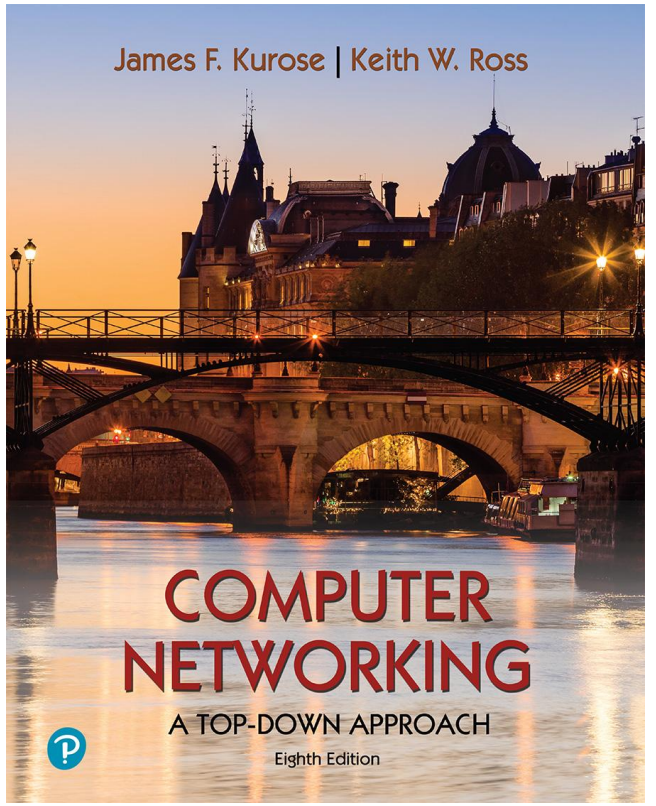
Chapter 1 Introduction

Chuming Qiao/Yaxiong Xie

Department of Computer Science and Engineering
University at Buffalo, SUNY



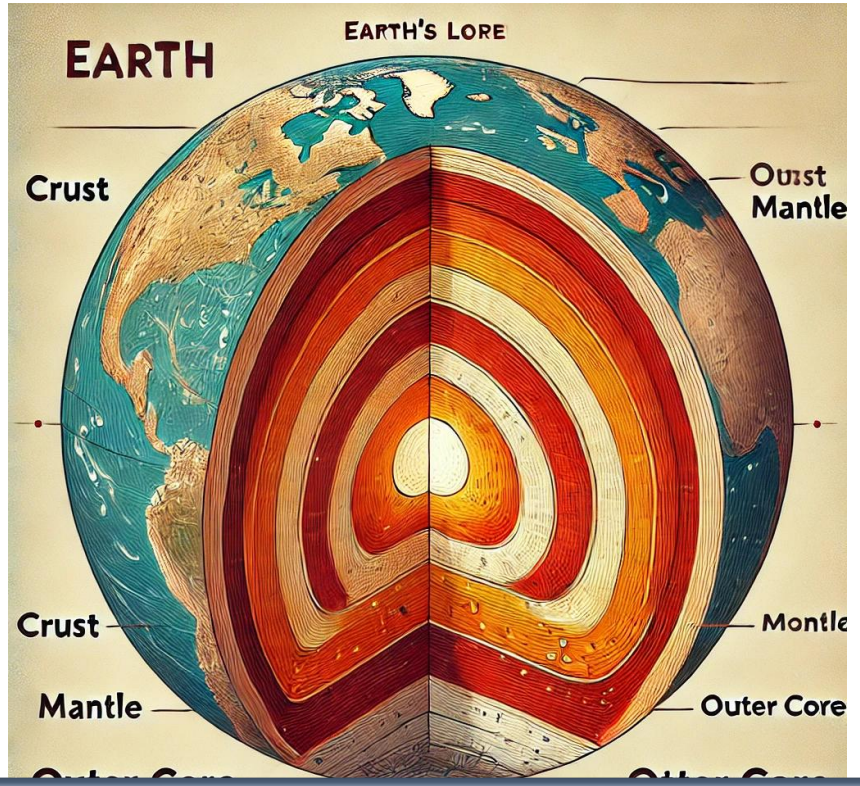
Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Adapted from the slides of the book's authors

Chapter 1: roadmap

- What *is* the Internet?
- What *is* a protocol?
- Network edge: hosts, access network, physical media
- Network core: packet/circuit switching, internet structure
- Performance: loss, delay, throughput
- Protocol layers, service models
- Security
- History

Layers in Computer Networks

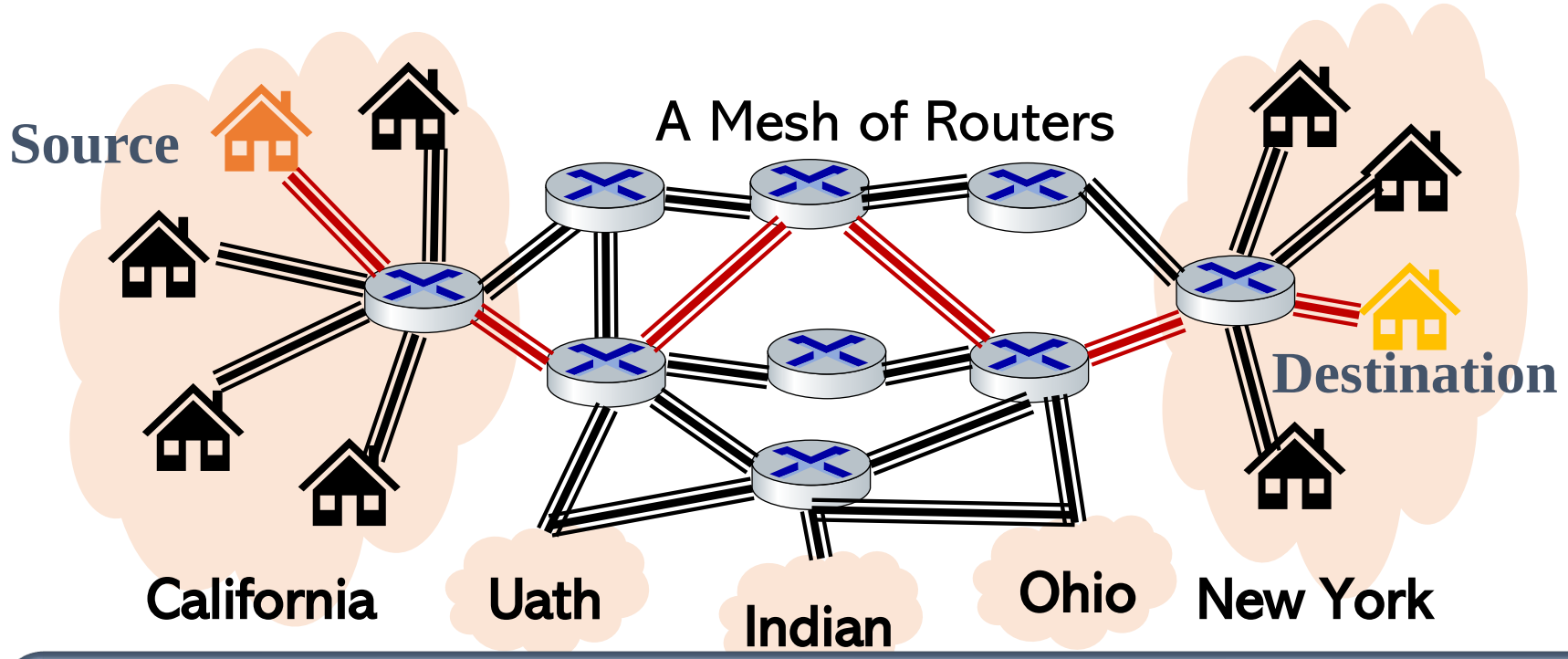


What's Layers in Computer Networks?
Why we need layers?

Layers in Computer Networks

- In computer networking, **layers** refer to different levels of abstraction that help in designing, implementing, and troubleshooting communication systems.
- The idea behind layering is to break down complex networking functions into smaller, manageable parts.
- Each layer performs a specific role and interacts with the layers directly above and below it.

Example: Two types of Computer Networks

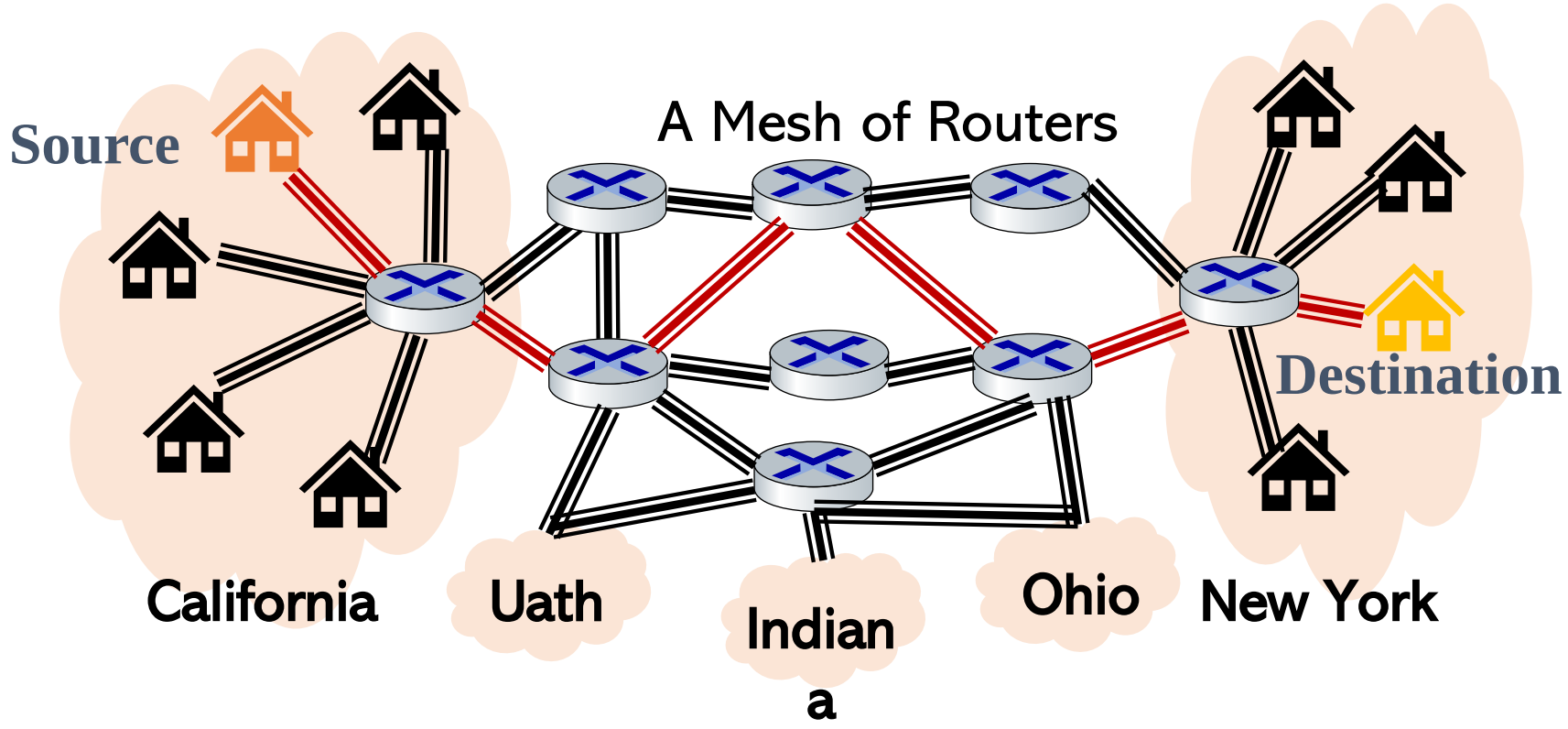


The Network ask: Give me

- **Data you want to transmit**
- **The IP of the destination**
- **Which router the packet should travel**
- **What happens if the packets are dropped**
- **How should I tell you if the**

Of course you can tell the network the answers after you taking this course ☺ !

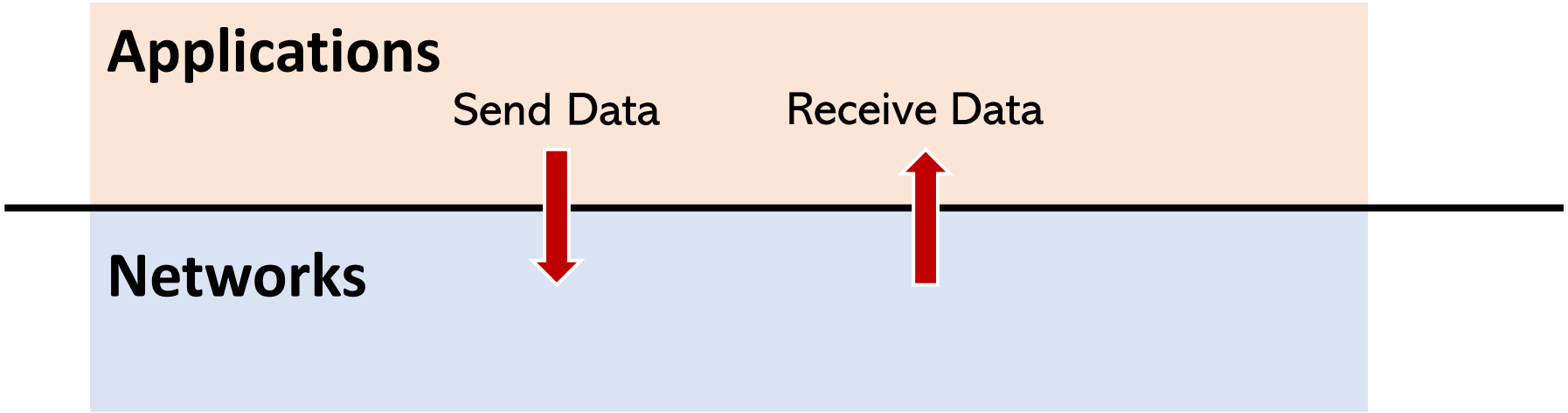
Example: Two types of Computer Networks



Another Network Says

- **Don’t worry, just give me the data and the destination I will handle the other things for you!**

Abstractions make things much simpler



Example: Program Developing

Wi-Fi

Cellular

Qualcomm

BROADCOM

intel

Qualcomm

ERICSSON

MEDIATEK

SAMSUNG

Example: Program Developing

Wi-Fi

Cellular

Qualcomm

BROADCOM

intel

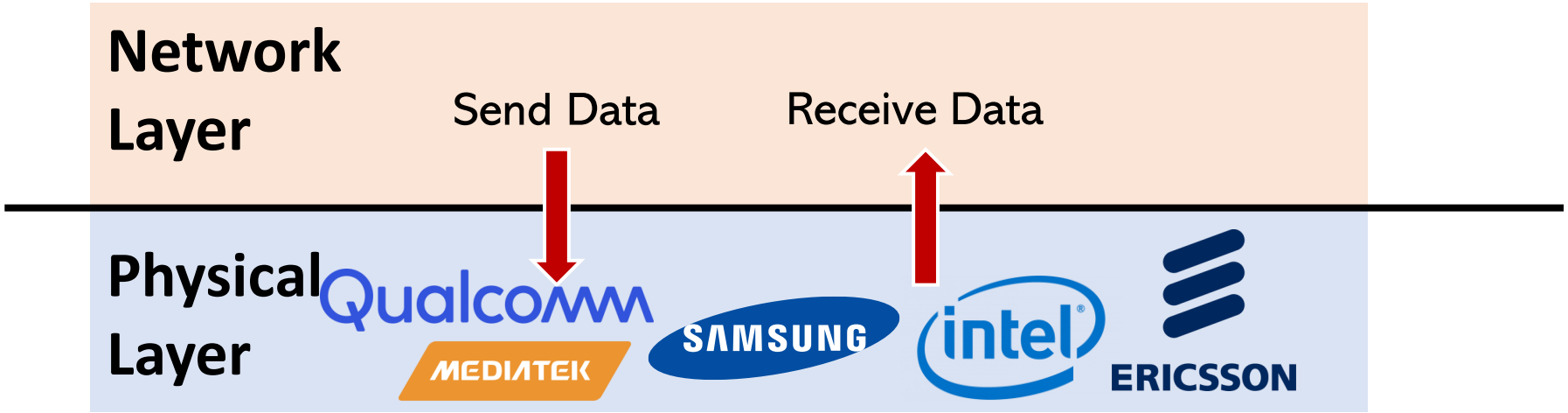
Qualcomm

ERICSSON

MEDIATEK

SAMSUNG

Abstractions enables interoperability



Example: Technology Innovation

200Mbps ⟶ 2 Gbps

Network Layer

Send Data

Receive Data

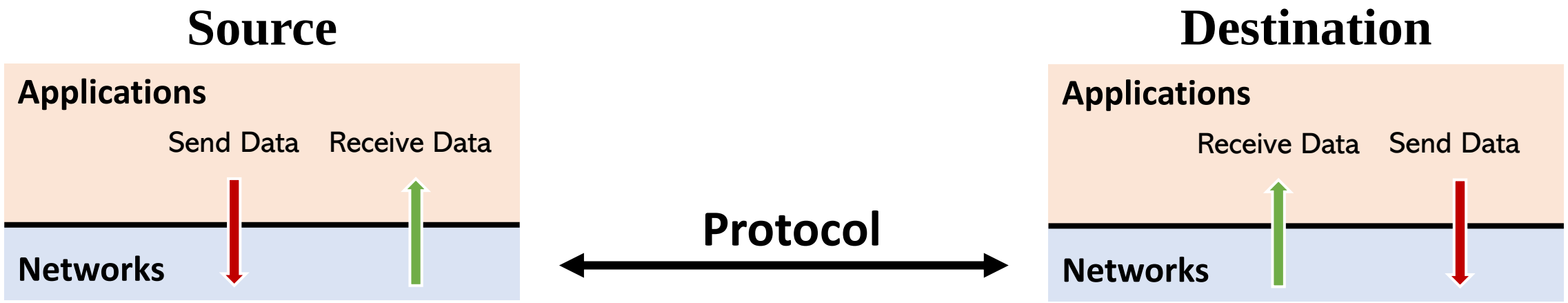
Physical Layer

Qualcomm MEDIATEK SAMSUNG intel ERICSSON

Benefit of Layers

- Modular Design: Makes networking easier to understand and manage.
- Interoperability: Ensures different systems and technologies can communicate.
- Abstraction: Allows developers to focus on specific functions without worrying about the entire network.
- Innovation: Easy to deploy new technology without changing the whole network stack
- Troubleshooting: Simplifies diagnosing issues by isolating problems within specific layers.

Structure of the layer design

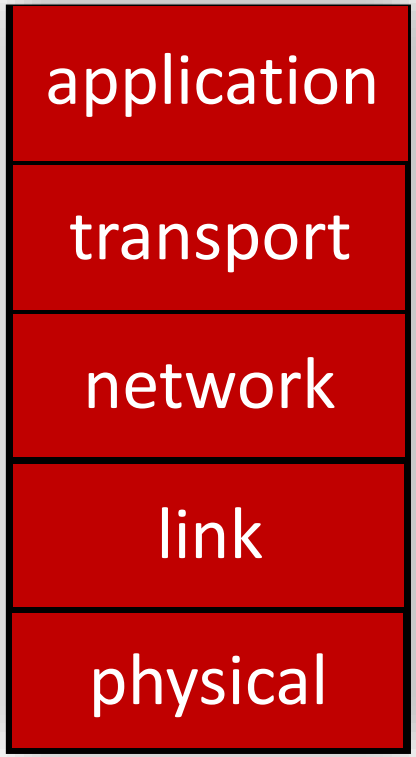


- **Service:** **What** a layer does
- **Service interface:** **How to access** the service
  - Interface for the layer **above**

- **Protocol interface:** **How peers communicate** to implement service
  - Set of rules and formats that govern the communication **between two Internet hosts**

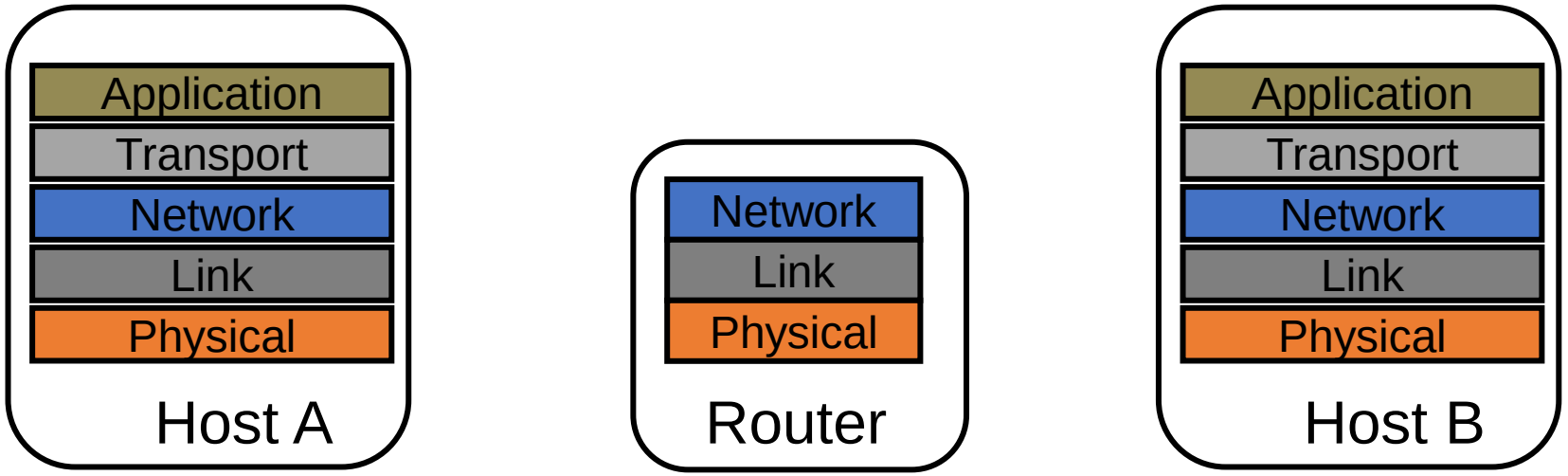
Layered Internet protocol stack

- *application:* supporting network applications
  - HTTP, IMAP, SMTP, DNS
- *transport:* process-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.11 (WiFi), PPP
- *physical:* bits “on the wire”



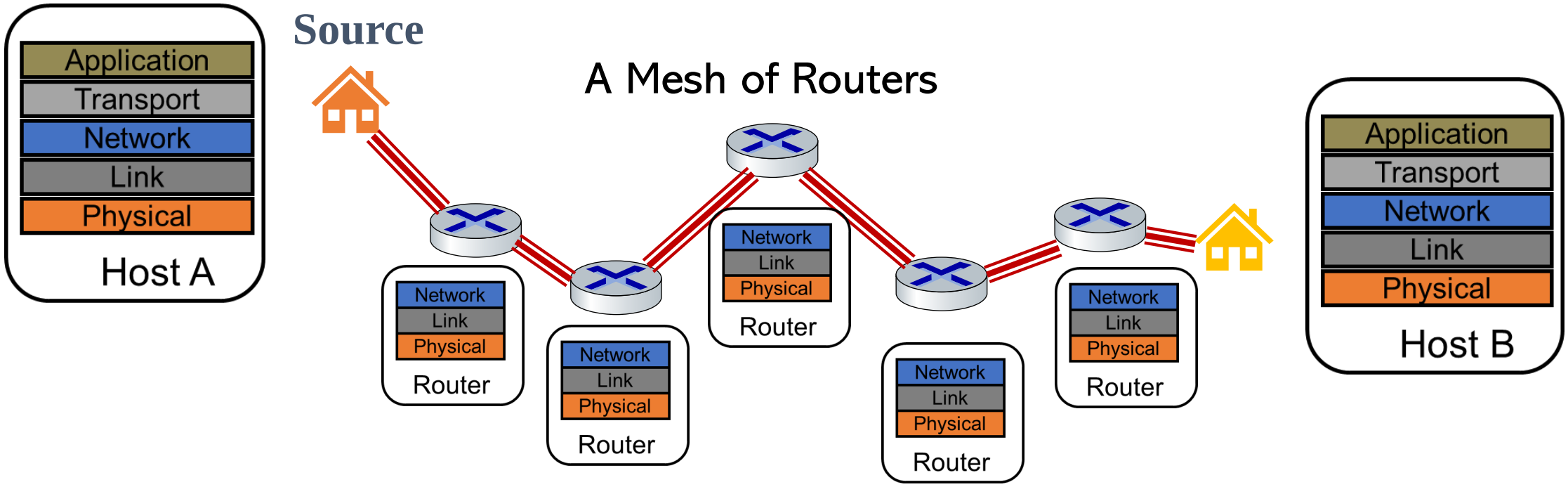
Layers inside network

- Five layers
  - **Lower three layers** are implemented **everywhere**
  - **Top two layers** are implemented **only at end hosts**
    - **Their protocols are *end-to-end***



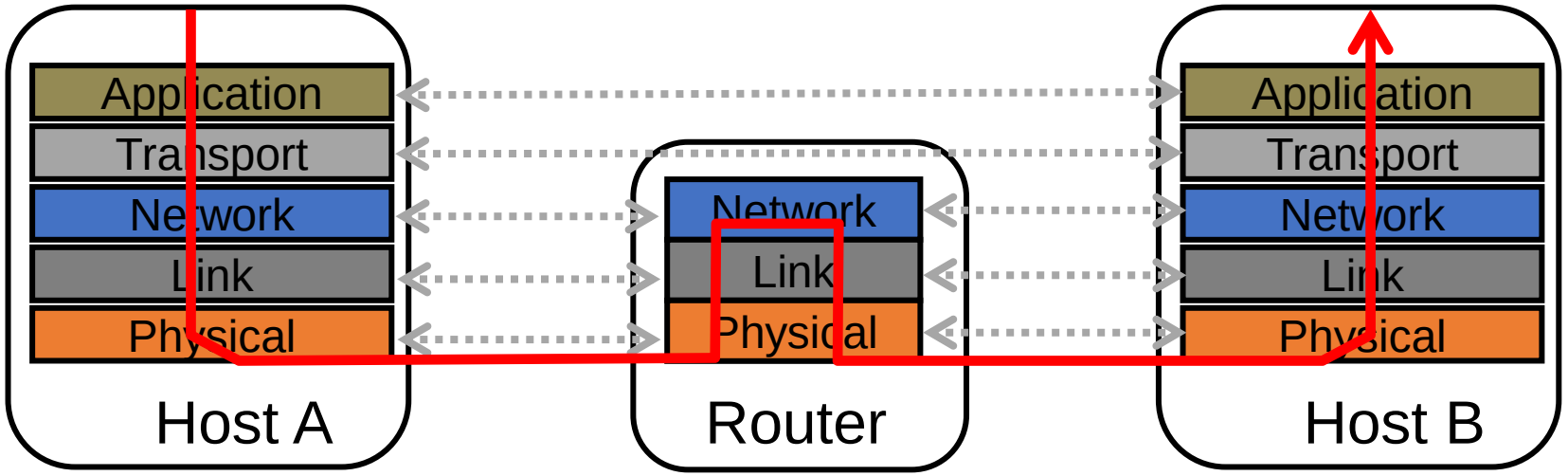
Layers inside network

- Five layers
  - **Lower three layers** are implemented **everywhere**
  - **Top two layers** are implemented **only at end hosts**
    - **Their protocols are *end-to-end***



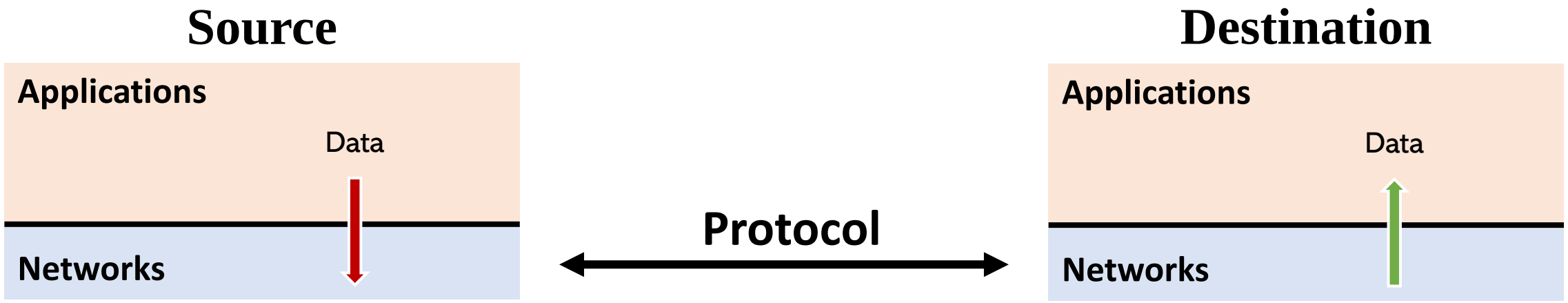
Physical path across the Internet

- Communication **goes down to physical network**
- Then from **network peer to peer**
- Then **up to the relevant layer**



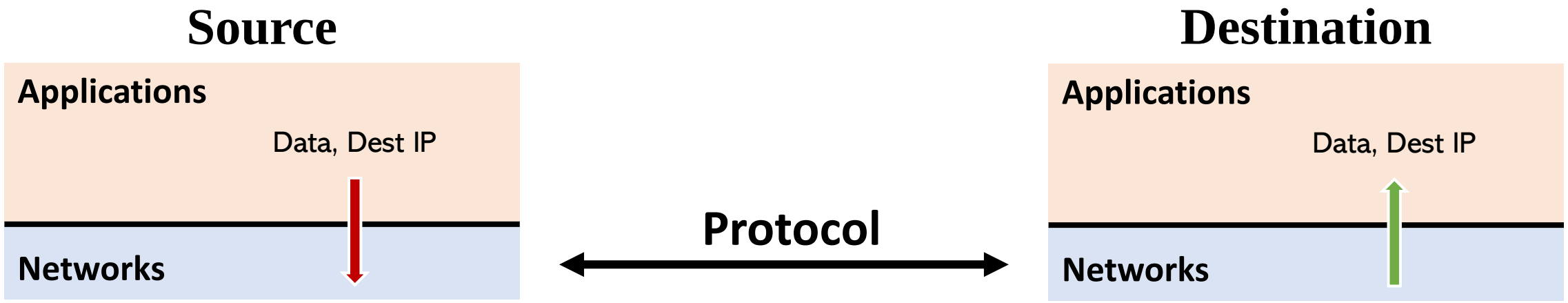
Encapsulation in Networks

- Addressing



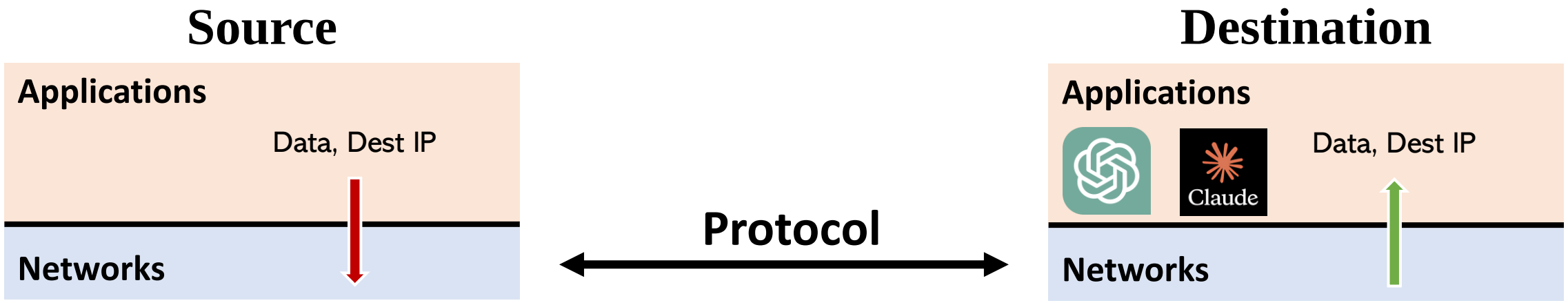
Encapsulation in Networks

- Addressing and routing



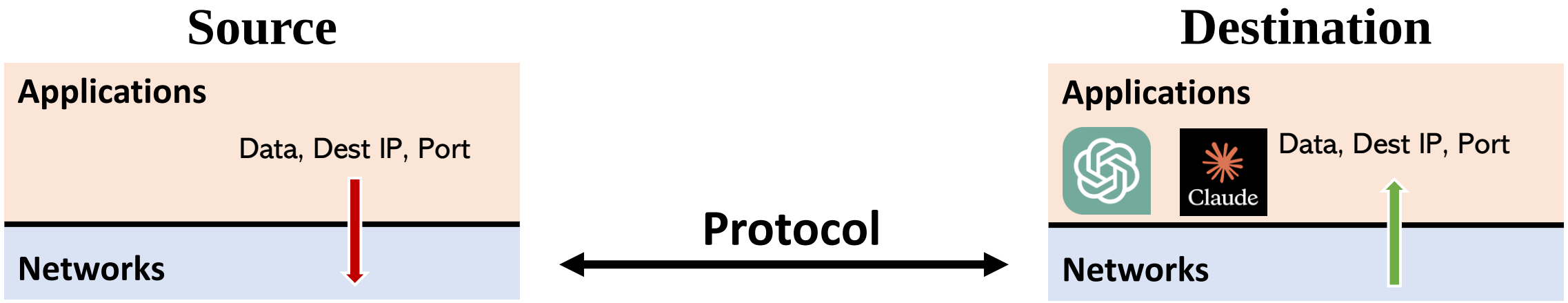
Encapsulation in Networks

- Addressing and routing
- Multiplexing



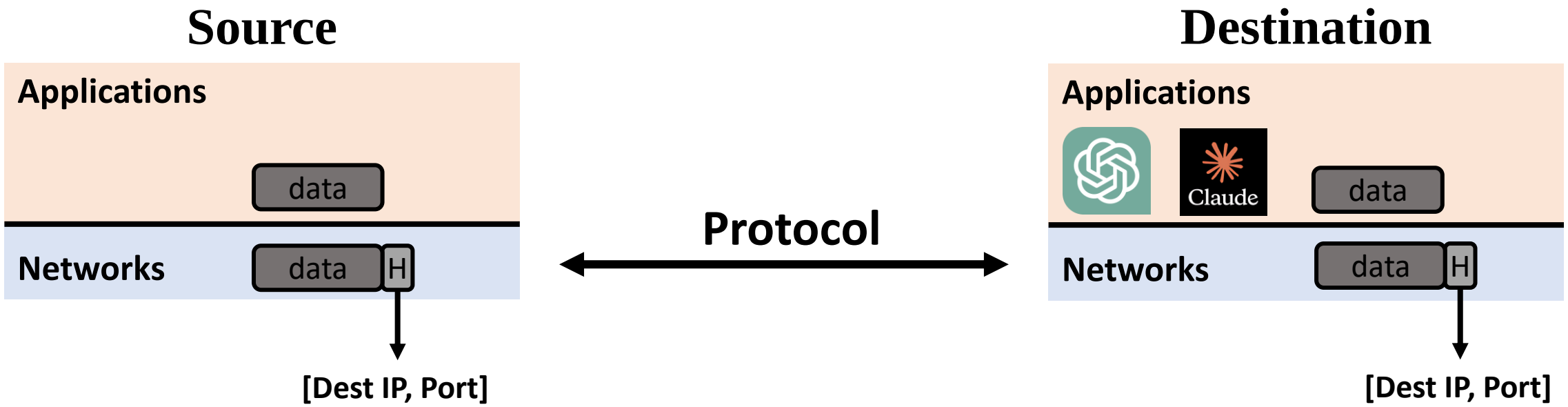
Encapsulation in Networks

- Addressing and routing
- Multiplexing



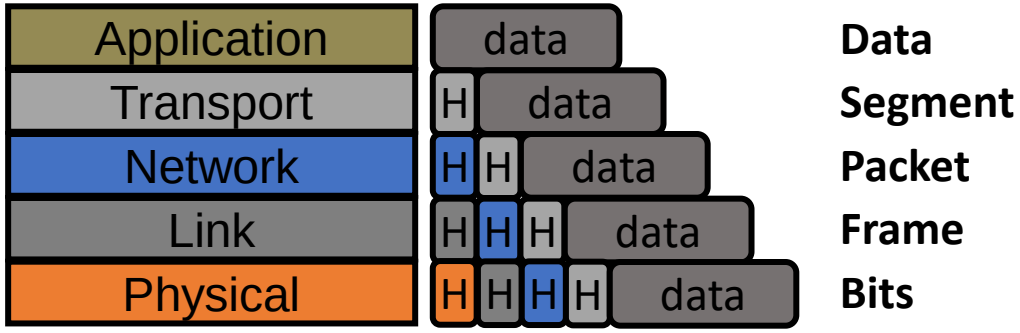
Encapsulation in Networks

- Addressing and routing
- Multiplexing



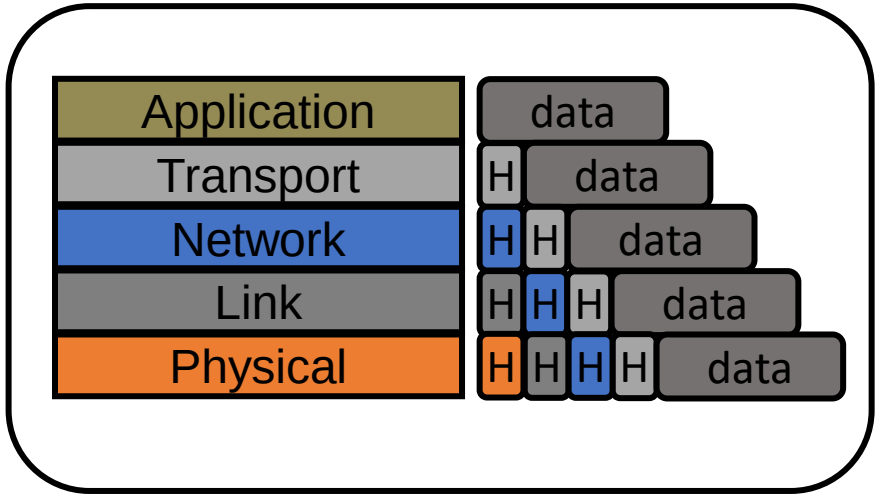
Encapsulation in Networks

- Encapsulation happens at all the layers

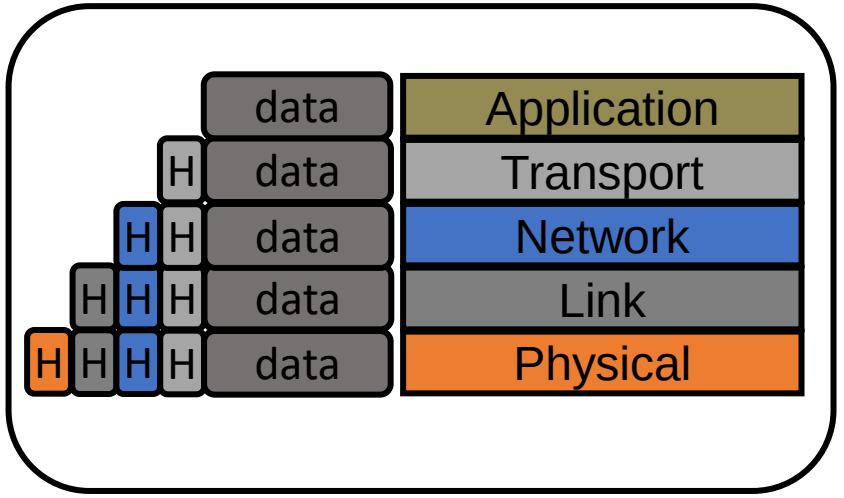


Encapsulation in Networks

- Encapsulation happens at all the layers
- On reception, layer **inspects and removes** its own header
  - Higher layers **don't see** lower layers' headers

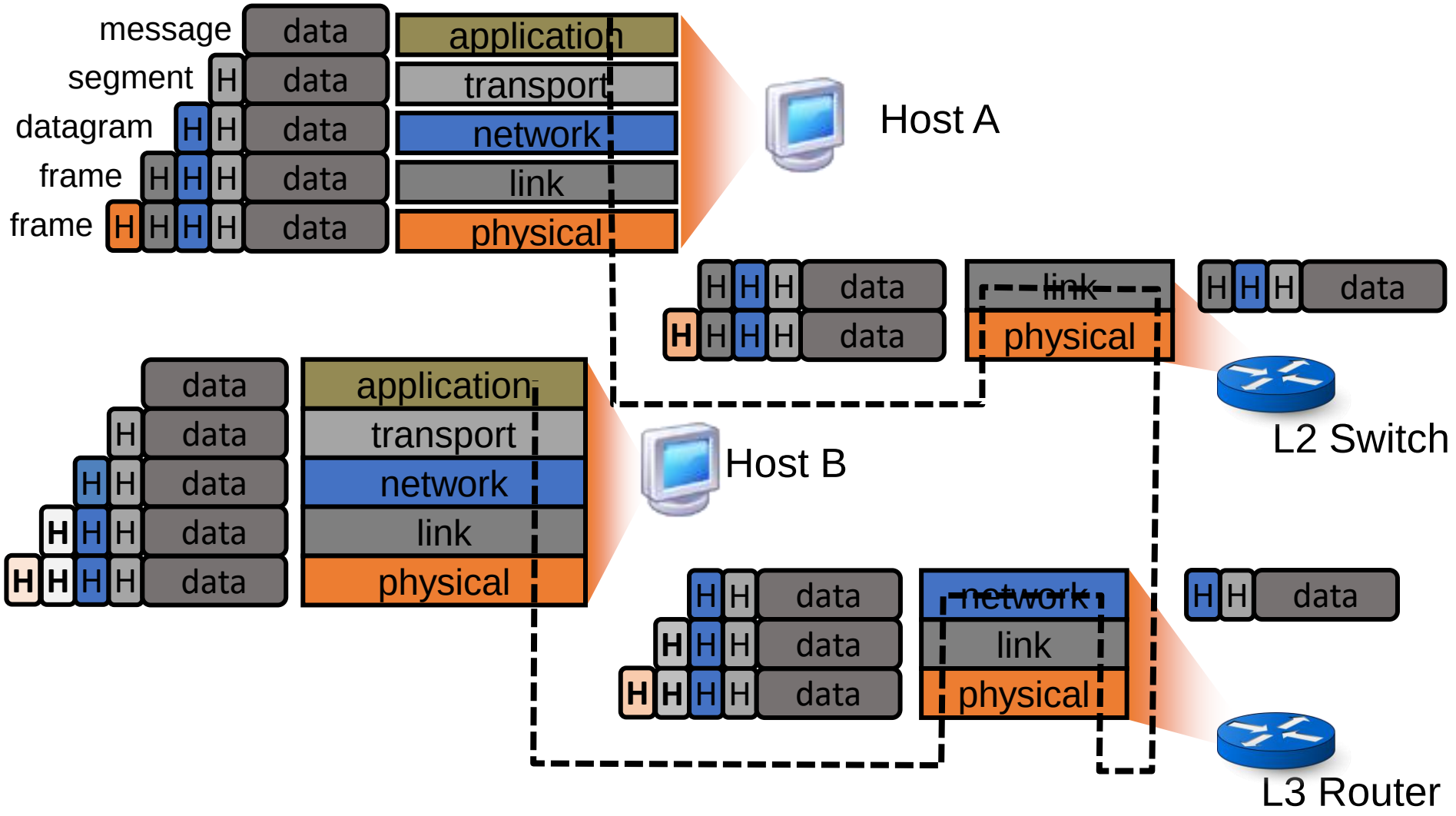


Host A



Host B

Encapsulation in the Internet



Chapter 1: roadmap

- What *is* the Internet?
- What *is* a protocol?
- Network edge: hosts, access network, physical media
- Network core: packet/circuit switching, internet structure
- Performance: loss, delay, throughput
- Protocol layers, service models
- Security
- History

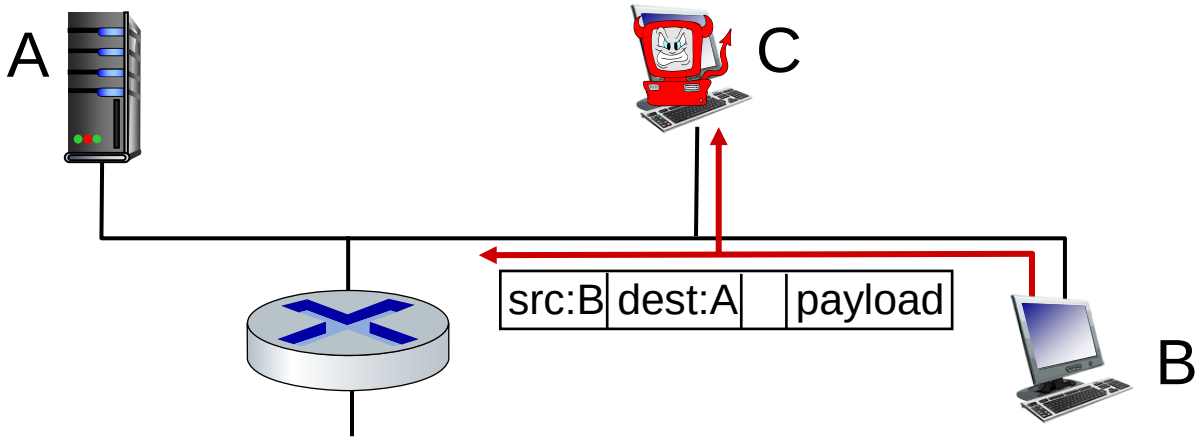
Network security

- Internet not originally designed with (much) security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network" ☺
  - Internet protocol designers playing "catch-up"
  - security considerations in all layers!
- We now need to think about:
  - how bad guys can attack computer networks
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks

Bad guys: packet interception

packet "sniffing":

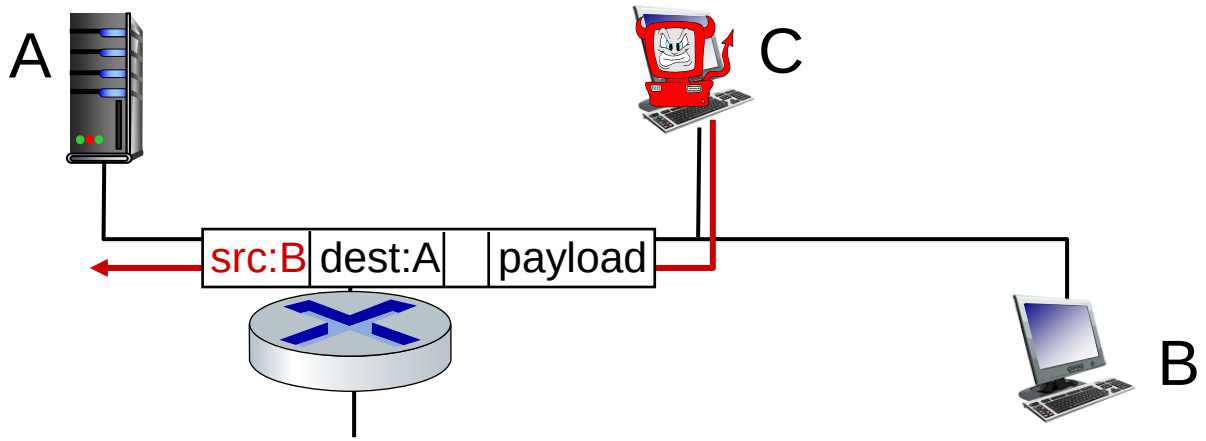
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



Wireshark software used for our end-of-chapter labs is a (free) packet-sniffer

Bad guys: fake identity

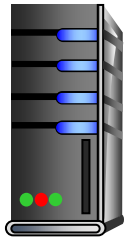
IP spoofing: injection of packet with false source address



Bad guys: denial of service

Denial of Service (DoS): attackers make resource (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

Client

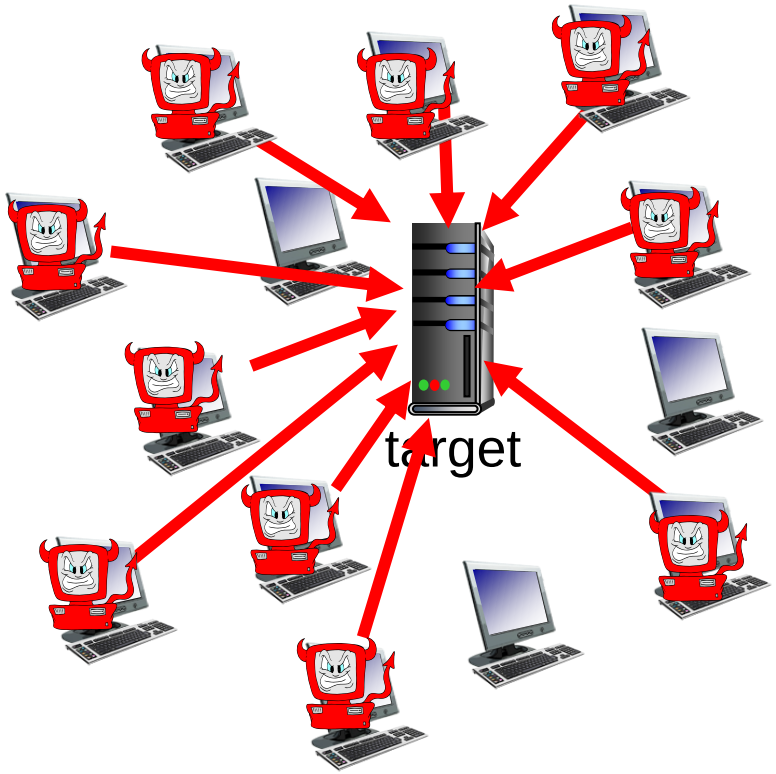


Server

Bad guys: denial of service

Denial of Service (DoS): attackers make resource (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

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



Lines of defense:

- authentication: proving you are who you say you are
  - cellular networks provides hardware identity via SIM card; no such hardware assist in traditional Internet
- confidentiality: via encryption
- integrity checks: digital signatures prevent/detect tampering
- access restrictions: password-protected VPNs
- firewalls: specialized "middleboxes" in access and core networks:
  - off-by-default: filter incoming packets to restrict senders, receivers, applications
  - detecting/reacting to DOS attacks

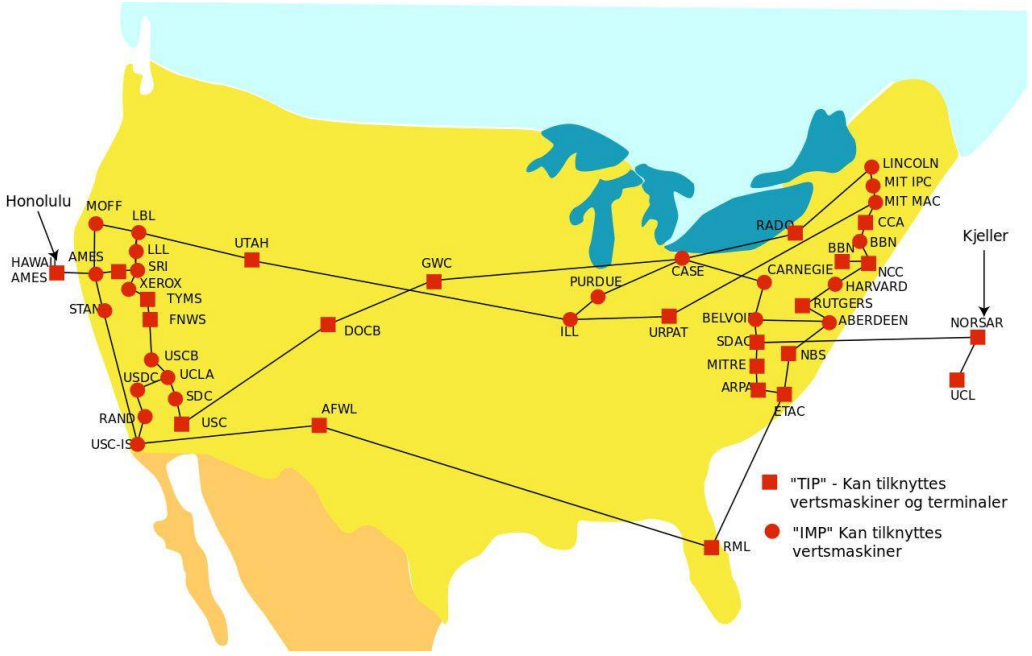
Chapter 1: roadmap

- What *is* the Internet?
- What *is* a protocol?
- Network edge: hosts, access network, physical media
- Network core: packet/circuit switching, internet structure
- Performance: loss, delay, throughput
- Security
- Protocol layers, service models
- History

ARPANET – The Birth of the Internet (1969)

- Funded by DARPA (U.S. Defense Advanced Research Projects Agency).
- First message sent **Oct 29, 1969** between UCLA and Stanford.
- Key technology: **Packet switching**.
  - Connected universities and research institutions.

The first message sent over ARPANET happened on Oct. 29, 1969. Charley Kline, who was a student at the University of California Los Angeles (UCLA), tried to log in to the mainframe at the Stanford Research Institute (SRI). He successfully typed in the characters *L* and *O*, but the computer crashed when he typed the *G* of the command `LOGIN`. They were able to overcome the initial crash, however, and had a successful connection that same day.



Expanding ARPANET and TCP/IP (1970s-1980s)

- **1973:** First international connection (UK & Norway).
- **1974: TCP/IP protocol** proposed by **Vinton Cerf & Bob Kahn**.
- **1983:** ARPANET switches to **TCP/IP**, officially creating the Internet.
  - **1986: NSFNET** expands network beyond military & academia.

Commercialization and the World Wide Web (1990s)

- **1991:** Tim Berners-Lee develops **World Wide Web (WWW)**.
- **1993:** First web browser **Mosaic** released (led to Netscape).
- **1995:** NSF lifts commercial restrictions → **Birth of Internet Service Providers (ISPs)**.
- **1998:** Google founded, changing web search.

The Dot-Com Boom and Wireless Internet (2000s)

- Rise of **e-commerce (Amazon, eBay, PayPal)**.
- **Wi-Fi, broadband, mobile networks** increase connectivity.
- **2004:** Facebook launches, followed by **social media explosion**.
- **2007:** Apple releases the **iPhone**, boosting mobile Internet.

Modern Internet (2010s-Present)

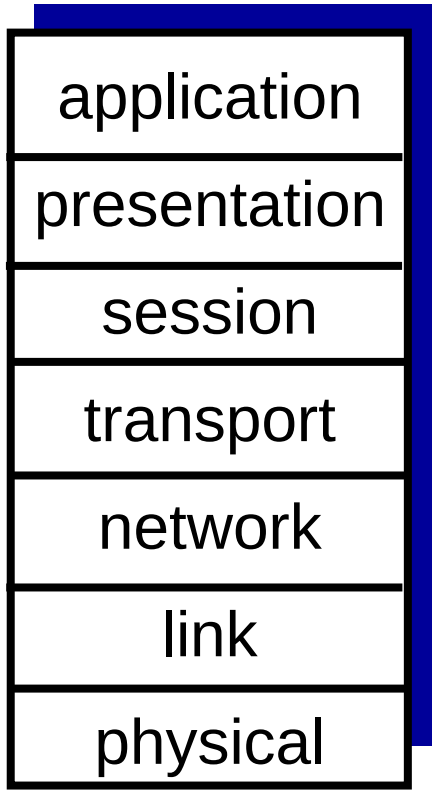
- Cloud computing, streaming services, and 5G.
- **IoT (Internet of Things)** connects smart devices.
- **AI & Machine Learning** reshape content delivery.

Additional Chapter 1 slides

ISO/OSI reference model

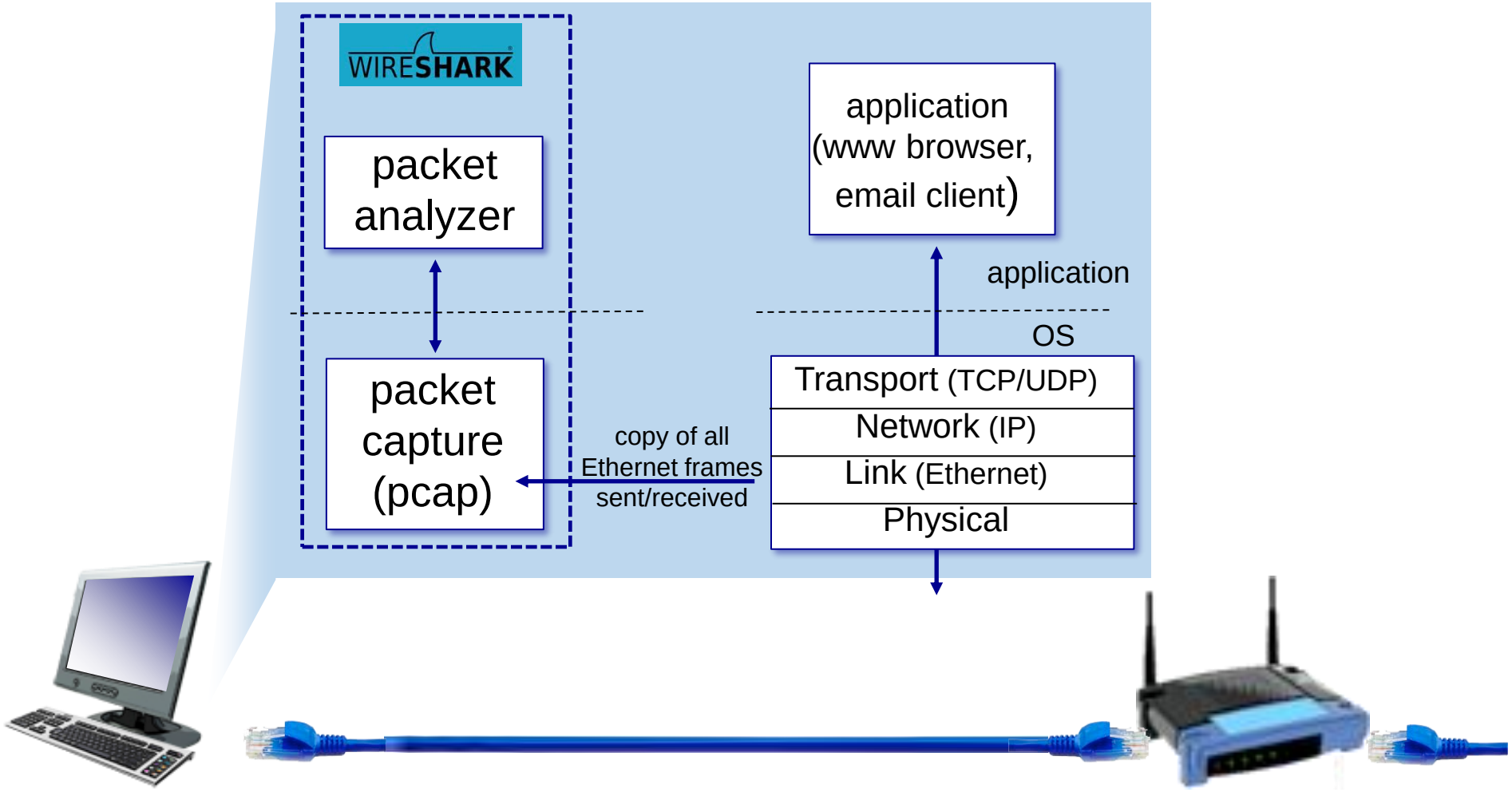
Two layers not found in Internet protocol stack!

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



The seven layer OSI/ISO reference model

Wireshark


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