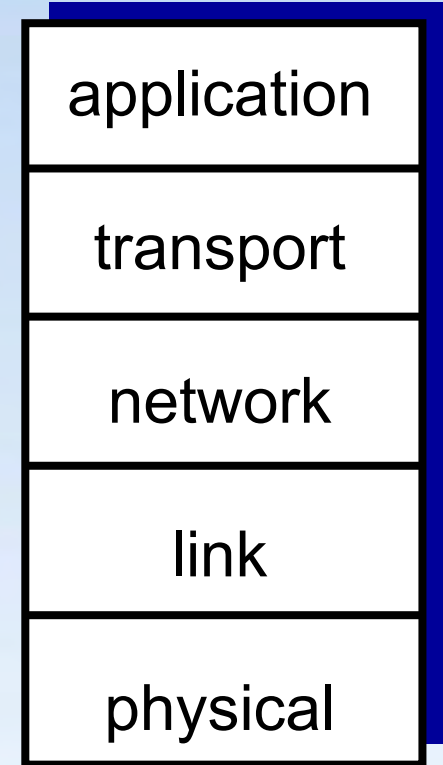
Outline

1. what *is* the Internet?
2. network edge
 - end systems, access networks, links
3. network core
 - packet switching, circuit switching, network structure
4. protocol layers, service models
5. networks under attack: security
6. history
7. Hand-on lab

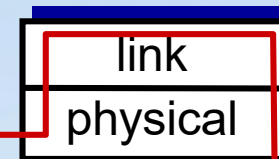
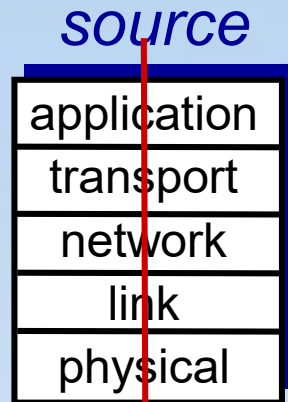
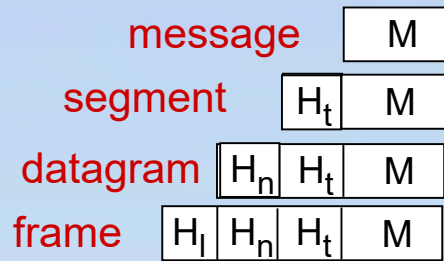


Internet protocol stack

- *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, 802.111 (WiFi), PPP
- *physical*: bits “on the wire”

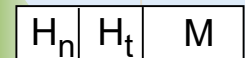
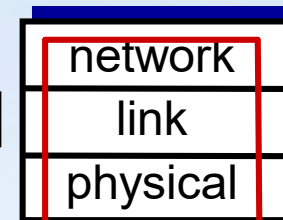
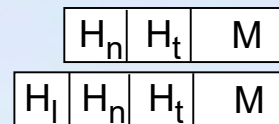
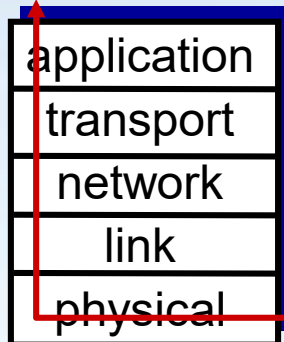


Encapsulation



switch

destination



router



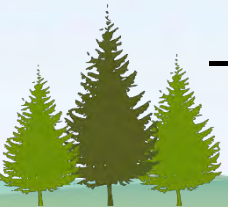
Outline

1. what *is* the Internet?
2. network edge
 - end systems, access networks, links
3. network core
 - packet switching, circuit switching, network structure
4. protocol layers, service models
5. networks under attack: security
6. history
7. Hand-on lab



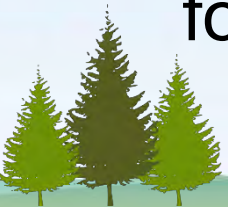
Network security

- field of network security:
 - how bad guys can attack computer networks
 - how we can defend networks against attacks
 - how to design architectures that are immune to attacks
- Internet not originally designed with (much) security in mind
 - *original vision*: “a group of mutually trusting users attached to a transparent network” 😊
 - Internet protocol designers playing “catch-up”
 - security considerations in all layers!



Bad guys: put malware into hosts via Internet

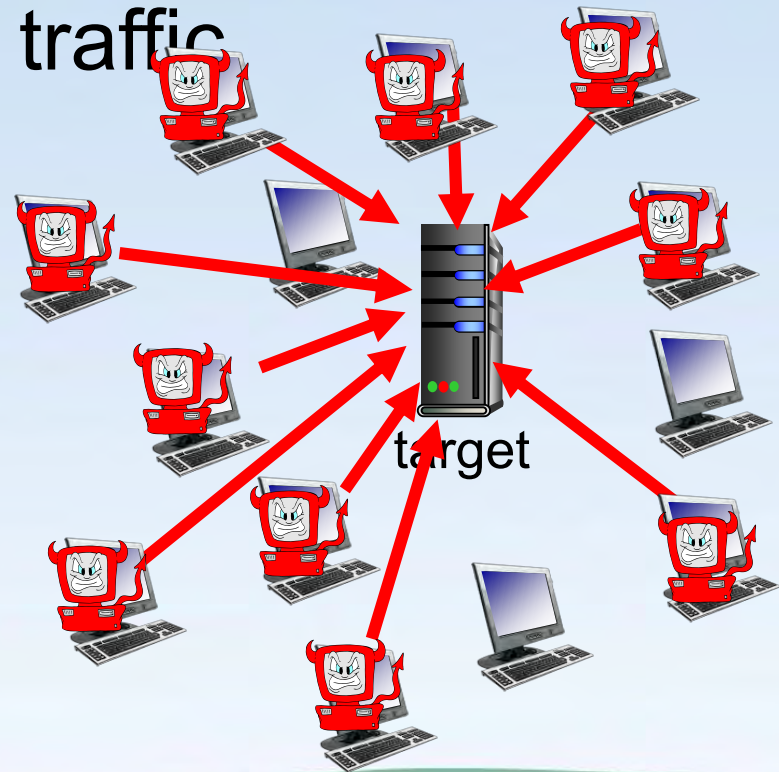
- malware can get in host from:
 - *virus*: self-replicating infection by receiving/executing object (e.g., e-mail attachment)
 - *worm*: self-replicating infection by passively receiving object that gets itself executed
- **spyware malware** can record keystrokes, web sites visited, upload info to collection site
- infected host can be enrolled in **botnet**, used for spam. DDoS attacks



Bad guys: attack server, network infrastructure

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

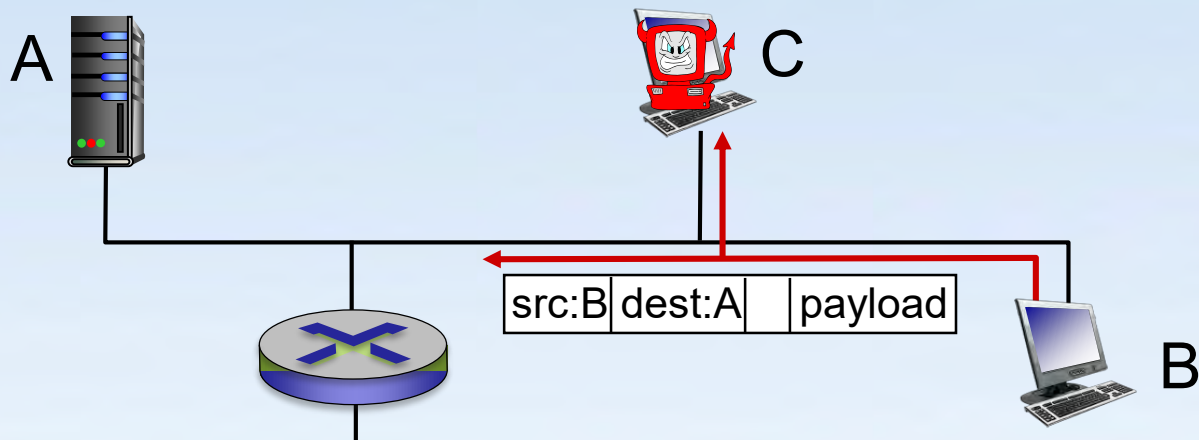
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Bad guys can sniff packets

packet “sniffing”:

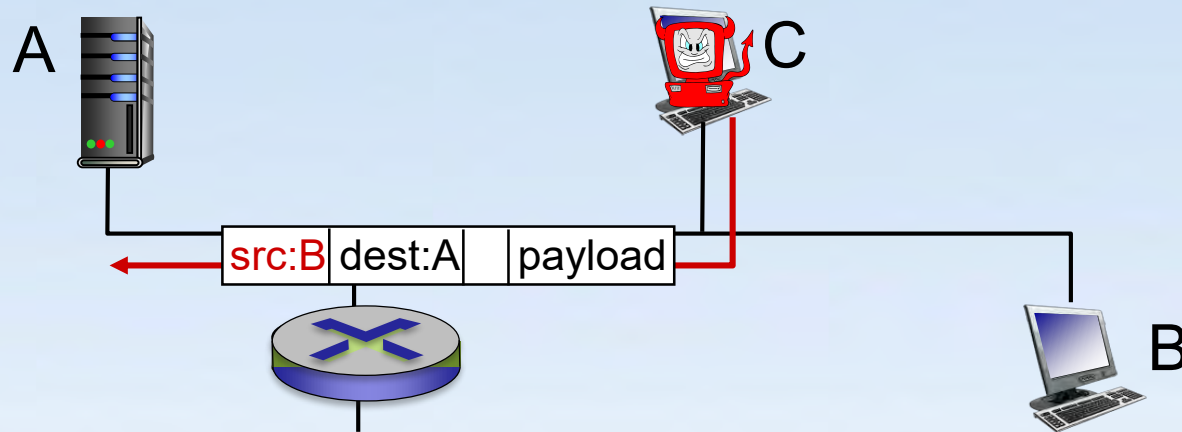
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- wireshark software used for end-of-chapter labs is a (free) packet-sniffer

Bad guys can use fake addresses

IP spoofing: send packet with false source address



... lots more on security (throughout, Chapter 8)

Outline

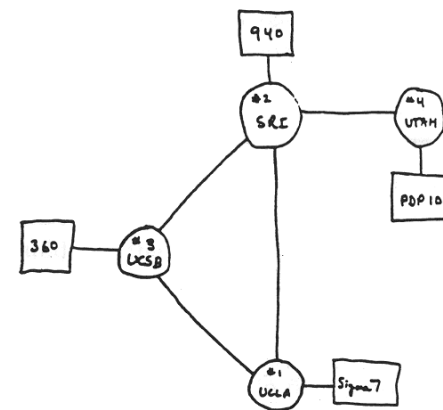
1. what *is* the Internet?
2. network edge
 - end systems, access networks, links
3. 3 network core
 - packet switching, circuit switching, network structure
4. protocol layers, service models
5. networks under attack: security
6. history
7. Hand-on lab



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
 - ARPAnet has 15 nodes



THE ARPA NETWORK

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)

Cerf and Kahn's internetworking principles:

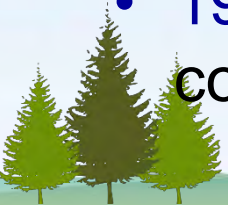
- minimalism, autonomy - no internal changes required to interconnect networks
- best effort service model
- stateless routers
- decentralized control

define today's Internet architecture

Internet history

1980-1990: new protocols, a proliferation of networks

- 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
- new national networks: CSnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks



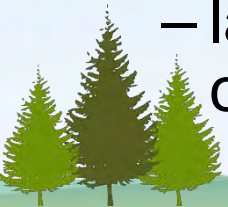
Internet history

1990, 2000 's: commercialization, the Web, new apps

- 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:

- more killer apps: instant messaging, P2P file sharing
- network security to forefront
- est. 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: ~ one billion users
- 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 EC2)



Introduction: summary

covered a “ton” of material!

- Internet overview
- what’s a protocol?
- network edge, core, access network
 - packet-switching versus circuit-switching
 - Internet structure
- performance: loss, delay, throughput
- layering, service models
- security
- history

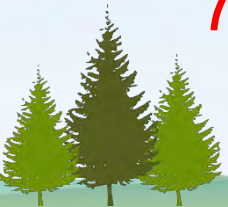
you now have:

- context, overview, “feel” of networking
- more depth, detail *to follow!*



Outline

1. what *is* the Internet?
2. network edge
 - end systems, access networks, links
3. network core
 - packet switching, circuit switching, network structure
4. protocol layers, service models
5. networks under attack: security
6. history
7. Hand-on lab



DDoS against Chat Server

- Denial of service of a chat app/server---
create too many connections to a chat
server and use up its allowed users

