Welcome to

Data Communication and Computer Networks (DCCN)

By Ihsan Ul Haq,

Assistant Professor

Tentative Policy

- **Grading Policy:**
- Final Exam: 60%
- Mid Term Exam: 20%

- Sessional:
- Project Presentations: 7%
- Home Assignments: 8%
- Pop Up Quizzes: 10%

Mailing List

Data Communication and Networks (DCN)

https://groups.yahoo.com/neo/groups/commSysFall18/info

Contact Hours: Wednesday 2 – 4 pm
Location: Office adjacent to Lab-1

Academic Honesty

- **Your work in this class must be your own**

• If students are found to have collaborated excessively or to have cheated (e.g. by copying or sharing answers in assignments or Quizes), all involved will at a minimum receive grades of **0** for the first infraction

- Further infractions will result in failure in the course

NO MOBILE DURING CLASS & OBSERVE THE CLASS TIMINGS

Text Book

- William Stallings, “Data & Computer Communications”. Prentice-Hall, Tenth Edition
- Computer Networks Top down Approach By Ross 7th Edition
- Larry Peterson, Bruce Davie, “Computer Networks”, Morgan Kaufmann 5th Edition
- Behrouz A. Ferouzan, “Data Communications & Networking”, McGraw-Hill, 5th Edition

Data and Computer Communications

CHAPTER 1

Data Communications, Data Networks, and the Internet

THIS INTRODUCTORY CHAPTER BEGINS WITH A GENERAL MODEL OF COMMUNICATIONS.

“The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point”

- *The Mathematical Theory of Communication*,

Claude Shannon

Learning Objectives

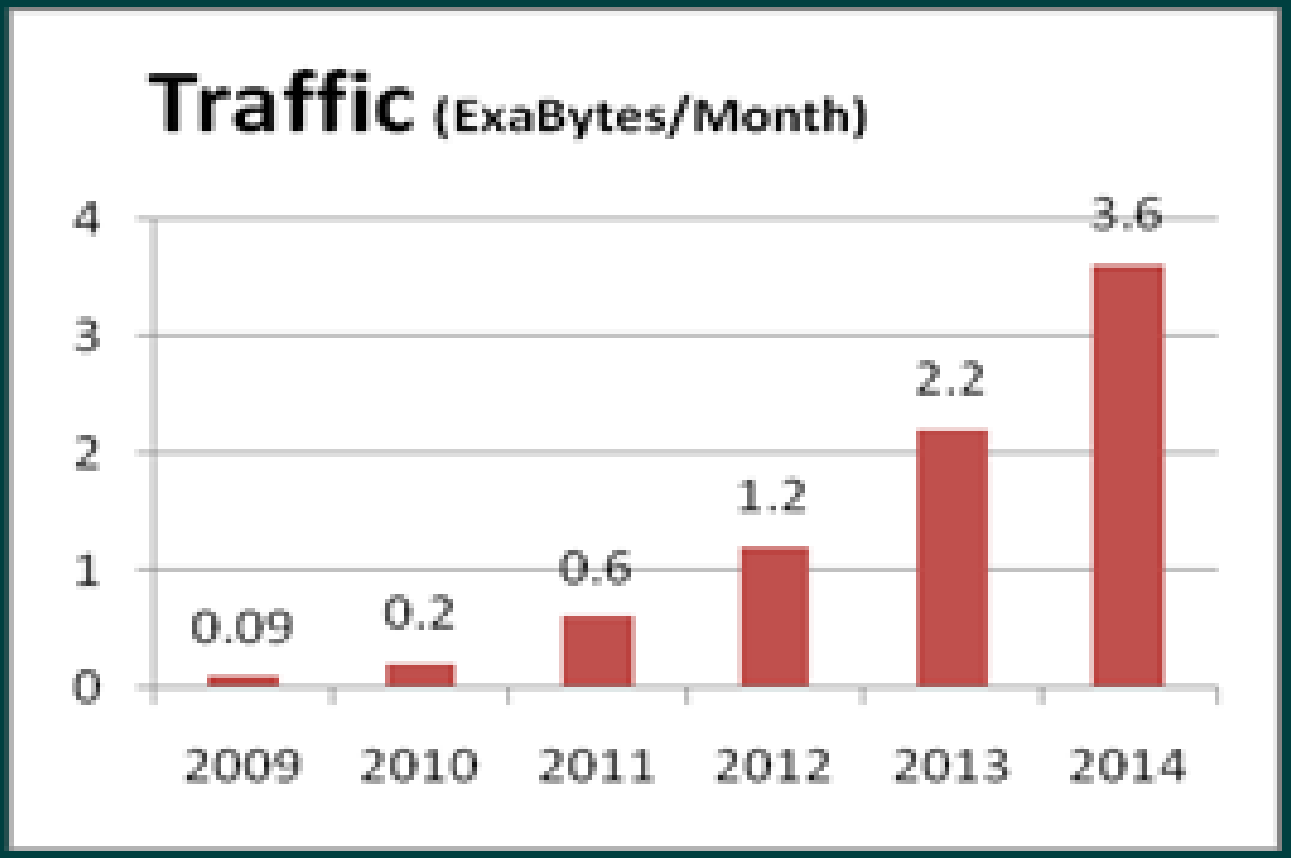
- Present an overview of data communications traffic volume trends.
- Understand the key elements of a data communications system.
- Summarize the types of data communications networks.
- Present an overview of the overall architecture of the Internet.

Key Points

- The scope of this course is broad, covering three general areas: *data communications, networking, and protocols*
- Data communications deals with the transmission of signals in a reliable and efficient manner. Topics covered include signal generation, transmission, transmission media, signal encoding, interfacing, data link control, and multiplexing.
- Networking deals with the technology and architecture of the communications networks used to interconnect communicating devices. This field is generally divided into local area networks (LANs) and wide area networks (WANs)

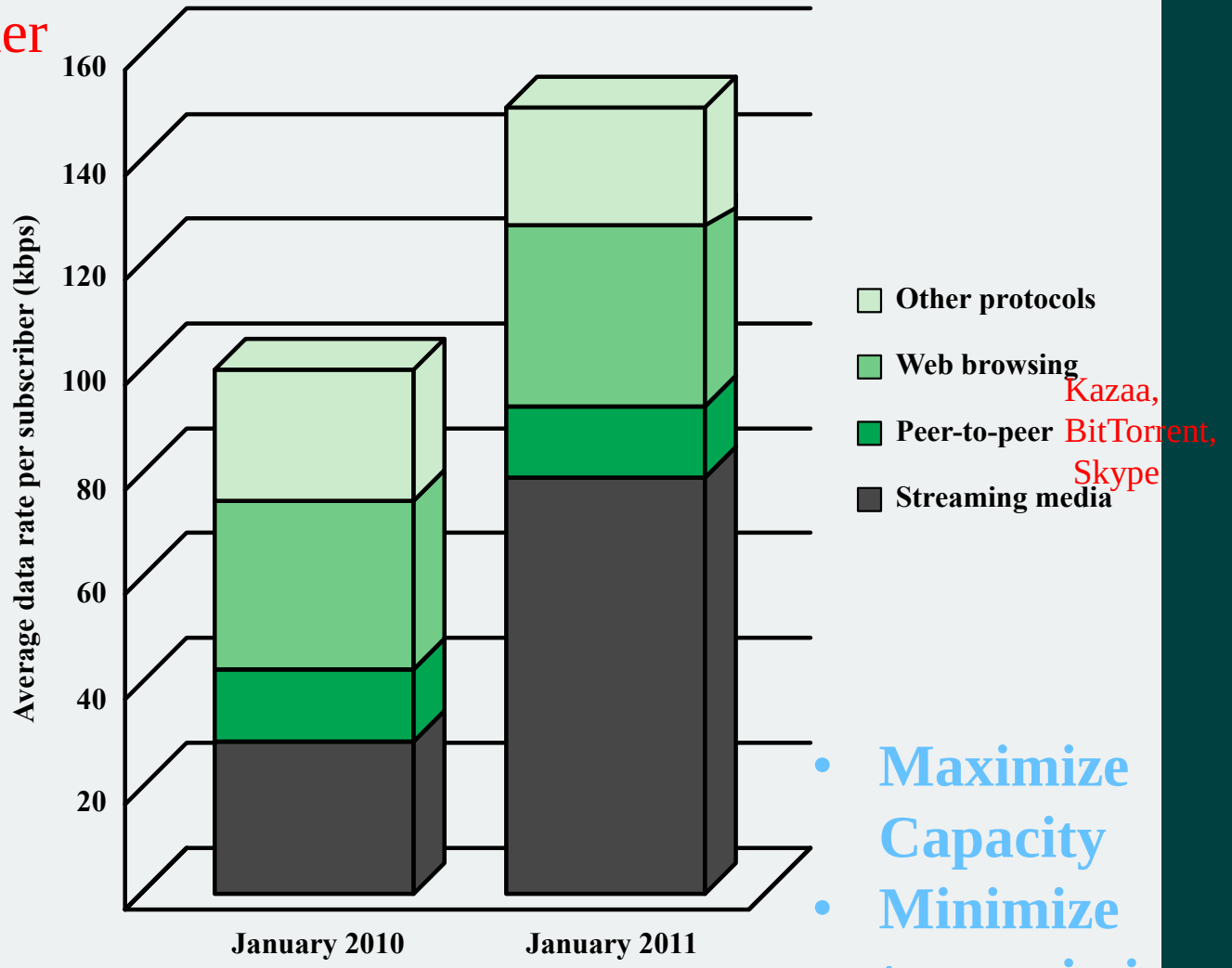
Technological Advancement Driving Forces

Cisco VNI Mobile, 2010



1 Exa = 10^{18}

Streaming media is multimedia that is constantly received by and presented to an end-user while being delivered by a provider



- **Maximize Capacity**
- **Minimize transmission cost**

Figure 1.1 Average Downstream Traffic per Internet Subscriber

Notable Trends

Trend toward faster and cheaper, in both computing and communication

- More powerful computers supporting more demanding applications
- The increasing use of optical fiber and high-speed wireless has brought transmission prices down and greatly increased capacity

Today's networks are more "intelligent"

- Differing levels of quality of service (QoS)
- Variety of customizable services in the areas of network management and security

The Internet, the Web, and associated applications have emerged as dominant features for both business and personal network landscapes

- "Everything over IP"
- Intranets and extranets are being used to isolate proprietary information

Mobility

- iPhone, Droid (smartphone by Motorolla), and iPad have become drivers of the evolution of business networks and their use
- Enterprise applications are now routinely delivered on mobile devices
- Cloud computing is being embraced

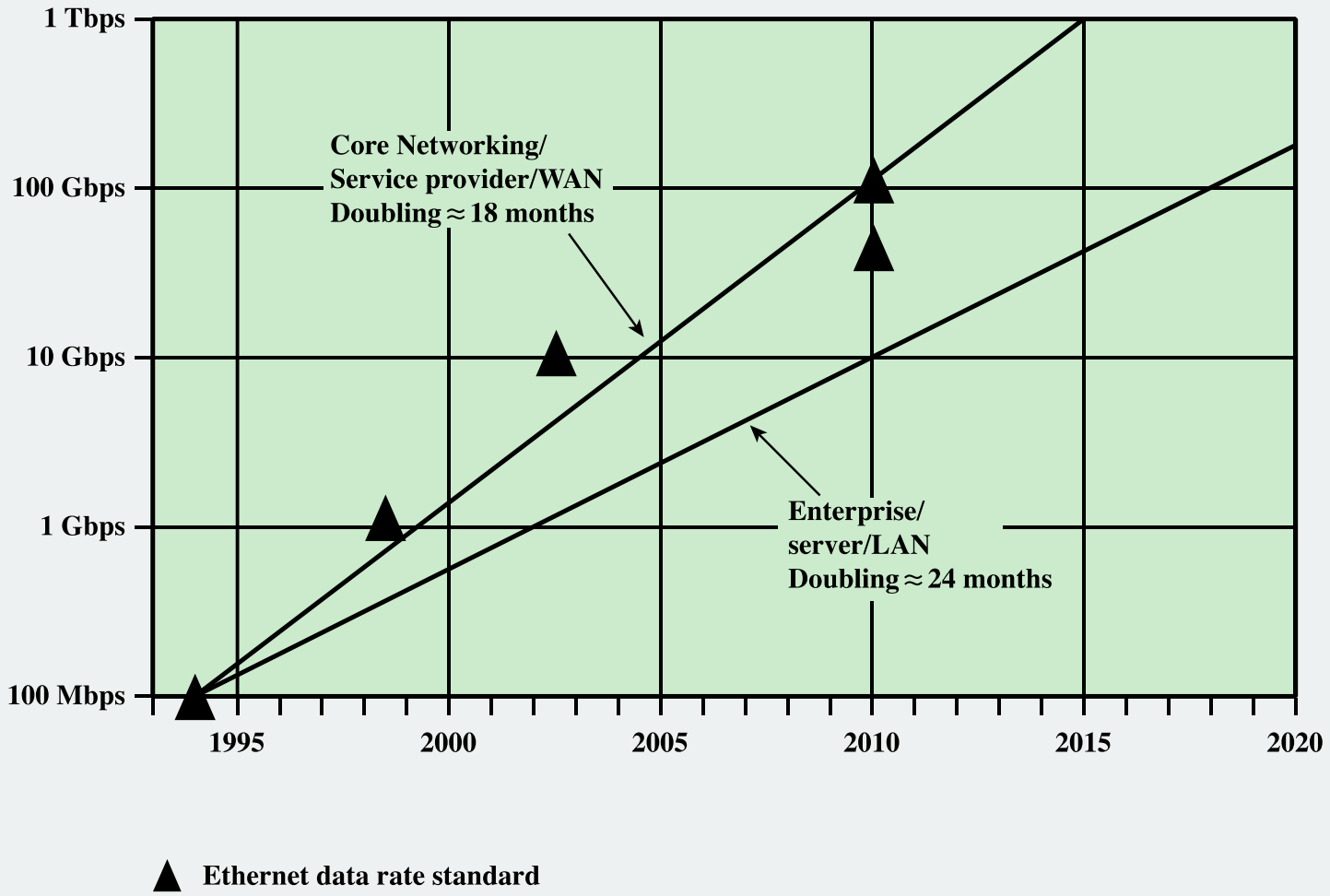


Figure 1.2 Past and Projected Growth in Ethernet Data Rate Demand Compared to Existing Ethernet Data Rates

Changes in Networking Technology

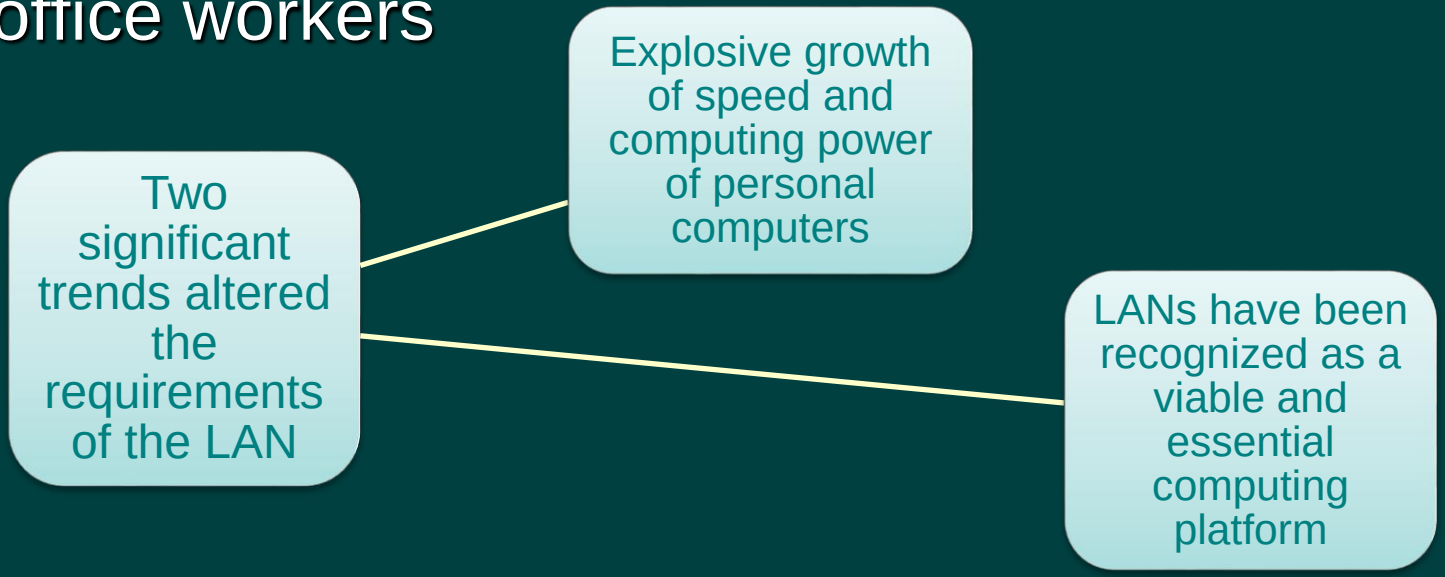
- Emergence of high-speed LANs
  - The speed and computing power of PC

* Corporate WAN needs

* Digital electronics

Emergence of High-Speed LANs

- Personal computers and microcomputer workstations have become an essential tool for office workers



- Examples of requirements that call for higher-speed LANs:
  - Centralized server farms
  - Power workgroups
  - High-speed local backbone

Corporate Wide Area Networking Needs

Changes in corporate data traffic patterns are driving the creation of high-speed WANs

- Growing use of telecommuting
- Nature of the application structure has changed
- Intranet computing
- More reliance on personal computers, workstations, and servers
- More data-intensive applications
- Most organizations require access to the Internet
- Traffic patterns have become more unpredictable
- Average traffic load has risen
- More data is transported off premises and into the wide area

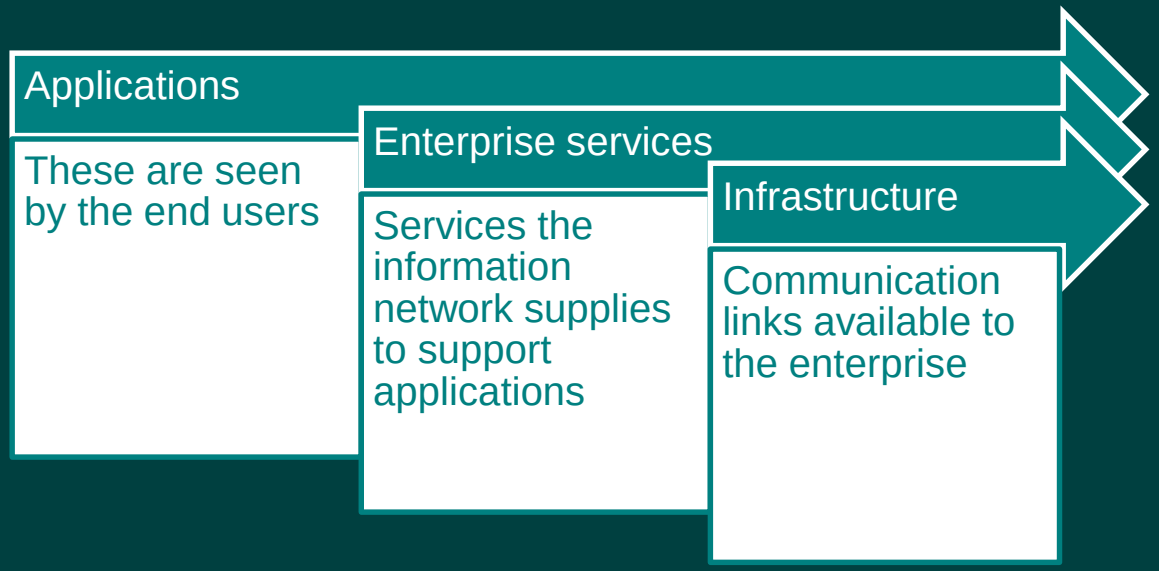
Digital Electronics

- The rapid conversion of consumer electronics to digital technology is having an impact on both the Internet and corporate intranets
  - Image and video traffic carried by networks is dramatically increasing
    - Because of their huge storage capacity digital versatile disks (DVDs) are being incorporated into Web sites
    - Digital camcorders have made it easier to make digital video files to be placed on corporate and Internet Web sites

Convergence

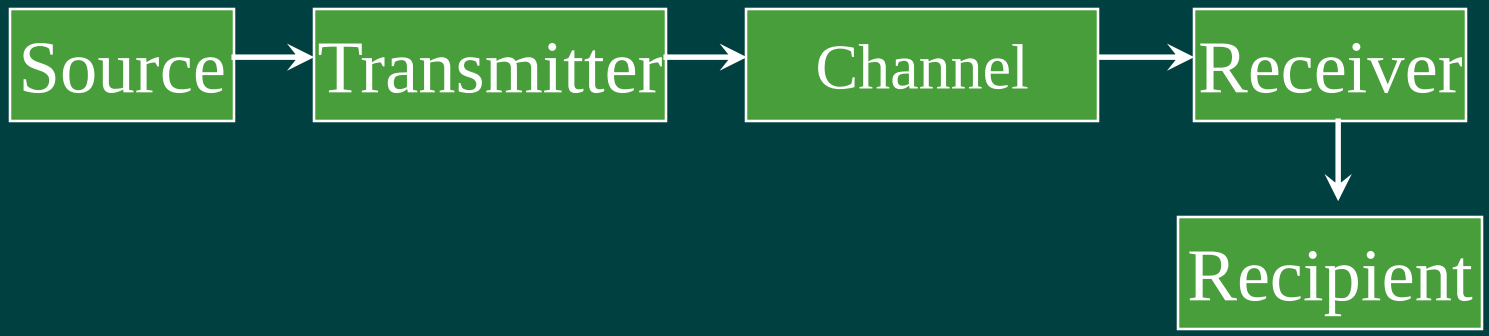
- The merger of previously distinct telephony and information technologies and markets
  - Involves:
    - Moving voice into a data infrastructure
    - Integrating all the voice and data networks inside a user organization into a single data network infrastructure
    - Then extending that into the wireless arena
  - Foundation is packet-based transmission using the Internet Protocol (IP)
  - Increases the function and scope of both the infrastructure and the application base

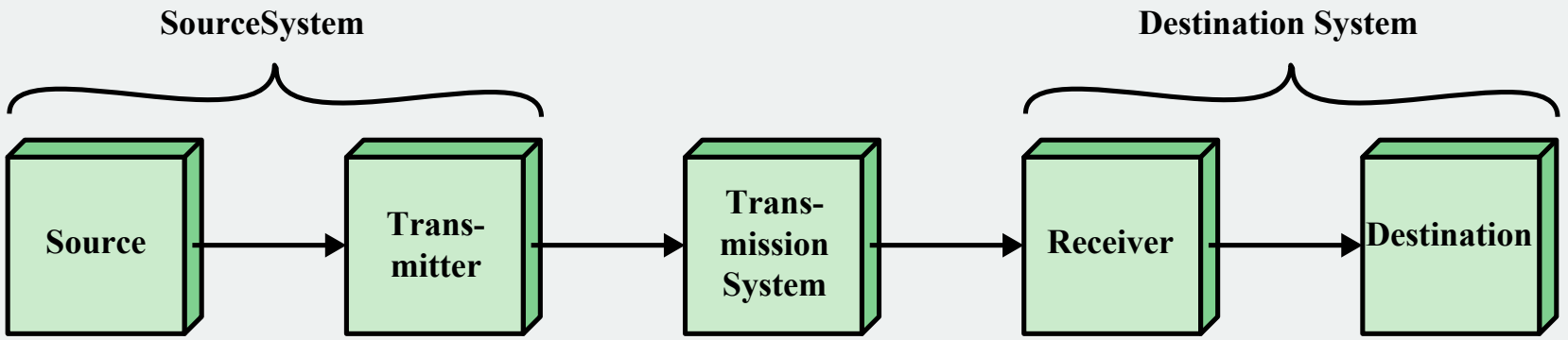
Layers:



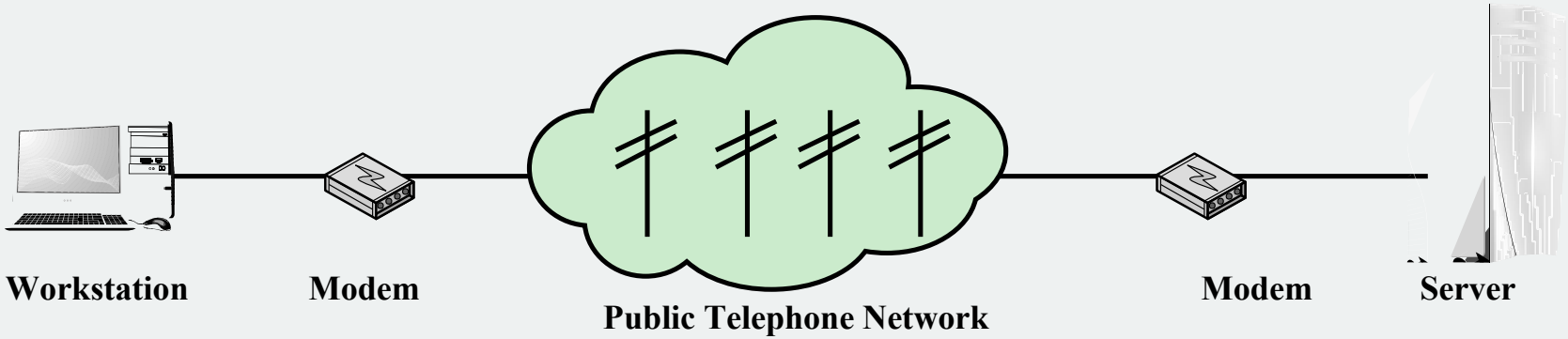
Communication

- Main purpose of communication is to transfer information from a source to a recipient via a channel or medium.
- Basic block diagram of a communication system:





(a) General block diagram



(b) Example

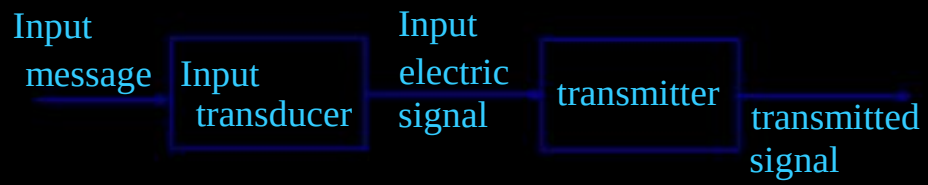
Figure 1.3 Simplified Communications Model

Brief Description

- **Source:** analog or digital
- **Transmitter:** transducer, amplifier, modulator, oscillator, power amp., antenna
- **Channel:** e.g. cable, optical fibre, free space
- **Receiver:** antenna, amplifier, demodulator, oscillator, power amplifier, transducer
- **Recipient:** e.g. person, (loud) speaker, computer

Source

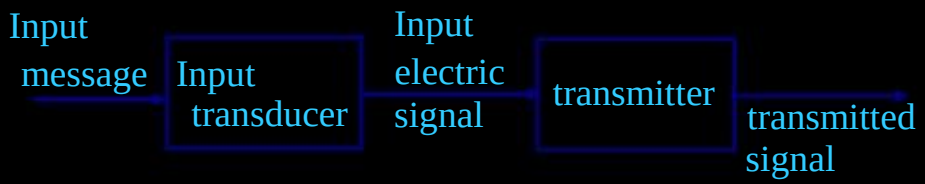
- Appear in many forms: a sequence of discrete symbols or letters, a single time-varying quantity (e.g. the acoustic pressure produced by speech or music, light intensity).



Transmitting Unit

Transmitter

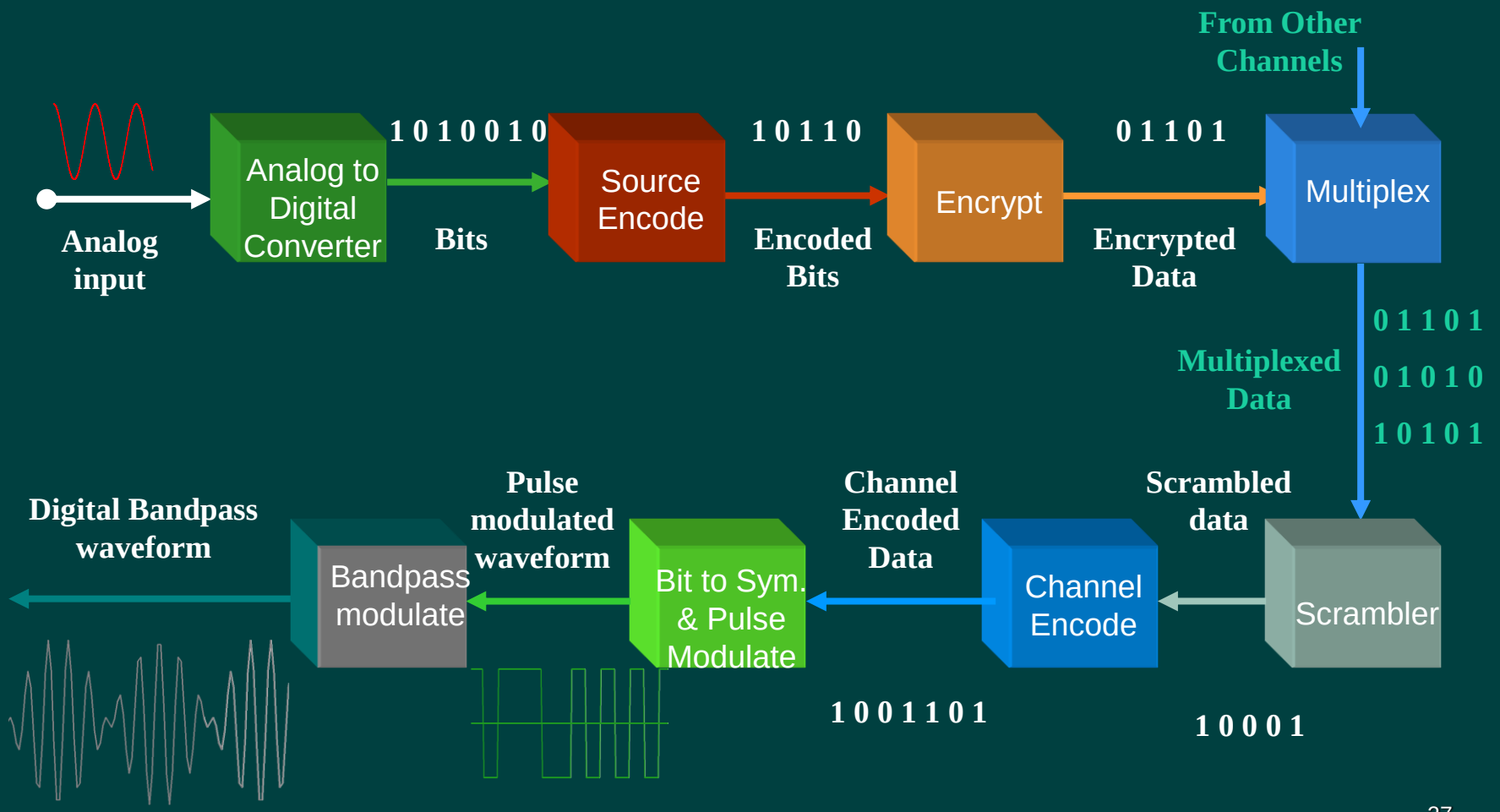
- The transmitter couples the message onto the channel in the form of transmitted signal.



Transmitting Unit

- This is where modulation takes place.

Digital Communication: Transmitter

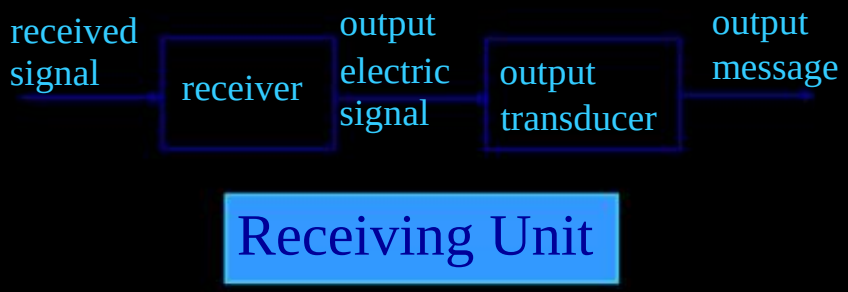


Channel

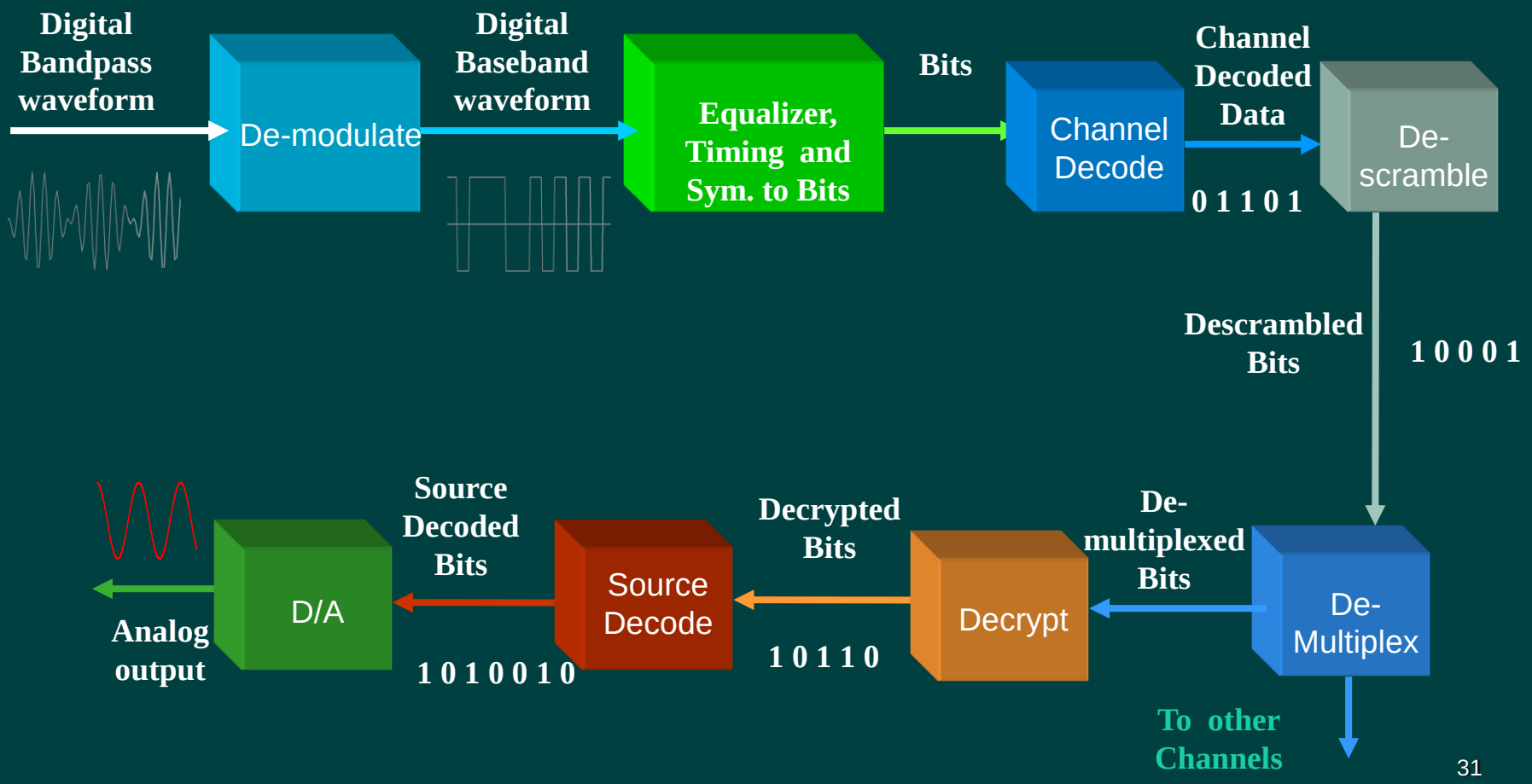
- The electrical medium that bridges the distance from source to destination
  - Hardwire
    - Coaxial cables
    - Fiber optic cables
    - Waveguides
    - Twisted--pair telephone lines
  - Softwire
    - Air
    - Vacuum
    - Sea water

Receiver

- To extract the desired signal from the received signal at the channel output and to convert it to a form suitable for the output transducer
- Main function – to demodulate the received signal (i.e. amplification, decoding, and filtering)



Digital Communication: Receiver



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

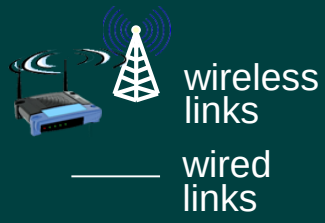
1.5 protocol layers, service models

1.6 networks under attack: security

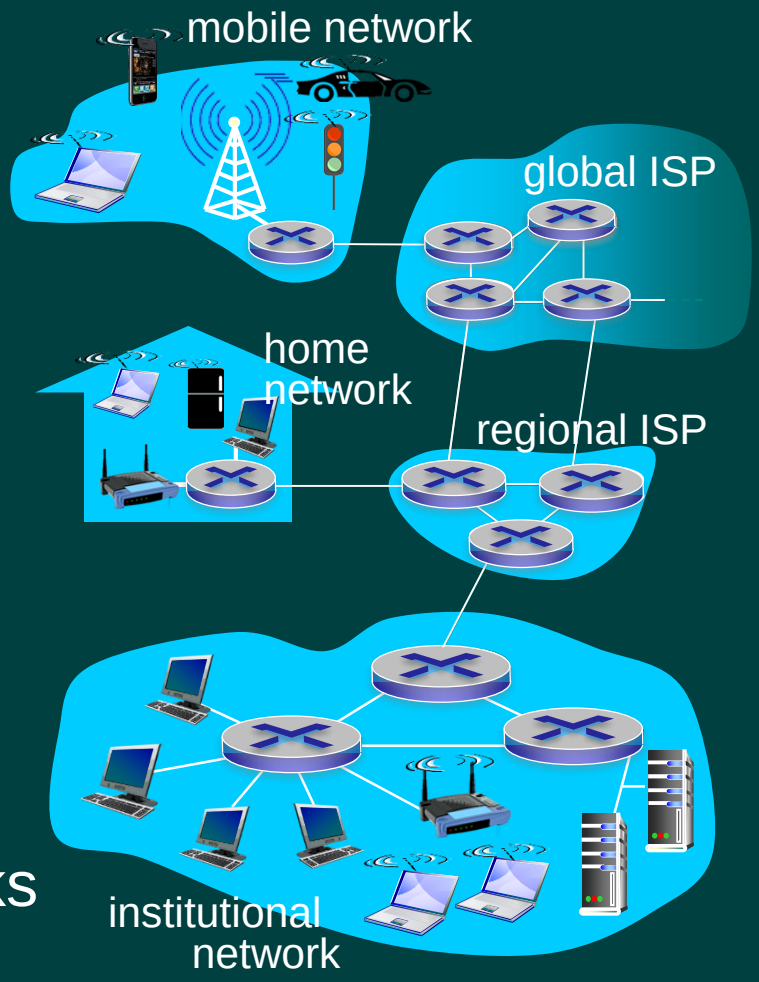
1.7 history

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

- billions of connected computing devices:
  - *hosts* = *end systems*
  - running *network apps*
- *communion links*
  - fiber, copper, radio, satellite
  - transmission rate: *bandwidth*



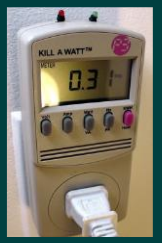
- *packet switches:* forward packets (chunks of data)
  - *routers* and *switches*



“Fun” Internet-connected devices

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

Web-enabled toaster + weather forecaster



Tweet-a-watt: monitor energy use

Slingbox: watch, control cable TV remotely

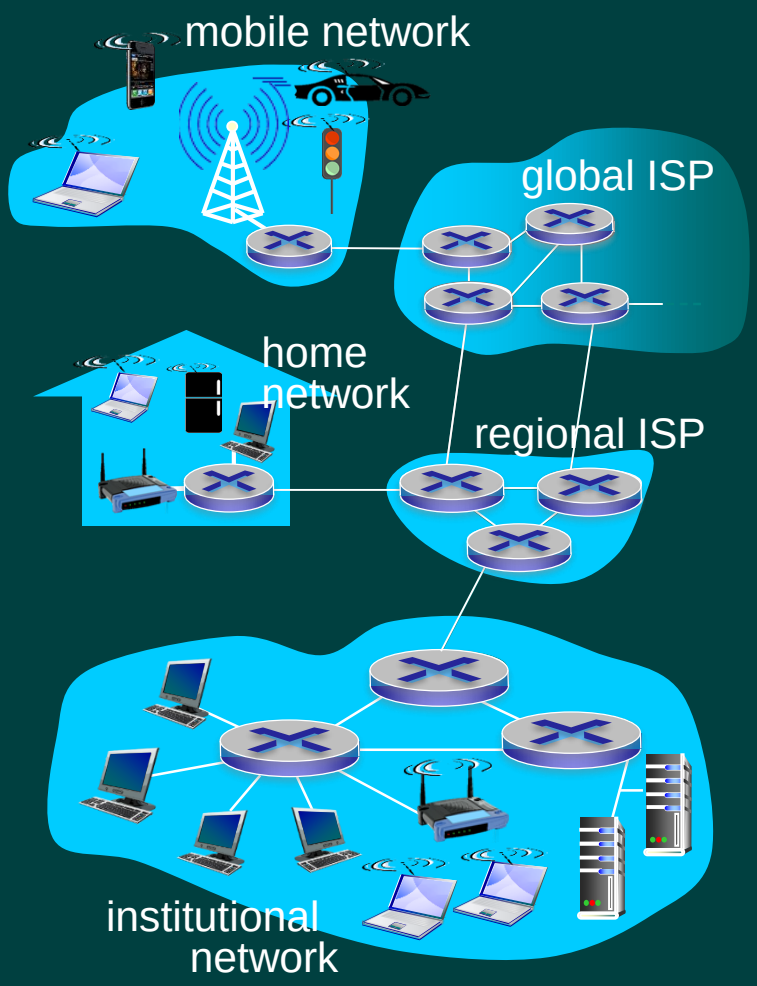
Internet refrigerator

sensorized, bed mattress

Internet phones

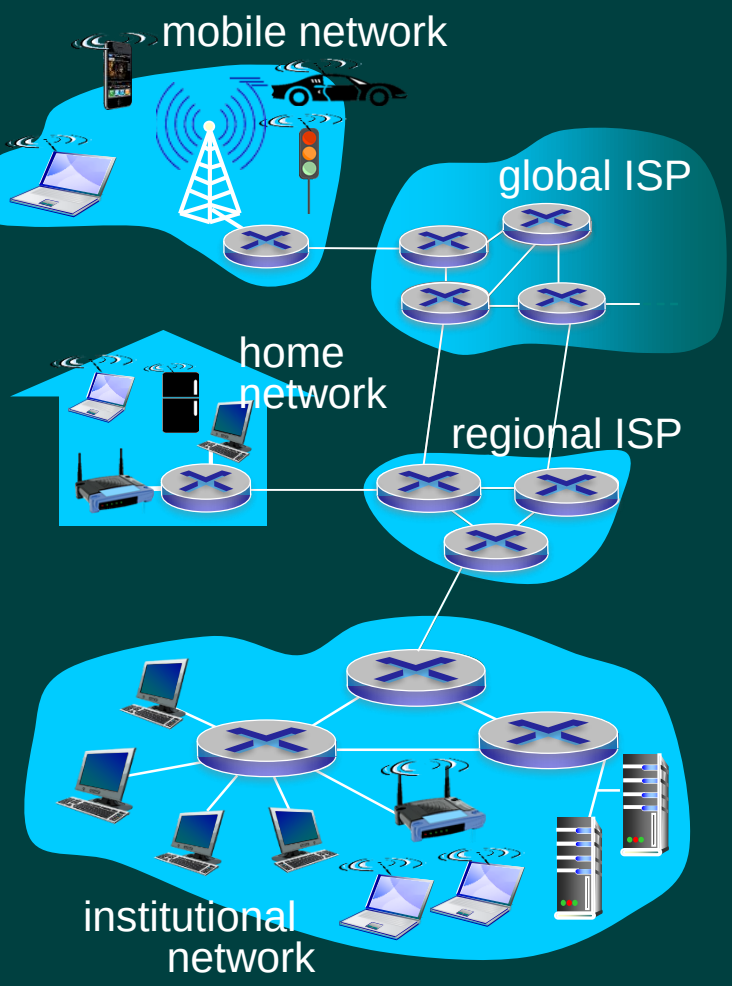
What's the Internet: "nuts and bolts" view

- *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

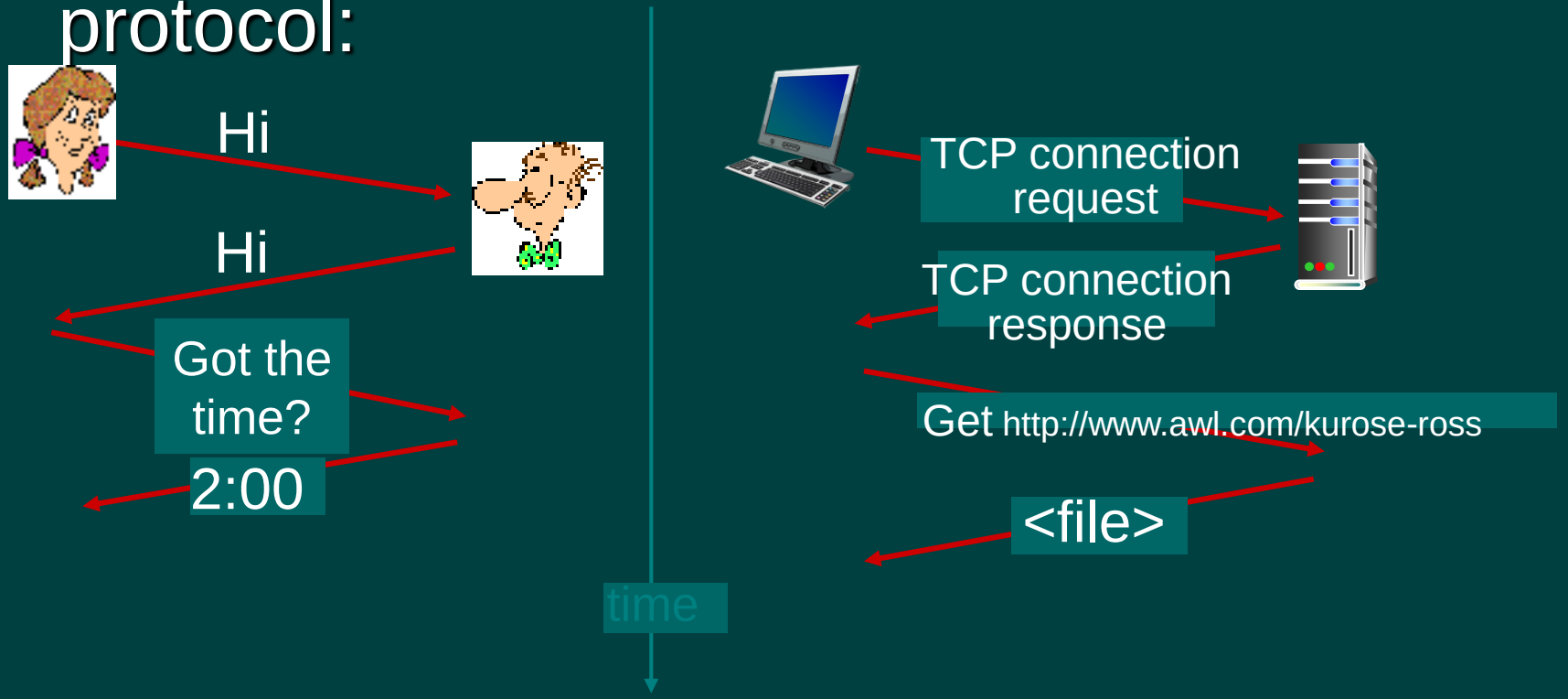
network protocols:

- 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

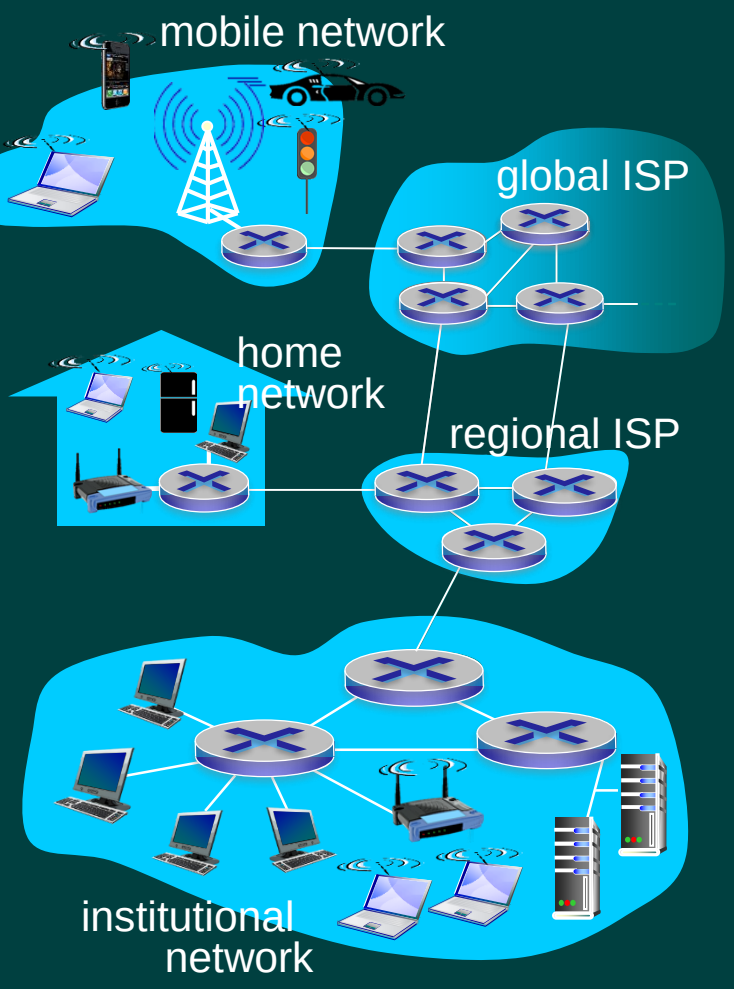
1.5 protocol layers, service models

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



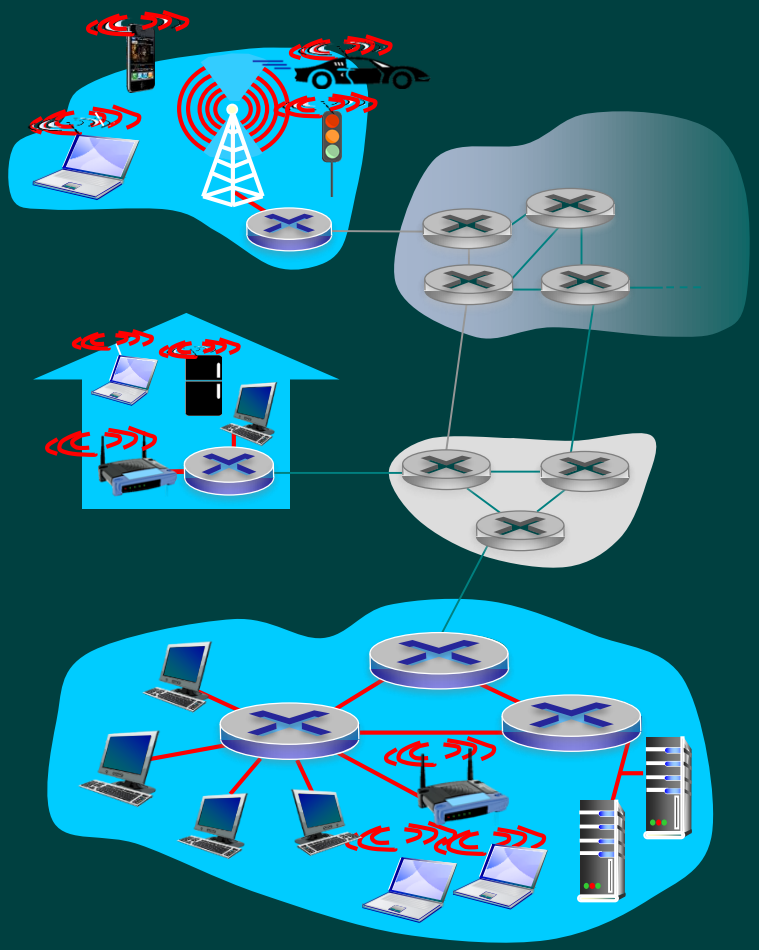
Access networks and physical media

Q: How to connect end systems to edge router?

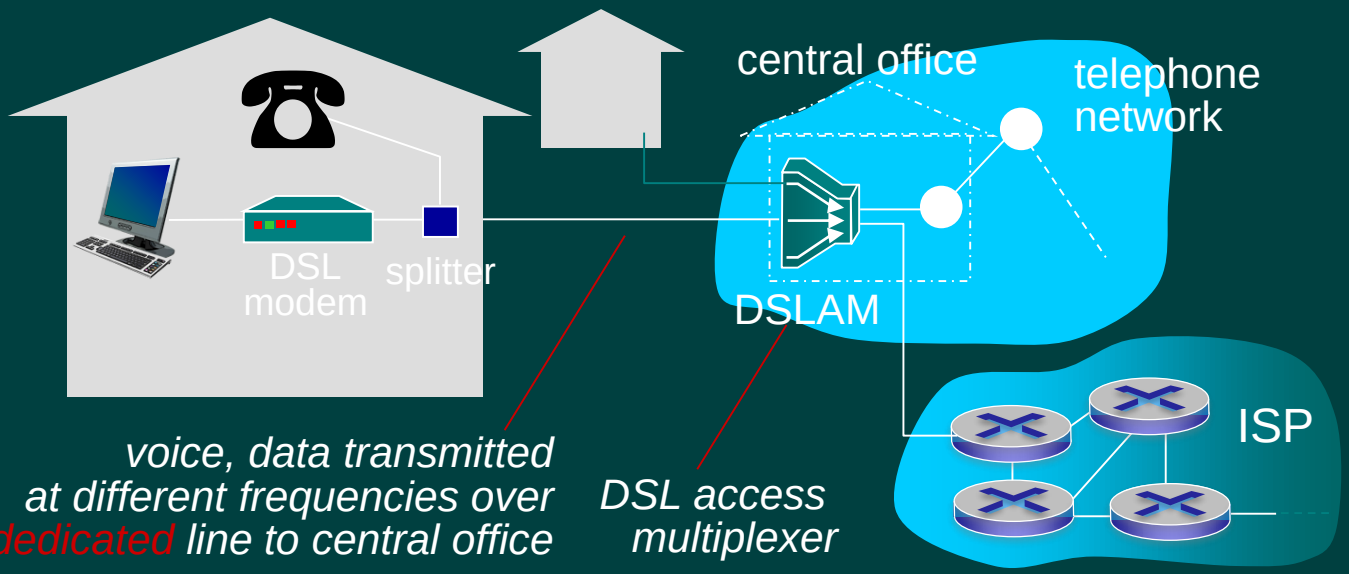
- residential access nets
- institutional access networks (school, company)
- mobile access networks

keep in mind:

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

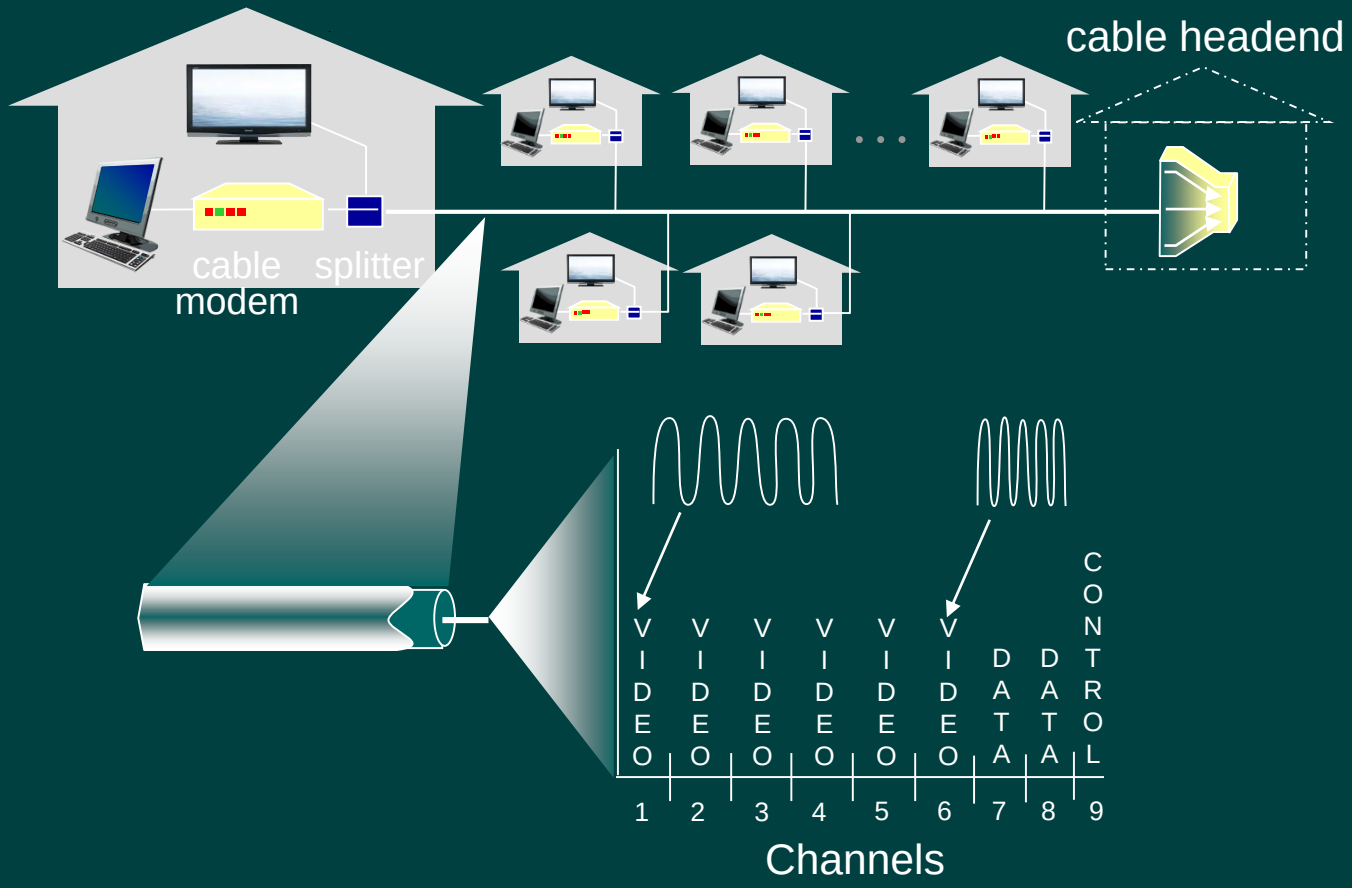


Access network: digital subscriber line (DSL)



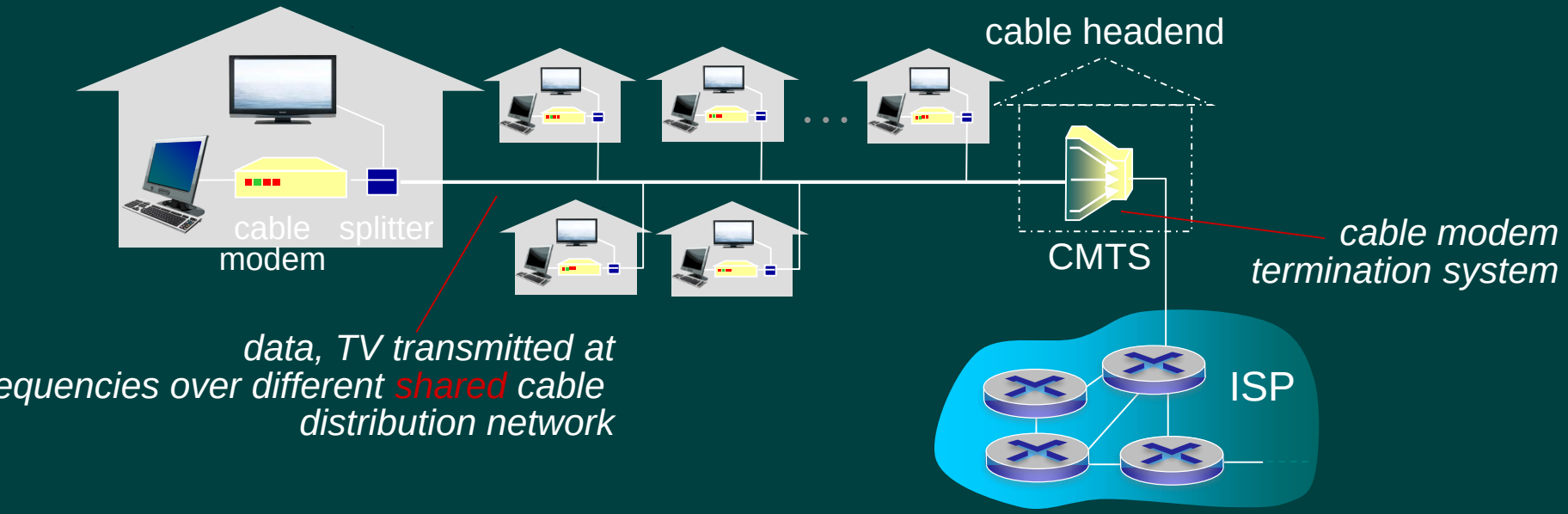
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access network: cable network



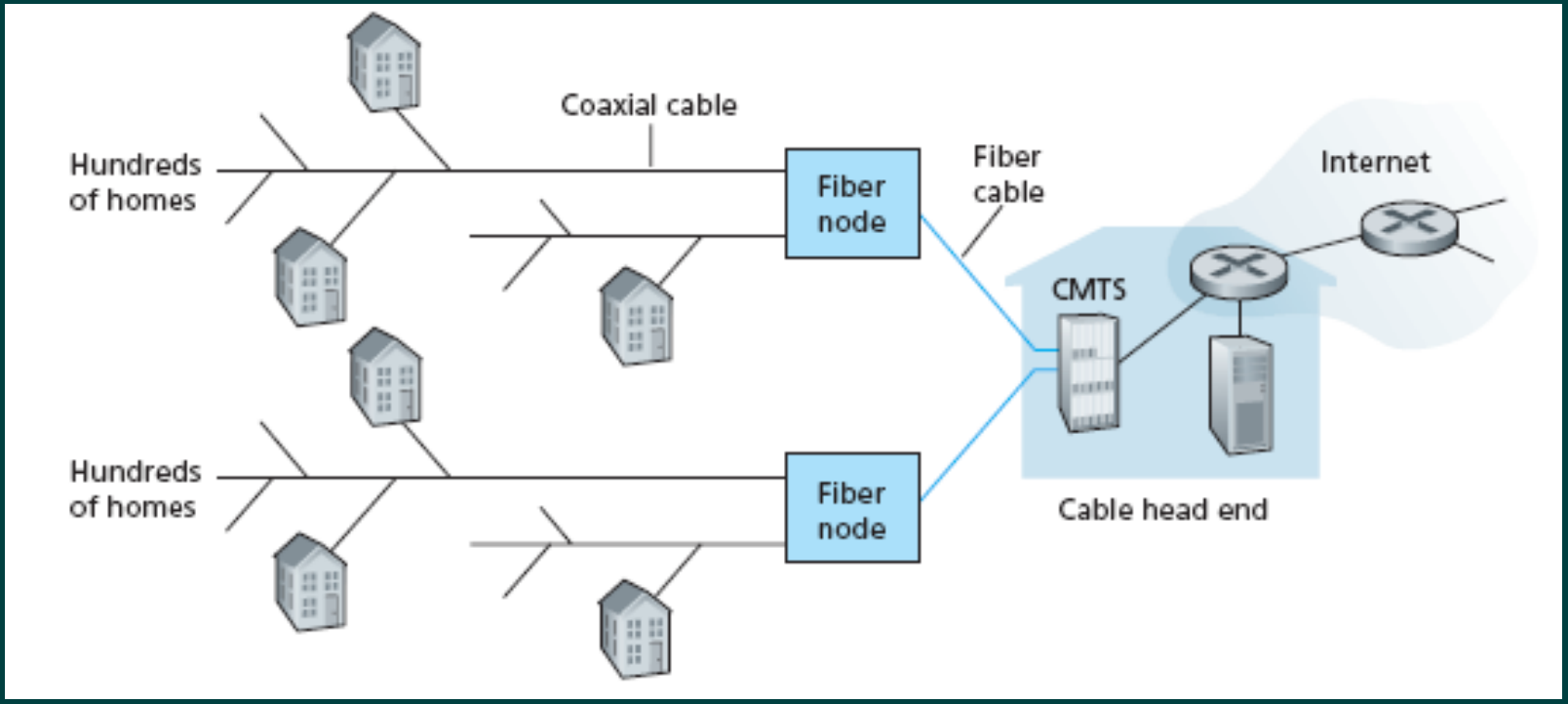
frequency division multiplexing: different channels transmitted in different frequency bands

Access network: cable network



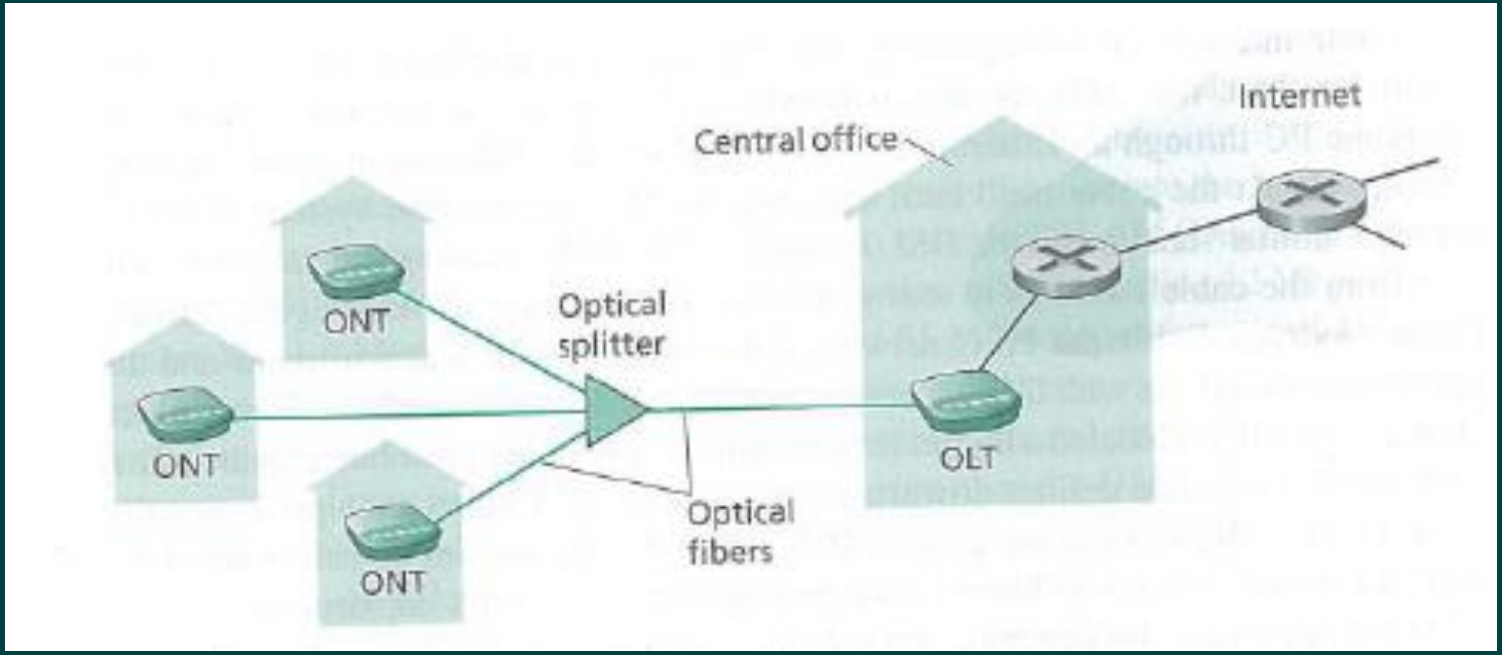
- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

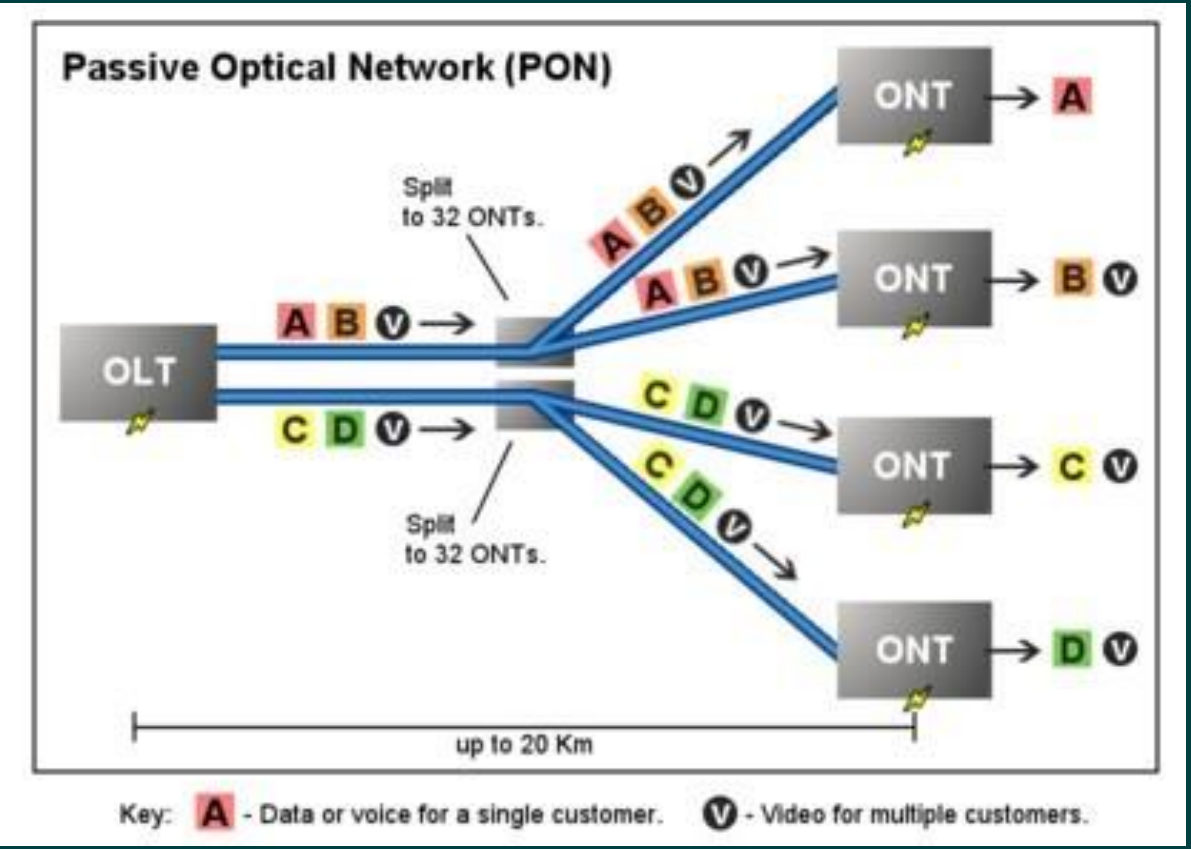
Access network: cable network



Access network: PON (FTTH)

A passive optical network does not include electrically powered switching equipment and instead uses optical splitters to separate and collect optical signals as they move through the network

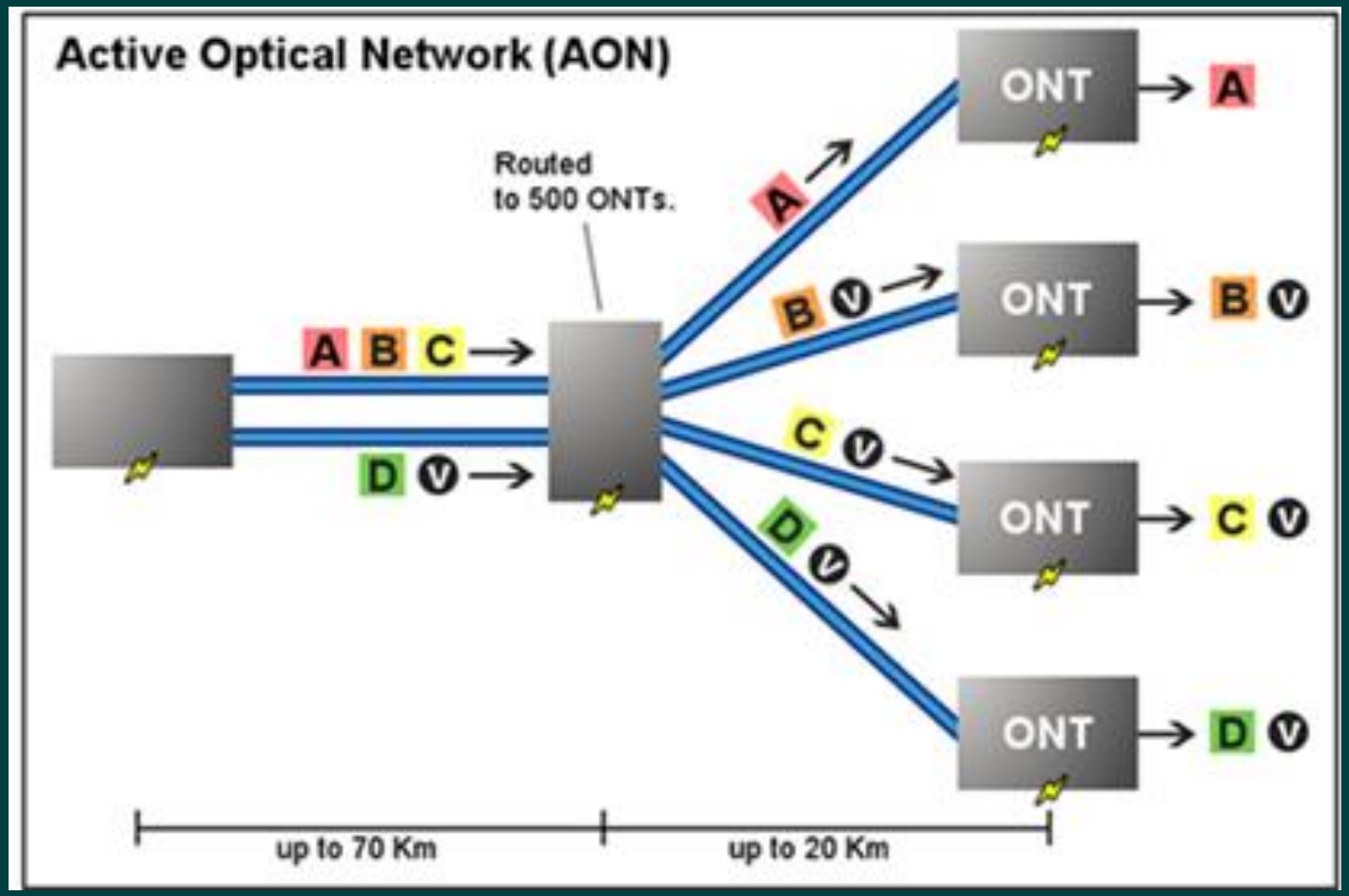



Passive Optical Network (PON)
OLT
Split
to 32 ONTs.
Split
to 32 ONTs.
ONT
ONT
ONT
ONT
A
B V
C V
D V
up to 20 Km
Key: A - Data or voice for a single customer. V - Video for multiple customers.

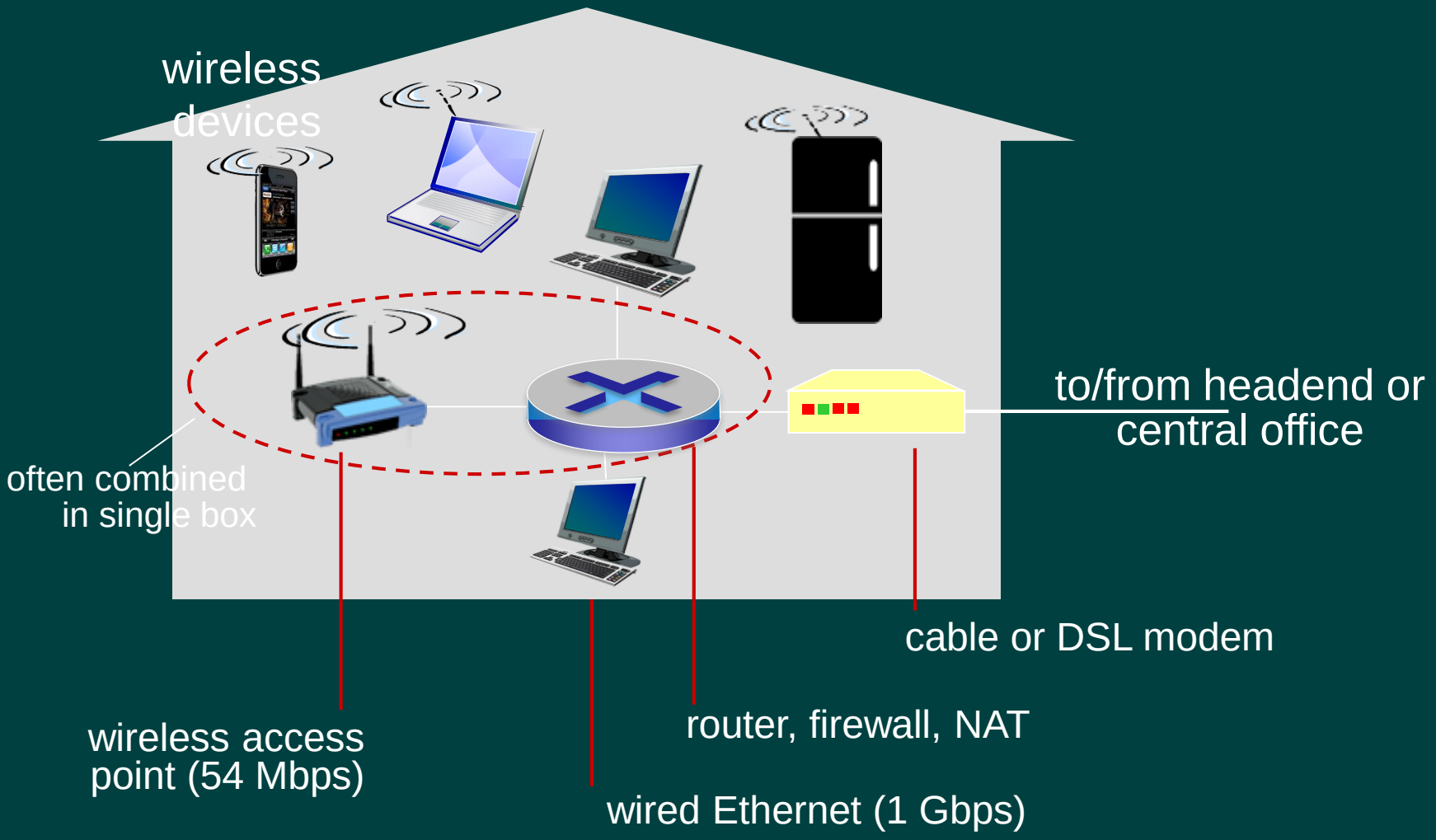
Access network: AON (FTTH)

- An active optical system uses electrically powered switching equipment, such as a router or a switch aggregator, to manage signal distribution and direct signals to specific customers. This switch opens and closes in various ways to direct the incoming and outgoing signals to the proper place.

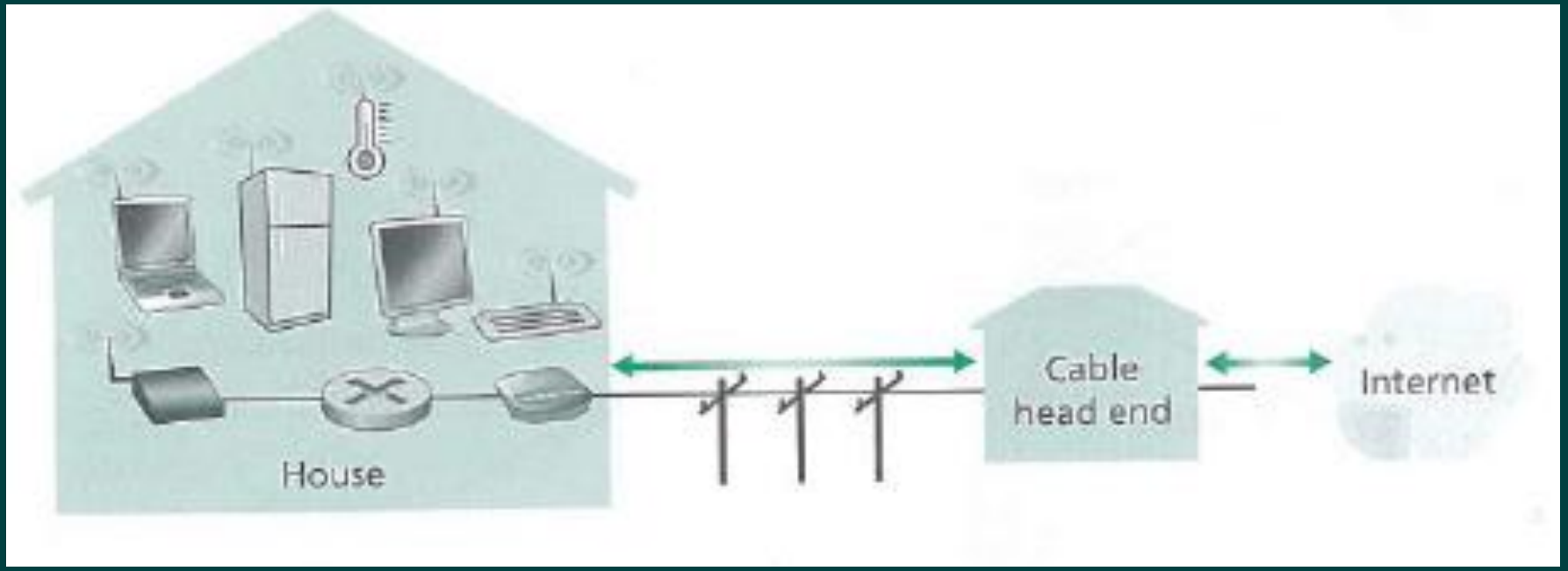
Access network: AON (FTTH)



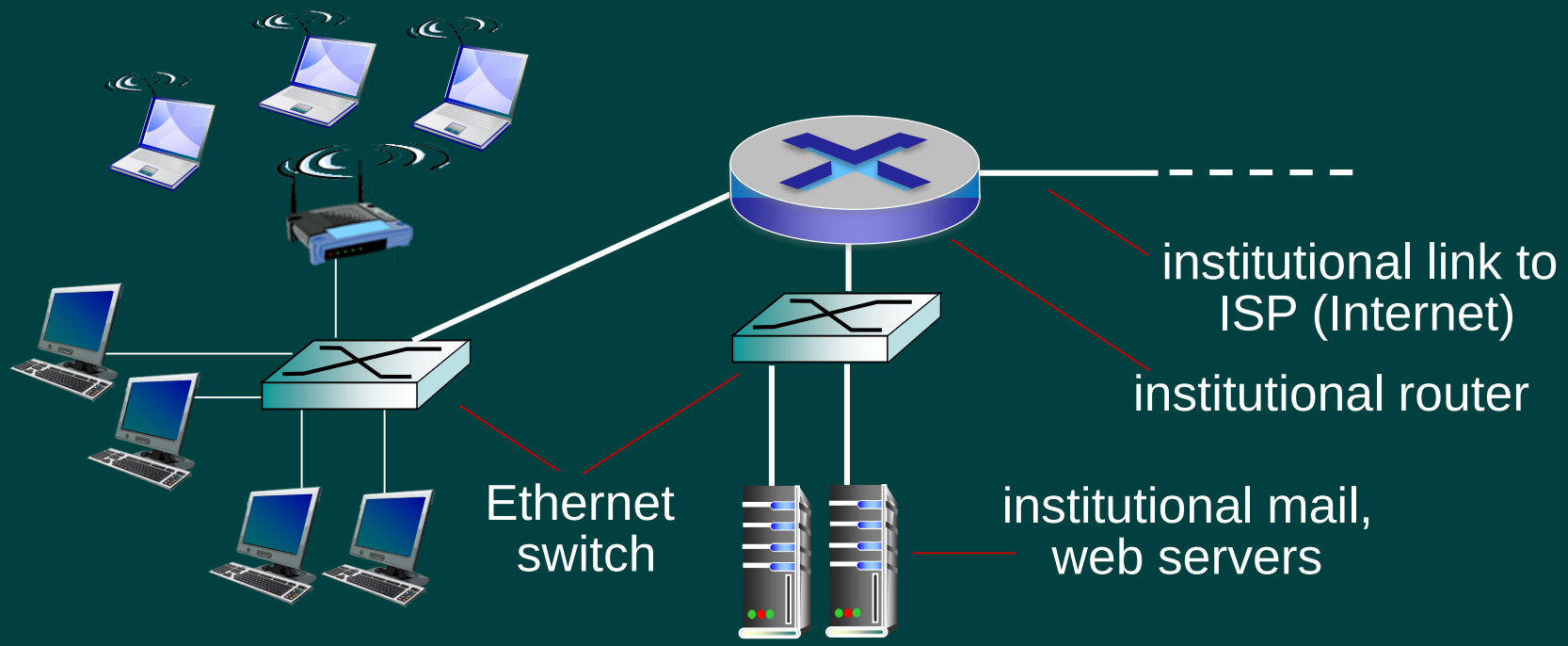
Access network: home network



Access network: home network

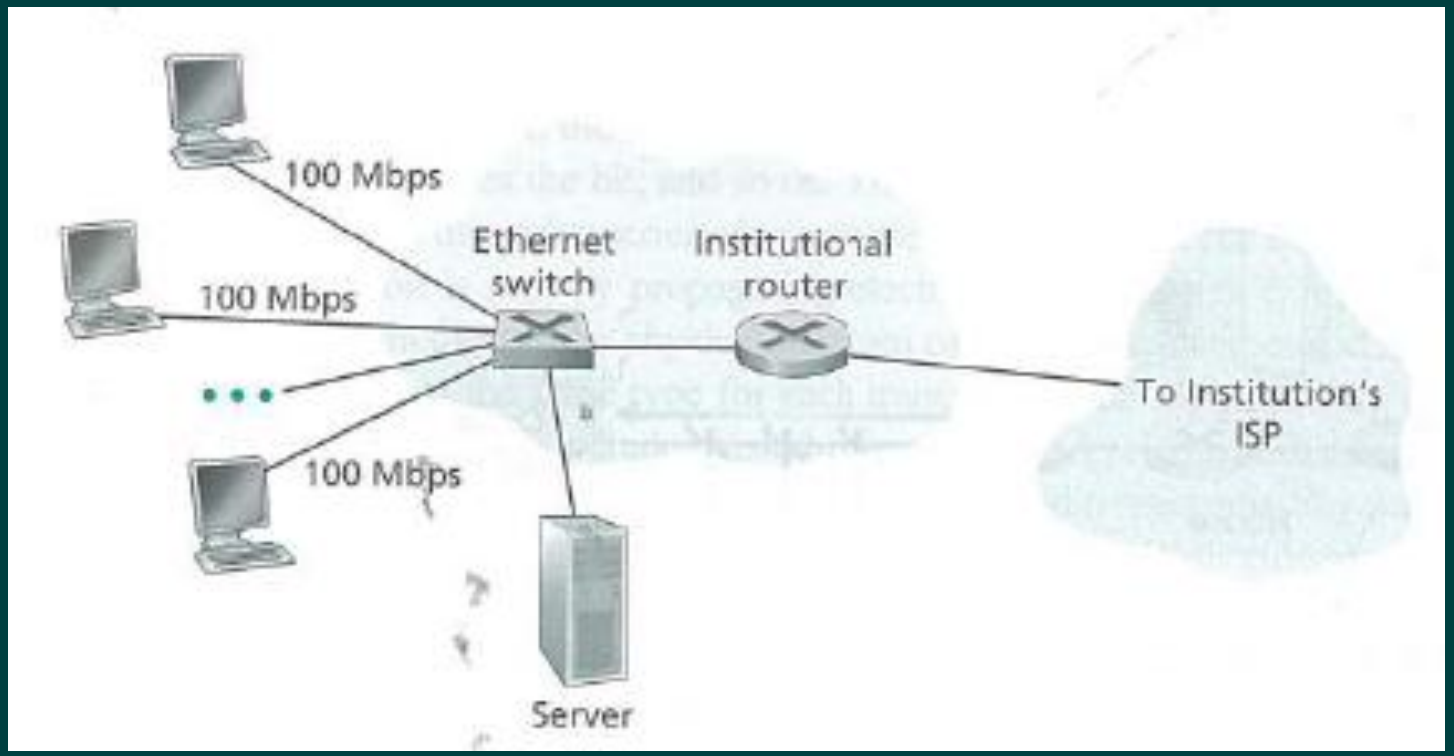


Enterprise access networks (Ethernet)



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

Enterprise access networks (Ethernet)



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

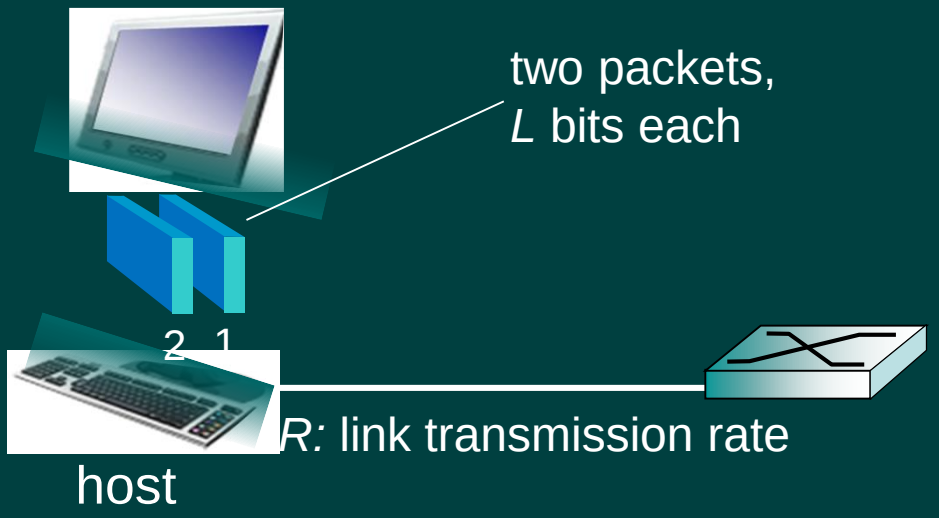
wide-area wireless access

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

Host: sends *packets* of data

host sending function:

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



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

Physical media

- bit: propagates between transmitter/receiver pairs
- physical link: what lies between transmitter & receiver
- guided media:
  - signals propagate in solid media: copper, fiber, coax
- unguided media:
  - signals propagate freely, e.g., radio

twisted pair (TP)

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

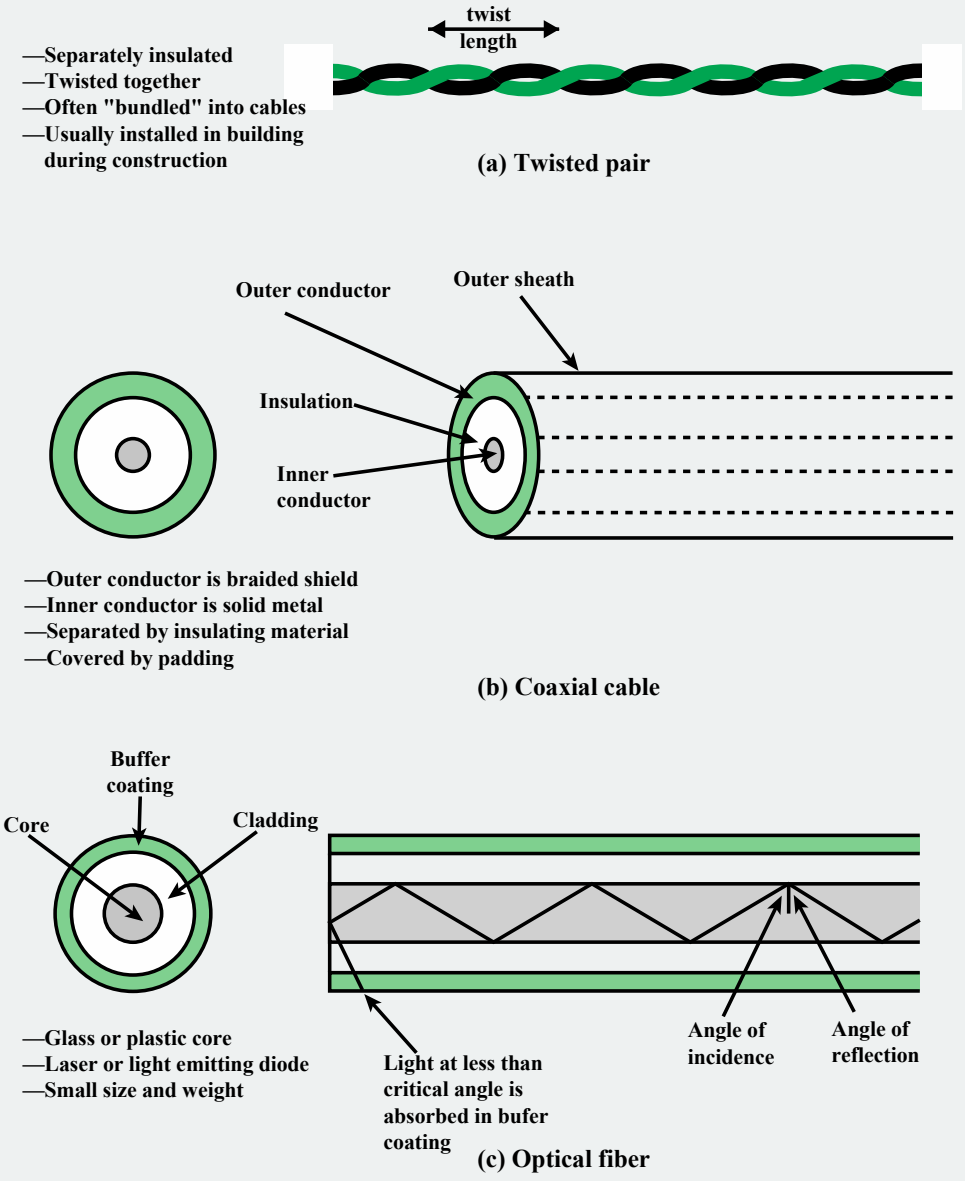
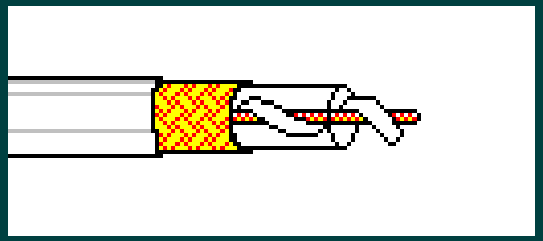


Figure 4.2 Guided Transmission Media

Physical media: coax, fiber

coaxial cable:

- two concentric copper conductors
- bidirectional
- broadband:
  - multiple channels on cable
  - HFC



fiber optic cable:

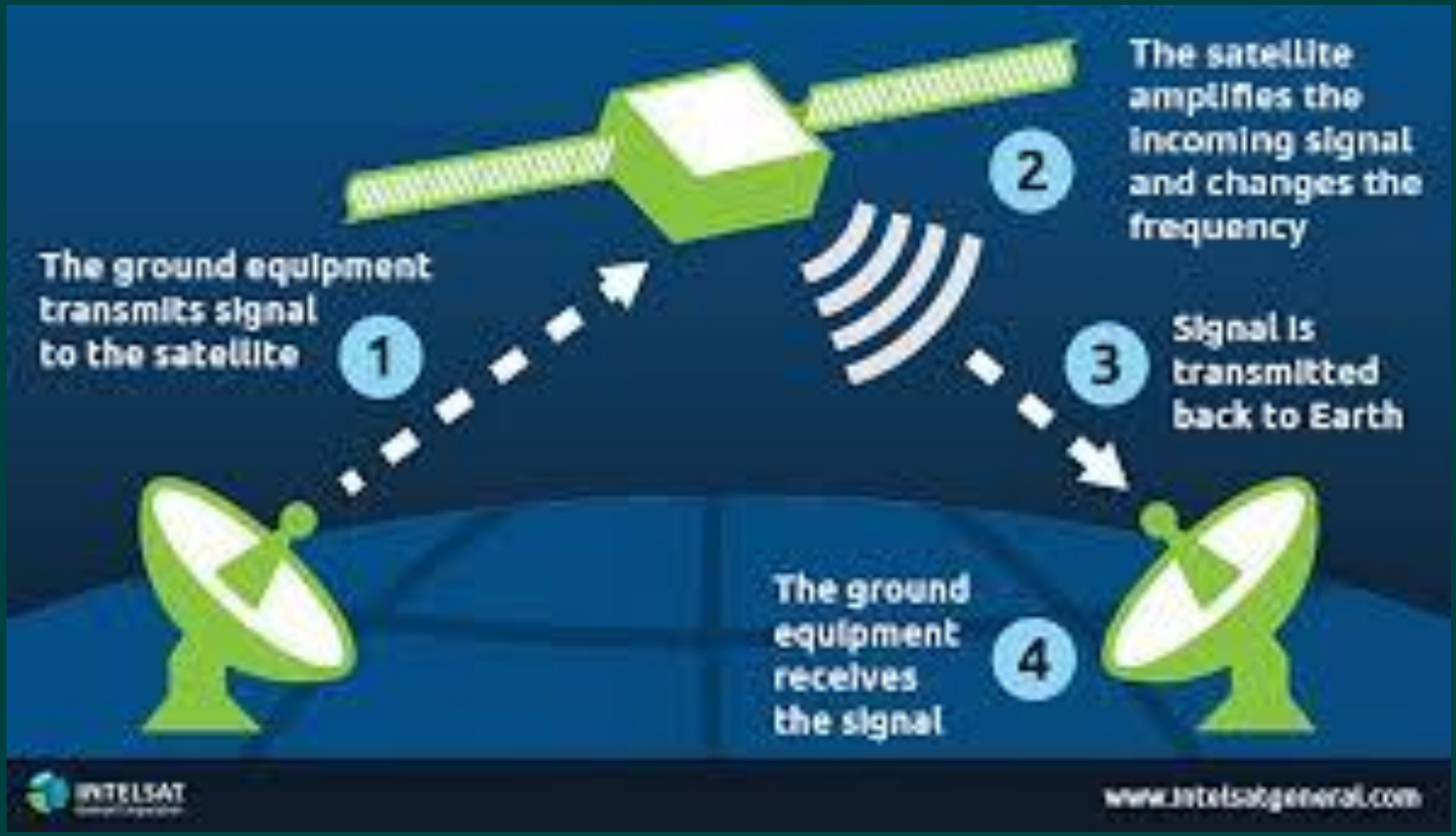
- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10's-100's Gbps transmission rate)
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise

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


The satellite amplifies the incoming signal and changes the frequency
2
The ground equipment transmits signal to the satellite
1
3
Signal is transmitted back to Earth
The ground equipment receives the signal
4
INTELSAT
www.intelsatgeneral.com

Terrestrial Radio Channels

Radio channels carry signals in the electromagnetic spectrum. They are an attractive medium because they require no physical wire to be installed, can penetrate walls, provide connectivity to a mobile user, and can potentially carry a signal for long distances.

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

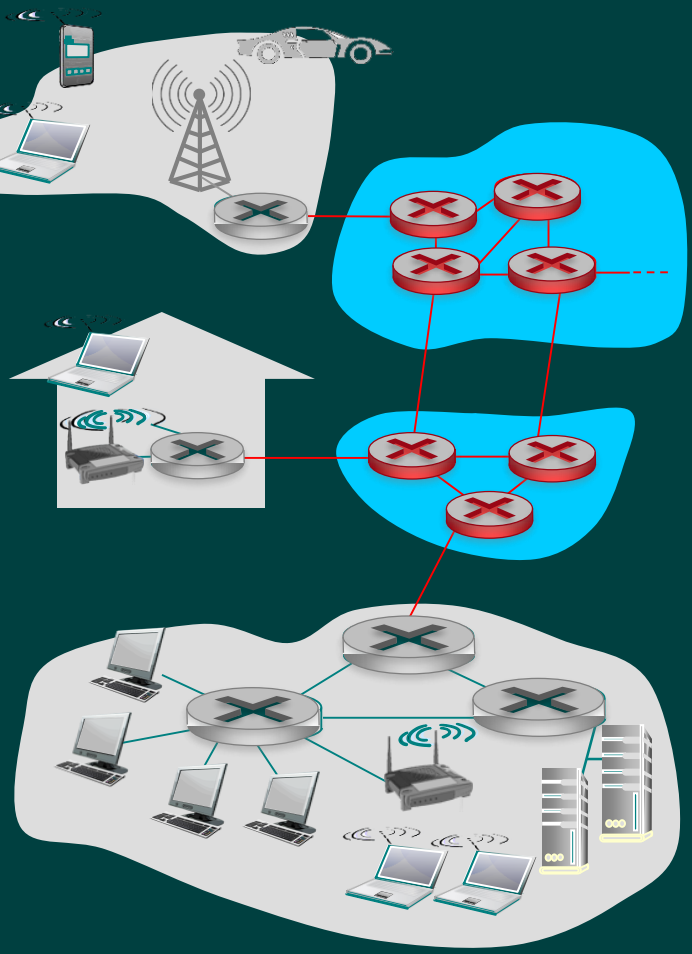
1.5 protocol layers, service models

1.6 networks under attack: security

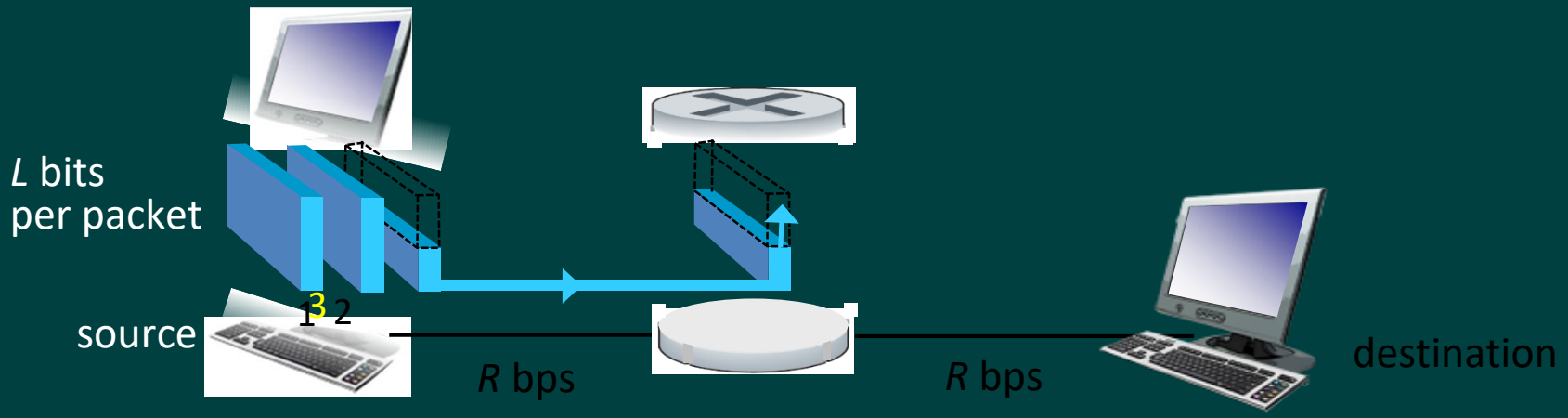
1.7 history

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

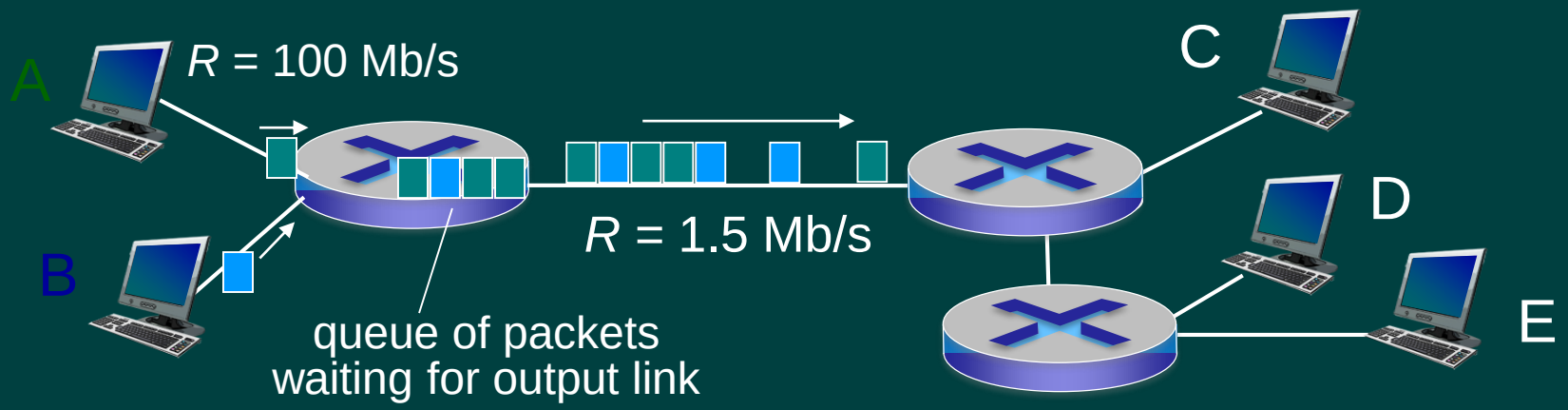
one-hop numerical example:

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

- end-end delay = 2*L*/*R* (assuming zero propagation delay)

} more on delay shortly …

Packet Switching: queueing delay, loss



queuing and loss:

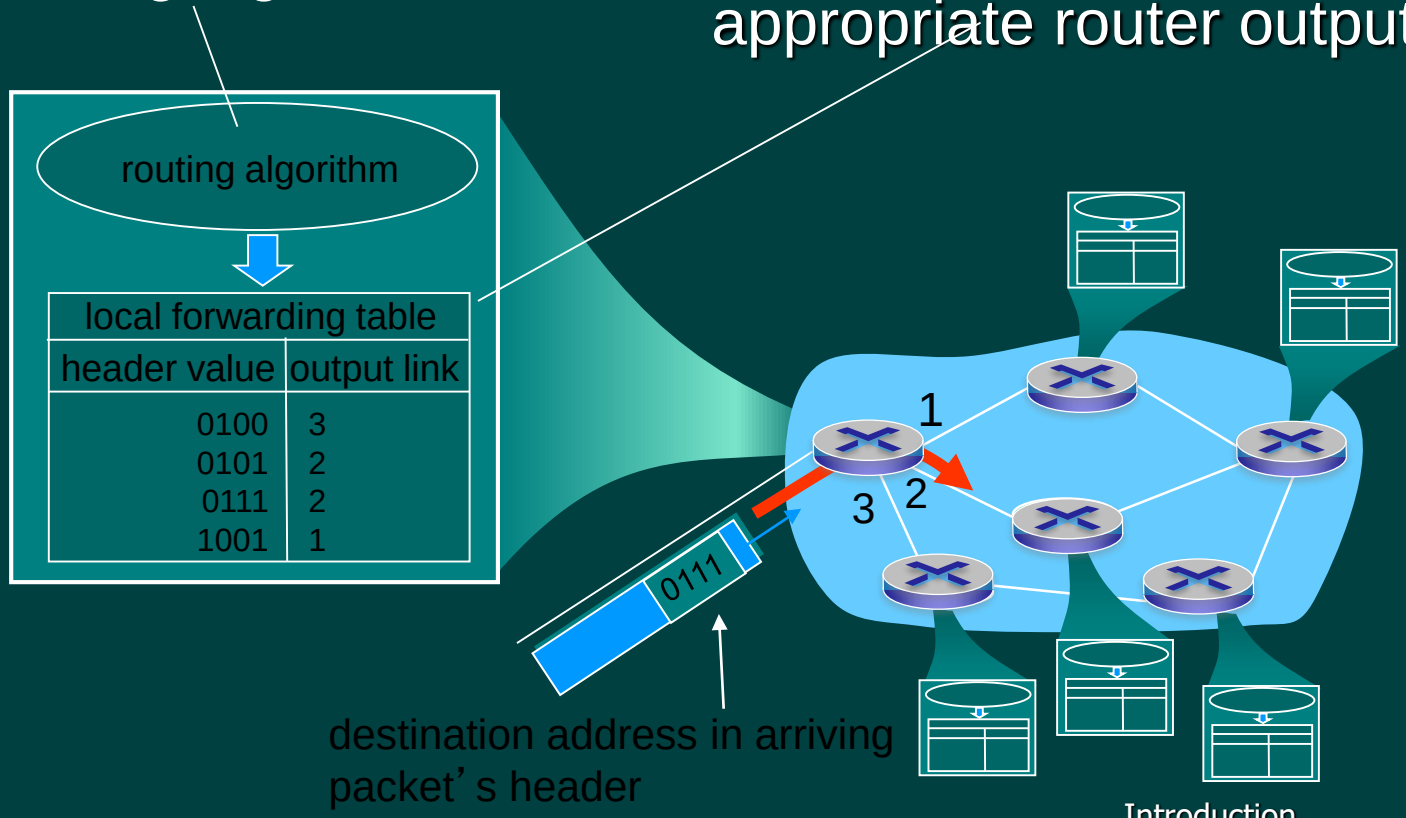
- if arrival rate (in bits) to link exceeds transmission rate of link for a period of time:
  - packets will queue, wait to be transmitted on link
  - packets can be dropped (lost) if memory (buffer) fills up

Two key network-core functions

routing: determines source-destination route taken by packets

- *routing algorithms*

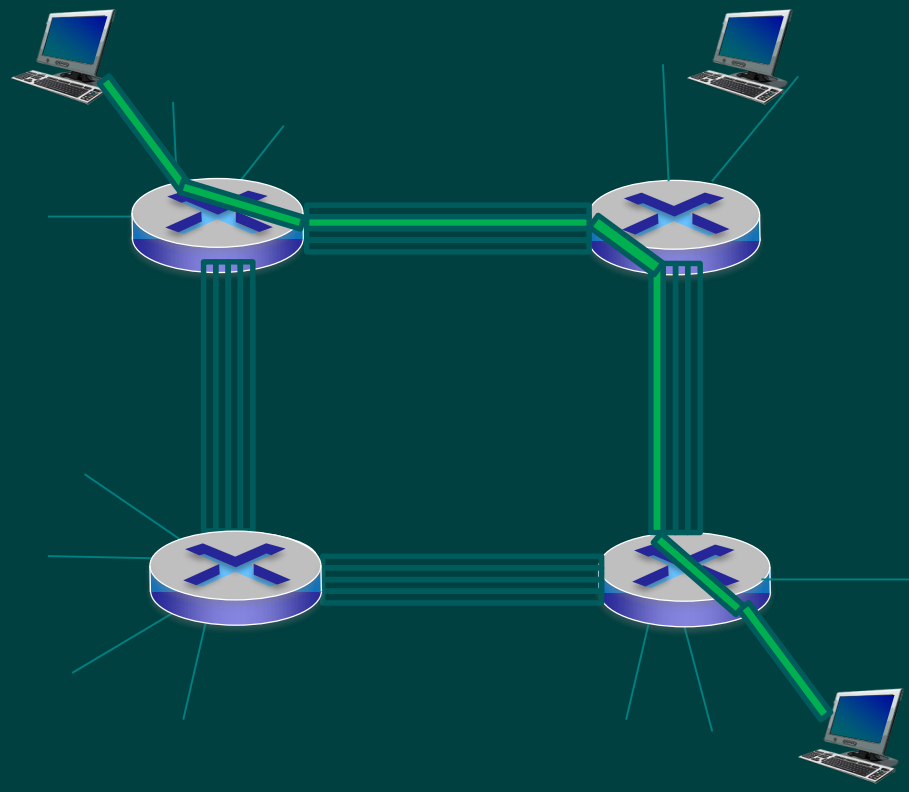
forwarding: move packets from router's input to appropriate router output



Alternative core: circuit switching

end-to-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

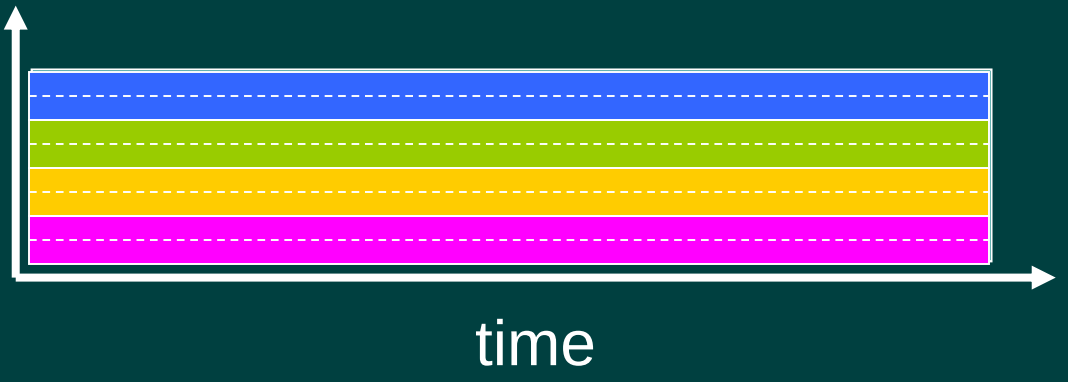


Circuit switching: FDM versus TDM

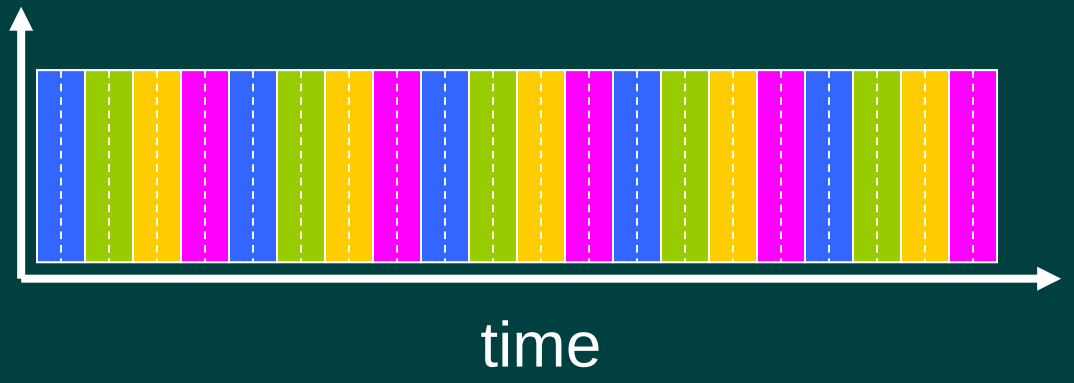
Example:

4 users

FDM



TDM

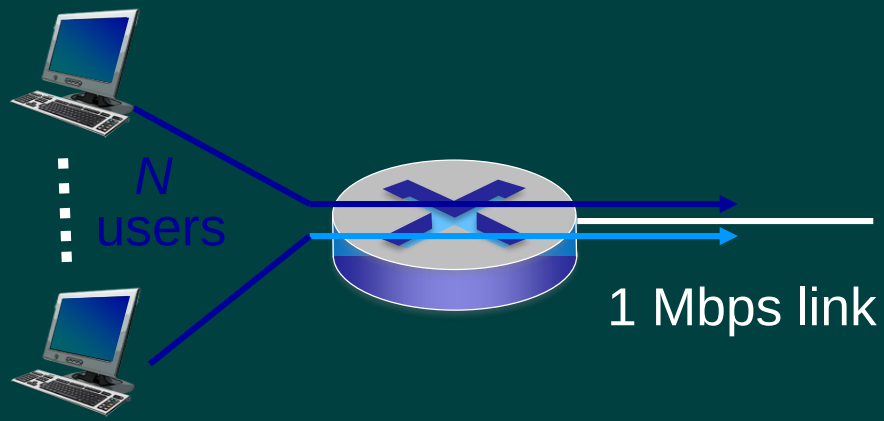


Packet switching versus circuit switching

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)

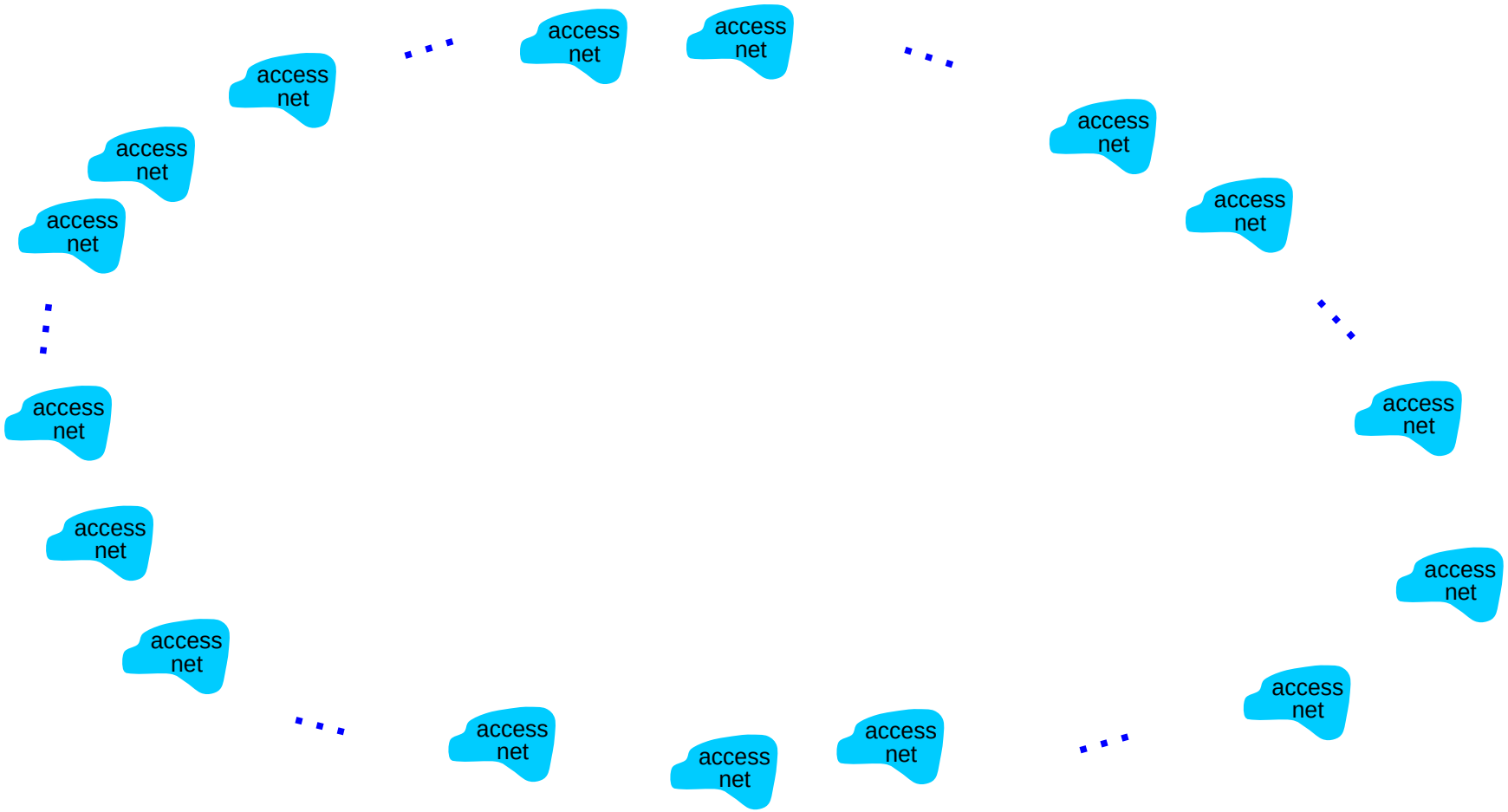
Q: human analogies of reserved resources (circuit switching) versus on-demand allocation (packet-switching)?

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

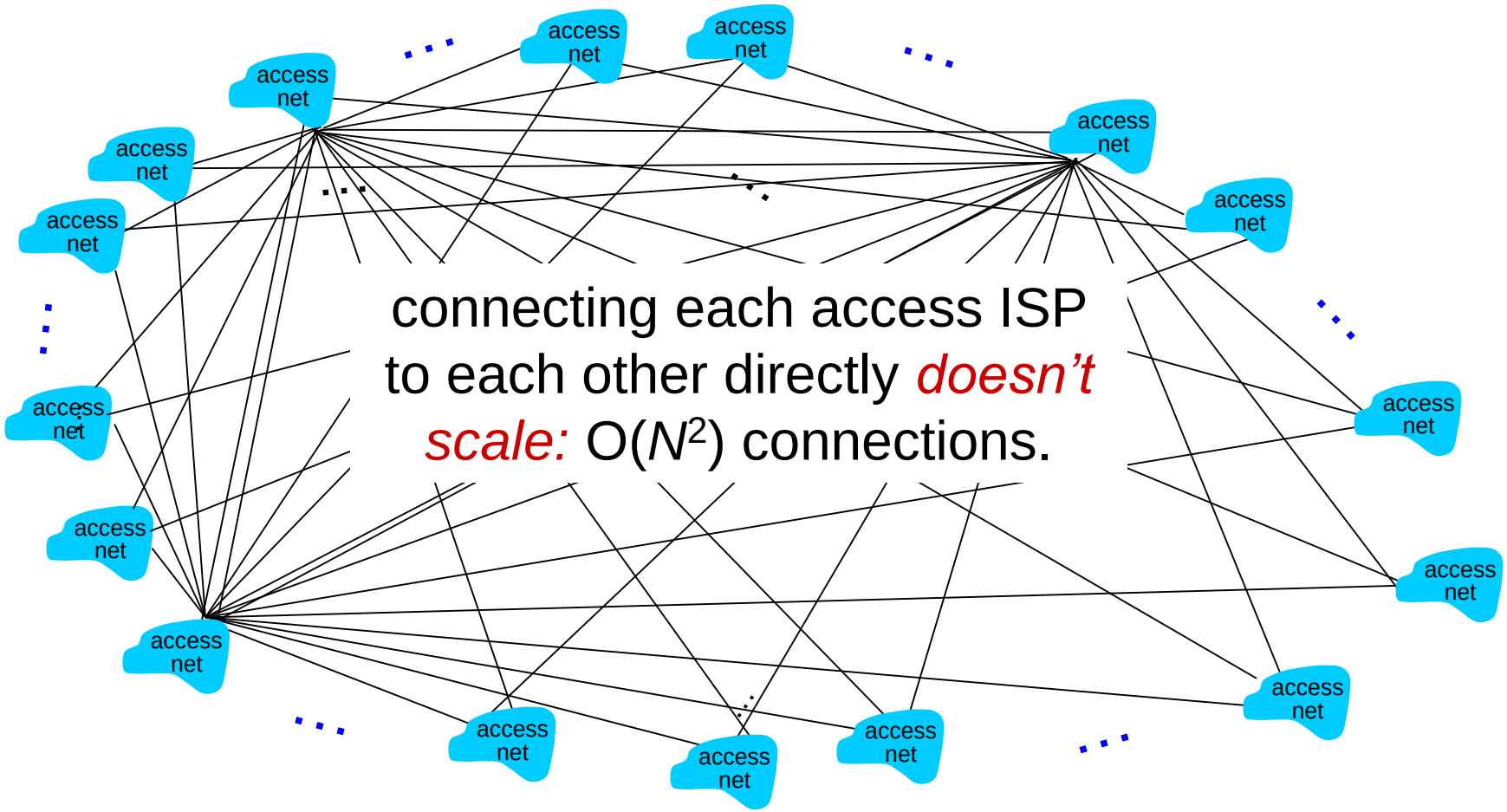
Internet structure: network of networks

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



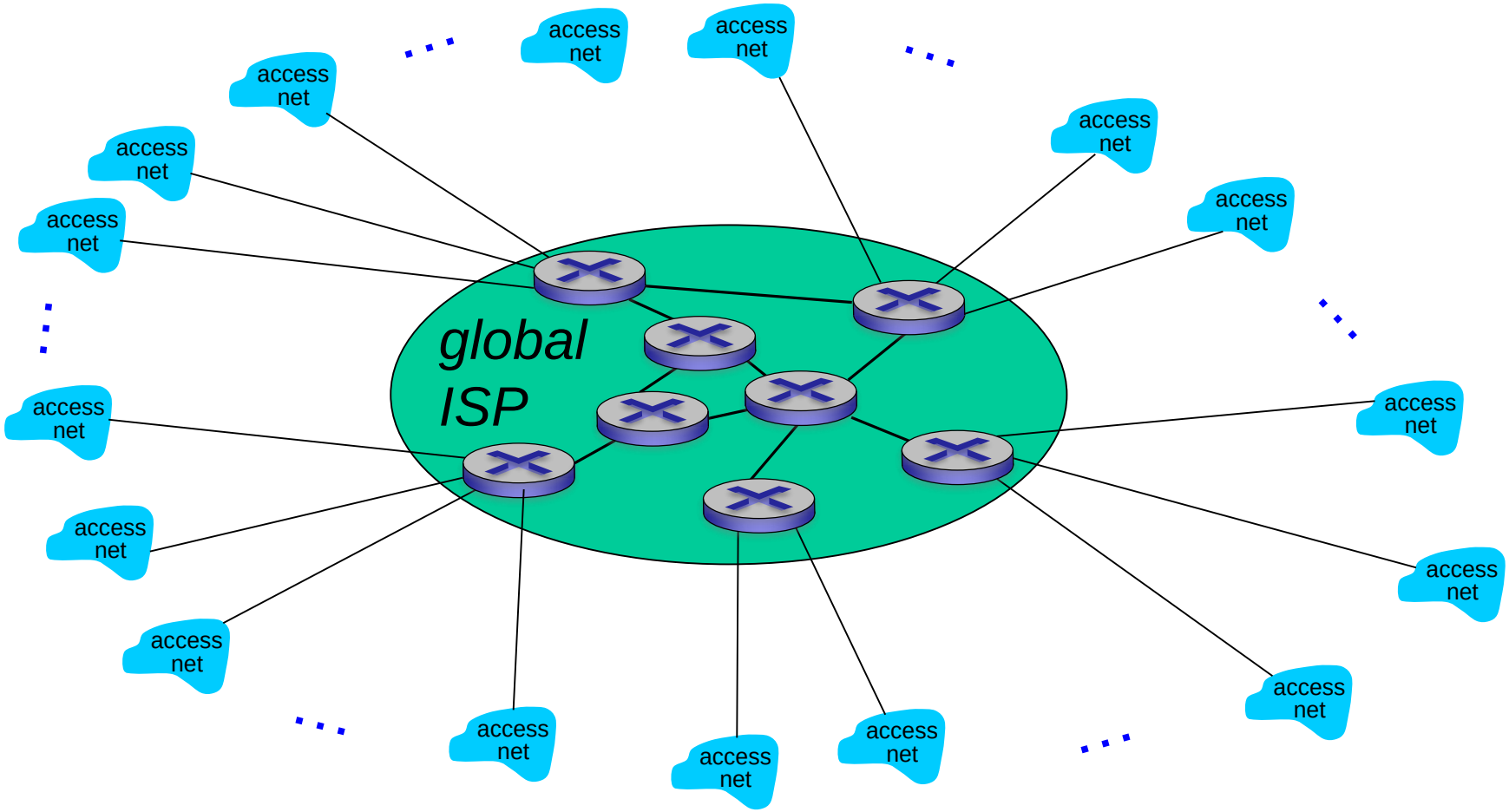
Internet structure: network of networks

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



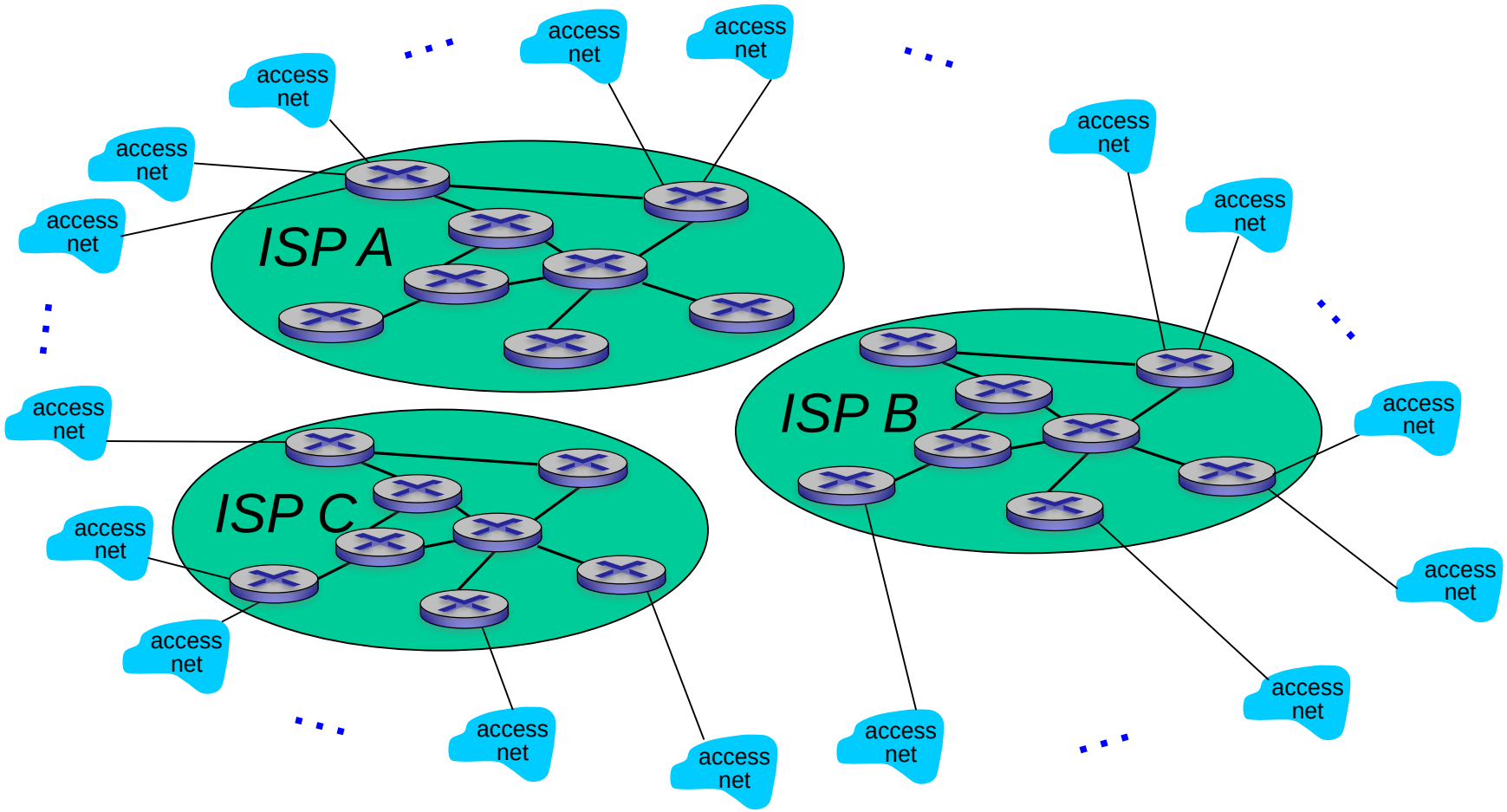
Internet structure: network of networks

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



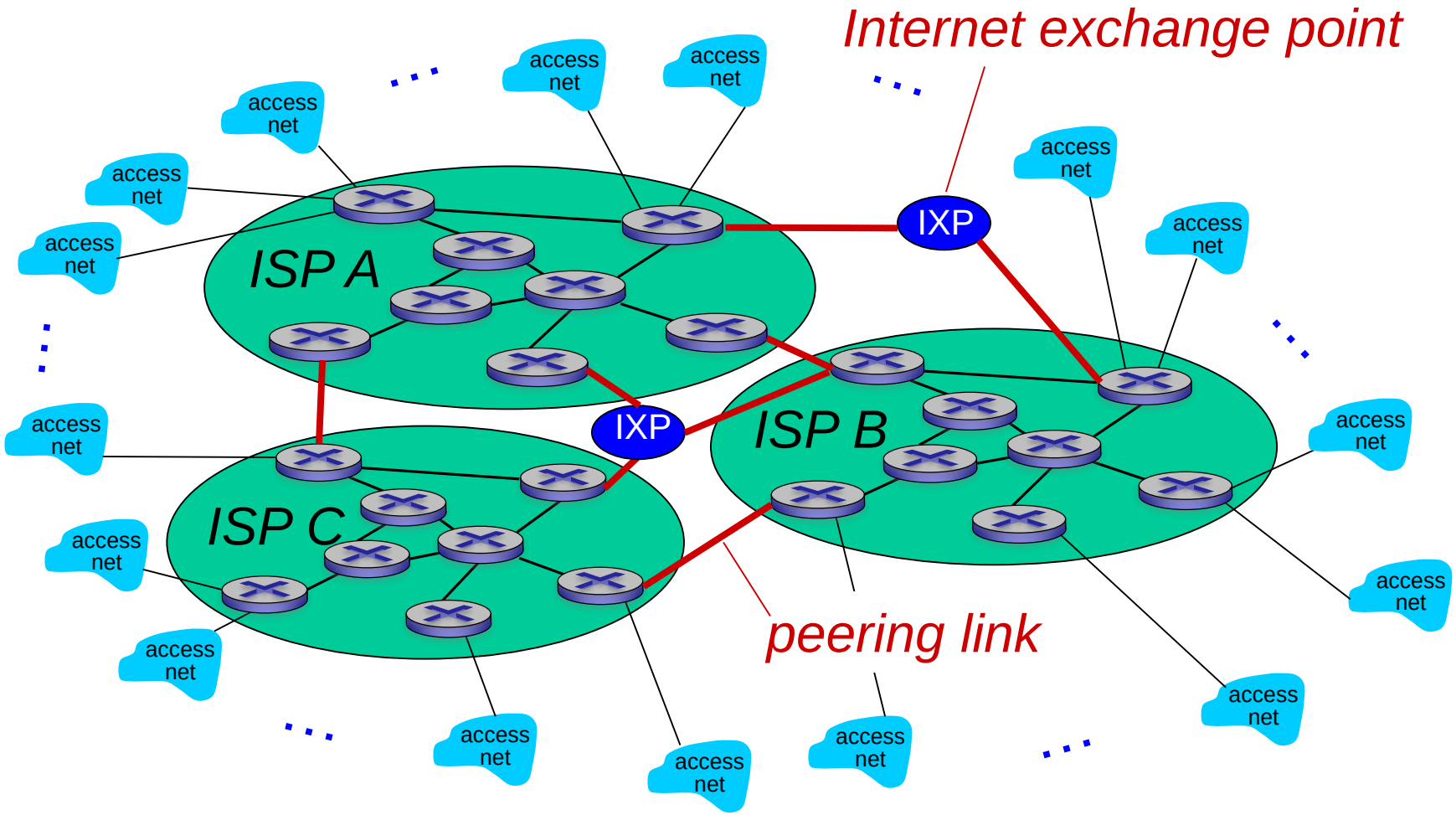
Internet structure: network of networks

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



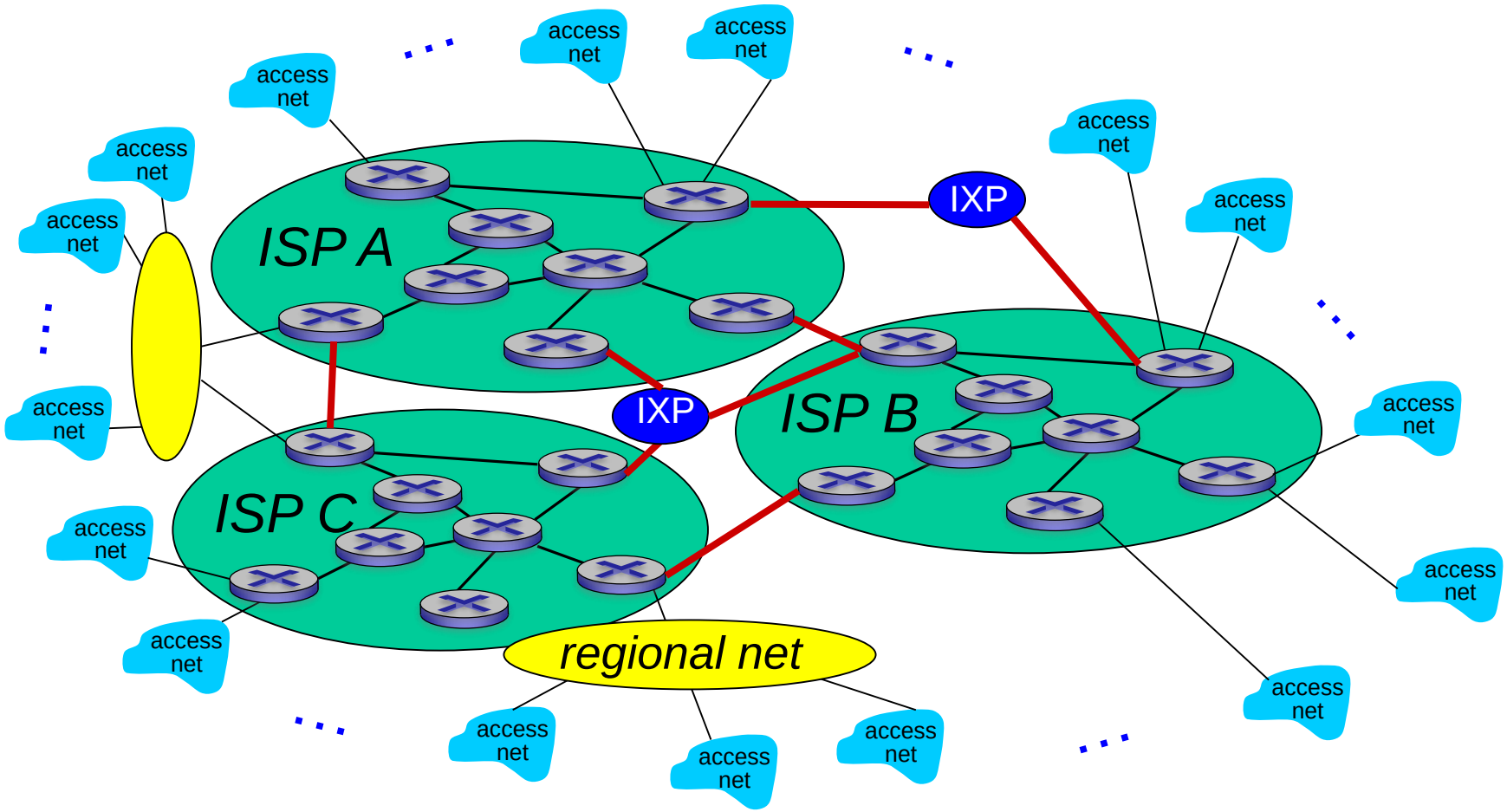
Internet structure: network of networks

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



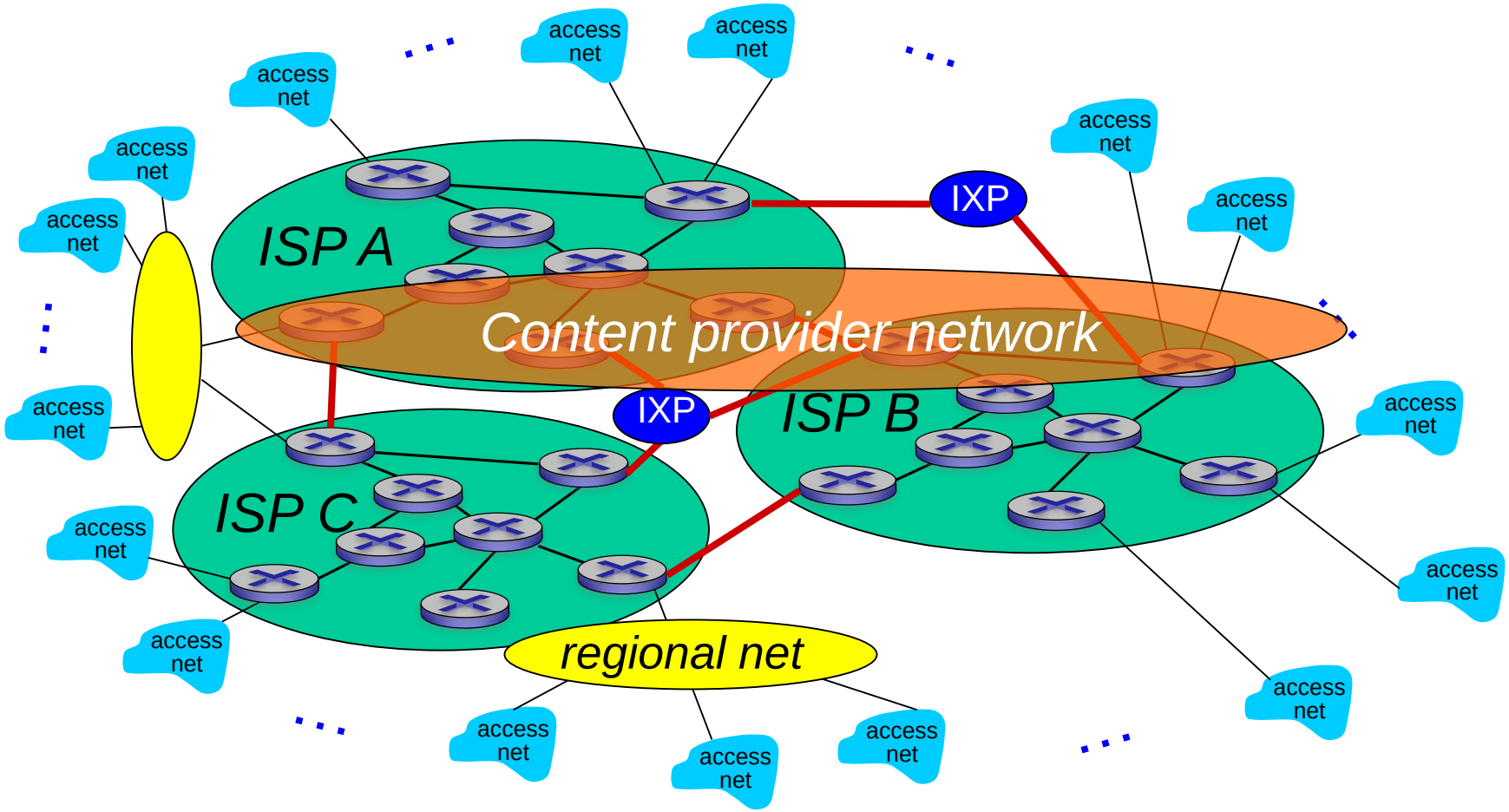
Internet structure: network of networks

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

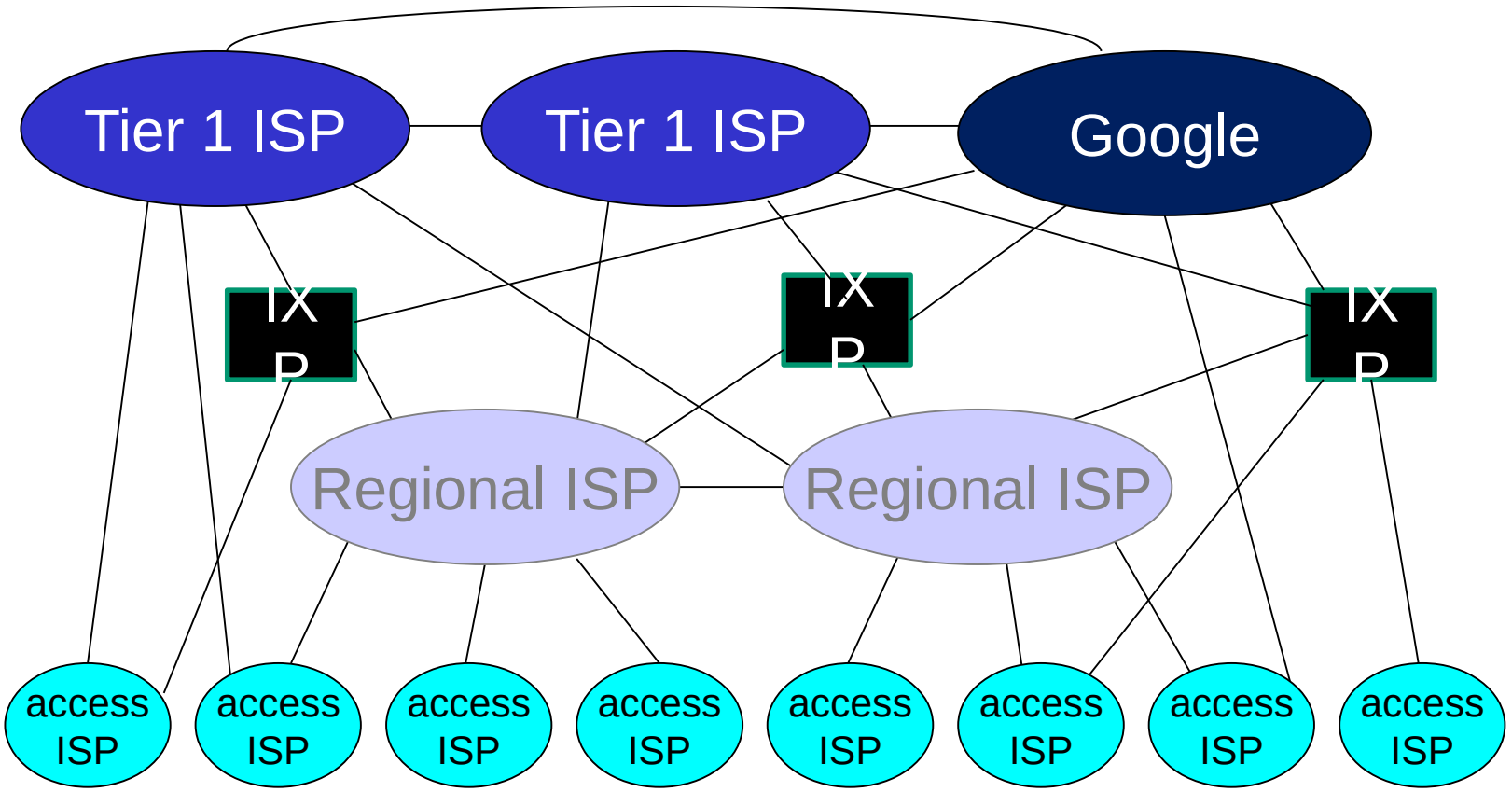


Internet structure: network of networks

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

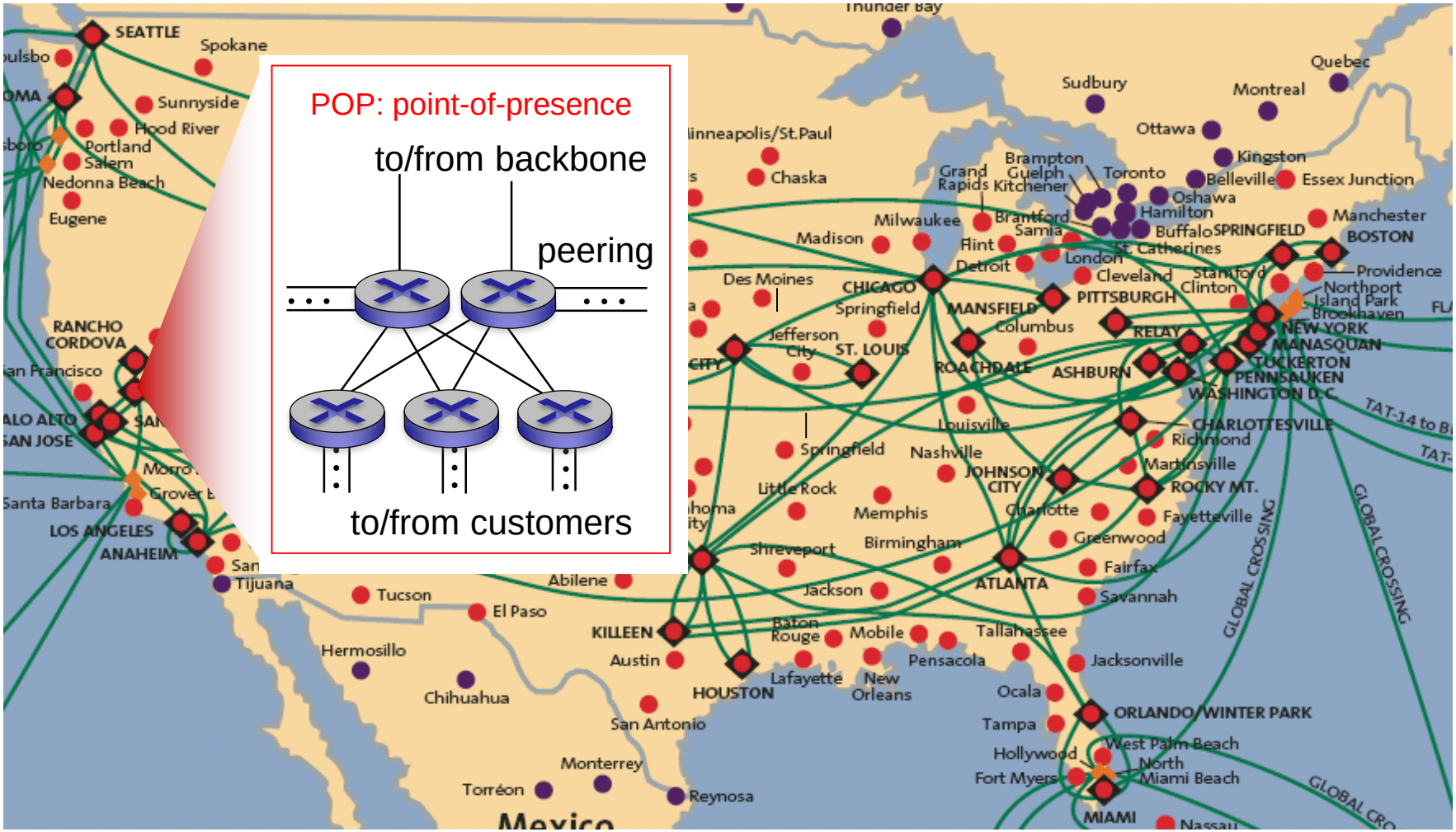


Internet structure: network of networks



- 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

1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

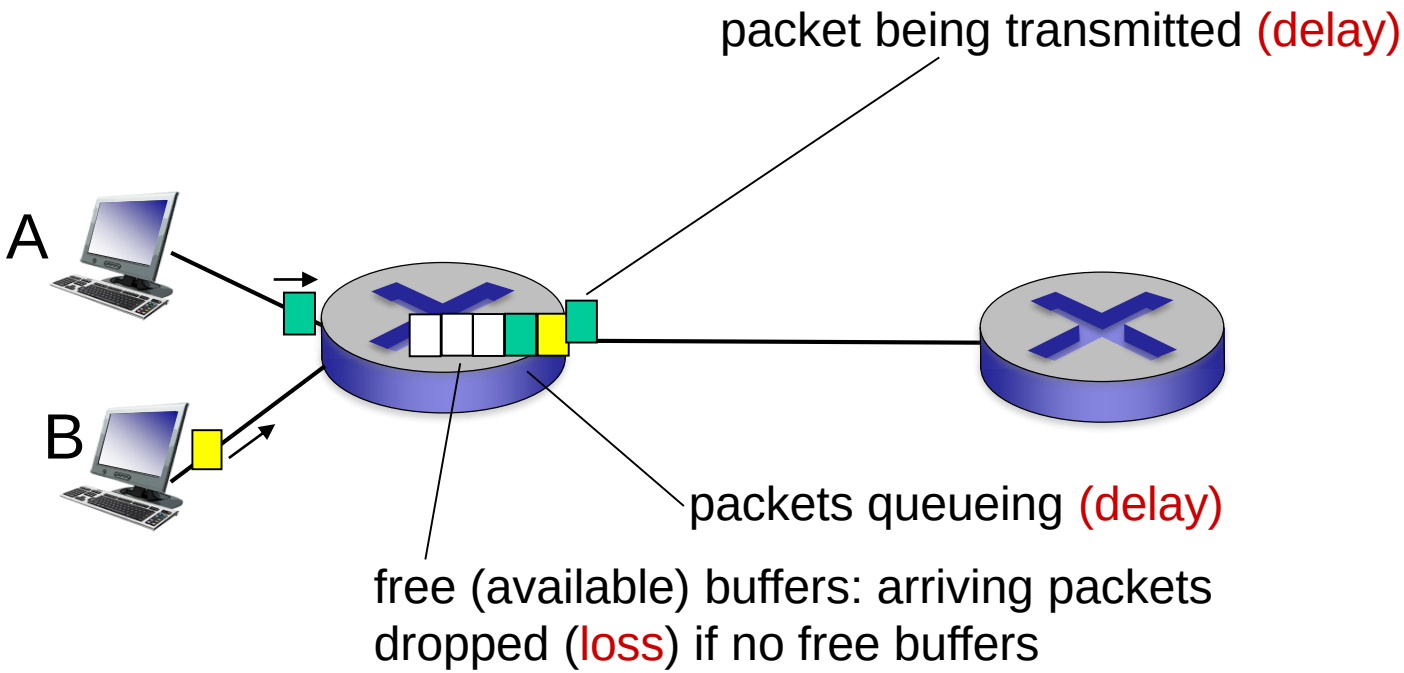
1.6 networks under attack: security

1.7 history

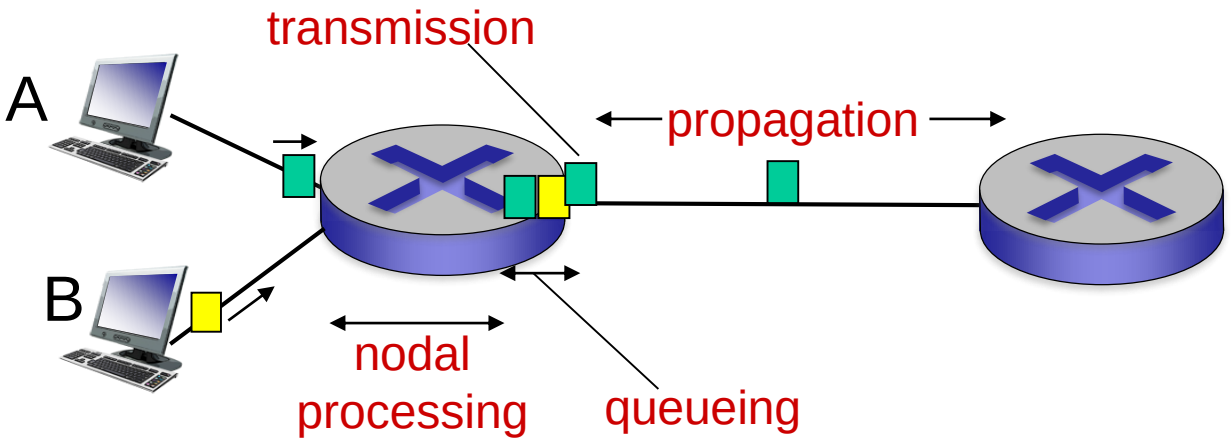
How do loss and delay occur?

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



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

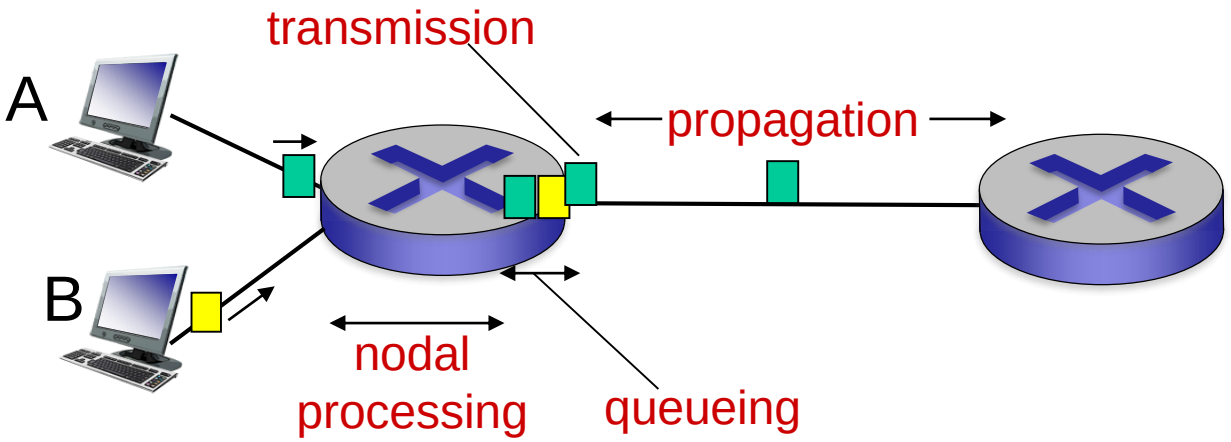
d_{proc}: nodal processing

- 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 (bps)*
- $d_{trans} = L/R$

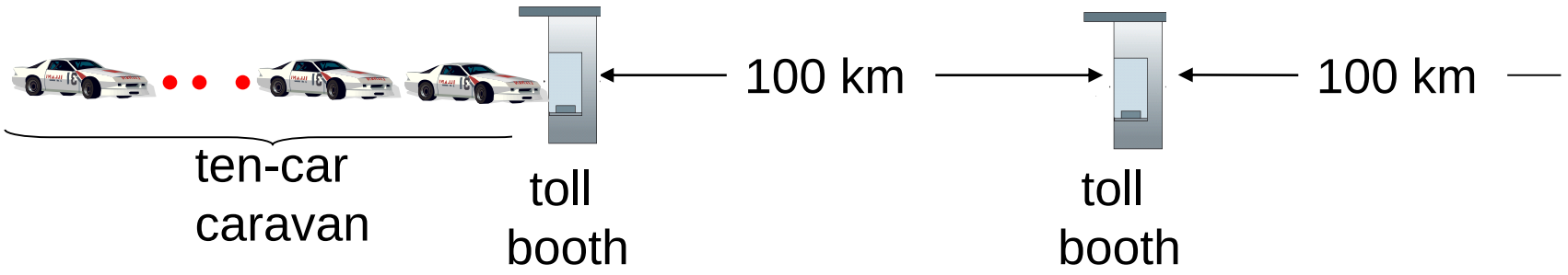
d_{trans} and d_{prop} *very* different

d_{prop}: propagation delay:

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

* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/
* Check out the Java applet for an interactive animation on trans vs. prop delay

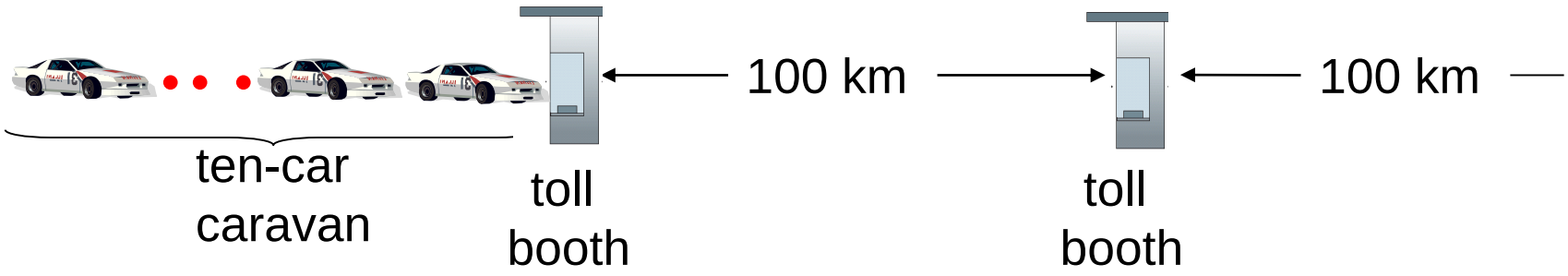
Caravan analogy



- cars "propagate" at 100 km/hr
- toll booth takes 12 sec to service car (bit transmission time)
- car ~ bit; caravan ~ packet
- *Q:* How long until caravan is lined up before 2nd toll booth?

- time to "push" entire caravan through toll booth onto highway = 12*10 = 120 sec
- time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr
- *A:* 62 minutes

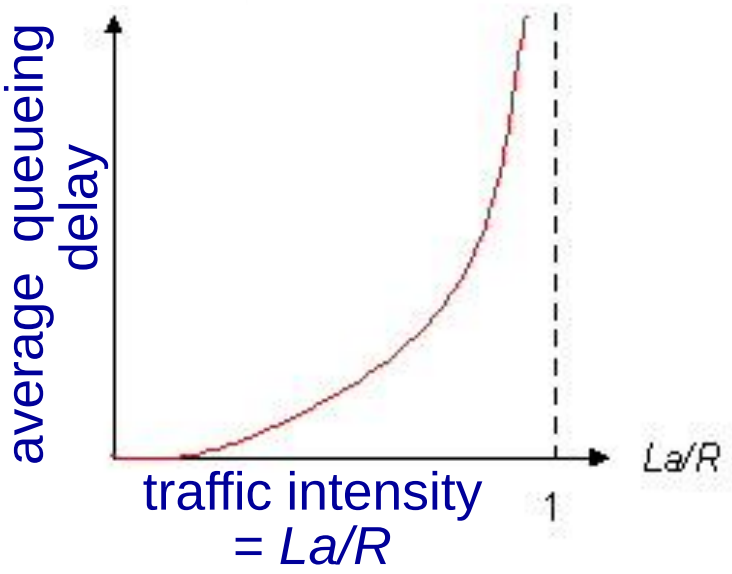
Caravan analogy (more)



- suppose cars now "propagate" at 1000 km/hr
- and suppose toll booth now takes one min to service a car
- *Q:* Will cars arrive to 2nd booth before all cars serviced at first booth?
  - *A: Yes!* after 7 min, first car arrives at second booth; three cars still at first booth

Queueing delay (revisited)

- *R:* link bandwidth (bps)
- *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!

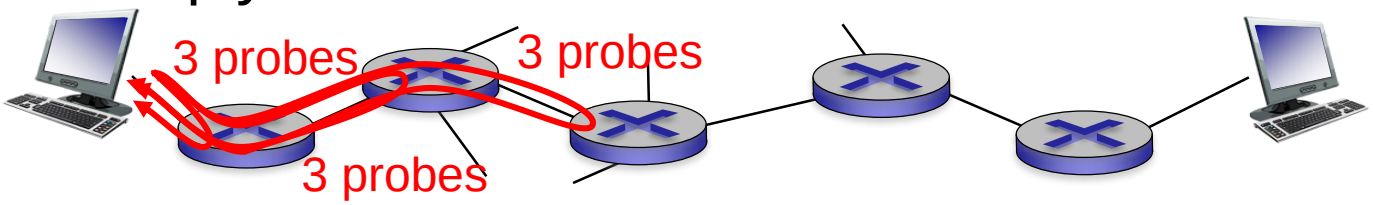
La/R ~ 0

La/R -> 1

* Check online interactive animation on queuing and loss

"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
```

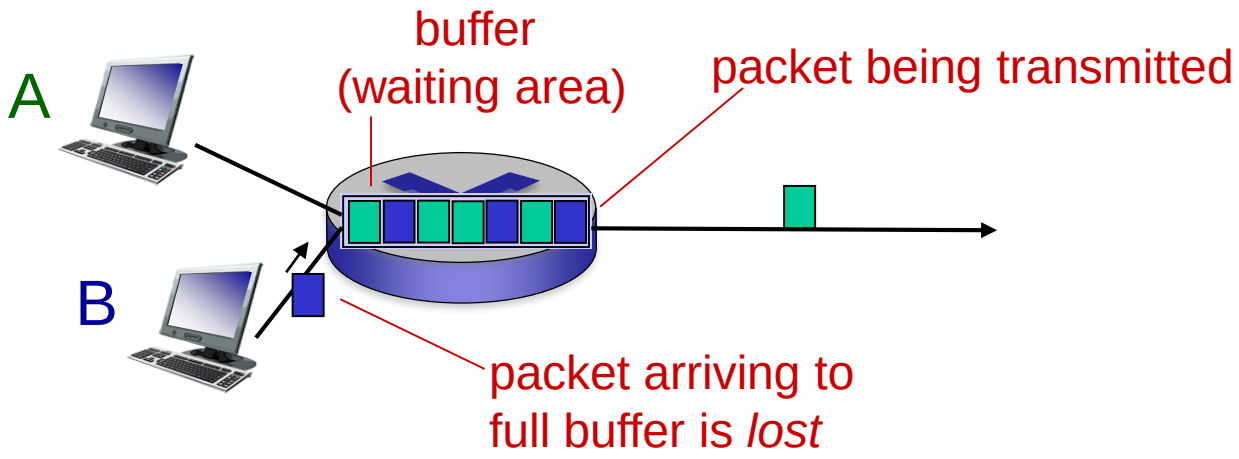
trans-oceanic link

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

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

Packet loss

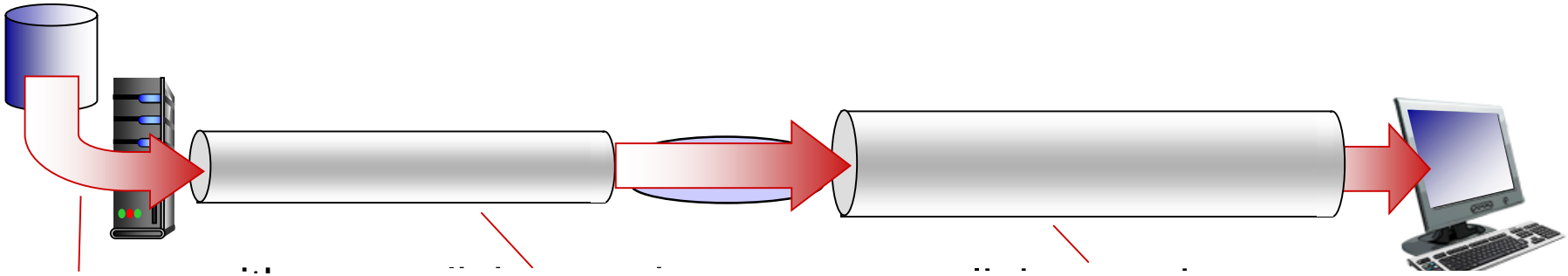
- queue (aka buffer) preceding link in buffer has finite capacity
- packet arriving to full queue dropped (aka lost)
- lost packet may be retransmitted by previous node, by source end system, or not at all



* Check out the Java applet for an interactive animation on queuing and loss

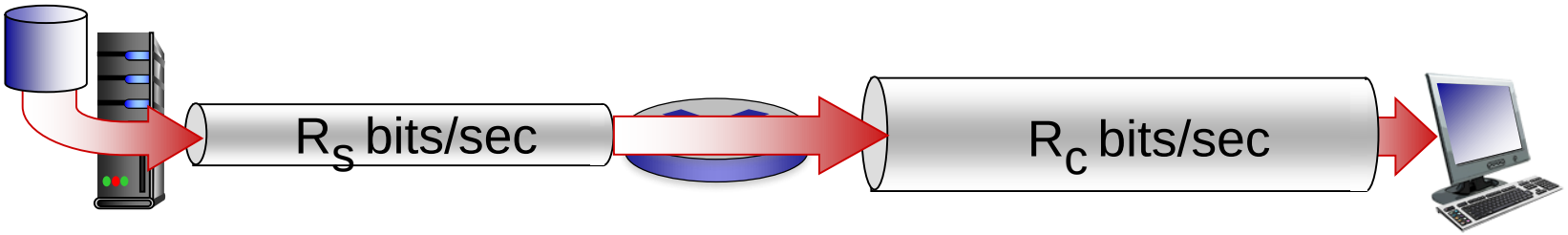
Throughput

- *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

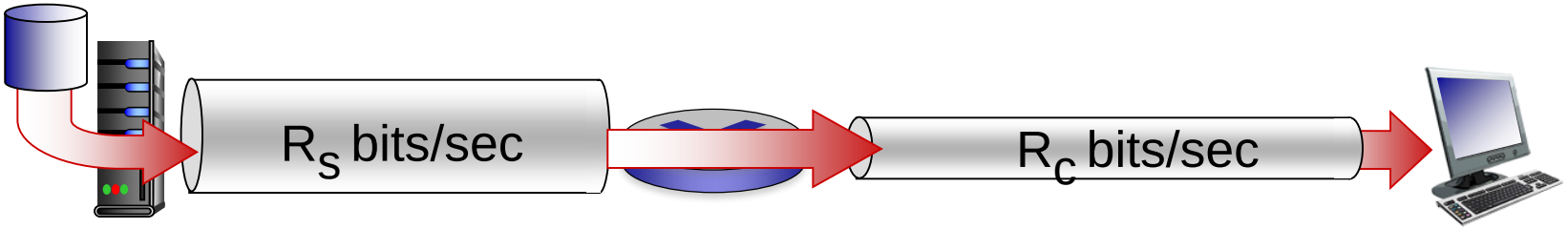


Throughput (more)

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



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

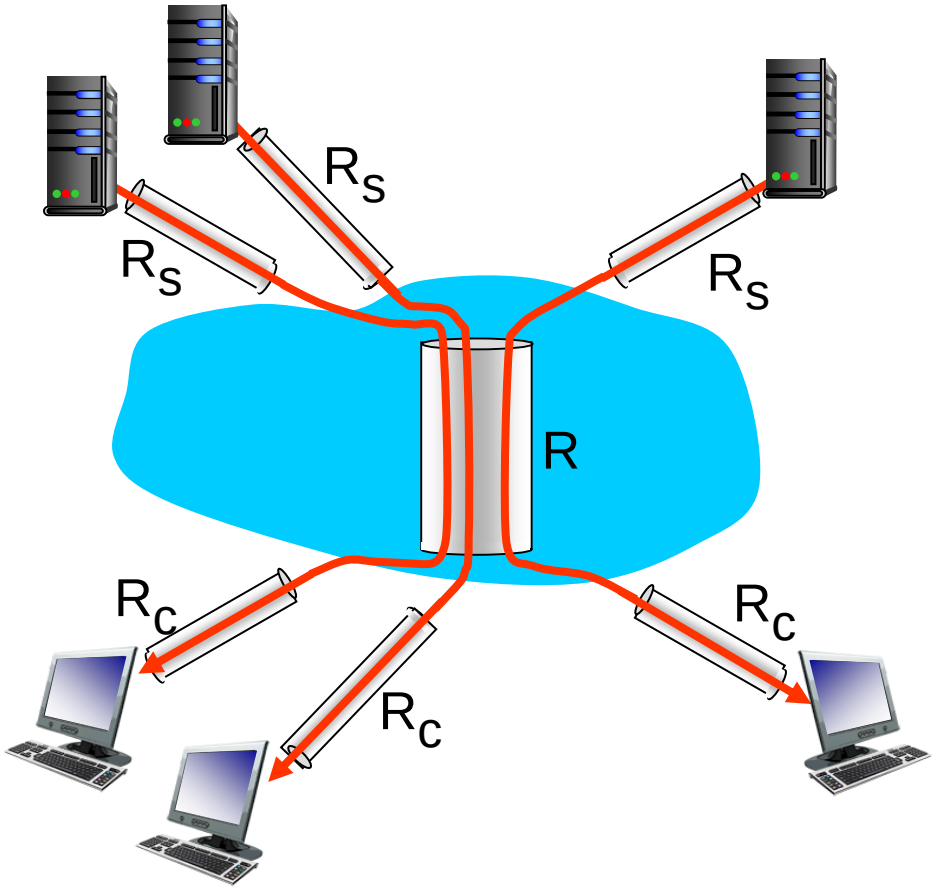


bottleneck link

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

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" ☺
  - Networks Vulnerable to attacks
  - What can go wrong and what are prevalent types of attacks
  - Internet protocol designers playing "catch-up"
  - security considerations in all layers!

Bad guys: put malware into hosts via Internet

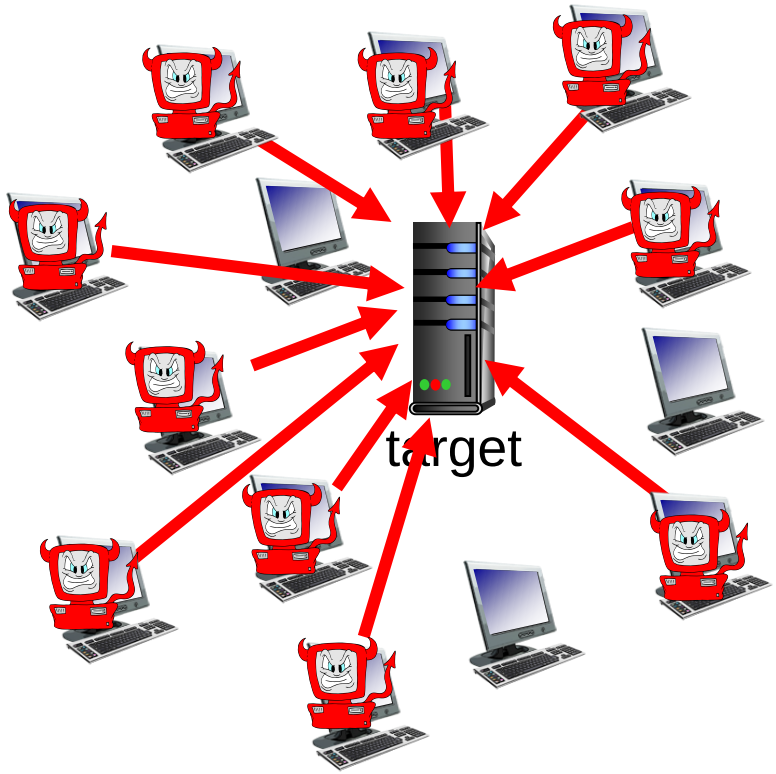
- malware can get in host from:
  - *virus:* self-replicating infection by receiving/executing object (e.g., e-mail attachment)
  - *worm:* self-replicating infection by passively receiving object that gets itself executed
- spyware malware can record keystrokes, web sites visited, upload info to collection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

- Trojan horse
  - is a program that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer.
  - Trojan horse is not able to replicate itself, nor can it propagate without an end user's assistance. This is why attackers must use social engineering tactics to trick the end user into executing the Trojan.

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

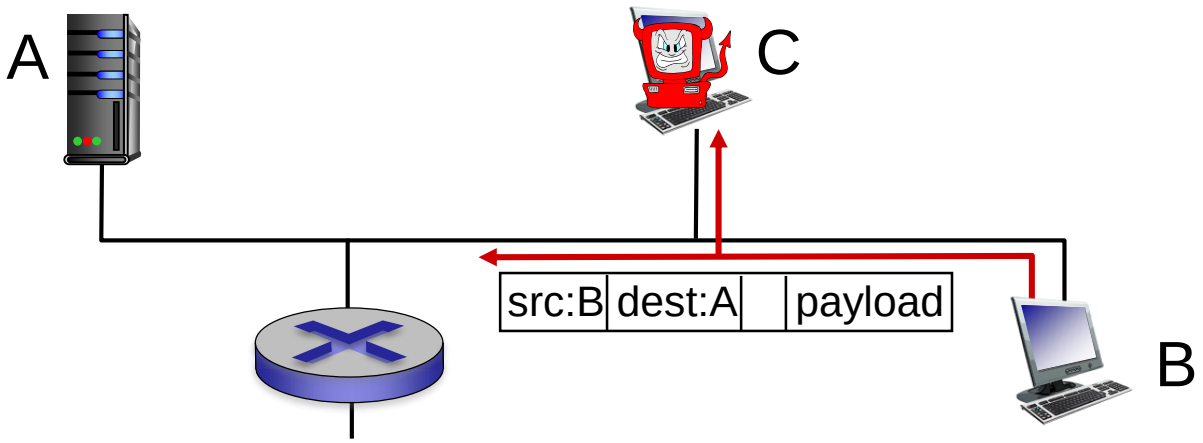
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Bad guys can sniff packets

packet "sniffing":

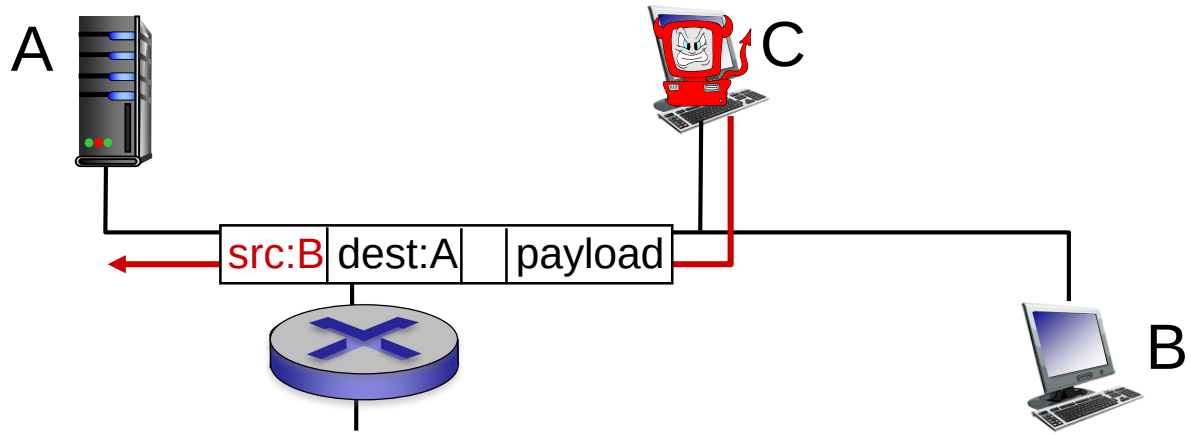
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- wireshark software used 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)

Bad guys can do

- Man in The Middle Attack
  - A man-in-the-middle attack requires three players. There's the victim, the entity with which the victim is trying to communicate, and the "man in the middle," who's intercepting the victim's communications. Critical to the scenario is that the victim isn't aware of the man in the middle.
- Cybercriminals can use MITM attacks to gain control of devices in a variety of ways.

- IP Spoofing
- DNS Spoofing
  - Domain Name Server, or DNS, spoofing is a technique that forces a user to a fake website rather than the real one the user intends to visit. If you are a victim of DNS spoofing, you may think you're visiting a safe, trusted website when you're actually interacting with a fraudster. The perpetrator's goal is to divert traffic from the real site or capture user login credentials.
- HTTPS spoofing
  - When doing business on the internet, seeing "HTTPS" in the URL, rather than "HTTP" is a sign that the website is secure and can be trusted. In fact, the "S" stands for "secure." An attacker can fool your browser into believing it's visiting a trusted website when it's not. By redirecting your browser to an unsecure website, the attacker can monitor your interactions with that website and possibly steal personal information you're sharing.

- Wi-Fi eavesdropping
  - Cybercriminals can set up Wi-Fi connections with very legitimate sounding names, similar to a nearby business. Once a user connects to the fraudster's Wi-Fi, the attacker will be able to monitor the user's online activity and be able to intercept login credentials, payment card information, and more. This is just one of several risks associated with using public Wi-Fi

Communications Tasks

key tasks that must be performed in a data communications system

Transmission system utilization	Addressing
Interfacing	Routing
Signal generation	Recovery
Synchronization	Message formatting
Exchange management	Security
Error detection and correction	Network management
Flow control	

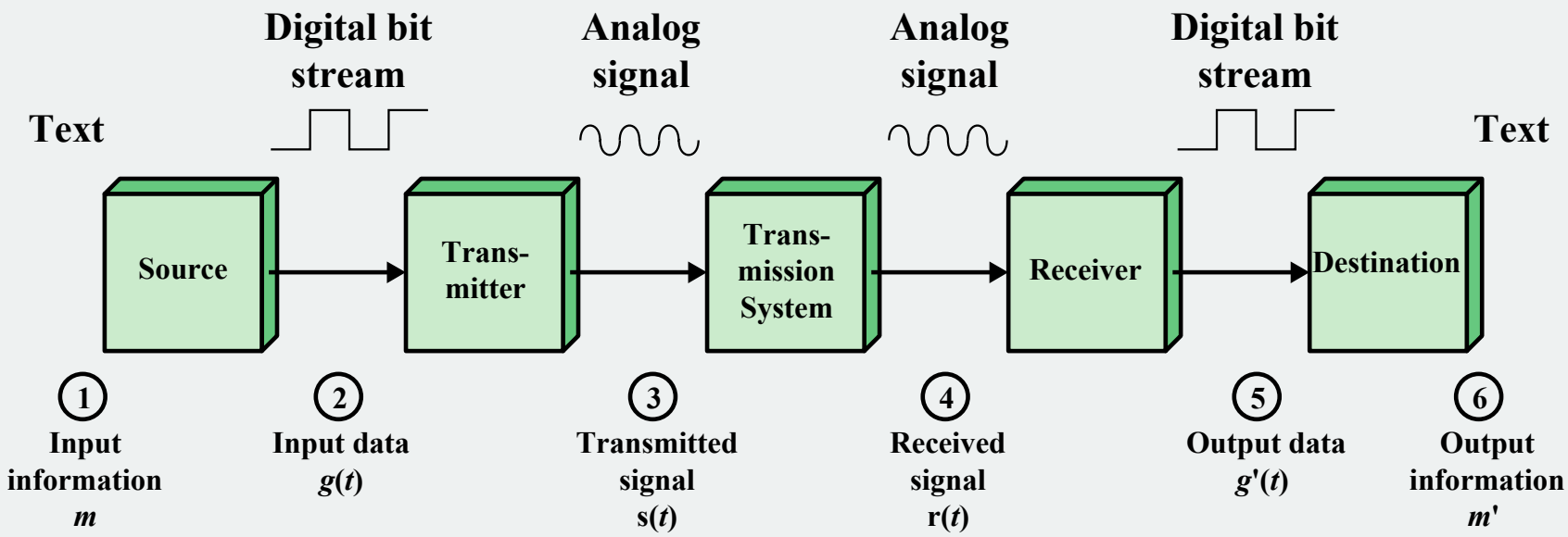
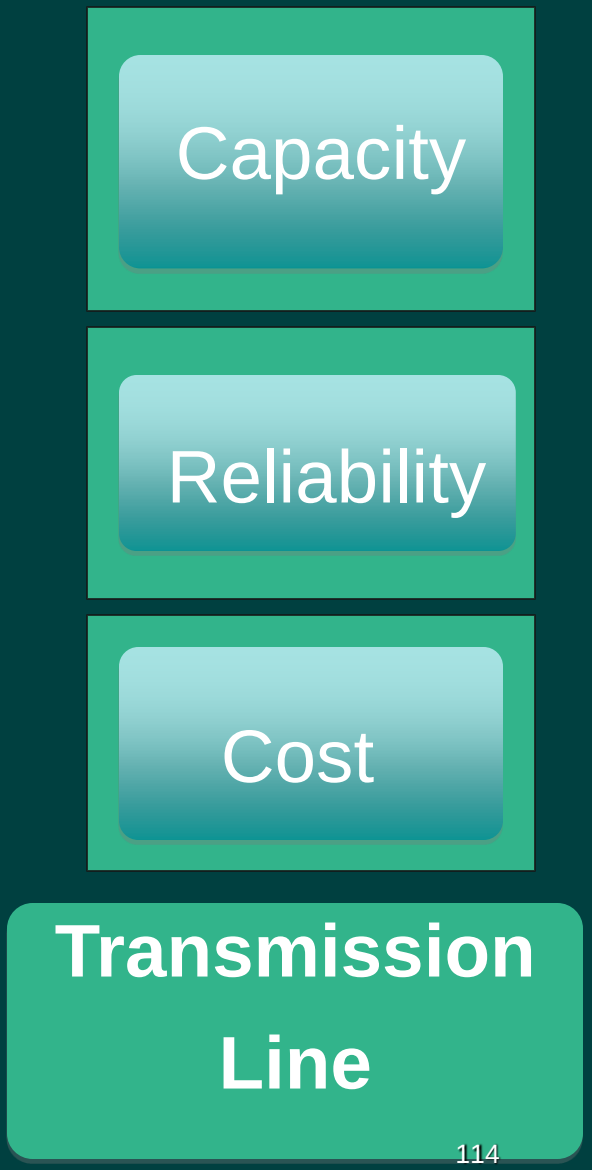


Figure 1.4 Simplified Data Communications Model

Transmission Lines

The basic building block of any communications facility is the transmission line

The business manager is concerned with a facility providing the required capacity, with acceptable reliability, at minimum cost



Transmission Mediums

Two mediums currently driving the evolution of data communications transmission are:

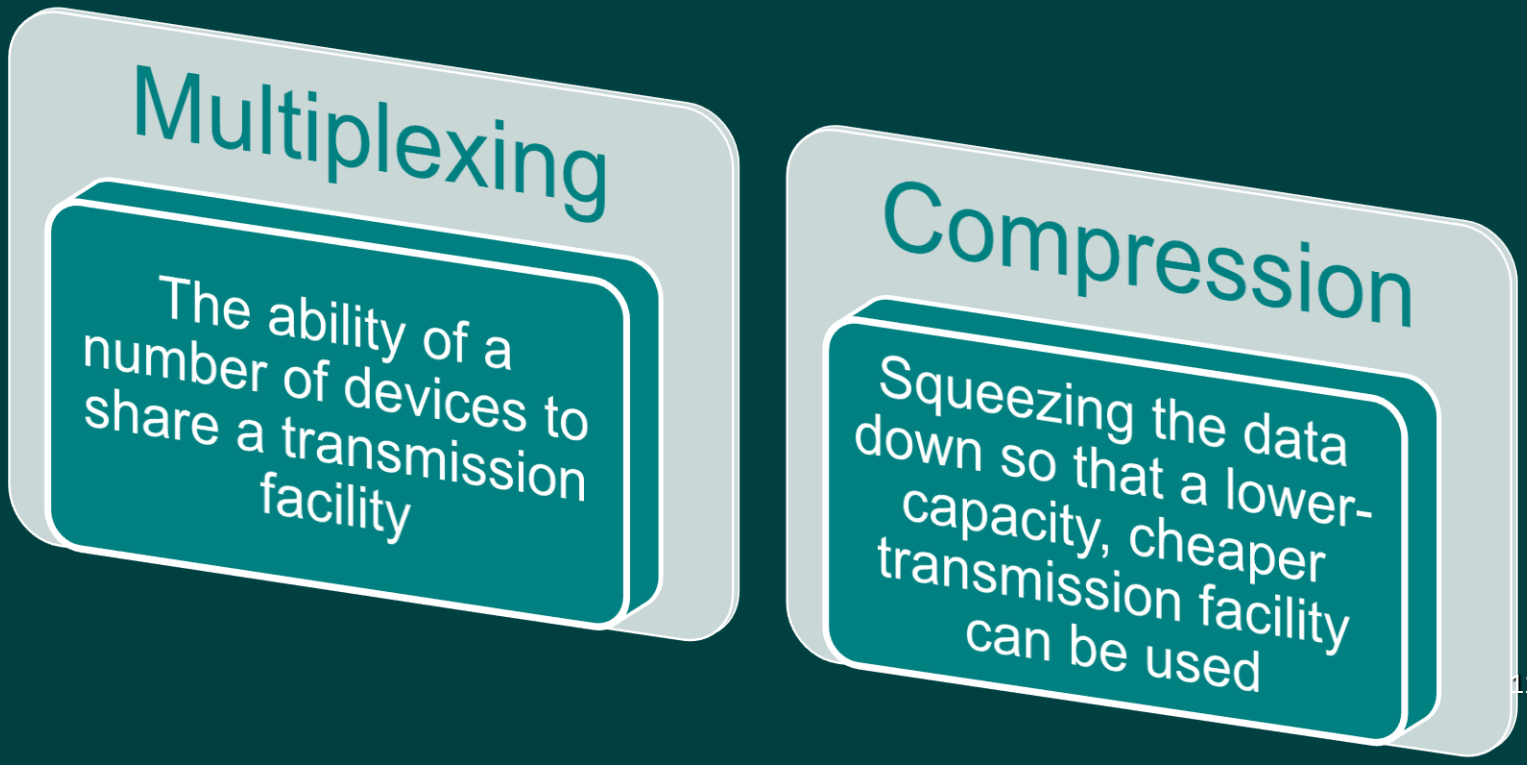
Fiber optic transmissions

and

Wireless transmissions

Transmission Services

- Remain the most costly component of a communications budget
- Two major approaches to greater efficiency:

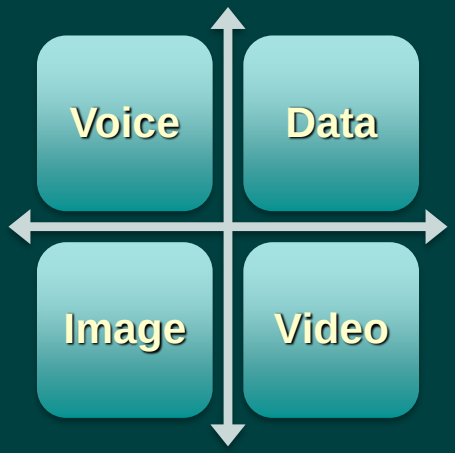


Networks

- It is estimated that by 2016 there will be over 20 billion fixed and mobile networked devices
  - This affects traffic volume in a number of ways:
    - It enables a user to be continuously consuming network capacity
    - Capacity can be consumed on multiple devices simultaneously
    - Different broadband devices enable different applications which may have greater traffic generation capability
    - The result is that the total annual traffic generated over the Internet and other IP-based networks is forecast to rise from 372 exabytes (372×2^{60} bytes) to 1.3 zettabytes (1.3×2^{70} bytes) in 2016

Networking

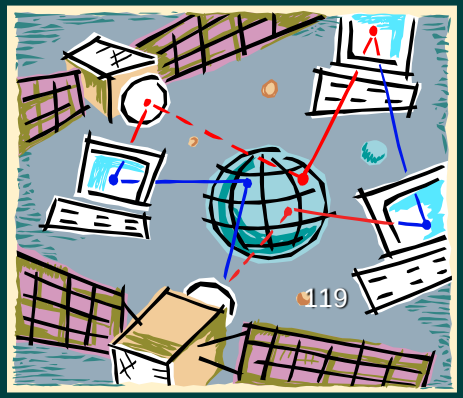
Advances in technology have led to greatly increased capacity and the concept of integration, allowing equipment and networks to work simultaneously



The development of switching **systems** that are capable of responding to the increasing capacities of transmission links and business communication traffic requirements is an ongoing challenge not yet conquered.

Wide Area Networks (WANs)

- Span a large geographical area
- Require the crossing of public right-of-ways
- Rely in part on common carrier circuits
- Typically consist of a number of interconnected switching nodes



Wide Area Networks

Alternative technologies used include:

- Circuit switching
- Packet switching
- Frame relay
- Asynchronous Transfer Mode (ATM)

Circuit Switching

- Uses a dedicated communications path
- Connected sequence of physical links between nodes
- Logical channel dedicated on each link
- Rapid transmission
- The most common example of circuit switching is the telephone network

Packet Switching

- Data are sent out in a sequence of small chunks called packets
- Packets are passed from node to node along a path leading from source to destination
- Packet-switching networks are commonly used for terminal-to-terminal computer and computer-to-computer communications

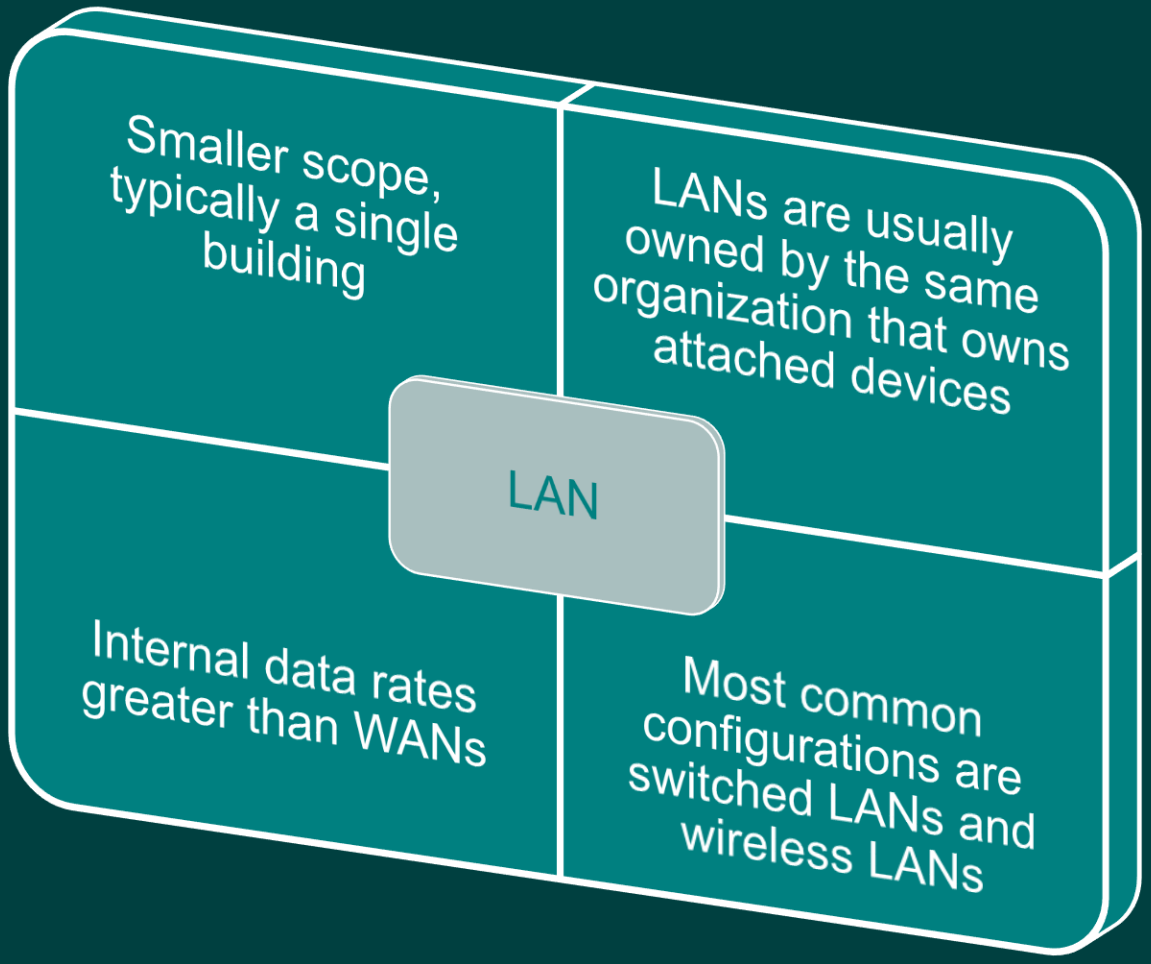
Frame Relay

- Developed to take advantage of high data rates and low error rates
- Operates at data rates of up to 2 Mbps
- Key to achieving high data rates is to strip out most of the overhead involved with error control

Asynchronous Transfer Mode (ATM)

- Referred to as cell relay
- Culmination of developments in circuit switching and packet switching
- Uses fixed-length packets called cells
- Works in range of 10s and 100s of Mbps and in the Gbps range
- Allows multiple channels with the data rate on each channel dynamically set on demand

Local Area Networks (LAN)



The Internet

- Internet evolved from ARPANET
- Developed to solve the dilemma of communicating across arbitrary, multiple, packet-switched networks
- Foundation is the TCP/IP protocol suite

Architecture and Operation

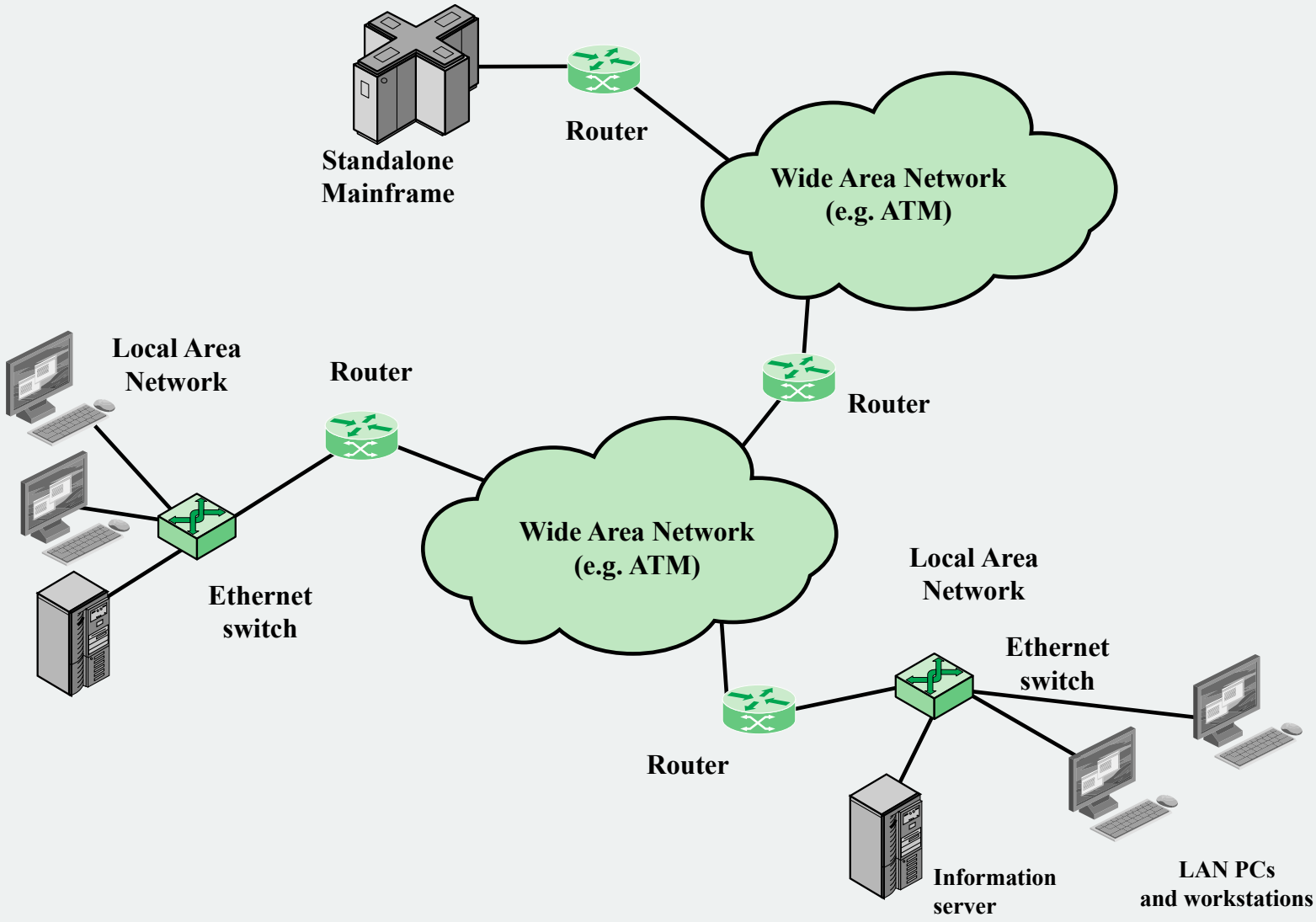


Figure 1.5 Key Elements of the Internet

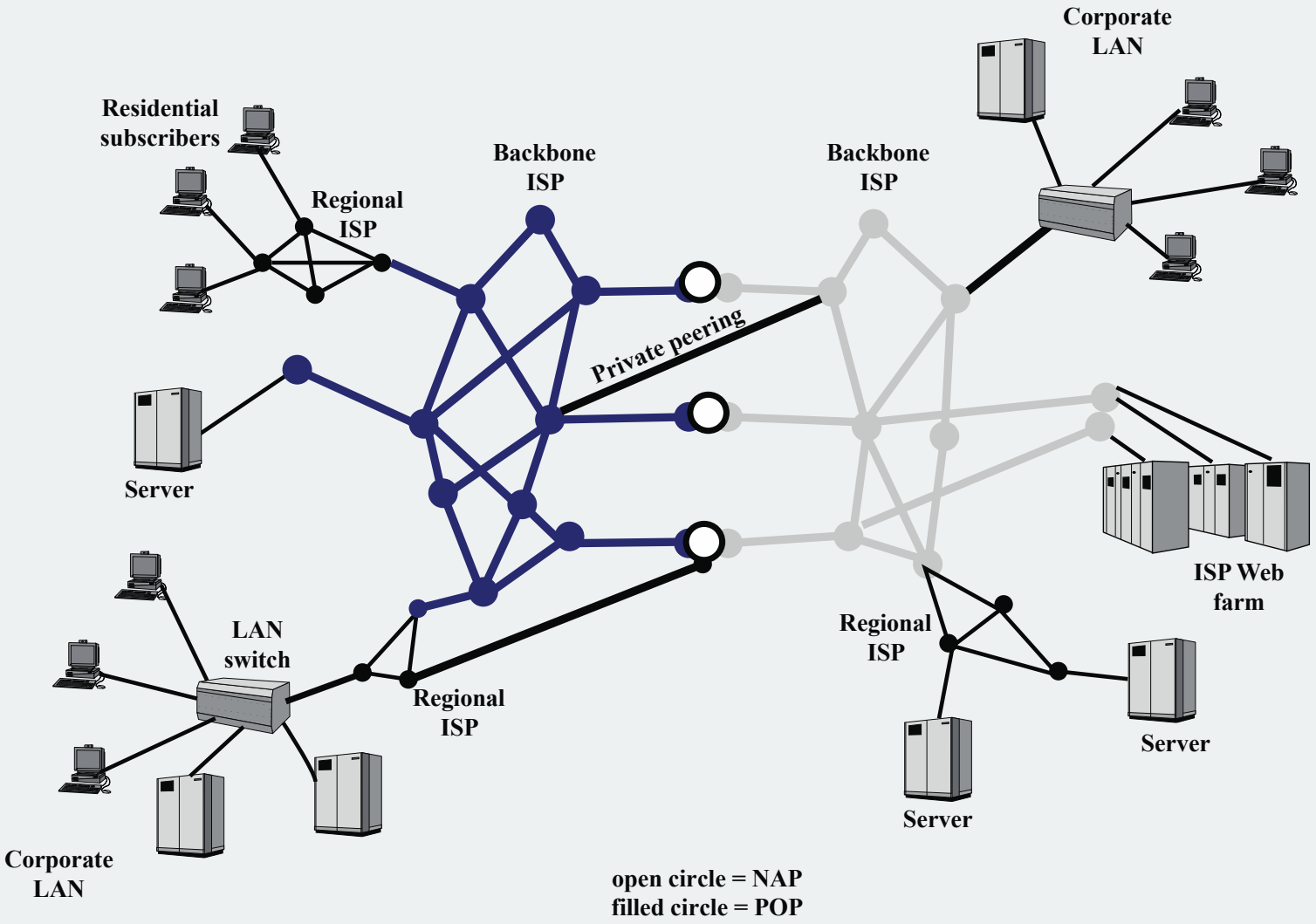


Figure 1.6 Simplified View of Portion of Internet

Table 1.2
Internet Terminology

- Central Office (CO)
  - The place where telephone companies terminate customer lines and locate switching equipment to interconnect those lines with other networks
- Customer Premises Equipment (CPE)
  - Telecommunications equipment that is located on the customer's premises
- Internet Service Provider (ISP)
  - A company that provides other companies or individuals with access to, or presence on, the Internet
- Network Access Point (NAP)
  - One of several major Internet interconnection points that serve to tie all the ISPs together
- Network Service Provider (NSP)
  - A company that provides backbone services to an Internet service provider (ISP)
- Point of Presence (POP)
  - A site that has a collection of telecommunications equipment, usually refers to ISP or telephone company sites

(Table can be found on page 27 in textbook)

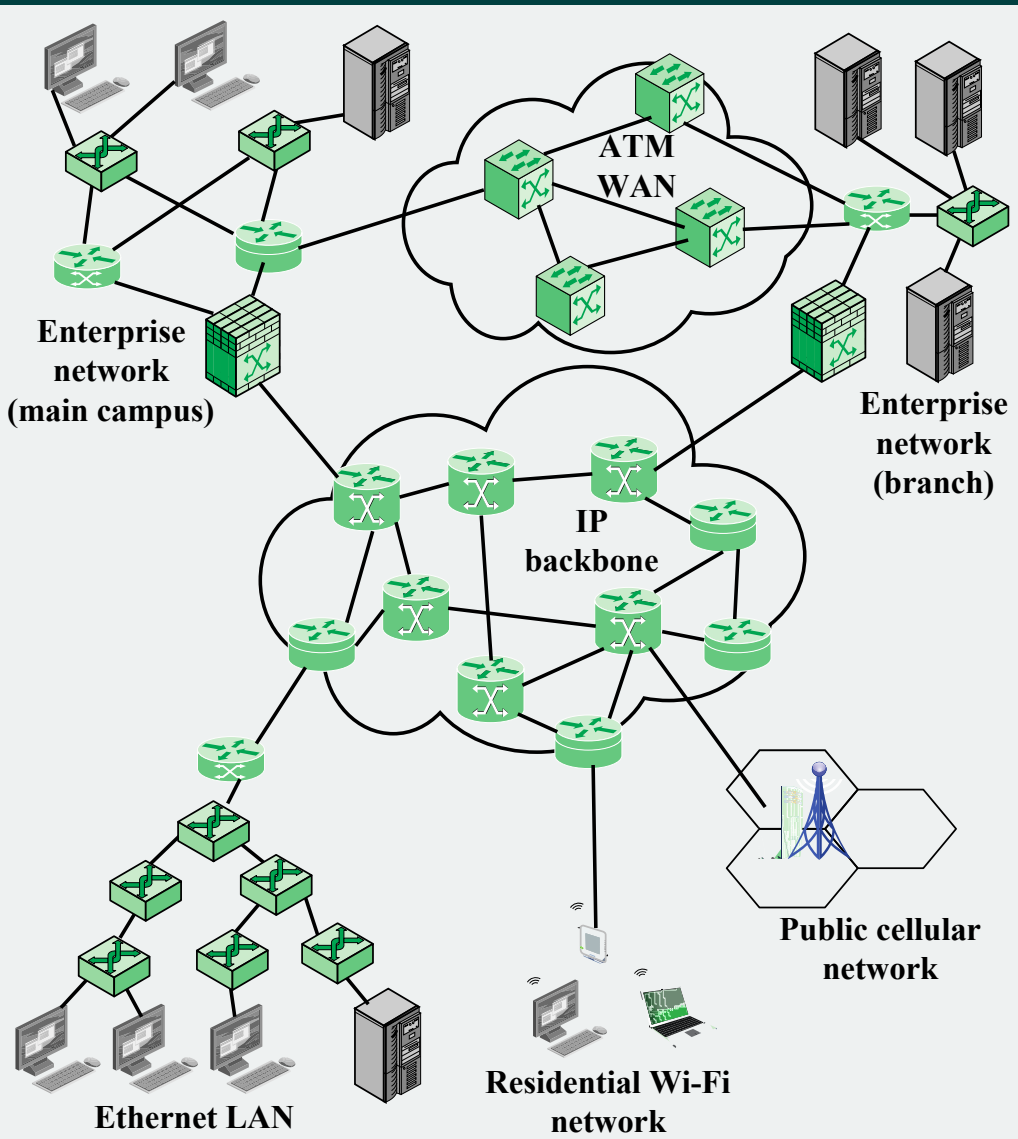


Figure 1.7 A Networking Configuration

Summary

- Transmission mediums
  - Fiber optic
  - Wireless
- Network categories:
  - Wide Area Networks
  - Local Area Networks
  - Wireless Networks
- Internet
  - Origin
  - Key elements
  - Internet architecture
- Trends challenging data communications:
  - Traffic growth
  - Development of new services
  - Advances in technology
- Data Transmission and Network Capacity Requirements
- Convergence