

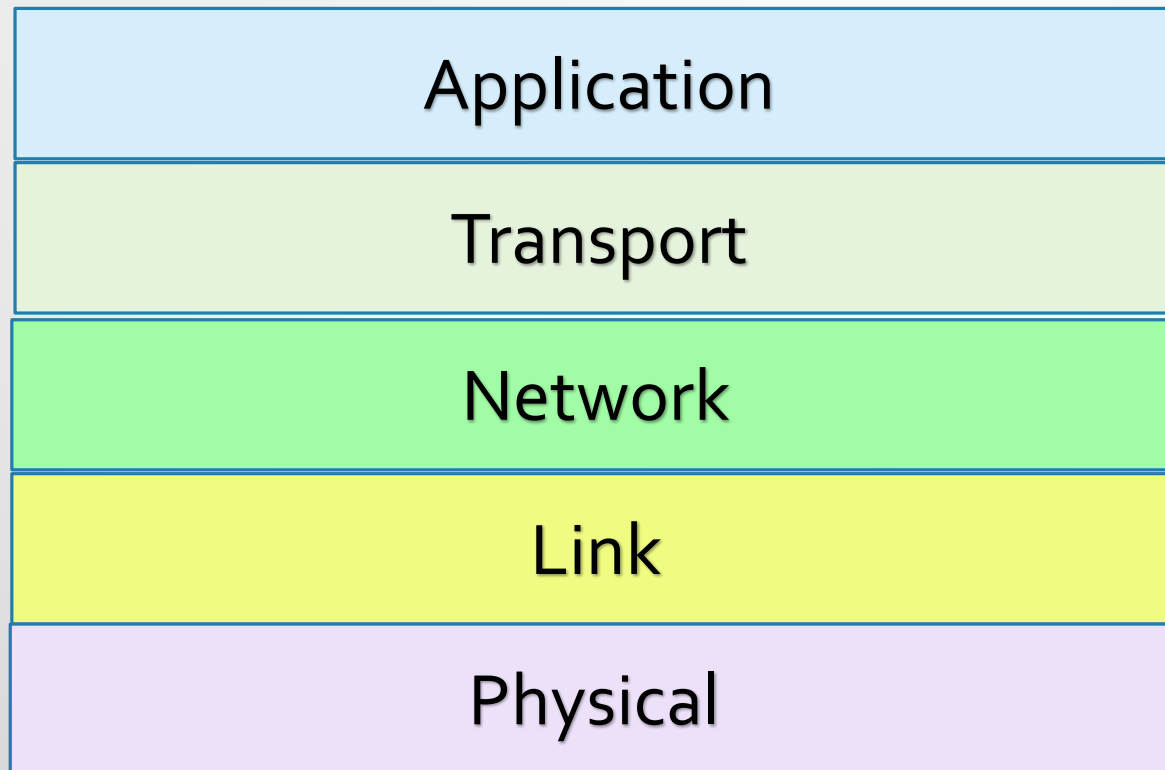


Intrusion & Anomaly Detection

Network Protocols

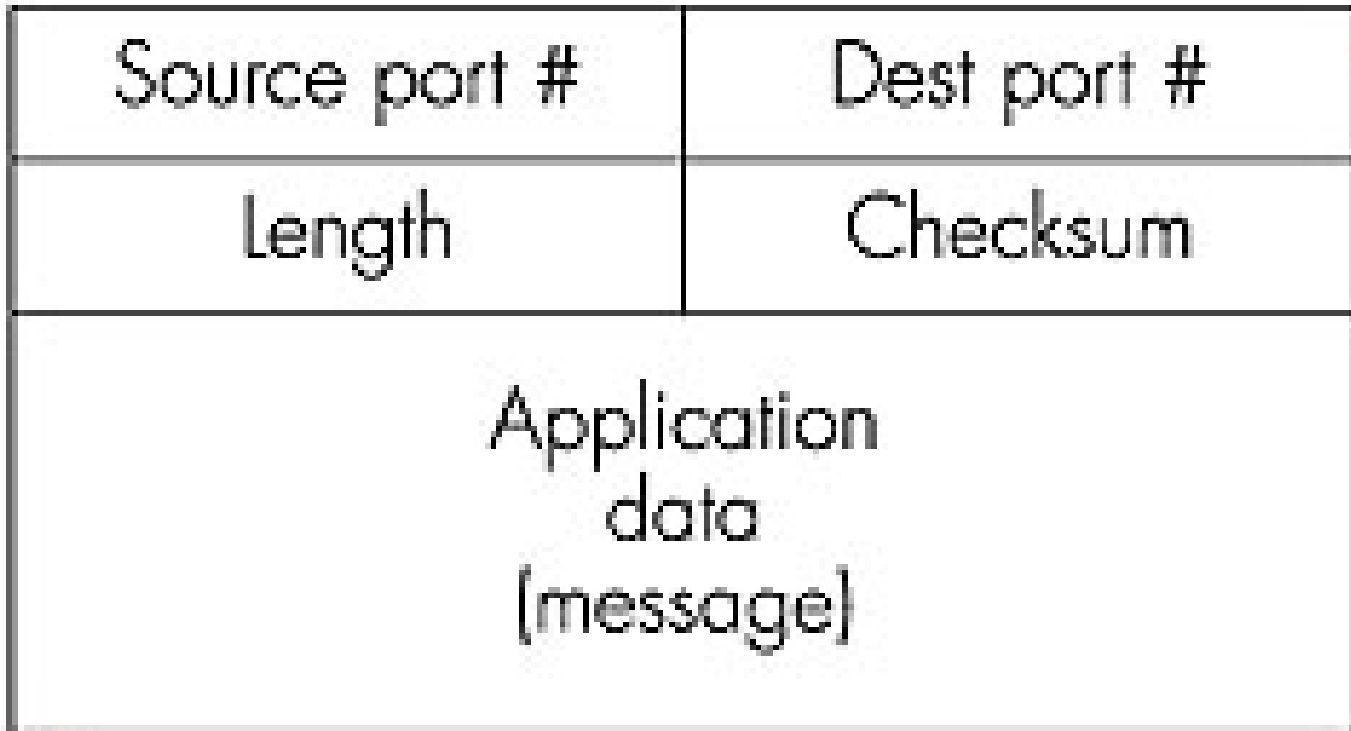
Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University

Internet Architecture Stack

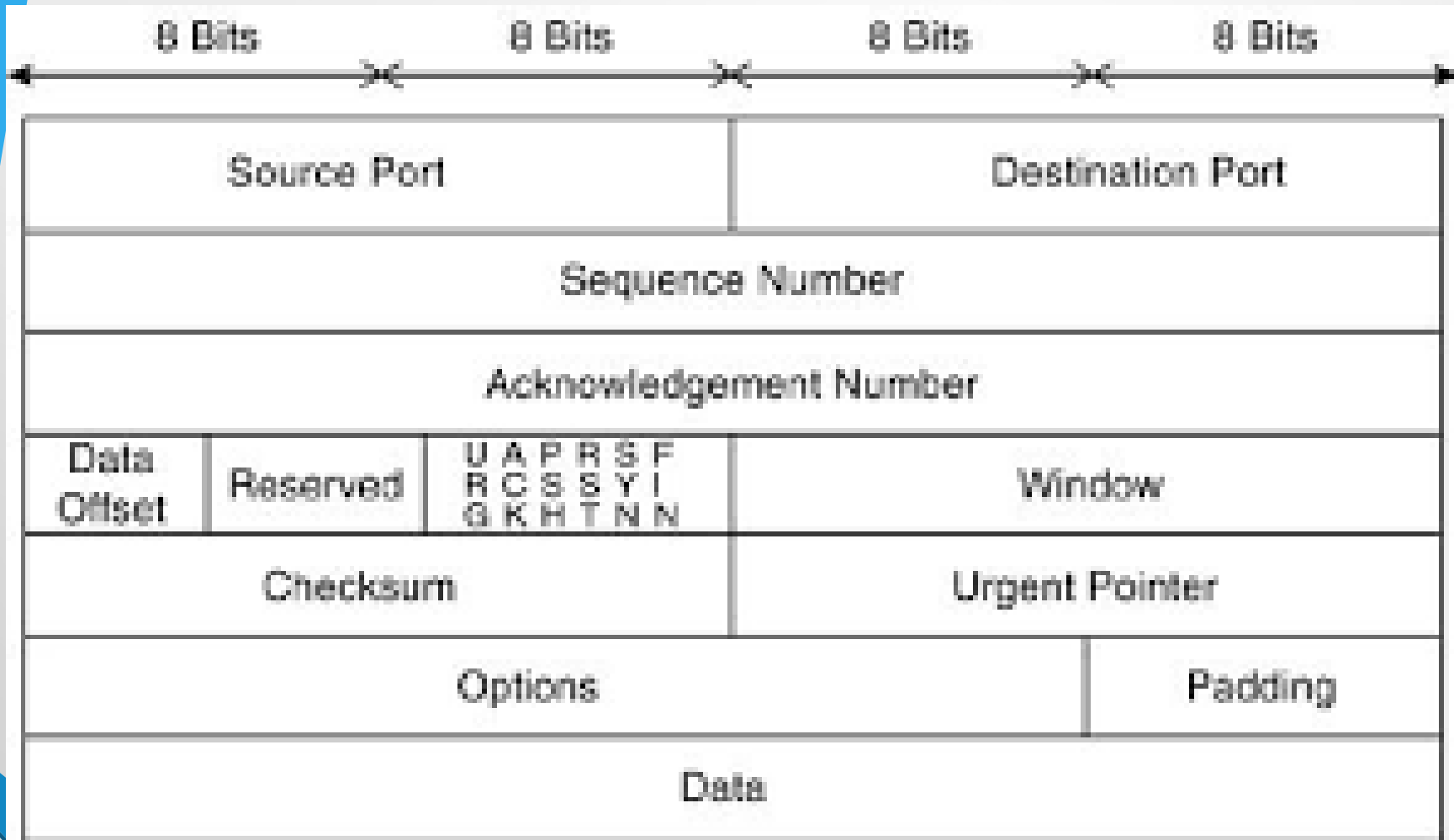


UDP Segment

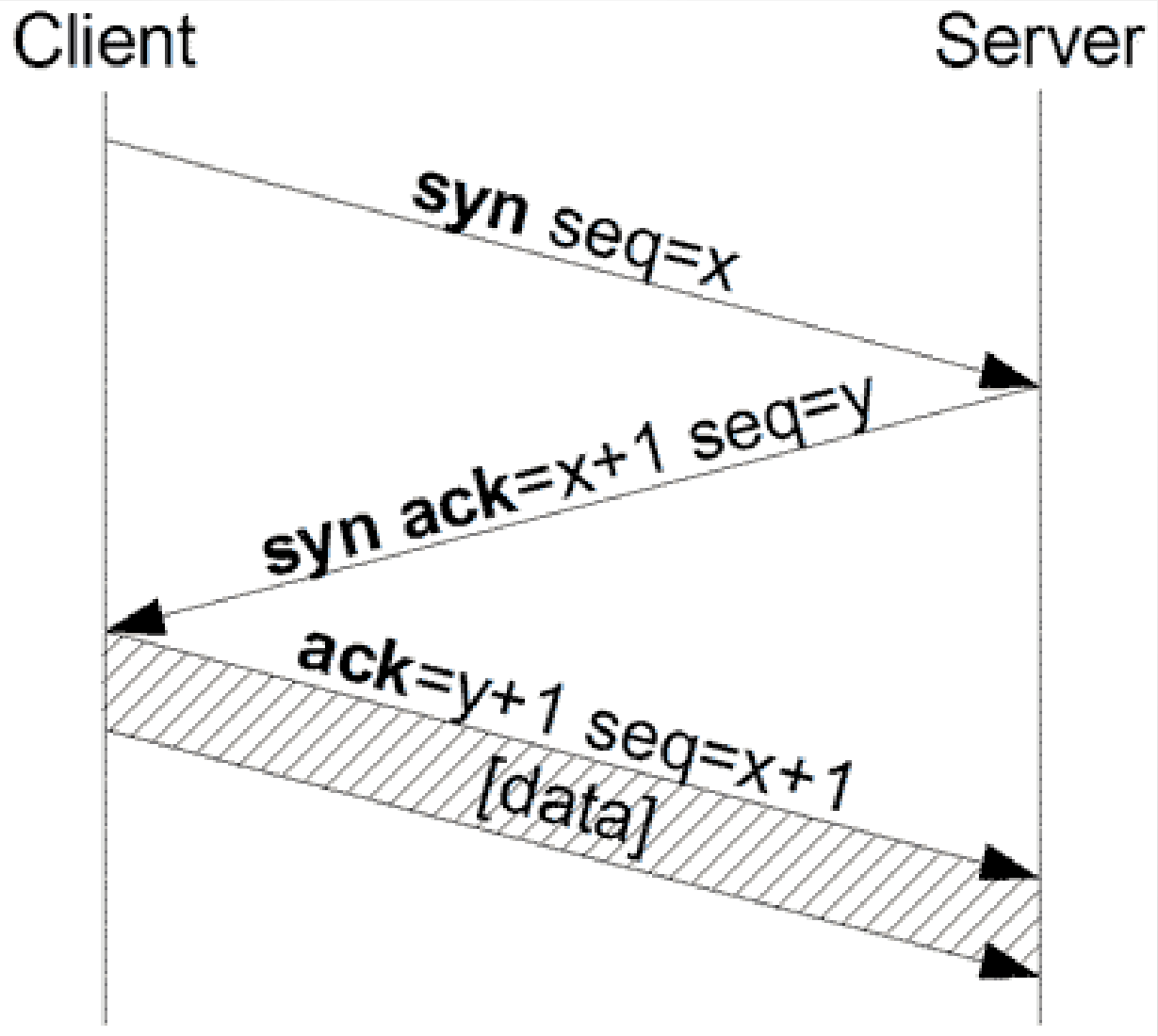
← 32 bits →



TCP Segment Structure



TCP Three-Way Handshake



Sequence Numbers

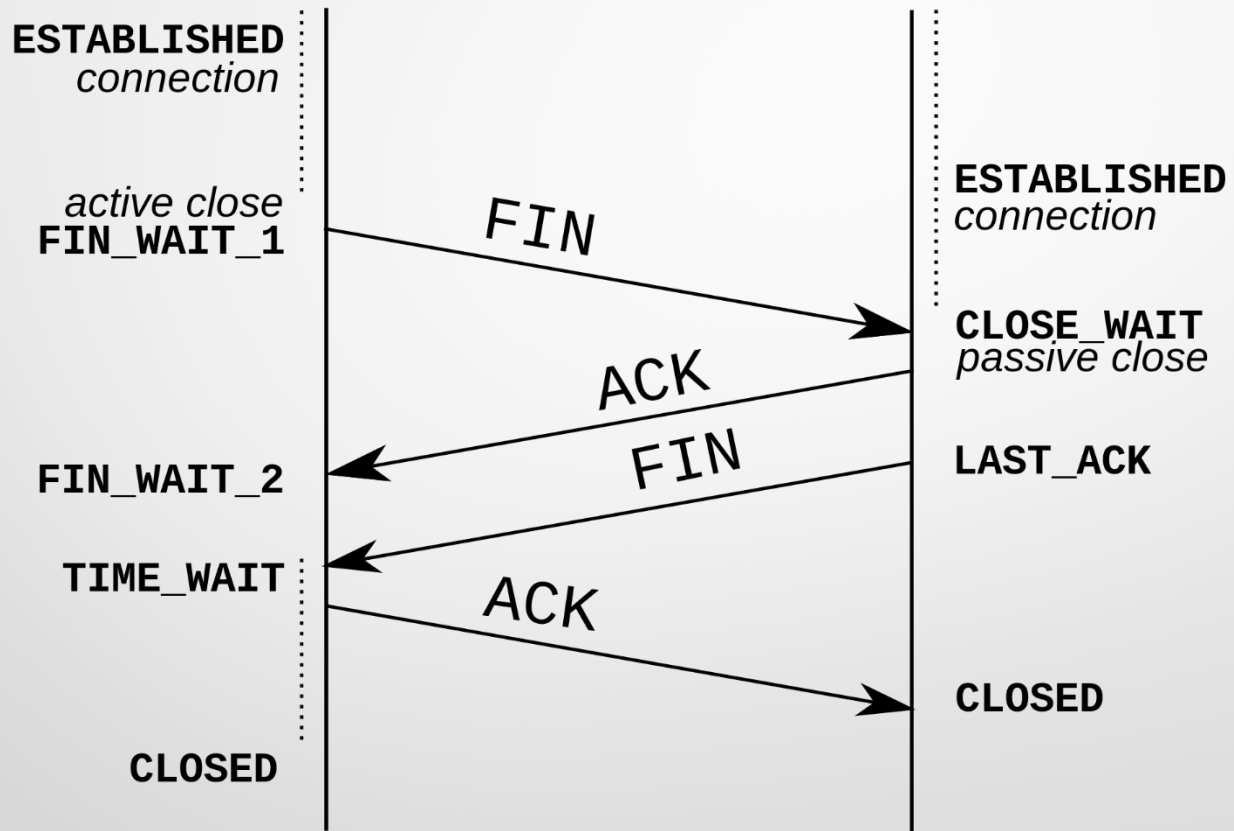
- Sequence Numbers
 - First byte numbered 0
 - File size 500,000 bytes
 - MSS 1,000 (500 segments)
 - Sequence #1=0, Sequence #2=1000, Sequence #3=2000, etc.
- Maximum Segment Size (MSS)
 - Application-layer data only
- Maximum Transfer Unit (MTU)
 - Application-layer data + transport-layer header +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

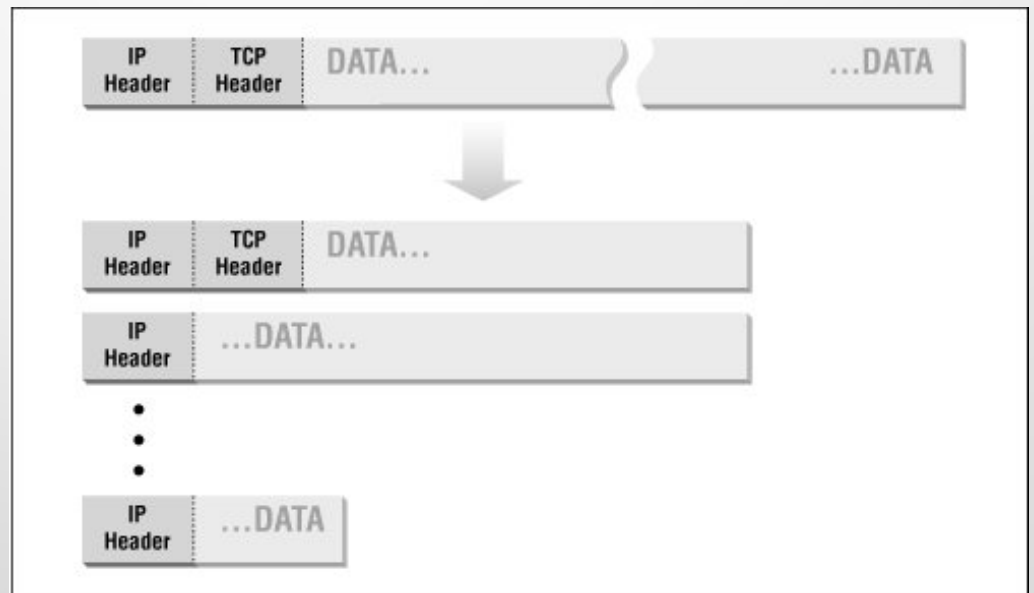
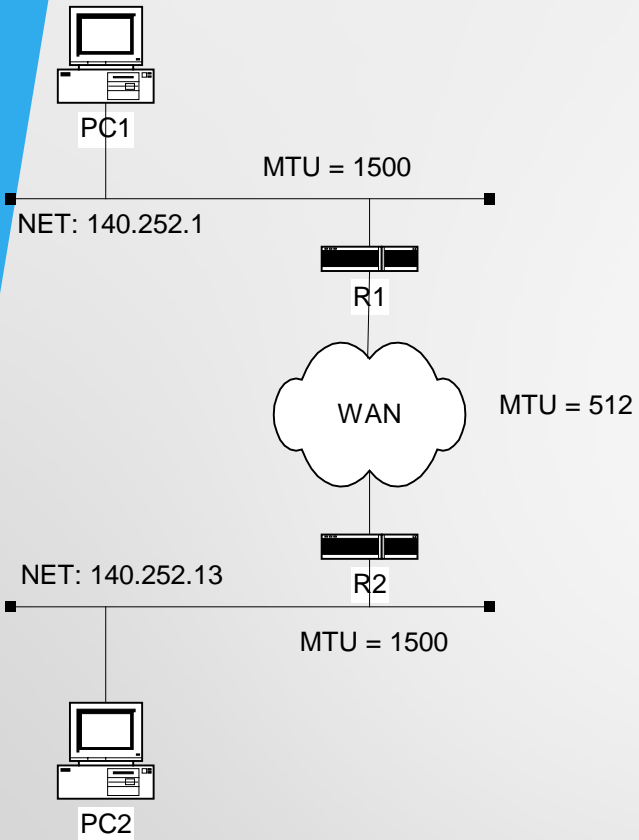
Initiator Receiver



Internet Protocol (IP)

Bits					
0	4	8	16	19	31
Version	Length	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol		Header Checksum	
Source Address					
Destination Address					
Options					
Data					

IP Fragmentation



Fragmentation & Reassembly

length	ID	fragflag	offset
=3980	=71	=0	=0

One large datagram becomes
several smaller datagrams

length	ID	fragflag	offset
=1500	=71	=1	=0

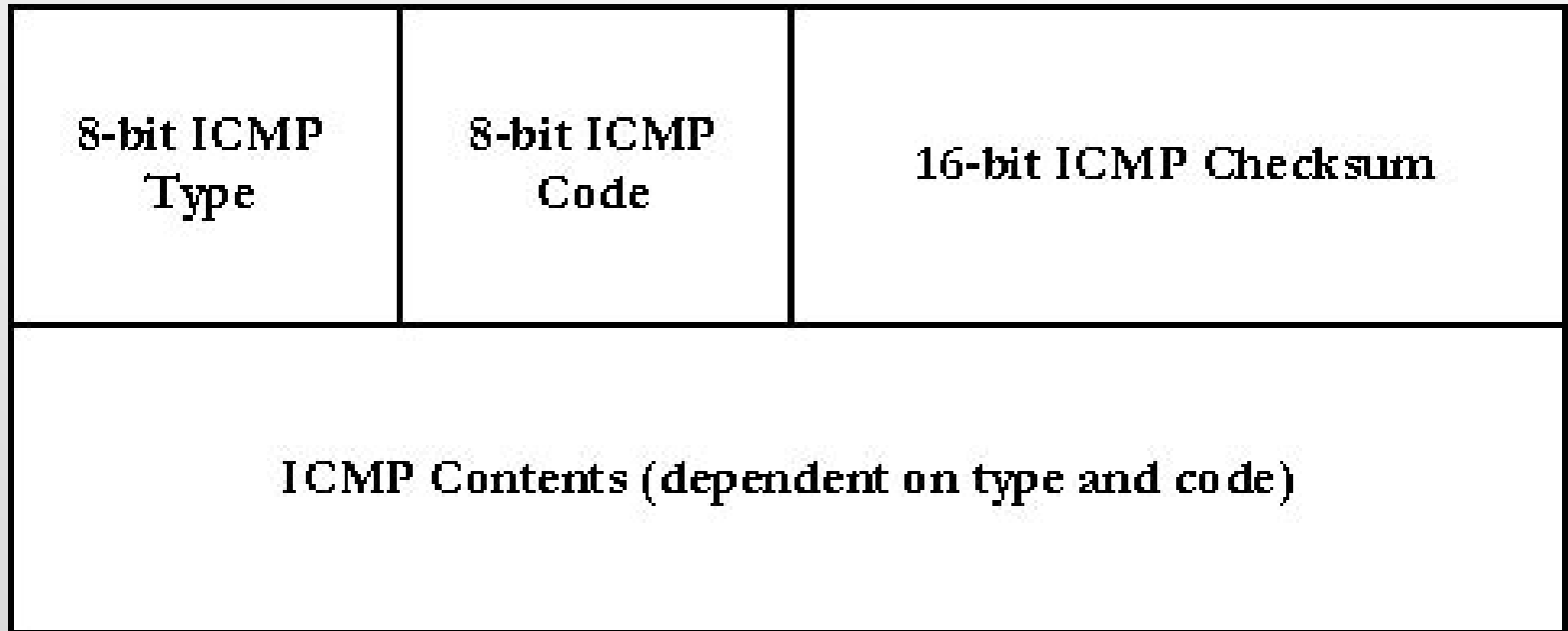
length	ID	fragflag	offset
=1500	=71	=1	=1480

length	ID	fragflag	offset
=1040	=71	=0	=2960

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

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

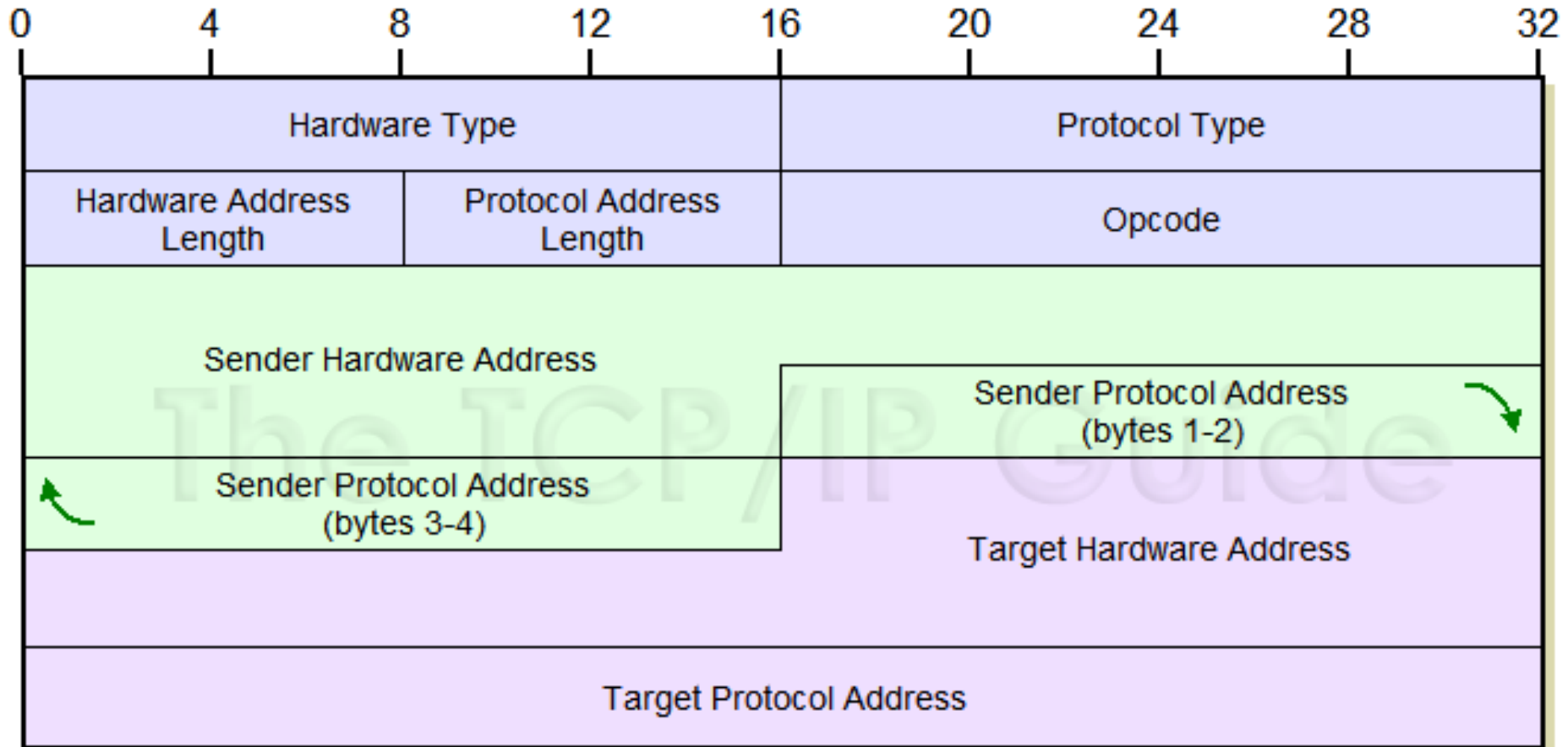
ARP

- 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 → straightforward
- Answer ARP requests from other hosts → more complex
 - Ethernet – best-effort delivery

ARP Message Format



ARP Message over Ethernet

0	8	16	31
ETHERNET ADDRESS TYPE (1)		IP ADDRESS TYPE (0800)	
ETH ADDR LEN (6)	IP ADDR LEN (4)	OPERATION	
SENDER'S ETH ADDR (first 4 octets)			
SENDER'S ETH ADDR (last 2 octets)		SENDER'S IP ADDR (first 2 octets)	
SENDER'S IP ADDR (last 2 octets)		TARGET'S ETH ADDR (first 2 octets)	
TARGET'S ETH ADDR (last 4 octets)			
TARGET'S IP ADDR (all 4 octets)			