Lecture 19 – Intro to Network

University of Illinois

ECE 422/CS 461

Announcement

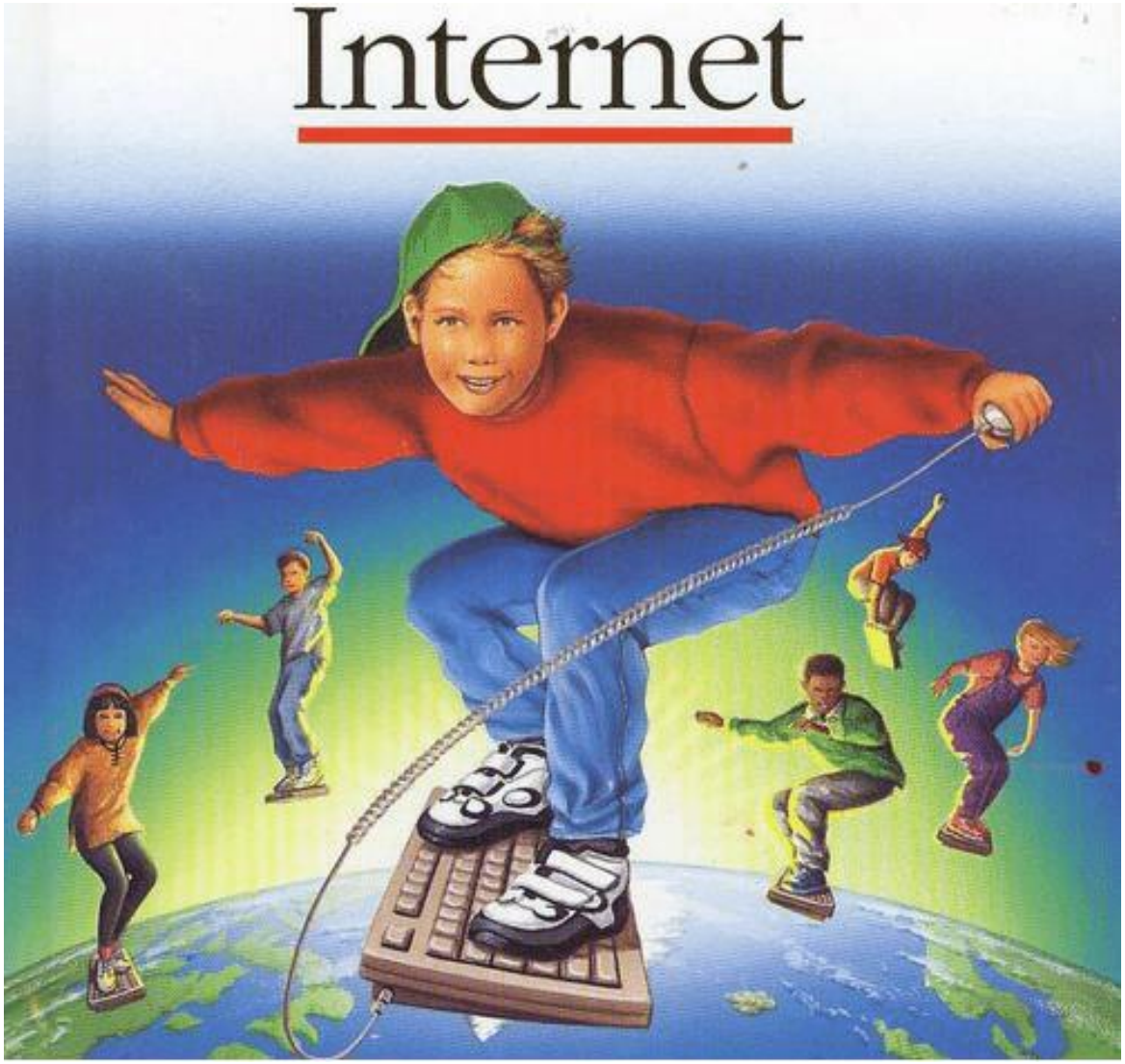
- MP3 due today, submit on GitHub

- Final Exam Dates:
  - May 12, 1:30 – 4:30 pm, 100 Noyes Laboratory
    - We likely won't use all 3 hours
  - Same policy as midterm
  - Similar format and difficulty, proportional in length

Goals of this Lecture

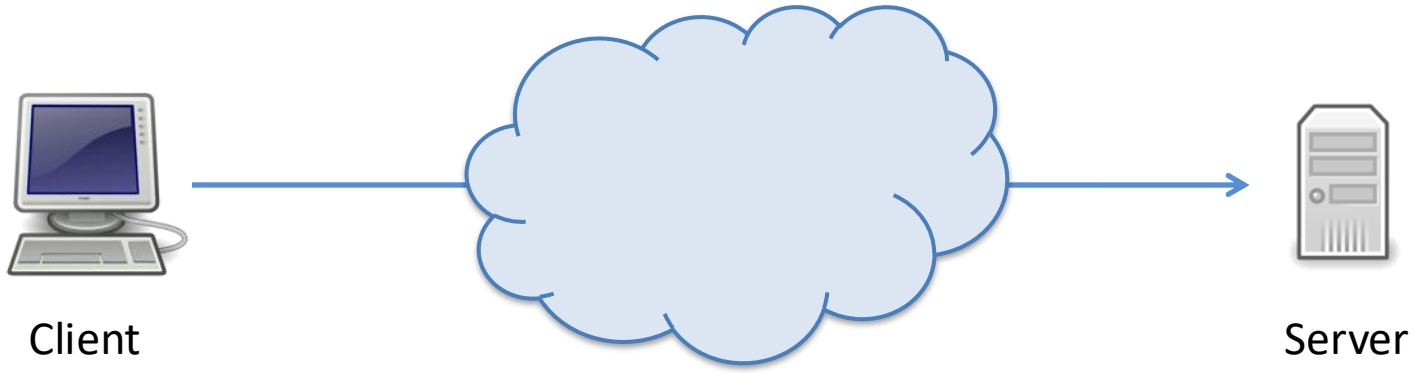
- By the end of this lecture you should…
  - Be familiar with the general workflow of network
  - Identify the different layers of the network stack
  - Know the purpose and function of each layer
  - Understand the security model of network

What is the Internet?



What is the Internet?

- To the layperson: useful services
  - Web, email, video, voice
- Technically: a global system that lets *hosts* communicate



Packet Switching

- **Packet:** a structured sequence of bytes
  - Header: metadata used by network
  - Payload: data to be transported

- Packets are forwarded by a sequence of routers from sender to destination

Routers

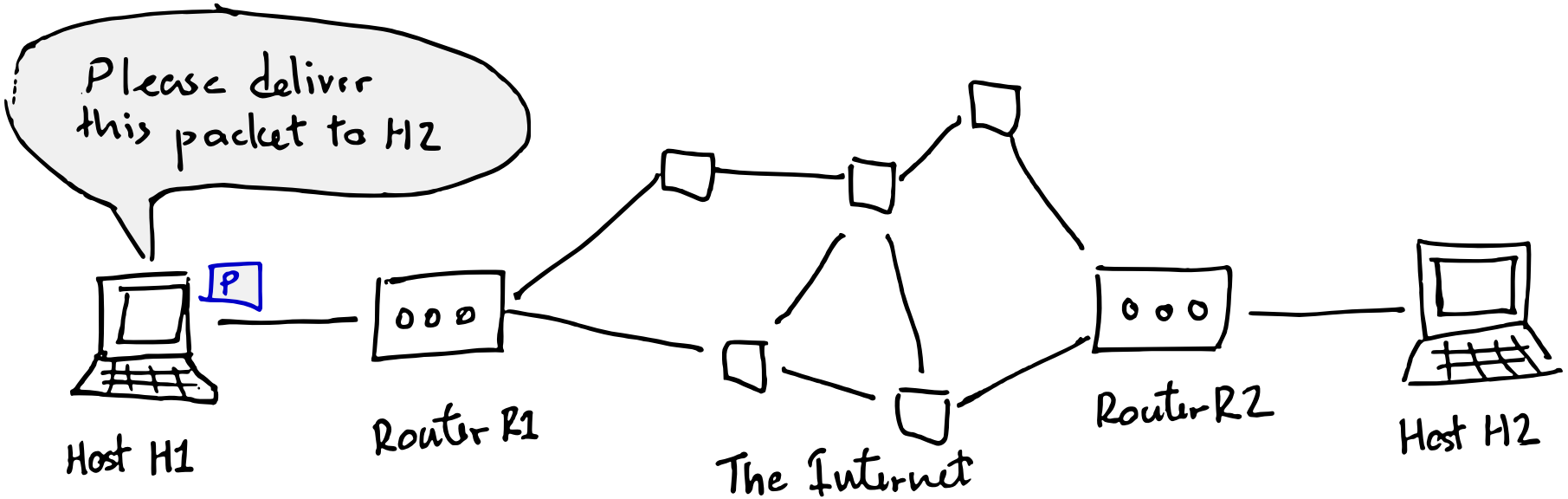
- Receive outgoing packets from local hosts and *attempt* to deliver them to destination
- Deliver incoming packets to local hosts

Internet Message Processor

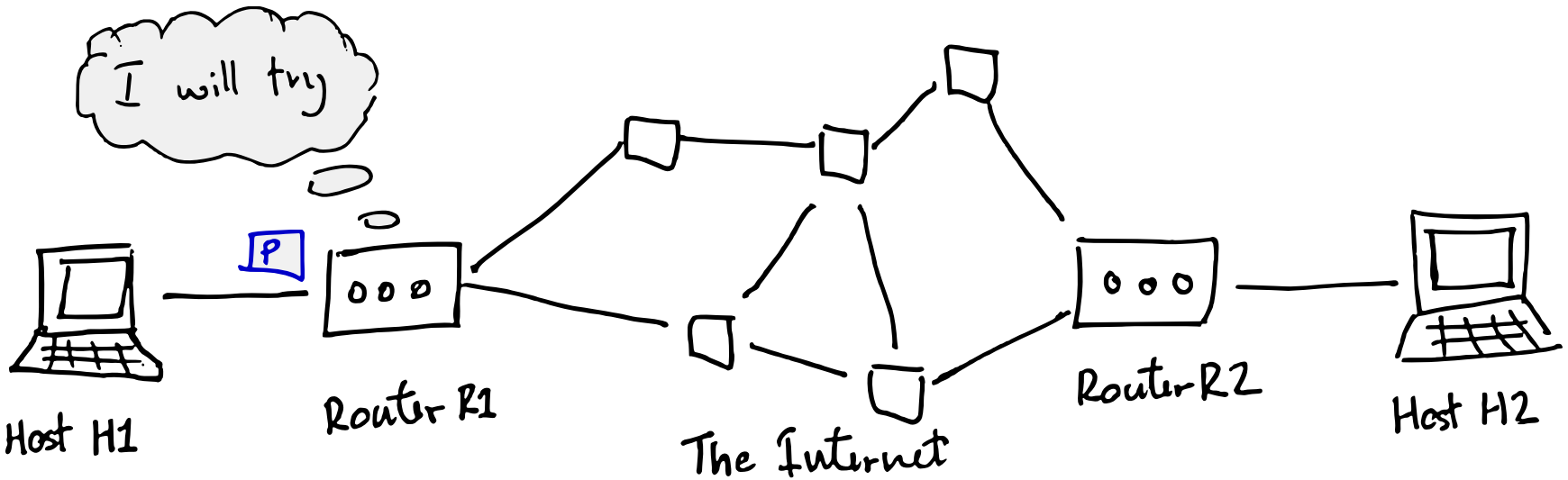
Linksys WRT54G

Cisco CRS-1

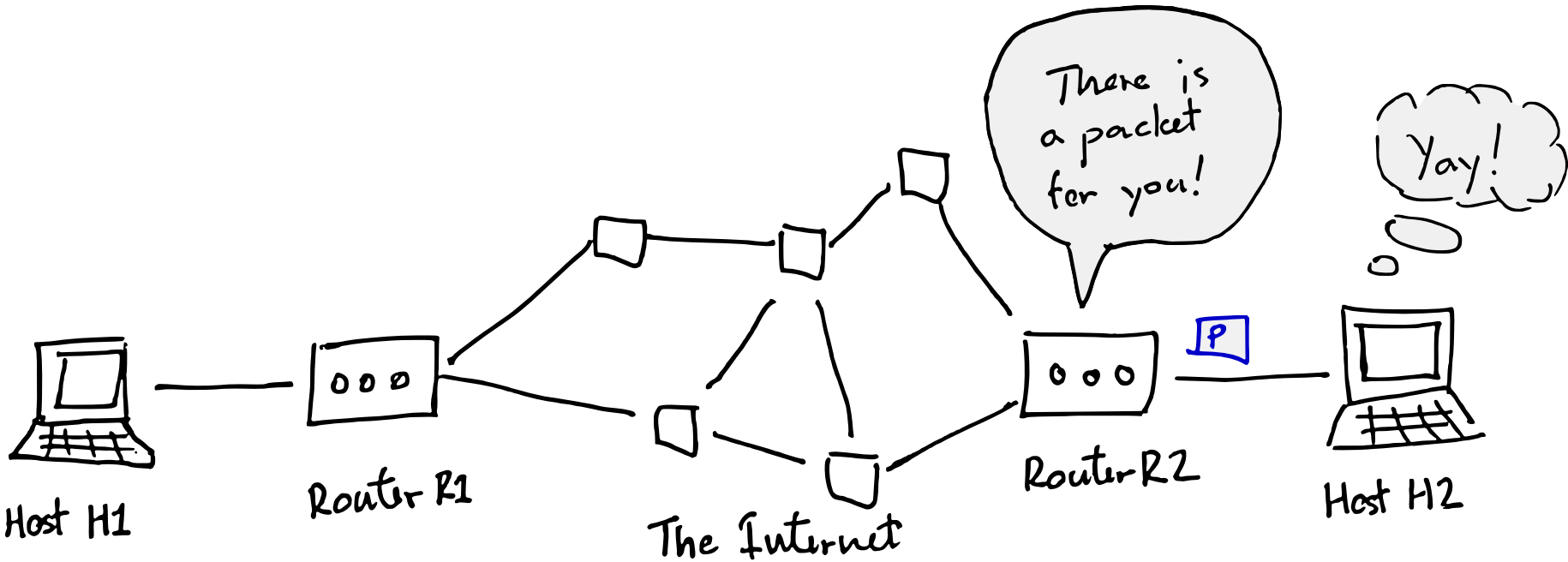
Packet Switching



Packet Switching



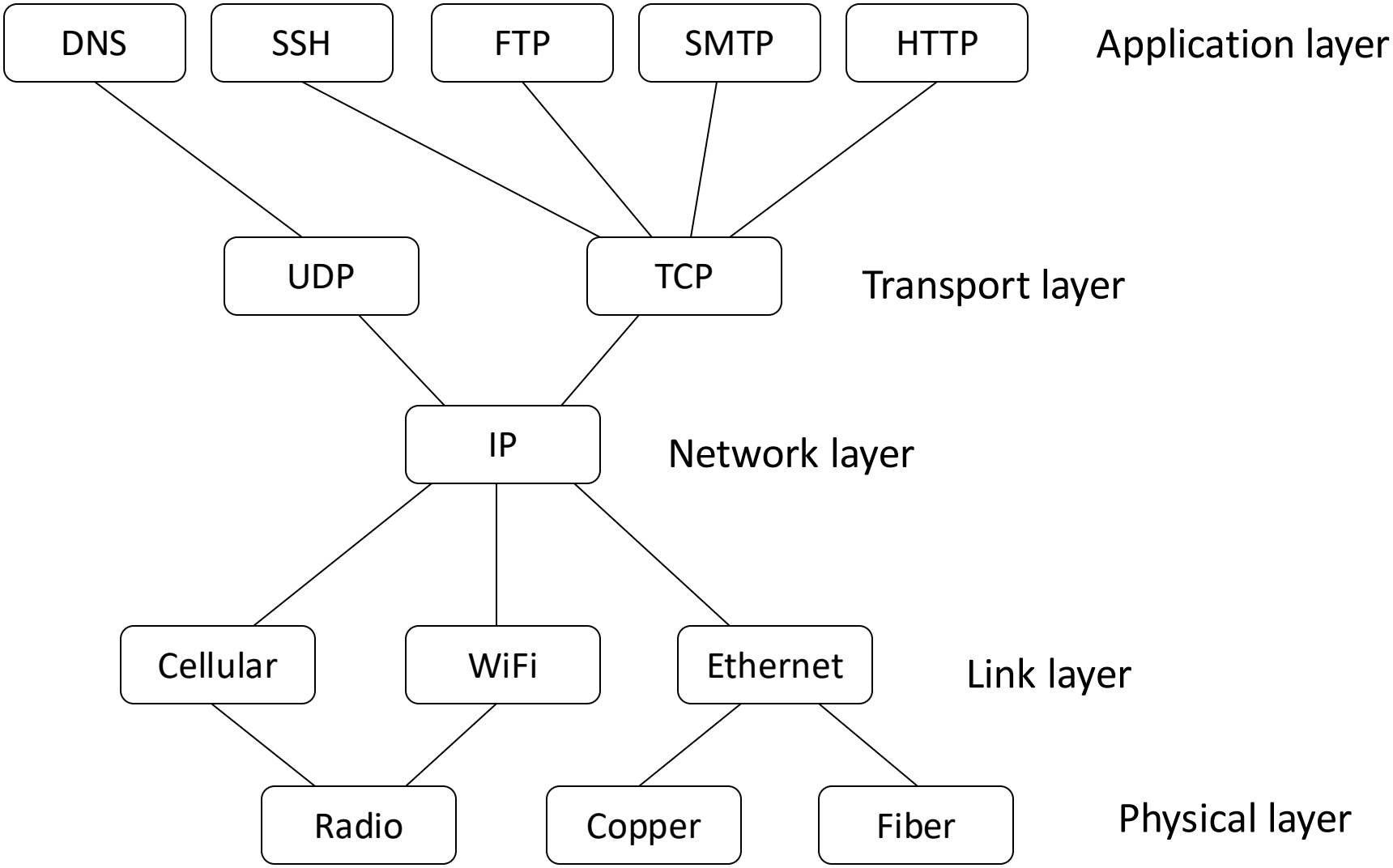
Packet Switching



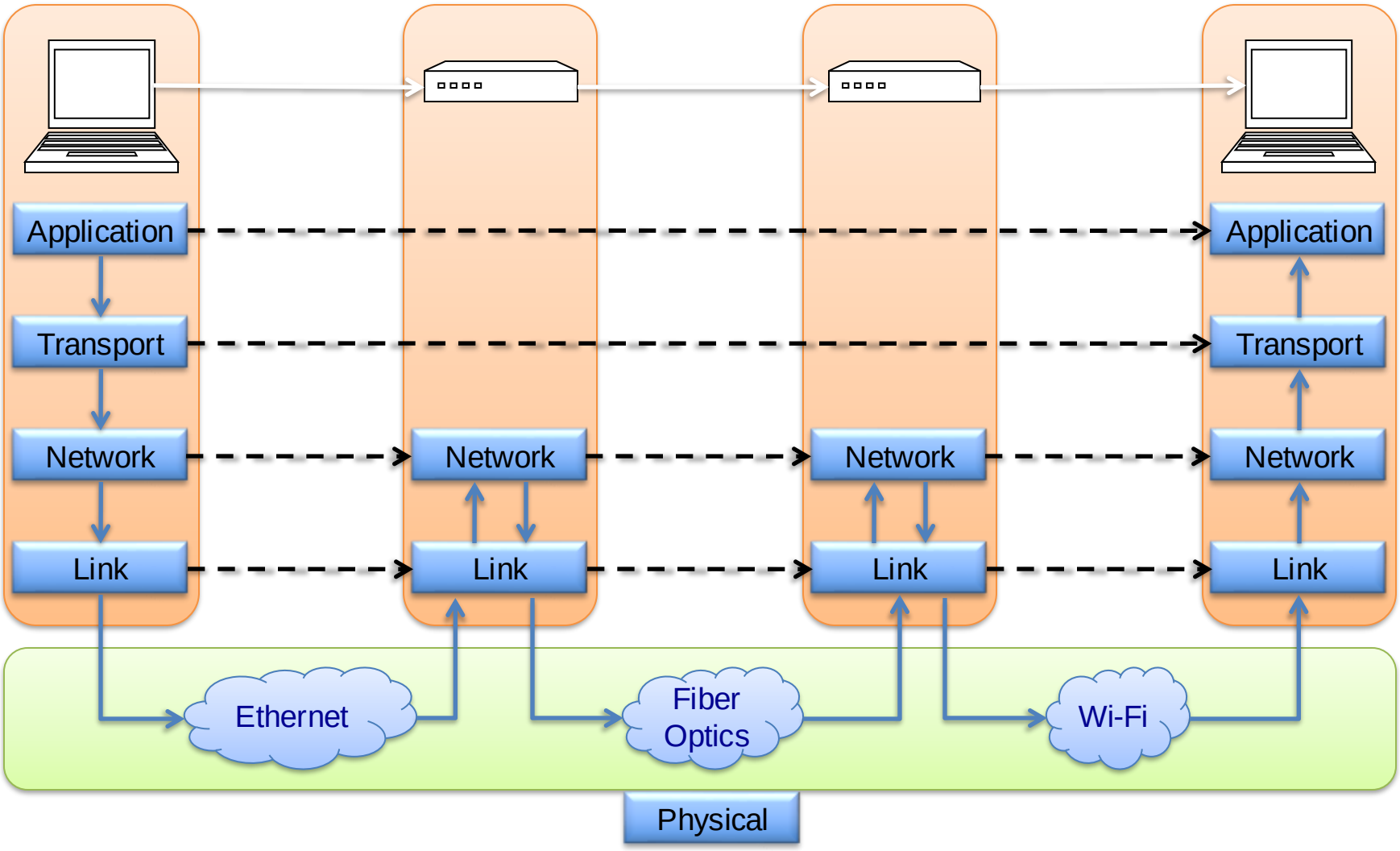
Protocol Layering

- A network isn't defined by one protocol, but a stack of protocols!
  - Lower layers provide services to layers above
  - Higher layers use services of layers below
  - A layer (largely) doesn't care how lower layers are implemented or what higher layers do

Layering of Protocols



The Internet Protocol Stack



The Internet Protocol Stack

- Physical Layer: Transmits raw bits over a physical data link
- Link Layer: Transmits packets between two hosts in the same network (i.e., physically connected)
- Network Layer: Transmits packets between two hosts in different networks (i.e., **internet**working)
- Transport Layer: Transmits packets between two processes on two hosts
- Application Layer: Transmits packets between end-user software

The Internet Protocol Stack

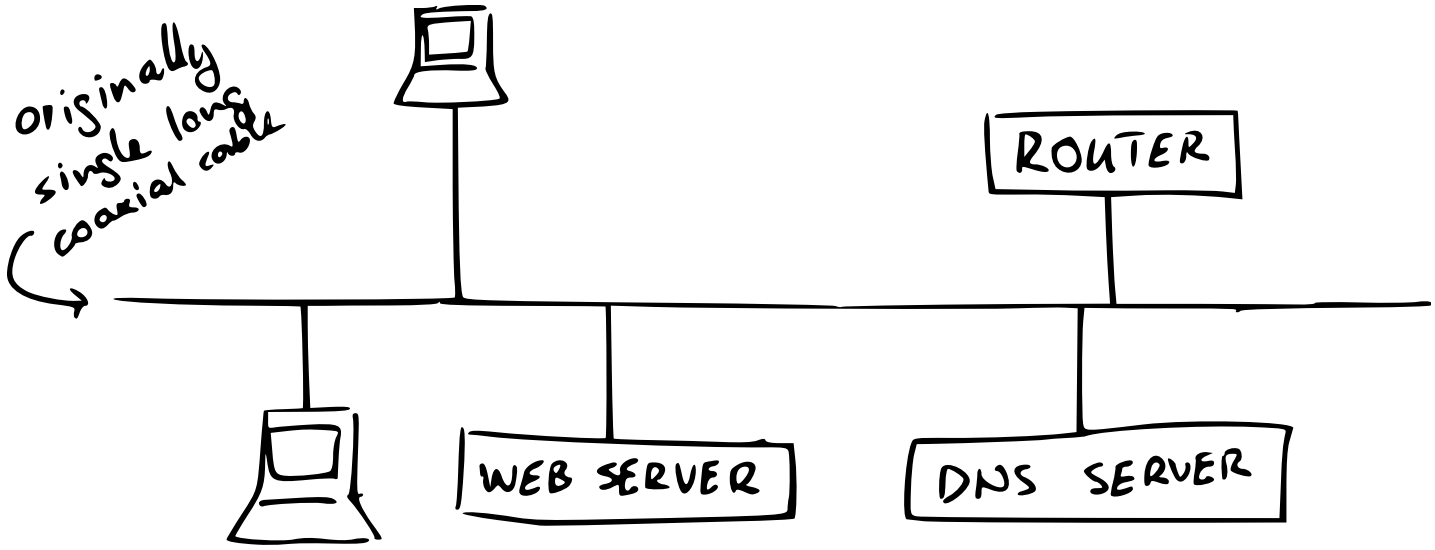
- Physical Layer: Transmits raw bits over a physical data link
- Link Layer: Transmits packets between two hosts in the same network (i.e., physically connected)
- Network Layer: Transmits packets between two hosts in different networks (i.e., **internet**working)
- Transport Layer: Transmits packets between two processes on two hosts
- Application Layer: Transmits packets between end-user software

The Internet Protocol Stack

- Physical Layer: Transmits raw bits over a physical data link
- Link Layer: Transmits packets between two hosts in the same network (i.e., physically connected)
- Network Layer: Transmits packets between two hosts in different networks (i.e., internetworking)
- Transport Layer: Transmits packets between two processes on two hosts
- Application Layer: Transmits packets between end-user software

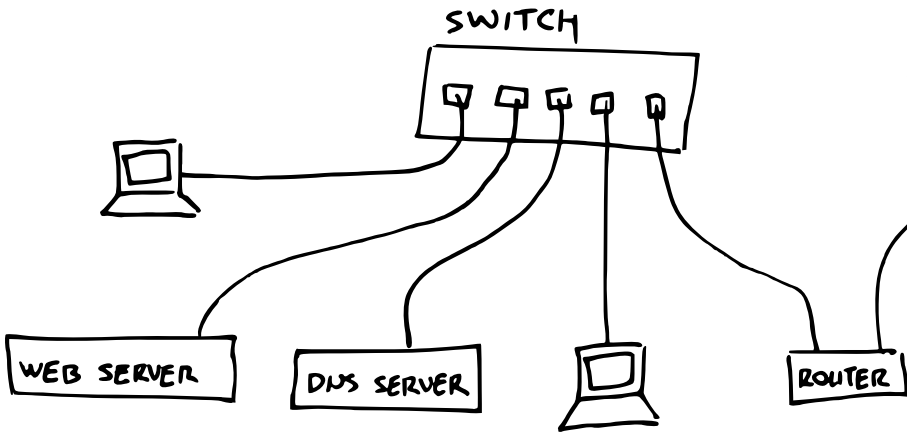
What is a Network?

- Over the years, its meaning has expanded …
- But originally, a network means a collection of *physically connected* devices



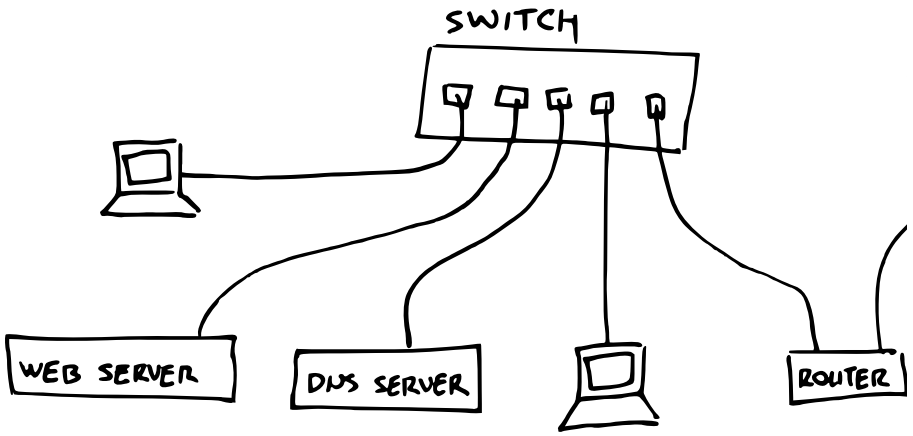
What is a Network?

- Over the years, its meaning has expanded …
- But originally, a network means a collection of *physically connected* devices
  - A more modern view: a switch replaces the single telephone line



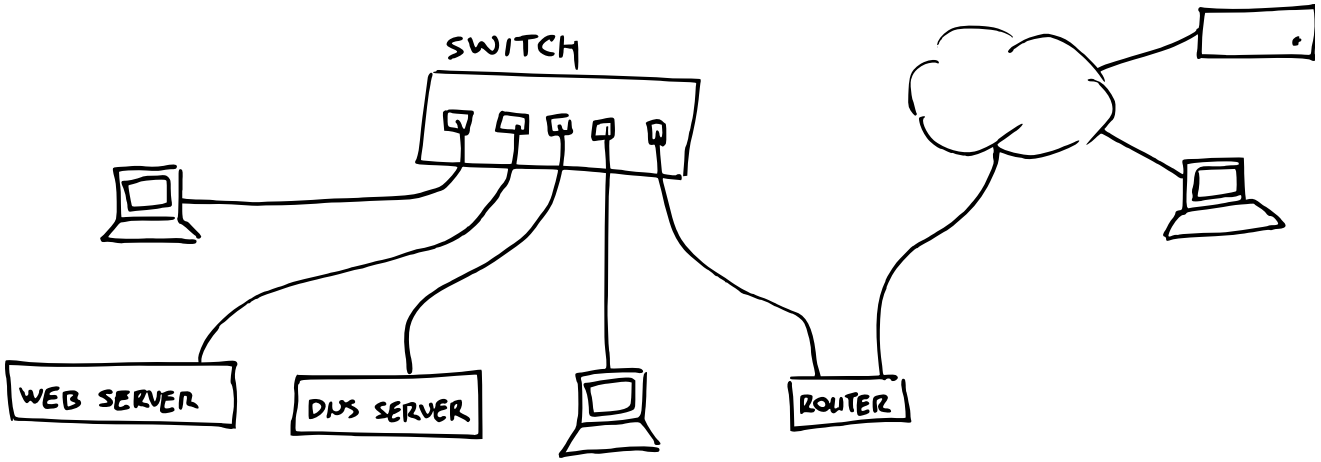
What is a Network?

- These physically connected devices (in the same network) communicate via a link-layer protocol
- How do they talk to outside devices?
  - Rely on the **gateway router** and **internetworking**



Internetwork

- Connects multiple “networks”
- Over the years, one such internetwork got really big, now called **the Internet**
- Network layer uses the Internet Protocol (IP)



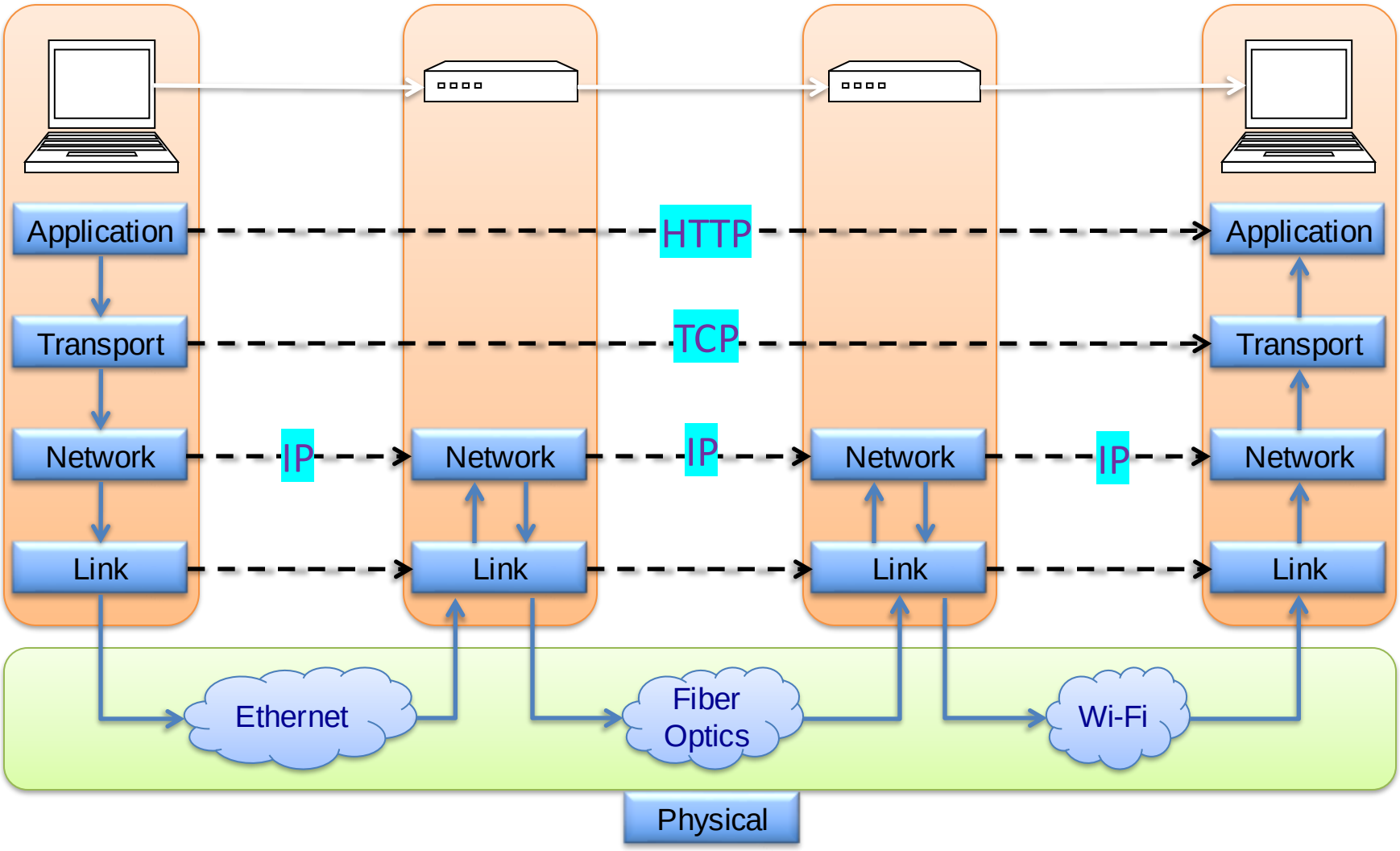
The Internet Protocol Stack

- Physical Layer: Transmits raw bits over a physical data link
- Link Layer: Transmits packets between two hosts in the same network (i.e., physically connected)
- Network Layer: Transmits packets between two hosts in different networks (i.e., **internet**working)
- Transport Layer: Transmits packets between two processes on two hosts
- Application Layer: Transmits packets between end-user software

Comparing Layers

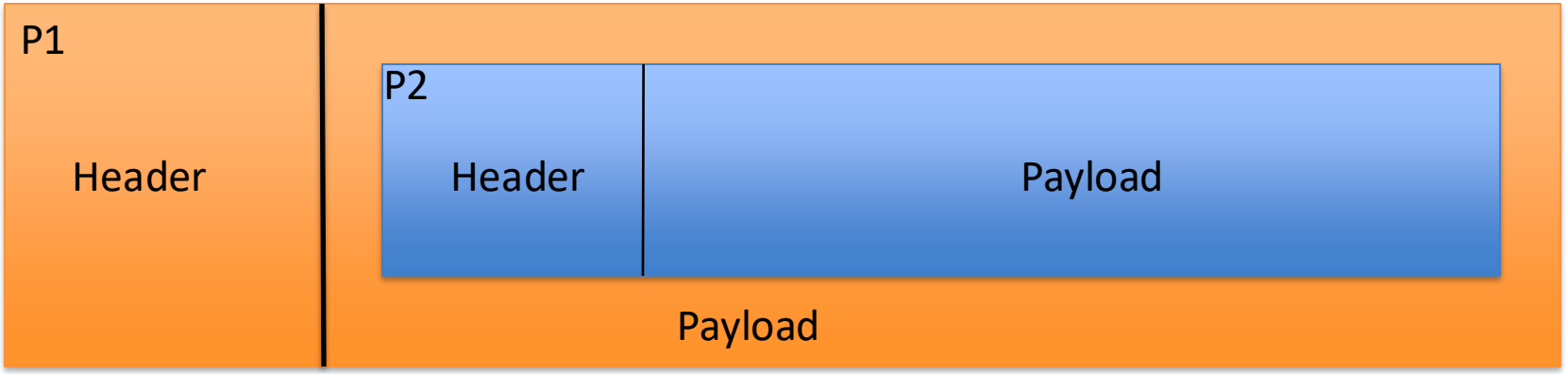
- Network layer (IP)
  - IP addresses
    - 192.138.1.52
  - Out-of-order delivery
  - Unreliable (best-effort)
- Link layer
  - MAC addresses
    - 2C:54:91:88:C9:E3
  - Out-of-order delivery
  - Unreliable (best-effort)
- Transport layer
  - (IP address, port)
  - TCP ensures in-order and reliable delivery, and adds flow control, congestion control, …
    - UDP does not do any of these

The Internet Protocol Stack



Packet Encapsulation

- A packet P2 of a higher level protocol is encapsulated into a packet P1 of a lower level protocol

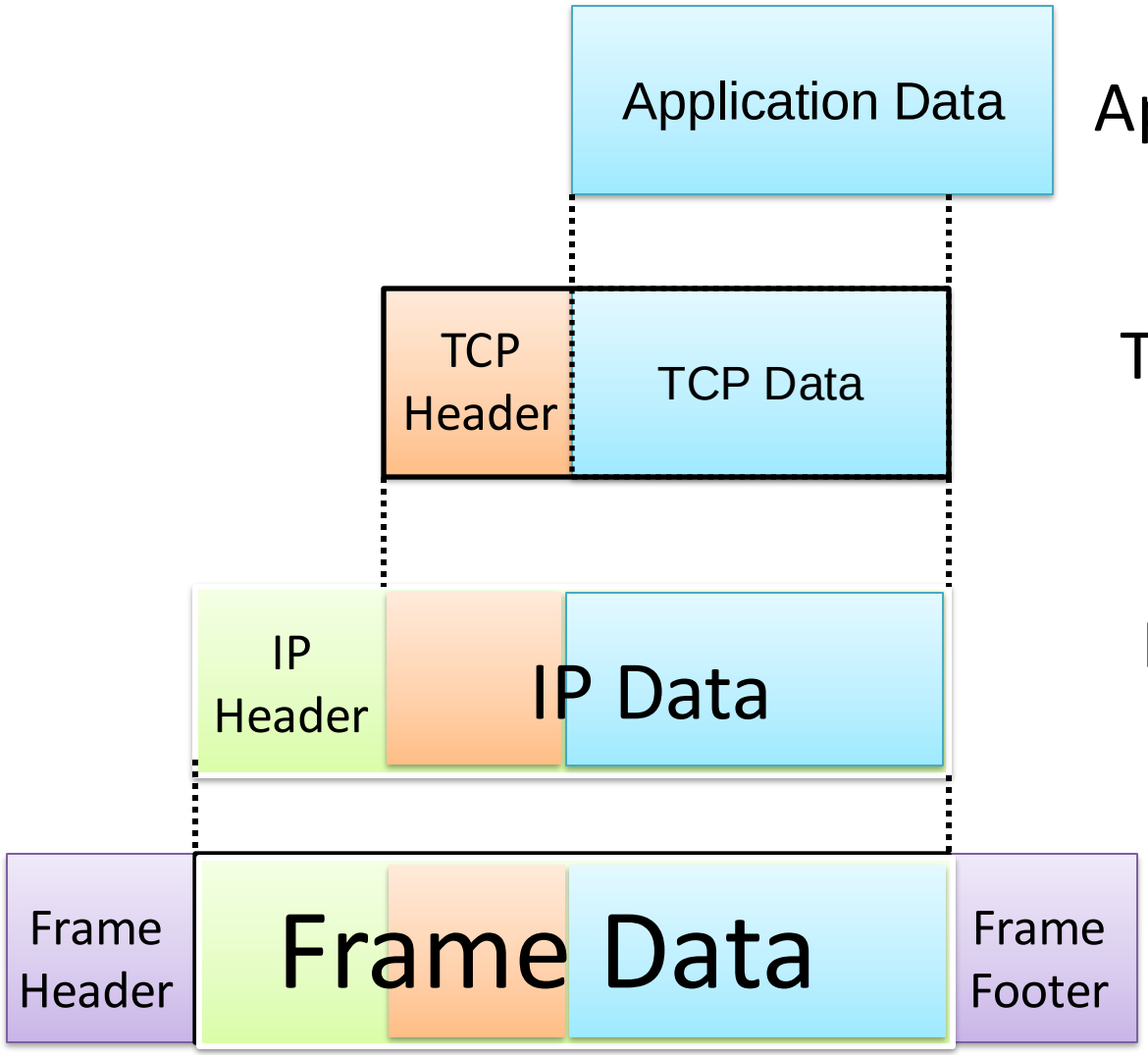


Internet Packet Encapsulation

- Technically, only the network layer use “packets”
  - Transport Layer Data Unit: Segments
  - Network Layer Data Unit: Packets
  - Link Layer Data Unit: Frames
  - Physical Layer Data Unit: just bits

  - But we will just call all of them packets

Internet Packet Encapsulation



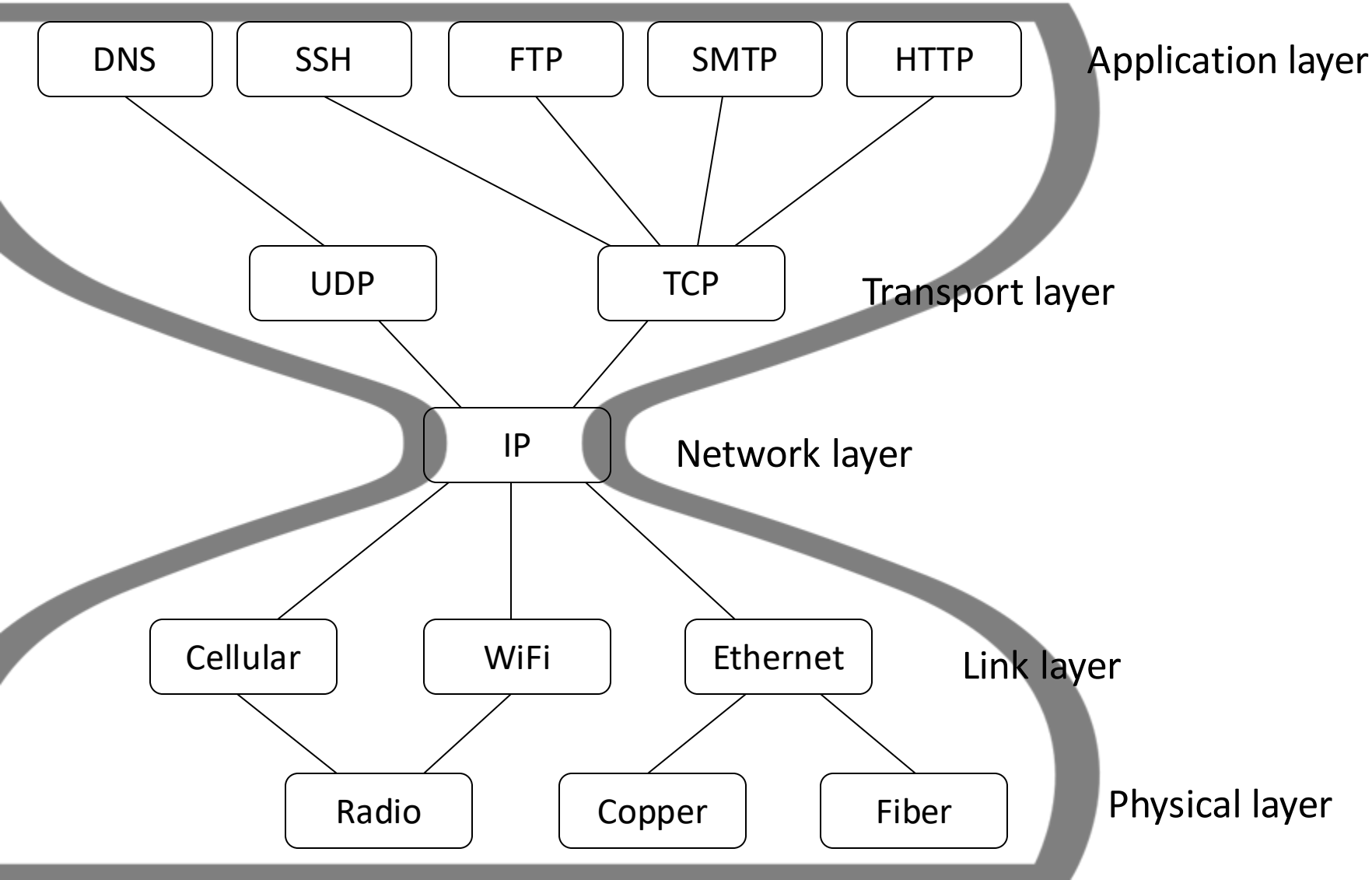
Application Layer

Transport Layer
A TCP segment

Network Layer
An IP packet

Link Layer
An Ethernet frame

Layering of Protocols



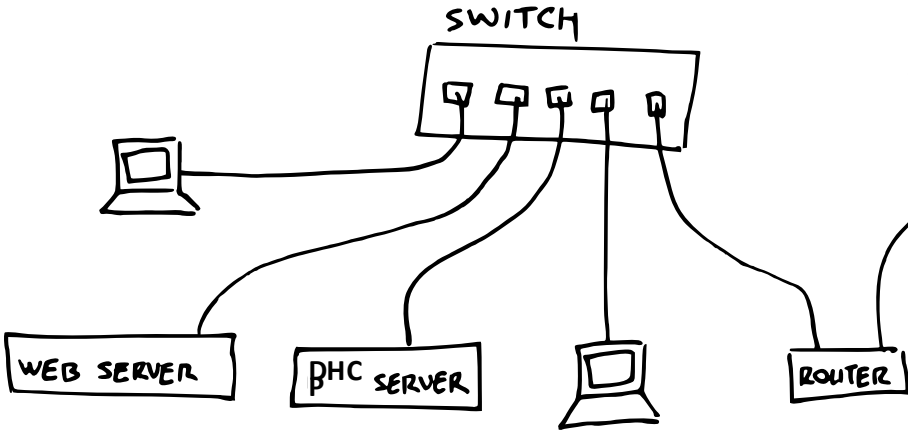
Implications of the Internet's Hourglass Shape?

- Easy to roll out new application protocols (new process)
- Possible, but harder, to roll out new transport protocols
- Easy to deploy new network architectures (e.g., 5G) and new physical media (e.g., fiber)
- A universally agreed upon protocol (IP) for connecting networks together

How does your laptop access the Internet?

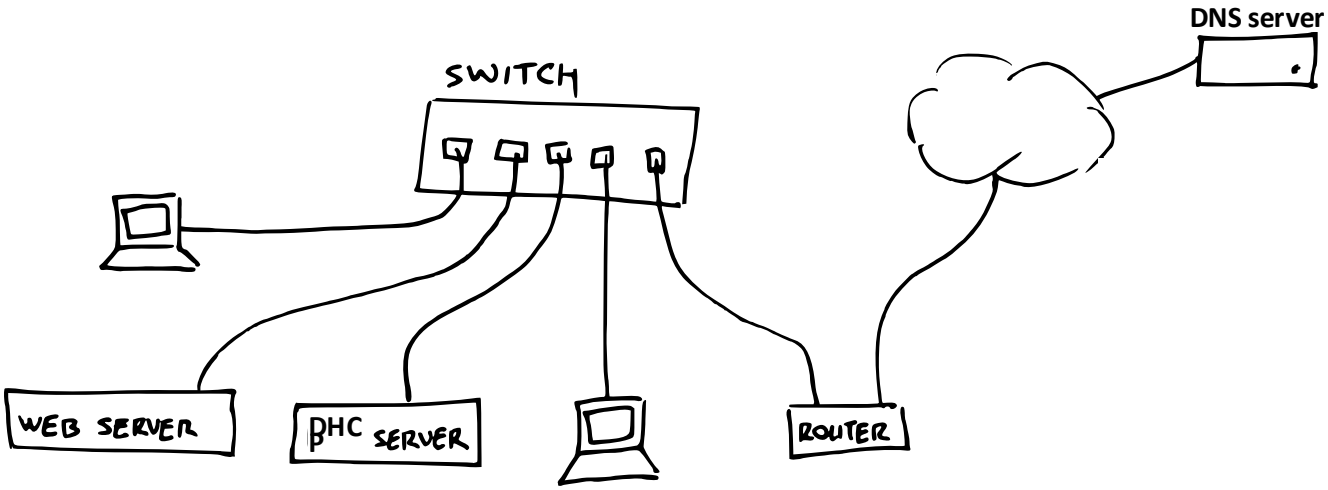
Step 0: Join a local network

- Establish a physical connection
- Get from a DHCP server:
  - IP address for your laptop and lease duration
  - IP address of gateway router
  - IP address of DNS server



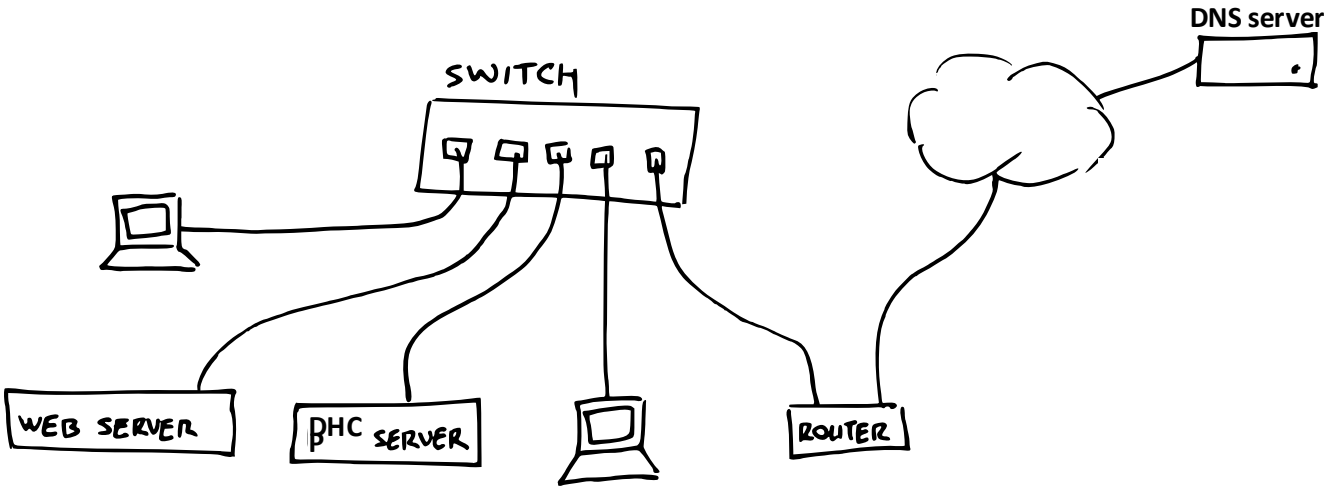
Step 1: DNS Lookup

- You type a URL example.com into the browser
- Browser queries DNS (Domain Name System) server for the IP address of example.com



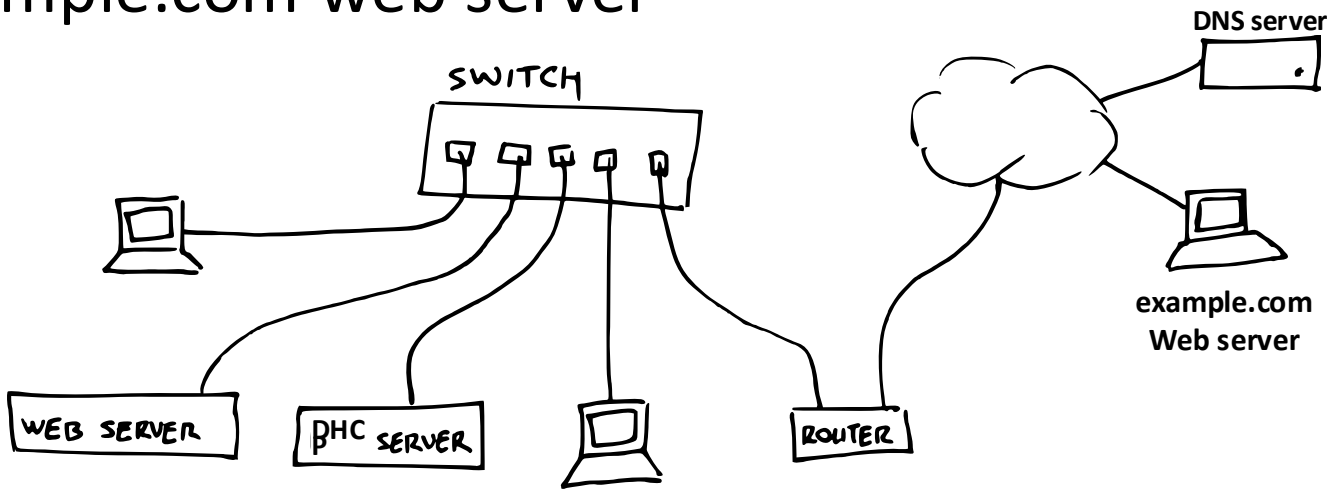
Step 1: DNS Lookup

- DNS is an application-layer protocol
  - Which uses UDP at transport-layer, which uses IP at network-layer, which uses link-layer …
  - Laptop → gateway router → router → … → router → DNS server



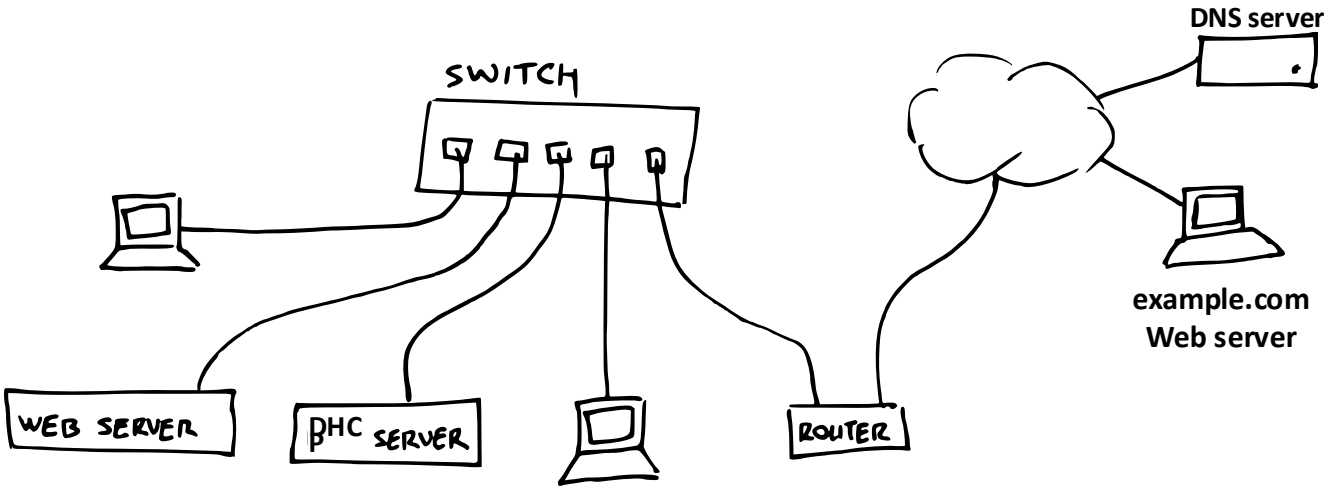
Step 2: TCP Connection

- Set up a TCP connection with example.com
- TCP is a transport-layer protocol
  - IP at network-layer, link-layer, …
  - Laptop → gateway router → router → … → router → example.com web server



Step 3: Start Communicating

- HTTP request and response
  - Using the TCP connection, IP, link-layer, …
  - Laptop → gateway router → router → … → router → example.com web server



(Lay) Security Properties

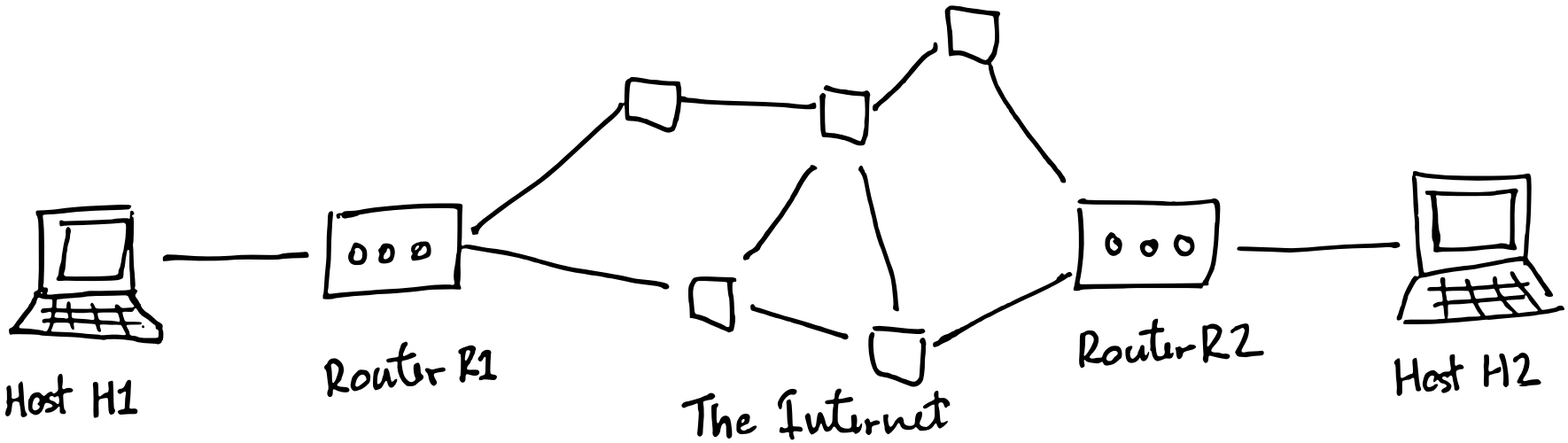
- **Availability:**
  no one can deny me access to services
- **Confidentiality:**
  no one can “see” my private information
- **Integrity:**
  no one can “mess with” my data
- **Authenticity:**
  no can pretend to be someone else

Network Security Properties

- **Availability:**
  attacker can't prevent communication
- **Confidentiality:**
  attacker can't learn protected information
- **Integrity:**
  attacker can't modify communications
- ***Authenticity:***
  attacker can't forge communications

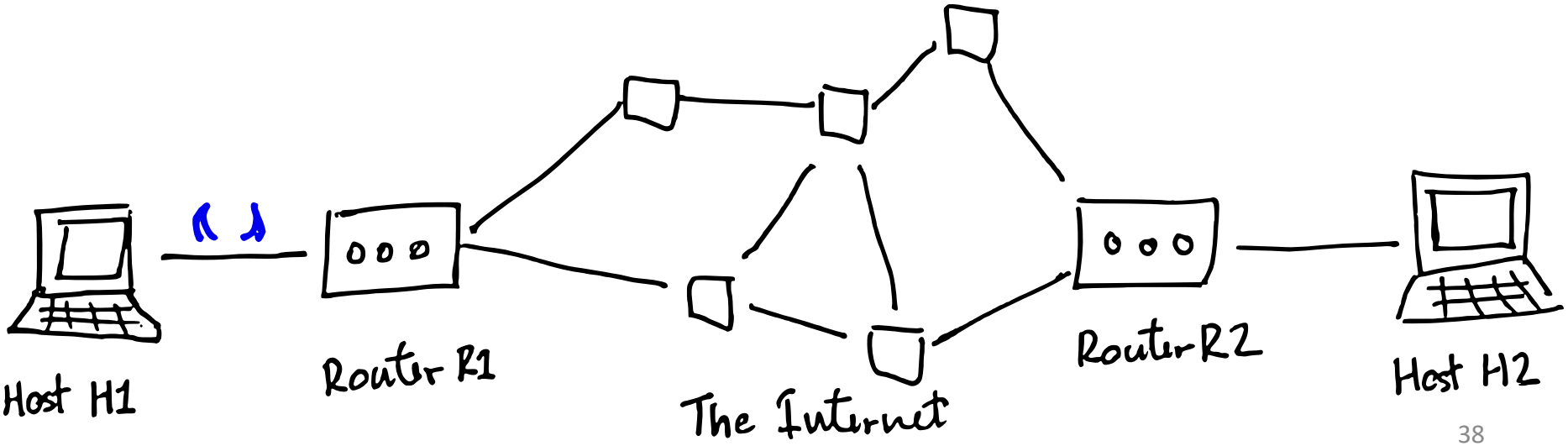
Network Security Threat Model

- Different attacker models:
  - Passive vs. active attackers
  - Off-path vs. on-path attackers



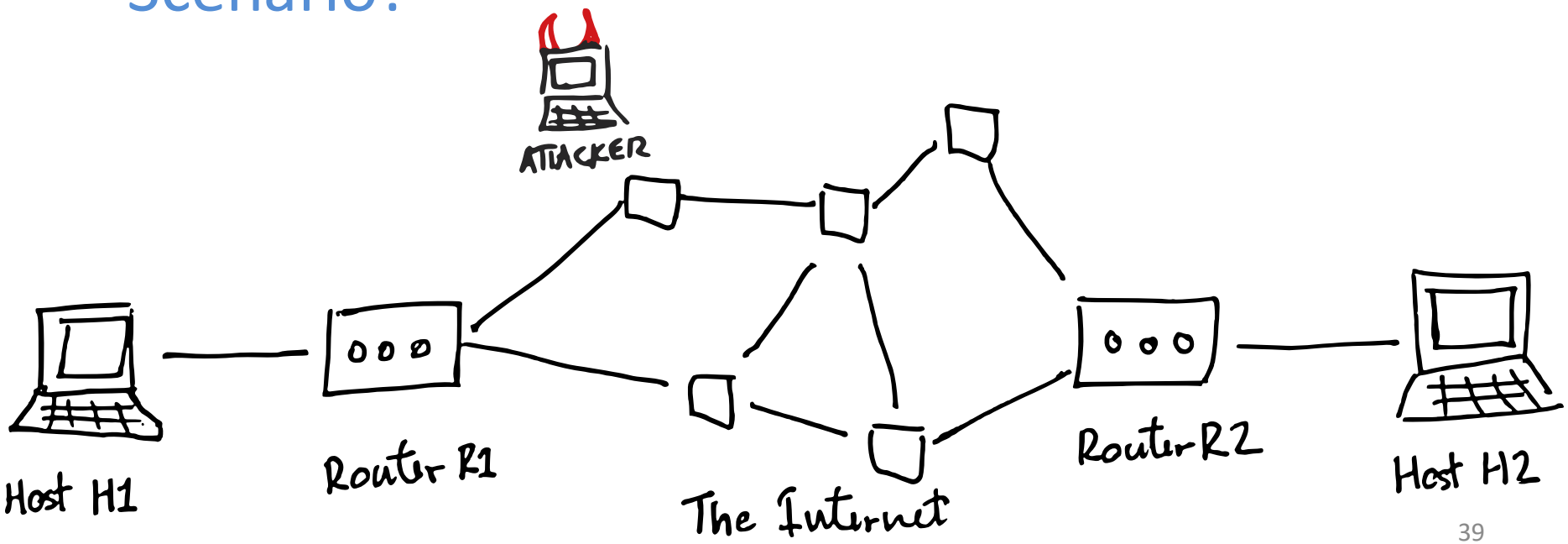
Network Attacker Models

- **Passive (on-path) attacker:** can see all packets but cannot (or will not) modify them
- Scenario?



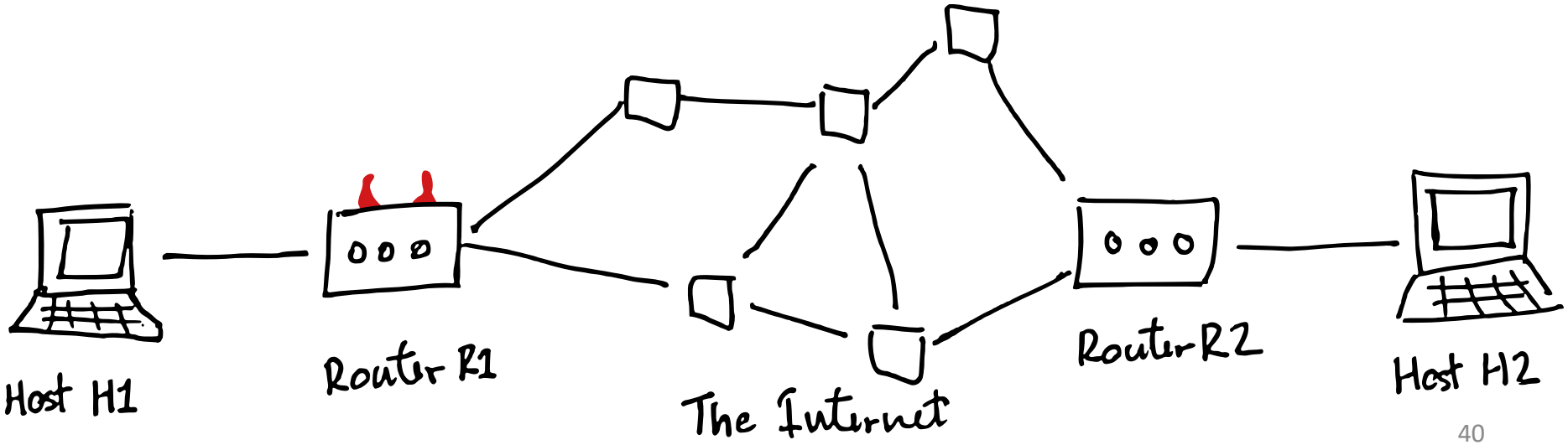
Network Attacker Models

- **Active off-path attacker:** can inject packets into the network, but *cannot* see traffic between hosts
- Scenario?



Network Attacker Models

- **Active on-path (man-in-the-middle) attacker:** can see, modify, inject, and drop all packets
- Scenario?



Network Security Properties

- Which properties may each type of attacker compromise?

	Passive	Off-Path	MitM
Availability			
Confidentiality			
Integrity			
Authenticity			

Network Security Properties

- MitM attacker can see, modify, inject, block traffic

	Passive	Off-Path	MitM
Availability			?
Confidentiality			?
Integrity			?
Authenticity			?

Network Security Properties

- MitM attacker can see, modify, inject, block traffic
- A passive attacker cannot modify or inject packets

	Passive	Off-Path	MitM
Availability	—		?
Confidentiality	?		?
Integrity	—		?
Authenticity	—		?

Network Security Properties

- MitM attacker can see, modify, inject, block traffic
- A passive attacker cannot modify or inject packets
- An off-path attacker cannot see or modify packets (since packets do not go through them by defn)

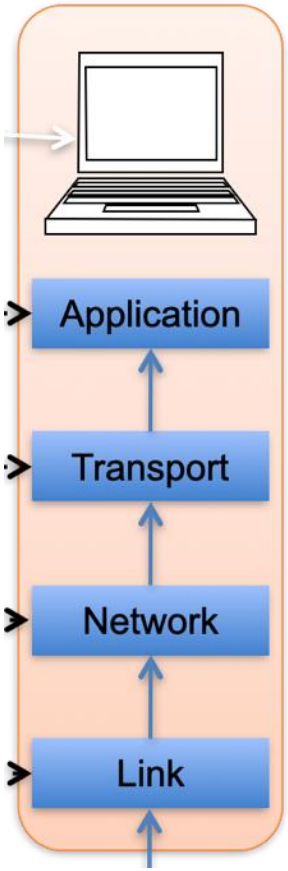
	Passive	Off-Path	MitM
Availability	—	?	?
Confidentiality	?	—	?
Integrity	—	—	?
Authenticity	—	?	?

Network Security Properties

- MitM attacker can see, modify, inject, block traffic
- A passive attacker cannot modify or inject packets
- An off-path attacker cannot see or modify packets (since packets do not go through them by defn)
  - But … may become on-path in poorly designed systems

	Passive	Off-Path	MitM
Availability	—	?	?
Confidentiality	?	— or ?	?
Integrity	—	— or ?	?
Authenticity	—	?	?

Roadmap for Network Security



- April 10 (today): Overview
- April 29 & May 1: DoS, anonymity
- April 24: DNS Security
- April 15 & 17: Transport-layer security
- April 22: Link- and Network-layer security