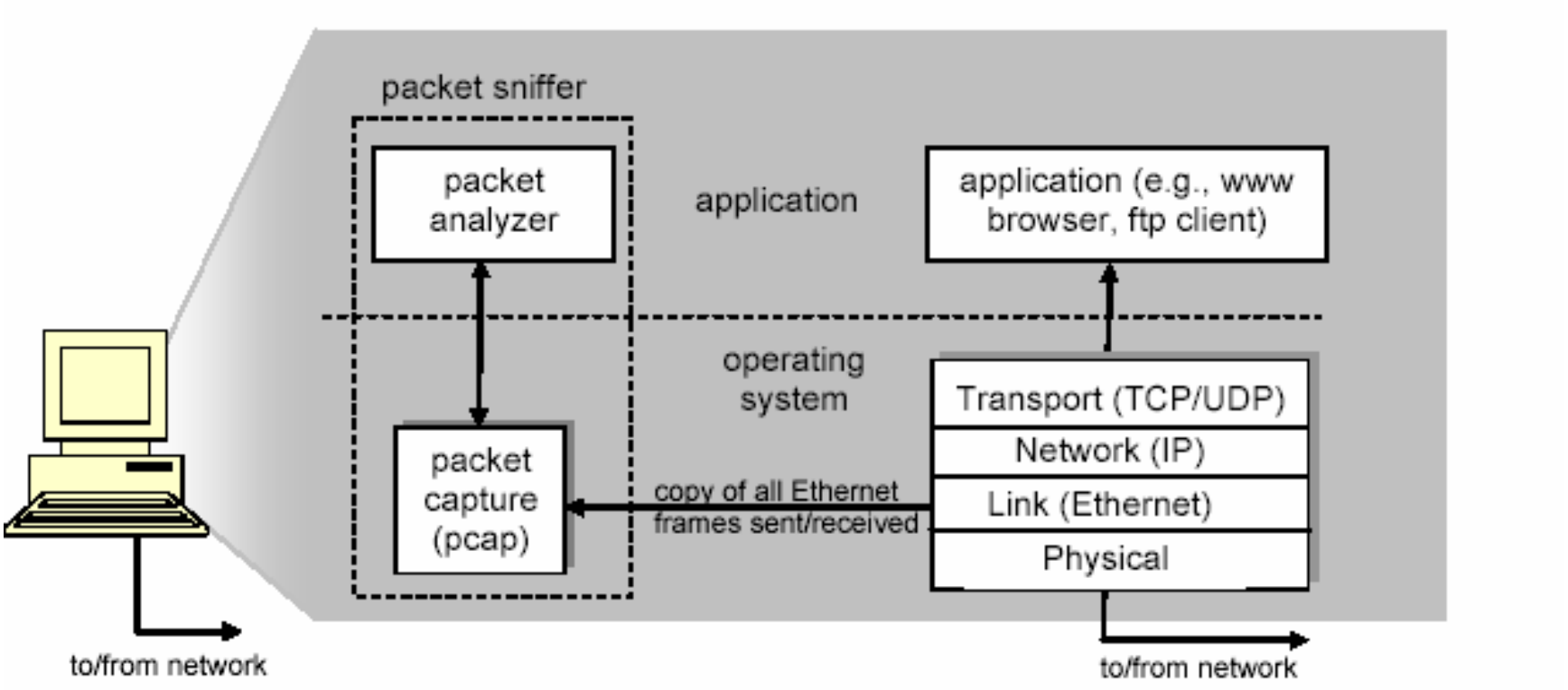
Lab 1: Packet Sniffing and Wireshark

Fengwei Zhang

Packet Sniffer

- Packet sniffer is a basic tool for observing network packet exchanges in a computer
- Capturing ("sniffs") packets being sent/received from/ by your computer
- A packet sniffer itself is passive
- Displaying the contents of the various protocol fields in these captured packets, but never sending packets itself

Packet Sniffer Structure



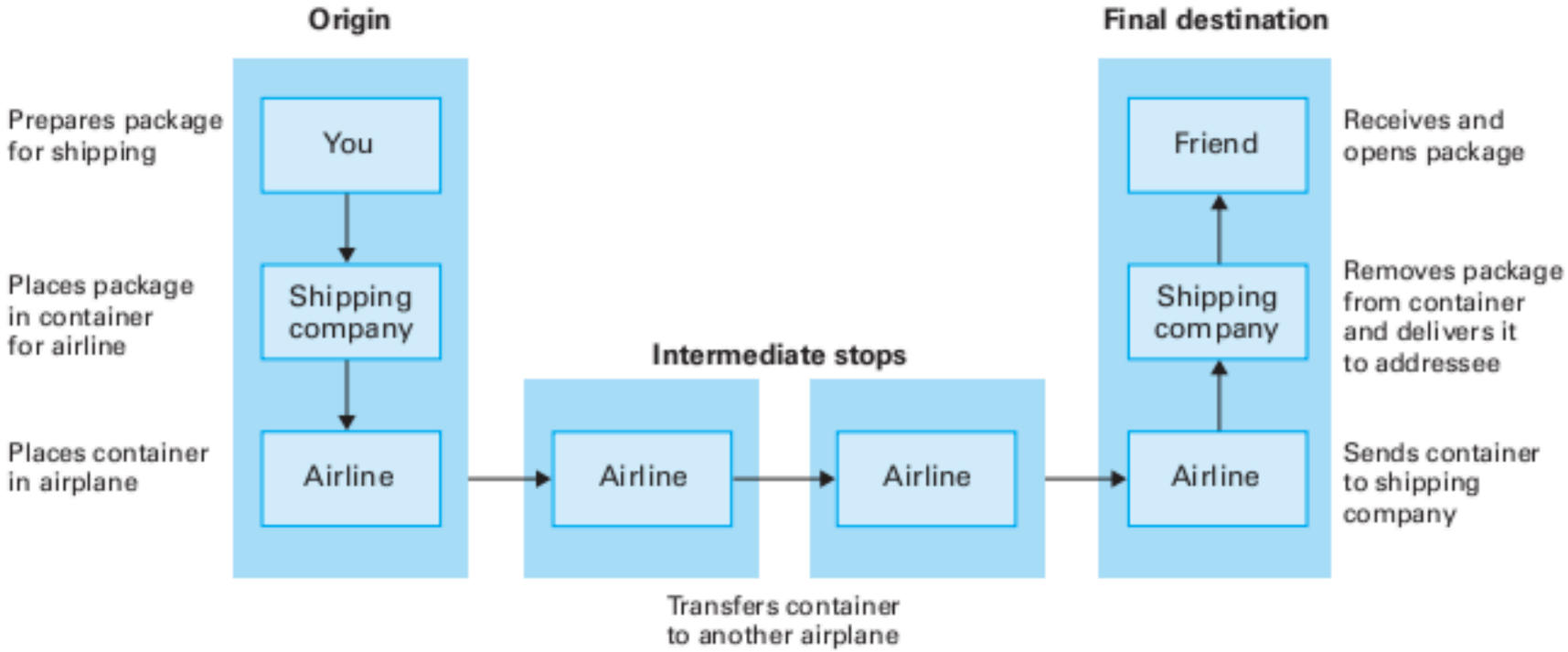
Packet Sniffer (cont'd)

- Applications (web browsers, FTP clients, email clients)
- Network protocols (Internet protocol)
- Packet capture
  - The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer
- Packet Analyzer
  - Displaying the contents of all fields within a protocol message
  - Understanding the structure of all messages exchanged by protocols
  - IP, TCP, HTTP headers
- Wireshark, TCPDump

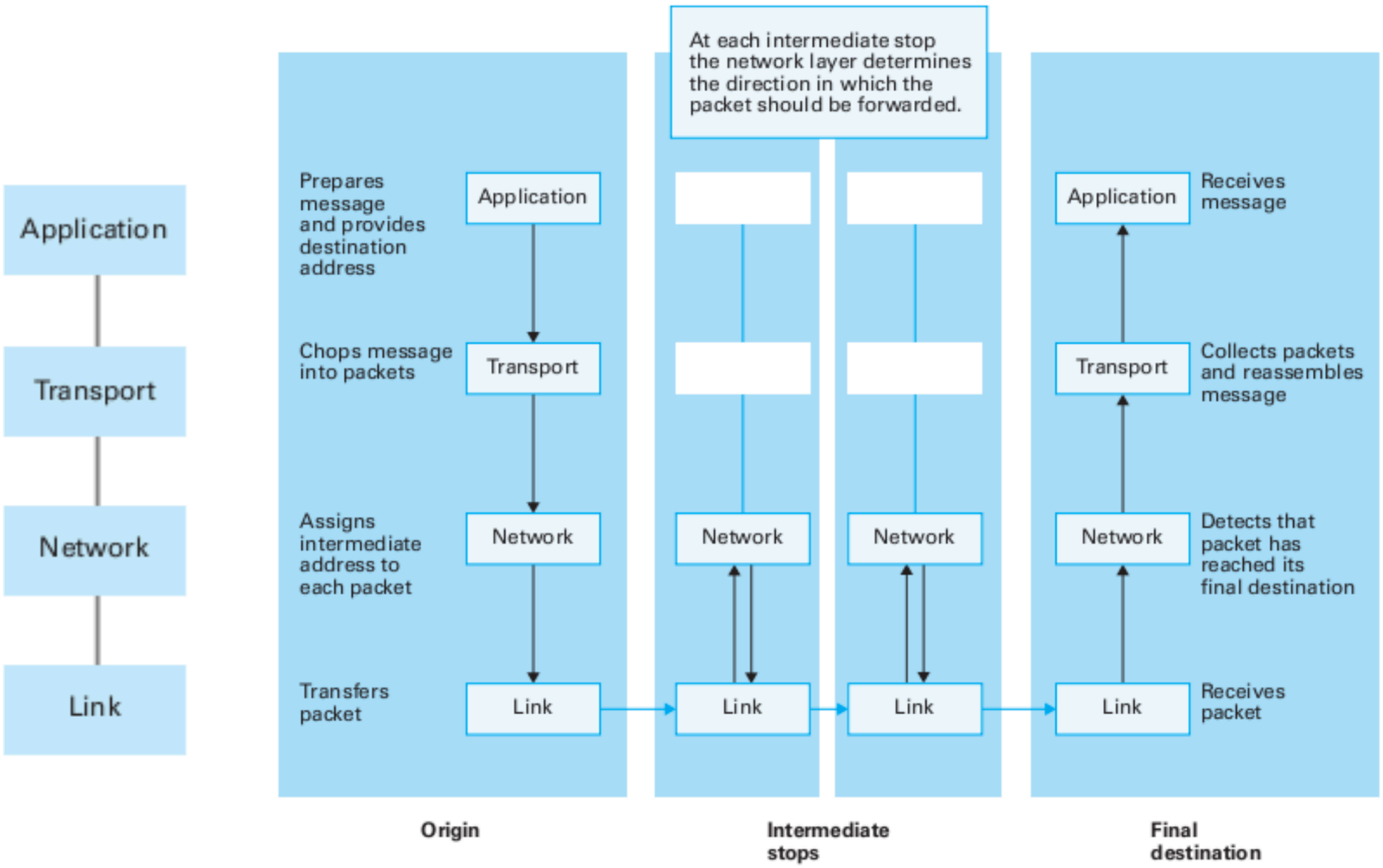
TCP/IP Network Stack

- TCP/IP is the most commonly used network model for Internet services.
- Because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP) were the first networking protocols defined in this standard, it is named as TCP/IP.
- It contains multiple layers including:
  - Application layer
  - Transport layer
  - Network layer
  - Data link layer

An Example Layered Approach



Network Layers



Application Layer

- The application layer includes the protocols used by most applications for providing user services

- Examples of application layer protocols are Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP)

Transport Layer

- The transport layer establishes process-to-process connectivity, and it provides end-to-end services that are independent of underlying user data.

- To implement the process-to-process communication, the protocol introduces a concept of port. The examples of transport layer protocols are Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

- The TCP provides flow control, connection establishment, and reliable transmission of data, while the UDP is a connectionless transmission model.

Internet Layer

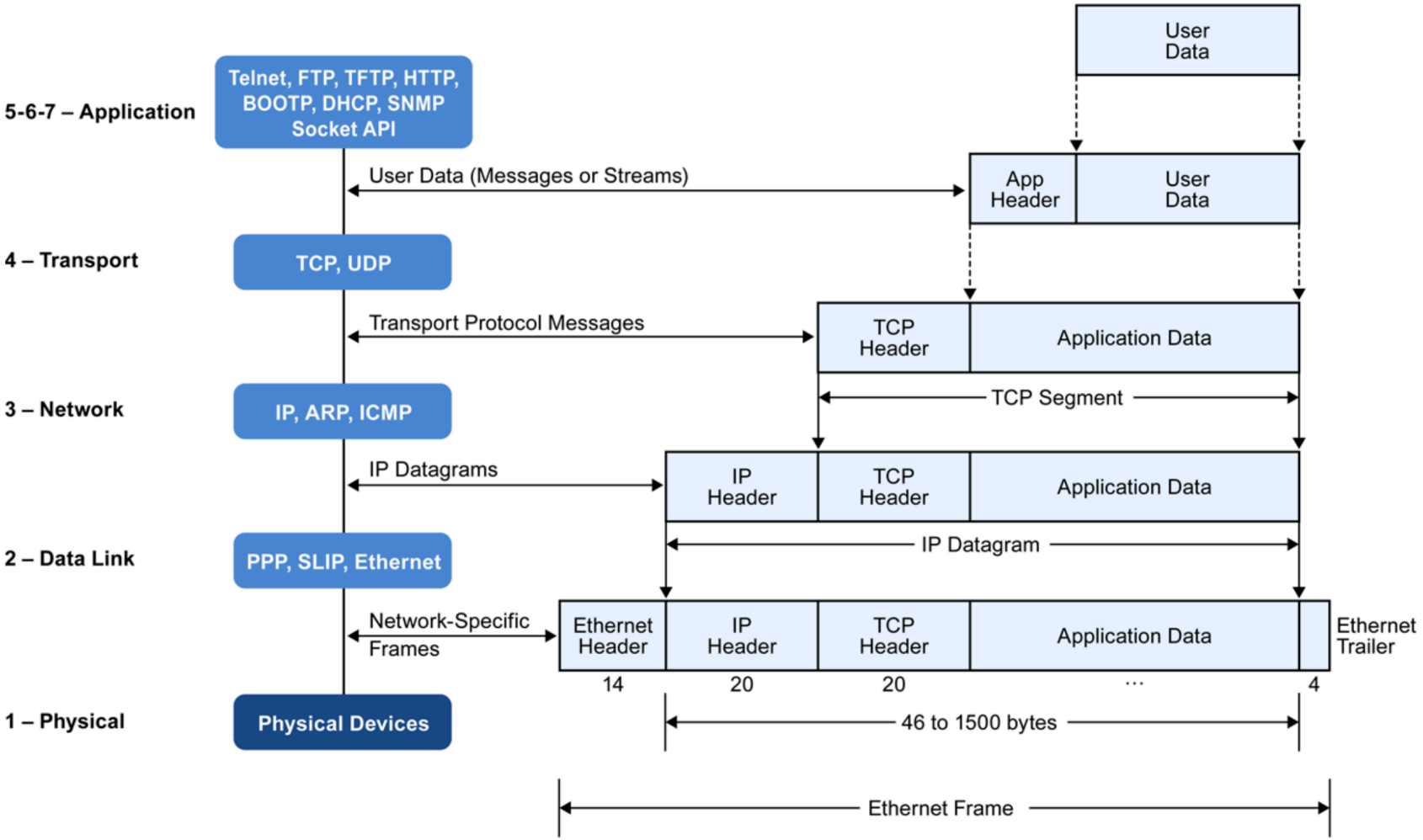
- The Internet layer is responsible for sending packets to across networks.
- It has two functions: 1) Host identification by using IP addressing system (IPv4 and IPv6); and 2) packets routing from source to destination.
- The examples of Internet layer protocols are Internet Protocol (IP), Internet Control Message Protocol (ICMP), and Address Resolution Protocol (ARP).

Link Layer

- The link layer defines the networking methods within the scope of the local network link.

- It is used to move the packets between two hosts on the same link. An common example of link layer protocols is Ethernet.

Data Encapsulation in Network Stack



Lab 0

- Make sure you can login as CSC 5290 student on Zero Client
  - Using your WSU access ID and password
  - Providing VM images for lab experiments

Lab 0 (cont'd)

- Subscribe course mailing-list
  - csc5290@lists.wayne.edu
  - List Home page (web interface for subscribers to join/ leave list, post messages, view archives): http://lists.wayne.edu
- Send an email to the list to introduce yourself by next class
- Send a zipped test.txt file on Backboard by this week