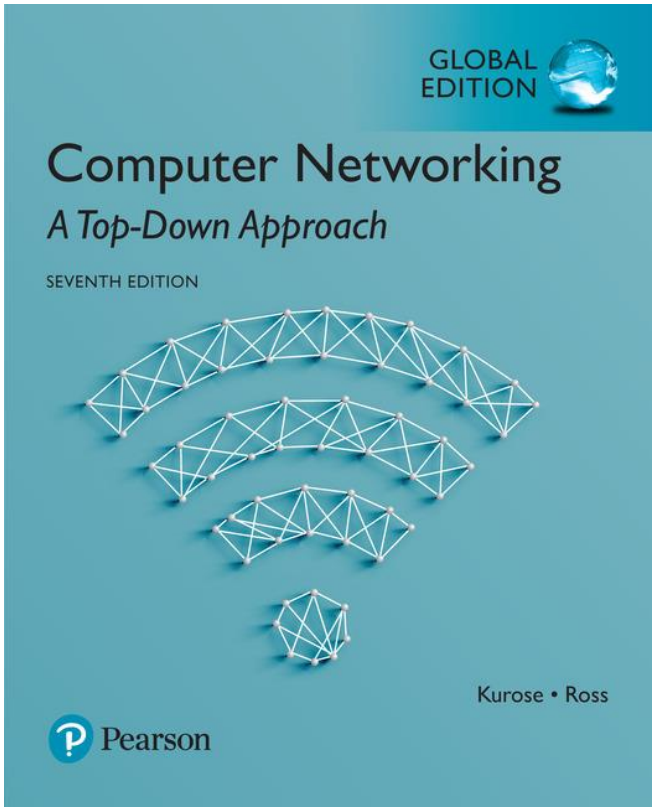
BLG 113 E – Introduction to Computer Engineering and Ethics

2021 – 2022 Fall

Technical Talk: Computer Communication

Asst. Prof. Gökhan Seçinti

Chapter 1 Introduction



Computer Networking: A Top Down Approach

7th Edition, Global Edition
Jim Kurose, Keith Ross
Pearson
April 2016

A note on the use of these Powerpoint slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Outline

1. Introduction
2. Computer Networks
   - 2.1 what is the Internet?
   - 2.2 network edge
   - 2.3 network core
   - 2.5 protocol layers, service models
   - 1.6 networks under attack: security
   - 1.7 history
3. Ethics
4. Ongoing Research at BAAL

Introduction

- **Assistant Professor,**
  Computer Engineering., İTÜ;
  Apr 4, 2019 - ...
- **Vice Chair**,
  Computer Engineering, İTÜ;
  Apr 8, 2019 – March 2021
- **Postdoctoral Research Associate,**
  Electrical and Computer Eng., Northeastern University, Boston, MA, USA;
  2017 - 2019

- PhD, Computer Engineering, İTÜ, 2012 - 2017
- MSc, Computer Engineering, İTÜ, 2009 - 2012
- BSc, Computer Engineering, İTÜ, 2005 - 2009

Research Interests:

- Aerial Networks
- MAC Protocol Design for Ad-hoc Networks
- Software-defined Networks

Introduction

Member of **Computer Networks Research .. Laboratory (Bilgisayar Ağları Araştırma Lab. – BAAL) at İ.T.Ü.**

Prof. Dr.
Sema Fatma Oktuğ
Dean

Prof. Dr.
Berk Canberk
Vice Dean (Research)

Assist. Prof. Dr.
Gökhan Seçinti

Recent[1] Selected Publications:

- "CLAN: A Robust Control Link for Aerial Mesh Networks in Contested Environments", F. R. Kilic, M. O. Ozdogan, G. Secinti, and B.Canberk, EAI INISCOM, 2021. [Best Paper Award]
- "Chain RTS/CTS Scheme for Aerial Multihop Communications", T.T. Sarı, G. Secinti, IEEE CCNC 2021.
- "WiFED Mobile: WiFi Friendly Energy Delivery With Mobile Distributed Beamforming", S Mohanti, E Bozkaya, MY Naderi, B Canberk, G Secinti, KR Chowdhury, IEEE/ACM Transactions on Networkingi 2021.
- "AI-Driven Partial Topology Discovery Algorithm for Broadband Networks", K Duran, B Karanlik, B Canberk, 2021 IEEE 18th Annual Consumer Communications & Networking Conference, 2021.
- "Waste-to-Energy Framework: An intelligent energy recycling management", K Kaya, E Ak, Y Yaslan, SF Oktug, Sustainable Computing: Informatics and Systems, 2021.
- "Mobile Air Quality Monitoring in the ITU Campus", SF Oktuğ, E Onay, EN Şen, 2020 28th Signal Processing and Communications Applications Conference, 2020.

[1] This list compiled in March,2021.

Introduction to Computer Net.

our goal:

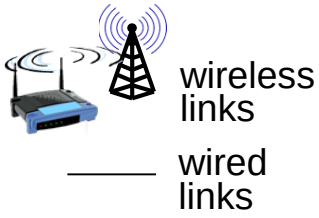
- get "feel" and terminology
- more depth, detail *later* in course
- approach:
  - use Internet as example

overview:

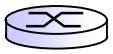
- what's the Internet?
- what's a protocol?
- network edge; hosts, access net, physical media
- network core: packet/circuit switching, Internet structure
- security
- protocol layers, service models
- history

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

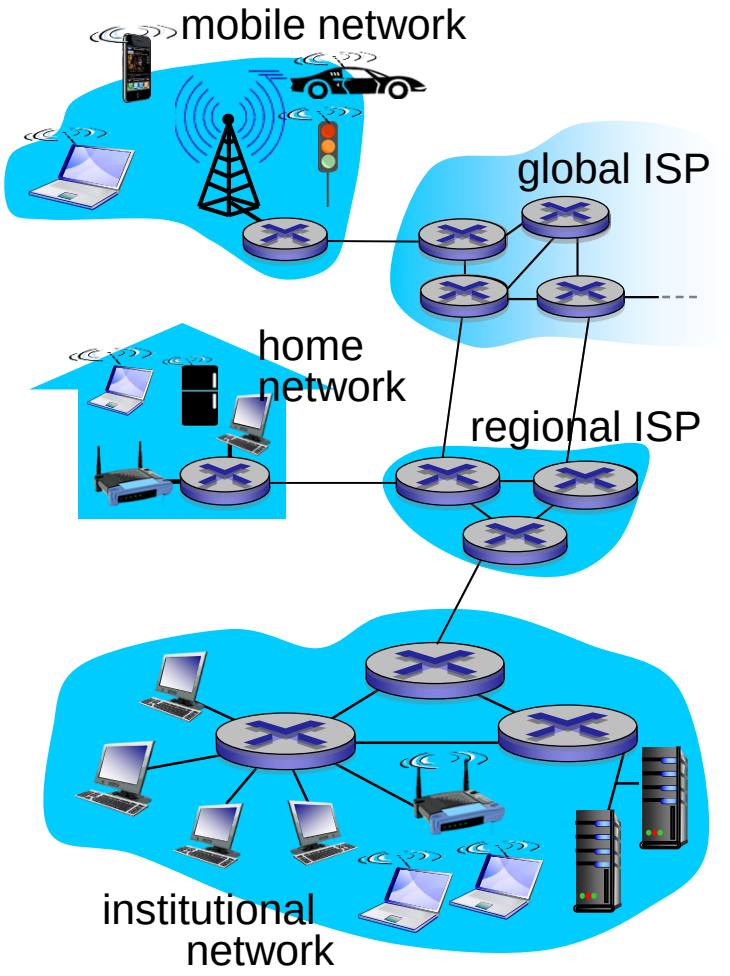
- billions of connected computing devices:
  - *hosts* = *end systems*
  - running *network apps*



- *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

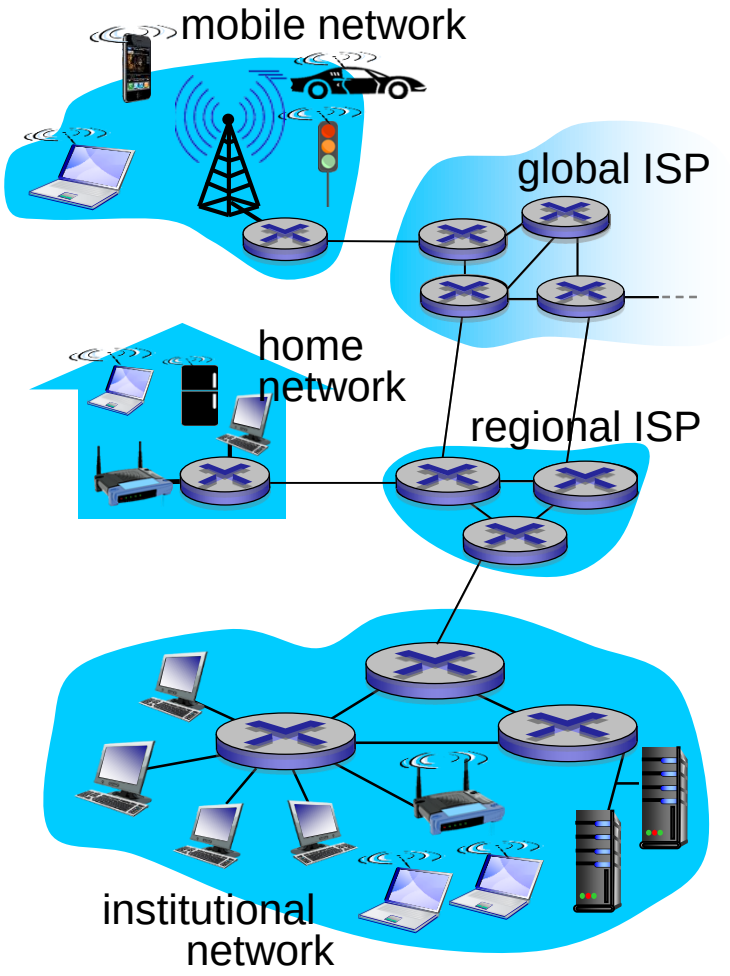
Slingbox: watch,
control cable TV remotely

sensorized,
bed
mattress

Internet phones

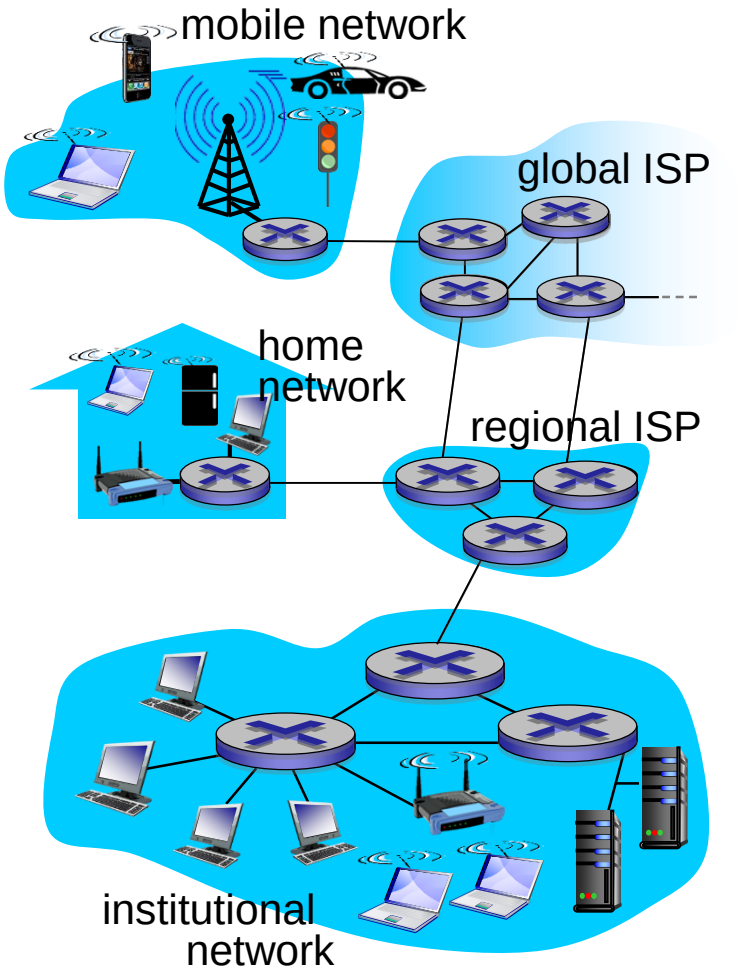
What's the Internet: "nuts and bolts" view

- *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

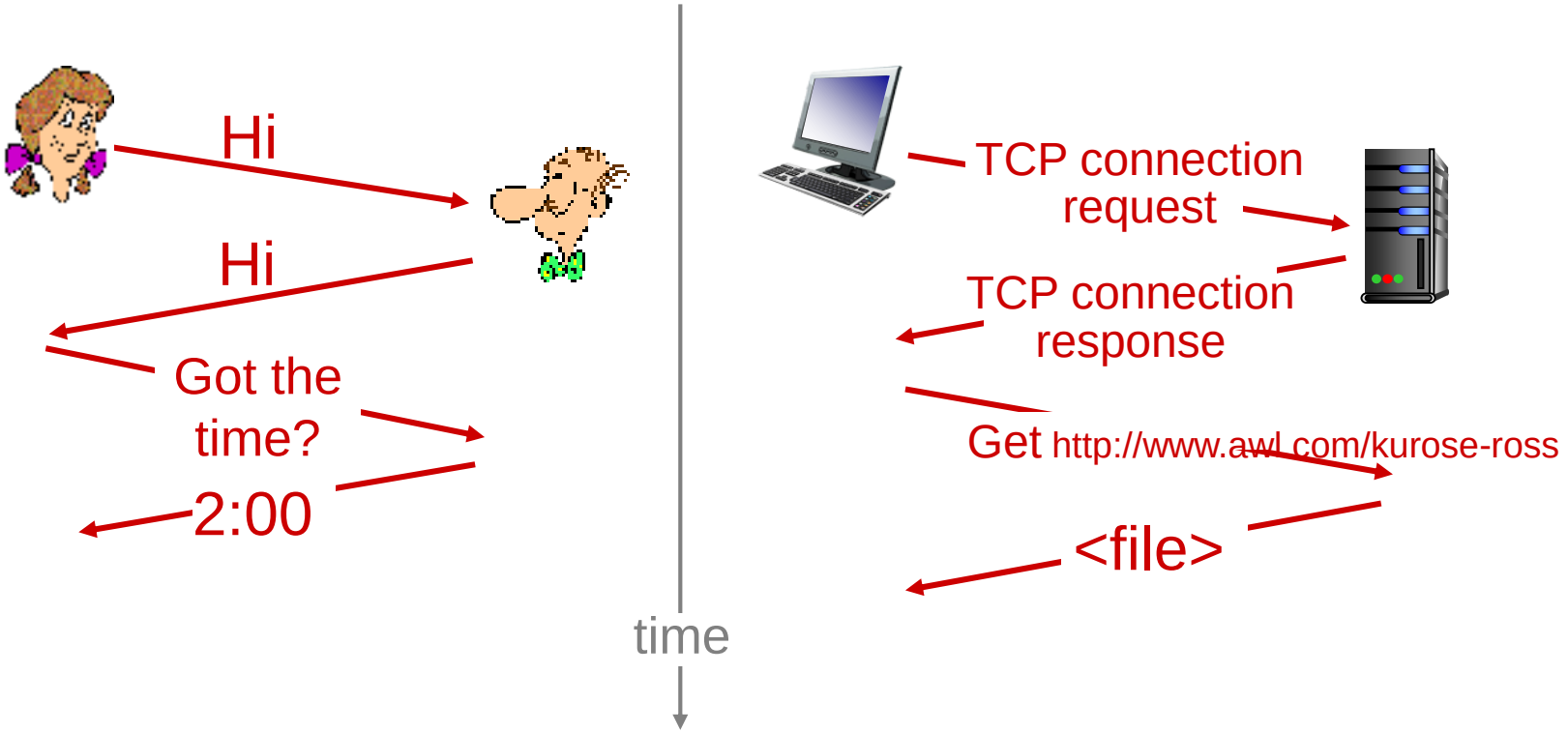
network protocols:

- 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

1.1 what *is* the Internet?

1.2 network edge

- end systems, access networks, links

1.3 network core

- packet switching, circuit switching, network structure

1.4 delay, loss, throughput in networks

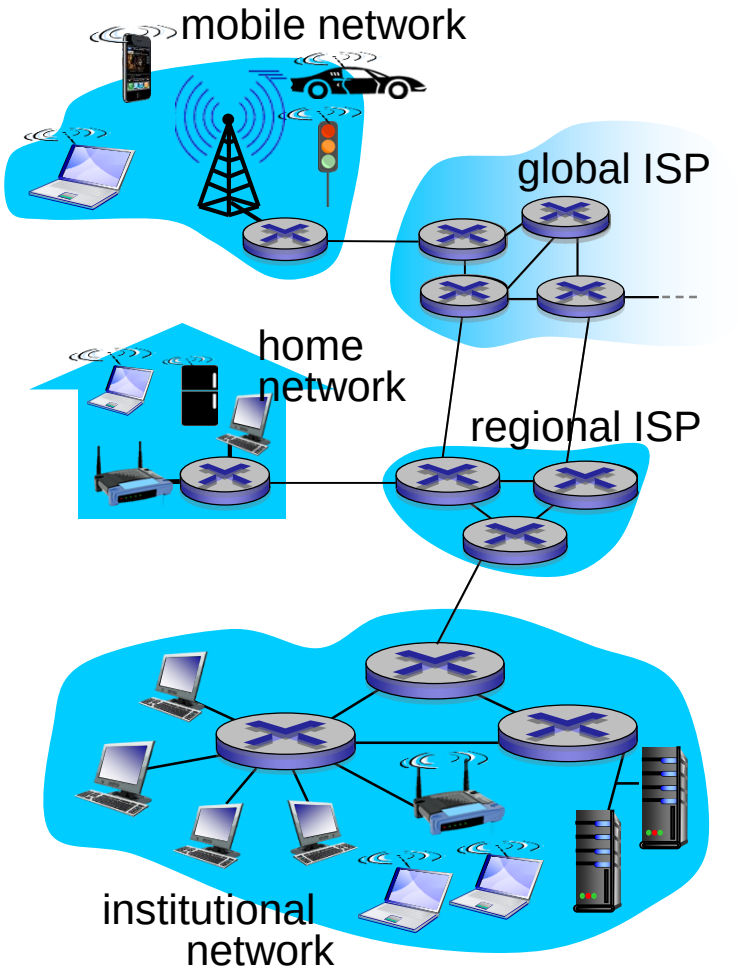
1.5 protocol layers, service models

1.6 networks under attack: security

1.7 history

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



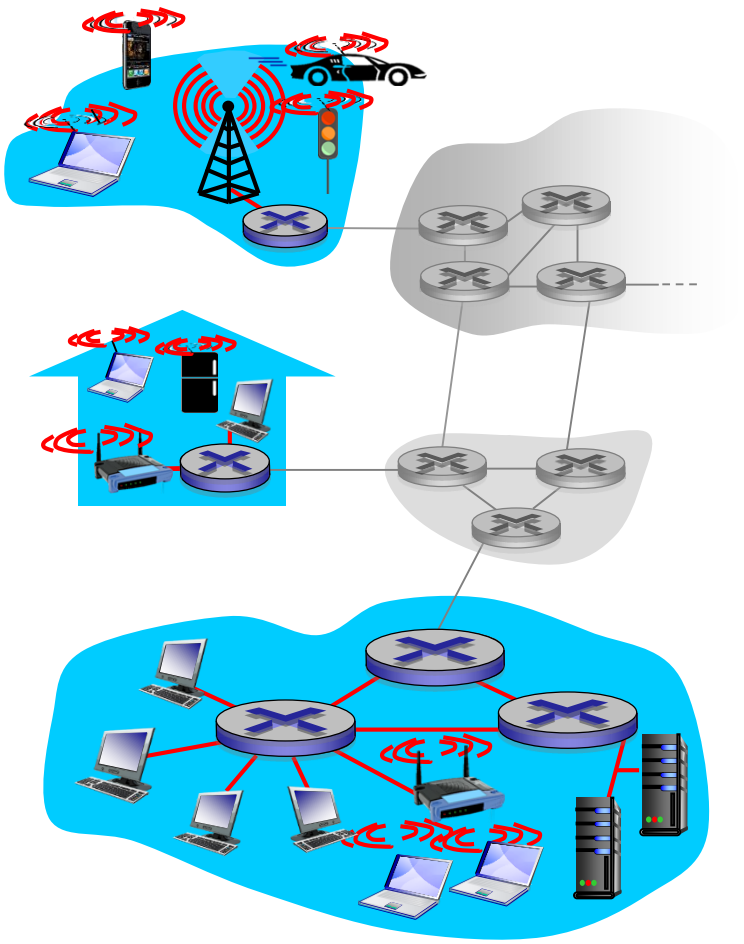
Access networks and physical media

Q: How to connect end systems to edge router?

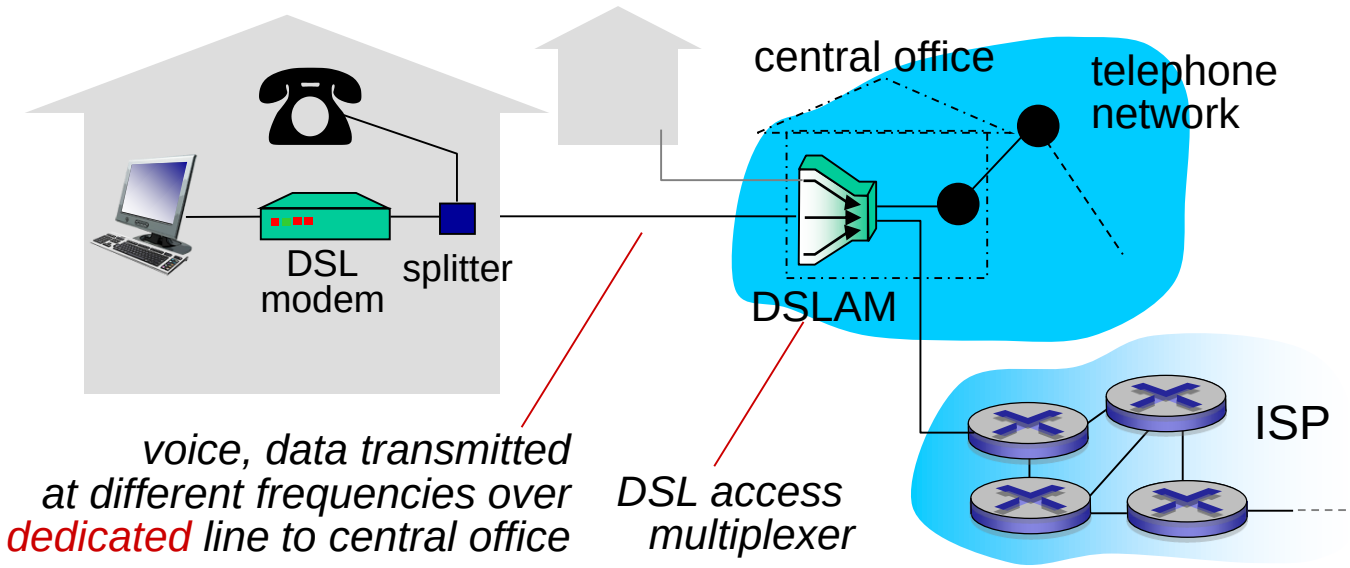
- residential access nets
- institutional access networks (school, company)
- mobile access networks

keep in mind:

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

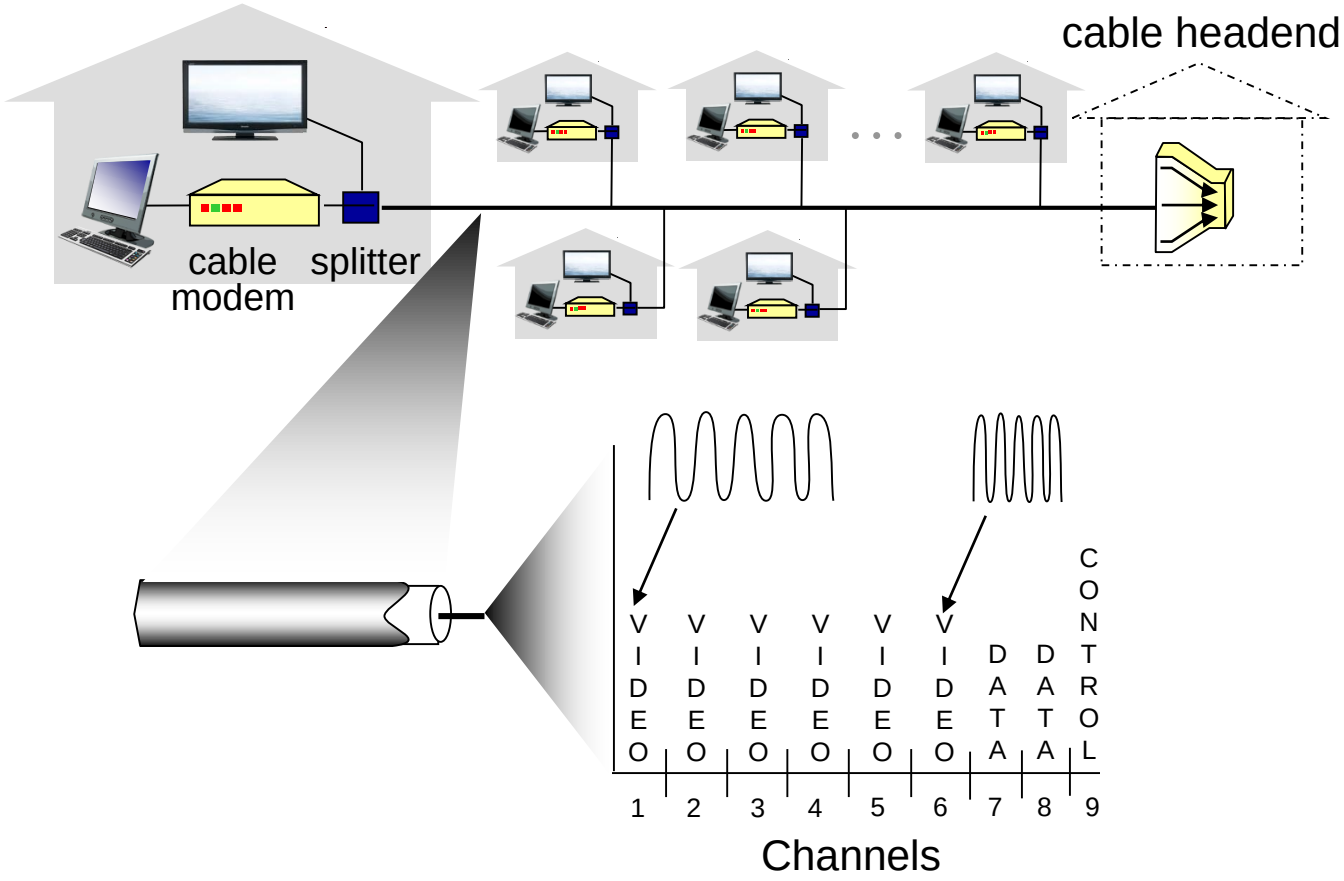


Access network: digital subscriber line (DSL)



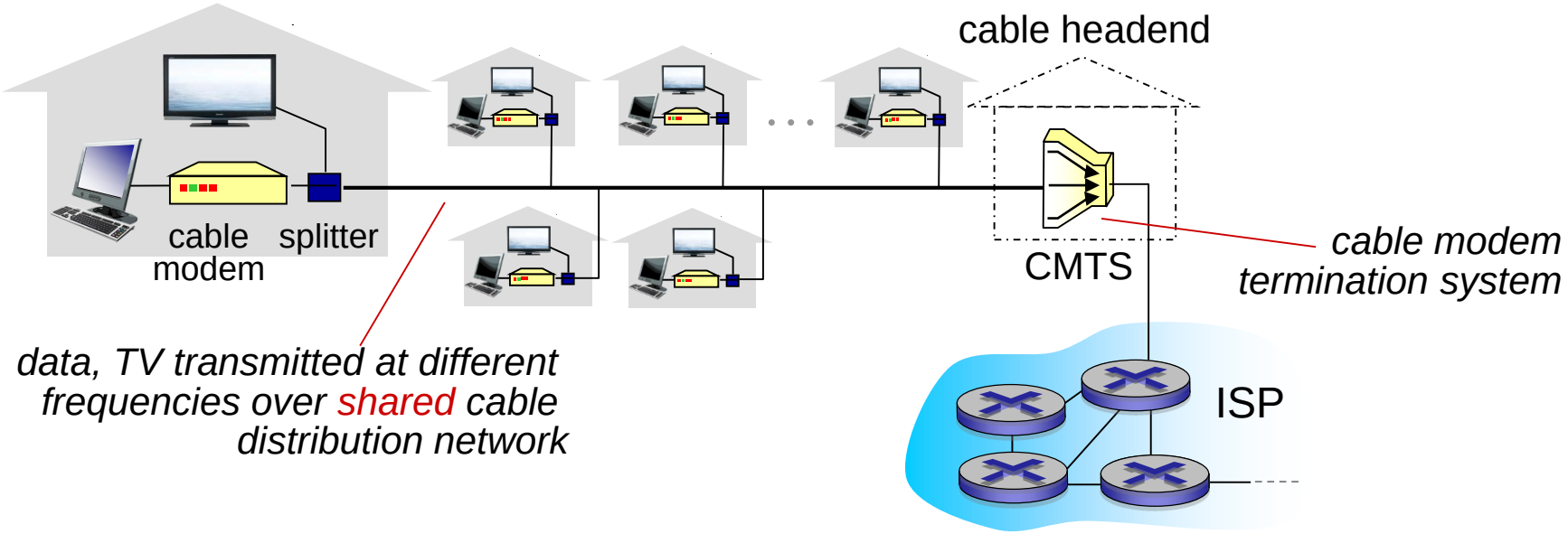
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access network: cable network



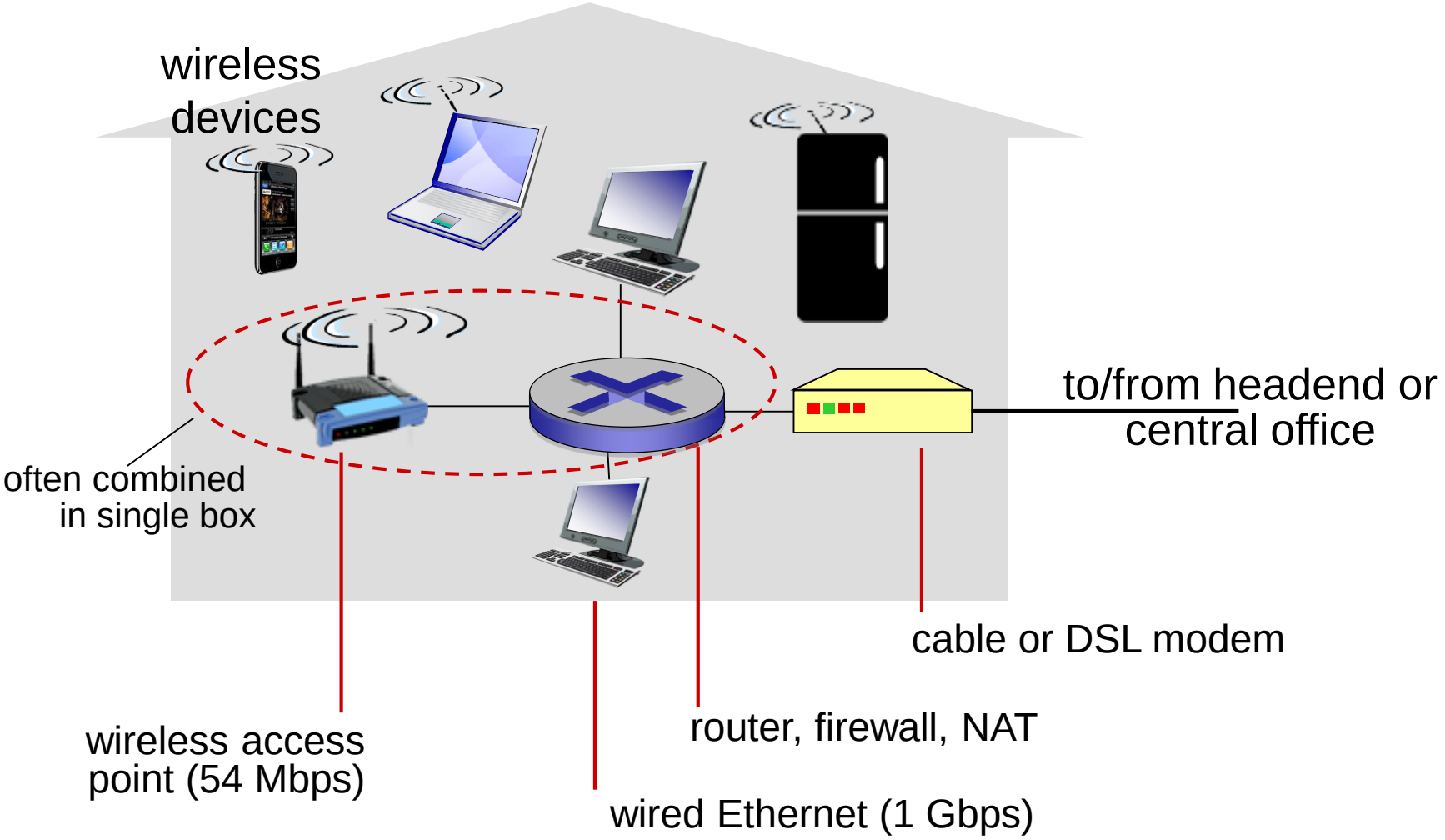
frequency division multiplexing: different channels transmitted in different frequency bands

Access network: cable network

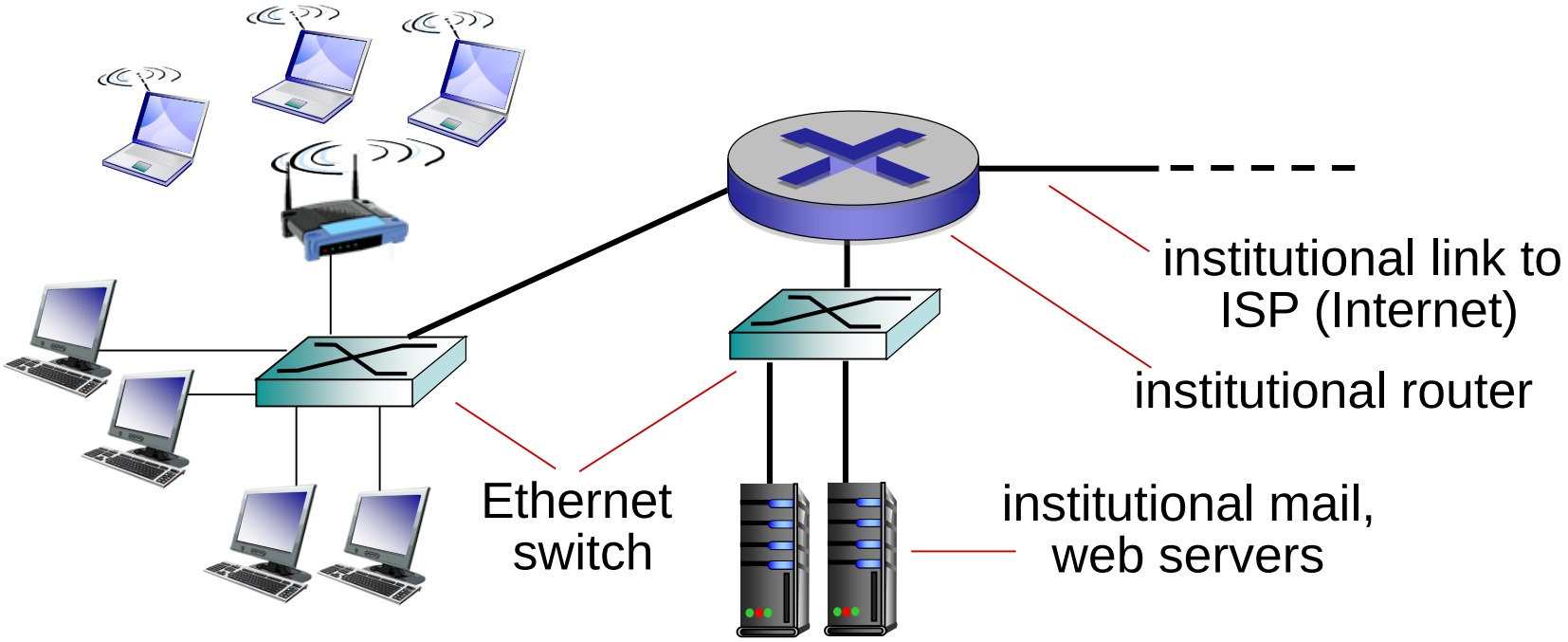


- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

Access network: home 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

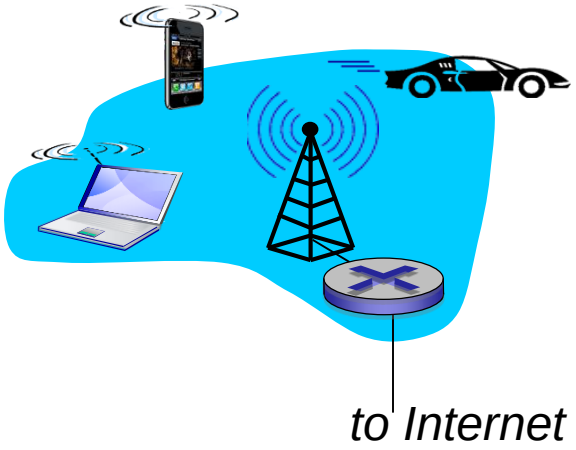
- shared *wireless* access network connects end system to router
  - via base station aka "access point"

wireless LANs:

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

wide-area wireless access

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



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

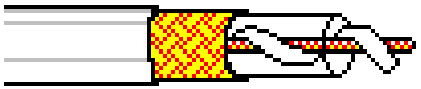
twisted pair (TP)

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

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:
  - high-speed point-to-point transmission (e.g., 10's-100's 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)
  - 270 msec end-end delay
  - geosynchronous versus low altitude

Chapter 1: roadmap

1.1 what *is* the Internet?

1.2 network edge

- end systems, access networks, links

1.3 network core

- packet switching, circuit switching, network structure

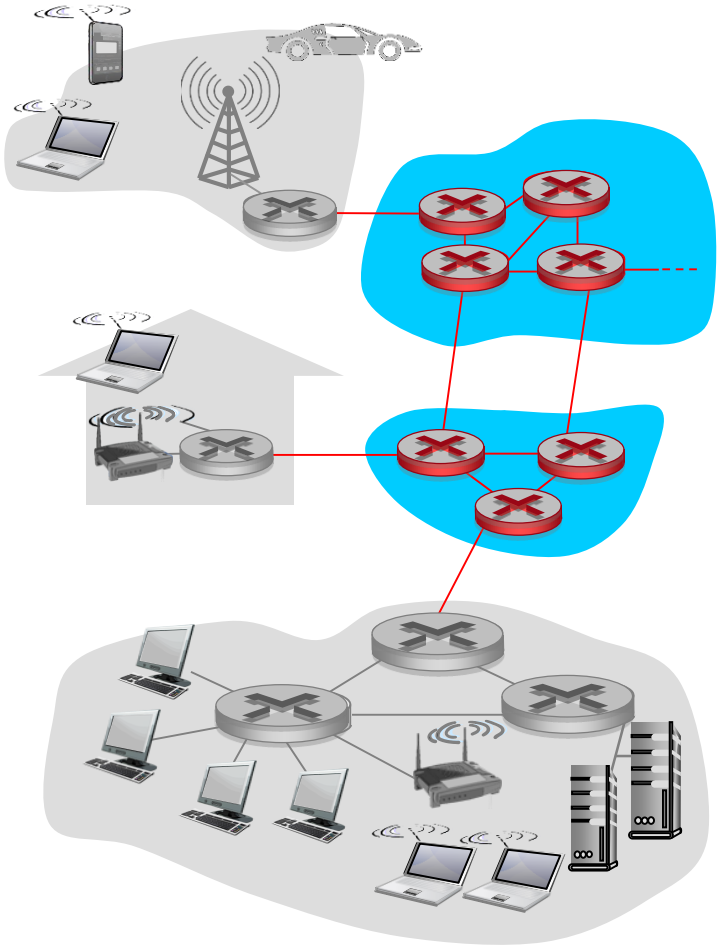
1.5 protocol layers, service models

1.6 networks under attack: security

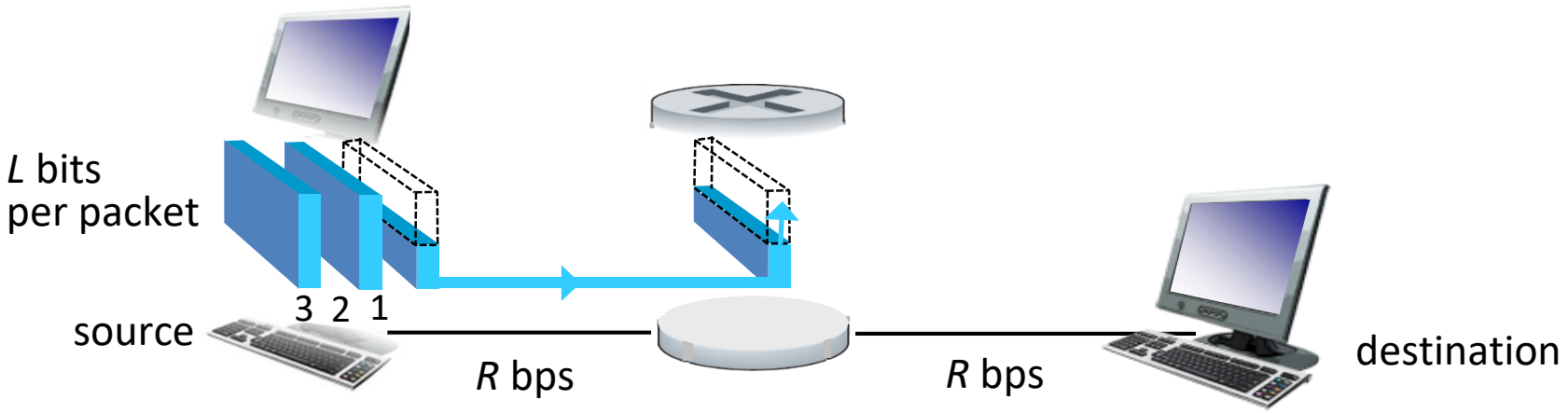
1.7 history

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



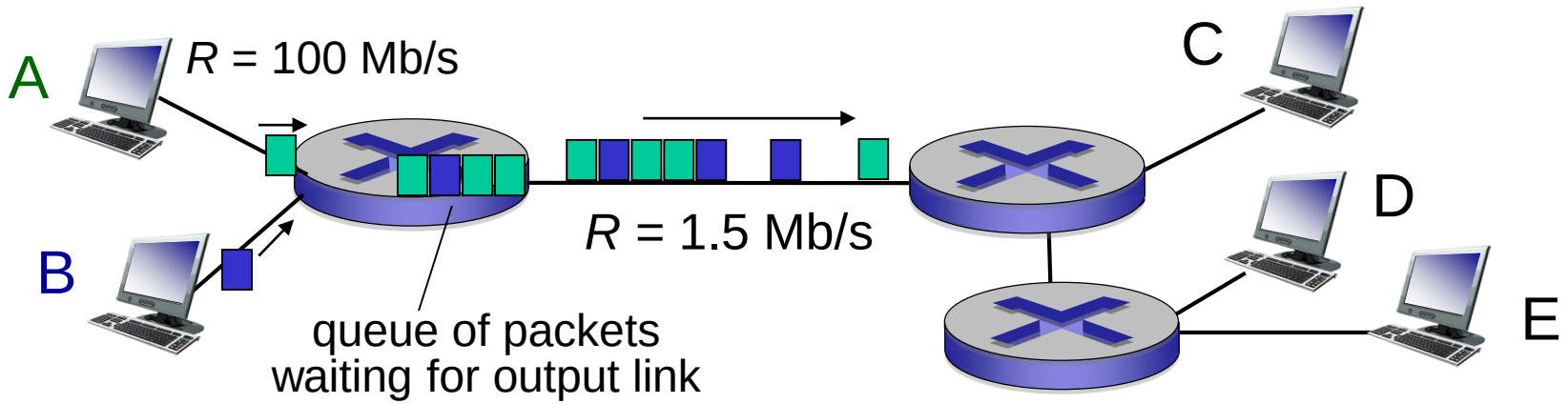
- takes *L*/*R* seconds to transmit (push out) *L*-bit packet into link at *R* bps
- *store and forward:* entire packet must arrive at router before it can be transmitted on next link
- end-end delay = 2*L*/*R* (assuming zero propagation delay)

one-hop numerical example:

- *L* = 7.5 Mbits
- *R* = 1.5 Mbps
- one-hop transmission delay = 5 sec

more on delay shortly …

Packet Switching: queueing delay, loss



queuing and loss:

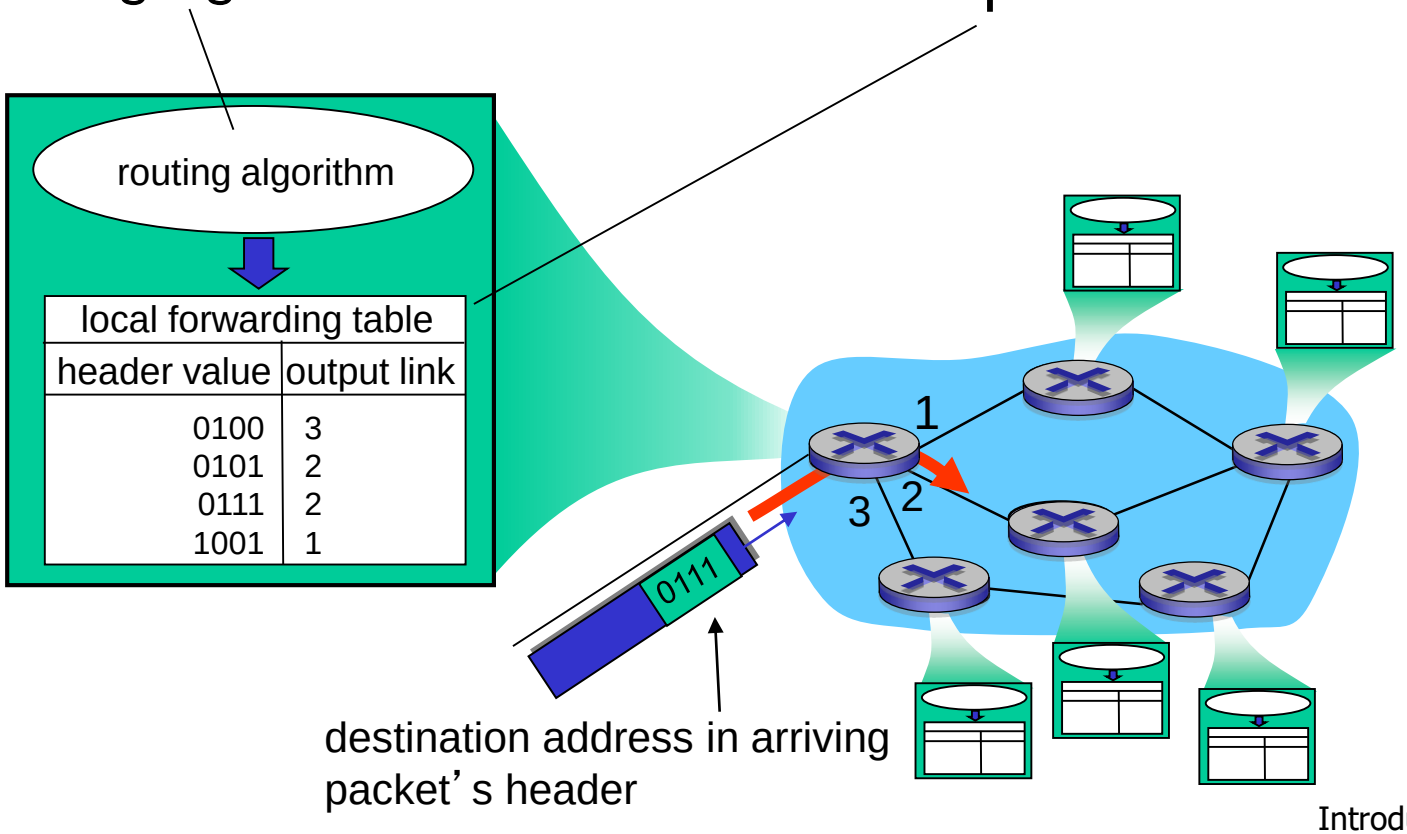
- if arrival rate (in bits) to link exceeds transmission rate of link for a period of time:
  - packets will queue, wait to be transmitted on link
  - packets can be dropped (lost) if memory (buffer) fills up

Two key network-core functions

routing: determines source-destination route taken by packets

- *routing algorithms*

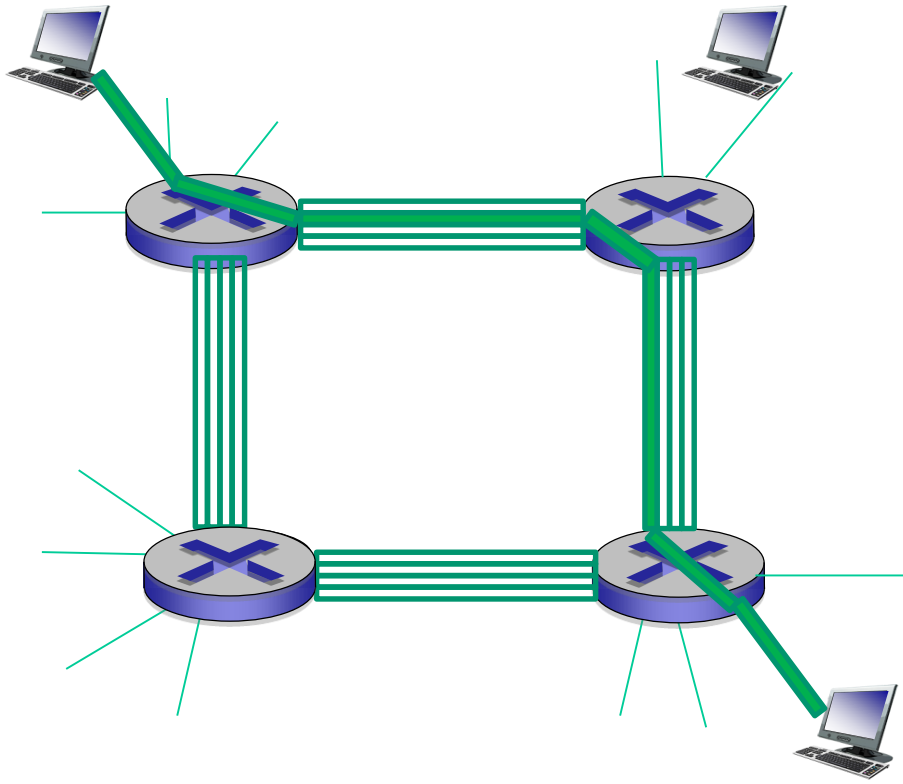
forwarding: move packets from router's input to appropriate router output



Alternative core: circuit switching

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

- in diagram, each link has four circuits.
  - call gets 2nd circuit in top link and 1st circuit in right link.
- dedicated resources: no sharing
  - circuit-like (guaranteed) performance
- circuit segment idle if not used by call *(no sharing)*
- commonly used in traditional telephone networks

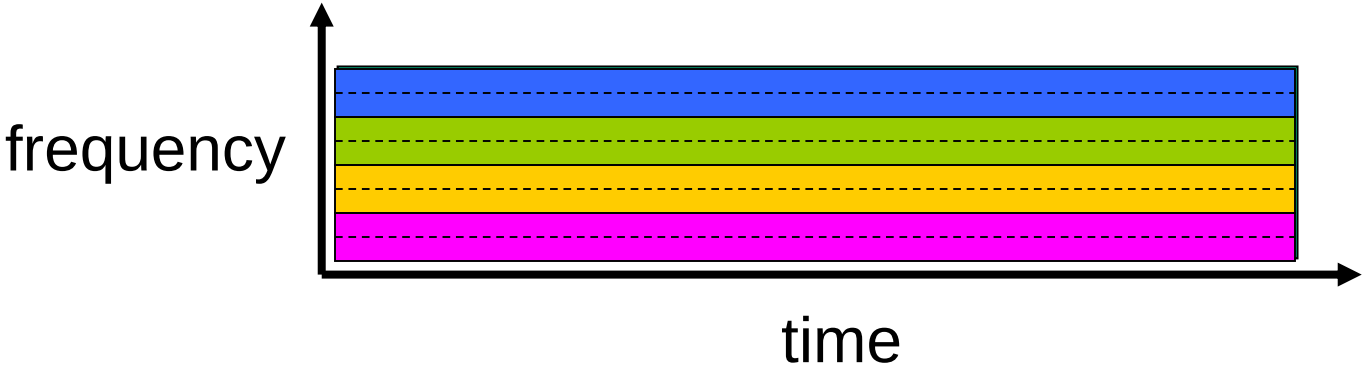


Circuit switching: FDM versus TDM

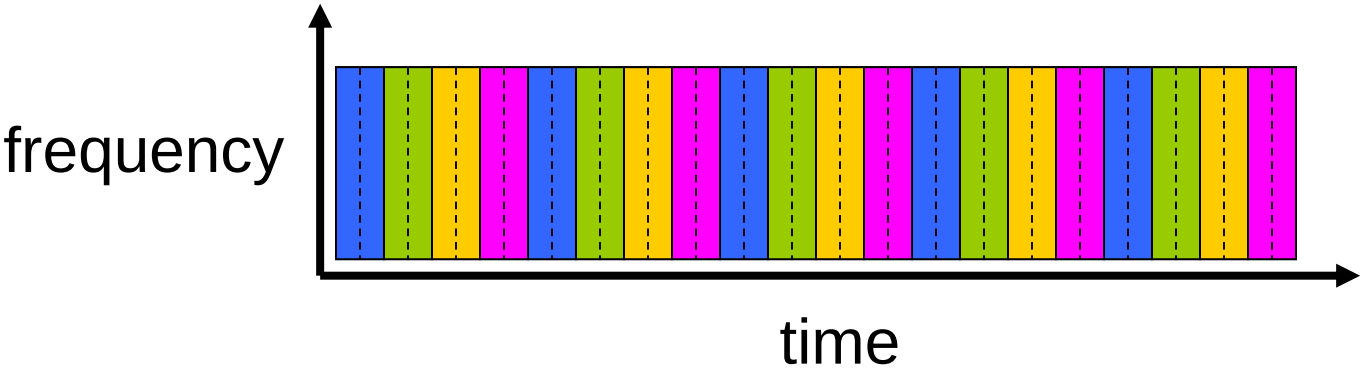
Example:

4 users

FDM



TDM

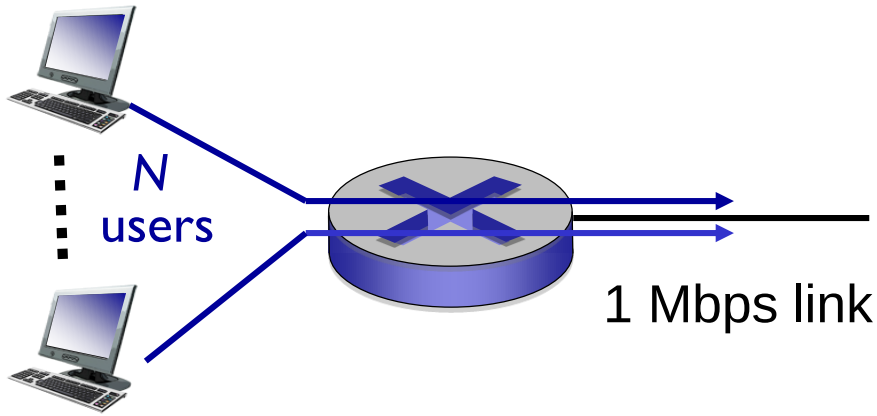


Packet switching versus circuit switching

packet switching allows more users to use network!

example:

- 1 Mb/s link
- each user:
  - 100 kb/s when "active"
  - active 10% of time



- *circuit-switching:*
  - 10 users
- *packet switching:*
  - with 35 users, probability > 10 active at same time is less than .0004 *

Q: how did we get value 0.0004?

Q: what happens if > 35 users ?

* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Packet switching versus circuit switching

is packet switching a "slam dunk winner?"

- great for bursty data
  - resource sharing
  - simpler, no call setup
- excessive congestion possible: packet delay and loss
  - protocols needed for reliable data transfer, congestion control
- *Q:* How to provide circuit-like behavior?
  - bandwidth guarantees needed for audio/video apps
  - still an unsolved problem (chapter 7)

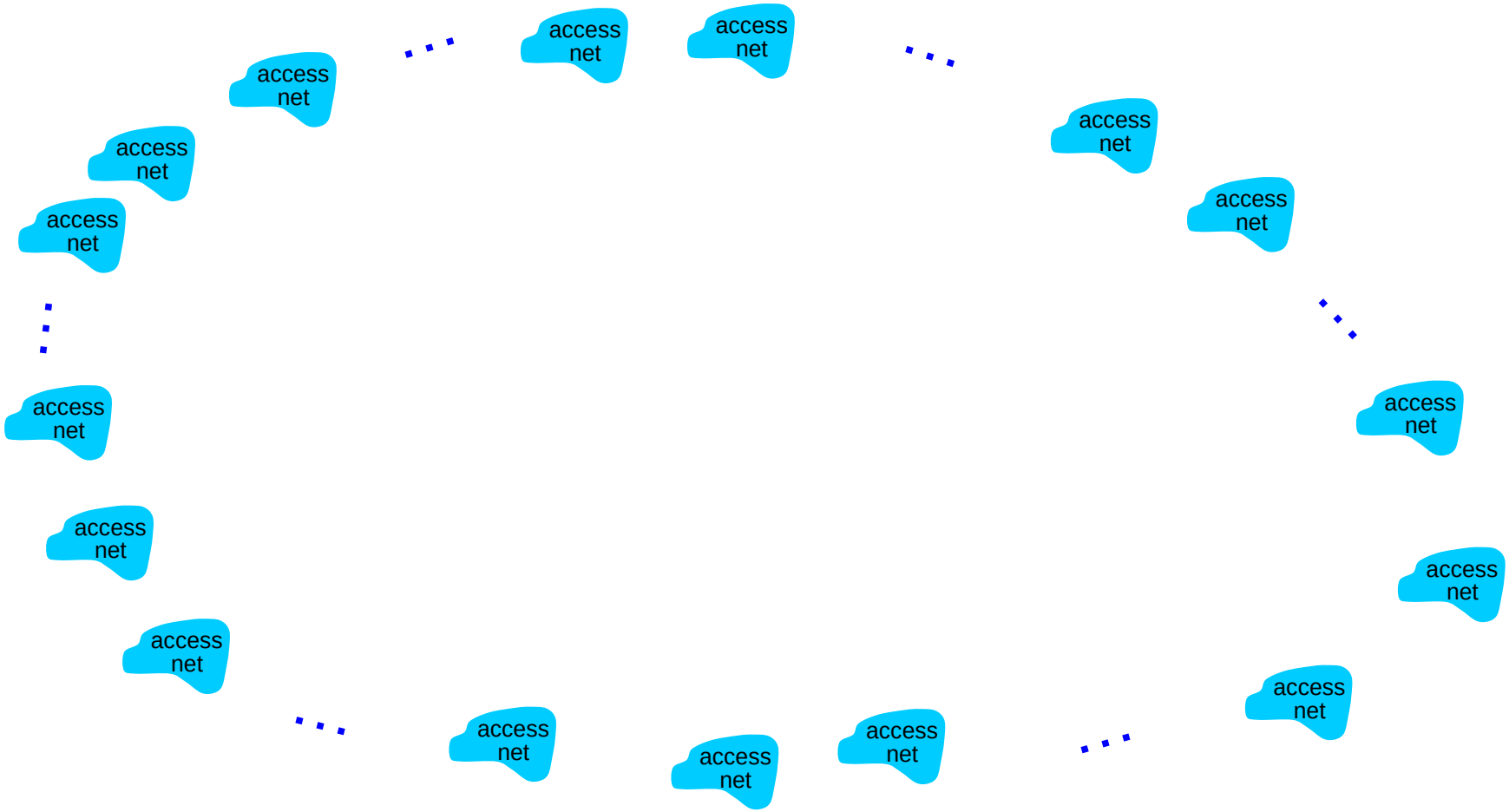
Q: human analogies of reserved resources (circuit switching) versus on-demand allocation (packet-switching)?

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

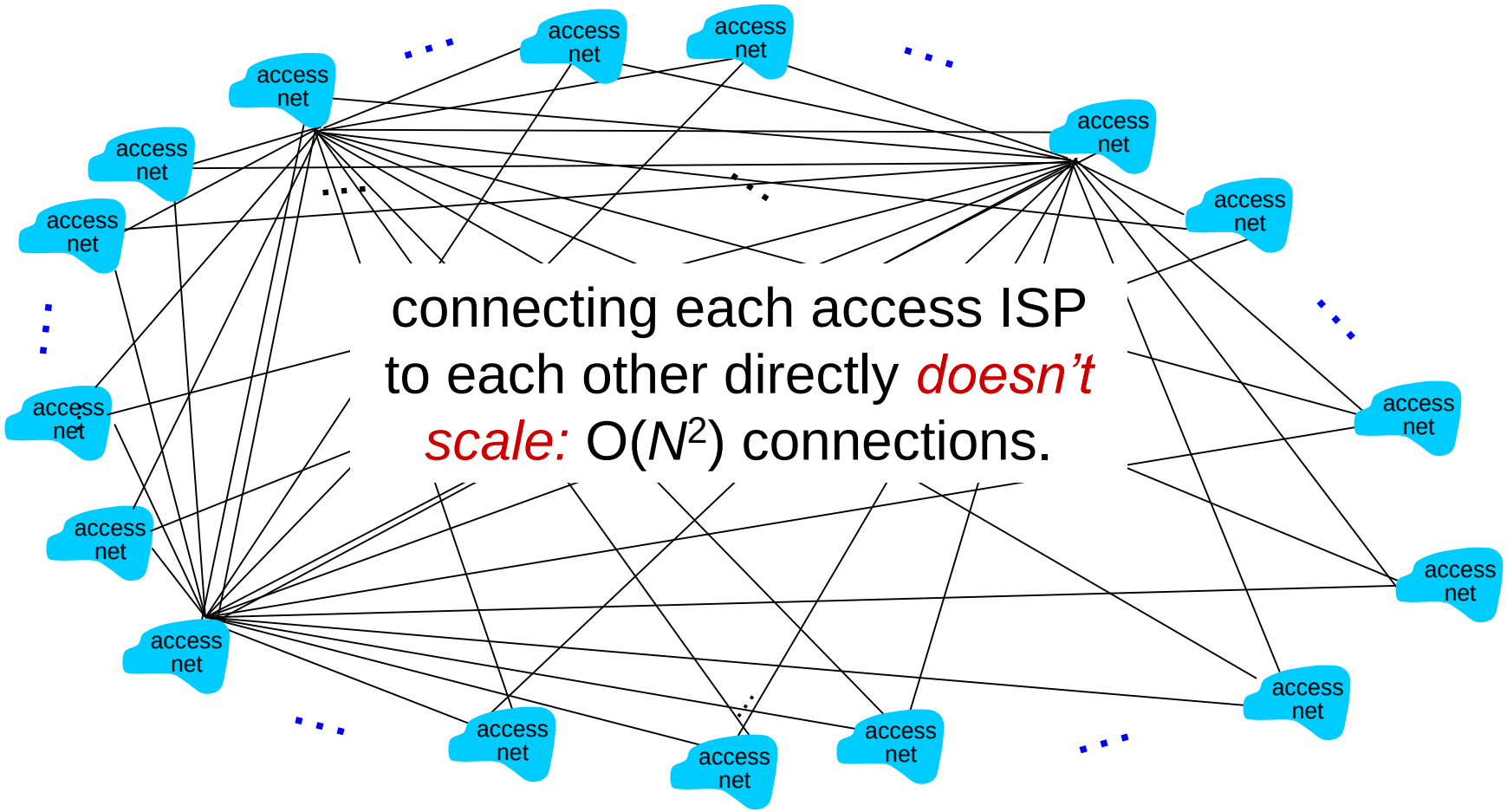
Internet structure: network of networks

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



Internet structure: network of networks

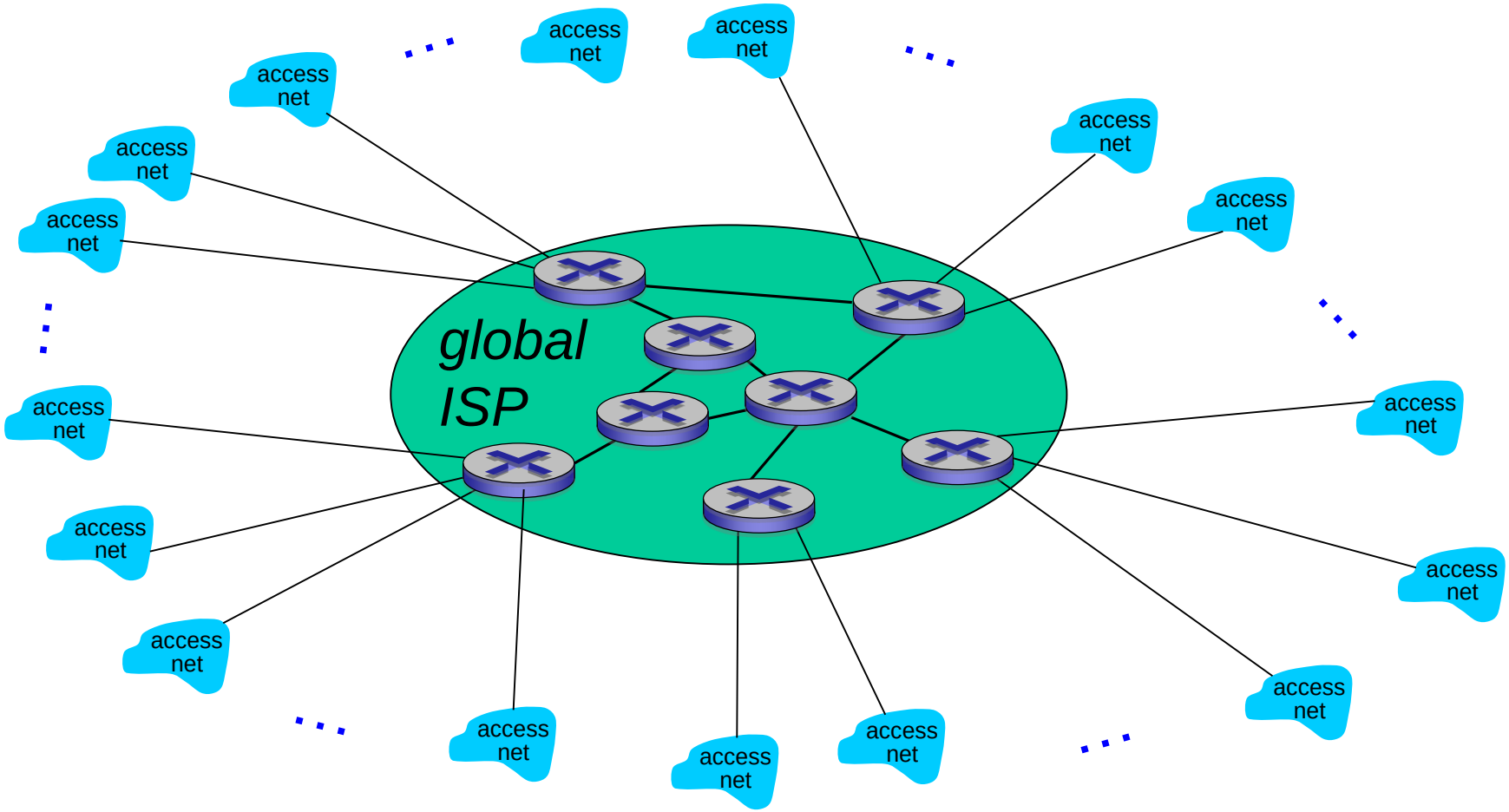
Option: connect each access ISP to every other access ISP?



Internet structure: network of networks

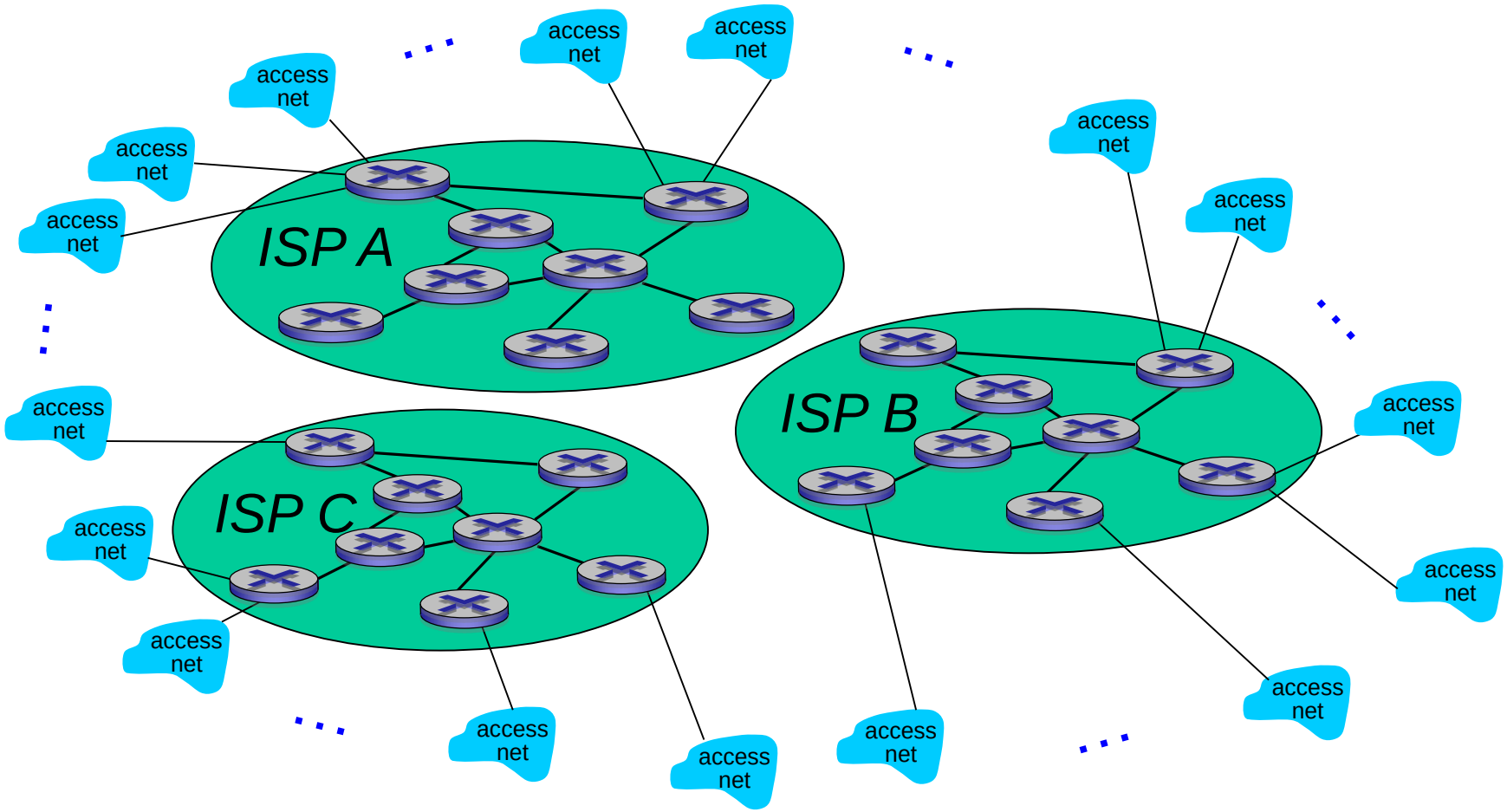
Option: connect each access ISP to one global transit ISP?

Customer and provider ISPs have economic agreement.



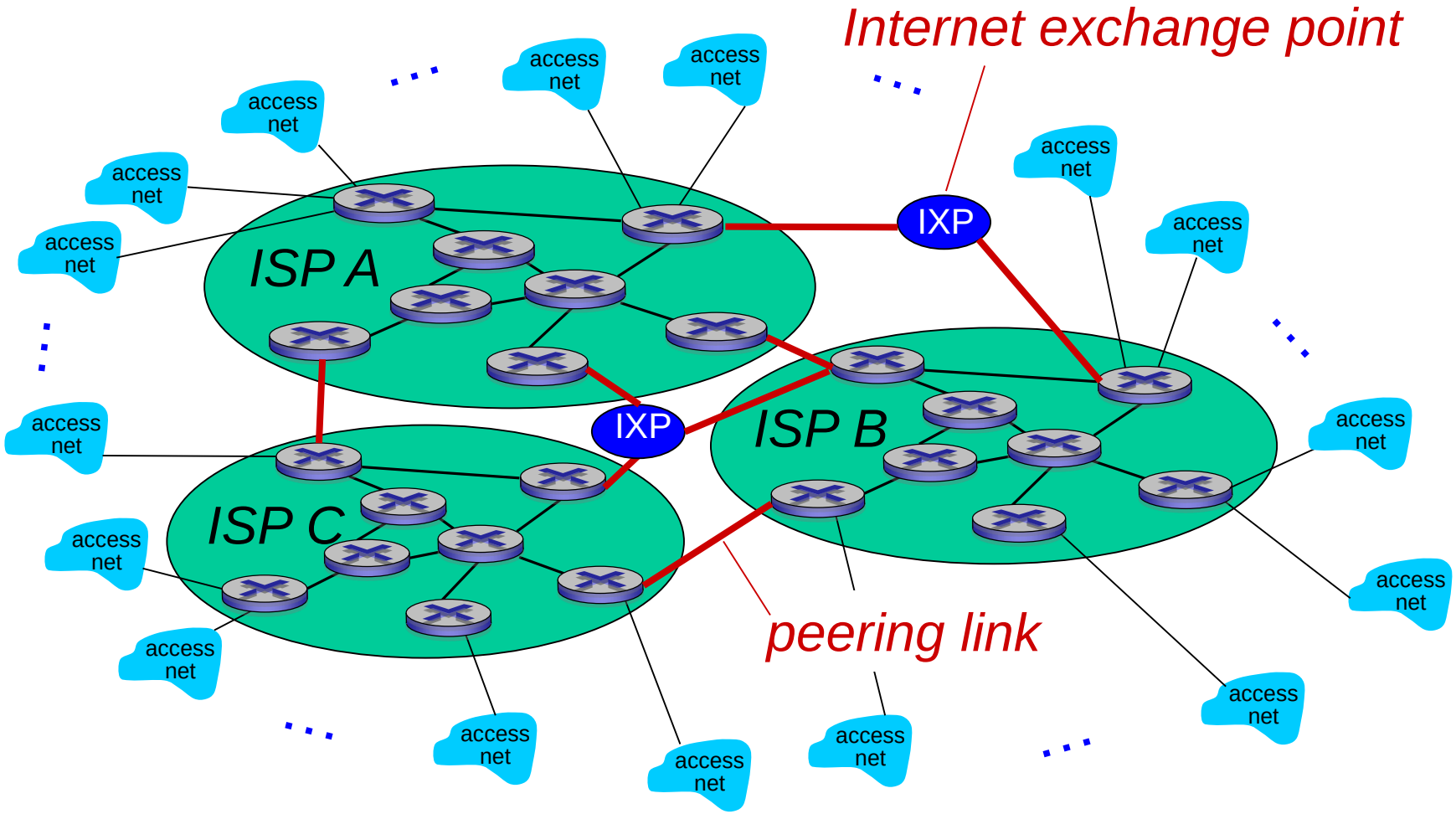
Internet structure: network of networks

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



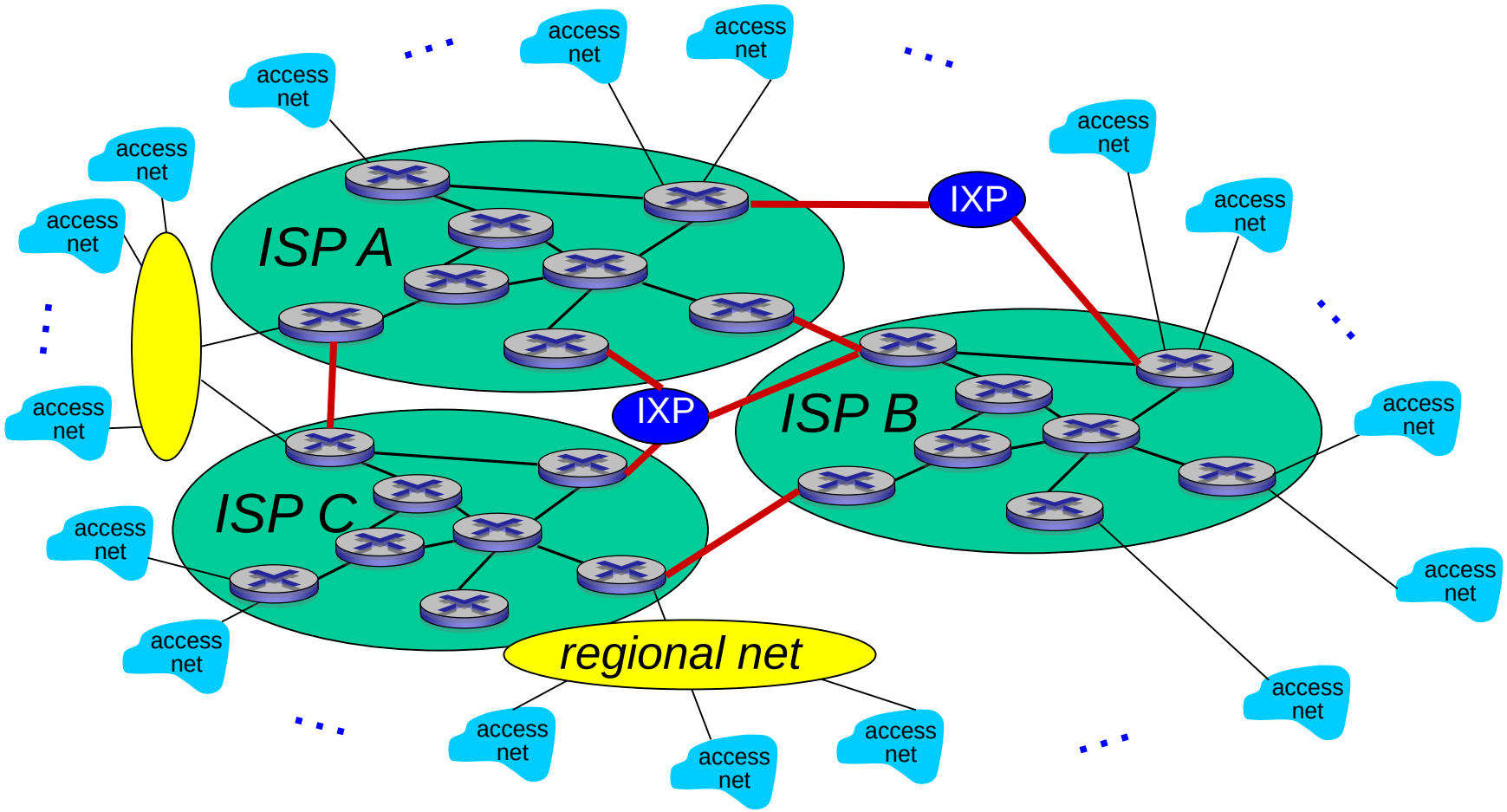
Internet structure: network of networks

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



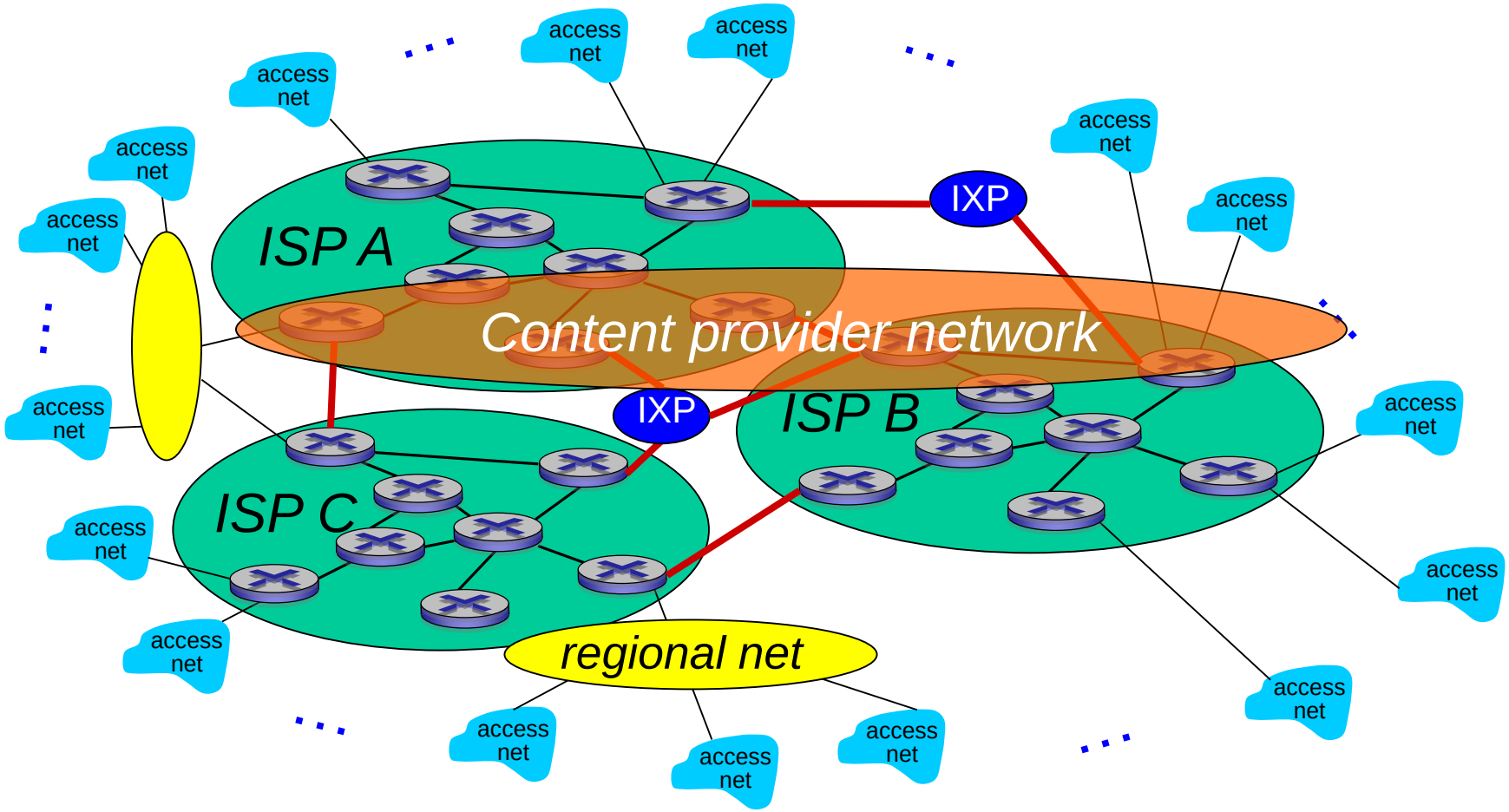
Internet structure: network of networks

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

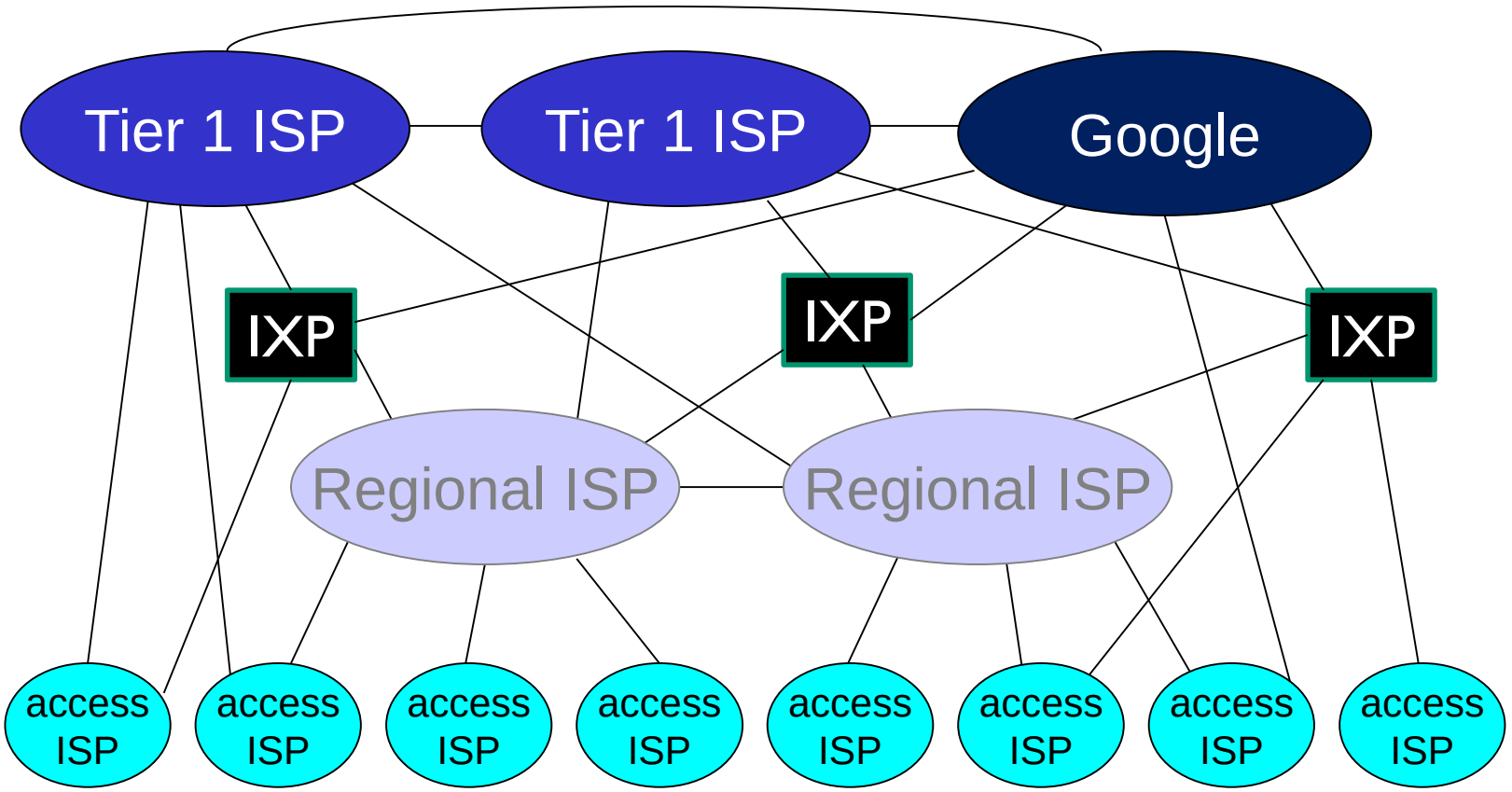


Internet structure: network of networks

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

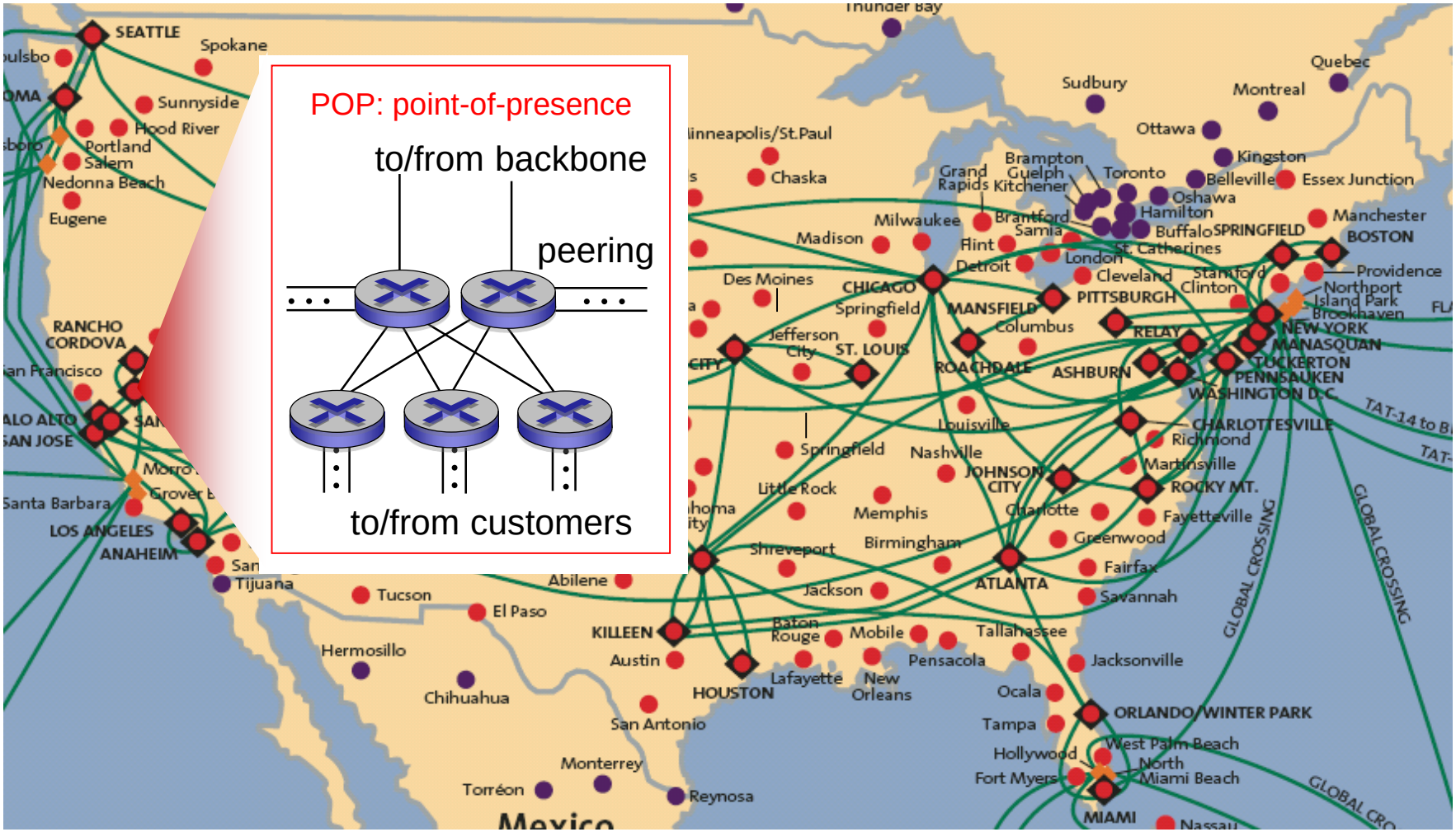


Internet structure: network of networks



- 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 it data centers to Internet, often bypassing tier-1, regional ISPs

Tier-1 ISP: e.g., Sprint



Chapter 1: roadmap

1.1 what *is* the Internet?

1.2 network edge

- end systems, access networks, links

1.3 network core

- packet switching, circuit switching, network structure

1.5 protocol layers, service models

1.6 networks under attack: security

1.7 history

Protocol "layers"

Networks are complex, with many "pieces":

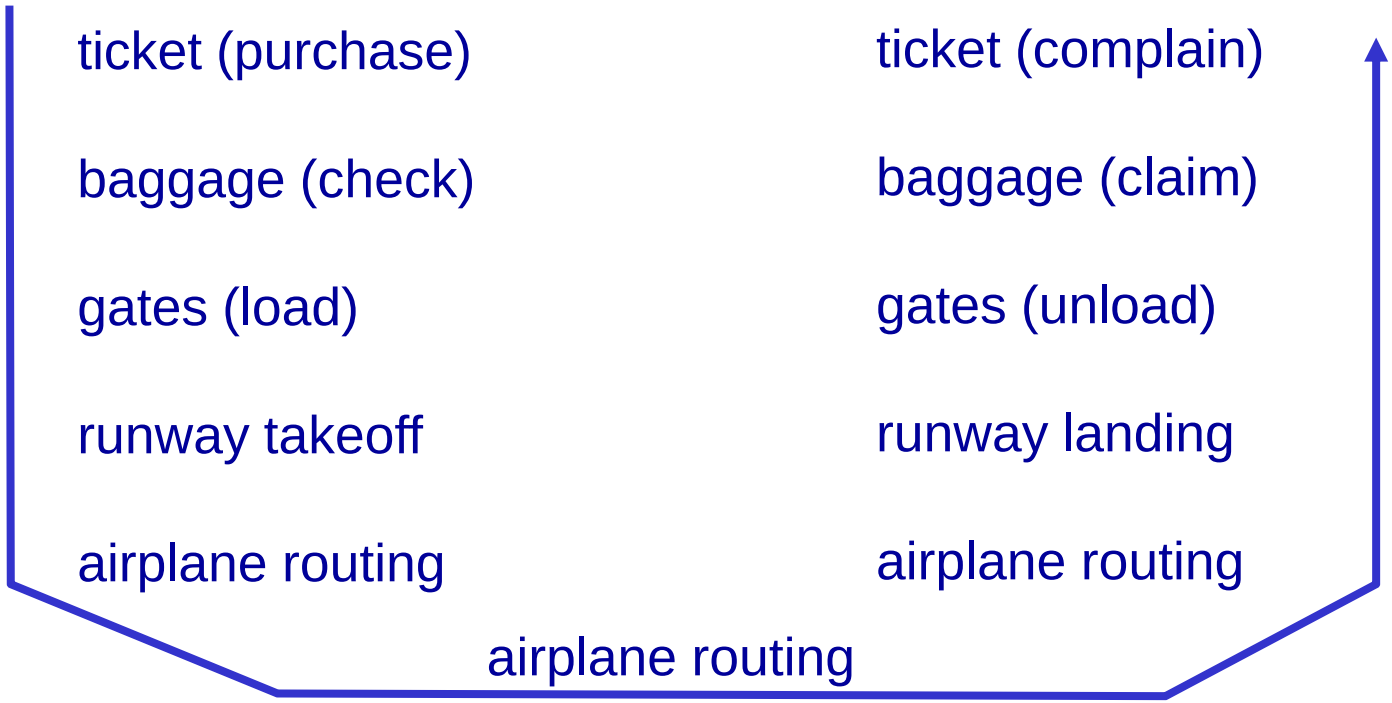
- hosts
- routers
- links of various media
- applications
- protocols
- hardware, software

Question:

is there any hope of *organizing* structure of network?

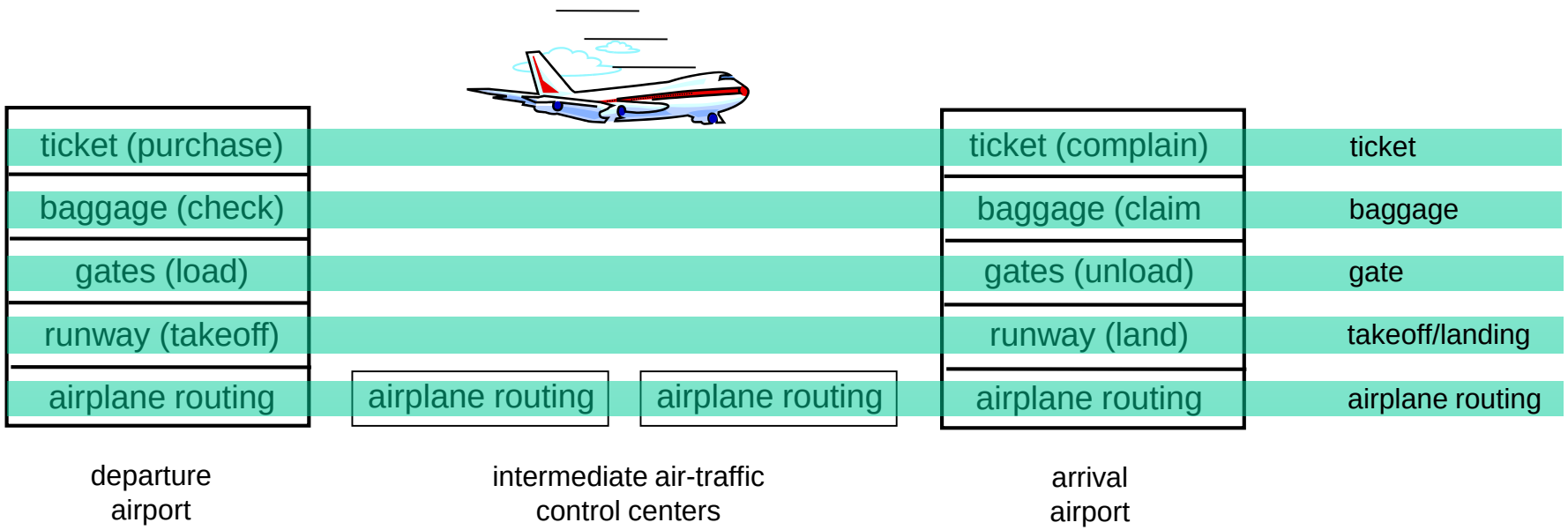
…. or at least our discussion of networks?

Organization of air travel



- a series of steps

Layering of airline functionality



layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

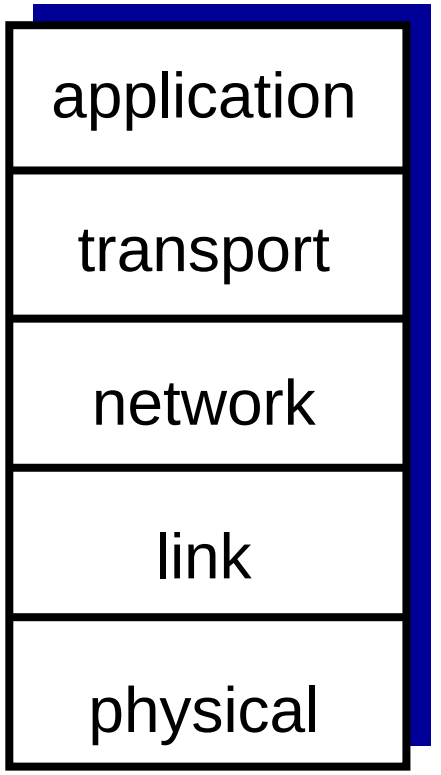
Why layering?

dealing with complex systems:

- explicit structure allows identification, relationship of complex system's pieces
  - layered *reference model* for discussion
- modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system
  - e.g., change in gate procedure doesn't affect rest of system
- layering considered harmful?

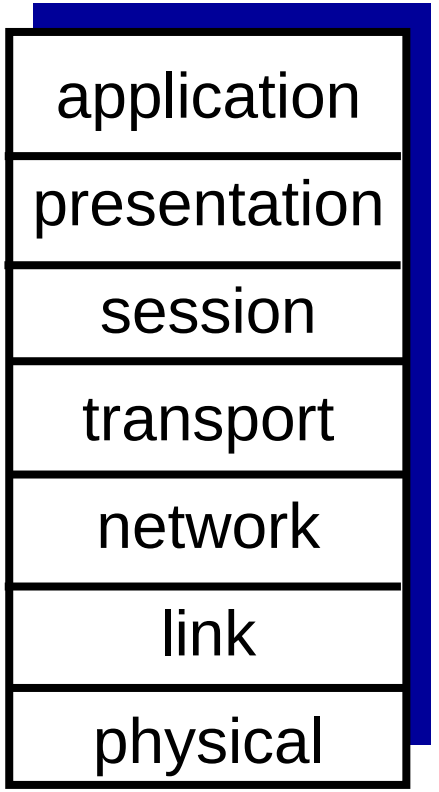
Internet protocol stack

- *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 neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits "on the wire"

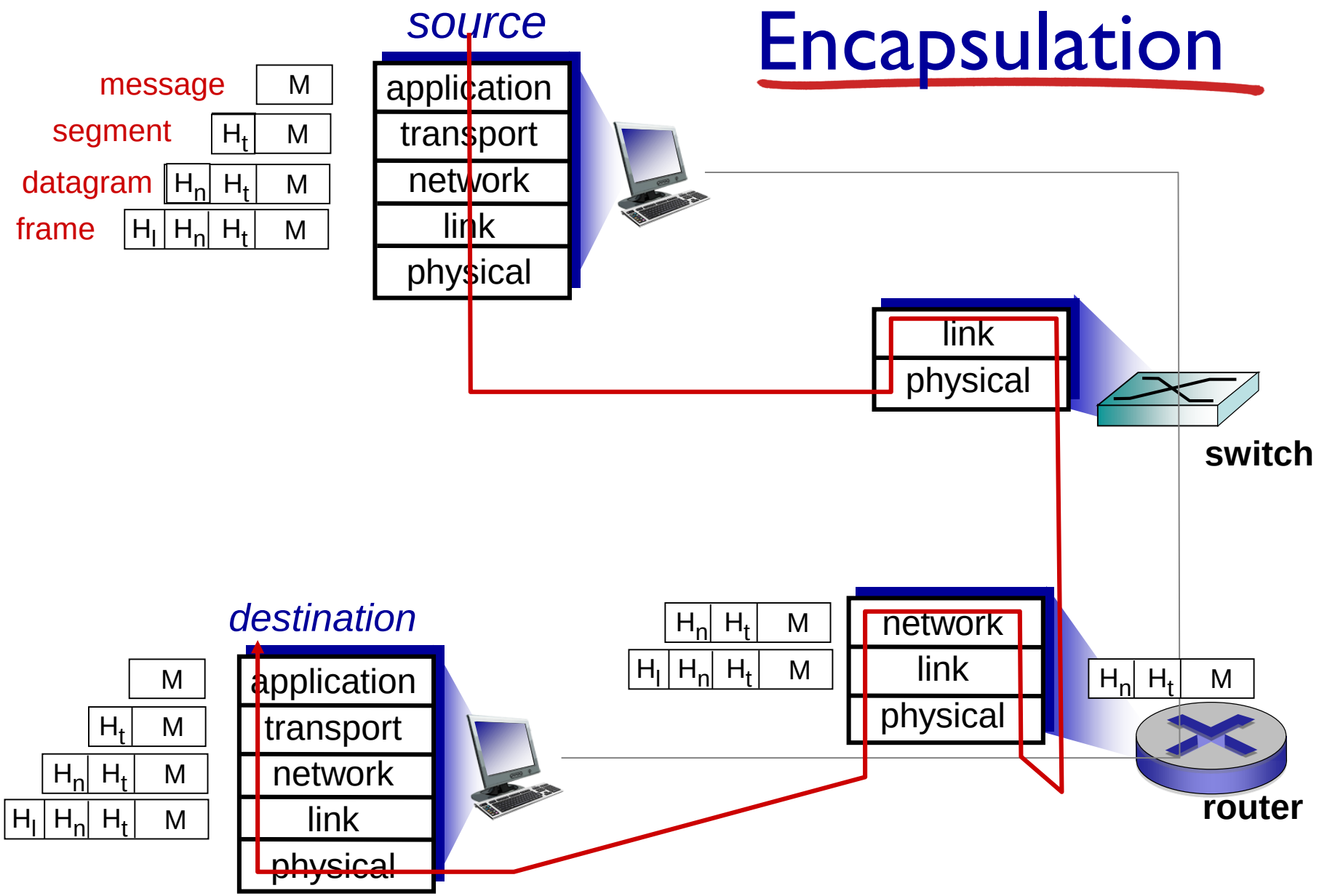


ISO/OSI reference model

- *presentation:* allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- *session:* synchronization, checkpointing, recovery of data exchange
- Internet stack "missing" these layers!
  - these services, *if needed,* must be implemented in application
  - needed?



Encapsulation



Chapter 1: roadmap

1.1 what *is* the Internet?

1.2 network edge

- end systems, access networks, links

1.3 network core

- packet switching, circuit switching, network structure

1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

1.6 networks under attack: security

1.7 history

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!

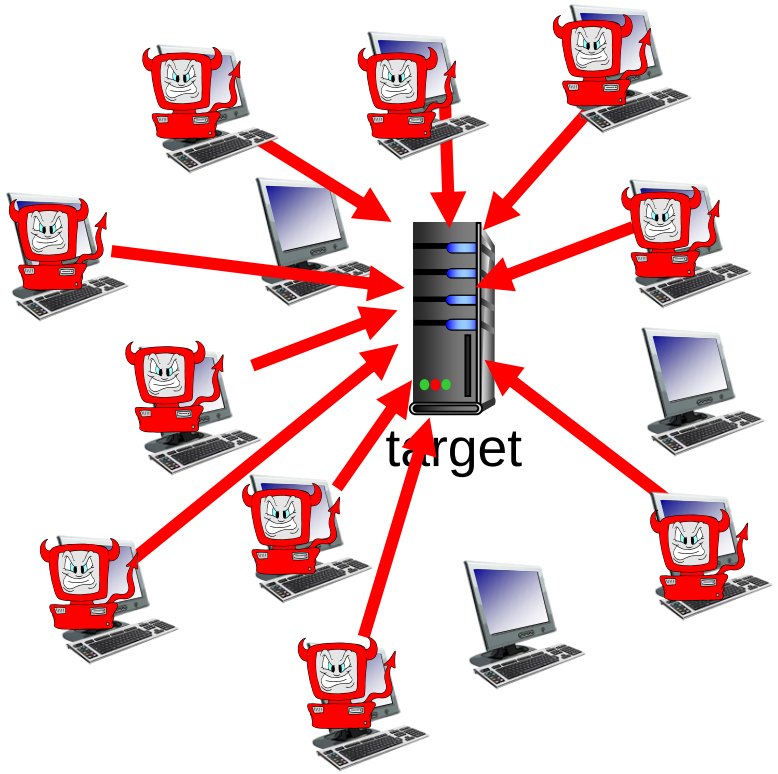
Bad guys: put malware into hosts via Internet

- 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

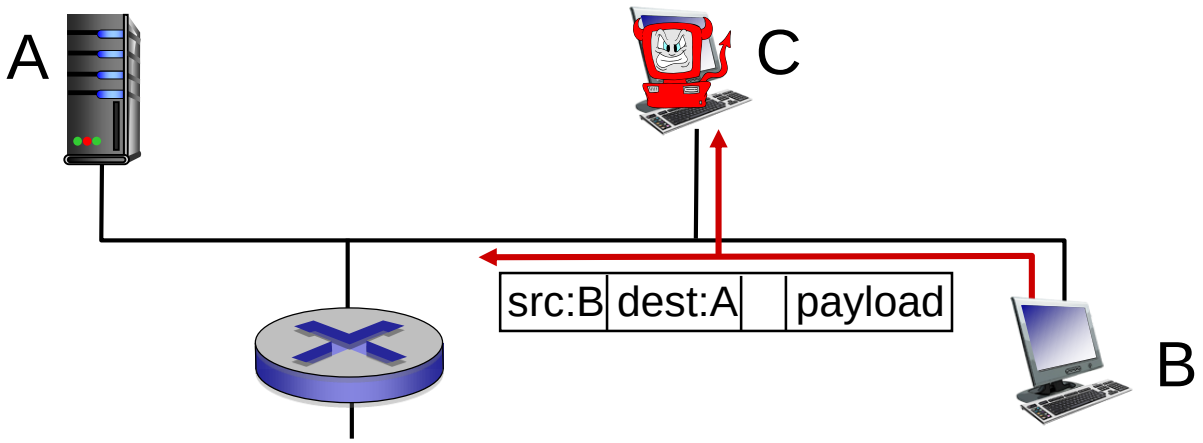
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Bad guys can sniff packets

packet "sniffing":

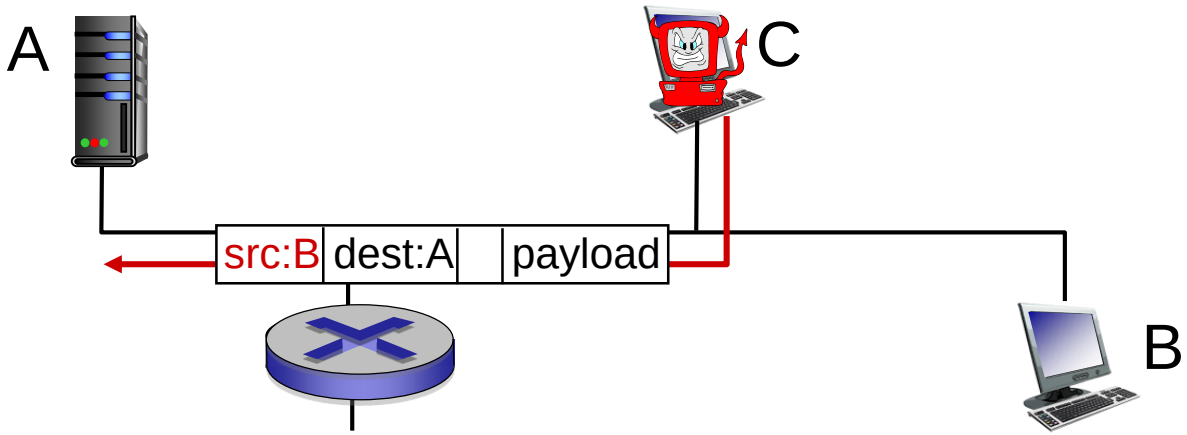
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- 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)

Chapter 1: roadmap

1.1 what *is* the Internet?

1.2 network edge

- end systems, access networks, links

1.3 network core

- packet switching, circuit switching, network structure

1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

1.6 networks under attack: security

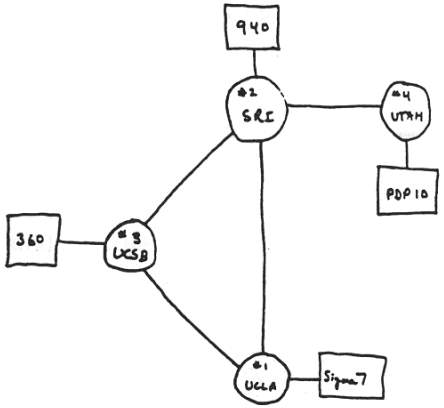
1.7 history

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)
- 1979: ARPAnet has 200 nodes

Cerf and Kahn's internetworking principles:

- minimalism, autonomy - no internal changes required to interconnect networks
- best effort service model
- stateless 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!*

A Gift of Fire

Third edition

Sara Baase

Chapter 3: Freedom of Speech

What We Will Cover

- Changing Communication Paradigms
- Controlling Offensive Speech
- Censorship on the Global Net
- Political Campaign Regulations in Cyberspace
- Anonymity
- Protecting Access and Innovation: Net Neutrality or De-regulation?

Changing Communication Paradigms

Regulating Communications Media:

- First Amendment protection and government regulation
  - Print media (newspapers, magazines, books)
  - Broadcast (television, radio)
  - Common carries (telephones, postal system)

Changing Communication Paradigms (cont.)

Free-speech Principles:

- Written for offensive and/or controversial speech and ideas
- Restriction on the power of government, not individuals or private businesses

Changing Communication Paradigms (cont.)

Free-speech Principles (cont.):

- Supreme Court principles and guidelines
  - Advocating illegal acts is legal
  - Does not protect libel and direct, specific threats
  - Inciting violence is illegal
  - Allows some restrictions on advertising
  - Protect anonymous speech

Controlling Offensive Speech

What is it? What is illegal?

- Answer depends on who you are
- Many efforts to censor the Internet with a focus on child pornography or sexually explicit material

Controlling Offensive Speech (cont.)

Internet Censorship Laws & Alternatives:

- Communication Decency Act (CDA)
  - Federal judge stated that the Internet is the most participatory form of mass communication
  - Attempted to avoid conflict with first amendment by focusing on children
  - The Internet deserves the highest protection from government intrusion

Controlling Offensive Speech (cont.)

Internet Censorship Laws & Alternatives (cont.):

- Filters
  - Blocks sites with specific words, phrases or images
  - Parental control for sex and violence
  - Updated frequently but may still screen out too much or too little
  - Not possible to eliminate all errors
  - What should be blocked?

Controlling Offensive Speech (cont.)

Spam:

- What's the problem?
  - Loosely described as unsolicited bulk email
  - Mostly commercial advertisement
  - Angers people because content and the way it's sent
- Free speech issues
  - Spam imposes a cost on others not protected by free speech
  - Spam filters do not violate free speech (free speech does not require anyone to listen)

Controlling Offensive Speech (cont.)

Spam (cont.):

- Anti-spam Laws
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
  - Targets commercial spam
  - Criticized for not banning all spam, legitimized commercial spam

Controlling Offensive Speech Discussion Questions

- Why is 'least restrictive means' important?
- Do you consider the Internet an appropriate tool for young children? Why or why not?

Censorship on the Global Net

Global Impact of Censorship

- Global nature of the Internet protects against censorship (banned in one country, move to another)
- May impose more restrictive censorship (block everything in an attempt to block one thing)
- Yahoo and French censorship
  - Yahoo, eBay and others make decisions to comply with foreign laws for business reasons

Censorship on the Global Net (cont.)

Censorship in Other Nations:

- Attempts to limit the flow of information on the Internet similar to earlier attempts to place limits on other communications media
- Some countries own the Internet backbone within their countries, block at the border specific sites and content
- Some countries ban all or certain types of access to the Internet

Censorship on the Global Net (cont.)

Aiding Foreign Censors:

- Companies who do business in countries that control Internet access must comply with the local laws
- Google argued that some access is better than no access

Censorship on the Global Net Discussion Questions

- What impact does the global net have on free speech?
- Does censorship in other countries have an impact on free speech in the U.S.?
- How does free speech in 'free countries' impact more restrictive countries?

Anonymity

Common Sense and the Internet:

- Anonymity protected by the First Amendment
- Services available to send anonymous email (Anonymizer.com)
- Anonymizing services used by individuals, businesses, law enforcement agencies, and government intelligence services

Anonymity (cont.)

Is Anonymity Protected?

- FEC (Federal Election Commutiy) exempted individuals and organizations that are not compensated from election laws that restrict anonymity
- Supreme Court has overturned state laws that restrict anonymity
- SLAPP, a Strategic Lawsuit Against Public Participation - lawsuits filed (generally libel) used to obtain the identities (via subpoena) of those expressing critical or dissenting opinions

Anonymity (cont.)

Against Anonymity:

- Fears
  - It hides crime or protects criminals
  - Glowing reviews (such as those posted on eBay or Amazon.com) may actually be from the author, publisher, seller, or their friends
- U.S. and European countries working on laws that require ISPs to maintain records of the true identity of each user and maintain records of online activity for potential use in criminal investigations

Anonymity Discussion Questions

- Where (if anywhere) is anonymity appropriate on the Internet?
- What are some kinds of Web sites that should prohibit anonymity?
- Where (if anywhere) should laws prohibit anonymity on the Internet?

Protecting Access and Innovation

Net Neutrality or De-regulation?

- FCC eliminated line-sharing requirements (2003-2005)
- Should companies be permitted to exclude or give special treatment to content transmitted based on the content itself or on the company that provides it?
- Should companies be permitted to provide different levels of speed at different prices?

Protecting Access and Innovation (cont.)

Net Neutrality or De-regulation? (cont.)

- Net Neutrality
  - Argue for equal treatment of all customers
- De-regulation
  - Flexibility and market incentives will benefit customers

Discussion Questions

- What are the pros and cons to anonymity on the Internet?
- The First-Amendment was created to protect political and offensive speech. Anonymity is key to that protection. Should the free speech principles of the First Amendment apply to the Internet, even to speech outside the U.S.?

Ongoing Research

Selected Recent Publications:

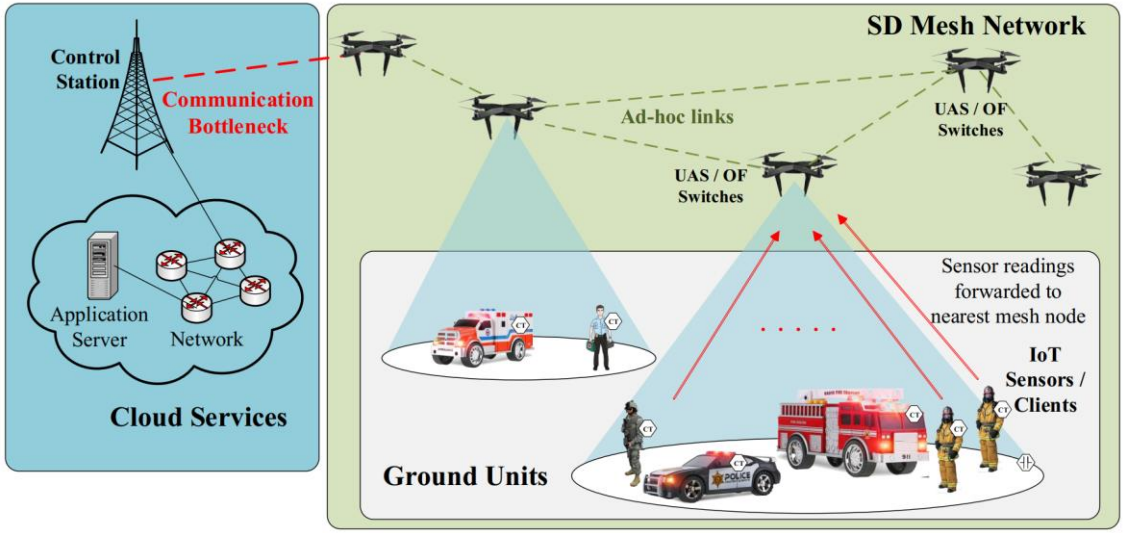
- Fog Computing on Software Defined Unmanned Aerial Networks (UAN)
- Extending RTS\CTS for UAV Networks
- Resilient Control Link Design for Aerial Networks
- Heterogenous IoT Design for Smart Campus Application
- Blockchain-based Public Emergency Alert System

Ongoing UAV test-bed experiments

Fog Computing on Software-Defined UAN

Motivation and Challenges:

- Performance (throughput) of mesh network declines when number of hops increases between two communicating end points.
- In addition, having remote computation unit (GCS) with limited network capacity creates a bottleneck and leads to congestions in the network.



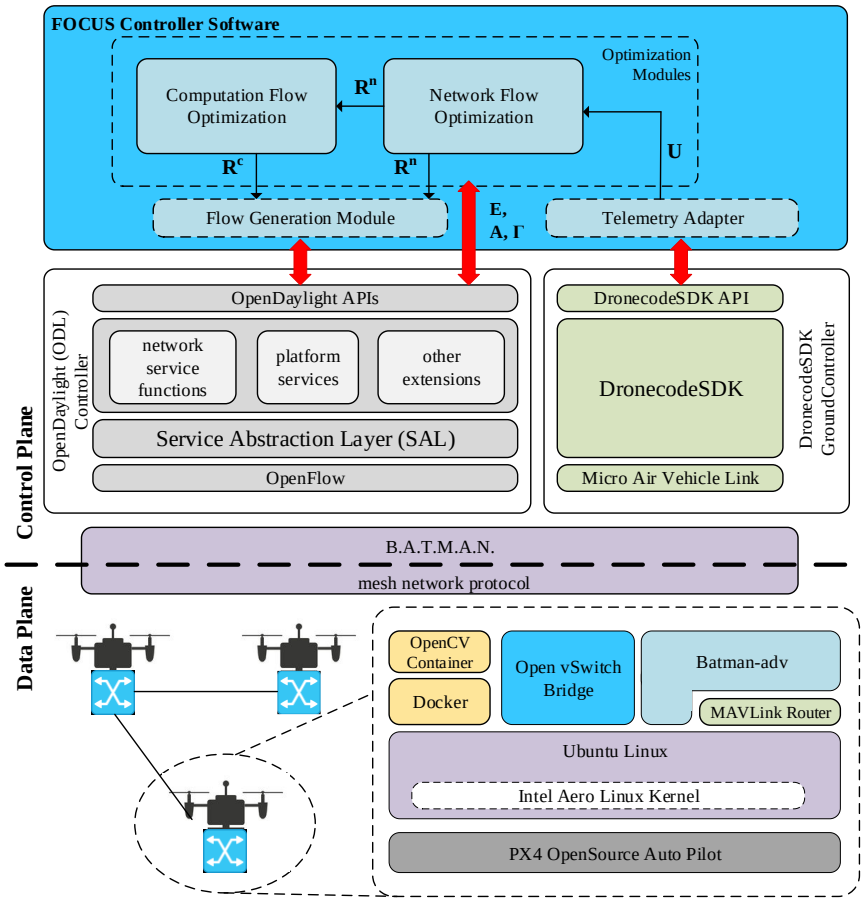
Computation on UAS Mesh Networks

Motivation and Challenges:

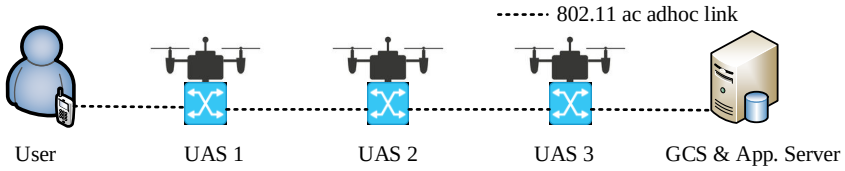
- Performance (throughput) of mesh network declines when number of hops increases between two communicating end points.
- In addition, having remote computation unit (GCS) with limited network capacity creates a bottleneck and leads to congestions in the network.

Proposed Software Stack [FOCUS]:

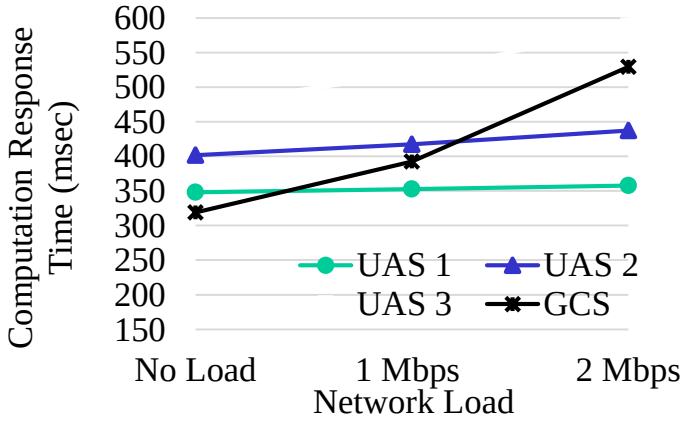
- Control Plane
  - SDN Controller
  - Drone Controller SDK
- Data Plane
  - **Docker** for seamless migration of tasks
  - Network Interfaces (BATMAN, OVS)

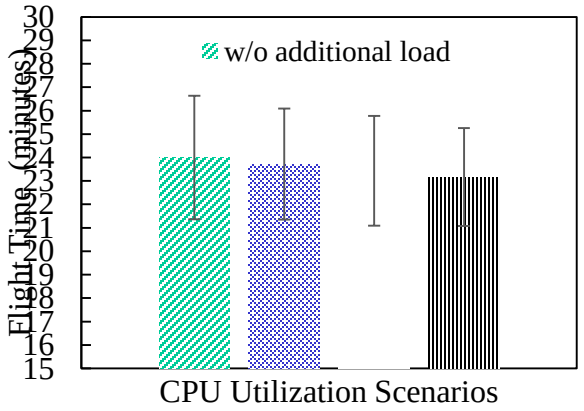


Offloading Computation to Aerial Units



We built simple linear network topology with Intel Aero Drones with additional WiFi Interfaces.



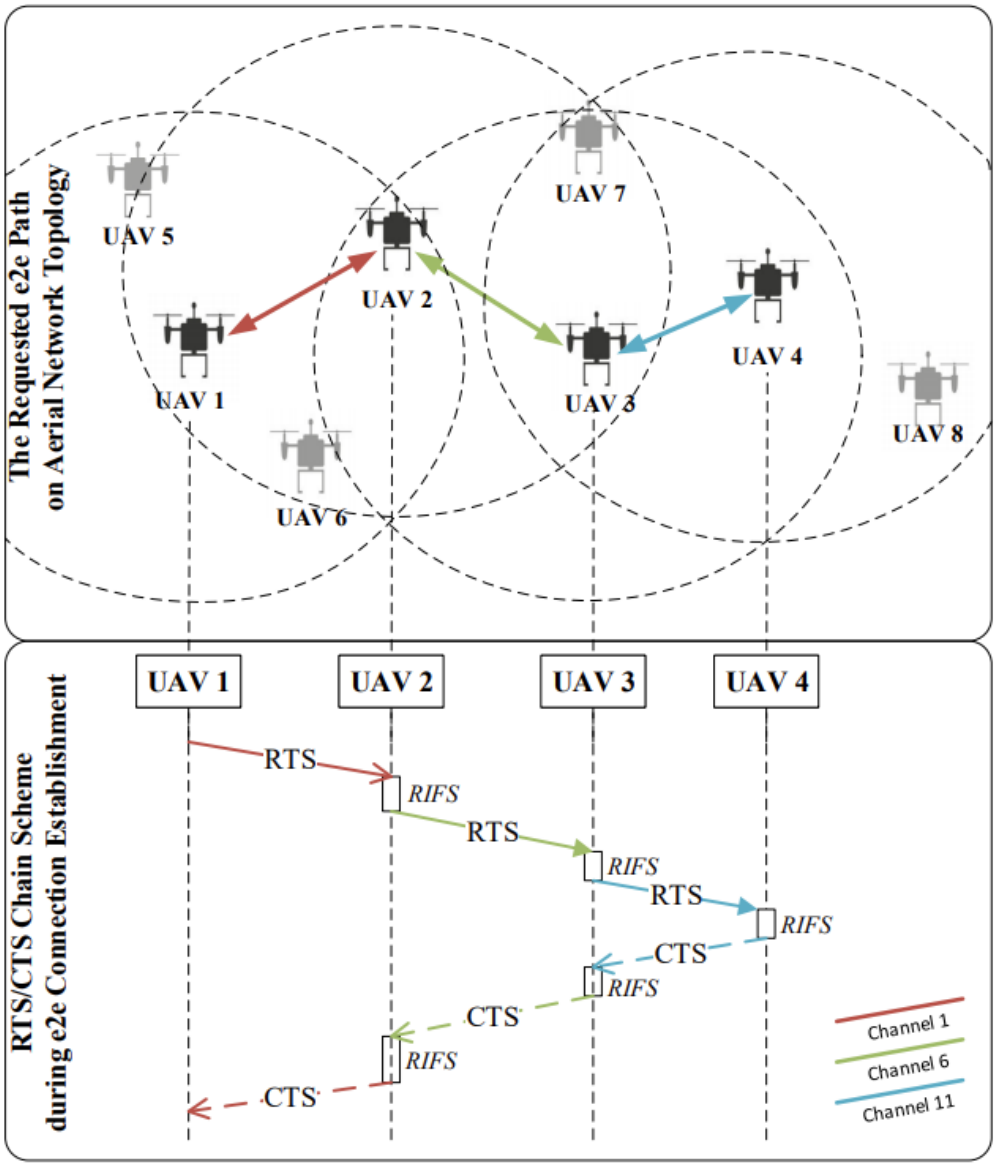


Preliminary experiments show that offloading computation to close aerial nodes provides significant improvement in terms of response time when there is additional network load.

Chain RTS/CTS

Main Contributions:

- Enabling multi-hop collision avoidance scheme with seamless channel hopping
- Dynamically adjusting the timeout counters and inter-frame spacing times
- Smart BW allocation, to ensure fairness and channel effectiveness



"Chain RTS/CTS Scheme for Aerial Multi-hop Communications", T.T. Sarı, G. Secinti, IEEE CCNC 2021.
"Multi-hop Collision Avoidance with Adaptive Bandwidth Allocation for Aerial Networks", under revision, Elsevier Computer Networks.

Chain RTS/CTS

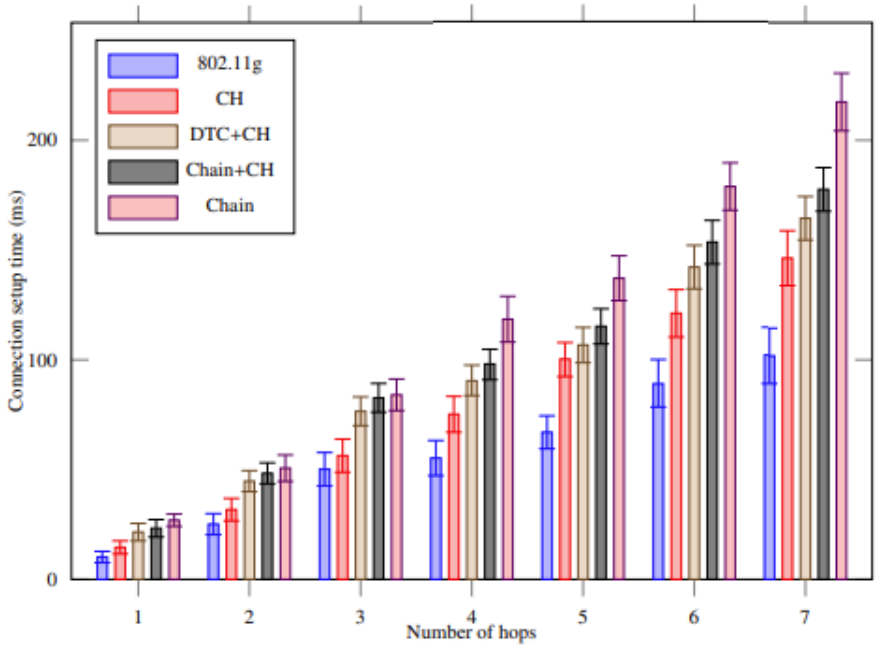
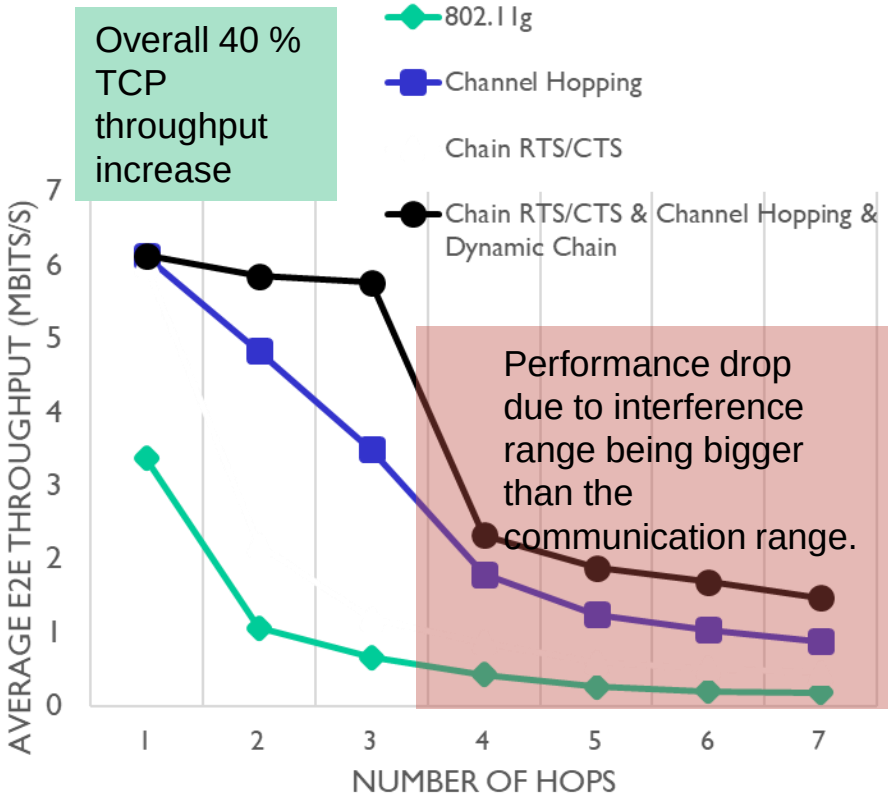
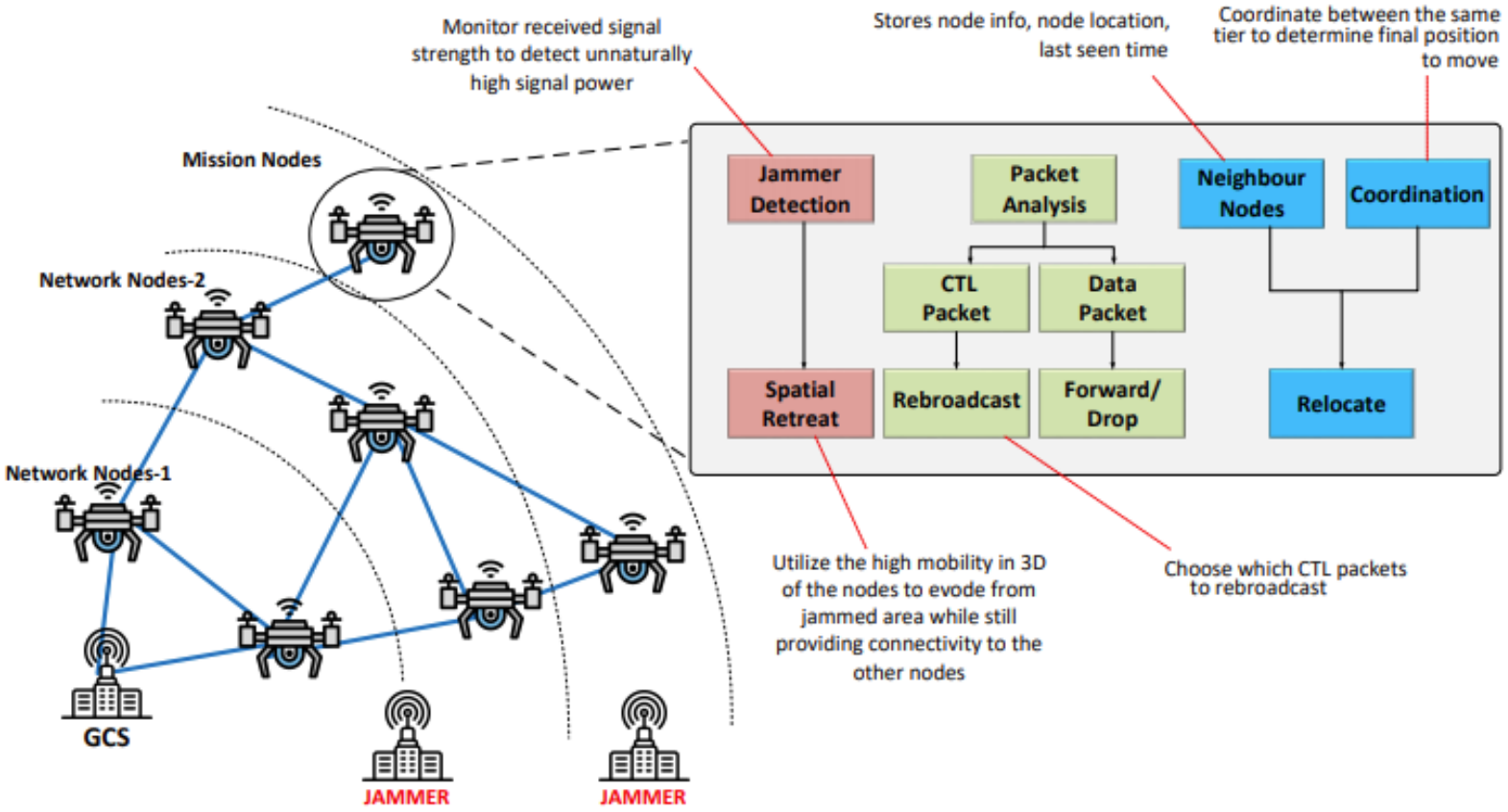


Figure 5: TCP connection establishment time.



"Chain RTS/CTS Scheme for Aerial Multi-hop Communications", T.T. Sarı, G. Secinti, IEEE CCNC 2021.
"Multi-hop Collision Avoidance with Adaptive Bandwidth Allocation for Aerial Networks", under revision, Elsevier Computer Networks.

CLAN: Control Link for Aerial Mesh



"CLAN: A Robust Control Link for Aerial Mesh Networks in Contested Environments", F. R. Kilic, M. O. Ozdogan, G. Secinti, and B.Canberk, EAI INISCOM, 2021. **[Best Paper Award]**

CLAN: Control Link for Aerial Mesh

- Protocol design, jointly optimizing the dissemination of both
  1. Mesh routing packages
  2. UAV control traffic
- Showcasing how signals on long range links are more vulnerable to jamming attacks, resulting disconnections in aerial networks

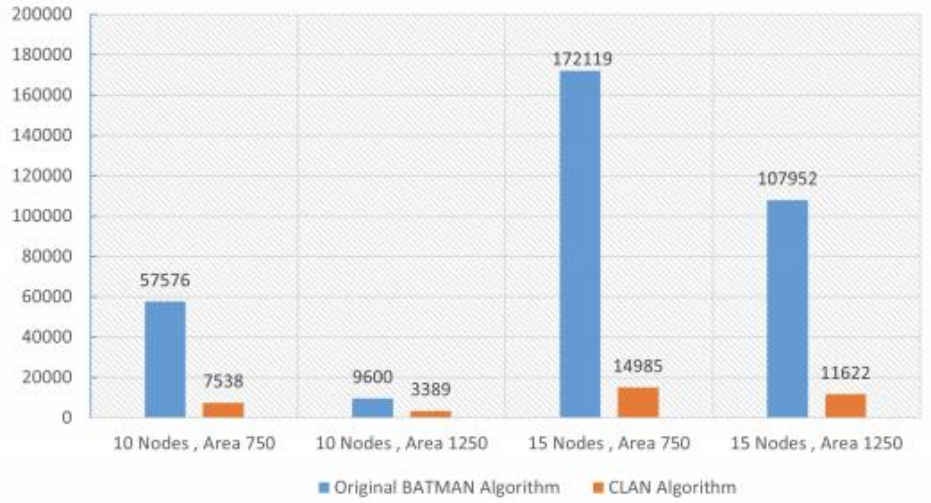


Fig. 4. Number of Traffic Control Messages in Proactive Routing

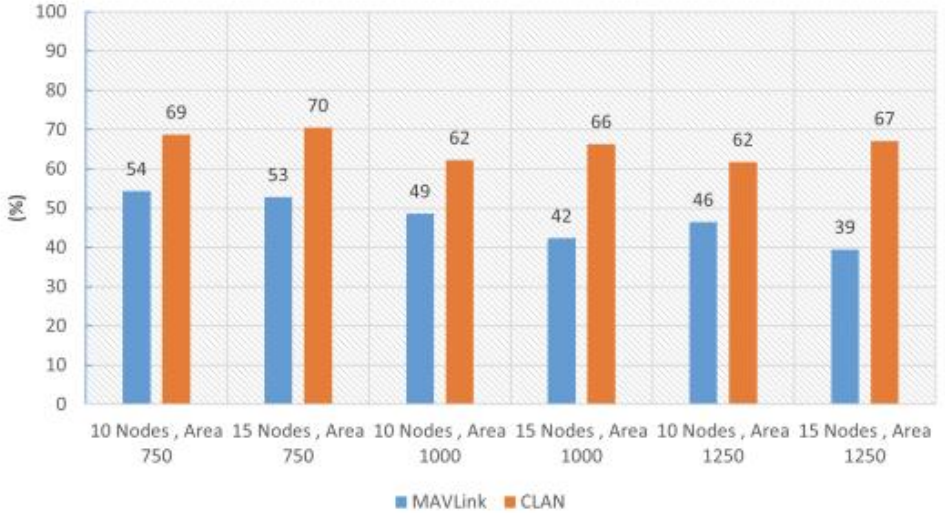


Fig. 7. Average Connectivity (3 Jammers)

"CLAN: A Robust Control Link for Aerial Mesh Networks in Contested Environments", F. R. Kilic, M. O. Ozdogan, G. Secinti, and B.Canberk, EAI INISCOM, 2021. **[Best Paper Award]**

Ongoing Research