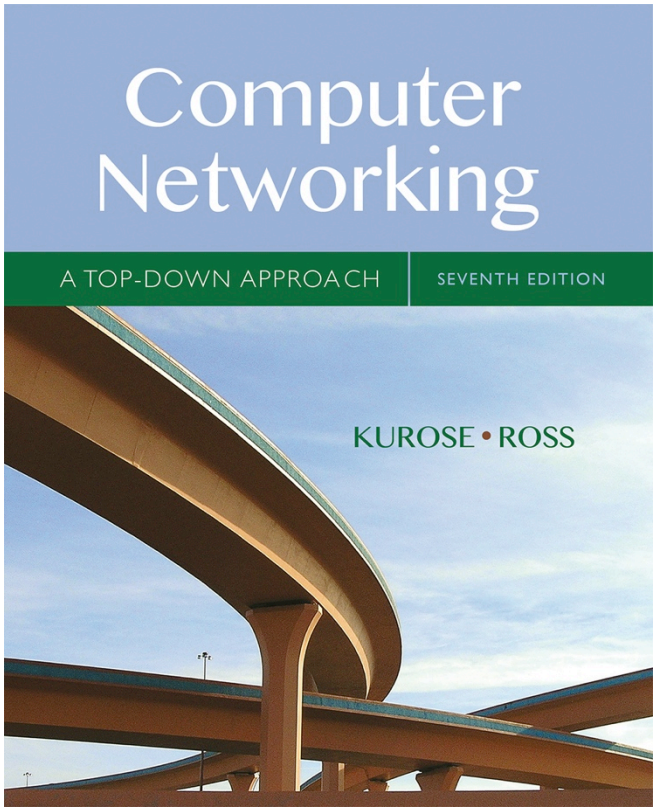
# Chapter 1
# Introduction




*Computer Networking: A Top Down Approach*

7th edition
Jim Kurose, Keith Ross
Pearson/Addison Wesley
April 2016

# Chapter 1: introduction

*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
- performance: loss, delay, throughput
- security
- protocol layers, service models

# 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

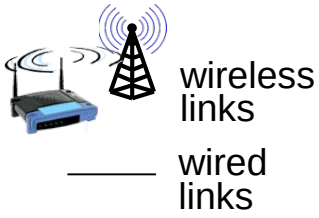
1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

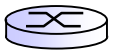
1.6 networks under attack: security

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

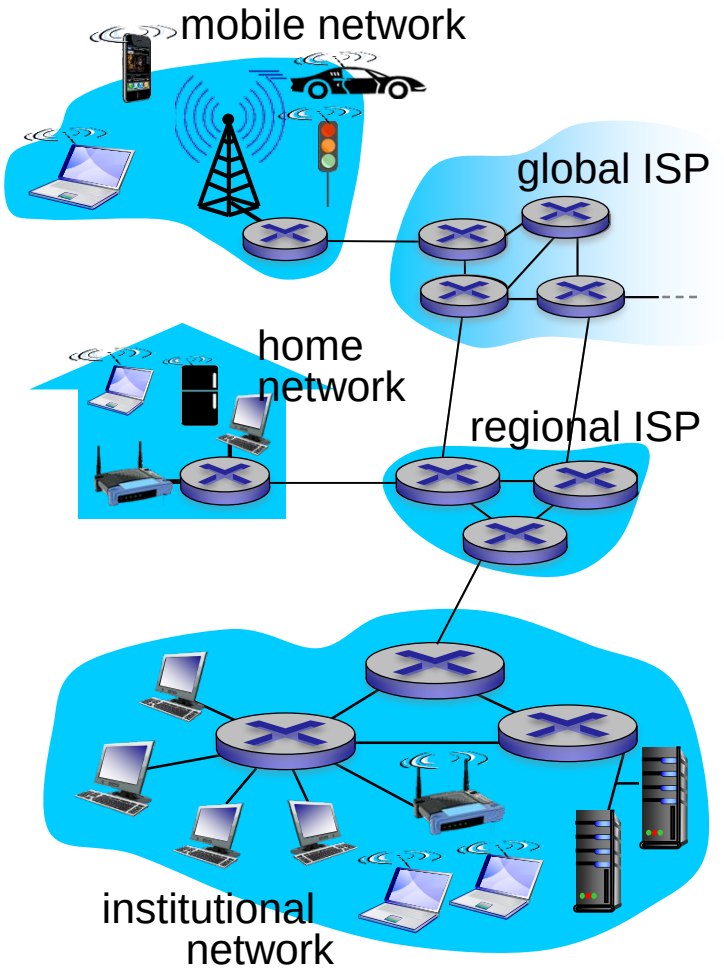

- billions of connected computing devices:
  - *hosts* = *end systems*
  - running *network apps*




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

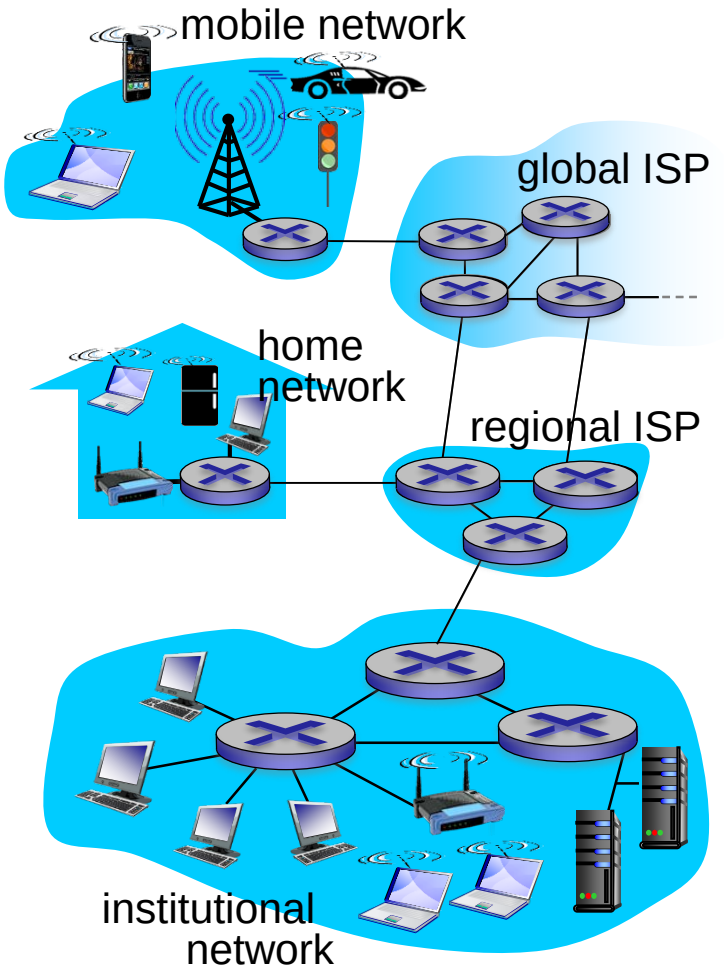



- *packet switches:* forward packets (chunks of data)
  - *routers* and *switches*



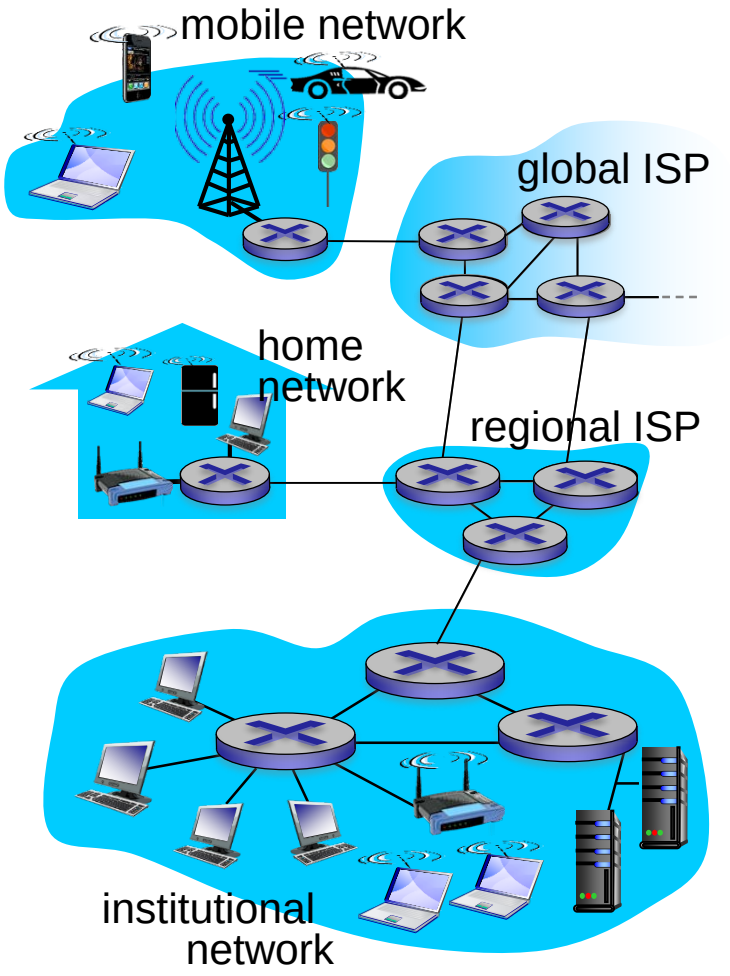
# What's the Internet: "nuts and bolts" view

- *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



# 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

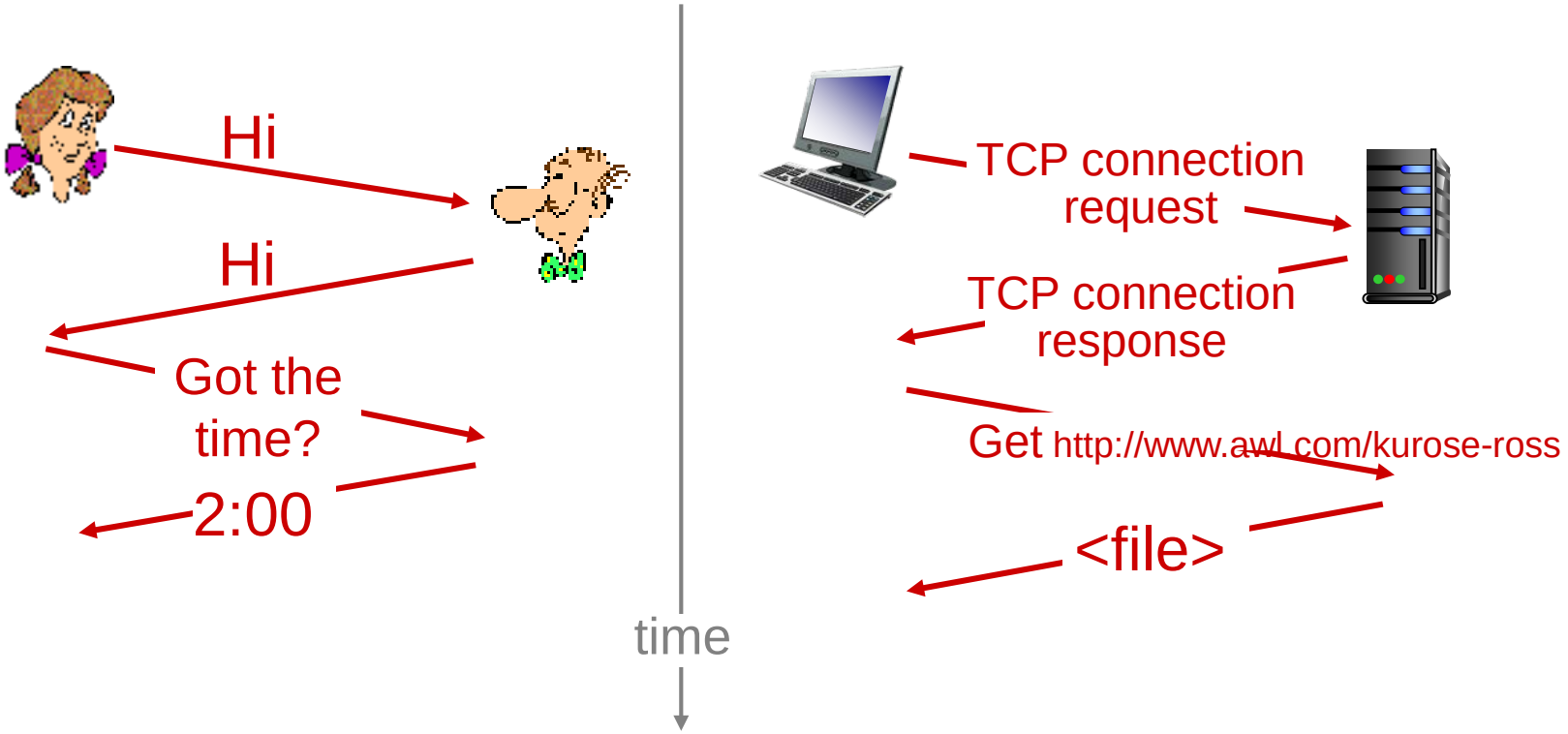
*network protocols:*

- 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:



# 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

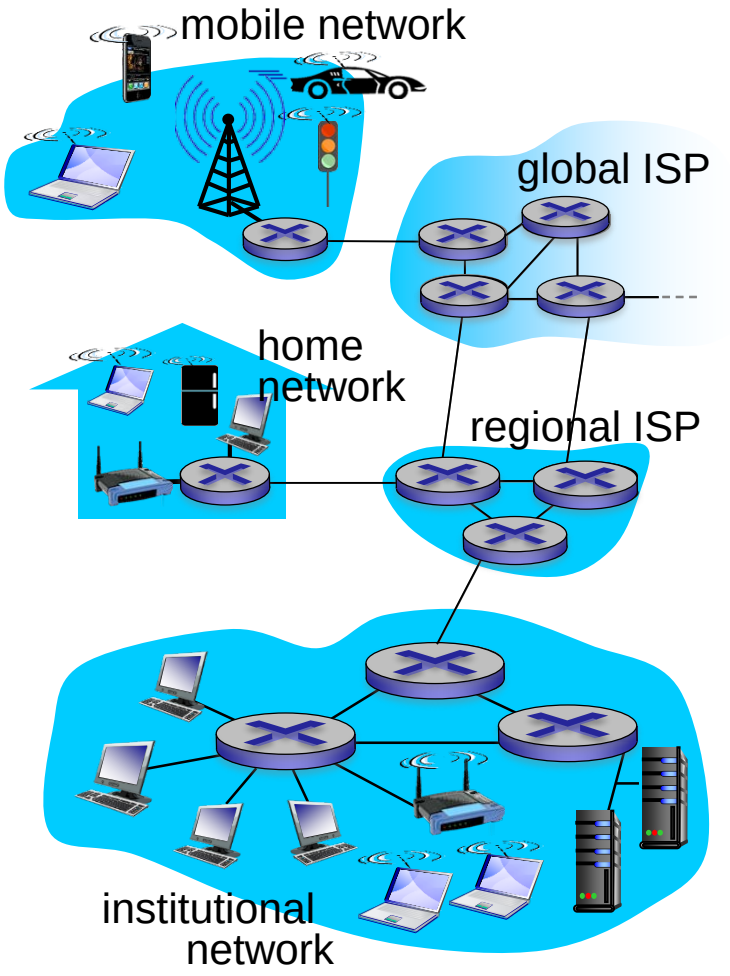
1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

1.6 networks under attack: security

# 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



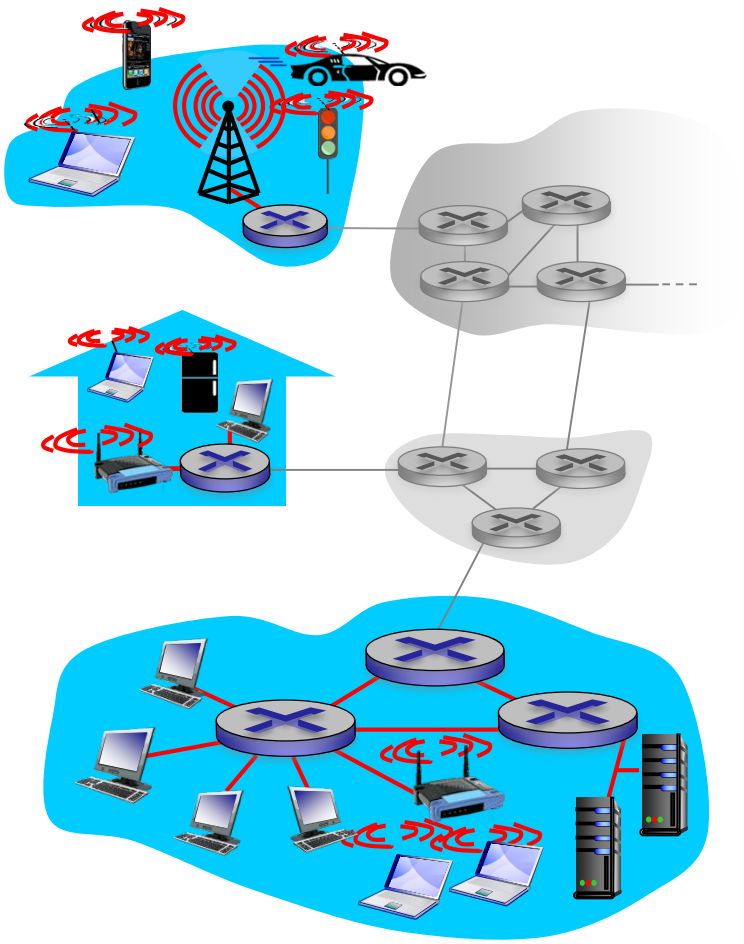
# Access networks and physical media

*Q: How to connect end systems to edge router?*

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

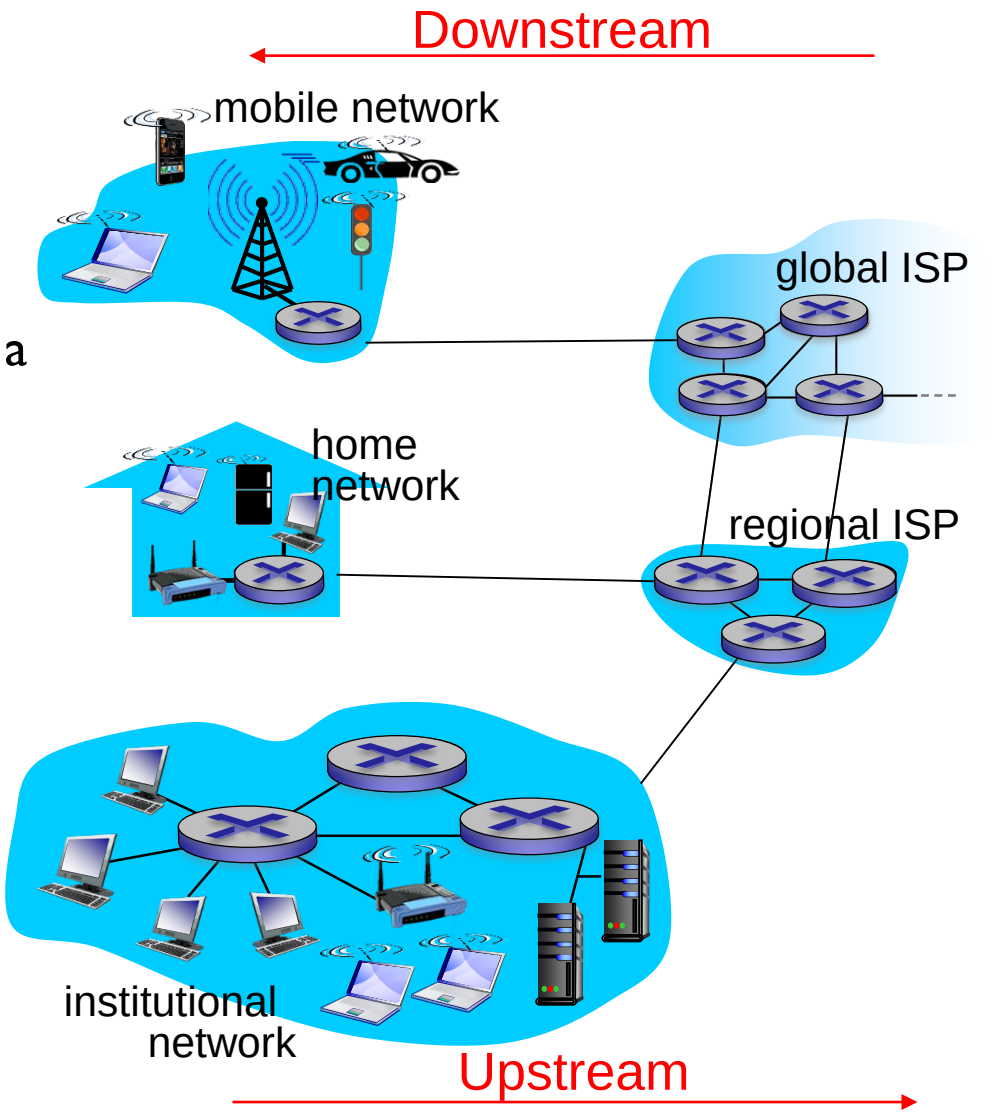
*keep in mind:*

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

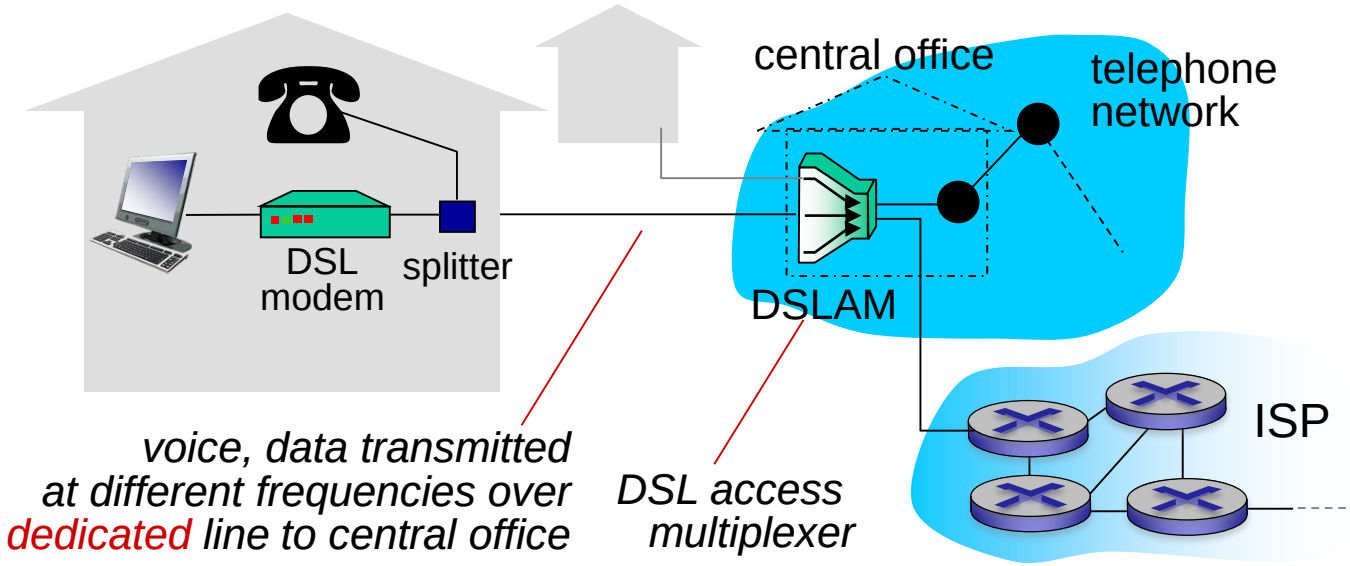


# Definition of Access network:

- *Physically connects end systems to the first edge router.*
  - Used in the network between a provider and a subscriber
- *Informally classified as either narrow or broad band.*
- *Many are asymmetric, with a higher data rate downstream.*
  - Note the end system downstream pays for the service.

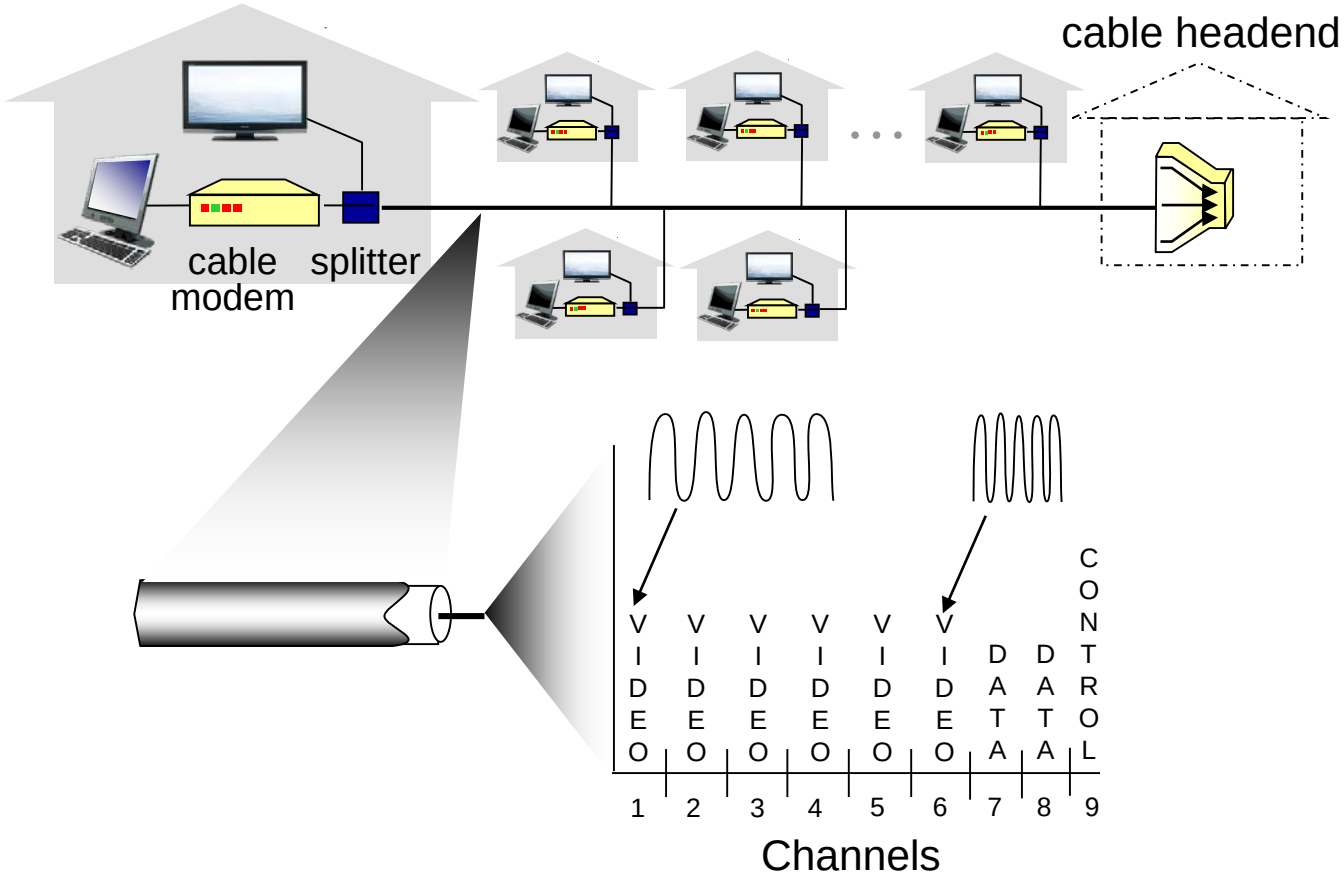


# Access network: digital subscriber line (DSL)



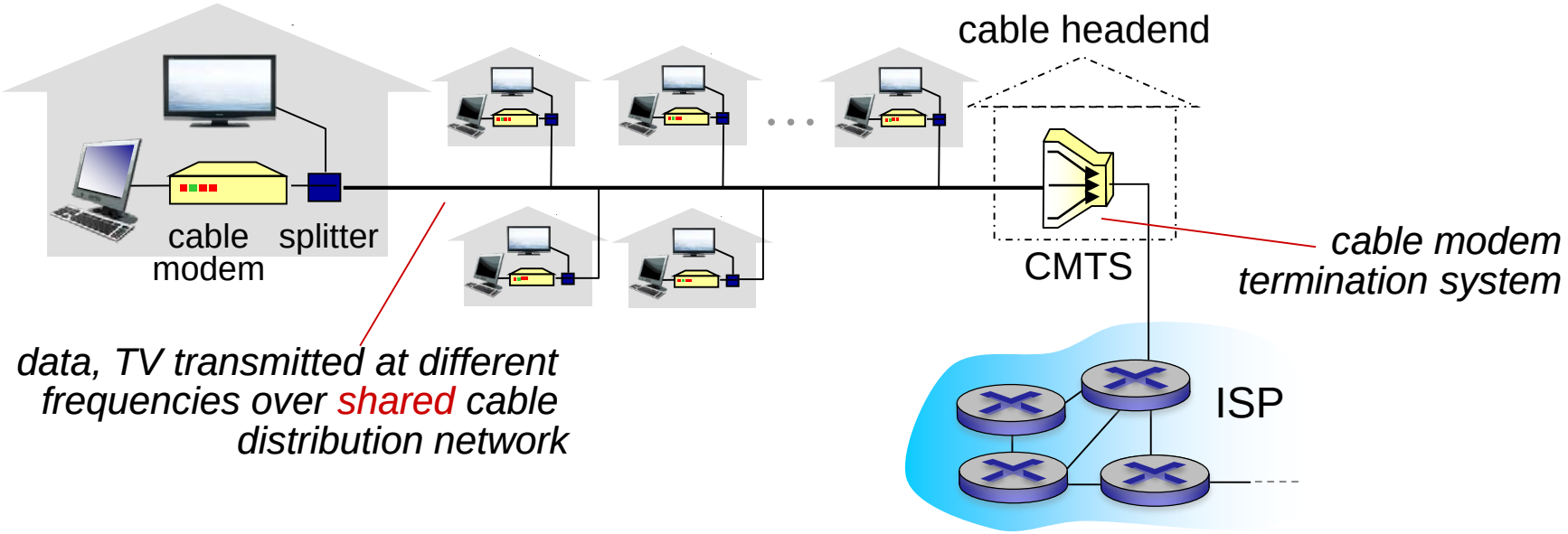

- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbits/s upstream transmission rate (typically < 1 Mbits/s)
- < 24 Mbits/s downstream transmission rate (typically < 10 Mbits/s)

# Access network: cable network



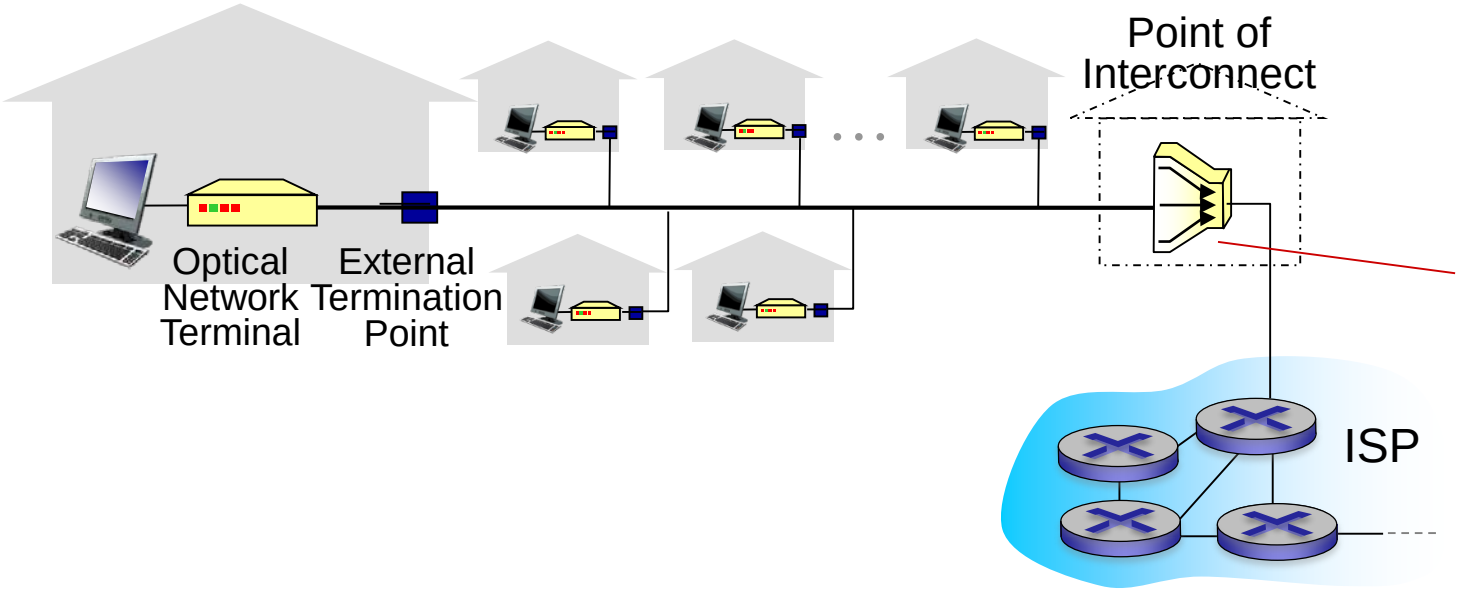

*frequency division multiplexing:* different channels transmitted in different frequency bands

# Access network: cable network



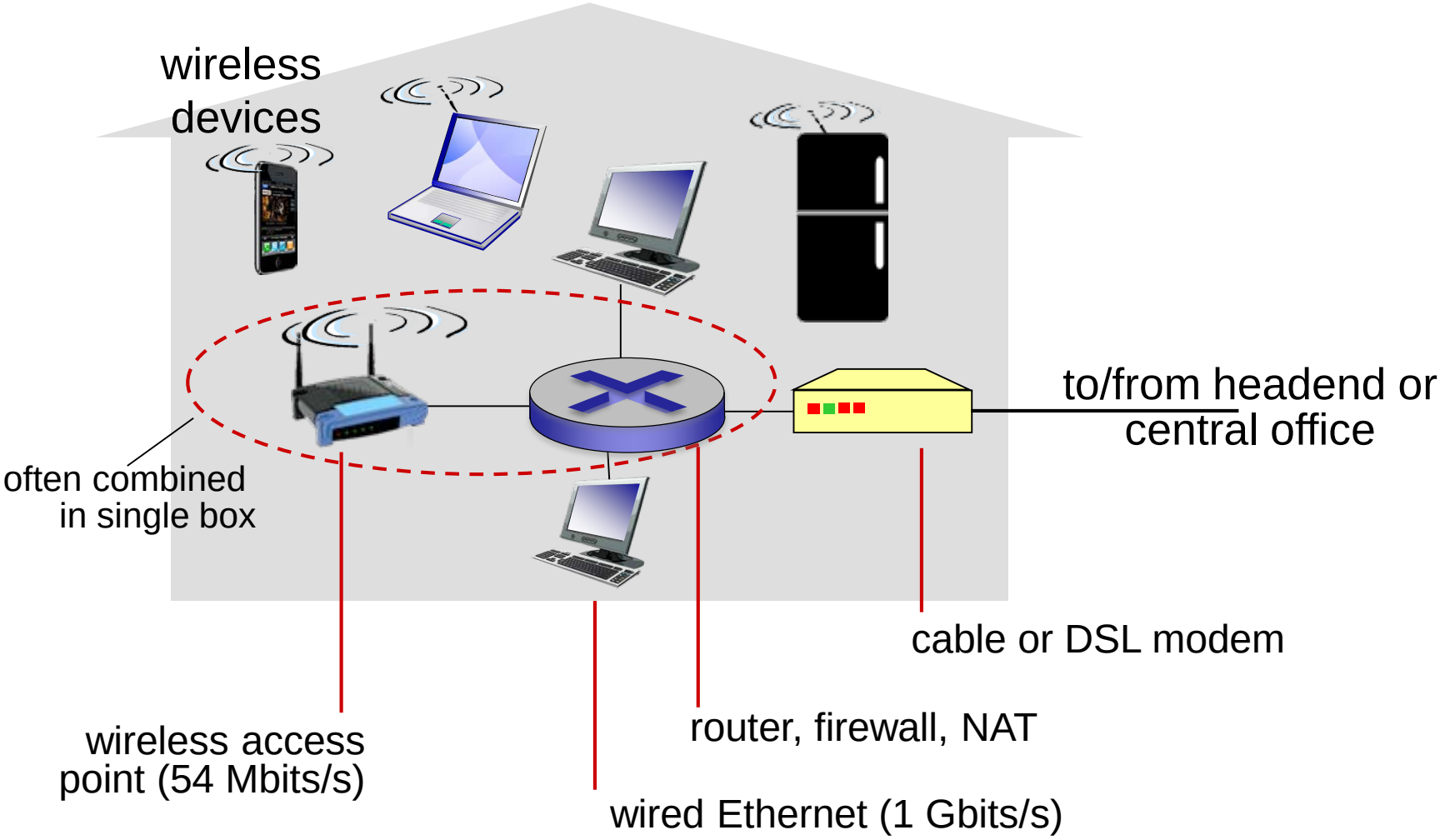

- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbits/s downstream transmission rate, 2 Mbits/s upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

# Access network: fibre network

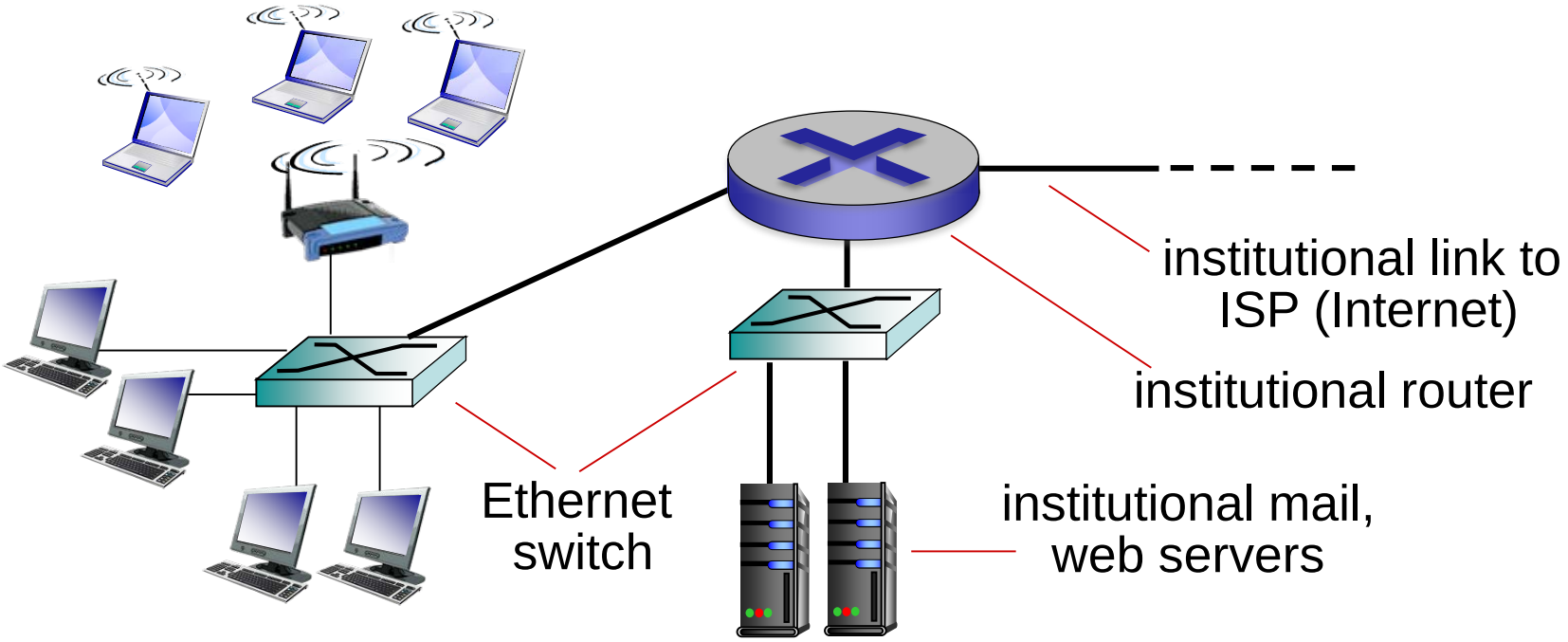



- GPON: gigabit-capable passive optical network
  - asymmetric: >30Mbits/s downstream transmission rate, >10 Mbits/s upstream transmission rate
- network of fiber attaches homes to ISP router
  - like DSL, there is dedicated access to the Point of Interconnect.

# Access network: home network



# Enterprise access networks (Ethernet)




- typically used in companies, universities, etc.
- 10 Mbits/s, 100Mbits/s, 1Gbits/s, 10Gbits/s transmission rates
- today, end systems typically connect into Ethernet switch

# Wireless access networks

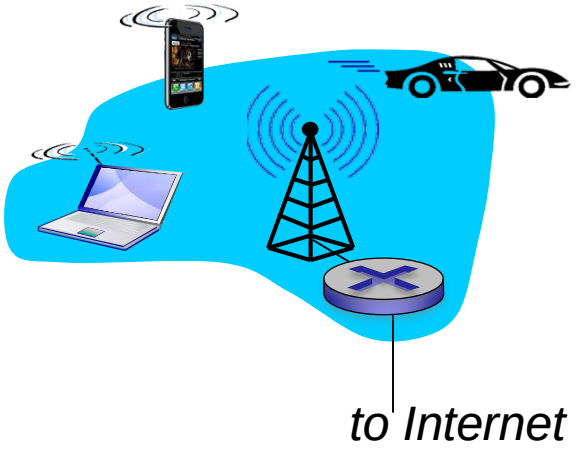
- shared *wireless* access network connects end system to router
  - via base station aka "access point"

*wireless LANs:*

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


wide-area wireless access

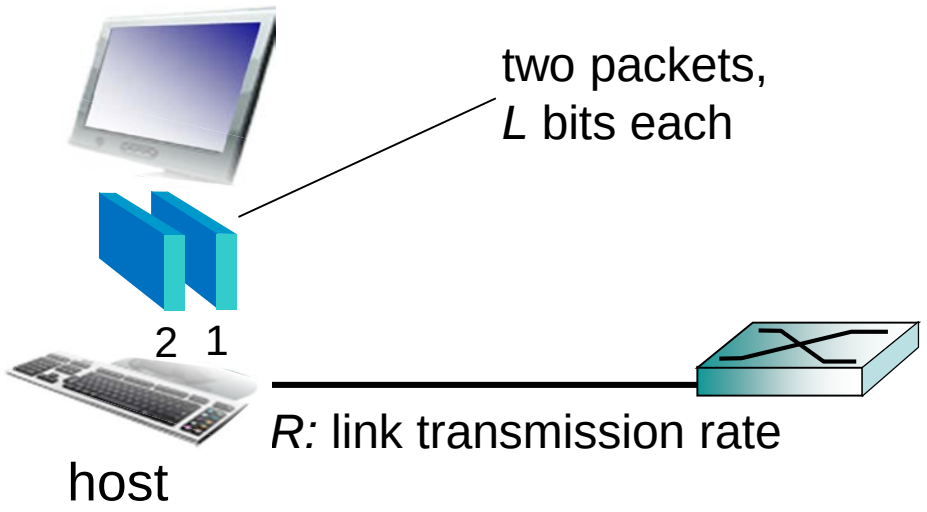
- provided by telco (cellular) operator, 10's km
- between 1 and 10 Mbits/s
- 3G, 4G: LTE



# Host: sends *packets* of data

host sending function:

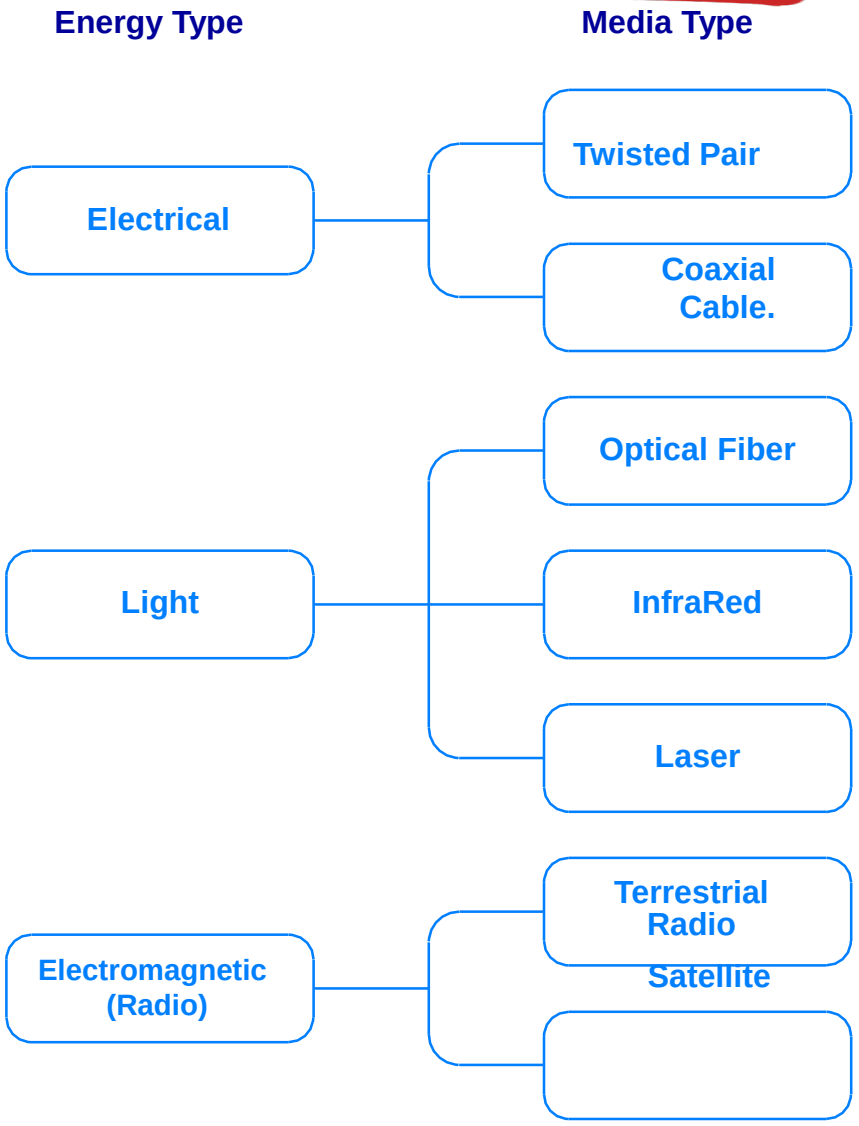
- takes application message
- breaks into smaller chunks, known as *packets*, of length *L* bits
- transmits packet into access network at *transmission rate R*
  - link transmission rate, aka link *capacity, aka link bandwidth*




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

# Physical media classified by energy type

- bits: propagates between transmitter/receiver pairs
- physical link: what lies between transmitter & receiver
- Physical media is classified according to the form of energy used to transmit data.
- guided media:
  - signals propagate in solid media: copper, fiber, coax
- unguided media:
  - signals propagate freely, e.g., radio



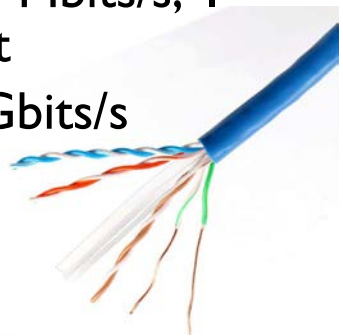
# Problems with transmission

- Loss, interference and noise
- Problems in the electrical and electromagnetic worlds
  - Resistance (leads to loss)
  - Capacitance (leads to distortion)
  - Inductance (leads to interference
- Random electromagnetic radiation is called noise
  - Can be generated by specific sources such as electric motor
  - Background radiation is an inescapable feature of the universe

# Physical media: twisted pair, coax, fiber

## *twisted pair (TP)*

- two insulated copper wires
  - Category 5: 100 Mbits/s, 1 Gbits/s Ethernet
  - Category 6: 10Gbits/s



## *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 Gbits/s 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 Mbits/s channels
- LAN (e.g., WiFi)
  - 54 Mbits/s
- wide-area (e.g., cellular)
  - 4G cellular: ~ 10 Mbits/s
- satellite
  - Kbits/s to 45Mbits/s 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

- circuit switching, packet switching, network structure

1.4 delay, loss, throughput in networks

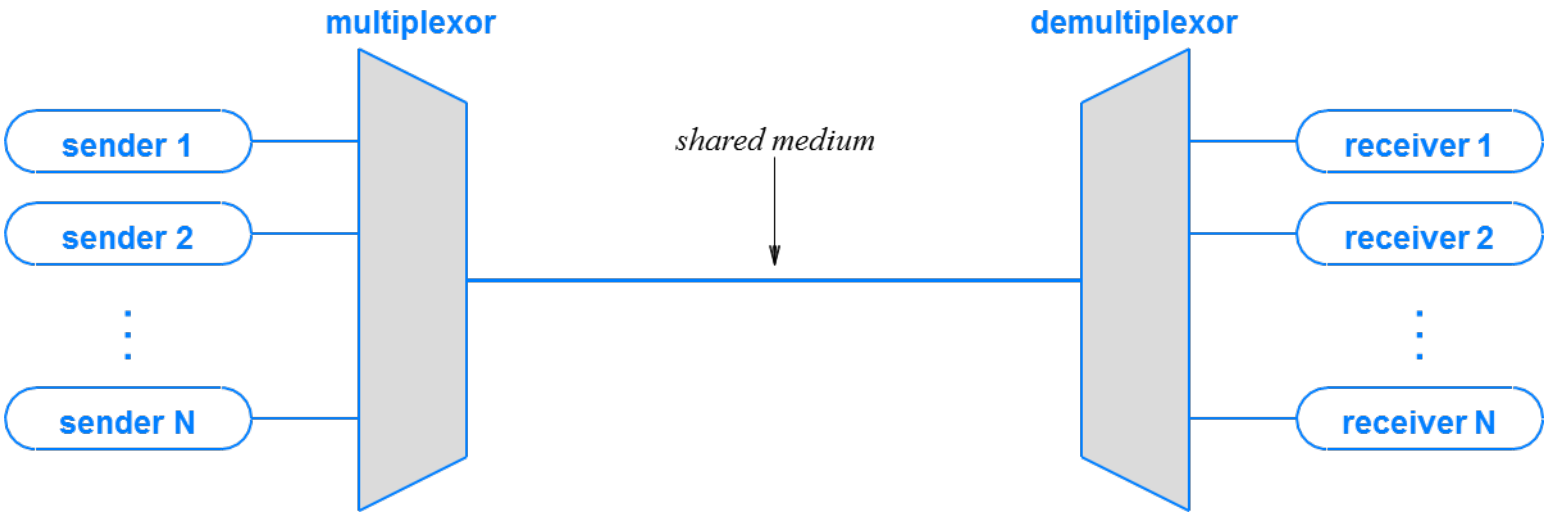
1.5 protocol layers, service models

1.6 networks under attack: security

# What is a Network

- Distinct from physical communication systems
- Attach multiple endpoints
- Two broad categories
  - Circuit switched
  - Packet switched

# Concept of Multiplexing



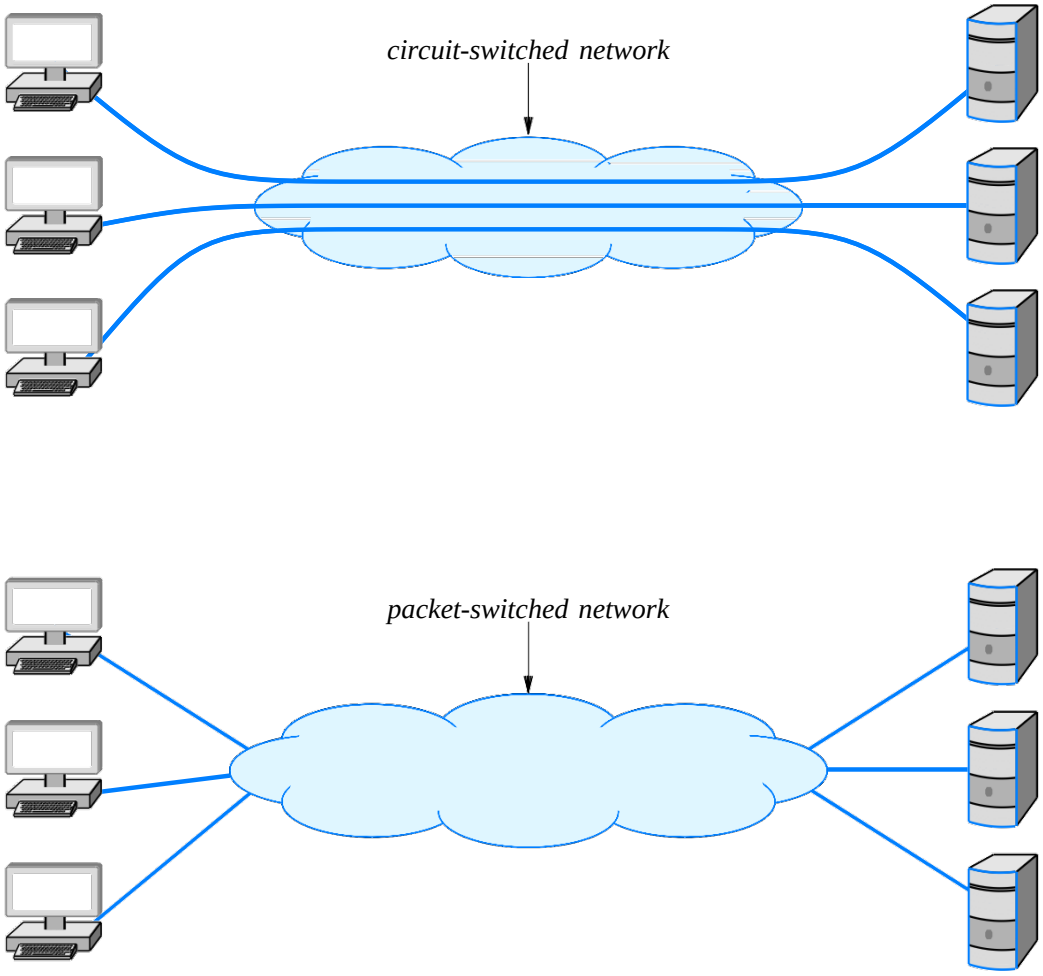
# Circuit Switching

- Provide point-to-point communication between pairs of endpoints
- Establish path between sender and receiver
- Separate steps for circuit creation, use, and termination
- Performance equivalent to an isolated physical path
- Circuit can be
  - Permanent/ provisioned (left in place for long periods)
  - Switched (created on demand)
- Concept: user leases piece of underlying infrastructure for a time period

# Packet Switching

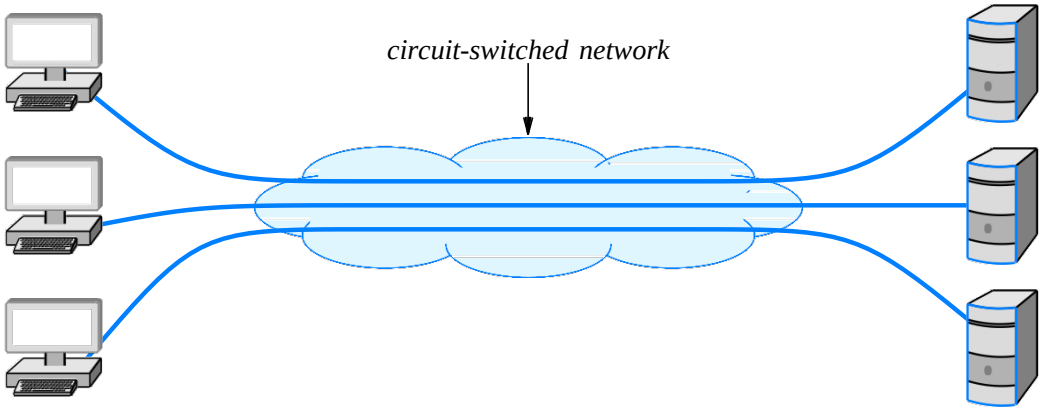
- Form the basis for the Internet
- Multiplex communication over shared media
- All data divided into packets (maximum size fixed)
- After sending one packet, sender allows others a chance to transmit before sending a second packet
- Arbitrary, asynchronous communication
- No set-up required before communication begins
- Performance varies due to statistical multiplexing
- Concept: underlying infrastructure is shared among users

# Circuit and Packet Switching

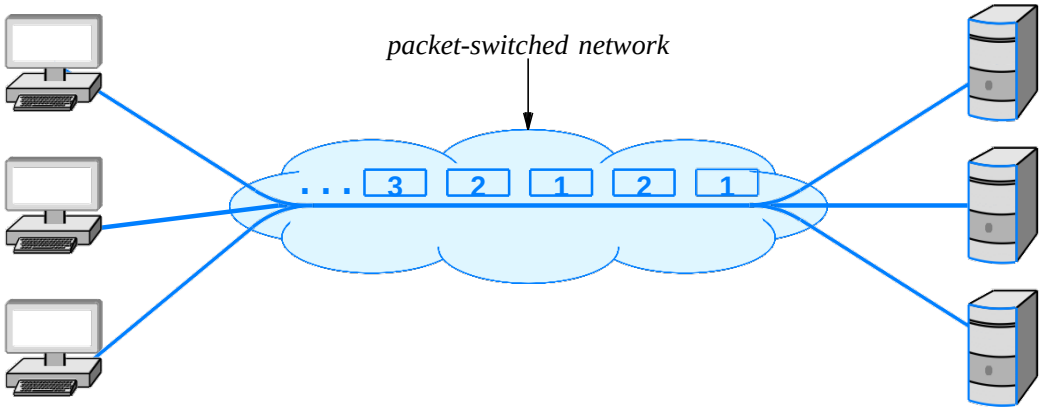


# Circuit and Packet Switching

Circuit switching provides 1-to-1 dedicated connections

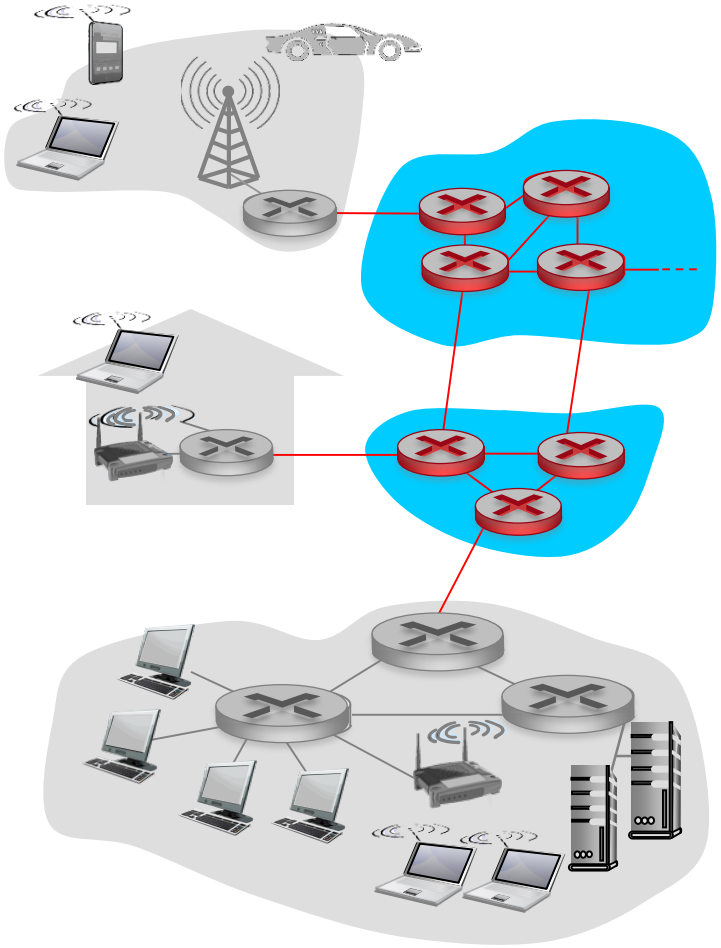



Packet switching provides statistical sharing of the connection

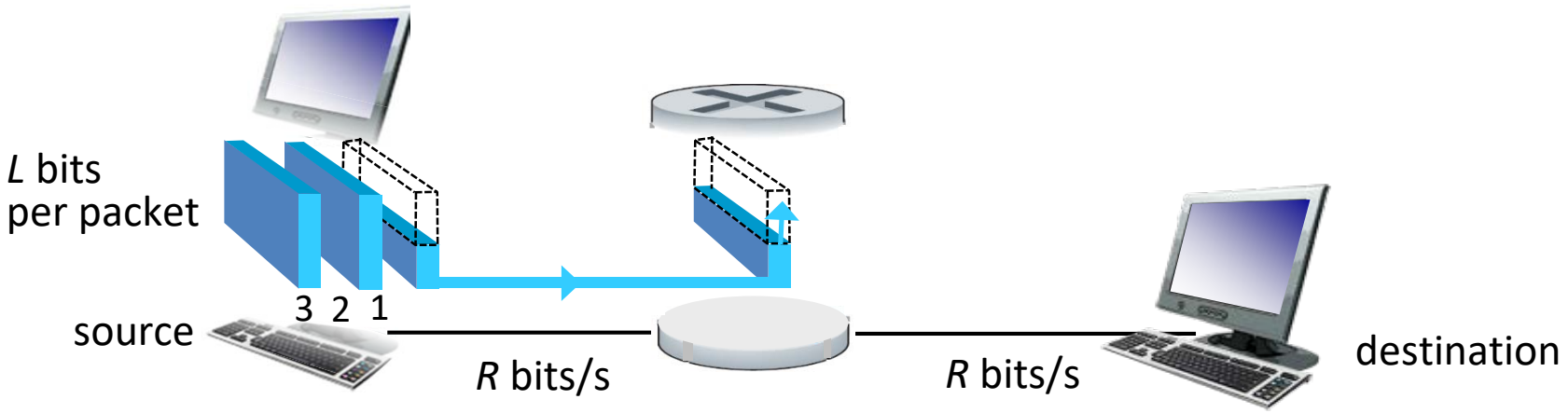


# The network core

- 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



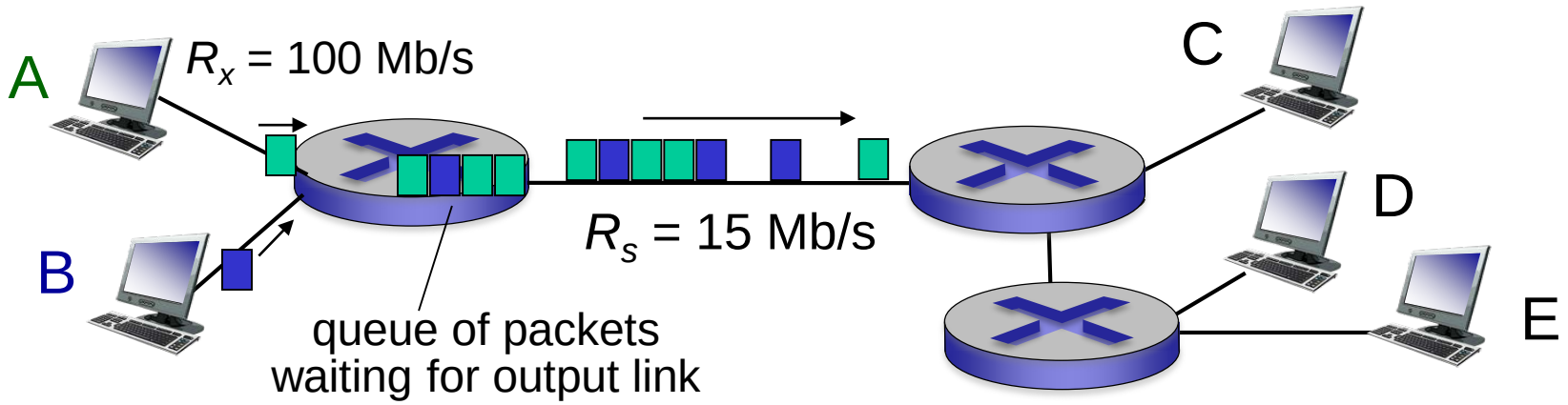

- takes *L*/*R* seconds to transmit (push out) *L*-bit packet into link at *R* bits/s
- *store and forward:* entire packet must arrive at router before it can be transmitted on next link
- end-end delay = 2*L*/*R* (assuming zero propagation delay)

*one-hop numerical example:*

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

more on delay shortly …

# Packet Switching: queueing delay, loss




queuing and loss:

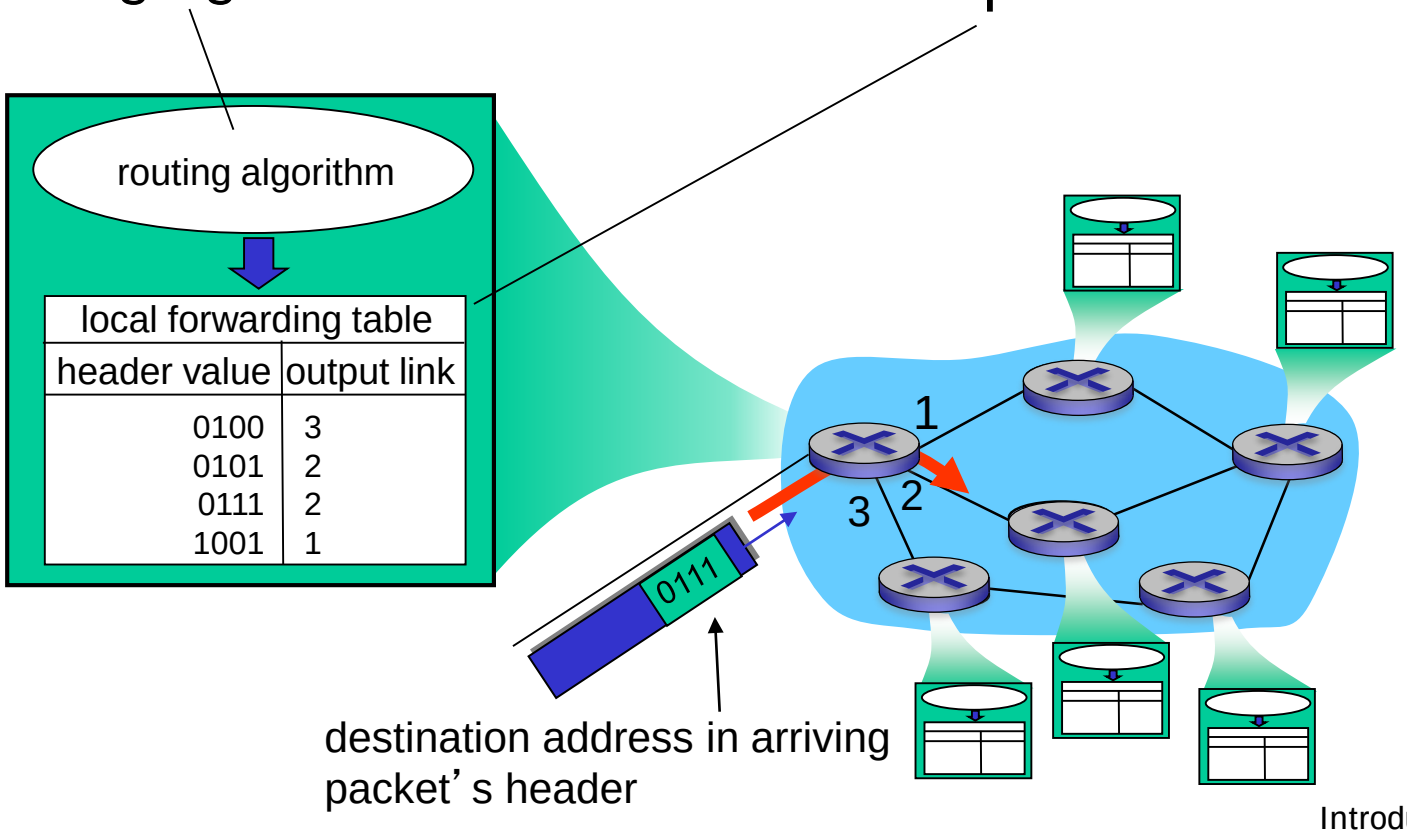
- if arrival rate (in bits) to link exceeds transmission rate of link for a period of time:
  - packets will queue, wait to be transmitted on link
  - packets can be dropped (lost) if memory (buffer) fills up

# 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

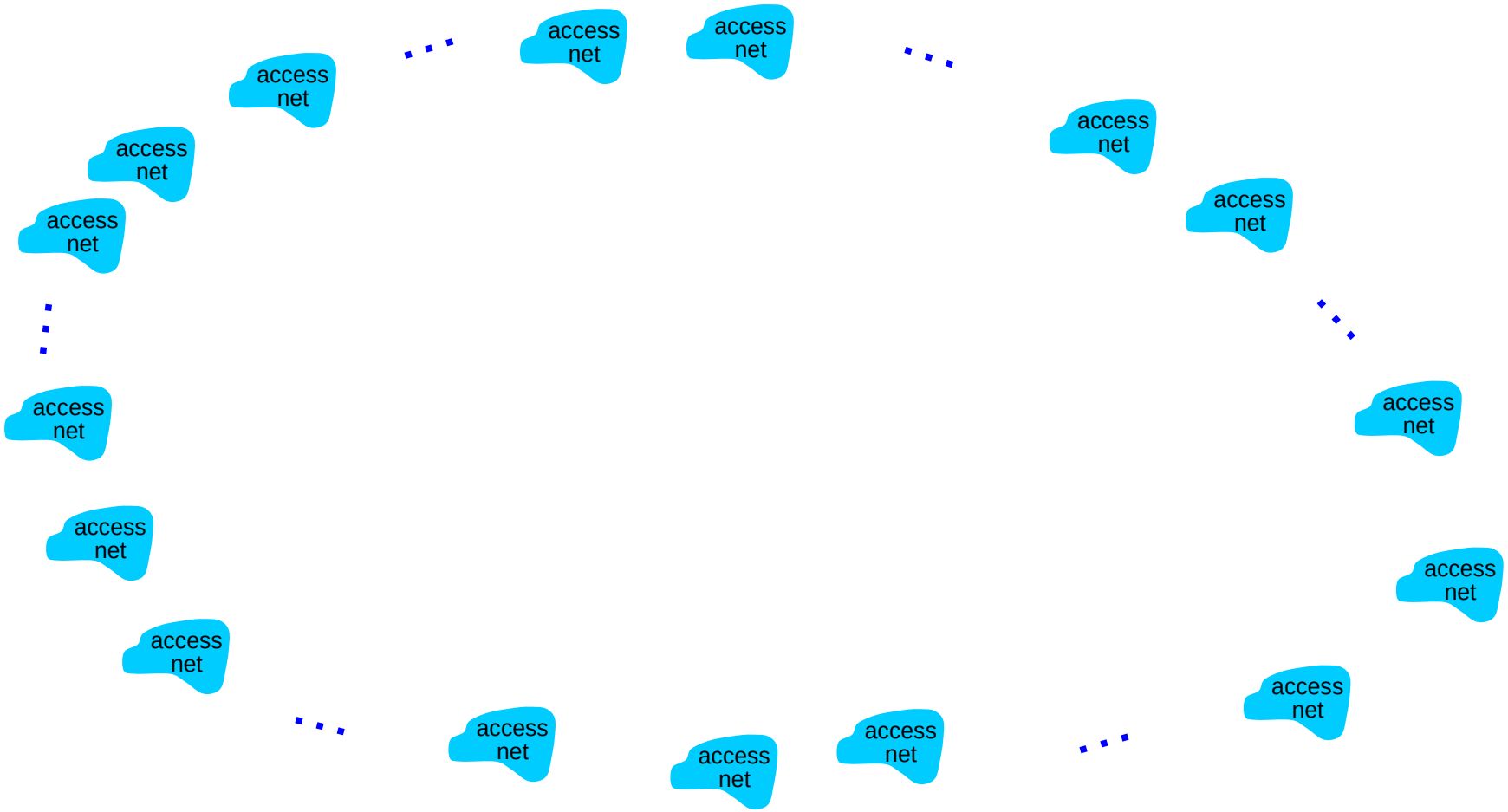


# Internet structure: network of networks

- 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

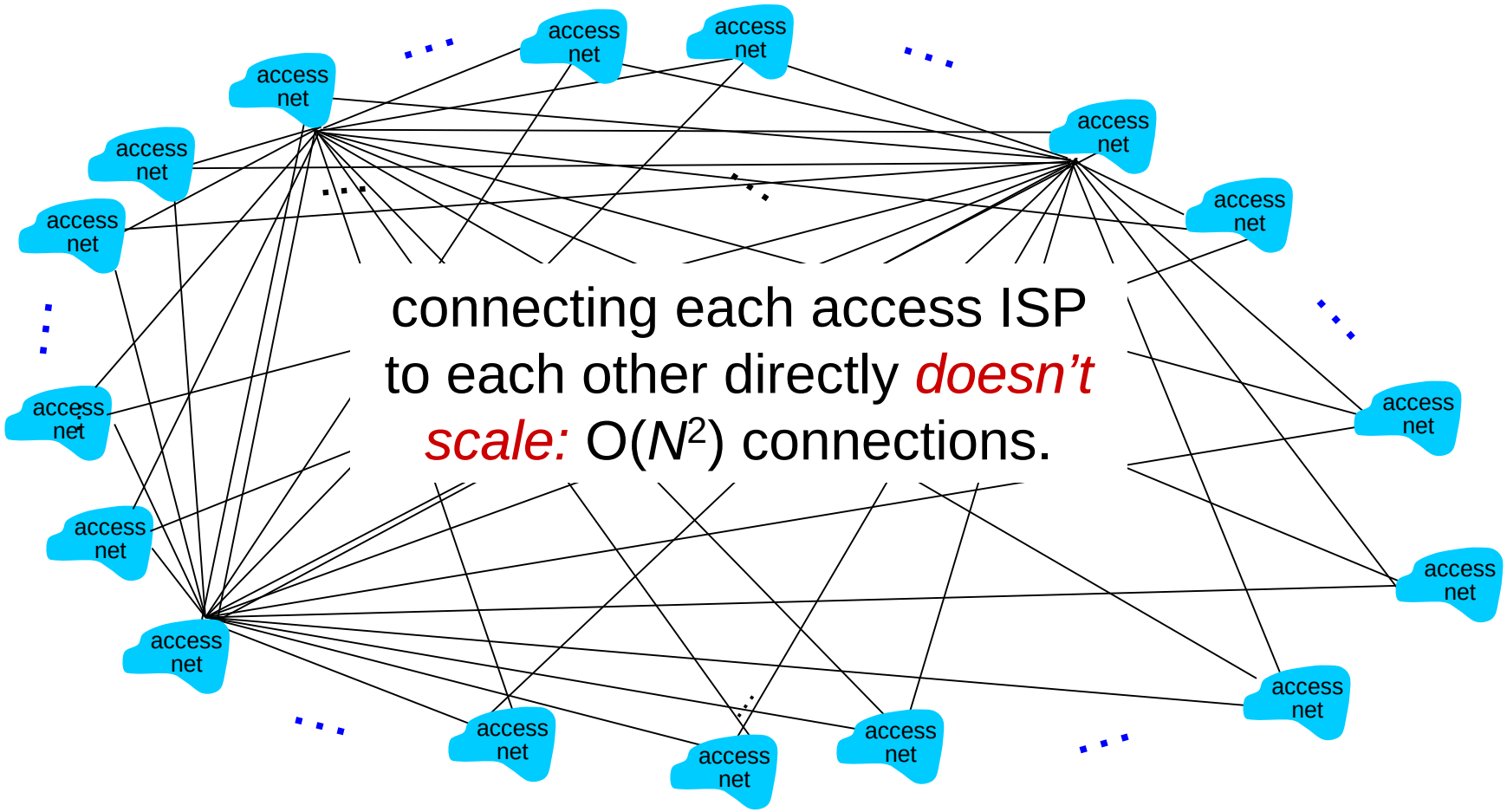
# Internet structure: network of networks

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



# Internet structure: network of networks

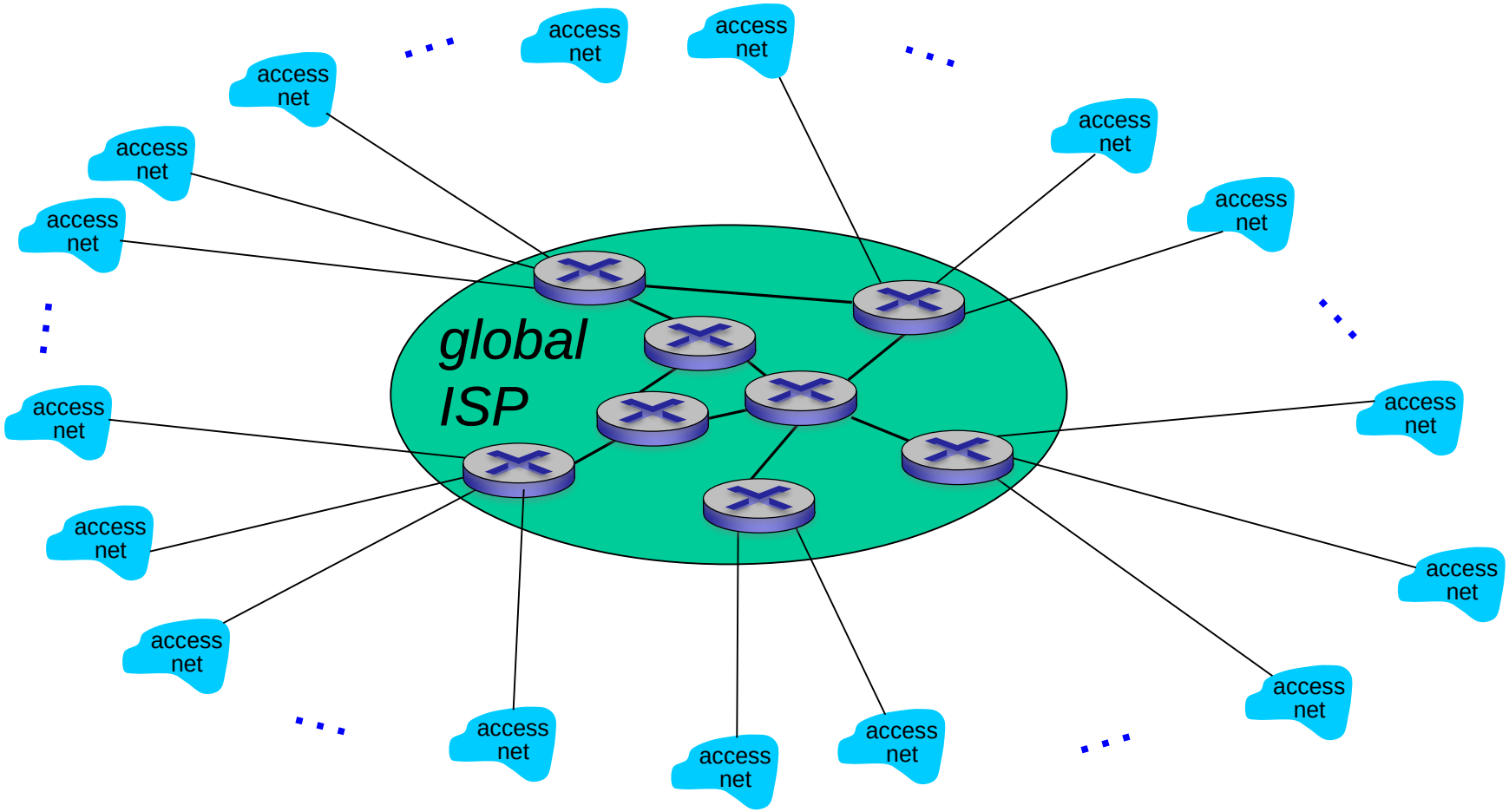
*Option: connect each access ISP to every other access ISP?*



# Internet structure: network of networks

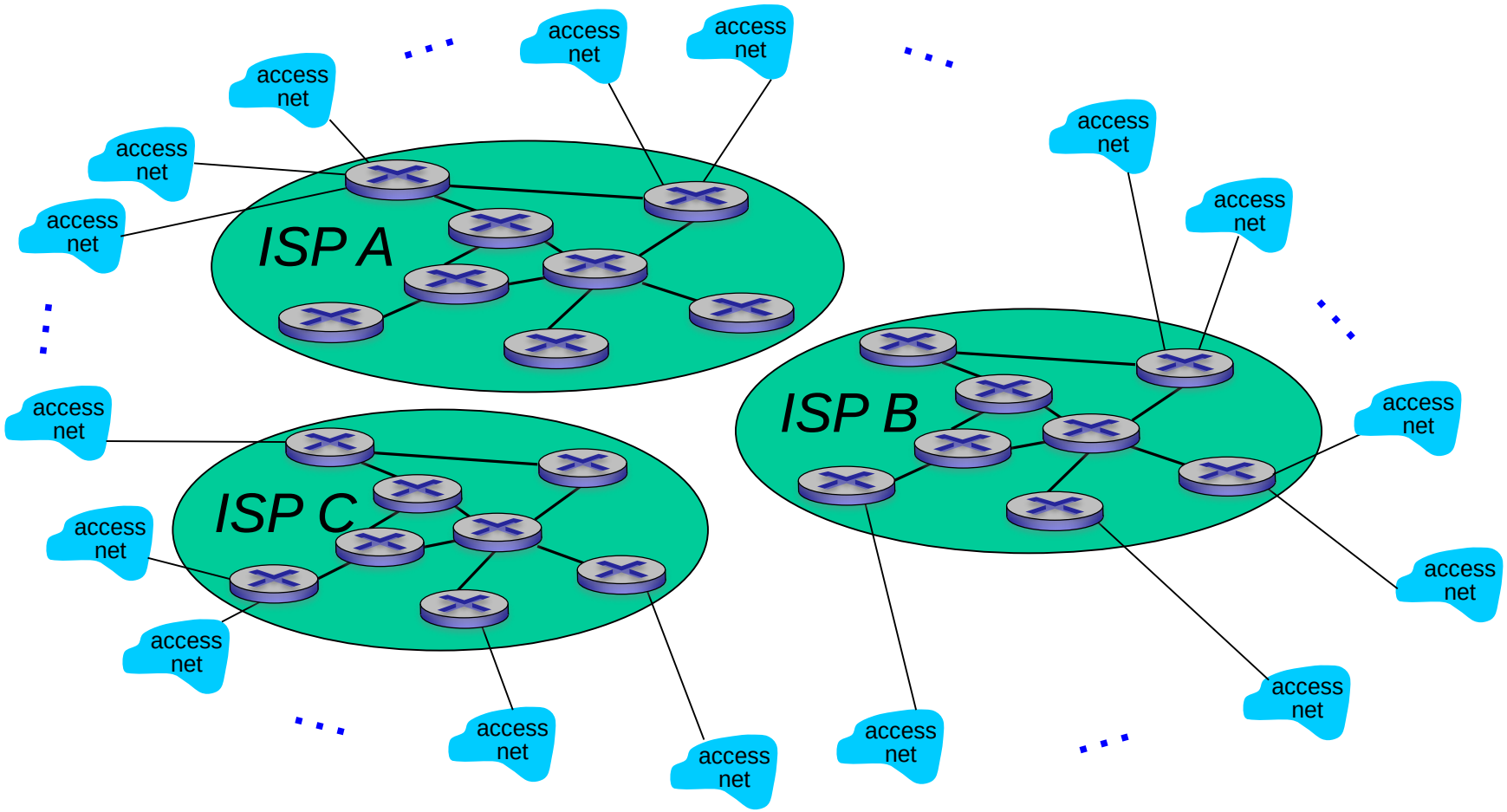
*Option: connect each access ISP to one global transit ISP?*

*Customer and provider ISPs have economic agreement.*



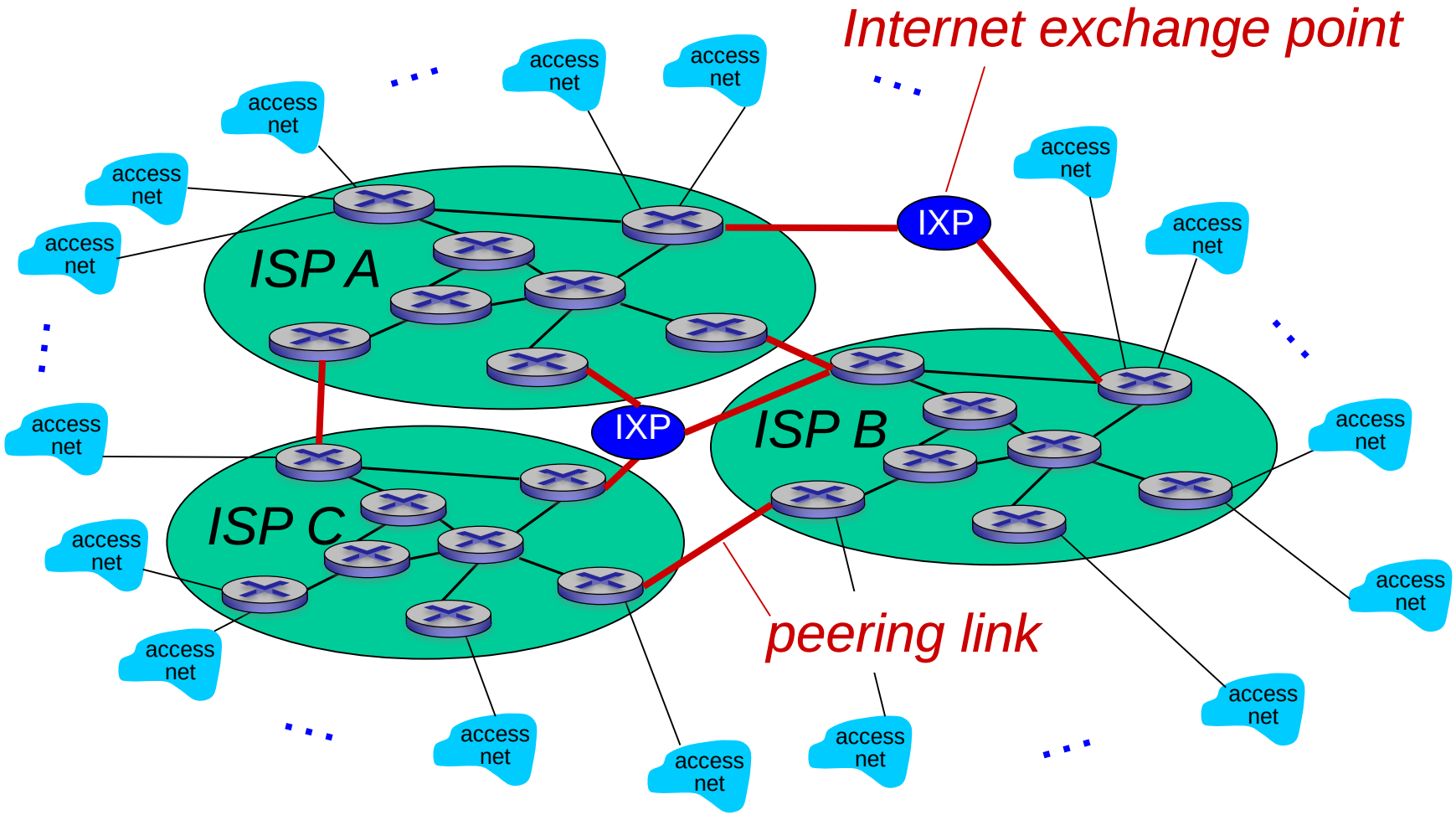
# Internet structure: network of networks

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



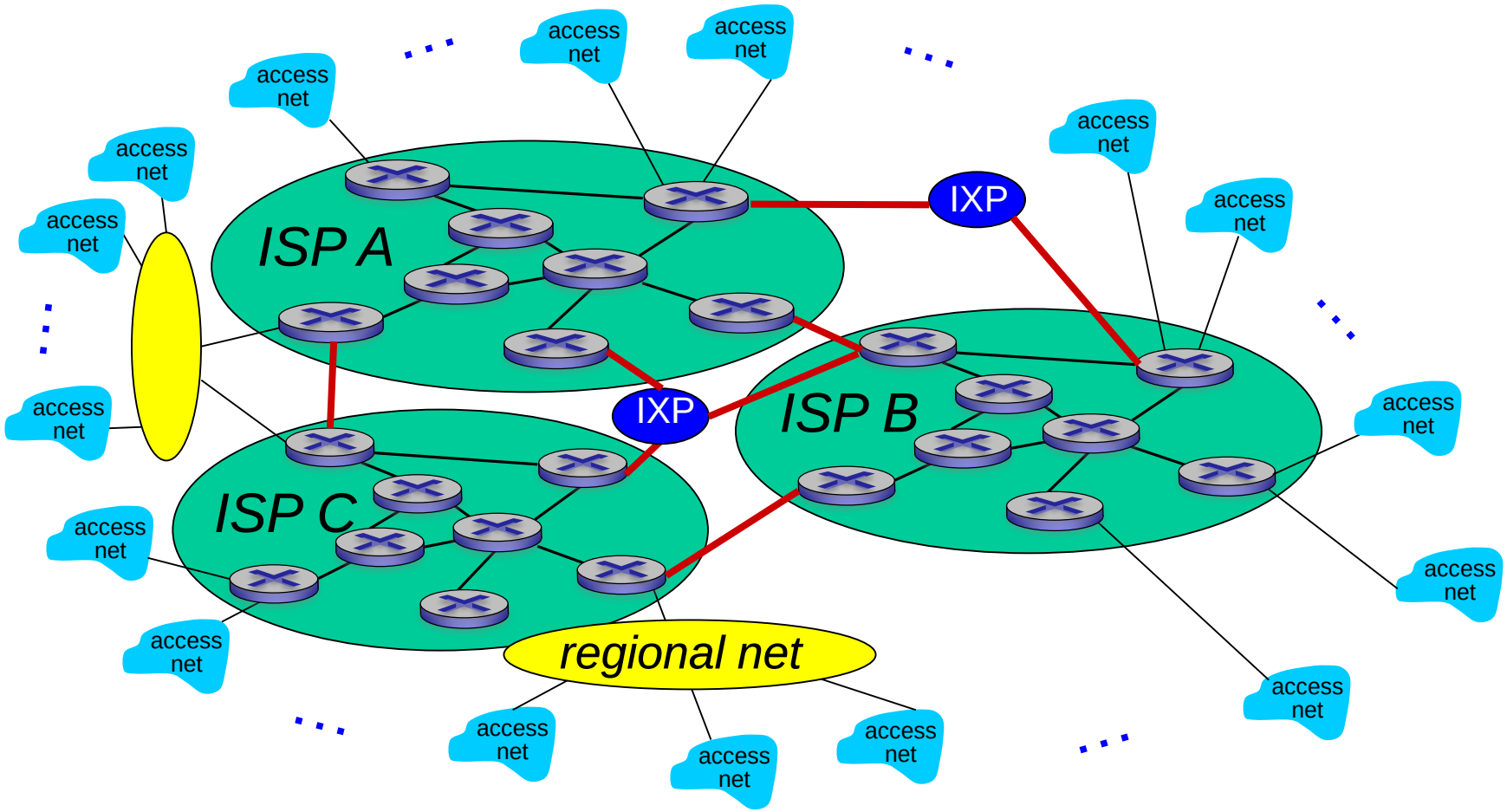
# Internet structure: network of networks

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



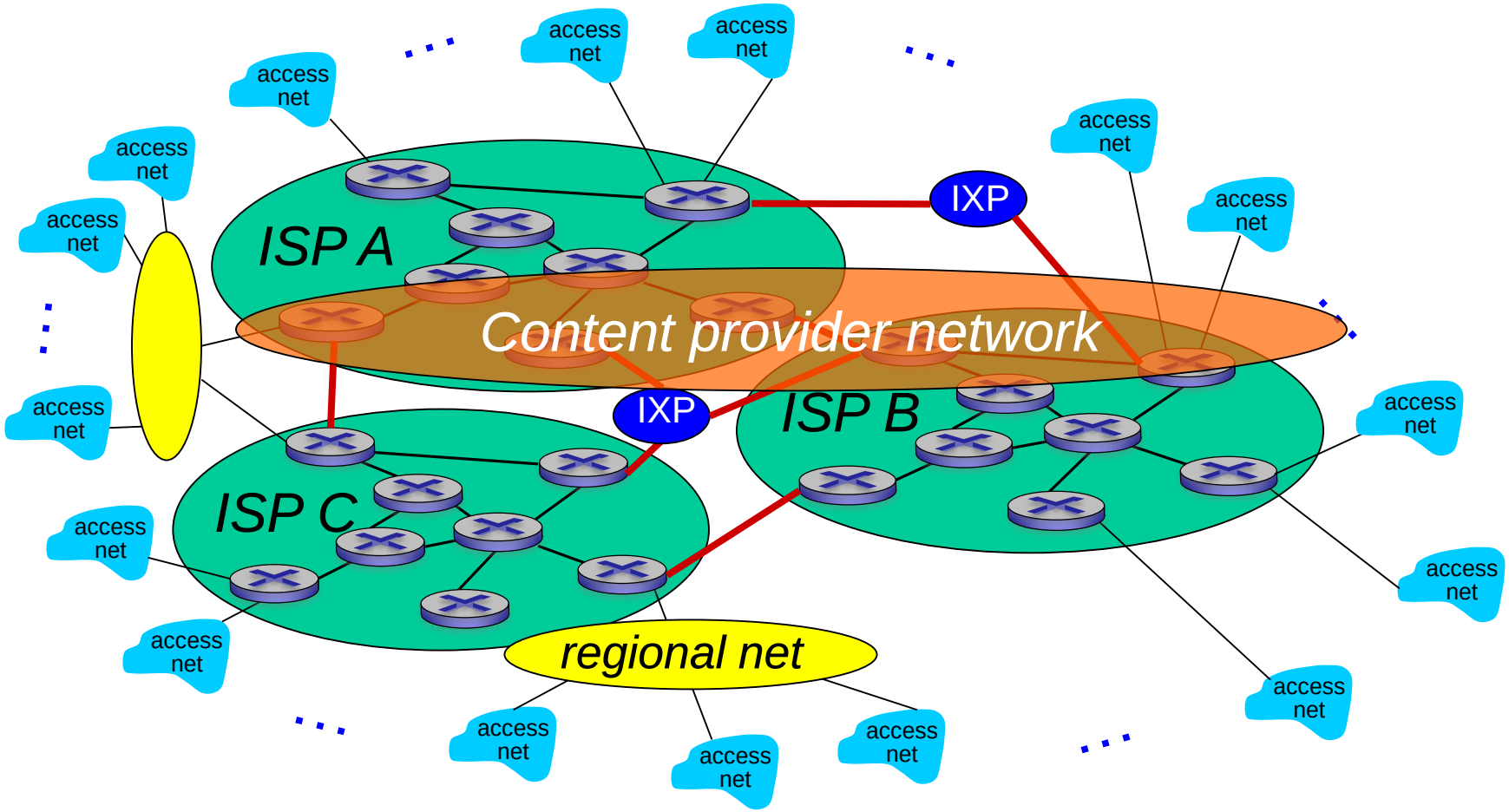
# Internet structure: network of networks

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

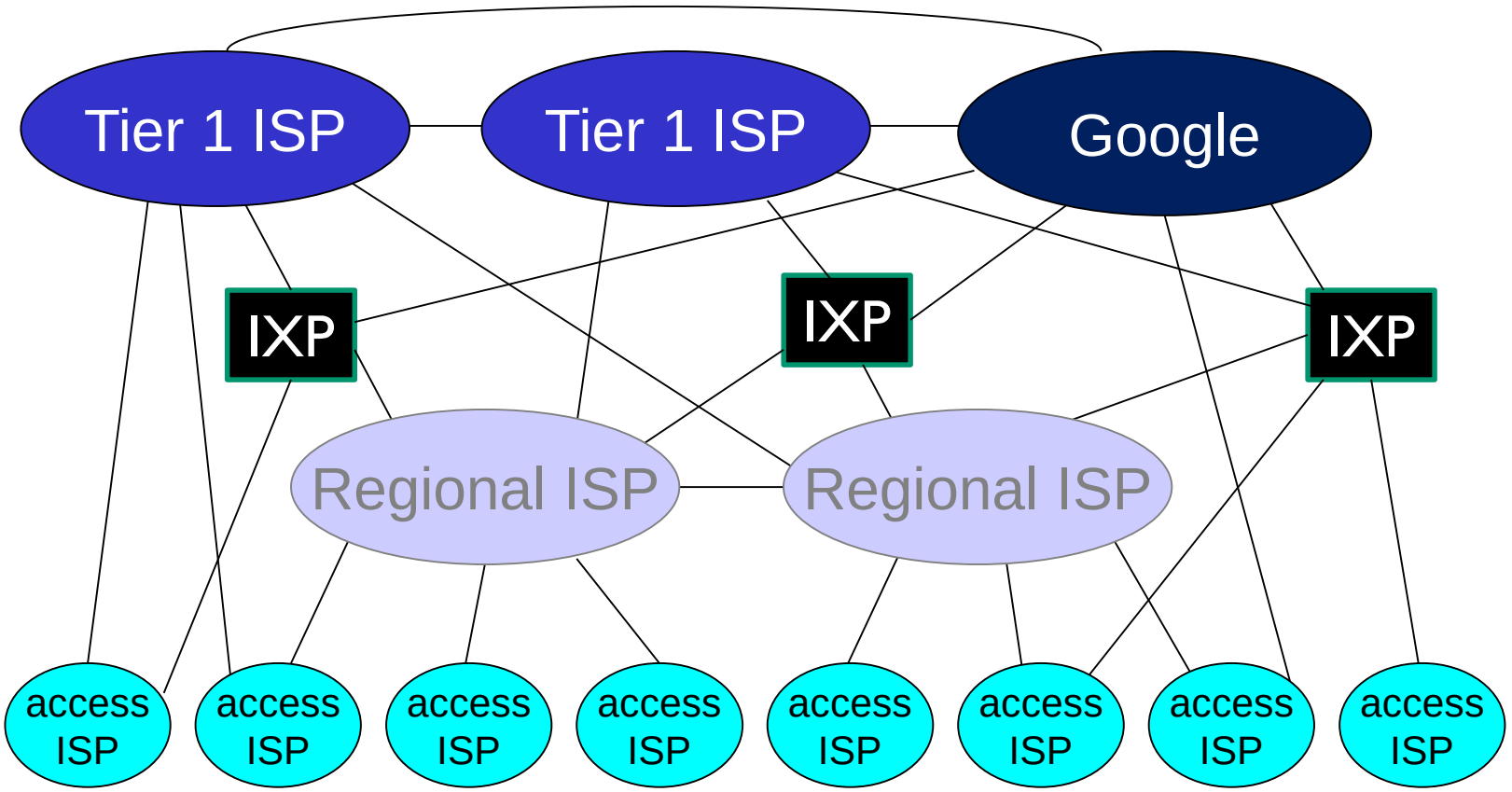


# Internet structure: network of networks

… 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., Vocus, Global Gateway, 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

# 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

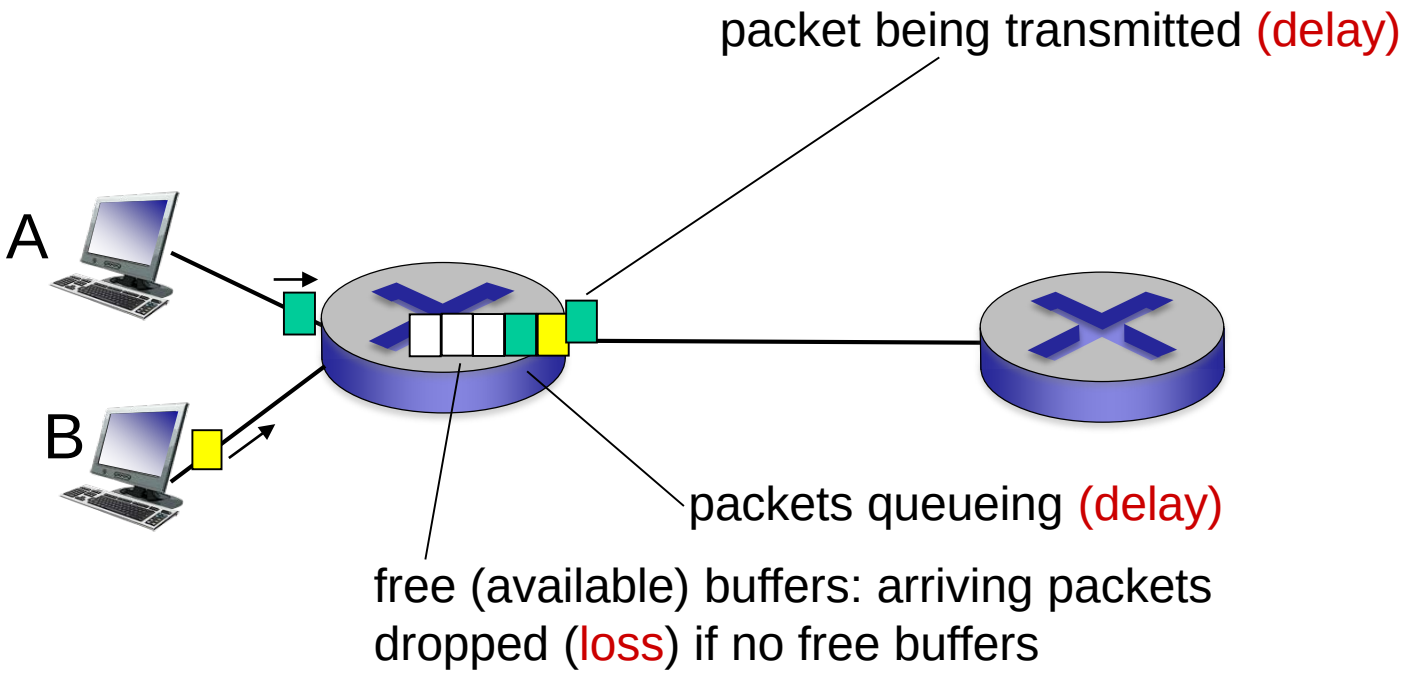
1.5 protocol layers, service models

1.6 networks under attack: security

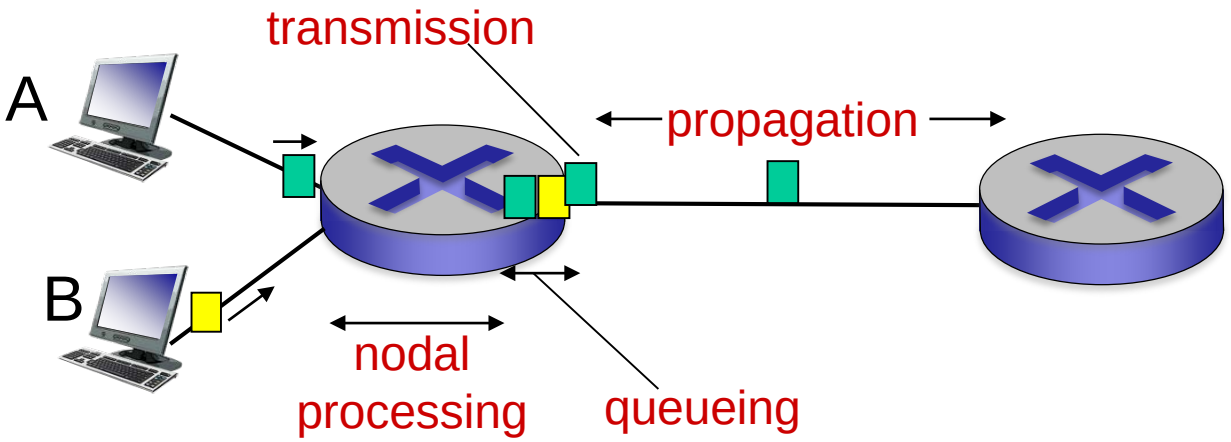
# How do loss and delay occur?

packets *queue* in router buffers

- packet arrival rate to link (temporarily) exceeds output link capacity
- packets queue, wait for turn



# Four sources of packet delay




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

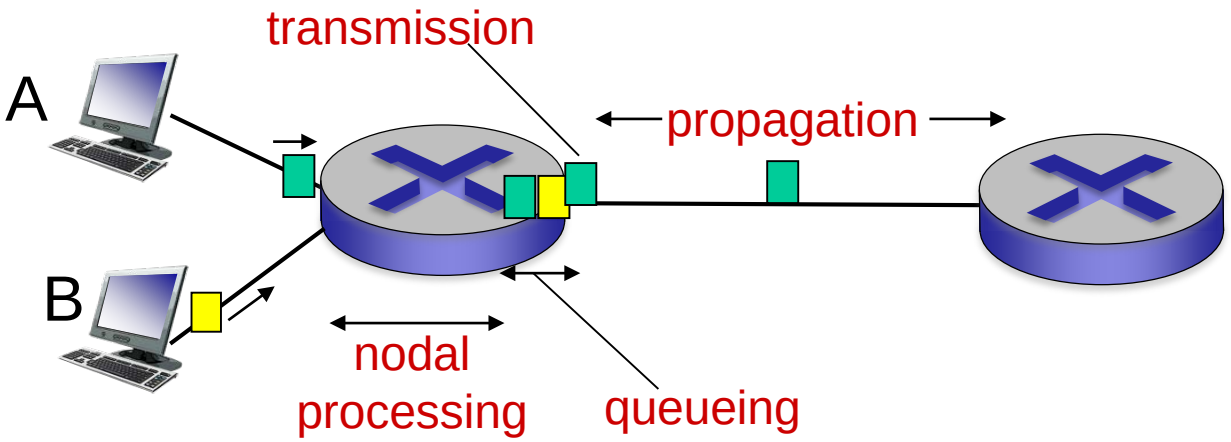
## $d_{proc}$: nodal processing

- check bit errors
- determine output link
- typically < msec

## $d_{queue}$: queueing delay

- time waiting at output link for transmission
- depends on congestion level of router

# Four sources of packet delay




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

$d_{trans}$: transmission delay:

- $L$: packet length (bits)
- $R$: link *bandwidth (bits/s)*
- $d_{trans} = L/R$

$d_{trans}$ and $d_{prop}$ *very* different

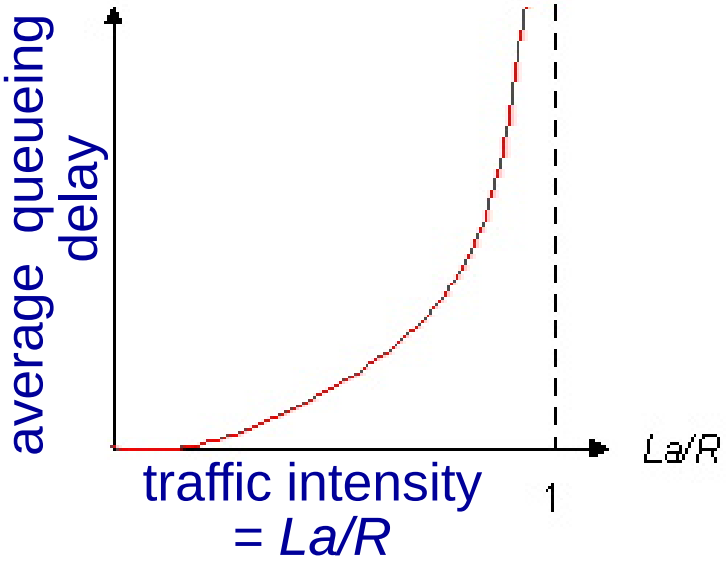
$d_{prop}$: propagation delay:

- $d$: length of physical link
- $s$: propagation speed (~$2 \times 10^8$ m/sec)
- $d_{prop} = d/s$

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

# Queueing delay (revisited)

- *R*: link bandwidth (bits/s)
- *L*: packet length (bits)
- a: average packet arrival rate



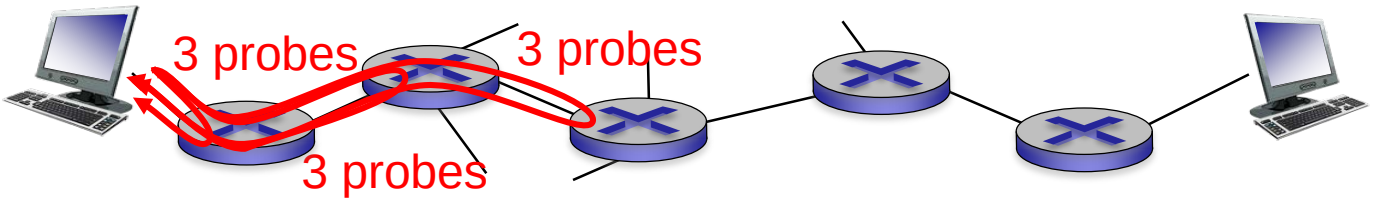

- *La/R* ~ 0: avg. queueing delay small
- *La/R* -> 1: avg. queueing delay large
- *La/R* > 1: more "work" arriving than can be serviced, average delay infinite!

*La/R* ~ 0

*La/R -> 1*

# "Real" Internet delays and routes

- what do "real" Internet delay & loss look like?
- `traceroute` program: provides delay measurement from source to router along end-end Internet path towards destination. For all *i:*
  - sends three packets that will reach router *i* on path towards destination
  - router *i* will return packets to sender
  - sender times interval between transmission and reply.



# "Real" Internet delays, routes

traceroute: gaia.cs.umass.edu to www.eurecom.fr

3 delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12  nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13  nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14  r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15  eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

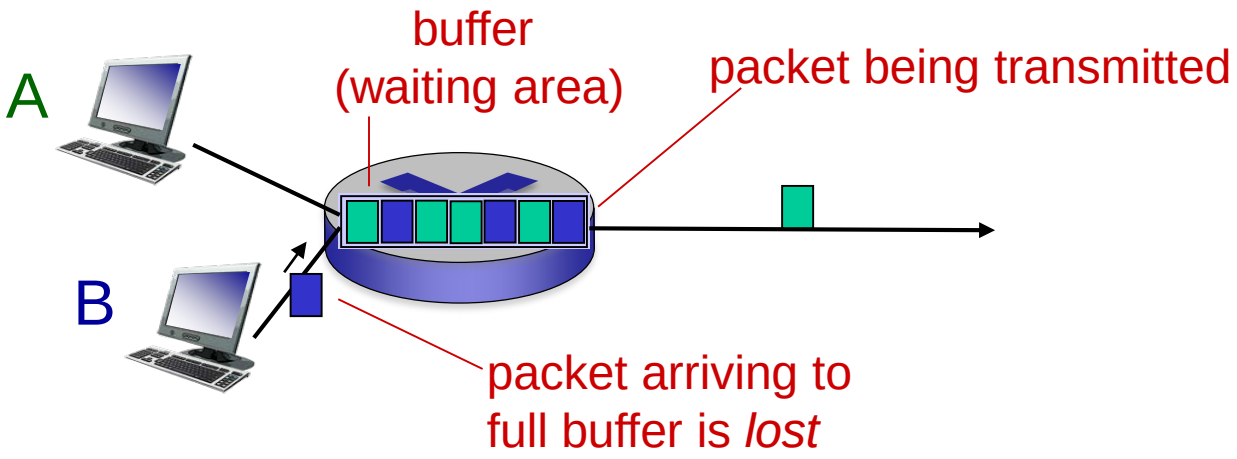
trans-oceanic link

* means no response (probe lost, router not replying)

* Do some traceroutes from exotic countries at www.traceroute.org

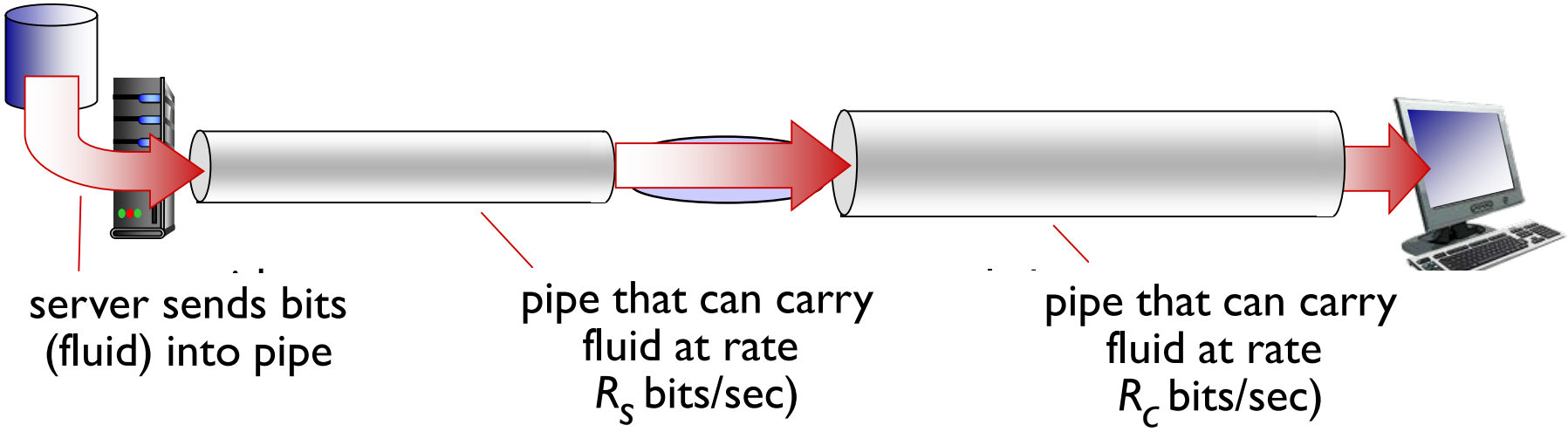
# Packet loss

- queue (aka buffer) preceding link in buffer has finite capacity
- packet arriving to full queue dropped (aka lost)
- lost packet may be retransmitted by previous node, by source end system, or not at all



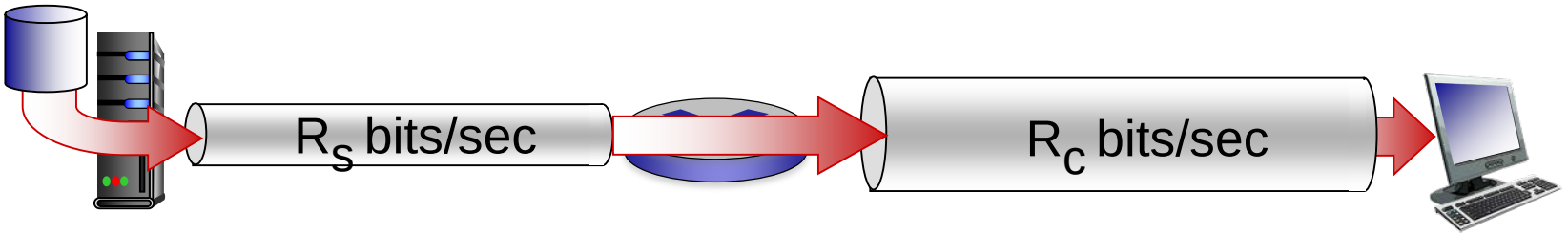
# Throughput

- *throughput:* rate (bits/time unit) at which bits transferred between sender/receiver
  - *instantaneous:* rate at given point in time
  - *average:* rate over longer period of time

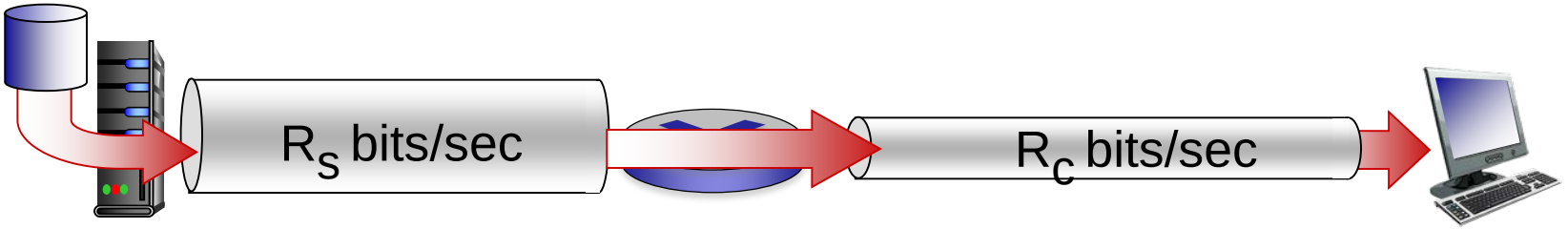


# Throughput (more)

- $R_s < R_c$ What is average end-end throughput?




- $R_s > R_c$ What is average end-end throughput?

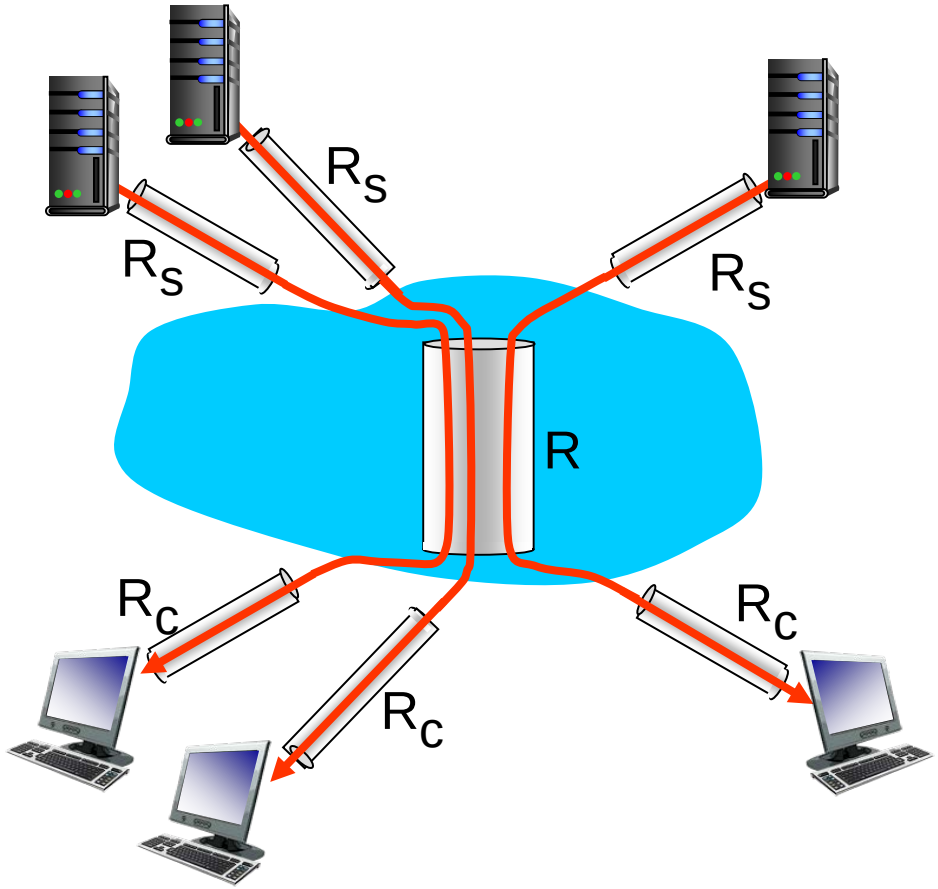



*bottleneck link*

link on end-end path that constrains end-end throughput

# Throughput: Internet scenario

- per-connection end-end throughput: *min(*$R_c$*,*$R_s$*,R/10)*
- in practice: $R_c$ or $R_s$ is often bottleneck




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

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

# 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

# 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?

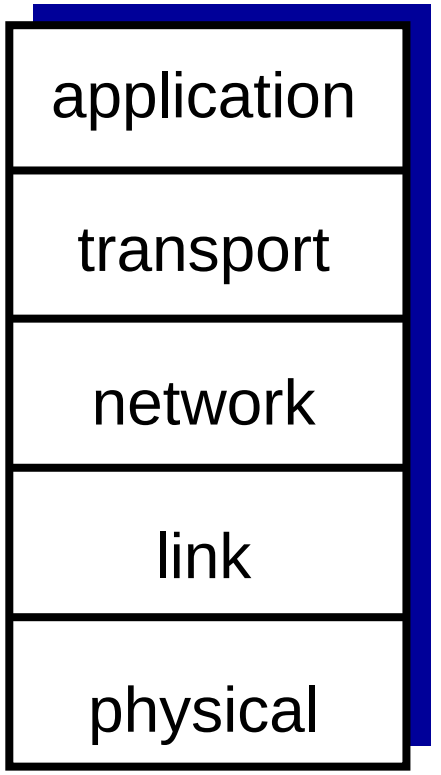
# Why layering?

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?

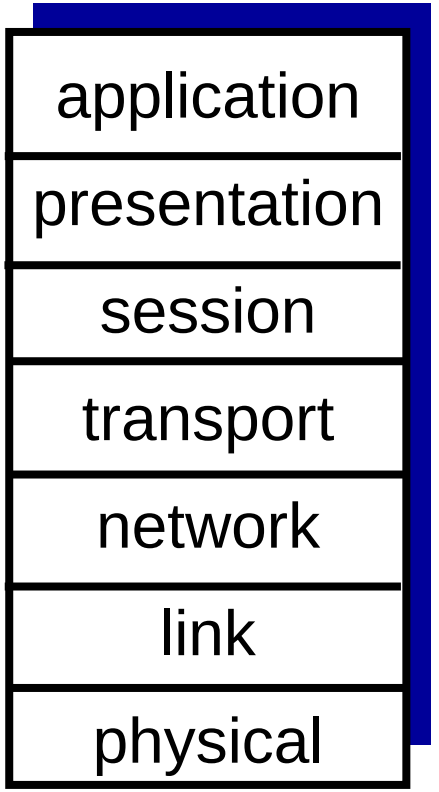
# Internet protocol stack

- *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"

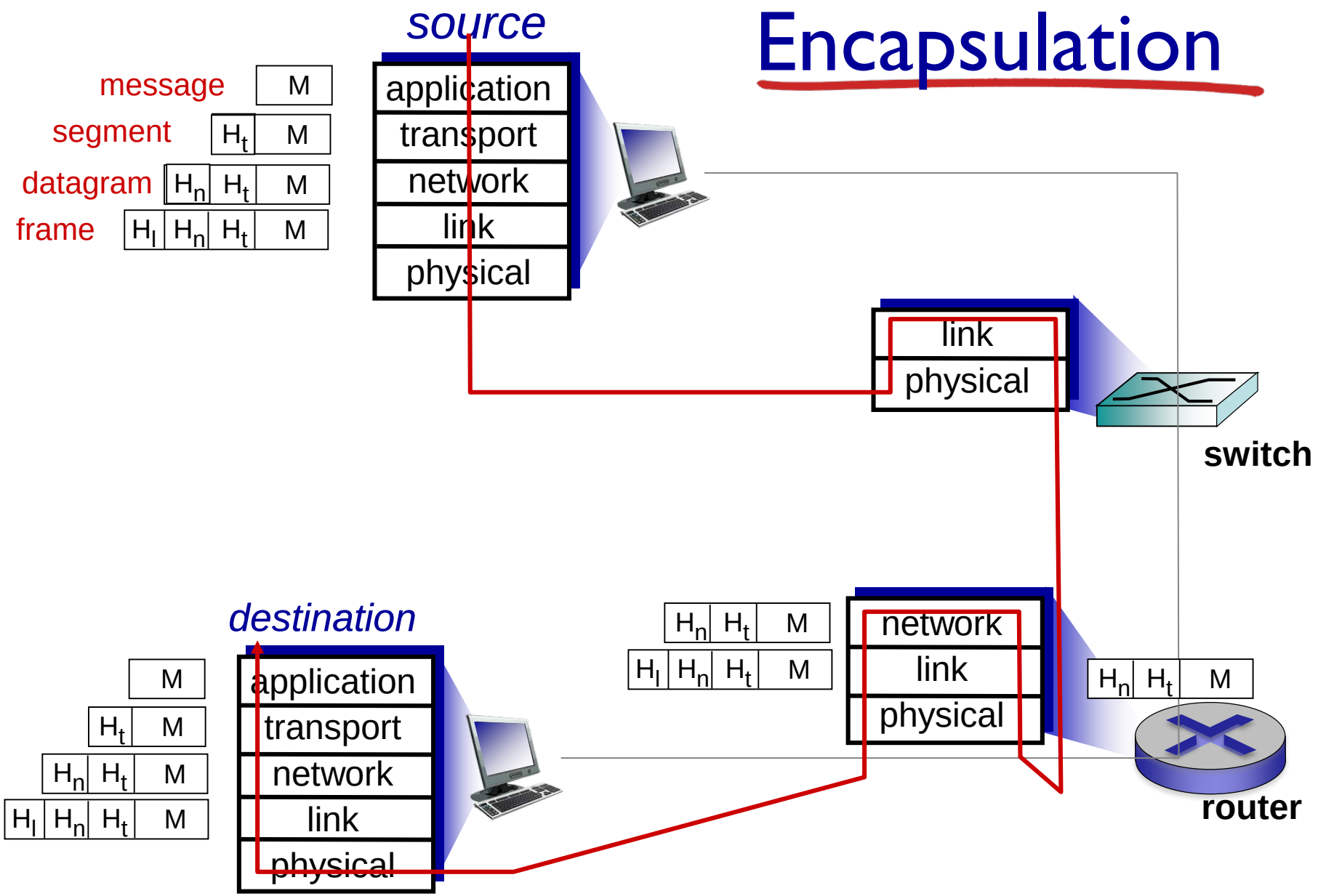


# ISO/OSI reference model

- *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?

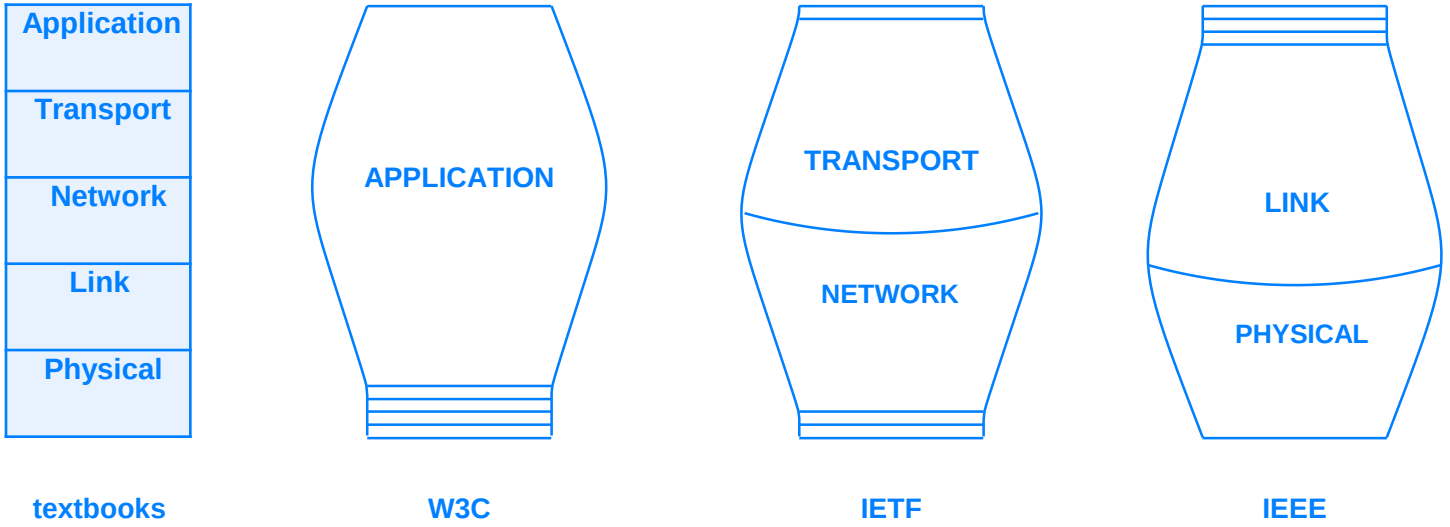


# Encapsulation



# Different perspectives

- Standards bodies and academic programs each emphasize certain layers of a protocol stack, leading to the following views



# 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

# 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!

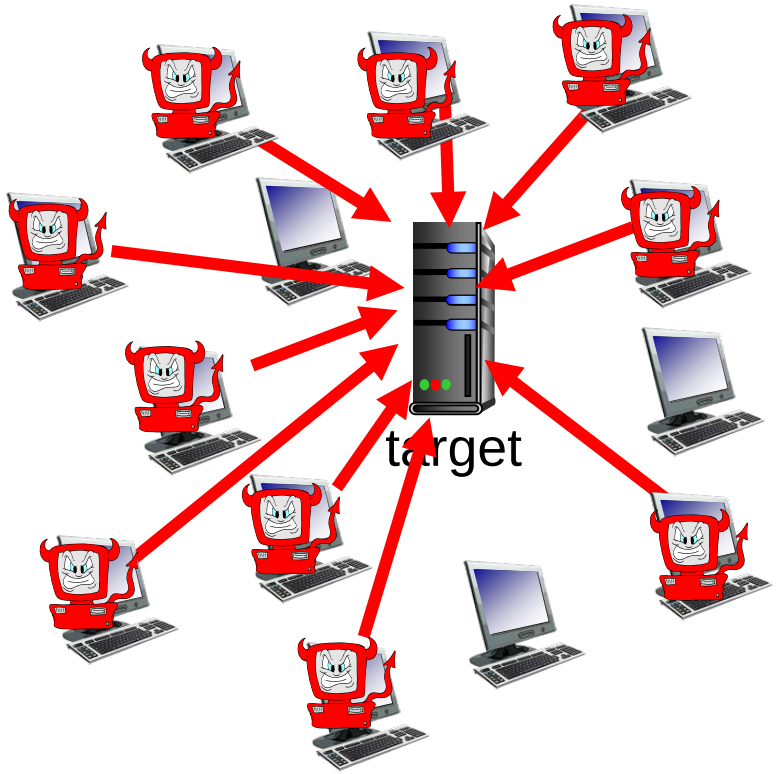
# Bad guys: put malware into hosts via Internet

- 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 a 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

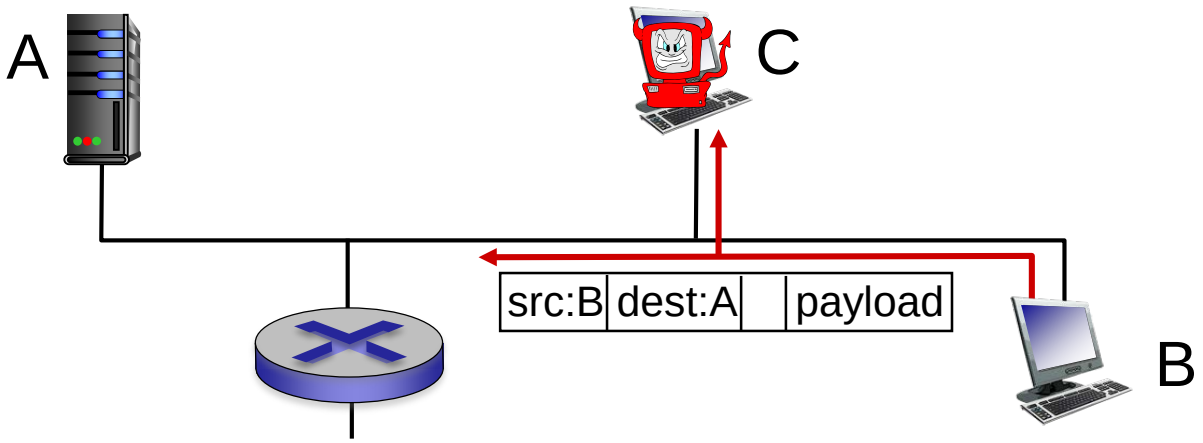
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



# Bad guys can sniff packets

*packet "sniffing":*

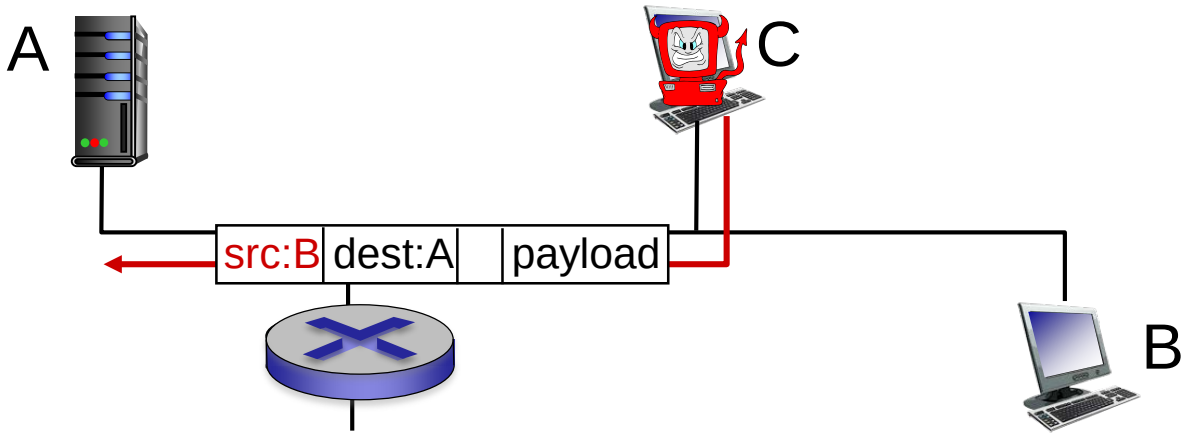
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by




- wireshark software used for network analysis is a (free) packet-sniffer

# Bad guys can use fake addresses

*IP spoofing:* send packet with false source address




*… lots more on security (in second half of the course)*

# 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

# Introduction: summary

*covered a "ton" of material!*

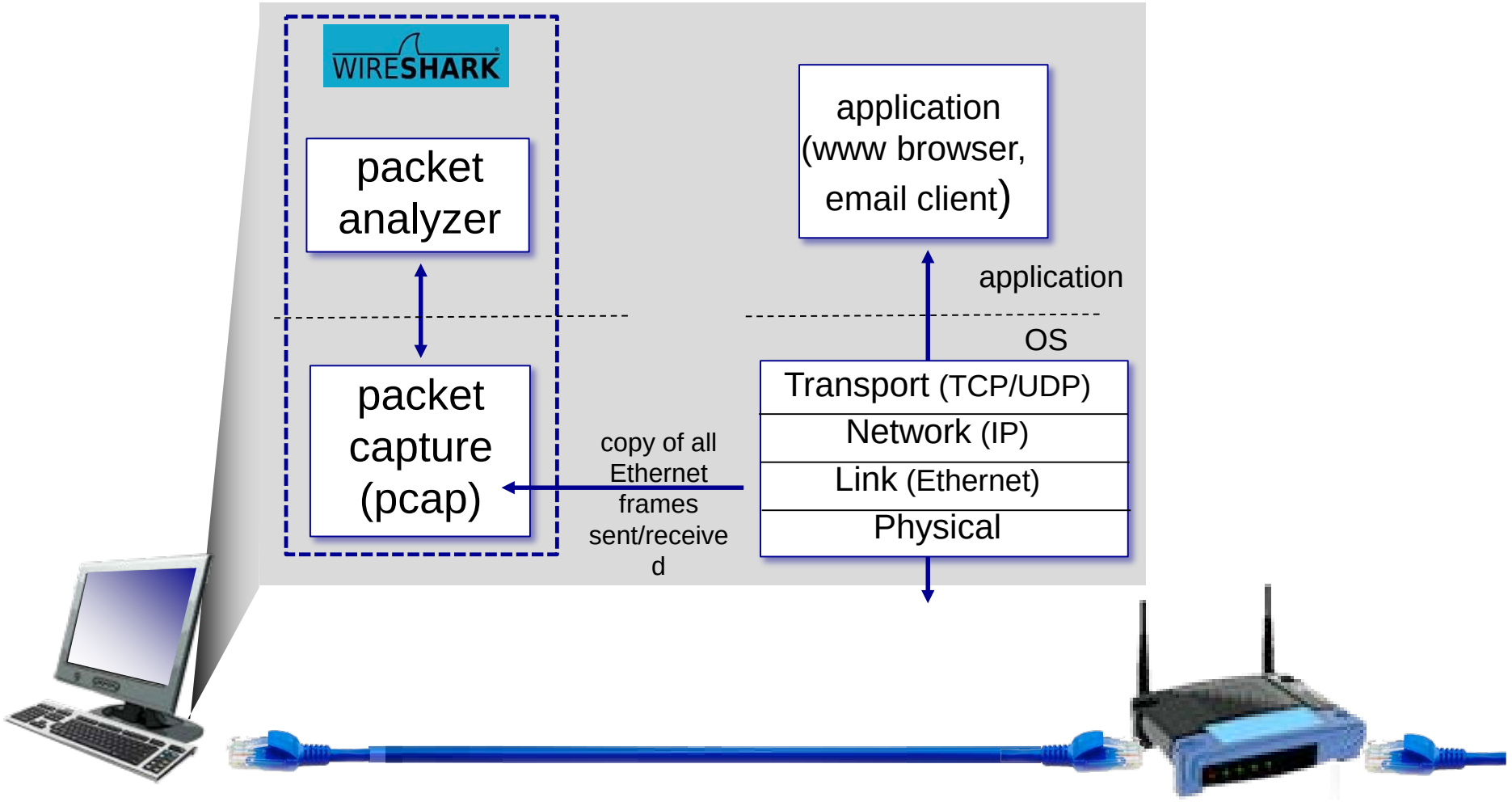
- Internet overview
- what's a protocol?
- network edge, core, access network
  - packet-switching versus circuit-switching
  - Internet structure
- performance: loss, delay, throughput
- layering, service models
- security

*you now have:*

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

# Acknowledgements


- The vast majority of these slides are supplied and/or adapted from Computer networks, A Top Down approach , by J.F. Kurose and K.W. Ross.
- Slides 12,21,22, 26-31, and 62 have been adapted from Computer Networks and internet by D.E. Comer.


WIRESHARK
packet analyzer
packet capture (pcap)
application (www browser, email client)
application
OS
Transport (TCP/UDP)
Network (IP)
Link (Ethernet)
Physical
copy of all Ethernet frames sent/received