CS 60: Computer Networks

Introduction

Agenda

1. Intro and course overview
2. Networking creates new possibilities and new challenges
3. What is the Internet anyway?
4. How are hosts connected?
5. Connecting ECSC (illustrative)

Introduction

Your background

- Undergrads/grads
- Macs/Windows/Linux

TA background

My background

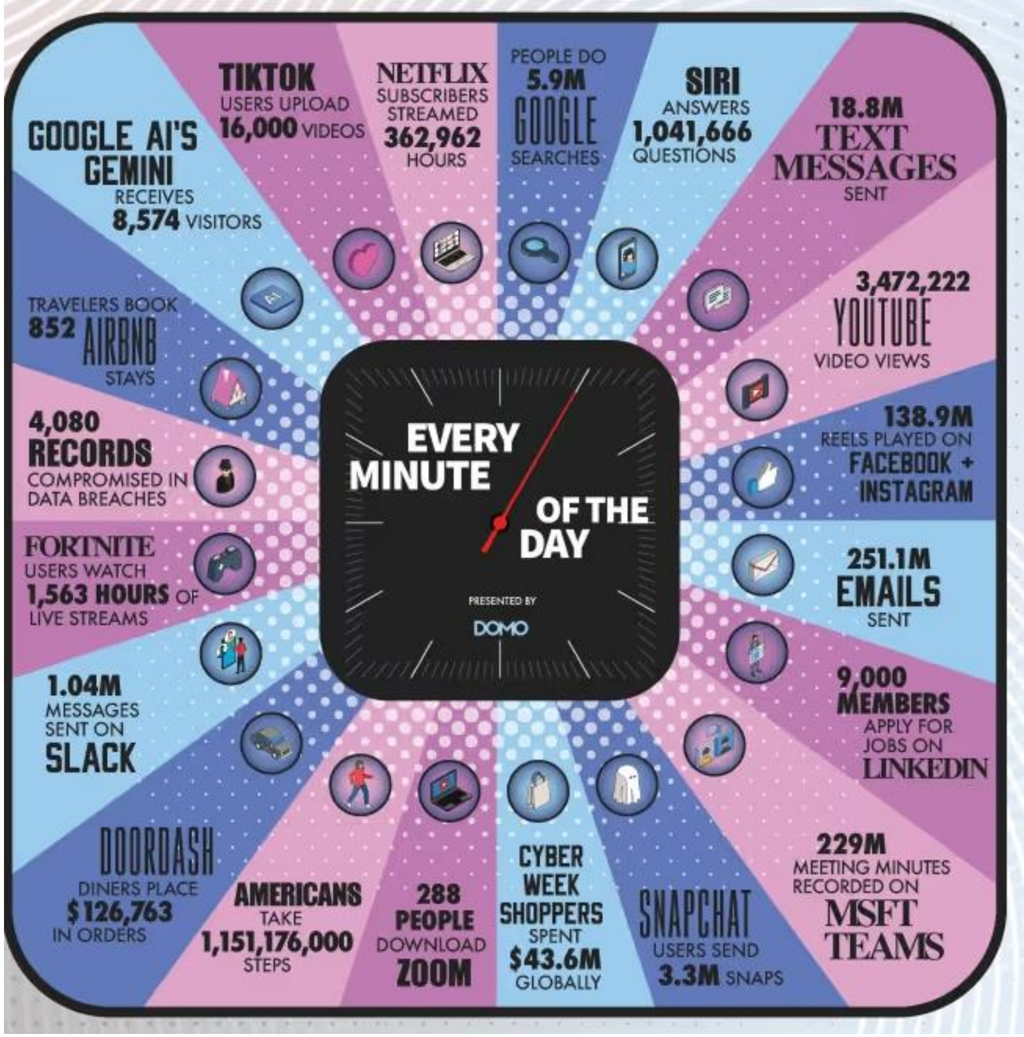
Why are you interested in computer networks?

- Estimated 19.8 billion devices on the Internet in 2025 (29 billion projected by 2030)[1]
- Devices exchange 402 *quintillion* bytes *every day*[2]
- 90% of world's data created last two years[3]
- Might be a good idea to know something about how this data is communicated

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[2] https://explodingtopics.com/blog/data-generated-per-day
[3] https://www.proofpoint.com/sites/default/files/infographics/pfpt-us-ig-a-brief-history-of-data.pdf

Big data is often characterized by the 5 V's

Every minute…


EVERY MINUTE OF THE DAY
PRESENTED BY DOMO
GOOGLE AI'S GEMINI RECEIVES 8,574 VISITORS
TIKTOK USERS UPLOAD 16,000 VIDEOS
NETFLIX SUBSCRIBERS STREAMED 362,962 HOURS
PEOPLE DO 5.9M GOOGLE SEARCHES
SIRI ANSWERS 1,041,666 QUESTIONS
18.8M TEXT MESSAGES SENT
3,472,222 YOUTUBE VIDEO VIEWS
138.9M REELS PLAYED ON FACEBOOK + INSTAGRAM
251.1M EMAILS SENT
9,000 MEMBERS APPLY FOR JOBS ON LINKEDIN
229M MEETING MINUTES RECORDED ON MSFT TEAMS
SNAPCHAT USERS SEND 3.3M SNAPS
CYBER WEEK SHOPPERS SPENT $43.6M GLOBALLY
288 PEOPLE DOWNLOAD ZOOM
AMERICANS TAKE 1,151,176,000 STEPS
DOORDASH DINERS PLACE $126,763 IN ORDERS
1.04M MESSAGES SENT ON SLACK
FORTNITE USERS WATCH 1,563 HOURS OF LIVE STREAMS
4,080 RECORDS COMPROMISED IN DATA BREACHES
TRAVELERS BOOK 852 AIRBNB STAYS

https://www.domo.com/learn/infographic/data-never-sleeps-12

Big data characterized by five V's:

1. **Volume**: quantity of data to be stored, systems can be scaled
   - Vertically : "get a bigger box"
   - Horizontally: "get more boxes"
2. **Velocity**: speed at which data must be processed
   - Stream processing: analyze data as it comes
   - Feedback loop: data generates recommendations, recommendations lead to more data
3. **Variety**: store data in many forms
   - Structured data: fits into predefined data model
   - Unstructured data: does not fit data model
4. **Veracity**: can the data be trusted?
5. **Value**: can we exact value from the data, perhaps by correlating with other data?

Data privacy concerns abound!

We will examine how data is sent over the Internet and the security ramifications

Major topics:

- Network basics
  - What is the Internet anyway
  - How are computers connected to the network
  - How do computers find each other on the network (ARP, DNS)
  - Socket programming/sniffing/spoofing network traffic
- Network layers
  - Application (HTTP, email)
  - Transport (TCP and UDP)
  - Network (routing)
  - Link (switching)
  - Physical (wired and wireless)
- Security
  - Crypto
  - Secure comms (TOR, VPNs, TLS)
  - Firewalls
  - Penetration testing (IDS/IPS)
  - Unintended networks

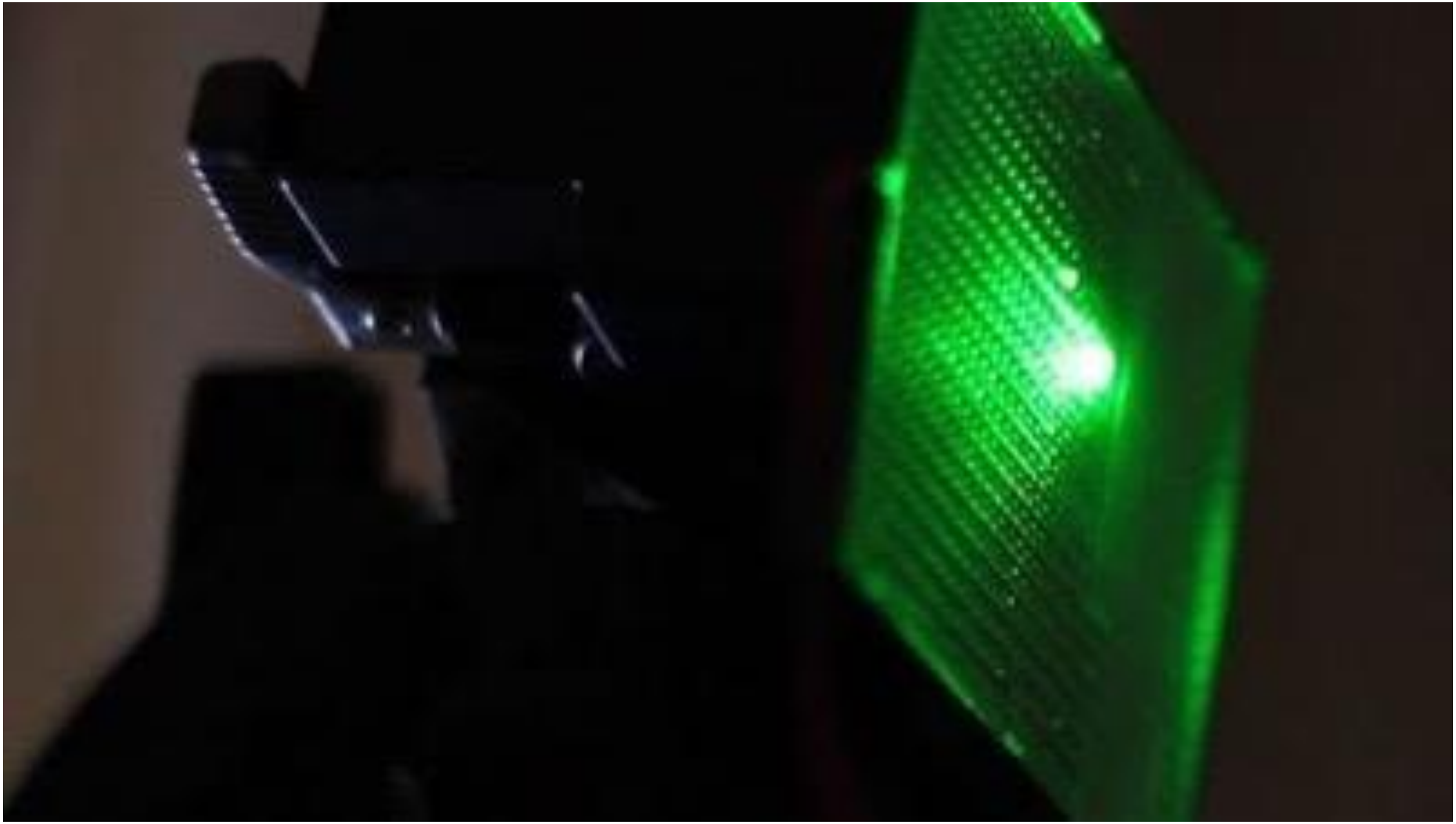
I remember the network layers as "plant" with the A at the end

We will cover them in order from Application down to Physical

At one point in the class, we will contemplate a wireless lie detector as part of unintended networks

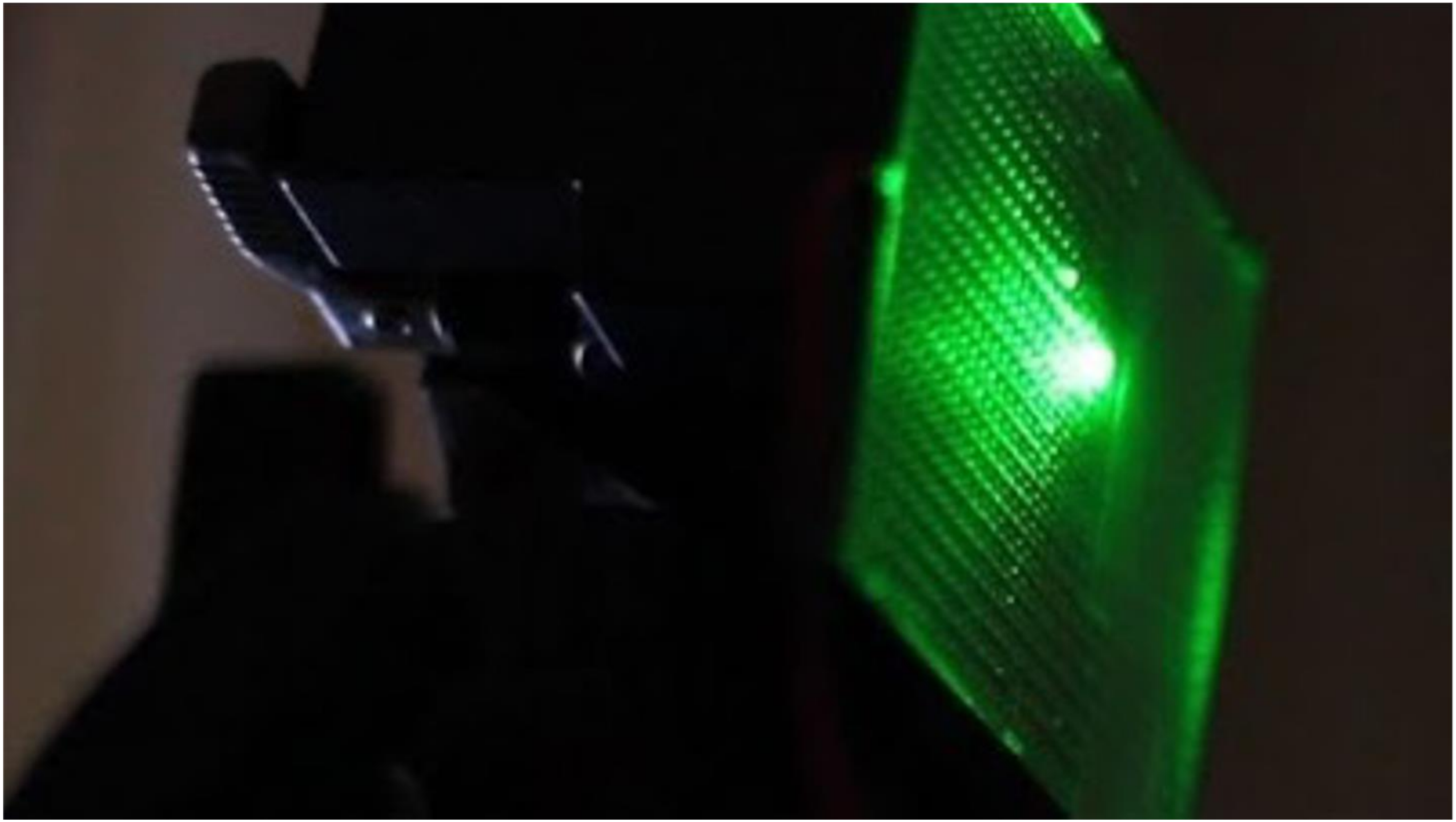
We will also consider other unintended "networks"

Laser microphone demo where a window glass pane is a communication media



https://www.youtube.com/watch?v=1zGU_30l6eU&start=270

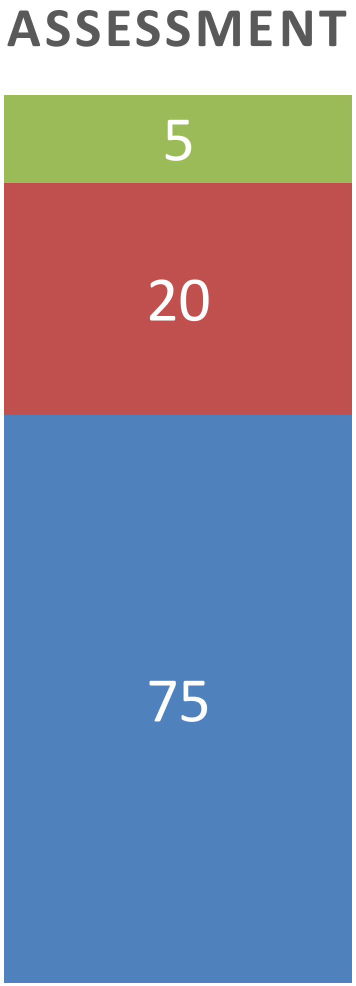
Laser microphone demo where a window glass pane is a communication media



https://www.youtube.com/watch?v=1zGU_30l6eU&start=270

Countermeasures?

Grading is comprised of labs, a final team project, and class engagement



Participation

Final project

Labs

- Five labs each worth 15%
- Completed in teams of two

NOTE:

There are <u>no exams</u>

Textbook:

Computer Networking: A Top-Down Approach, 9th edition, by Kurose and Ross

LLMs

- Can use them
- Recommend you try it yourself first
- Can not share prompts or LLM output
- Must cite

Come to lecture prepared!

Syllabus: http://www.cs.dartmouth.edu/~tjp/cs60

- I will expect you in class each day (participation portion of grade)

- The Schedule page of the course web indicates the material for that day, **read this material before each class period**

- I plan to spend roughly half of each class doing practice exercises
  - I will give a practice problem and time for you to work on the problem
  - Afterward I will randomly select one student to present their solution to the class (participation grade)
  - We will see there are often many ways to efficiently solve a problem, seeing how someone else solved a problem can often be useful

We will also be using Canvas and Slack for announcements and help

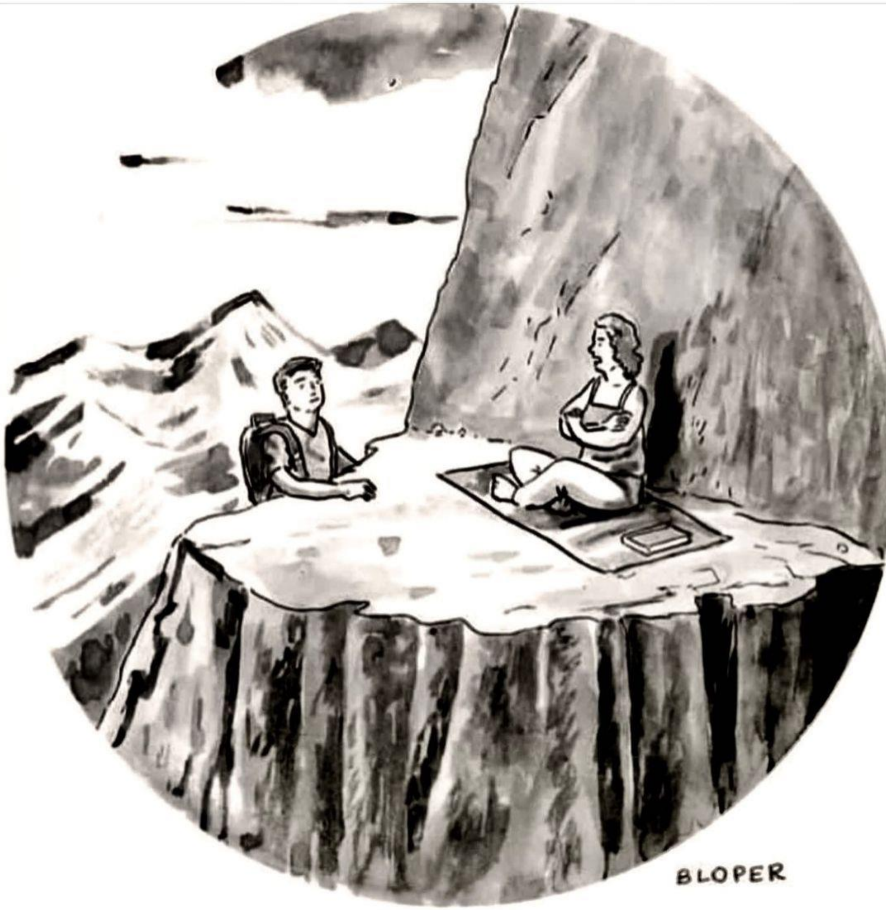
Canvas

- Course announcements
- Homework submissions

Slack (access via Canvas)

- Q&A forum
- Ask questions, get answers
- **Don't post code!**

Let me know if you don't have access



"The answers you seek can be found in the syllabus."

Lab 0 is out today

Lab 0

- Find it on Canvas
- Take course survey to understand your background
- Install software VM
- Read and acknowledge course policies

Agenda

1. Intro and course overview

➡ 2. Networking creates new possibilities and new challenges

3. What is the Internet anyway?

4. How are hosts connected?

5. Connecting ECSC (illustrative)

Devices other than computers also connect to the Internet (the Internet of Things)

Amazon Echo

Internet refrigerator

IP picture frame

Pacemaker & Monitor

Web-enabled toaster + weather forecaster

Security Camera

Slingbox: remote control cable TV

AR devices

Internet phones

Smart mattress

Fitbit

Adapted from Kurose and Ross

Devices communicating with each other can create new possibilities

Pacemaker device

Device programmer

- Implantable Medical Devices (IMDs) are often reprogrammed wirelessly
- Why?
  - Implanted medical devices cannot be physically connected to reprogram them
  - Surgery to access the IMD is dangerous
  - Patient's needs may change, so device programming must change too
  - New IMD software updates become available
  - Solution was wireless communications between pacemaker and a programmer
- Great idea!

Attack scenario

Imagine: many years after graduation

- Given your excellent education, you've become a very important person
- But it's been stressful climbing to the top
- So stressful that you now have an implantable medical device (IMD), in your case, a pacemaker
- But you've made enemies along the way…
- You're about to give a speech in public
- Someone sitting in the audience discreetly presses a button on a transmitter
- That transmitter sends a command to your pacemaker telling it to deliver a shock to your heart
- Things don't end well for you…
- The attacker strolls out of the room anonymously

What is the problem here?

The Internet of Things (IoT) can expose devices to attack!

Pacemaker device

Device programmer

- Early pacemakers did not authenticate commands[1]
- Anyone could send a wireless command to the pacemaker to shock the heart! (or rundown the battery)
- The U.S. Vice President Cheney had one in the past (his was modified[2])
- This problem has been fixed in general now
- Take away message: don't trust messages that come over the Internet, there are bad guys out there!
- Once we know more about how the Internet works, we will spend a lot of time on security

[1] https://news.umich.edu/holes-found-in-report-on-st-jude-medical-device-security/

[2] https://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview

Agenda

1. Intro and course overview

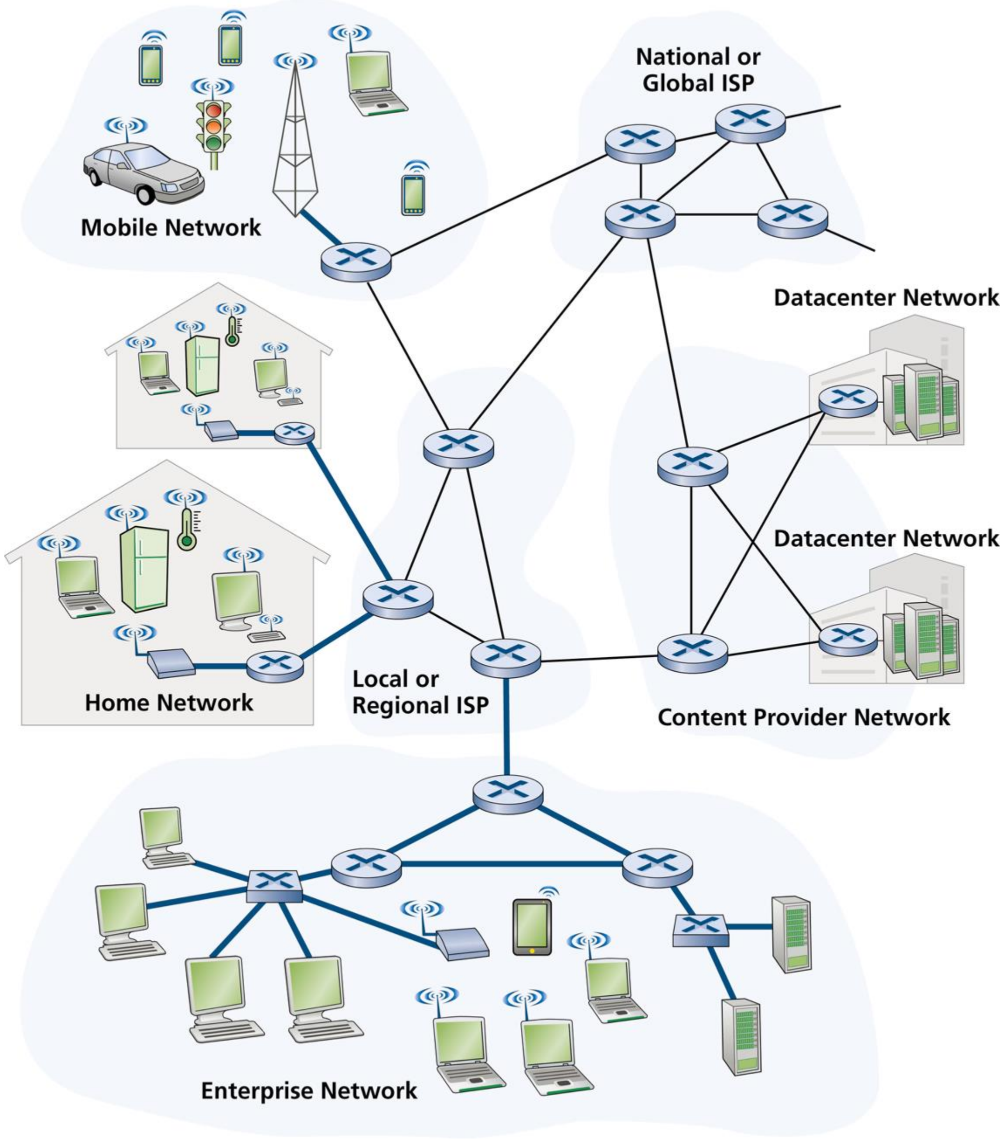
2. Networking creates new possibilities and new challenges

3. What is the Internet anyway?

4. How are hosts connected?

5. Connecting ECSC (illustrative)

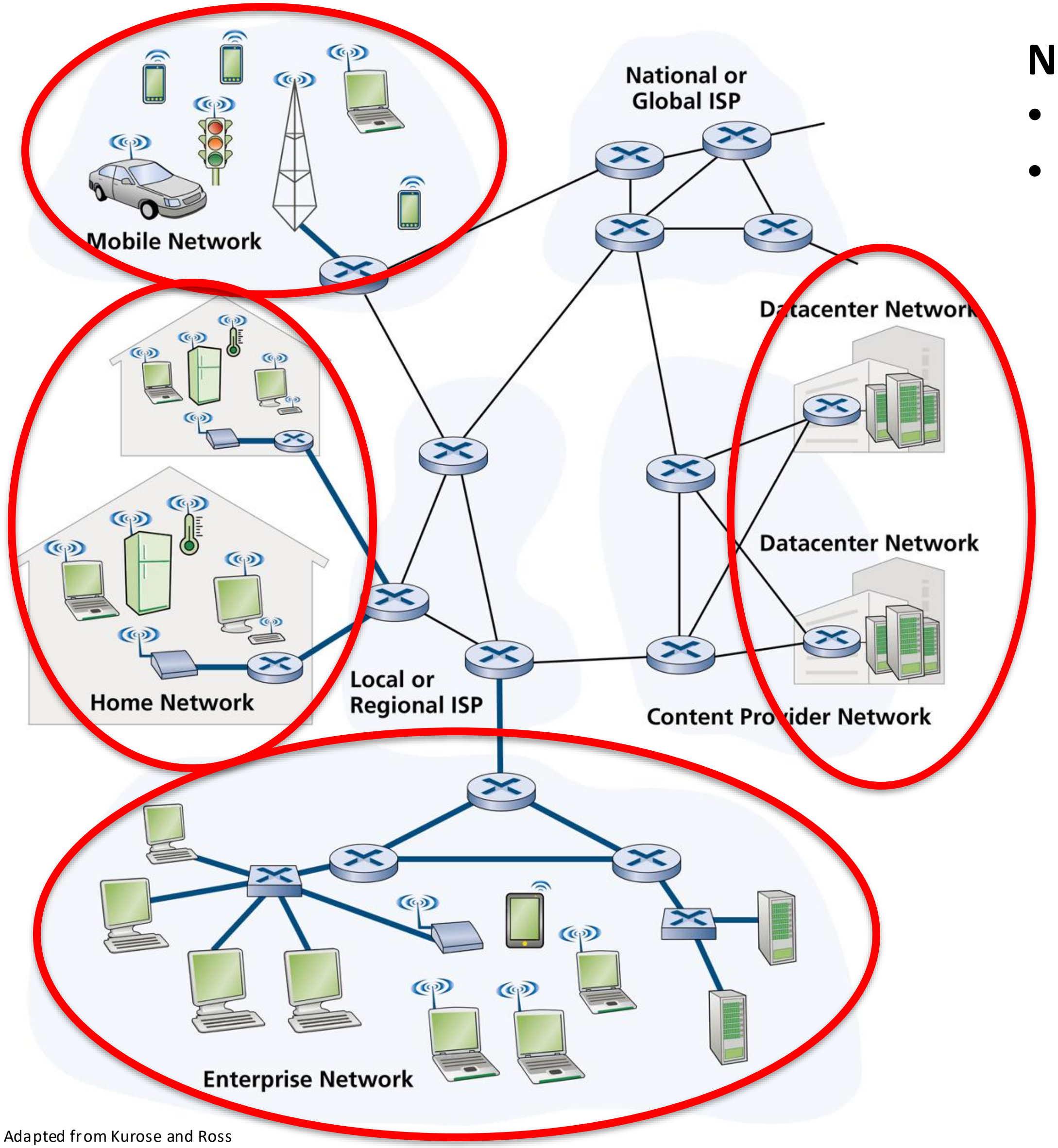
The Internet is a “network of networks”



Adapted from Kurose and Ross

- Devices on the Internet run network applications to communicate with each other
- We call these devices *hosts* and they are commonly either:
  - *Clients* (laptops, phones, tablets IoT devices)
  - *Servers* (often powerful machines located in data centers)
- Hosts connect to the Internet via *Internet Service Providers (ISPs)* that provide Internet access, normally for a fee
- Millions of ISPs are connected to form the *Internet*
- Hosts communicate over the Internet using predefined *protocols* such as the *Internet Protocol (IP)* and *Transmission Control Protocol (TCP)*

The Internet is a "network of networks"

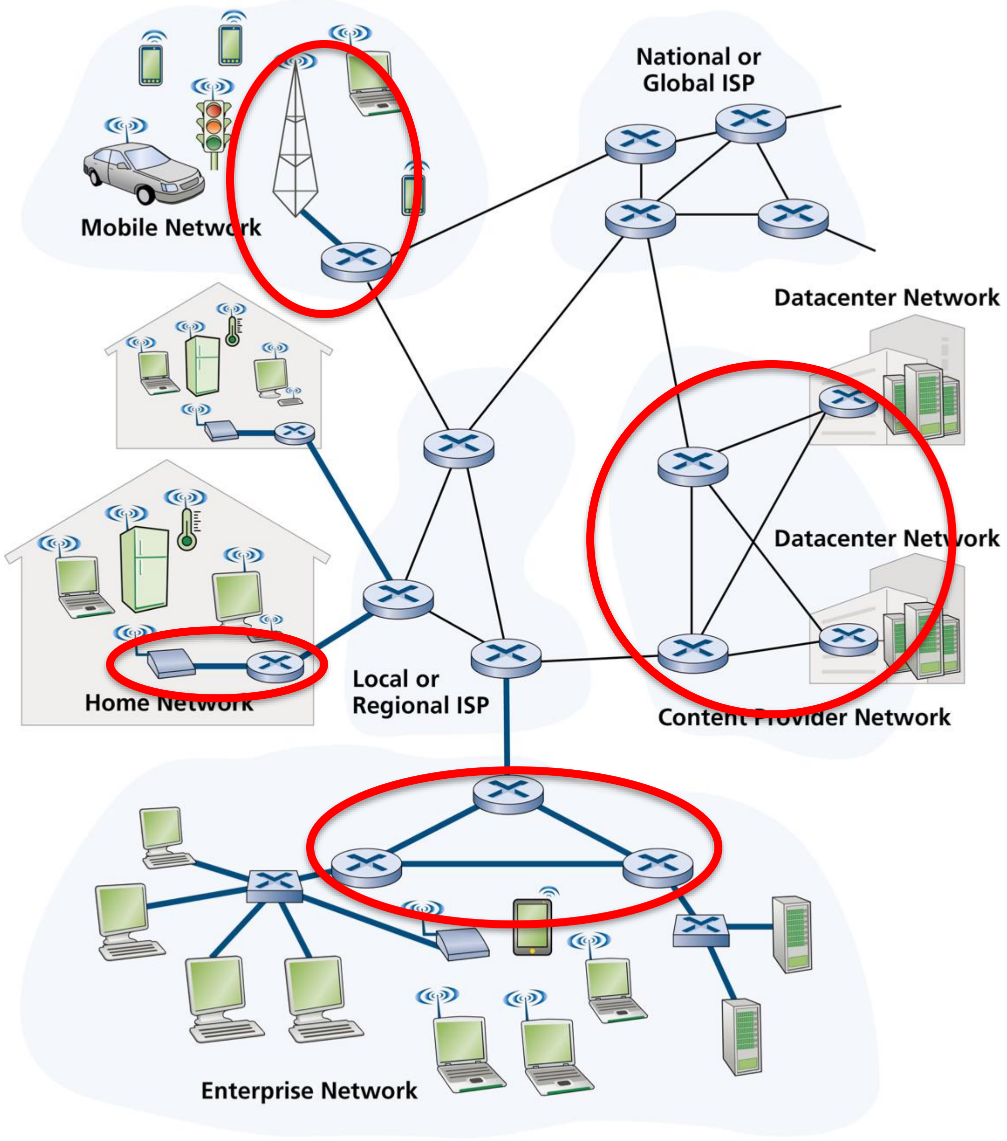


Network edge

- Hosts: clients and servers
- Servers: typically in data centers

Adapted from Kurose and Ross

The Internet is a “network of networks”



Adapted from Kurose and Ross

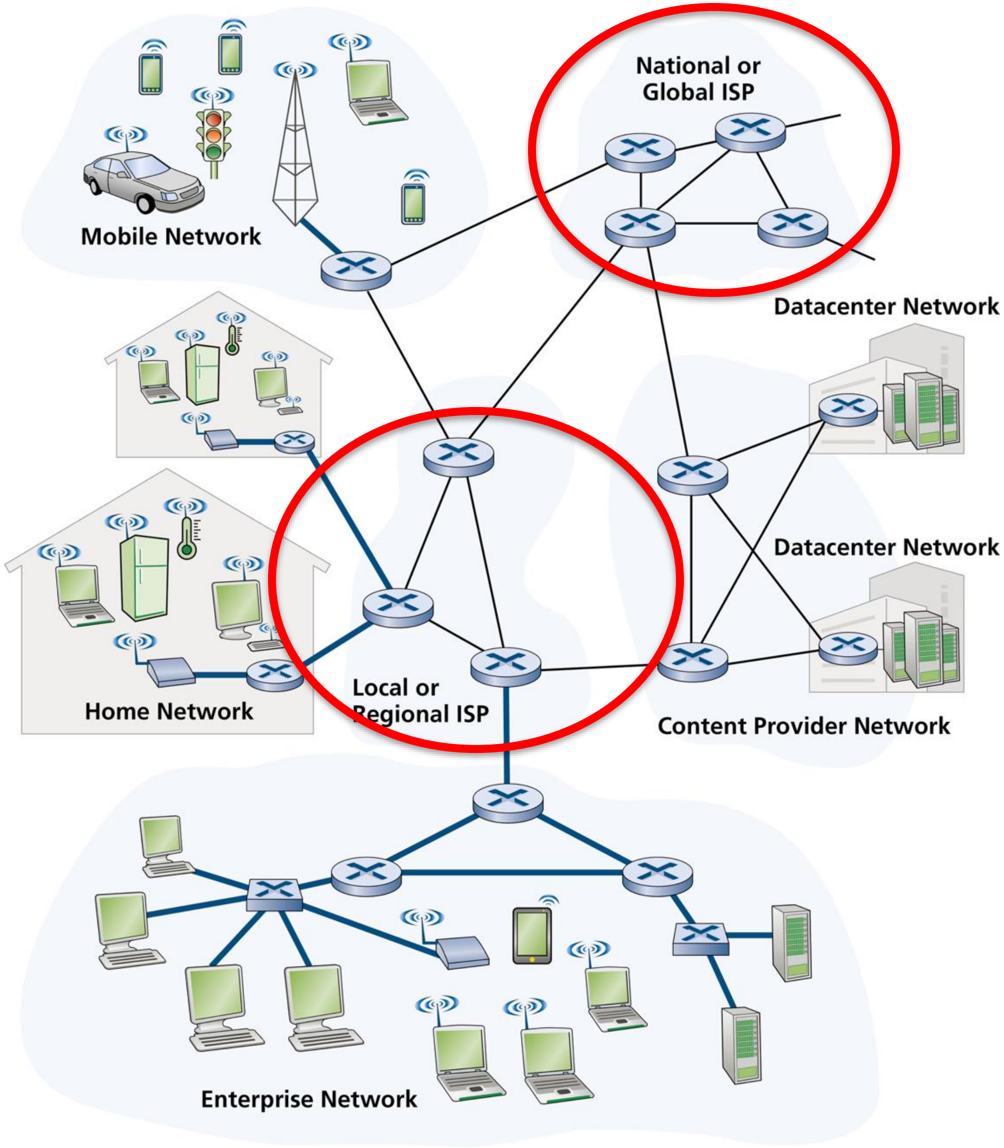
Network edge

- Hosts: clients and servers
- Servers: typically in data centers

Access networks

- Give access to the Internet
- Wired
- Wireless communication links
  - Wi-Fi
  - Cellular
  - LoRa

The Internet is a “network of networks”



Network edge

- Hosts: clients and servers
- Servers: typically in data centers

Access networks

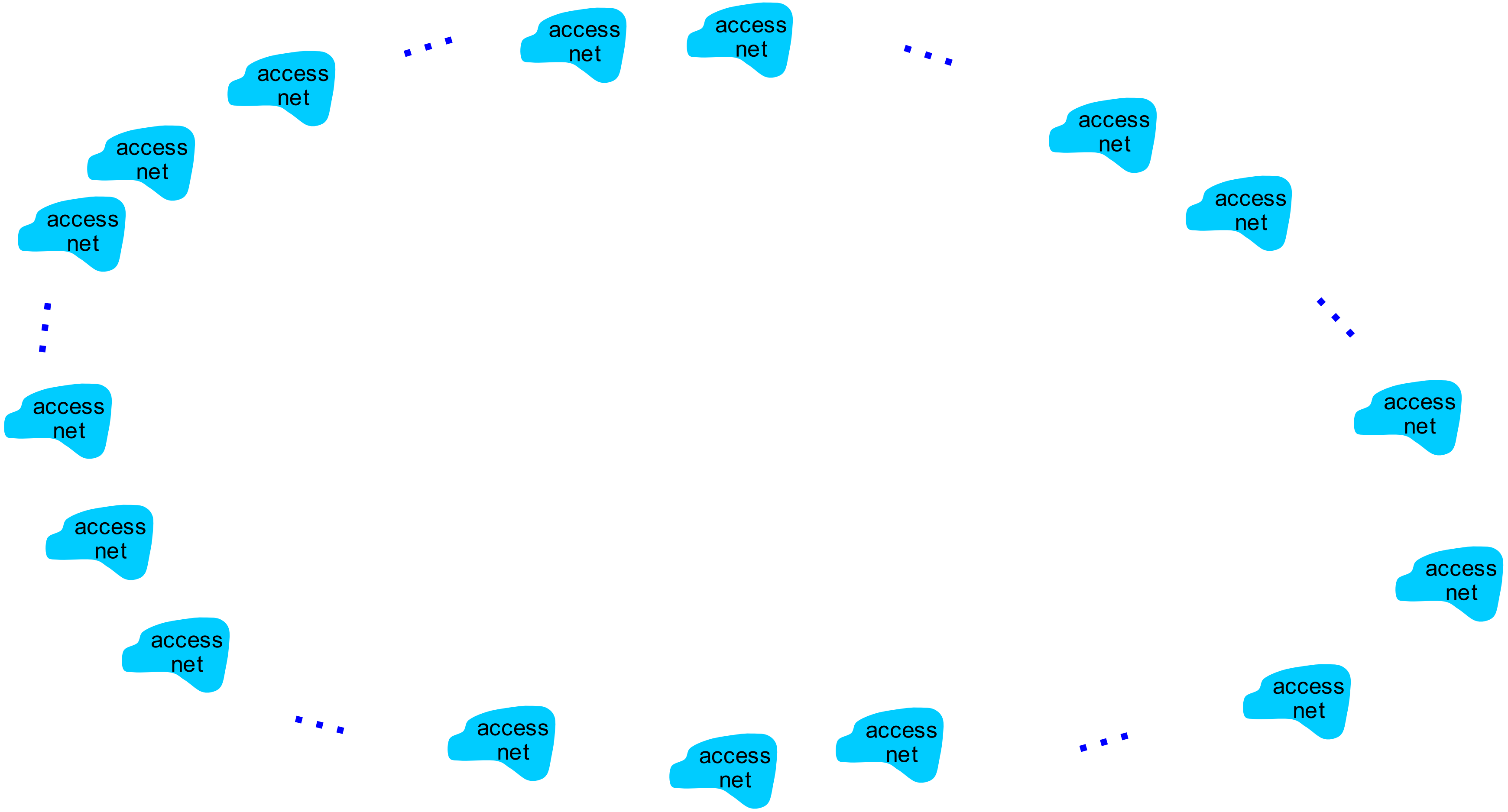
- Give access to the Internet
- Wired
- Wireless communication links
  - Wi-Fi
  - Cellular
  - LoRa

Network core

- Interconnected routers
- Forms network or networks
- Local or regional ISPs connected with national or global ISPs

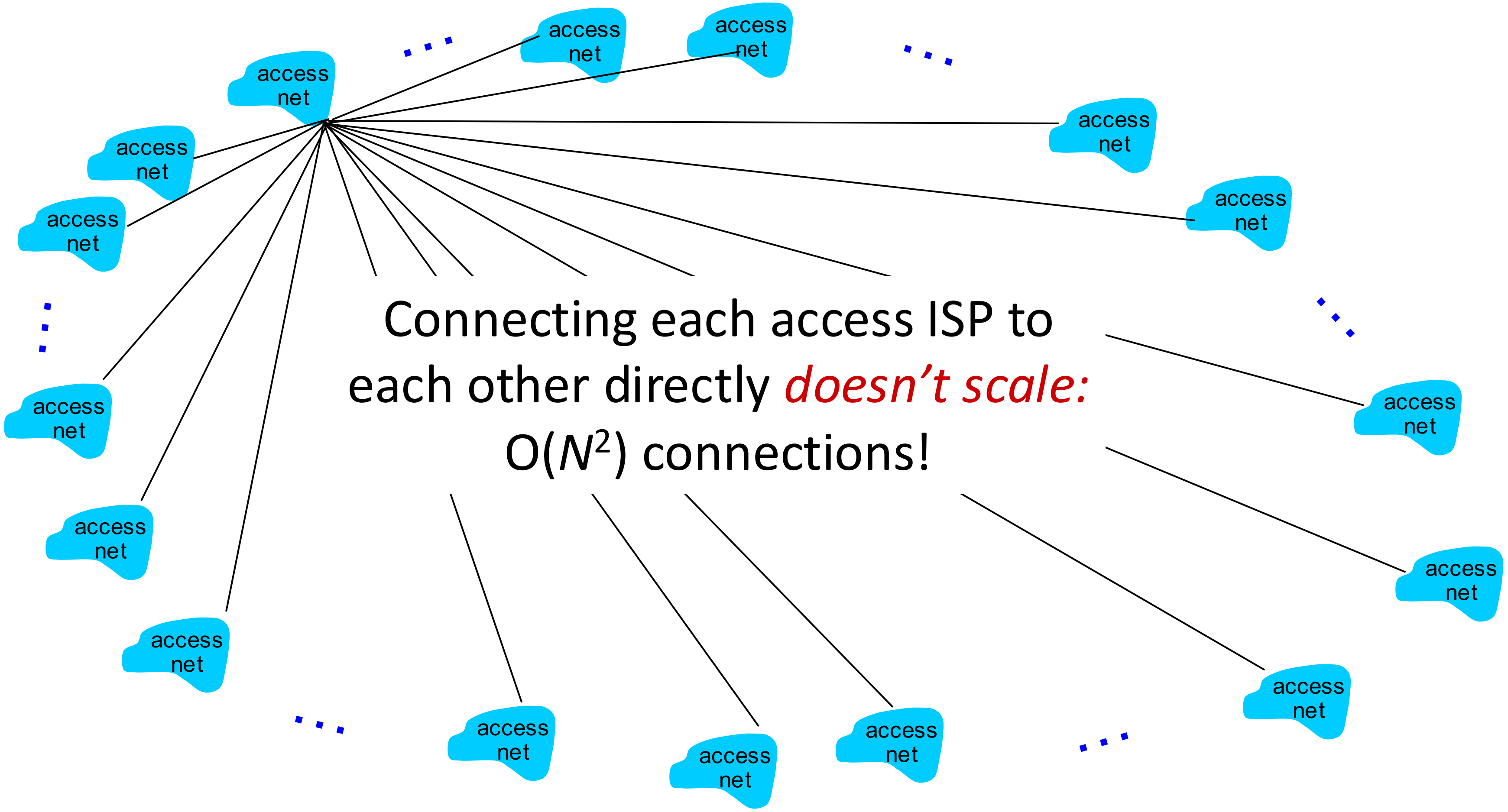
Adapted from Kurose and Ross

Question: Given millions of Access ISPs, how to connect them?



Adapted from Kurose and Ross

Interconnecting each Access ISP with every other Access ISP doesn't scale



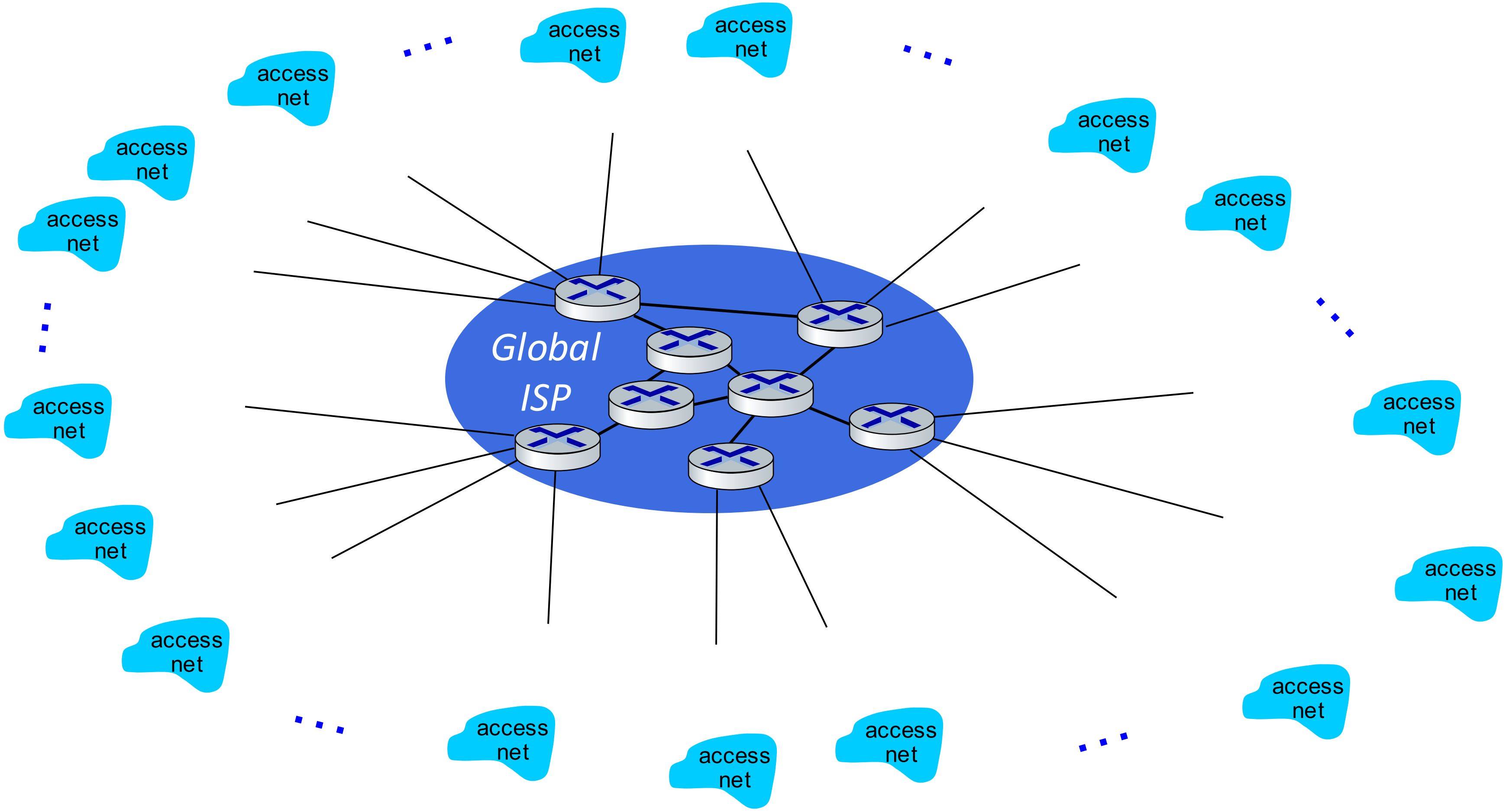
Connecting each access ISP to each other directly *doesn't scale:* O(N^2) connections!

Adapted from Kurose and Ross

One option: Connect each Access ISP to one Global ISP and charge for access

The Global ISP must have a router near each access ISP -- costly

Global ISP could charge access ISPs for connectivity



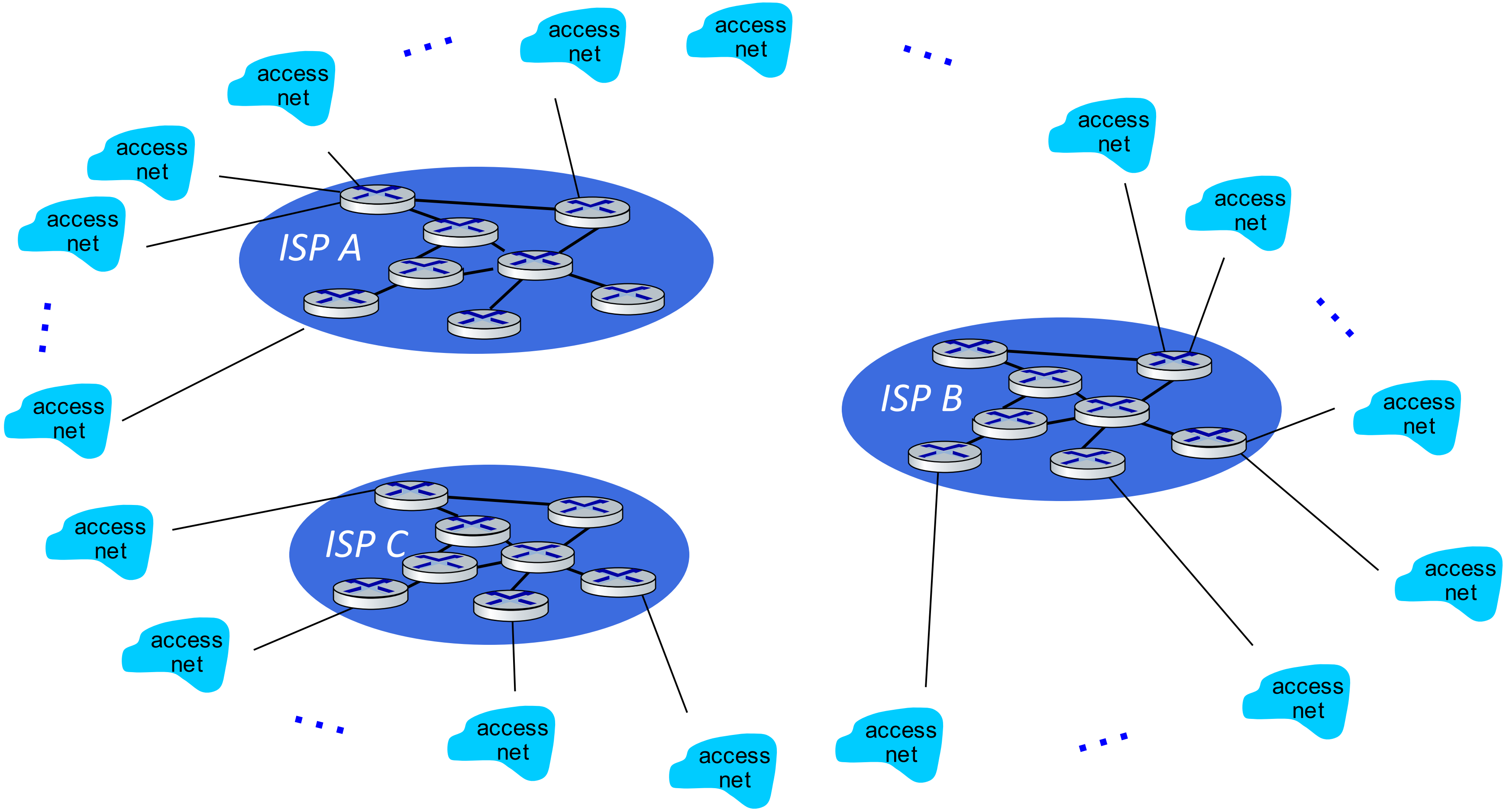
In reality, no organization has this kind of global reach in every city around the world!

Adapted from Kurose and Ross

If one Global ISP is profitable, there will be competition and the network fragments

Tier-1 ISPs charge Access ISPs for access to their network

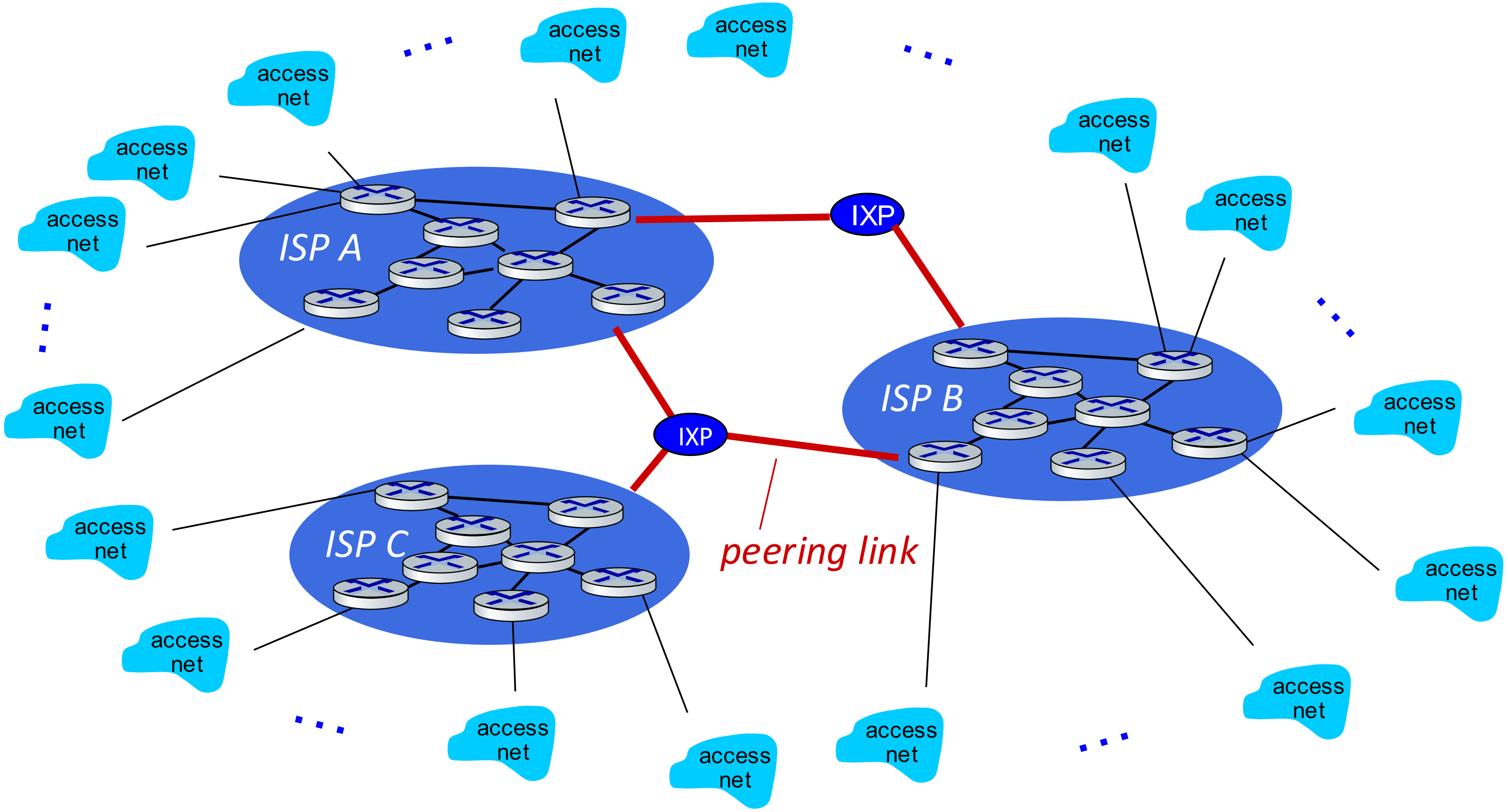
But there would likely be multiple Tier-1 ISPs around the world



Adapted from Kurose and Ross

Instead, Internet Exchange Points (IXPs) connect ISPs

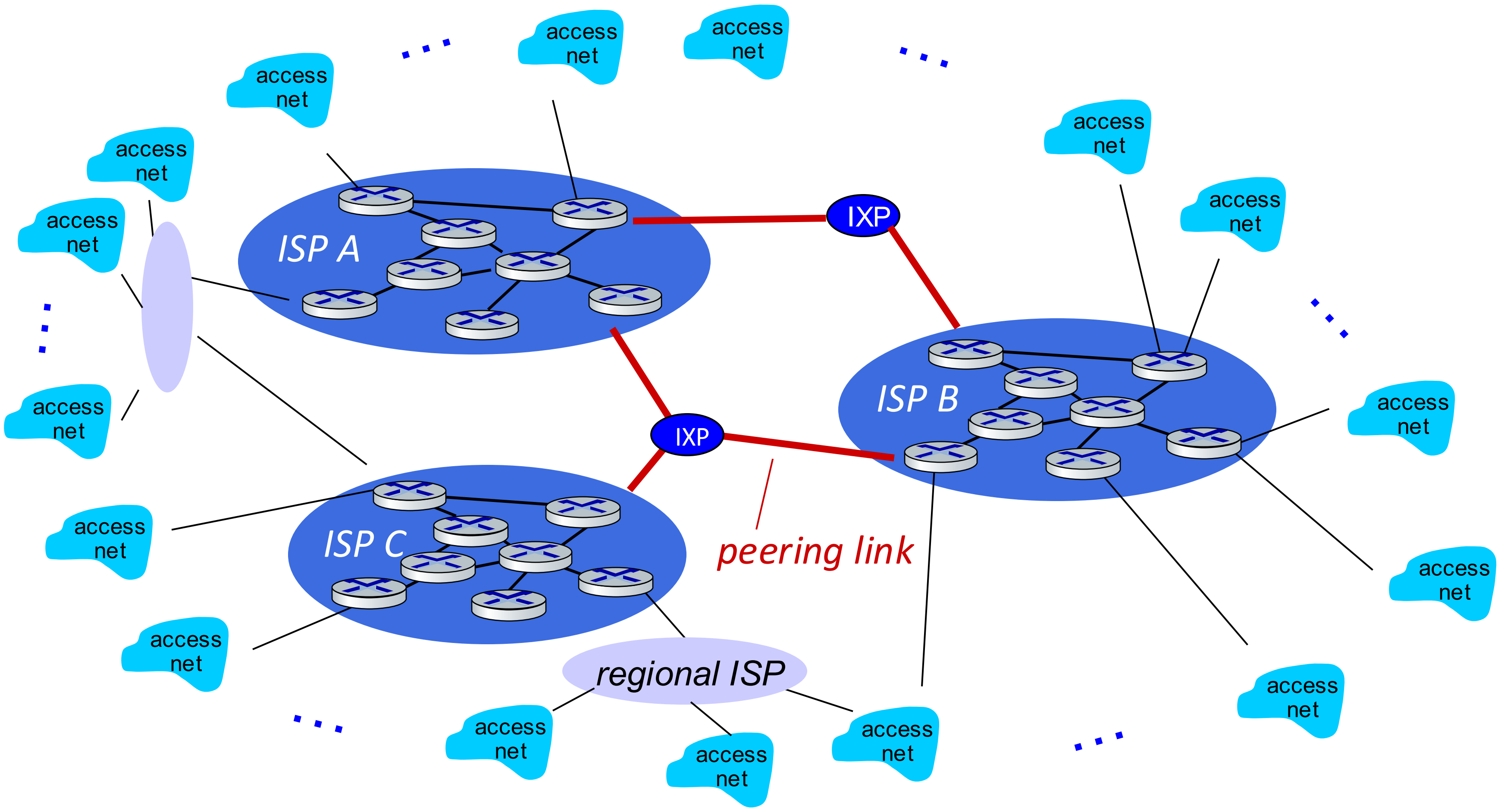
There are approximately a dozen Tier-1 ISPs including Level 3, AT&T, Sprint, and NTT



Adapted from Kurose and Ross

Regional ISPs extend Tier-1 ISPs reach

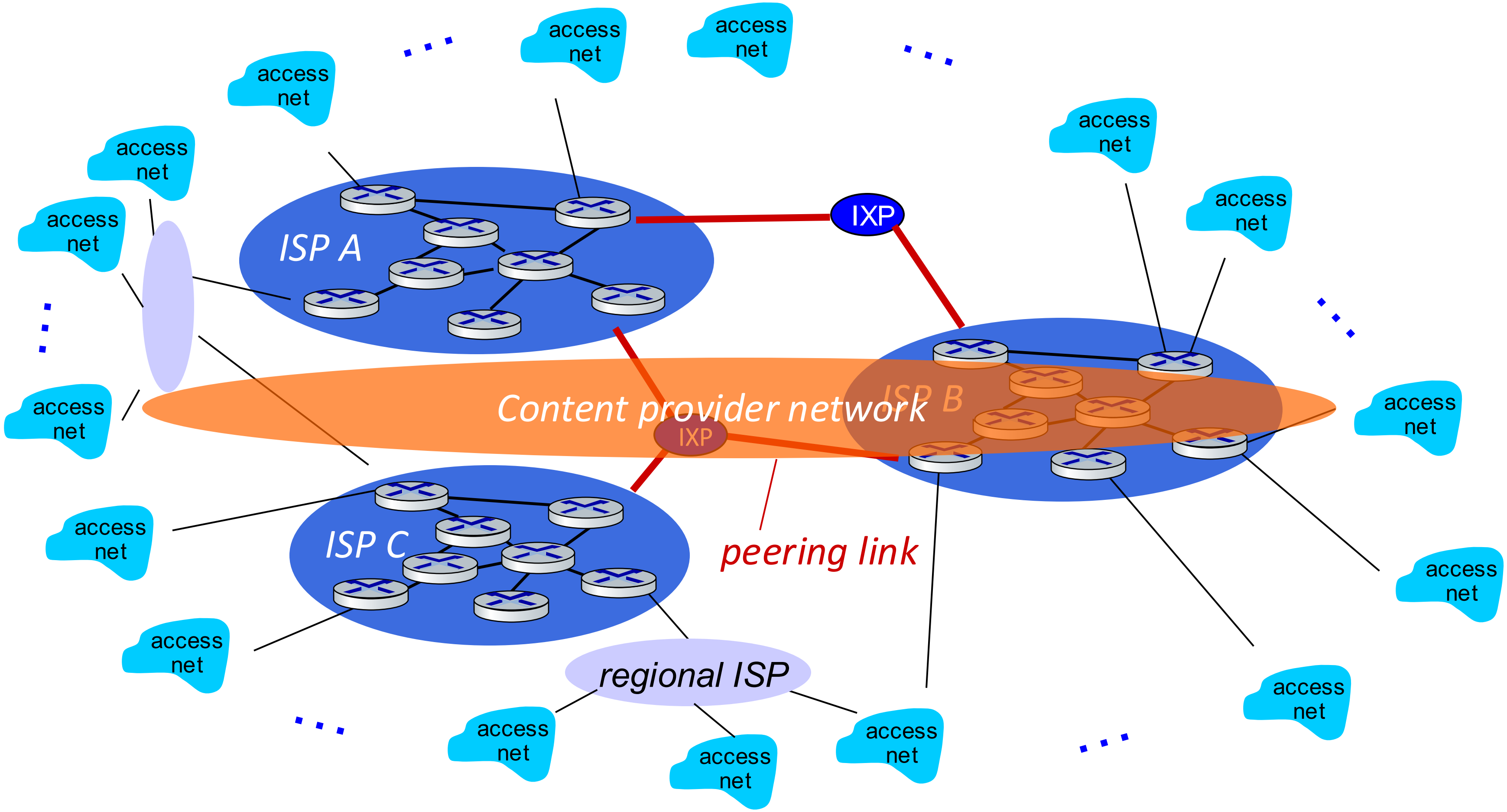
There are approximately a dozen Tier-1 ISPs including Level 3, AT&T, Sprint, and NTT



Adapted from Kurose and Ross

Content providers may run their own networks to bring content close to users

Companies like Google, Microsoft, and Akamai bring content close to users with Content Delivery Networks (CDNs)

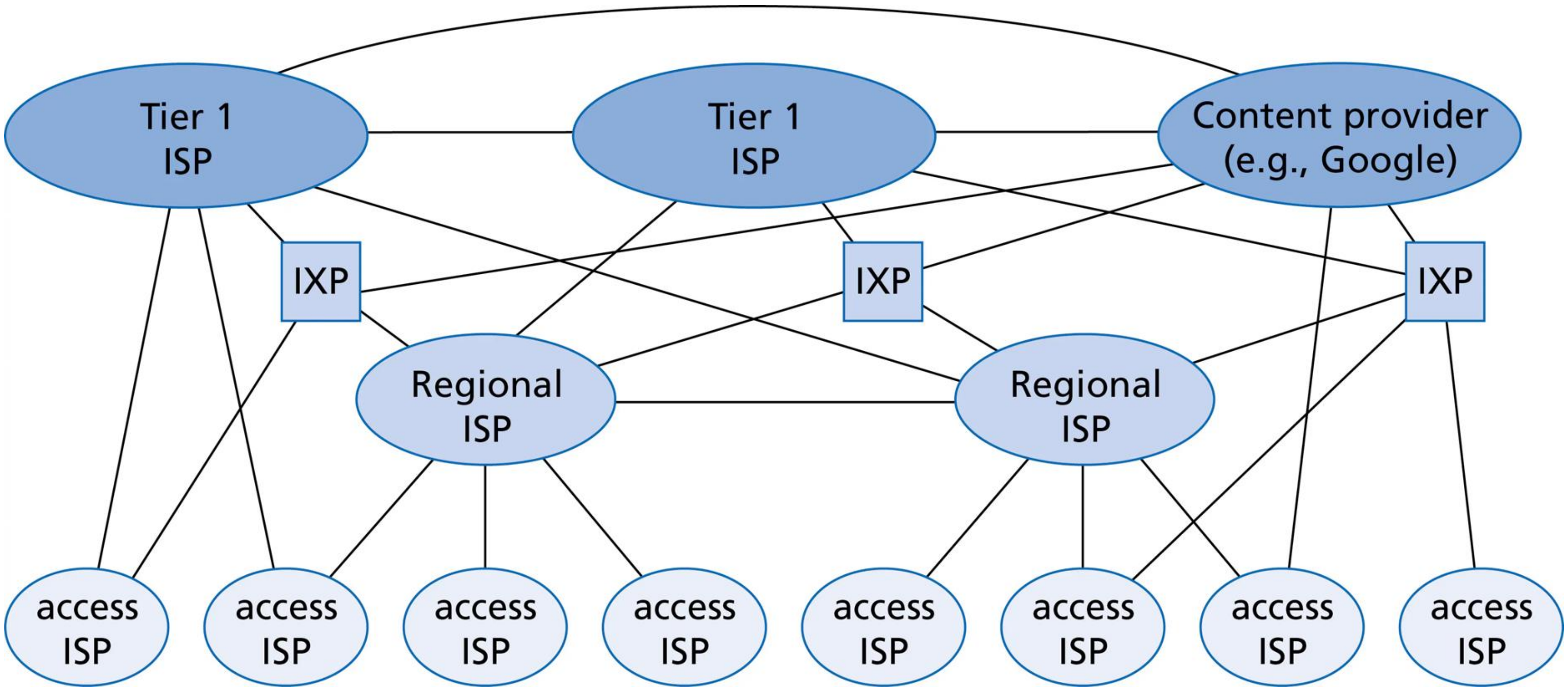


Adapted from Kurose and Ross

To achieve global coverage, today’s Internet is a mixture of many components

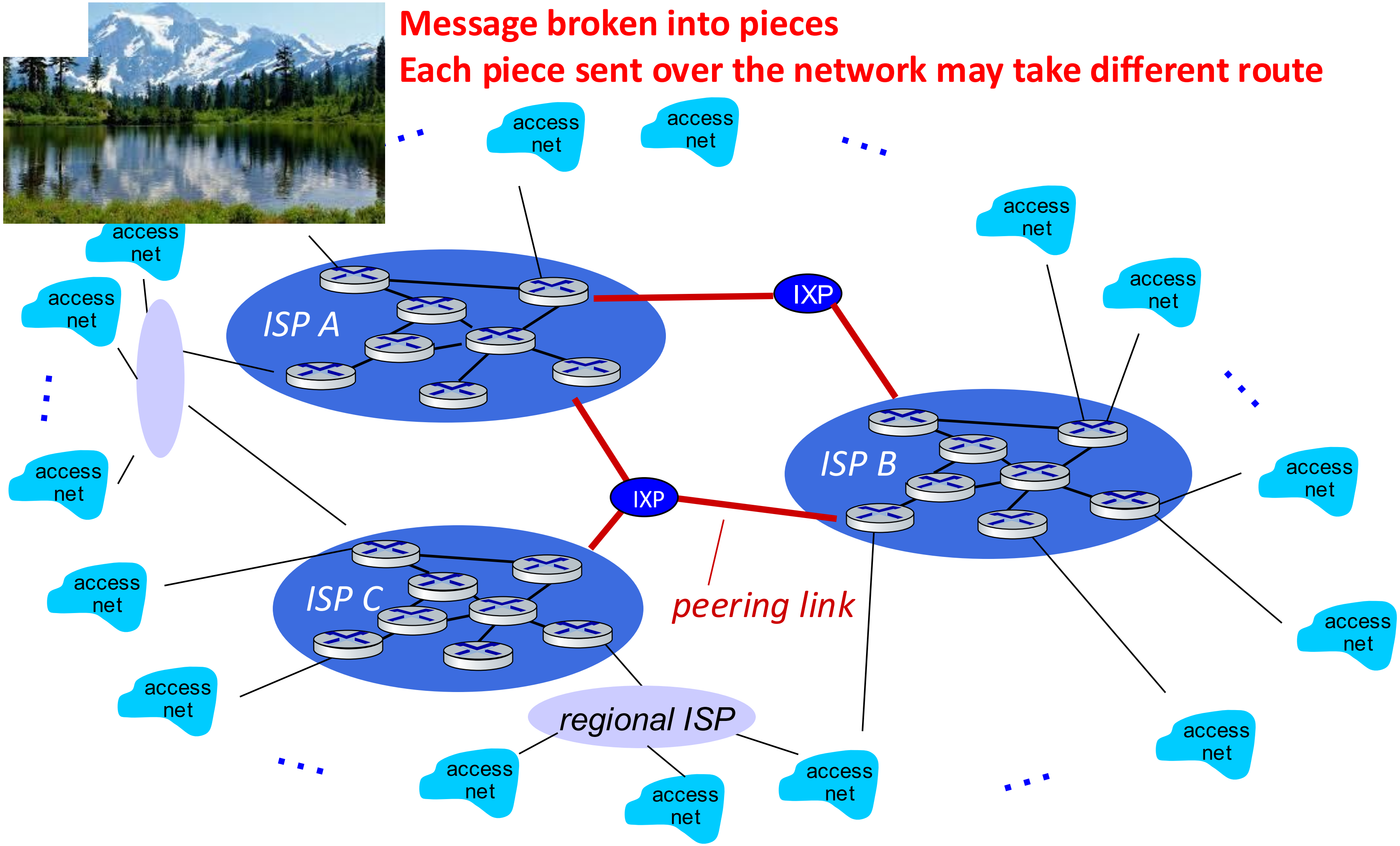
The Internet consists of about a dozen Tier-1 ISPs and hundreds of thousands of lower-tier ISPs, along with content providers that connect their data centers to the Internet

ISPs are diverse in their coverage areas; some span multiple continents and oceans, other are more limited in geographic coverage



Adapted from Kurose and Ross

Messages are broken into many pieces that travel the Internet independently

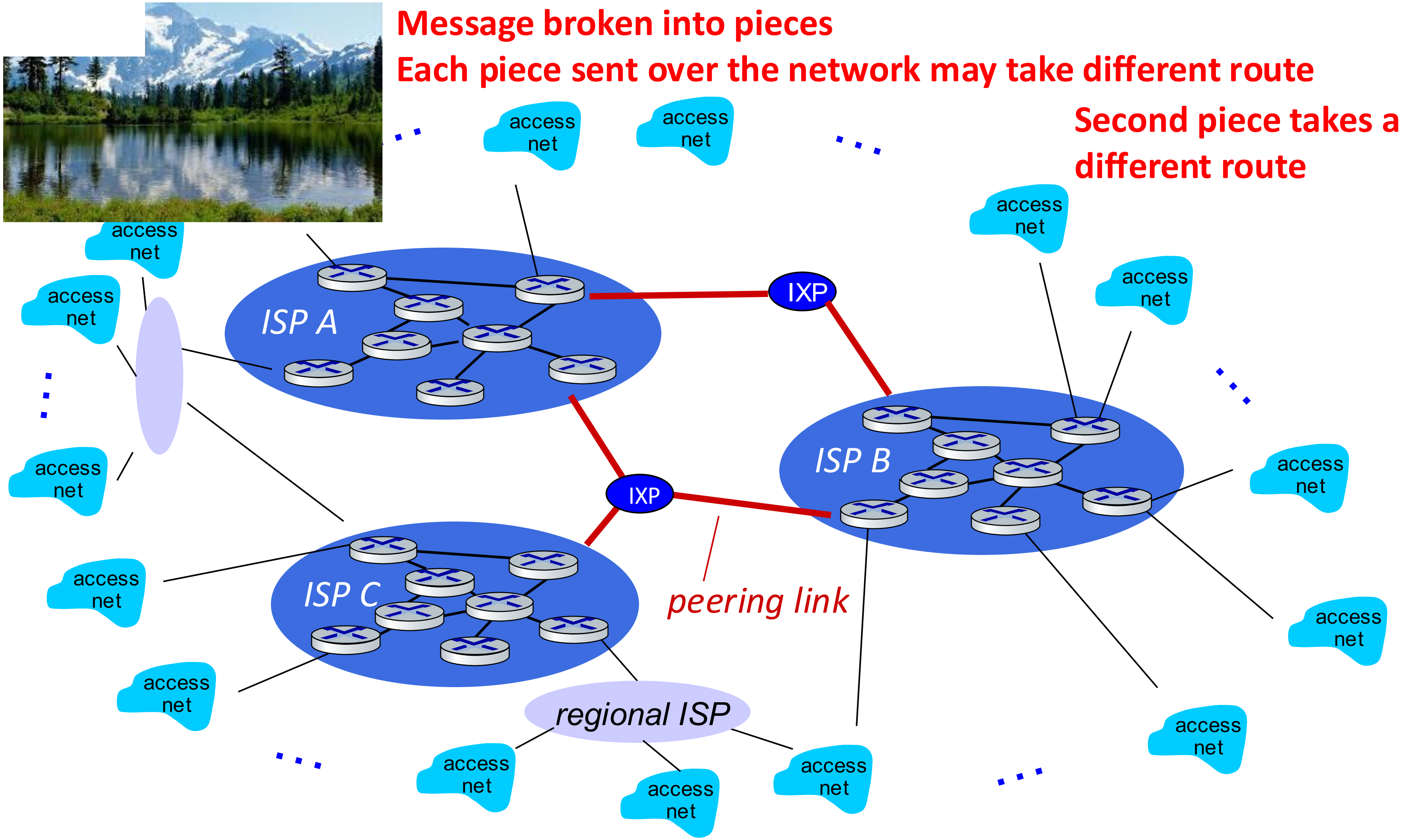


Message broken into pieces

Each piece sent over the network may take different route

Adapted from Kurose and Ross

Messages are broken into many pieces that travel the Internet independently



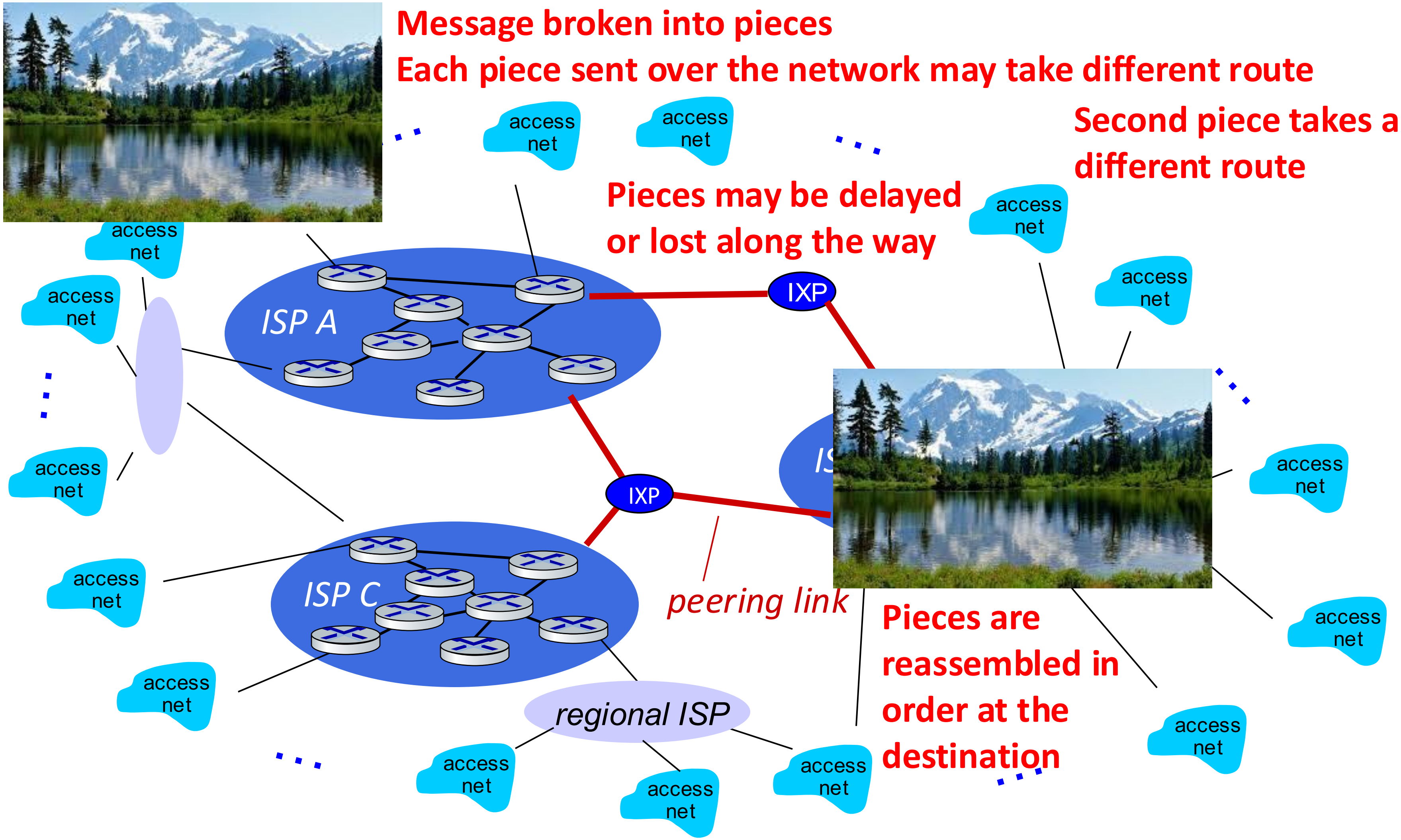
Message broken into pieces

Each piece sent over the network may take different route

Second piece takes a different route

Adapted from Kurose and Ross

Messages are broken into many pieces that travel the Internet independently



Message broken into pieces

Each piece sent over the network may take different route

Second piece takes a different route

Pieces may be delayed or lost along the way

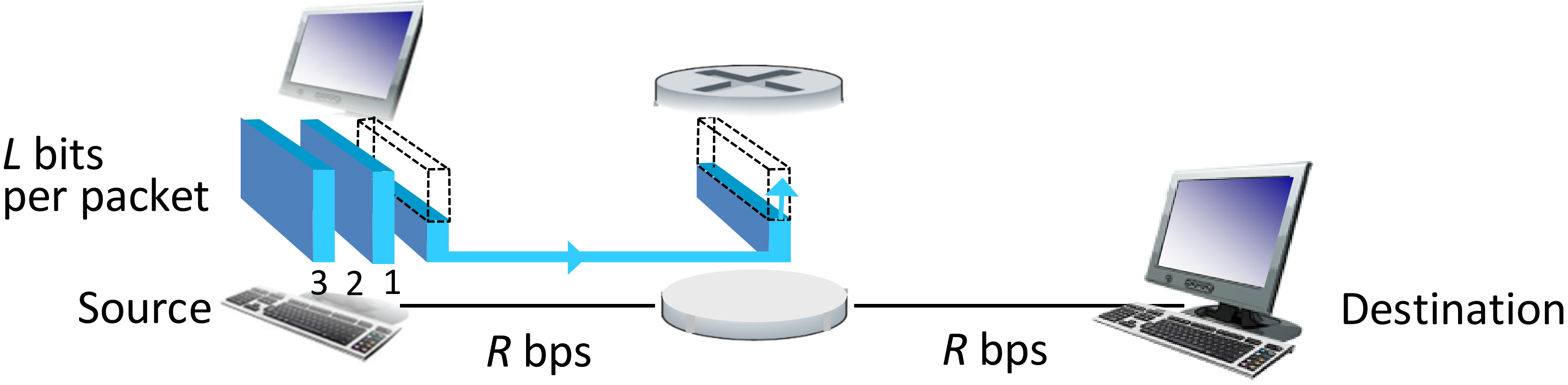
Pieces are reassembled in order at the destination

Adapted from Kurose and Ross

Question

Why can packets sometimes be delayed or lost?

Routers use a store and forward approach



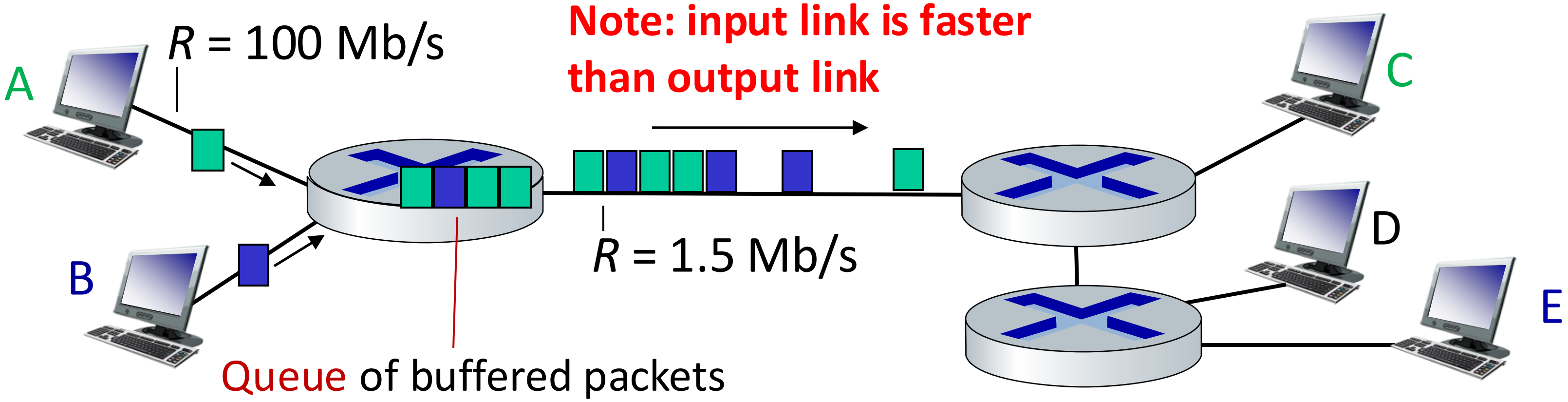
- Packet transmission delay: takes *L*/*R* seconds to transmit (send) *L*-bit packet into link at *R* bps
- *Store and forward: entire* packet must arrive at router before it can be transmitted on next link

One-hop numerical example:

- *L* = 10 Kbits
- *R* = 100 Mbps
- One-hop transmission delay = 0.1 msec

Adapted from Kurose and Ross

Packets are buffered if data arrives too quickly for the outbound link to serve



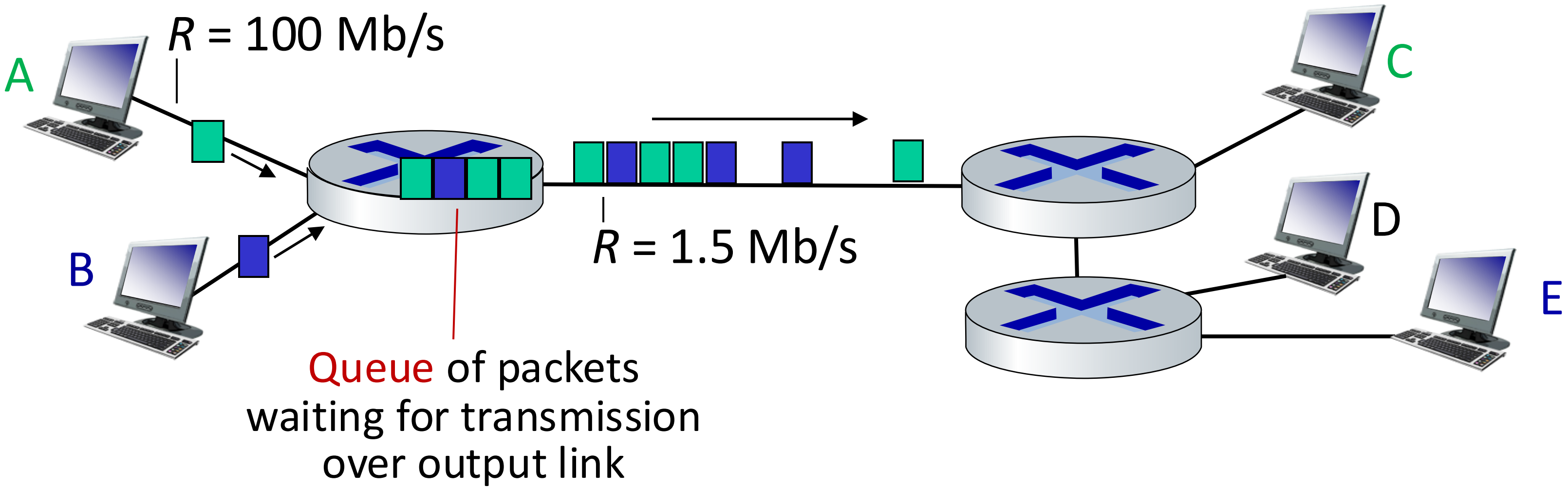
Note: input link is faster than output link

Queue of buffered packets waiting for transmission over slower output link

Queueing occurs when work arrives faster than it can be serviced:

Adapted from Kurose and Ross

Packet loss occurs when buffers fill



Packet queuing and loss: if arrival rate (in bps) to link exceeds transmission rate (bps) of link for some period of time:

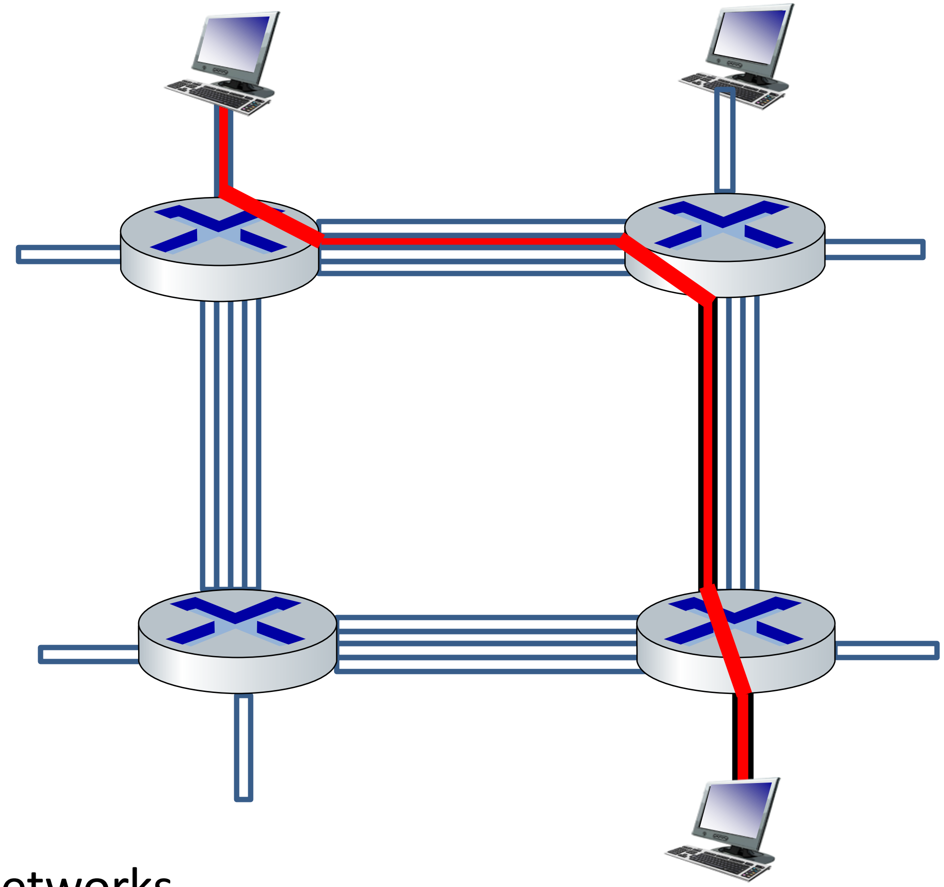
- Packets will queue, waiting to be transmitted on output link
- Packets can be dropped (lost) if memory (buffer) in router fills up

Adapted from Kurose and Ross

Circuit switching is an alternative to packet switching

End-end resources allocated to, reserved for "call" between source and destination

- 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)



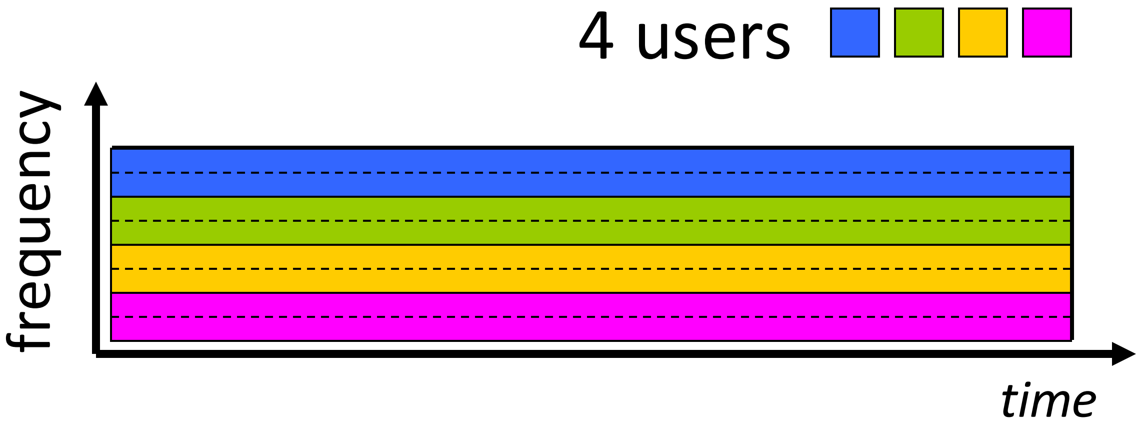
Commonly used in traditional telephone networks

Adapted from Kurose and Ross

Circuit switch commonly uses either FDM or TDM

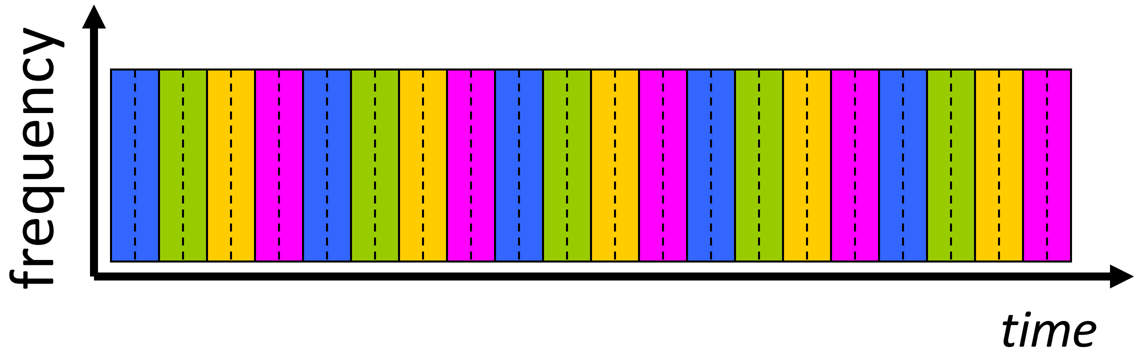
Frequency Division Multiplexing (FDM)

- Optical, electromagnetic frequencies divided into (narrow) frequency bands
- Each call allocated its own band, can transmit at max rate of that narrow band



Time Division Multiplexing (TDM)

- Time is divided into slots
- Each call transmit only during its assigned slot



Adapted from Kurose and Ross

Packet switching vs circuit switching

- Packet switching is great for “bursty” data – sometimes has data to send, but at other times not
  - Allows resource sharing
  - Simpler, no call setup
- Excessive congestion possible: packet delay and loss due to buffer overflow
  - Protocols needed for reliable data transfer, congestion control
- *Q:* How to provide circuit-like behavior with packet-switching?
  - “It’s complicated.” We’ll study various techniques that try to make packet switching as “circuit-like” as possible

Adapted from Kurose and Ross

Agenda

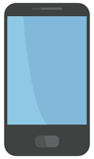
1. Intro and course overview
2. Networking creates new possibilities and new challenges
3. What is the Internet anyway?
4. How are hosts connected?
5. Connecting ECSC (illustrative)

Devices connect to other computers in different ways

Desktop

Laptop

Tablet


Phone

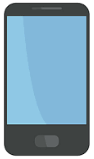
- Each device might have multiple ways to connect to other computers
  - Wired (Ethernet with RJ45 connector and Cat 5, 6, or 7 cable, maybe fiber optic cable)
  - Wireless (Wi-Fi, Bluetooth, cellular)
- Each connection is controlled by a Network Interface Card (NIC)
- Each NIC has a unique 48-byte Media Access Controller (MAC) address such as 5C:E9:1E:AA:BB:CC. MACs typically do not change values. We will soon call this Layer 2

Wired connections are typically in desktops computers or networking gear

Desktop

Laptop

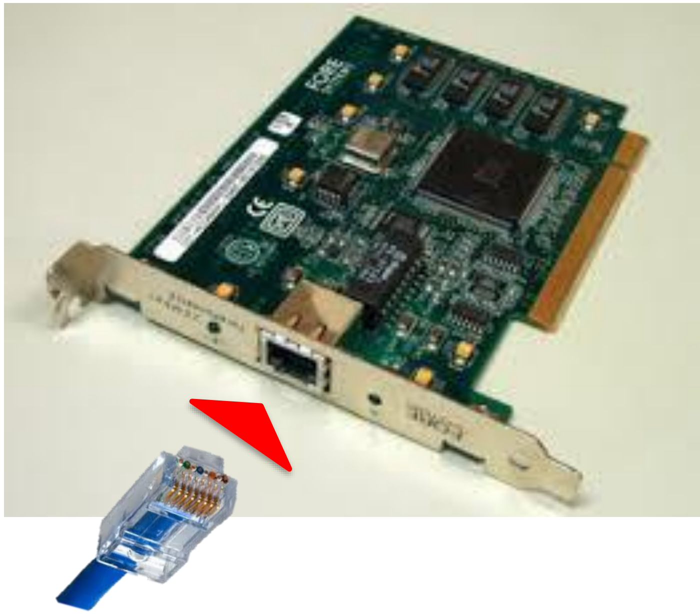
Tablet



Phone

- Each device might have multiple ways to connect to other computers
  - Wired (Ethernet with RJ45 connector and Cat 5, 6, or 7 cable, maybe fiber optic cable)
  - Wireless (Wi-Fi, Bluetooth, cellular)
- Each connection is controlled by a Network Interface Card (NIC)
- Each NIC has a unique 48-byte Media Access Controller (MAC) address such as 5C:E9:1E:AA:BB:CC. MACs typically do not change values. We will soon call this Layer 2

These days wired connections are typically in desktop computers, or in servers, hubs, switches, and routers

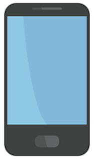


Wired connections are typically in desktops computers or networking gear

Desktop

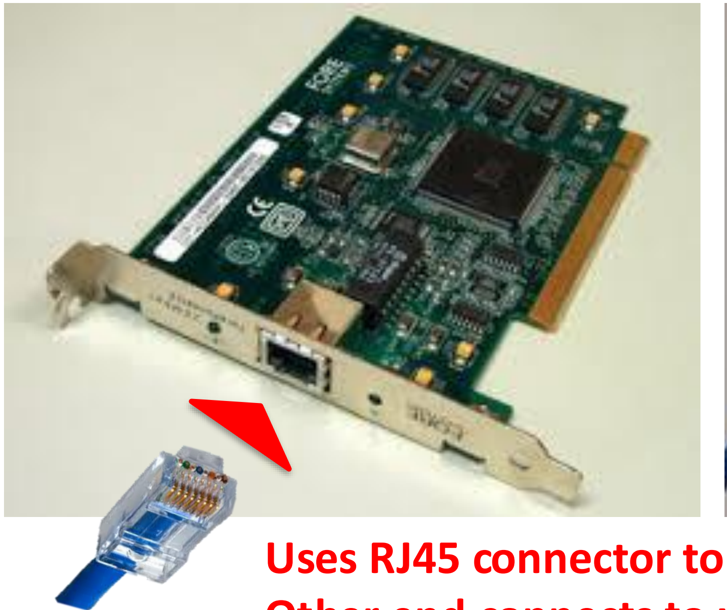
Laptop

Tablet



Phone

- Each device might have multiple ways to connect to other computers
  - Wired (Ethernet with RJ45 connector and Cat 5, 6, or 7 cable, maybe fiber optic cable)
  - Wireless (Wi-Fi, Bluetooth, cellular)
- Each connection is controlled by a Network Interface Card (NIC)
- Each NIC has a unique 48-byte Media Access Controller (MAC) address such as 5C:E9:1E:AA:BB:CC. MACs typically do not change values. We will soon call this Layer 2



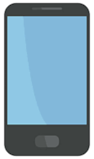
Uses RJ45 connector to Cat 5, 6, 7, or 8 cables
Other end connects to wall outlet

Mobile devices must use wireless!

Desktop

Laptop

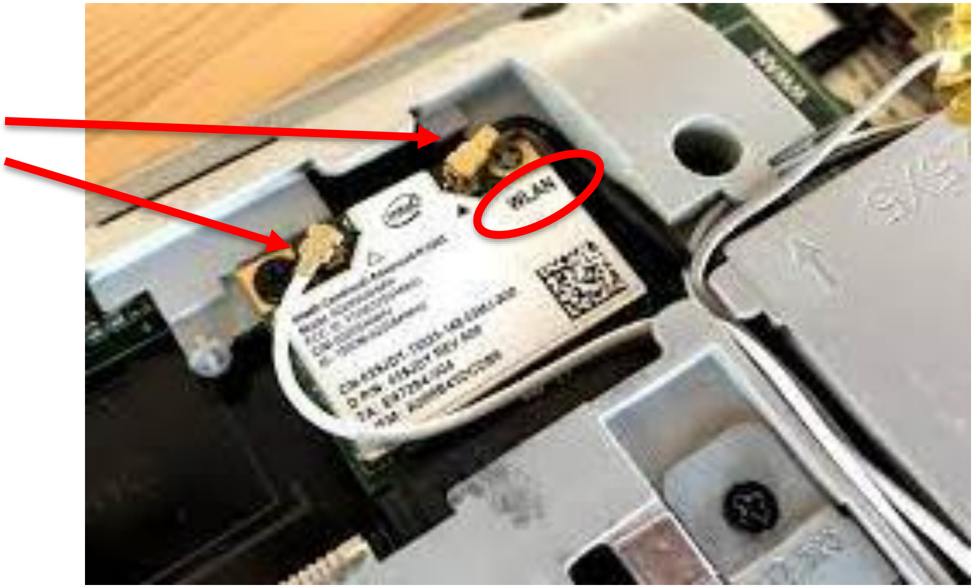
Tablet


Phone

- Each device might have multiple ways to connect to other computers
  - Wired (Ethernet with RJ45 connector and Cat 5, 6, or 7 cable, maybe fiber optic cable)
  - Wireless (Wi-Fi, Bluetooth, cellular)
- Each connection is controlled by a Network Interface Card (NIC)
- Each NIC has a unique 48-byte Media Access Controller (MAC) address such as 5C:E9:1E:AA:BB:CC. MACs typically do not change values. We will soon call this Layer 2

Modern wireless NICs have multiple antennas

Allows for beamforming where RF is directed toward a particular direction

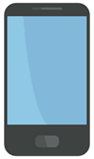


MAC address can tell you the NIC manufacturer

Desktop

Laptop

Tablet



Phone

- Each device might have multiple ways to connect to other computers
  - Wired (Ethernet with RJ45 connector and Cat 5, 6, or 7 cable, maybe fiber optic cable)
  - Wireless (Wi-Fi, Bluetooth, cellular)
- Each connection is controlled by a Network Interface Card (NIC)
- Each NIC has a unique 48-byte Media Access Controller (MAC) address such as 5C:E9:1E:AA:BB:CC. MACs typically do not change values. We will soon call this Layer 2
- Devices with the same make and model (e.g., two iPhone 16s) have different MAC addresses that uniquely identify them
- The first three octets of the MAC identify the manufacturer (e.g., 5C:E9:1E -> Apple Inc)
- These octets are called the Organizationally Unique Identifier (OUI) and are assigned by IEEE
- Wireshark[1] (and others) allow you to enter the OUI and get the manufacturer of the NIC
- One connected, devices are given an IP address (e.g., 123.123.123.123). IP addresses change depending on where the device is connected. We will soon call this Layer 3

What are the security implications (particularly for wireless mobile devices) if each device has its own unique (non-changing) MAC address?

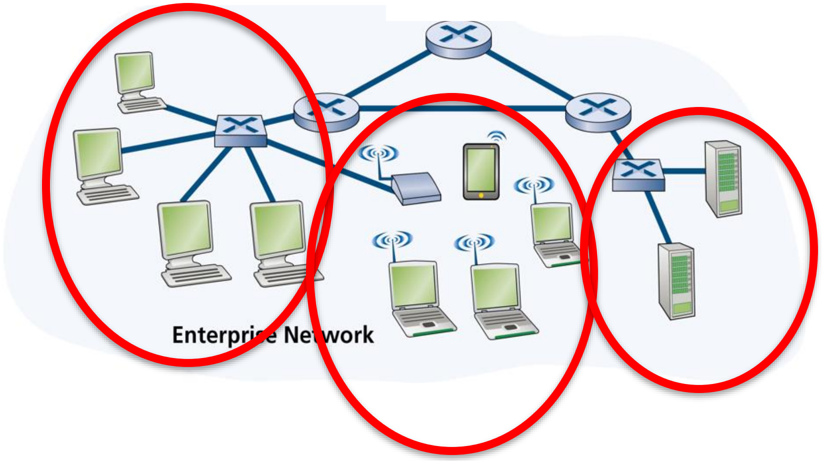
[1] https://www.wireshark.org/tools/oui-lookup.html

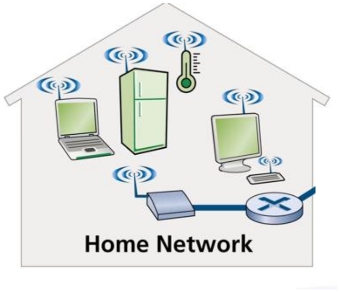
Device are connected into Local Area Networks (LANs)

A Local Area Network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, or office building.

Key Characteristics:

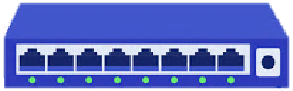
- Covers a small geographic area
- High data transfer rates
- Typically uses Ethernet or Wi-Fi
- Privately owned and managed





Source: Copilot

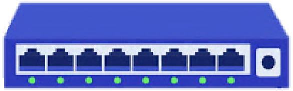
Local Area Network (LAN) devices are connected by hubs, switches, routers, APs



Hub: most basic connecting device

- Broadcasts data to all hub-connected devices
- Outdated for most modern networks due to their inefficiency
- Found mainly in small home LANs

Local Area Network (LAN) devices are connected by hubs, switches, routers, APs



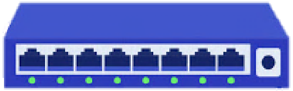
Hub: most basic connecting device

- Broadcasts data to all hub-connected devices
- Outdated for most modern networks due to their inefficiency
- Found mainly in small home LANs

Switch: more intelligent than hubs

- Directs traffic based on MAC addresses
- Improves network performance and creates multiple collision domains

Local Area Network (LAN) devices are connected by hubs, switches, routers, APs



Hub: most basic connecting device

- Broadcasts data to all hub-connected devices
- Outdated for most modern networks due to their inefficiency
- Found mainly in small home LANs

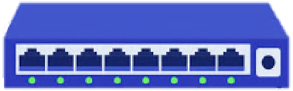
Switch: more intelligent than hubs

- Directs traffic based on MAC addresses
- Improves network performance and creates multiple collision domains

Router: connects networks

- Manages traffic between networks using IP addresses
- Enables internet connectivity
- Can provide additional services such as firewalls and DHCP

Local Area Network (LAN) devices are connected by hubs, switches, routers, APs



Hub: most basic connecting device

- Broadcasts data to all hub-connected devices
- Outdated for most modern networks due to their inefficiency
- Found mainly in small home LANs

Switch: more intelligent than hubs

- Directs traffic based on MAC addresses
- Improves network performance and creates multiple collision domains

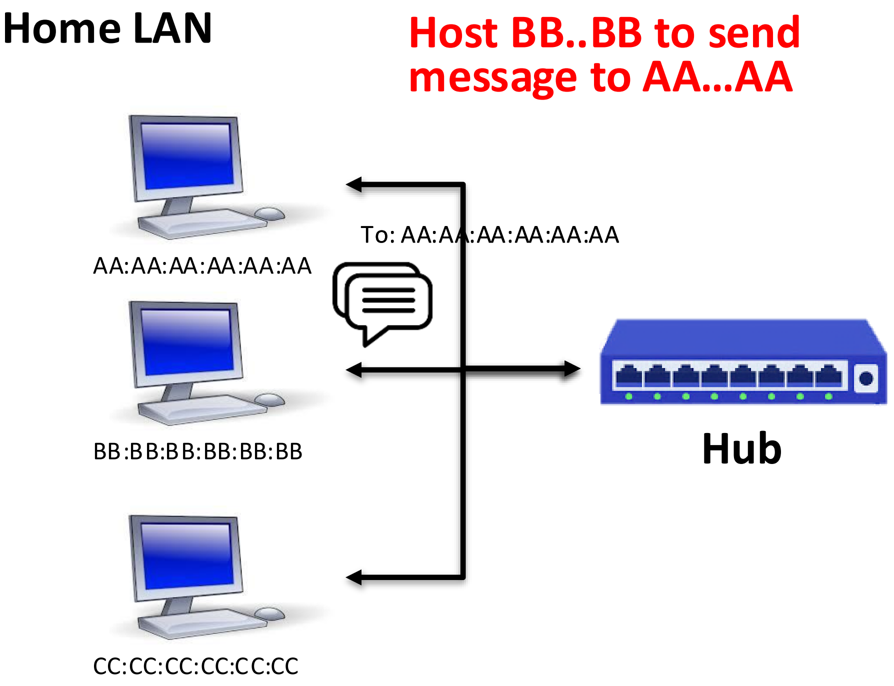
Router: connects networks

- Manages traffic between networks using IP addresses
- Enables internet connectivity
- Can provide additional services such as firewalls and DHCP

Wireless Access Point (AP): connects devices using radio frequencies (RF)

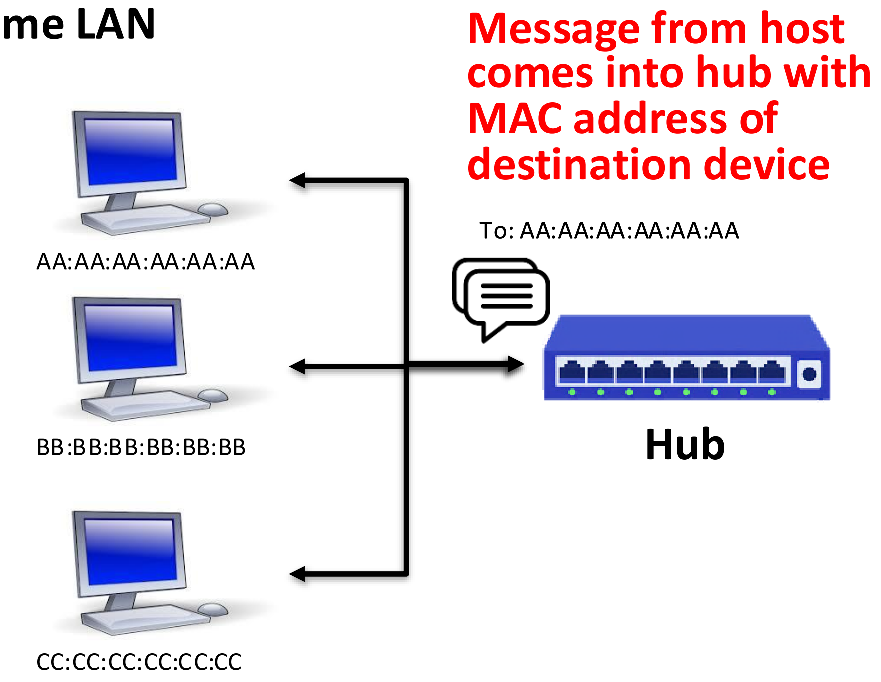
- Commonly acts like a router for mobile and wireless devices

Hubs allow computers in the LAN to communicate with each other



Function: Broadcasts all incoming data to all connected devices, regardless of the destination

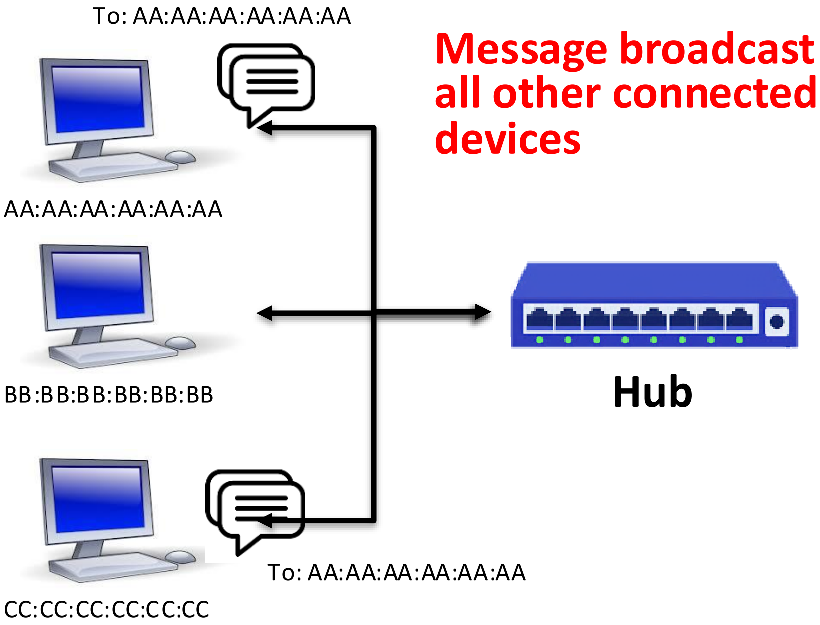
Hubs broadcast message to all devices in the LAN



Function: Broadcasts all incoming data to all connected devices, regardless of the destination

Devices see all traffic, ignore messages not addressed to their MAC address

Home LAN



To: AA:AA:AA:AA:AA:AA

AA:AA:AA:AA:AA:AA

BB:BB:BB:BB:BB:BB

CC:CC:CC:CC:CC:CC

To: AA:AA:AA:AA:AA:AA

Hub

Message broadcast to all other connected devices

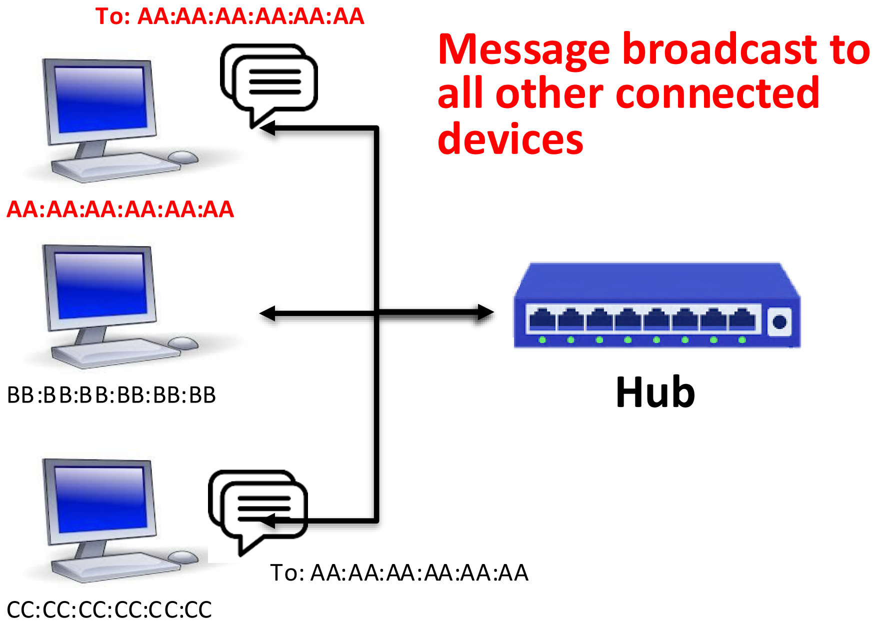
Function: Broadcasts all incoming data to all connected devices, regardless of the destination

All devices see all traffic

Each device looks at MAC address

Devices see all traffic, ignore messages not addressed to their MAC address

Home LAN



To: AA:AA:AA:AA:AA:AA

Message broadcast to all other connected devices

AA:AA:AA:AA:AA:AA

BB:BB:BB:BB:BB:BB

Hub

CC:CC:CC:CC:CC:CC

To: AA:AA:AA:AA:AA:AA

Function: Broadcasts all incoming data to all connected devices, regardless of the destination

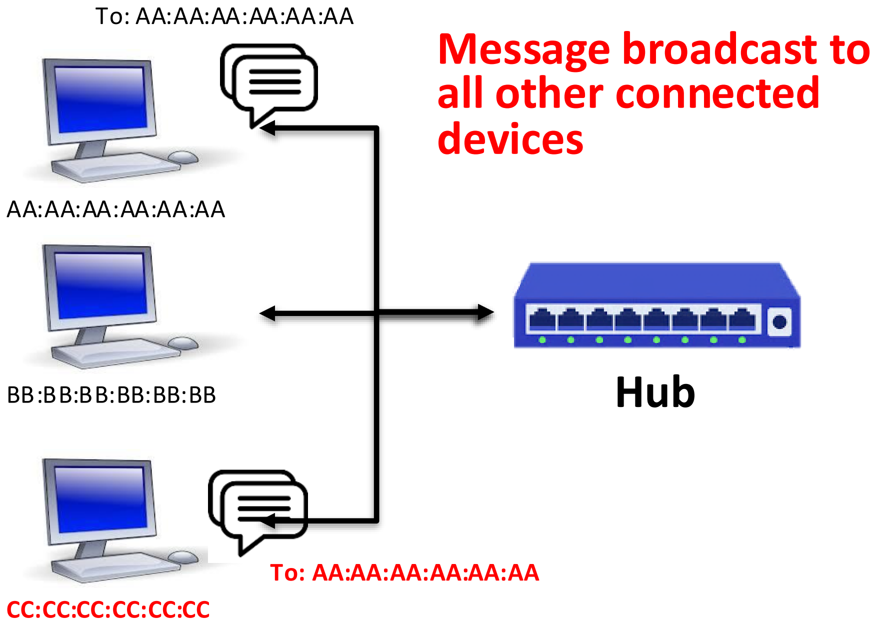
All devices see all traffic

Each device looks at MAC address

Device AA:AA:AA:AA:AA:AA processes message because MAC matches destination MAC

Devices see all traffic, ignore messages not addressed to their MAC address

Home LAN



Message broadcast to all other connected devices

Function: Broadcasts all incoming data to all connected devices, regardless of the destination

All devices see all traffic

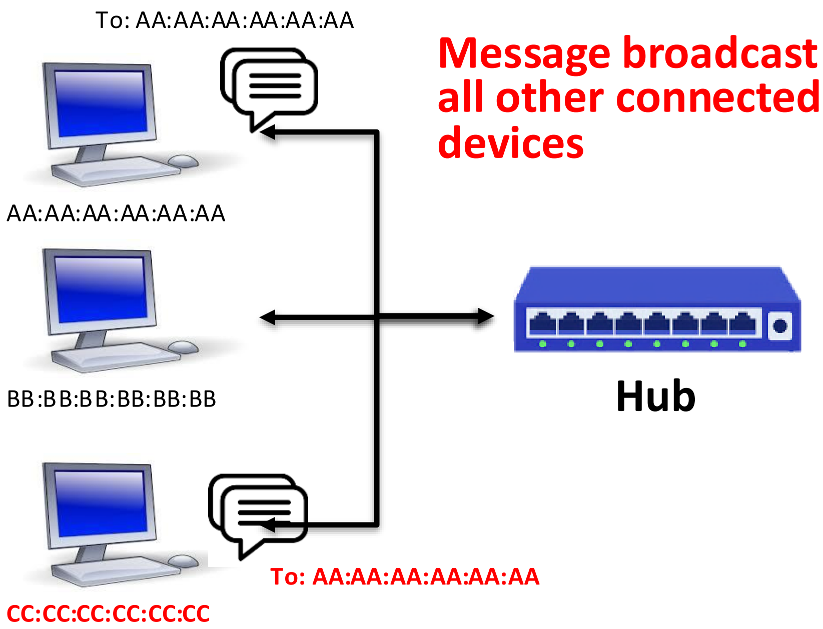
Each device looks at MAC address

Device AA:AA:AA:AA:AA:AA processes message because MAC matches destination MAC

Other devices (e.g., CC:CC:CC:CC:CC:CC) ignore message if not addressed to their MAC address

Hubs are not used much anymore, but you might run into them

Home LAN



Message broadcast to all other connected devices

All devices see all traffic

Each device looks at MAC address

Device AA:AA:AA:AA:AA:AA processes message because MAC matches destination MAC

Other devices (e.g., CC:CC:CC:CC:CC:CC) ignore message if not addressed to their MAC address

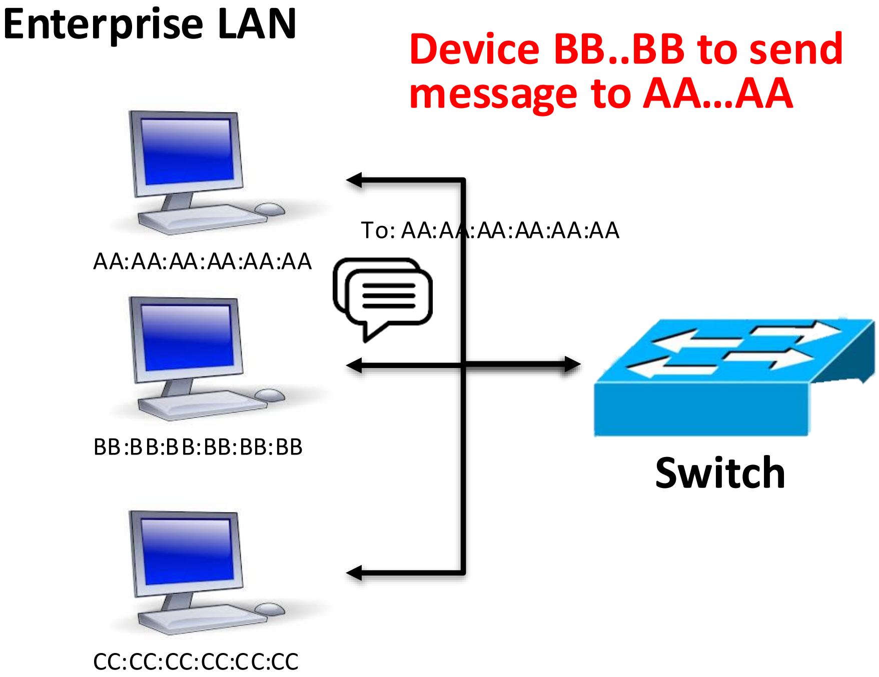
Function: Broadcasts all incoming data to all connected devices, regardless of the destination

Layer: Operates at the physical layer (Layer 1) of the network model

Complexity: Simple and inexpensive

Use Cases: Less commonly used now, primarily in very small networks, older setups, or to create multiple ports from a single network connection

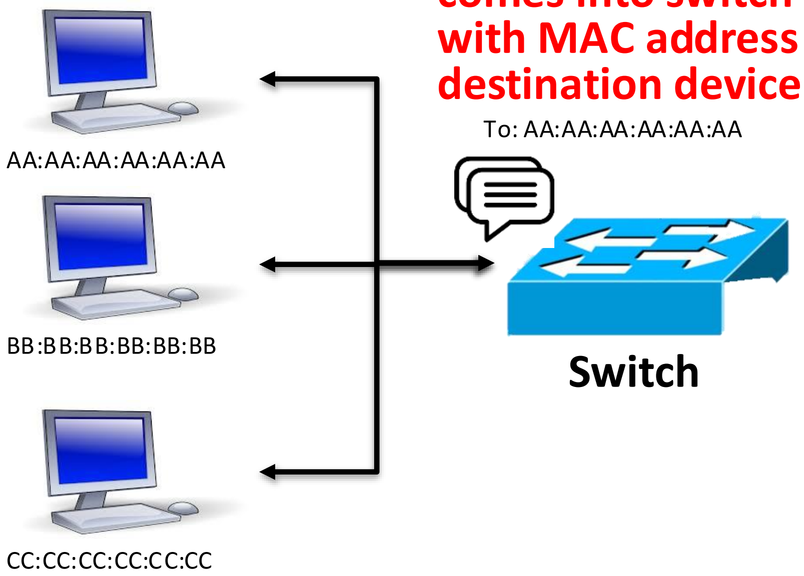
Switches are more intelligent than hubs, forward data to specific MAC addresses



Function: Analyzes the MAC address of incoming data packets and forwards them to the appropriate port, creating multiple isolated collision domains

Switches are more intelligent than hubs, forward data to specific MAC addresses

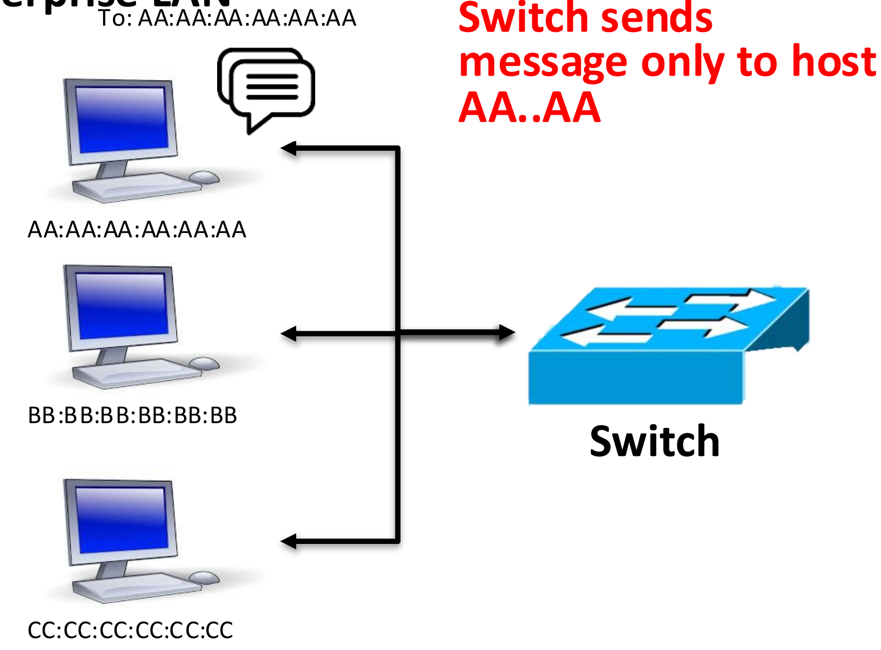
Enterprise LAN



Function: Analyzes the MAC address of incoming data packets and forwards them to the appropriate port, creating multiple isolated collision domains

Devices do not see traffic intended for other devices with a switch

Enterprise LAN

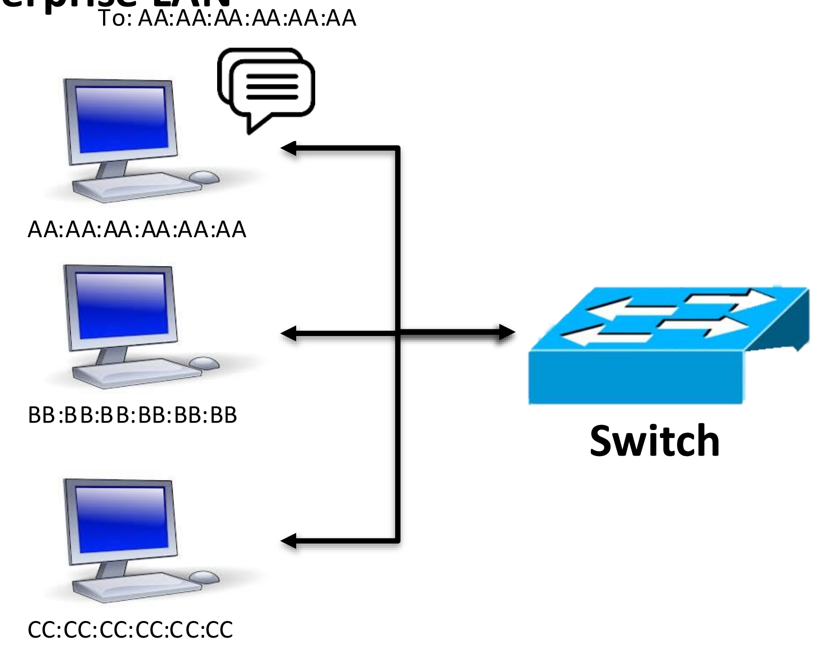


Switch sends message only to host AA..AA

Function: Analyzes the MAC address of incoming data packets and forwards them to the appropriate port, creating multiple isolated collision domains

Switches are more complicated than hubs, but are more efficient

Enterprise LAN



Function: Analyzes the MAC address of incoming data packets and forwards them to the appropriate port, creating multiple isolated collision domains

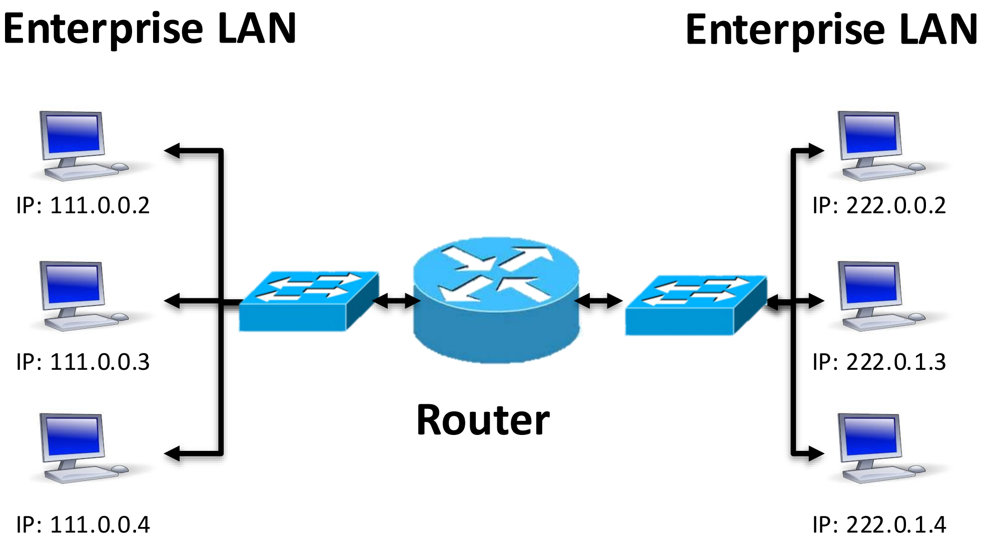
Layer: Operates at the data link layer (Layer 2) of the network model

Complexity: More complex than hubs, but less complex than routers

Advantages: Switches create multiple collision domains, allowing for simultaneous communication between different devices

Use Cases: Common in modern home and office networks for connecting devices within a LAN

Routers join networks together; directs traffic on IP address (not MAC)



Function: Connects multiple networks together, such as a home network to the Internet

Layer: Operates at the network layer (Layer 3) of the network model and uses IP addresses to forward packets between networks

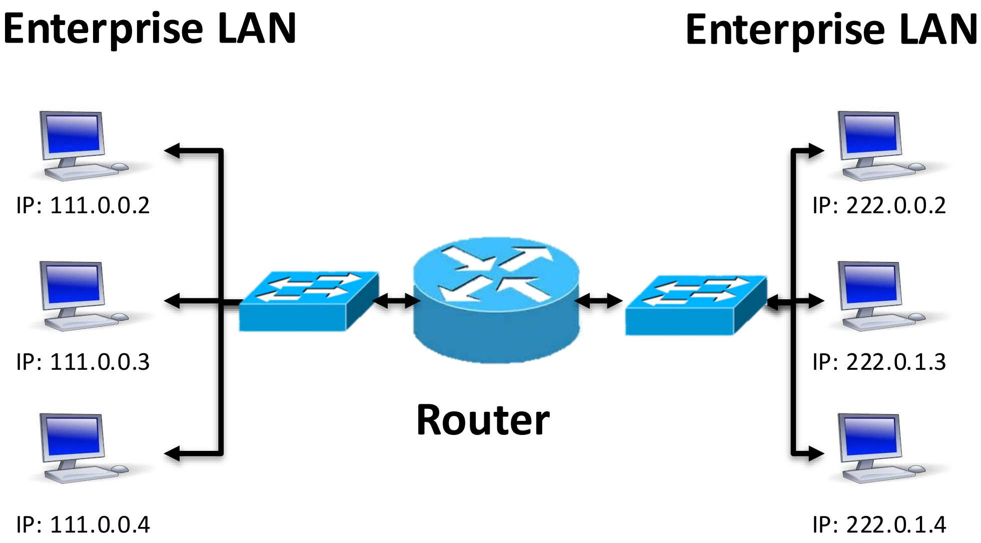
Complexity: More complex than hubs and switches

Advantages:

- Enable multiple devices on a local network to share a single public IP address (called NAT)
- Can provide security features like firewalls
- Allow for more complex network configurations and better traffic management

Use Cases: Connecting multiple LANs

Routers join networks together; directs traffic on IP address (not MAC)



Routers also commonly issue IP addresses to devices on the LAN using Dynamic Host Configuration Protocol (DHCP)

We will cover DHCP soon!

Function: Connects multiple networks together, such as a home network to the Internet

Layer: Operates at the network layer (Layer 3) of the network model and uses IP addresses to forward packets between networks

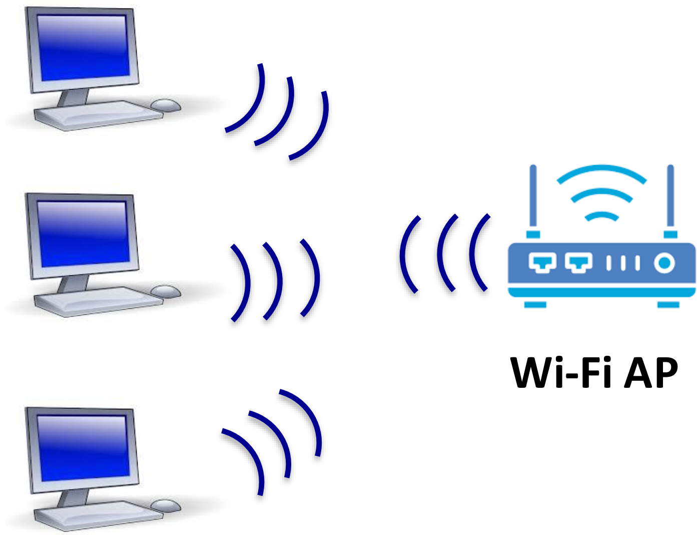
Complexity: More complex than hubs and switches

Advantages:

- Enable multiple devices on a local network to share a single public IP address (called NAT)
- Can provide security features like firewalls
- Allow for more complex network configurations and better traffic management

Use Cases: Connecting multiple LANs

Wi-Fi Access Points (APs) connect devices wireless like a router



Note: APs broadcast their signal wireless, so any device in radio range can hear it

In this way, APs are somewhat like hubs

Function: Connects devices within a limited geographical area, typically a building or campus, using radio waves instead of physical cables. Often gives accesses to the Internet

Layer: Operates at the data link layer (Layer 2) and the network layer (Layer 3) of the network model

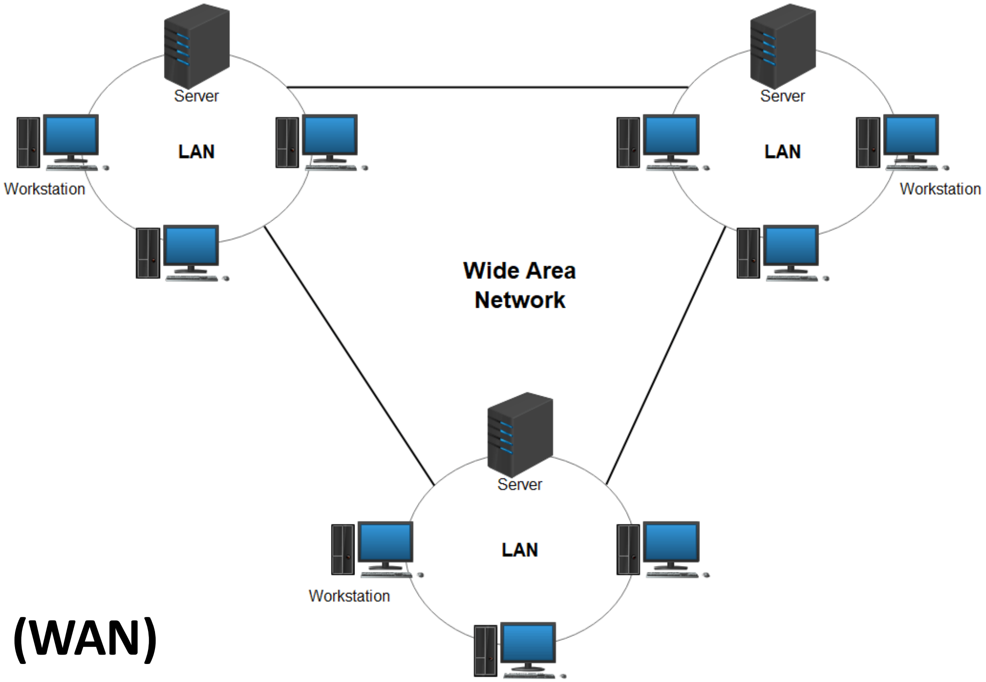
Complexity: More complex than hubs and switches

Use Cases: Connecting mobile devices like phones and laptops. Normally not used for servers and desktops

Advantages: Mobility, ease of installation

Disadvantages: Radio interference, all devices see radio broadcast like with a hub

Multiple LANs can be connected to form a Wide Area Network (WAN)



Wide Area Network (WAN)

- LANs are for local connections, WANs connect networks across larger distances
- WANs connect organizations with multiple locations, enabling communication, data sharing, and access to centralized resources
- Businesses with branch offices, universities with multiple campuses, and government agencies with offices in different locations all rely on WANs
- The Internet is the world's largest WAN

https://www.sangfor.com/glossary/cloud-and-infrastructure/what-is-wan-wide-area-network

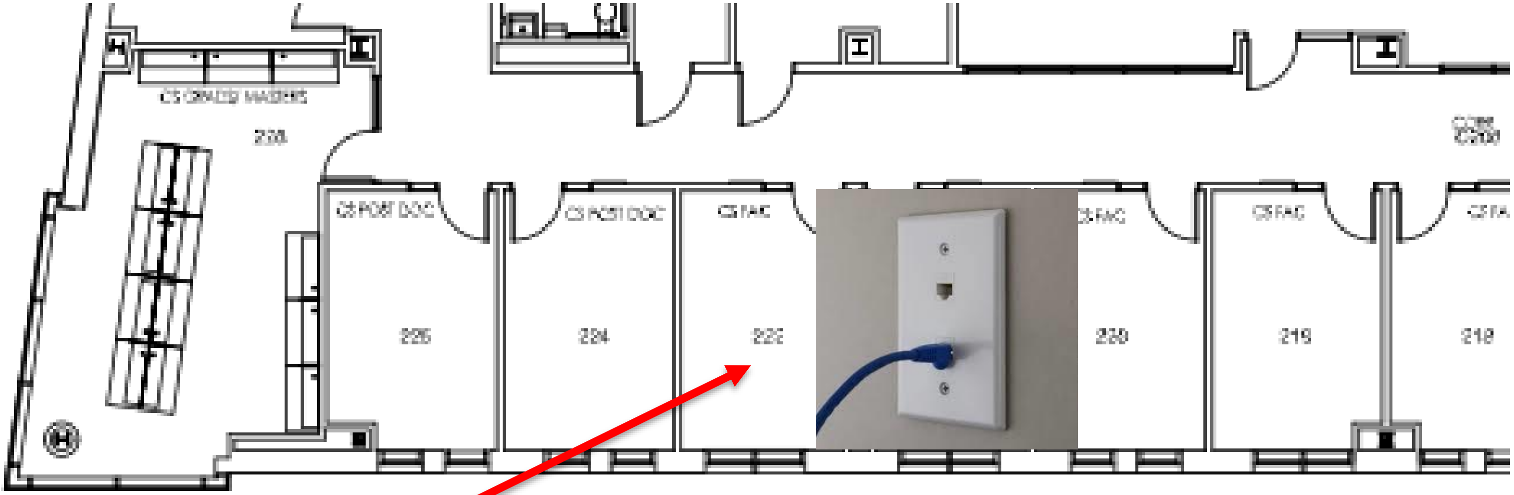
Agenda

1. Intro and course overview
2. Networking creates new possibilities and new challenges
3. What is the Internet anyway?
4. How are hosts connected?
5. Connecting ECSC (illustrative)

My office in ECSC has a network jack allowing me connectivity to the network

Illustrative

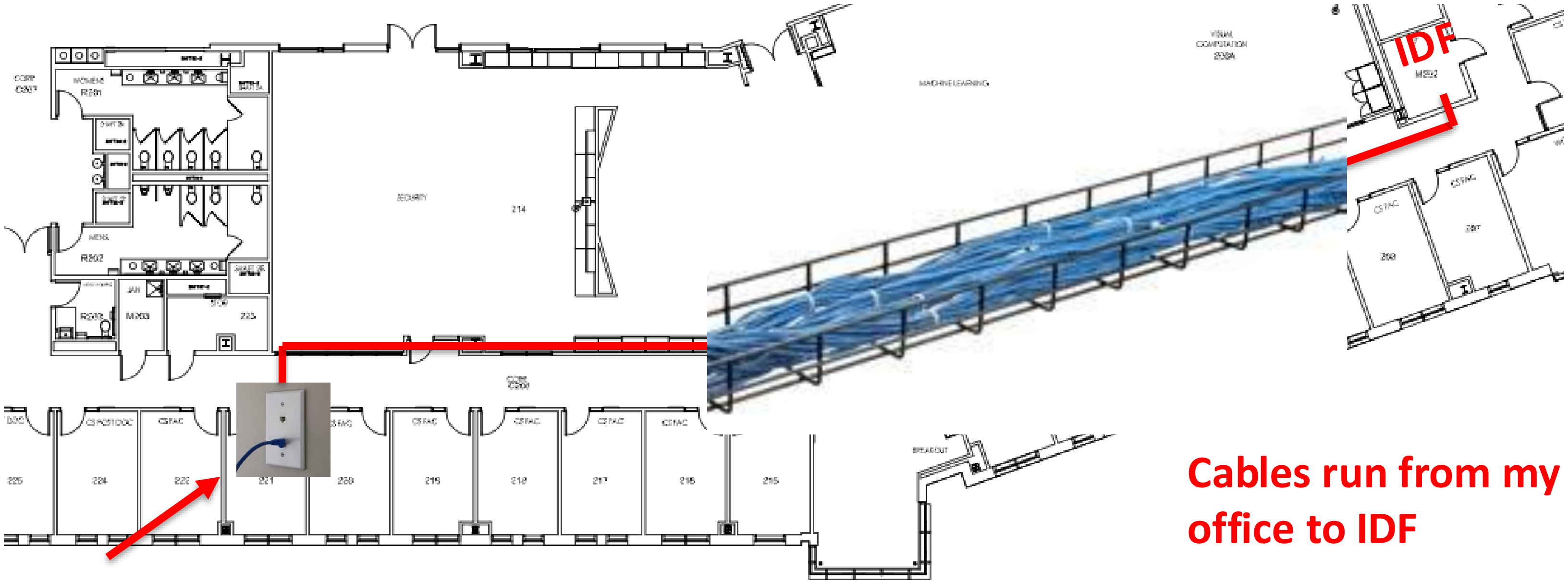
Illustrative, I do not know how the actual cables run, this is my guess



My office

Jack is wired via cable to a patch panel in an Intermediate Distribution Facility (IDF)

Illustrative



My office

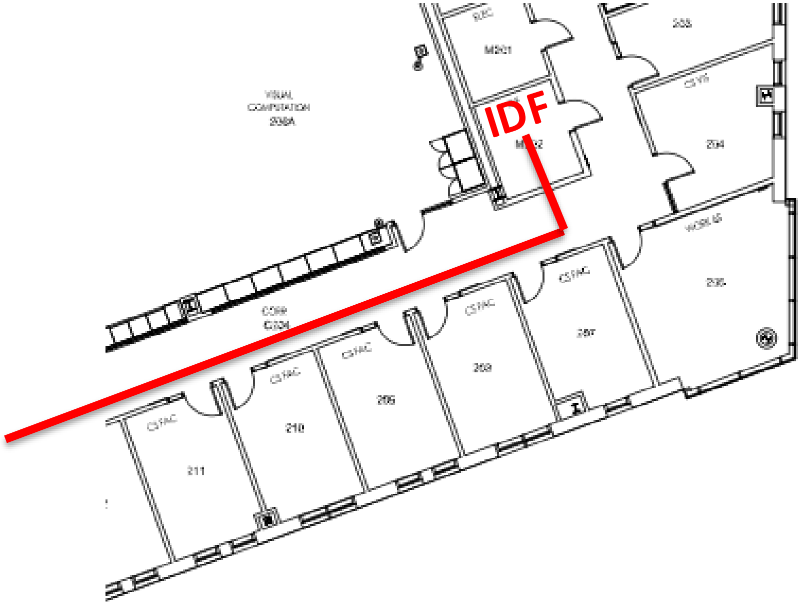
Cables run from my office to IDF

IDF also called

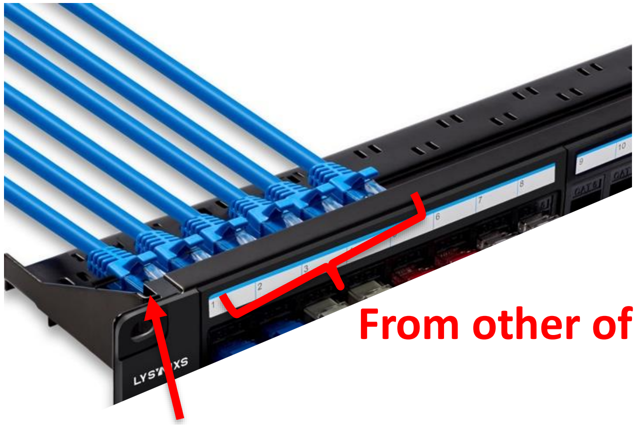
- Computer room
- Telephone room
- Network closet

The jack is connected to a patch panel in an Intermediate Distribution Facility (IDF)

Illustrative



Cable from my office (and other offices on the floor) enter back of patch panel

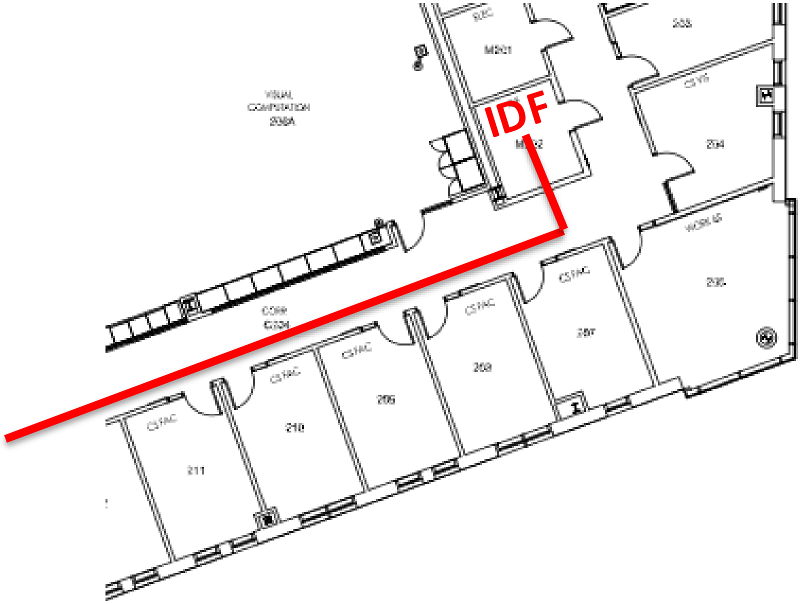


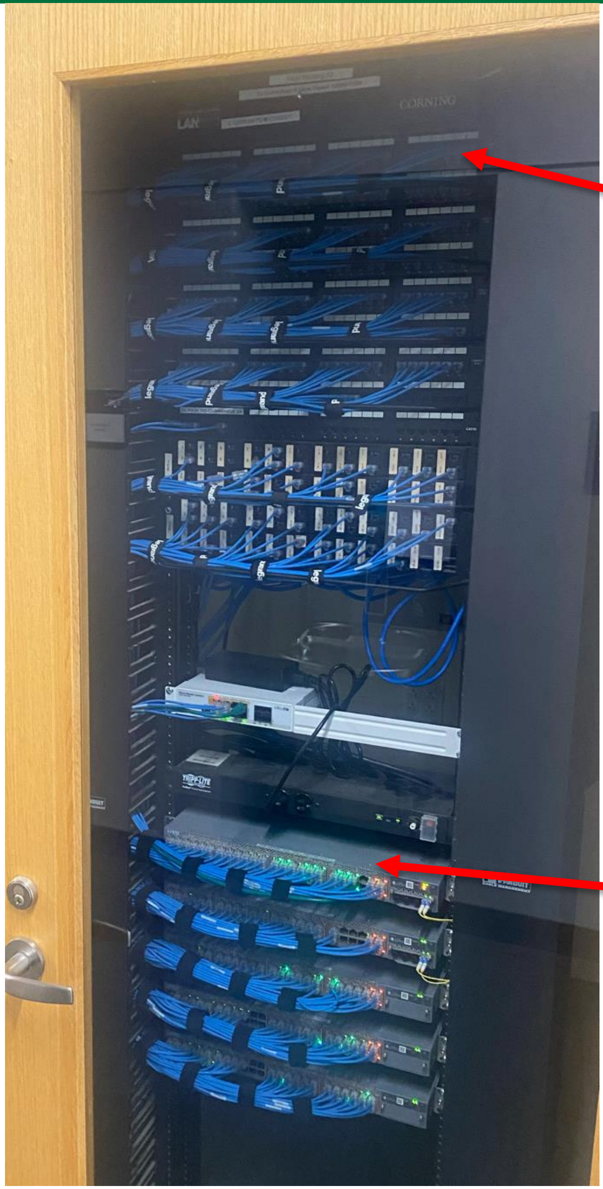
From other offices

From my office

Cables go from the from of the patch panel to connected to a switch in the IDF

Short patch cables exit the front of the patch panel and connect to a switch in a rack





Illustrative

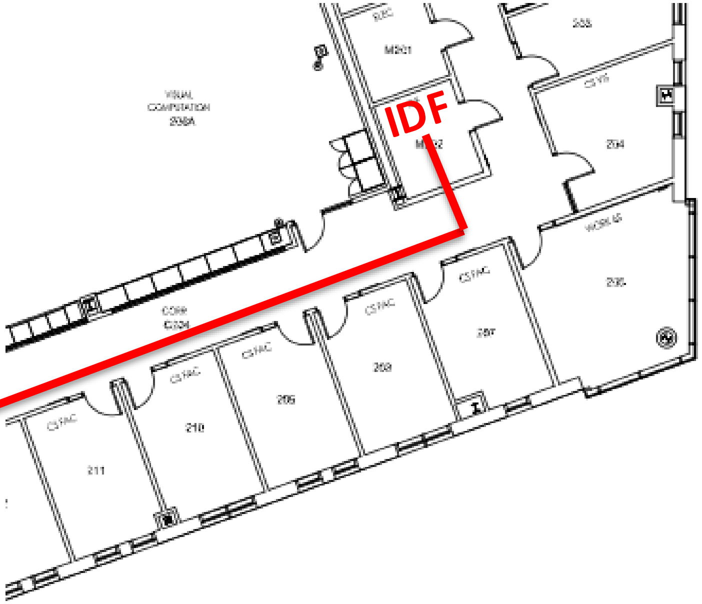
Patch panel with my office and others nearby

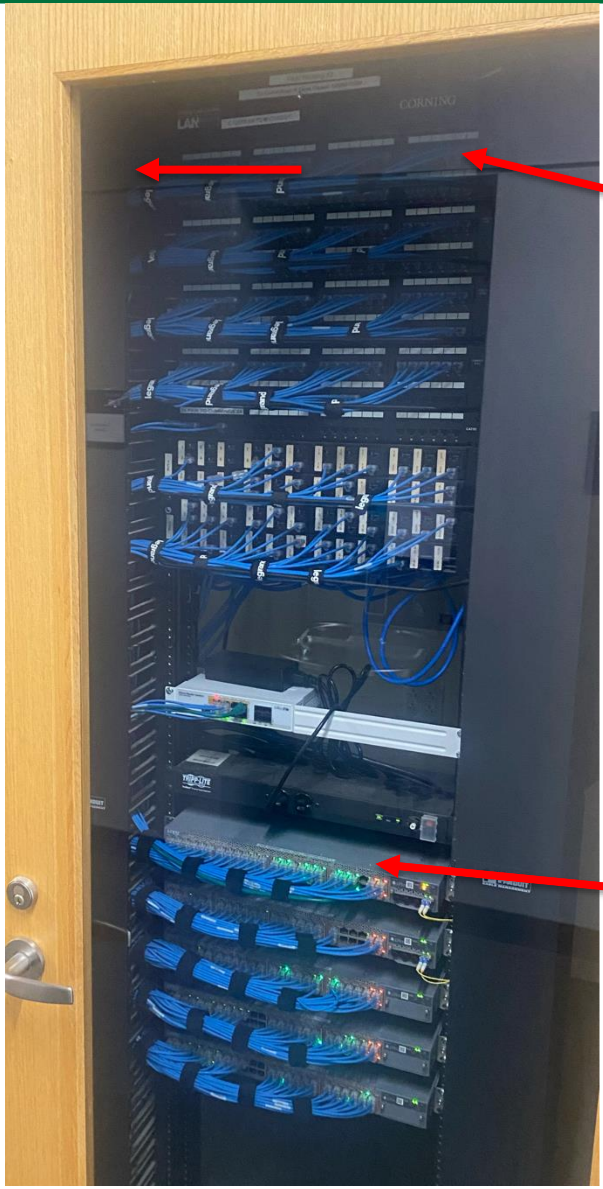
Switch

Cables go from the from of the patch panel to connected to a switch in the IDF

Illustrative

Short patch cables exit the front of the patch panel and connect to a switch in a rack





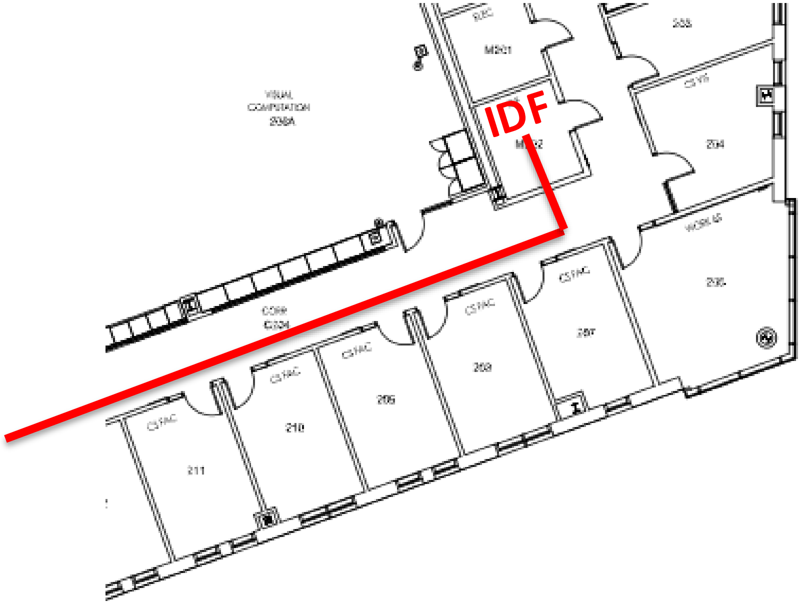
Patch panel with my office and others nearby

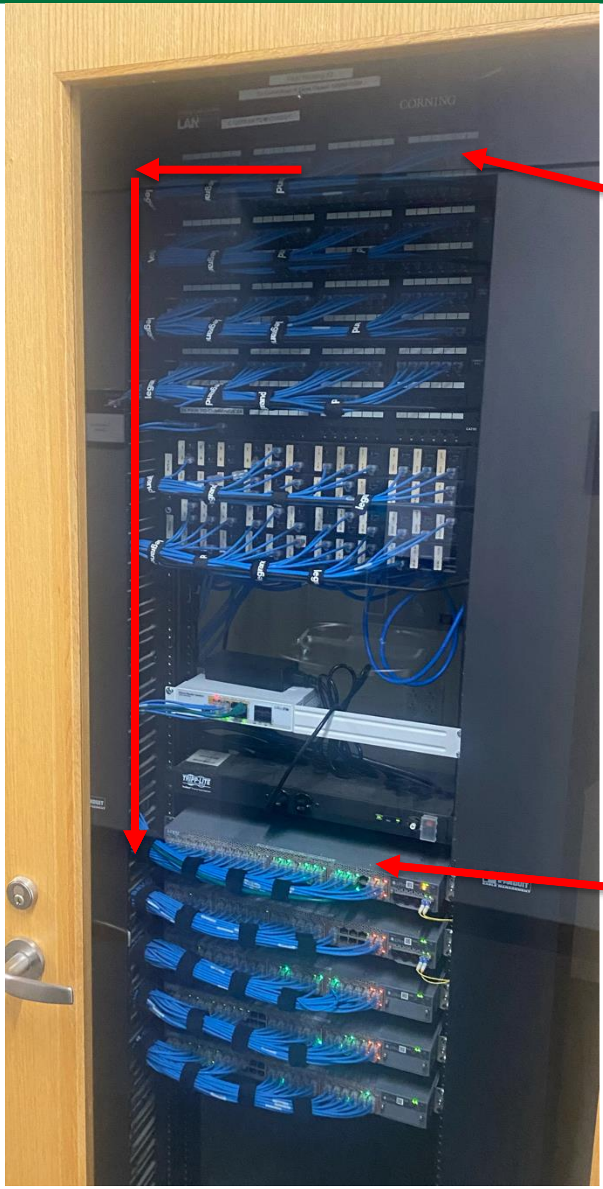
Switch

Thayer IDF

Cables go from the from of the patch panel to connected to a switch in the IDF

Short patch cables exit the front of the patch panel and connect to a switch in a rack





Illustrative

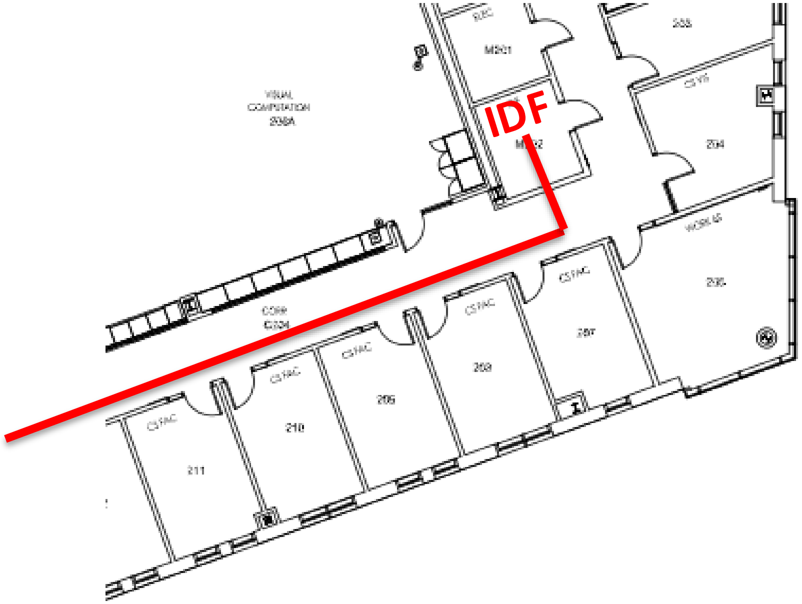
Patch panel with my office and others nearby

Switch

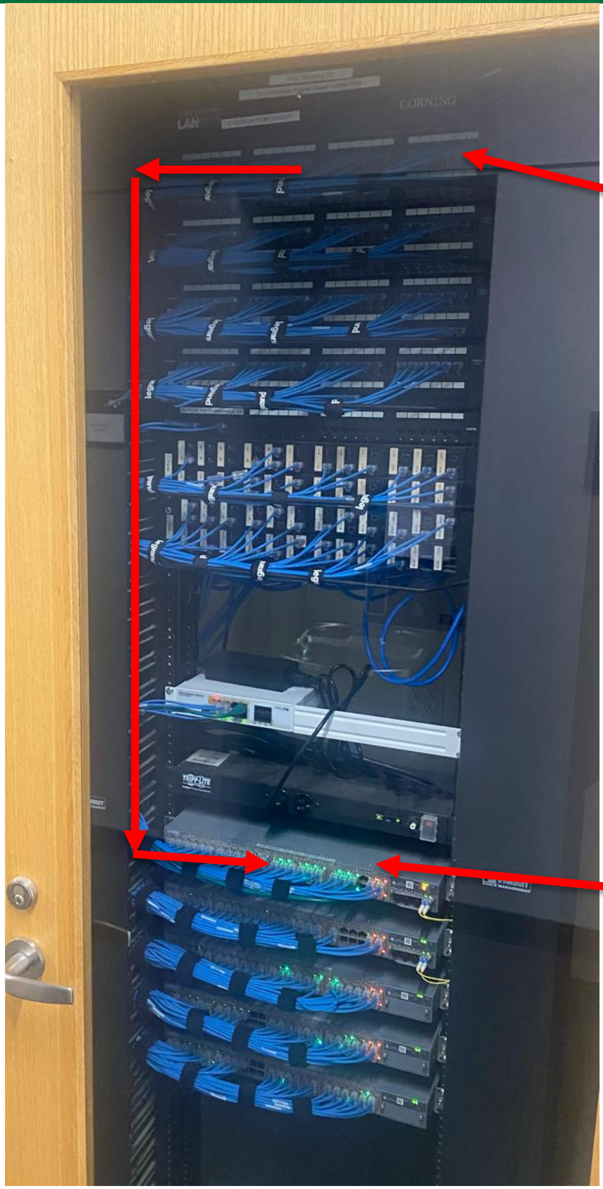
Thayer IDF

Cables go from the from of the patch panel to connected to a switch in the IDF

Short patch cables exit the front of the patch panel and connect to a switch in a rack



Illustrative



Patch panel with my office and others nearby

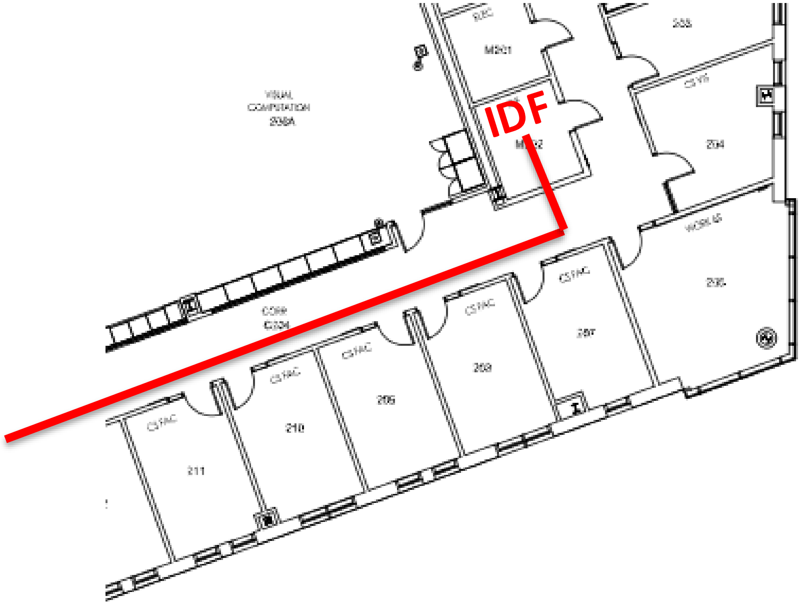
Switch

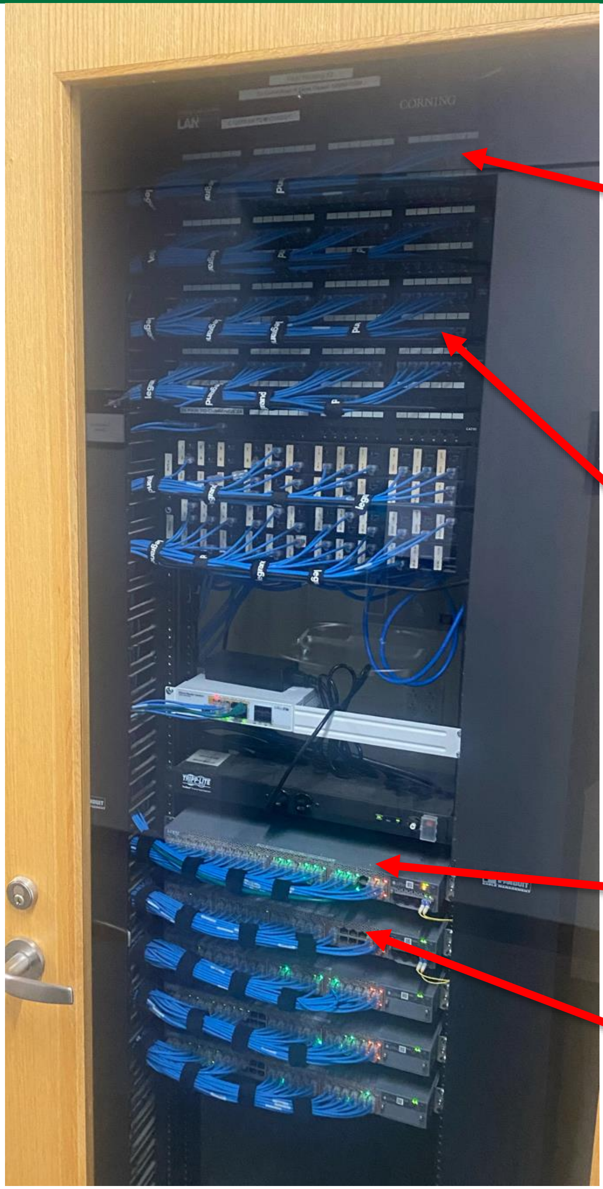
My office and other offices connect here

Thayer IDF

Cables go from the from of the patch panel to connected to a switch in the IDF

Short patch cables exit the front of the patch panel and connect to a switch in a rack





Illustrative

Patch panel with my office and others nearby

Additional patch panels for other offices on the same floor

Switch

More switches for more offices on the floor

Components in an IDF are often stored in a rack

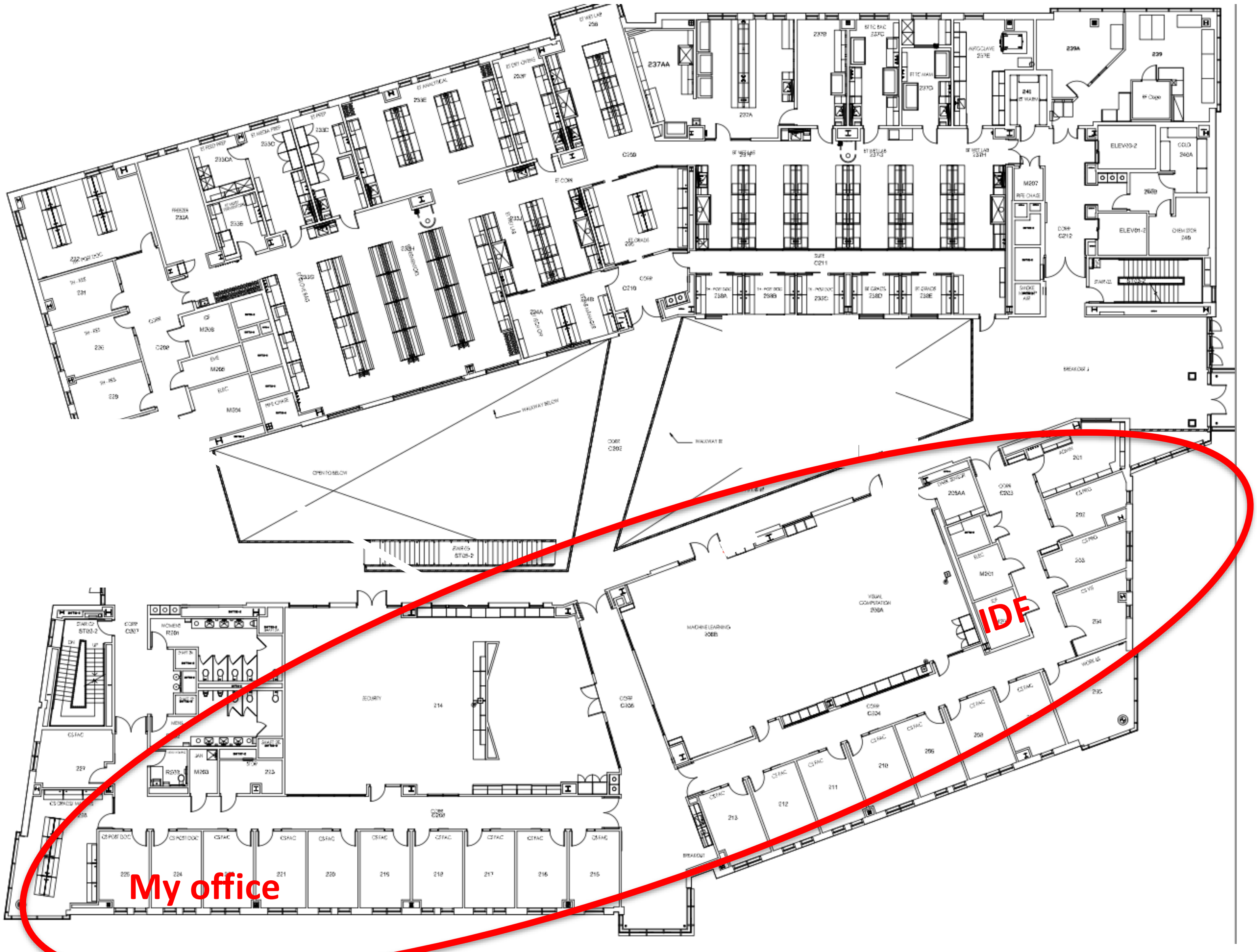
Rack

- Holds networking components
  - Patch panel
  - Switches/Routers
  - Servers
  - UPS
- A full rack is 42U high (1U = 1.75 inches)
- Each server (called a "Blade") and switch/router are commonly
  - 1U
  - 2U
  - 4U
- Pro tips:
  - Put light weight patch panel at top
  - Put heavy components like a UPS in bottom (why?)

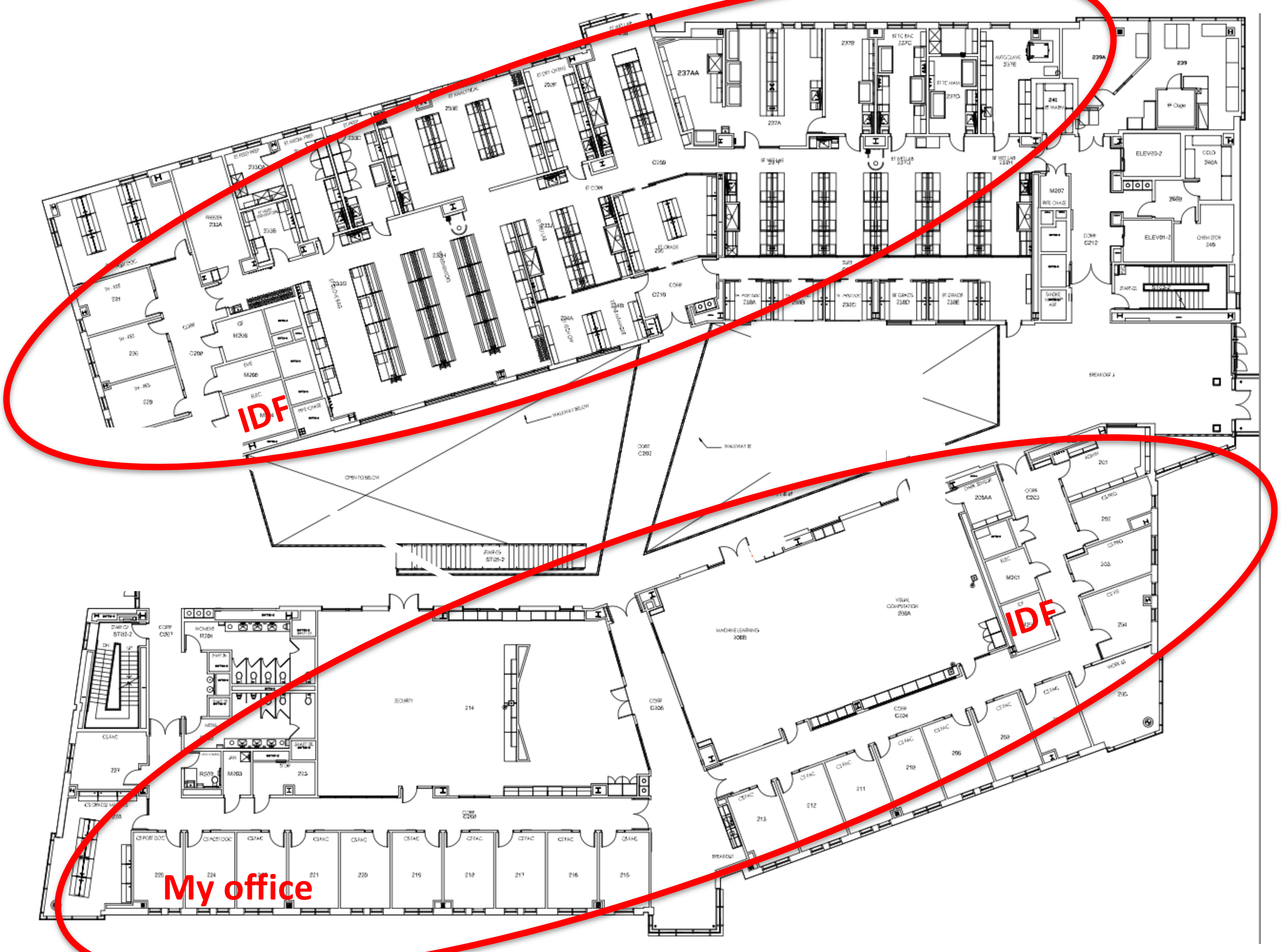
IDFs connect to Main Distribution Facilities (MDF) or Data Centers with many racks

The CS department is connected via IDF switches into a LAN for communications

Illustrative



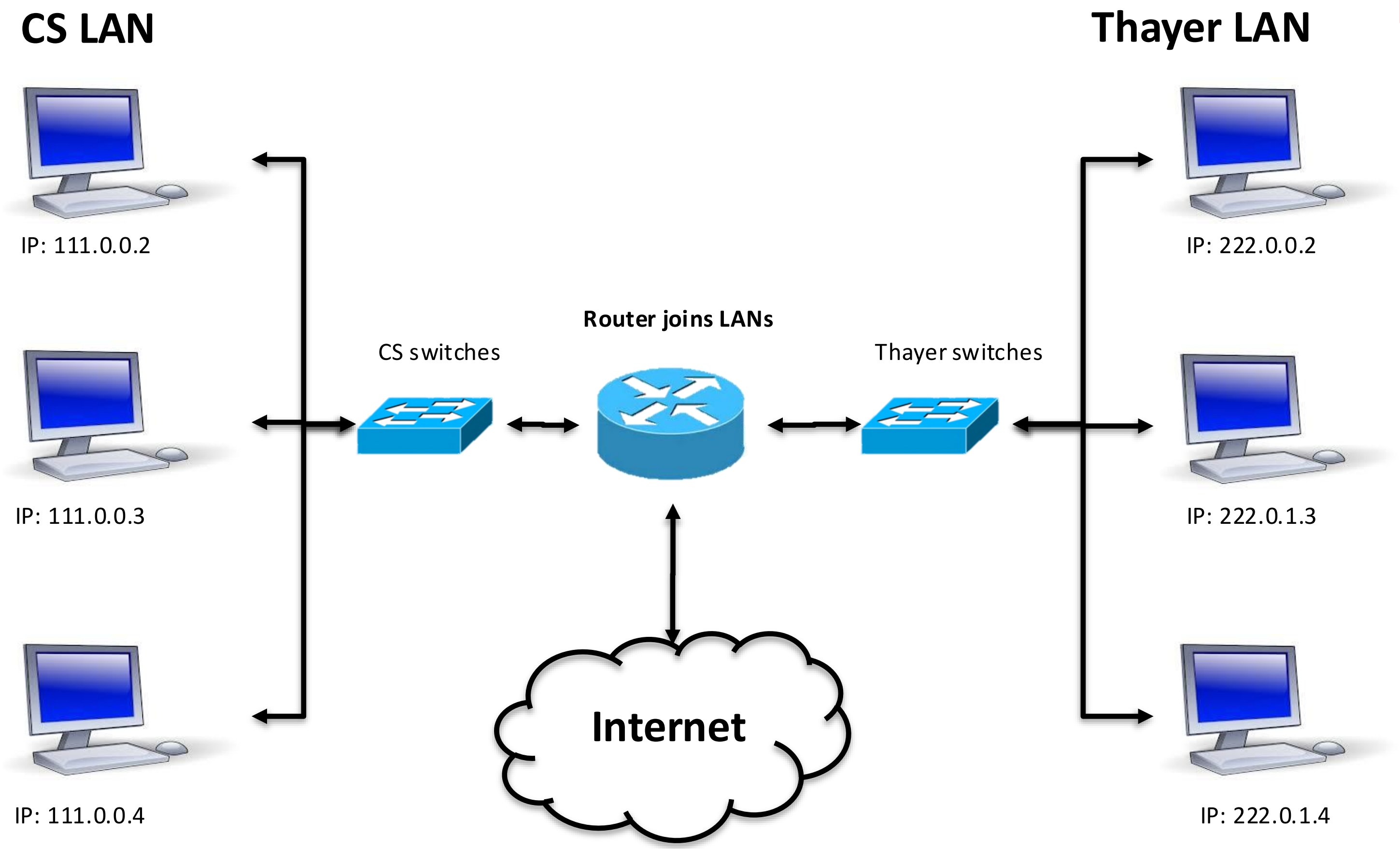
Thayer is connected into their own LAN via switches in another IDF



Illustrative

The CS and Thayer LANs are connected to each other and the Internet via a router

Illustrative



Exercises

Install the Virtual Machine following instructions on the course web page’s Software tab

Capture packets on your VM

- Start Wireshark and capture packets from your computer’s Wi-Fi interface (ens160 on my Mac)
- Start Firefox to generate network traffic

Lab 0 is out today

Lab 0

- Find it on Canvas
- Take course survey to understand your background
- Read and acknowledge course policies