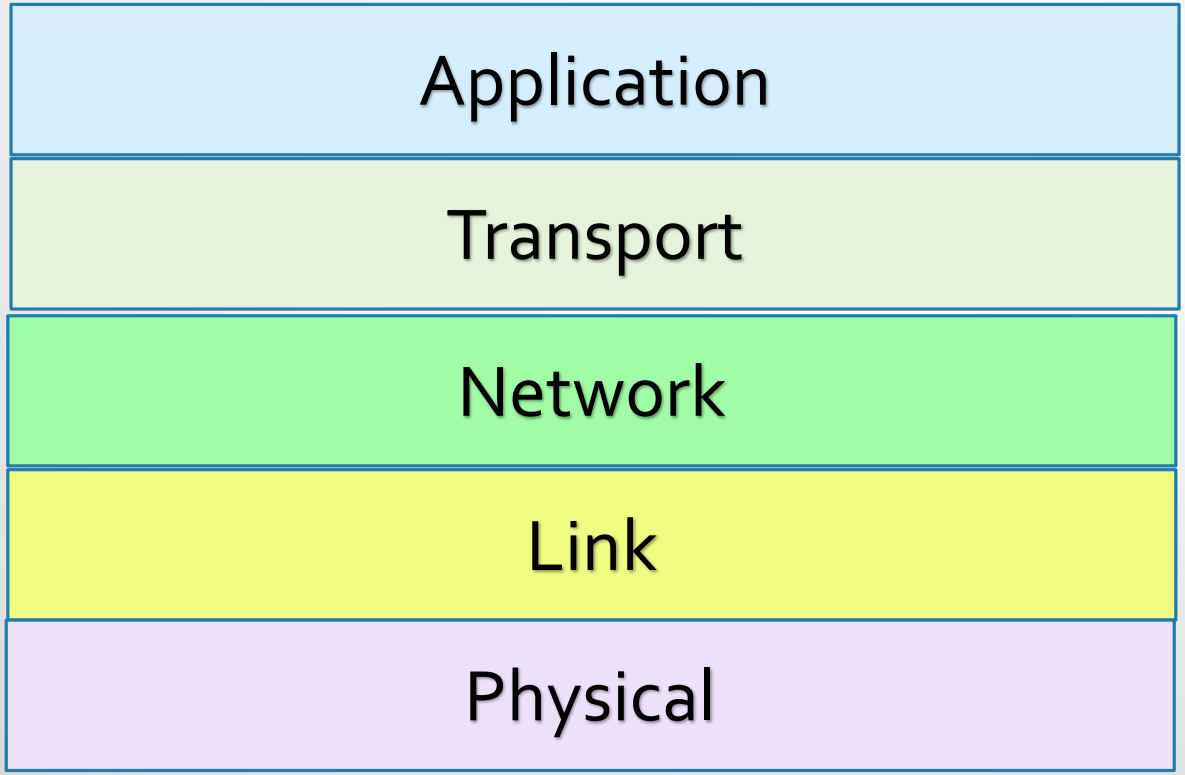
# Intrusion & Anomaly Detection

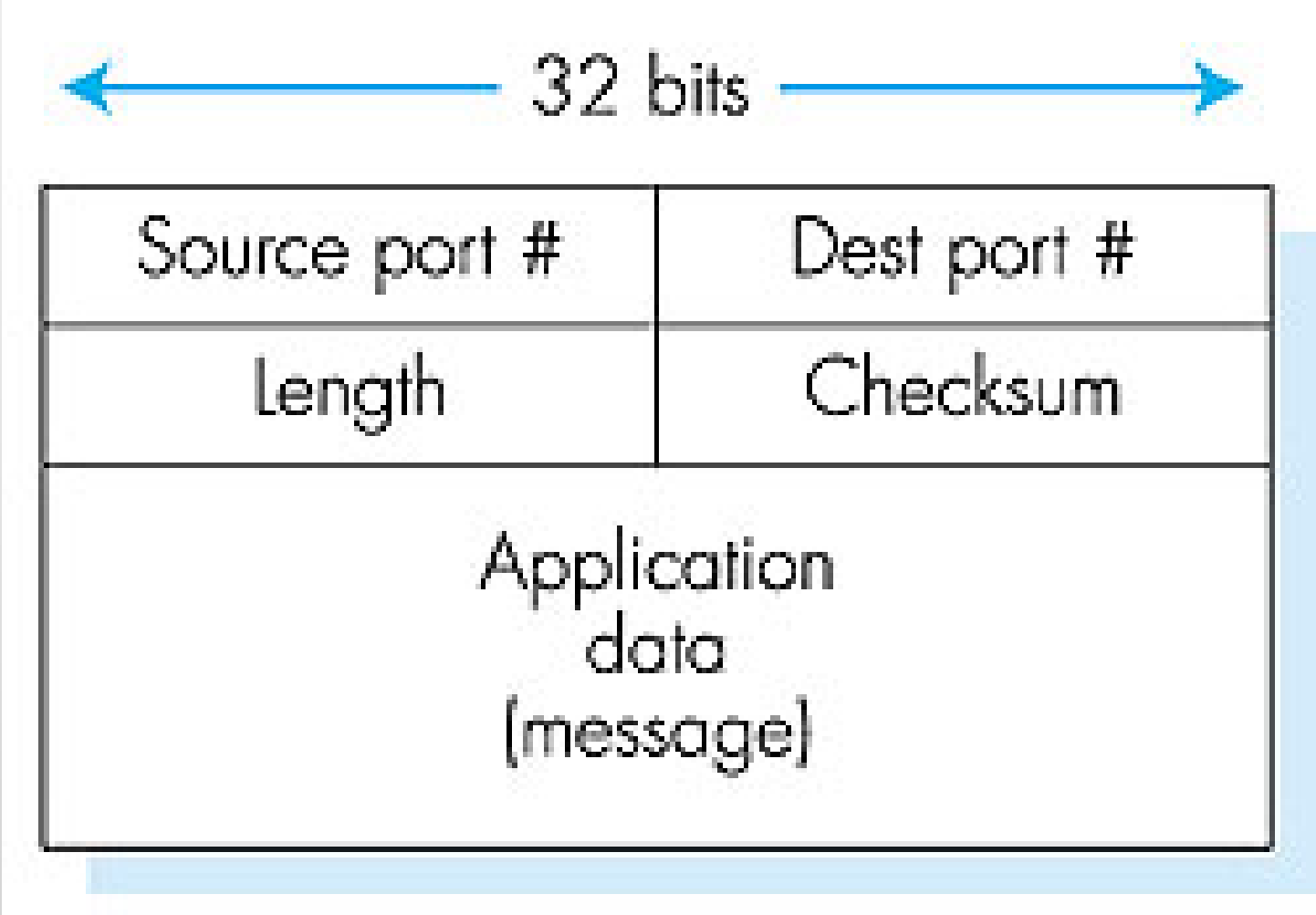
## Network Protocols

Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University

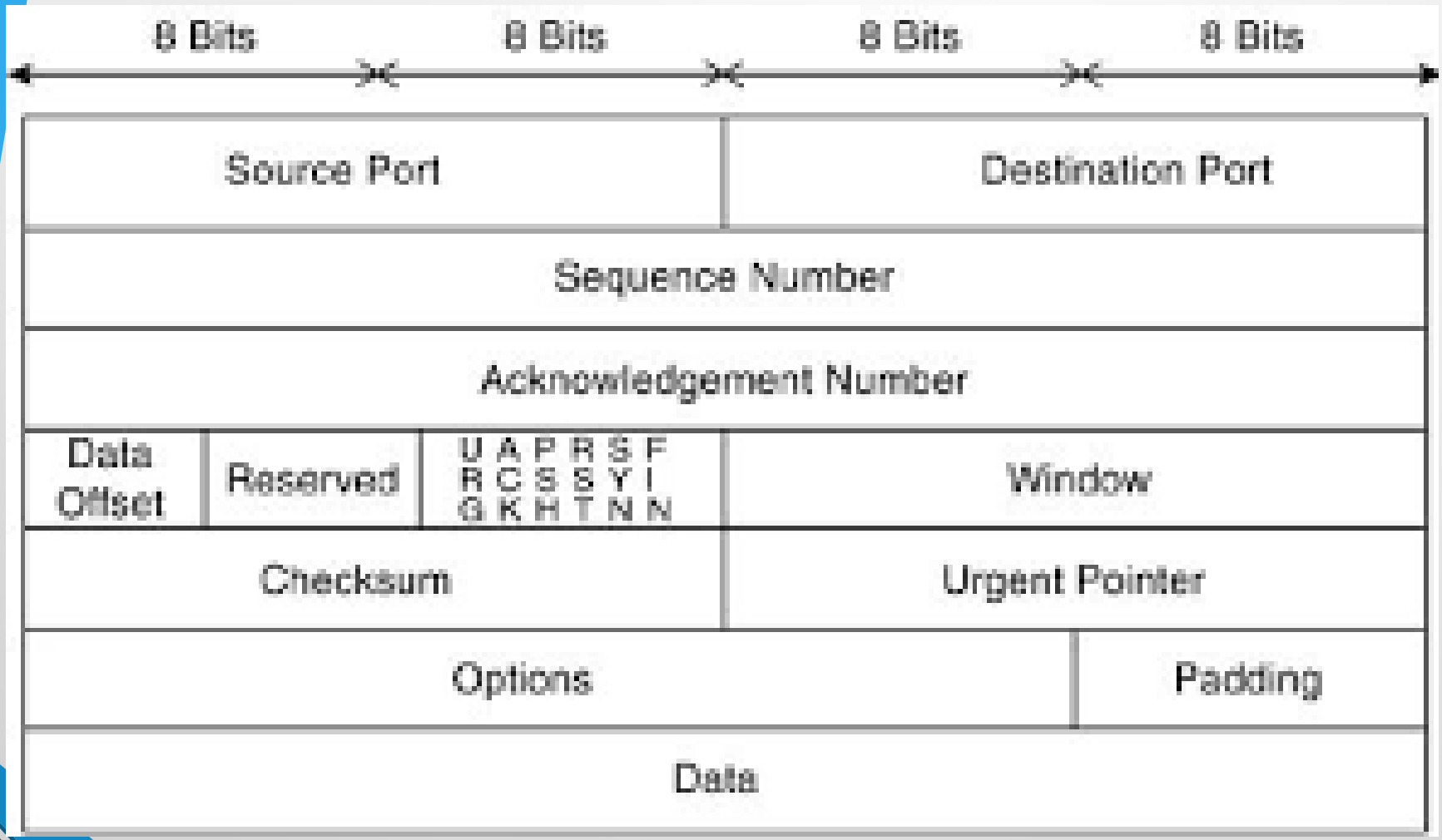
# Internet Architecture Stack



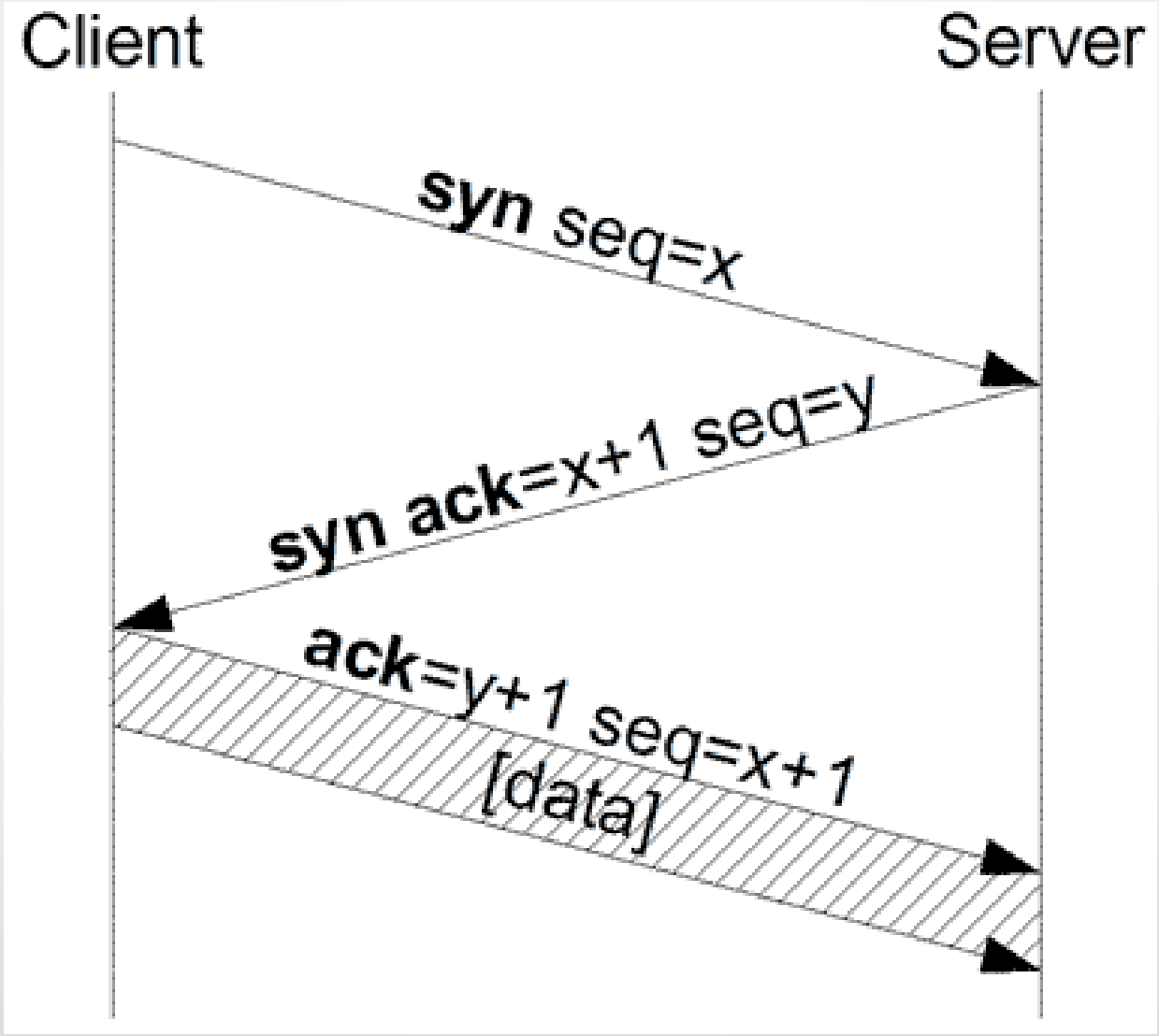
# UDP Segment


32 bits
Source port #
Dest port #
Length
Checksum
Application
data
(message)

# TCP Segment Structure



# TCP Three-Way Handshake



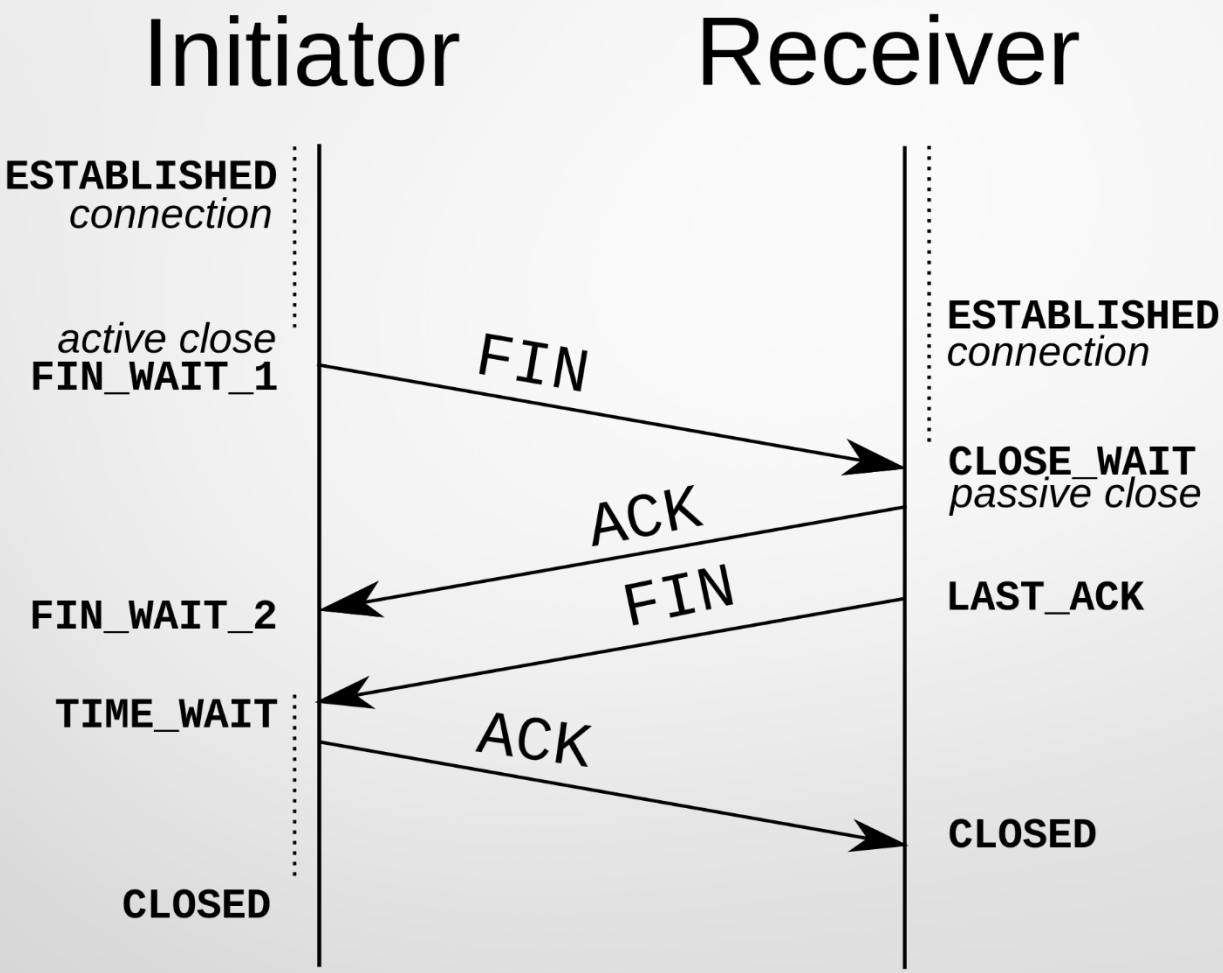
# Sequence Numbers

- Sequence Numbers
  - First byte numbered 0
  - File size 500,000 bytes
  - MSS 1,000 (500 segments)
  - Sequence #1=0, Sequence #2=1000, Sequence #3=2000, etc.
- Maximum Segment Size (MSS)
  - Application-layer data only
- Maximum Transfer Unit (MTU)
  - Application-layer data + transport-layer header + network-layer header

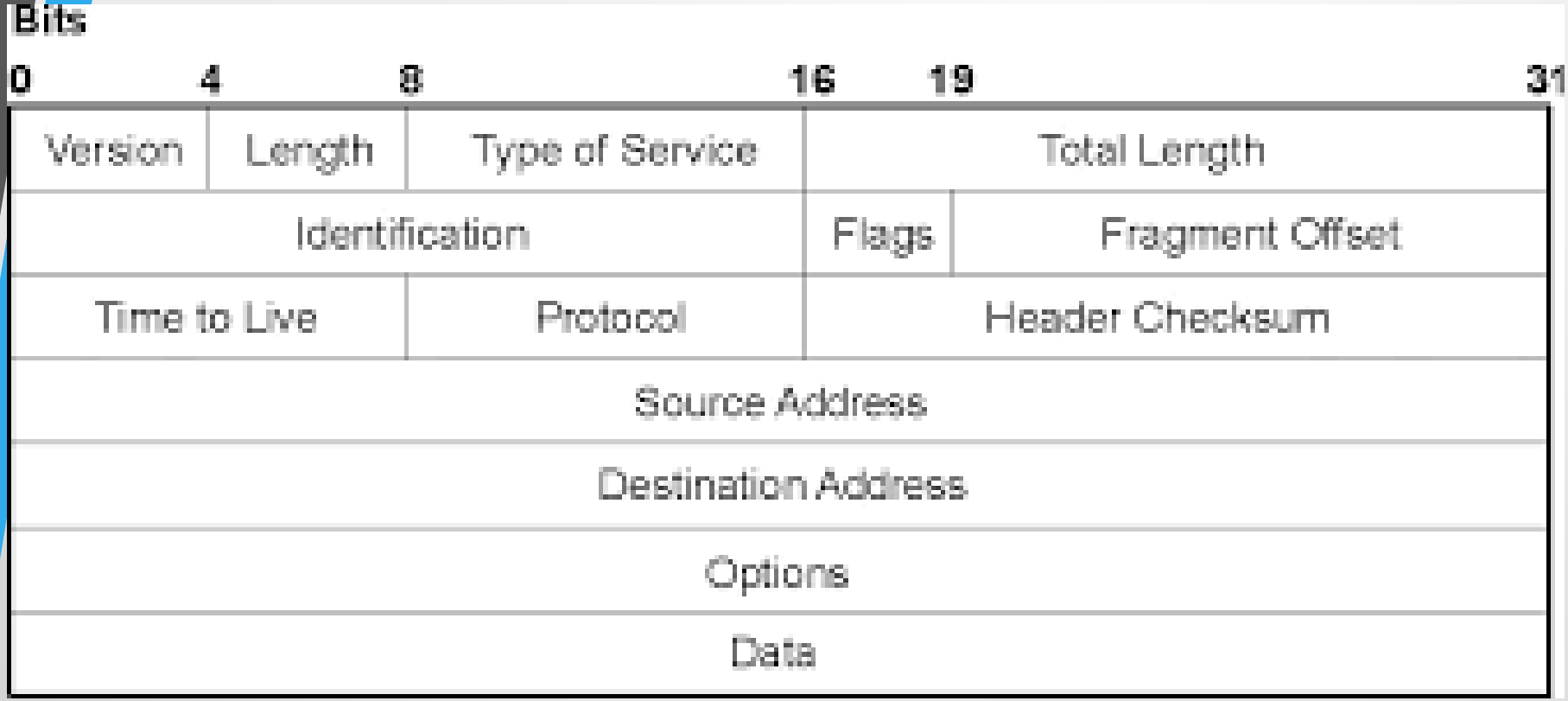
# Acknowledgement Numbers

- Sequence number of next segment expected
  - Received bytes 0 through 535
  - Waiting for byte 536
  - Puts 536 in acknowledgement number field of segment
- Buffer out-of-order segments

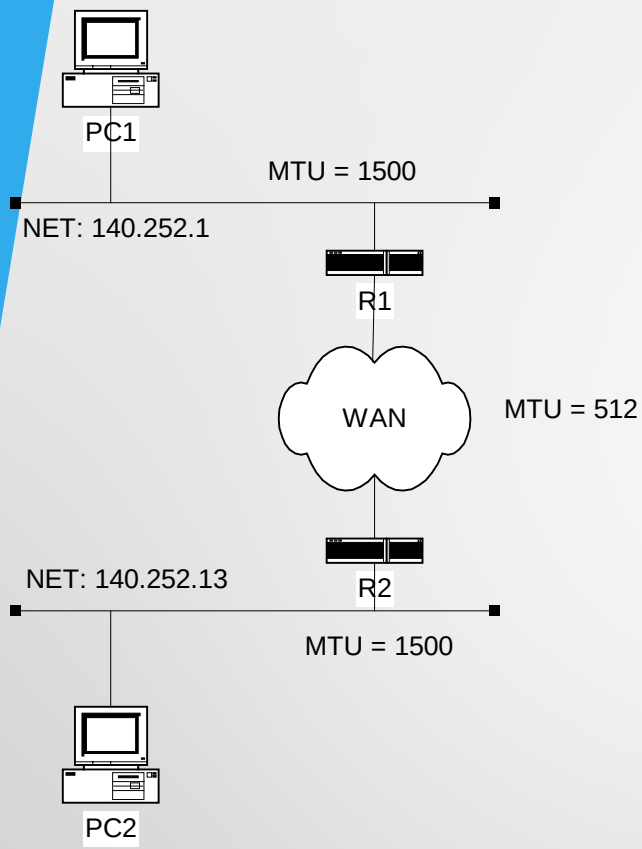
# TCP Modified Three-way Handshake

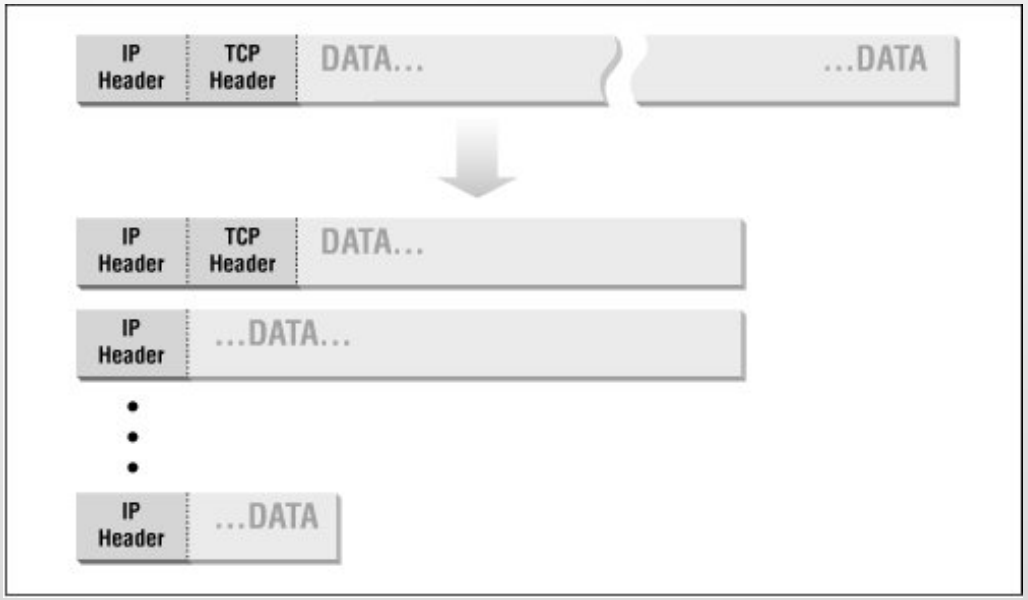


# Internet Protocol (IP)

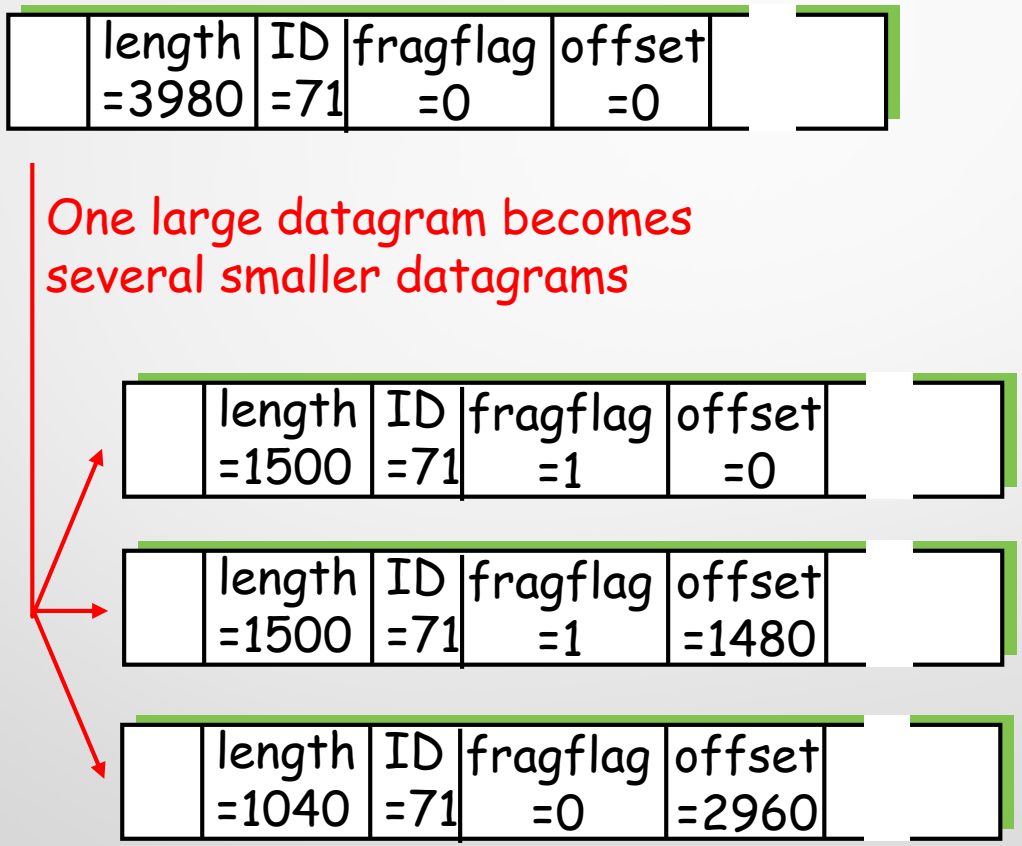


# IP Fragmentation



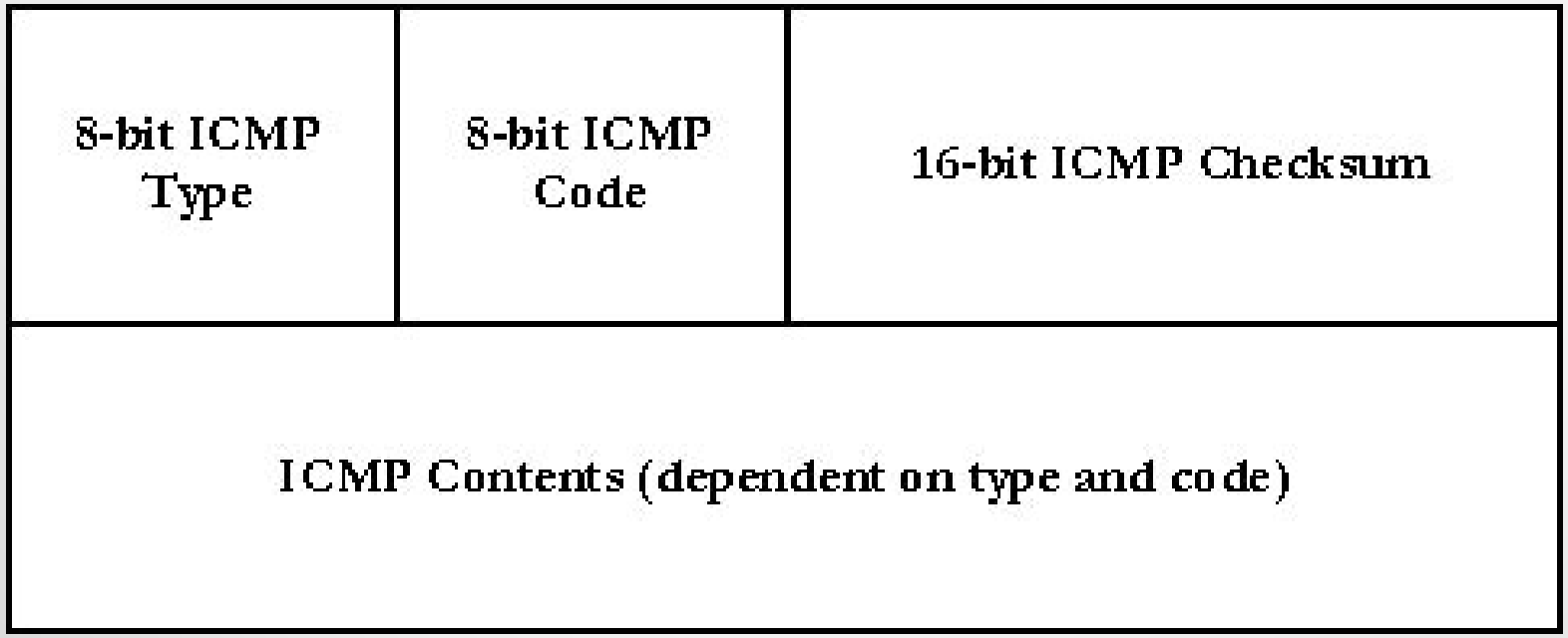
# Fragmentation & Reassembly



# ICMP

- Internet Control Message Protocol
- Error reporting
  - Reported back to source – why?
- Ping
  - Echo Request and Echo Reply messages
- Traceroute

# ICMP Message Format




- If reporting errors:
  - Header of datagram causing error
  - First 64 data bits of datagram causing error

# ICMP Type Field – common ones

| Type field | ICMP Message Type |
|---|---|
| 0 | Echo reply (ping response) |
| 3 | Destination unreachable |
| 4 | Source quench |
| 8 | Echo request (ping) |
| 9 | Router advertisement |
| 10 | Router solicitation |
| 11 | TTL = 0 |

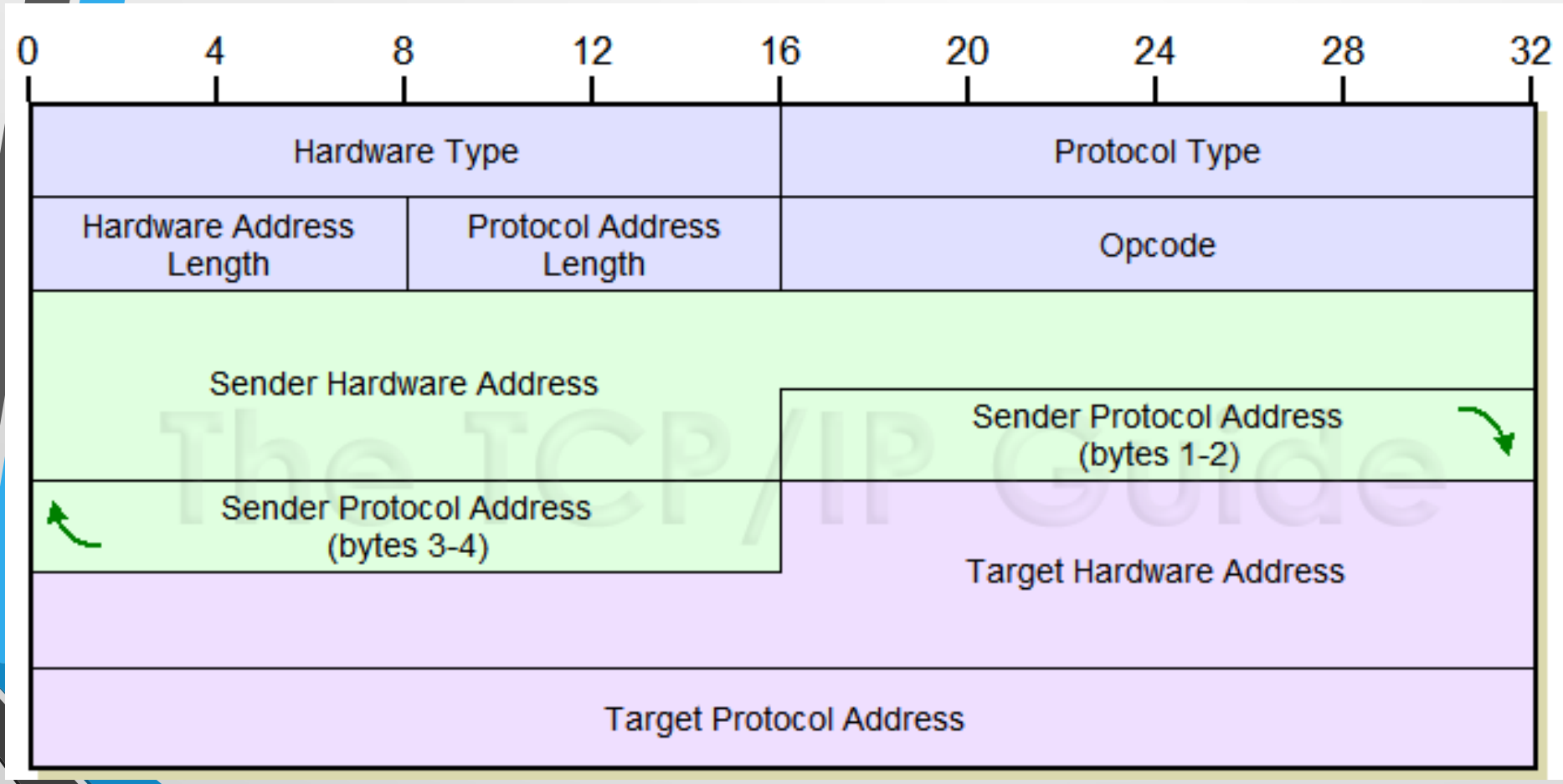
# ARP

- Address Resolution Protocol
- Network-layer addresses to link-layer addresses
- Same LAN only
- ARP broadcast
  - ARP reply
- Since use a broadcast to find MAC address, why not just broadcast the IP datagram?

# ARP Functions

- Map IP address to physical address when sending a packet → straighforward
- Answer ARP requests from other hosts → more complex
  - Ethernet – best-effort delivery

# ARP Message Format



# ARP Message over Ethernet