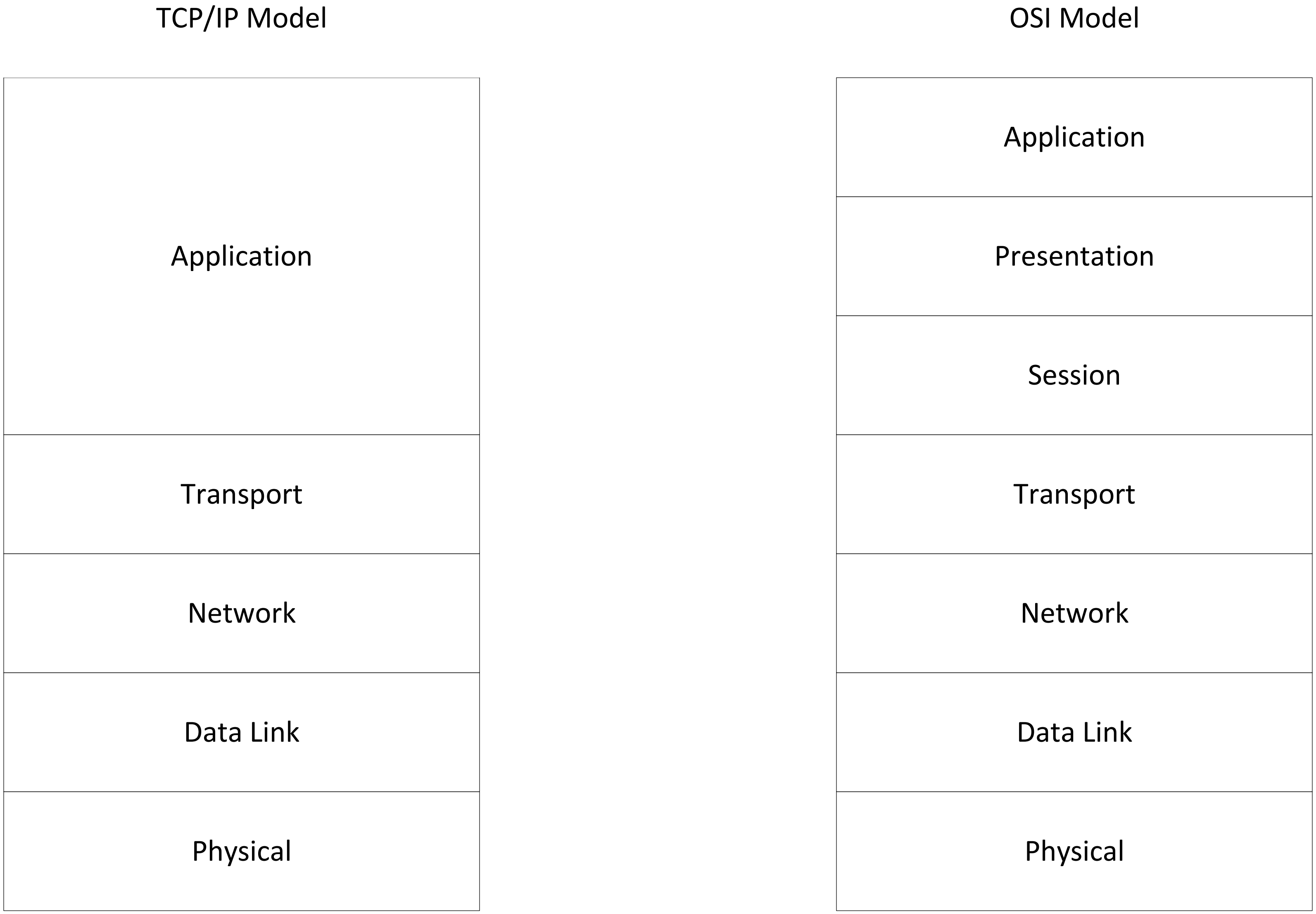
“Trying to get a job in [cyber]security without a deep understanding of how data packets work is a bit like trying to become a chemical engineer without first mastering the periodic table of elements.”

Brian Krebs

Thinking of a Cybersecurity Career? Read This

TCP/IP Model	Sample Protocols	Addressing
Application	HTTP, HTTPS, DNS, DHCP, SMTP, SNMP, ...	
Transport	TCP, UDP	
Network	IP, ICMP	IP
Data Link	ARP Ethernet, 802.11	MAC
Physical		

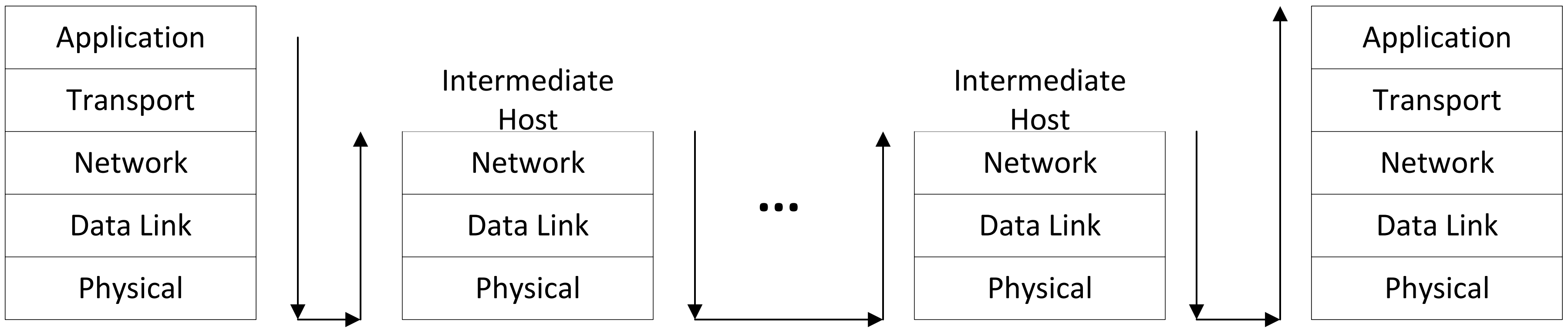


TCP/IP Model	OSI Model
Application	Application
	Presentation
	Session
Transport	Transport
Network	Network
Data Link	Data Link
Physical	Physical

How Messages Flow Across the Internet

202.56.66.33, tcp, 80

155.66.98.66, tcp, 57844



Application
Transport
Network
Data Link
Physical

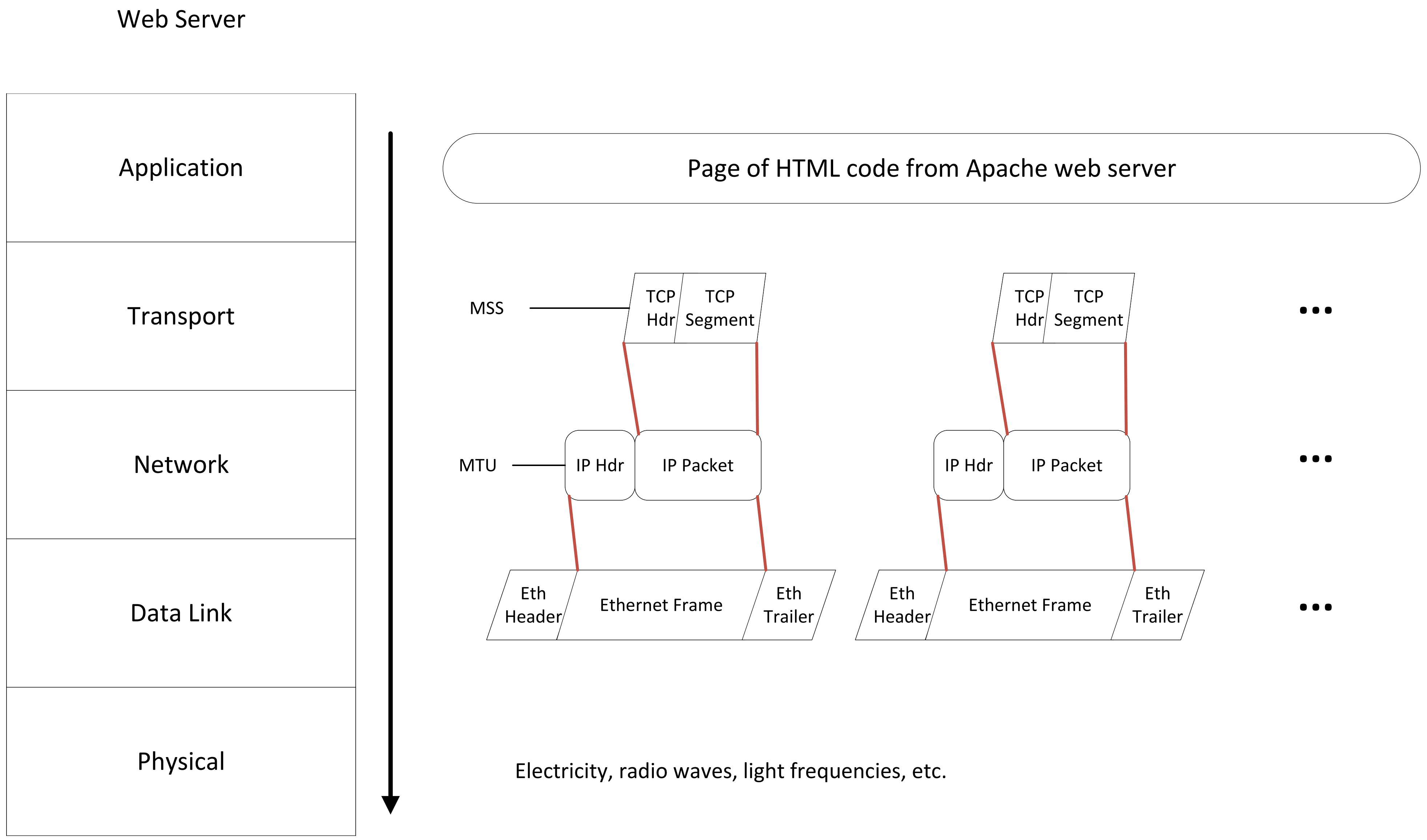
Intermediate Host
Network
Data Link
Physical

...

Intermediate Host
Network
Data Link
Physical

Application
Transport
Network
Data Link
Physical

Sending a web page



Web Server

Application

Transport

Network

Data Link

Physical

Page of HTML code from Apache web server

MSS

TCP Hdr

TCP Segment

TCP Hdr

TCP Segment

•••

MTU

IP Hdr

IP Packet

IP Hdr

IP Packet

•••

Eth Header

Ethernet Frame

Eth Trailer

Eth Header

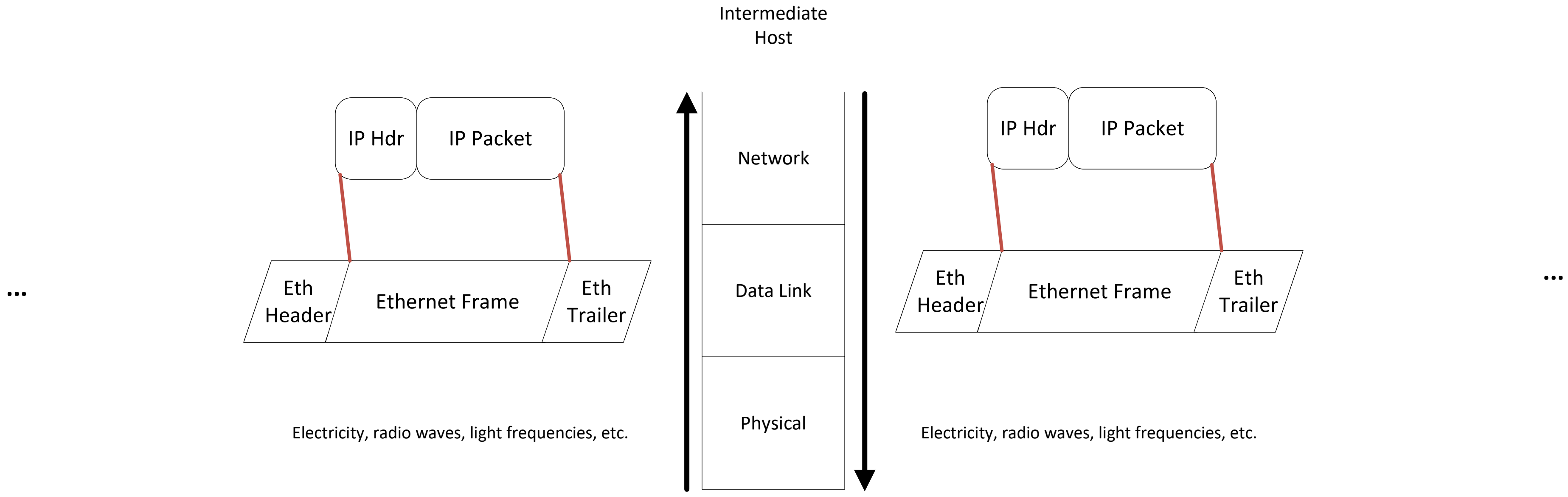
Ethernet Frame

Eth Trailer

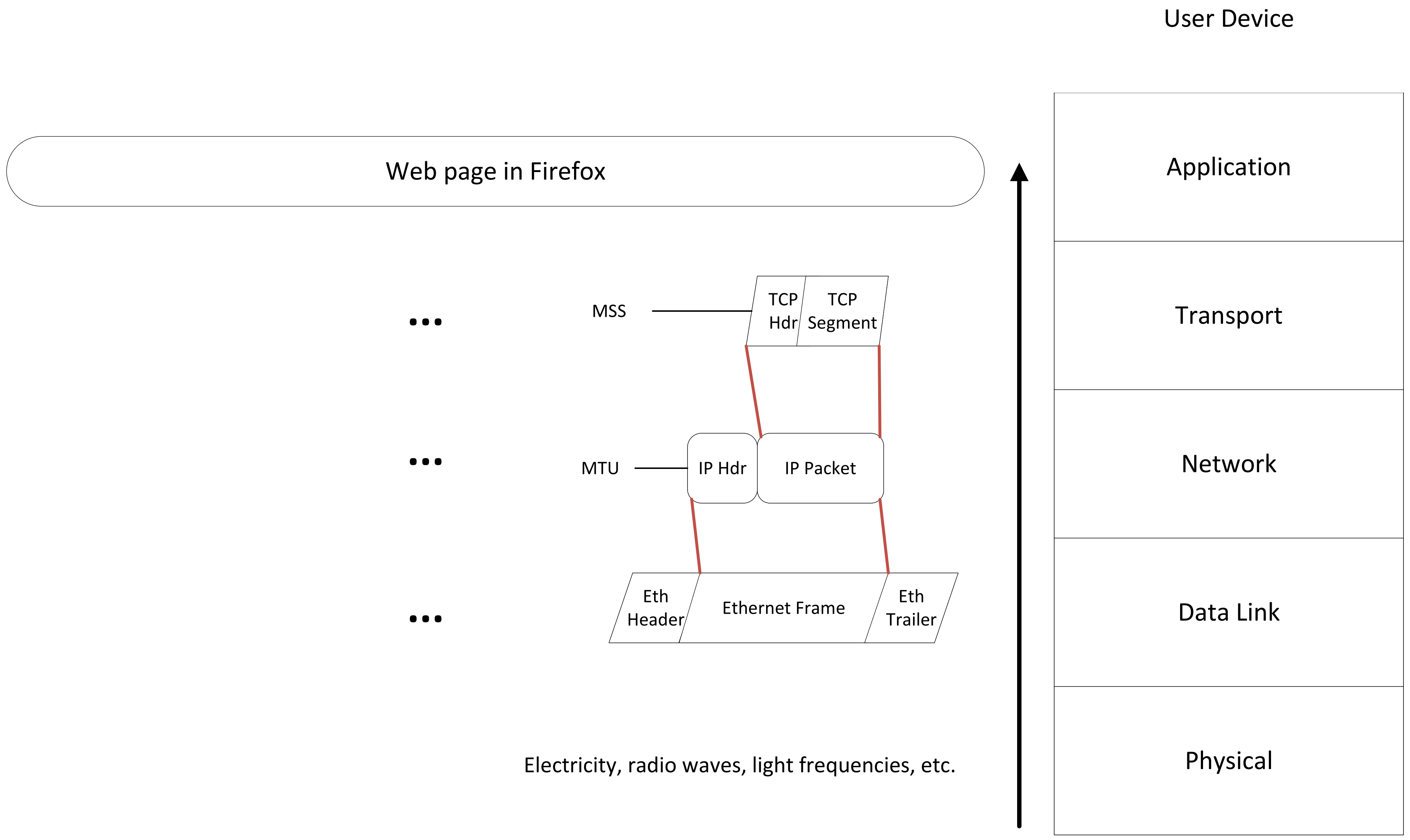
•••

Electricity, radio waves, light frequencies, etc.

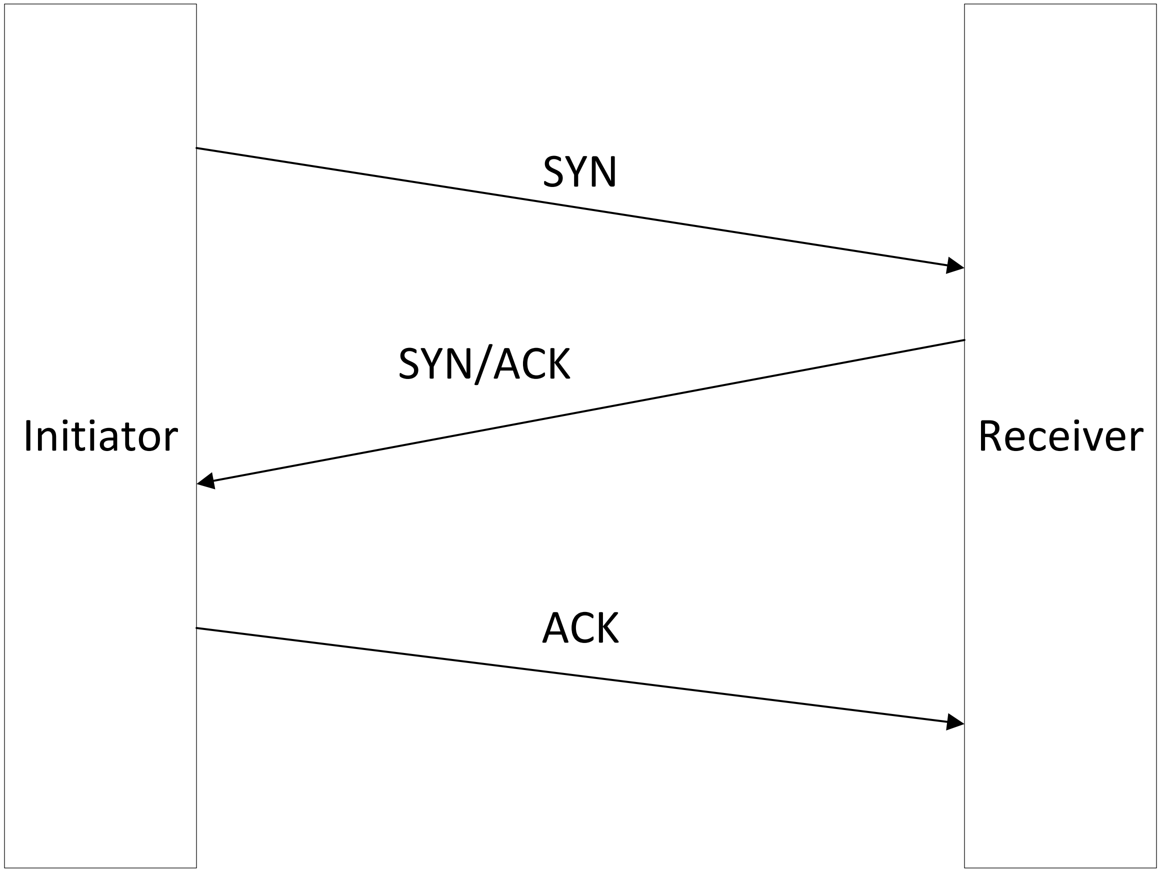
Intermediate routing



Receiving a web page



TCP 3-Way Handshake
To Establish Connection



Initiator

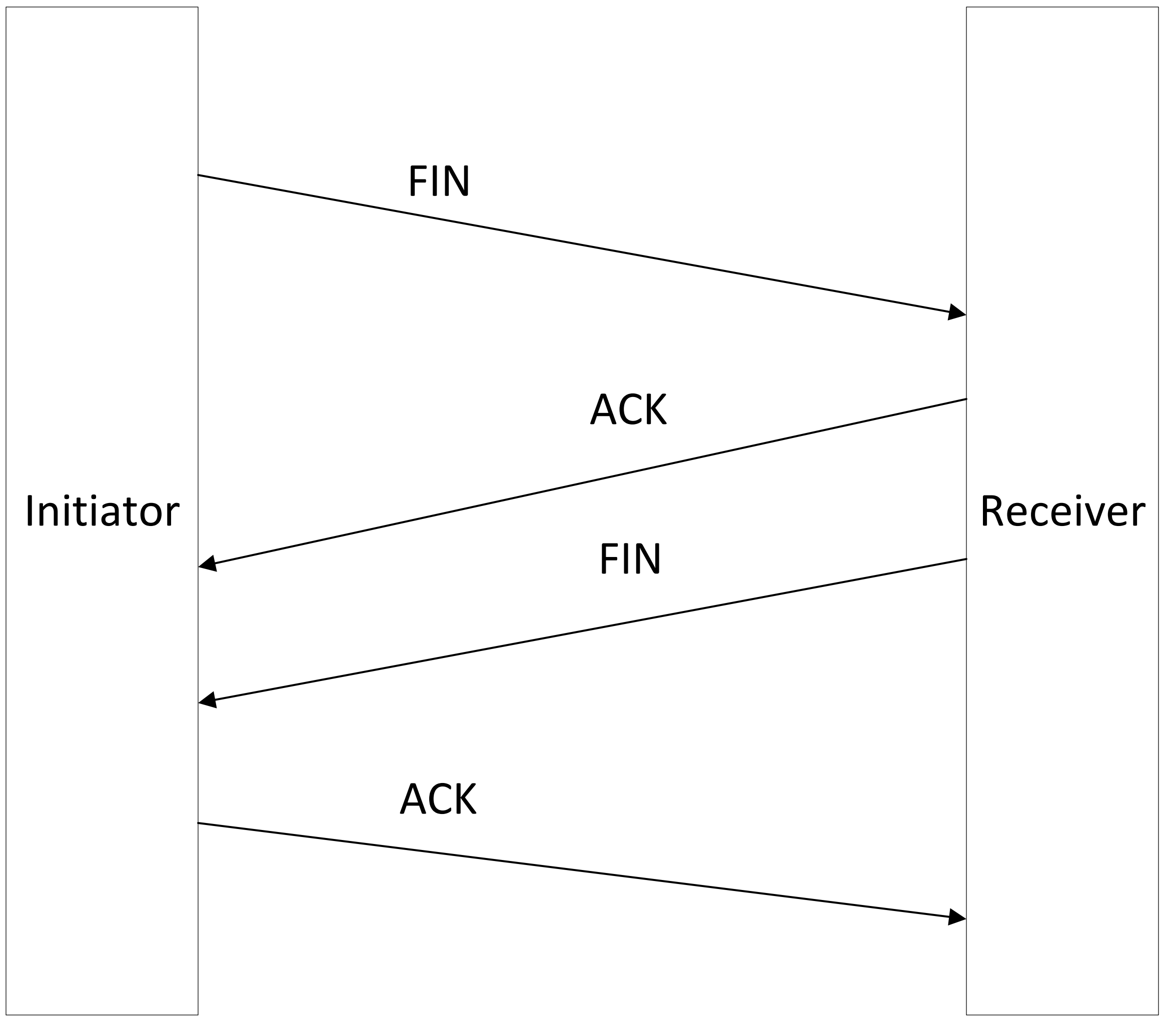
Receiver

SYN

SYN/ACK

ACK

TCP 3-Way Handshake



FIN

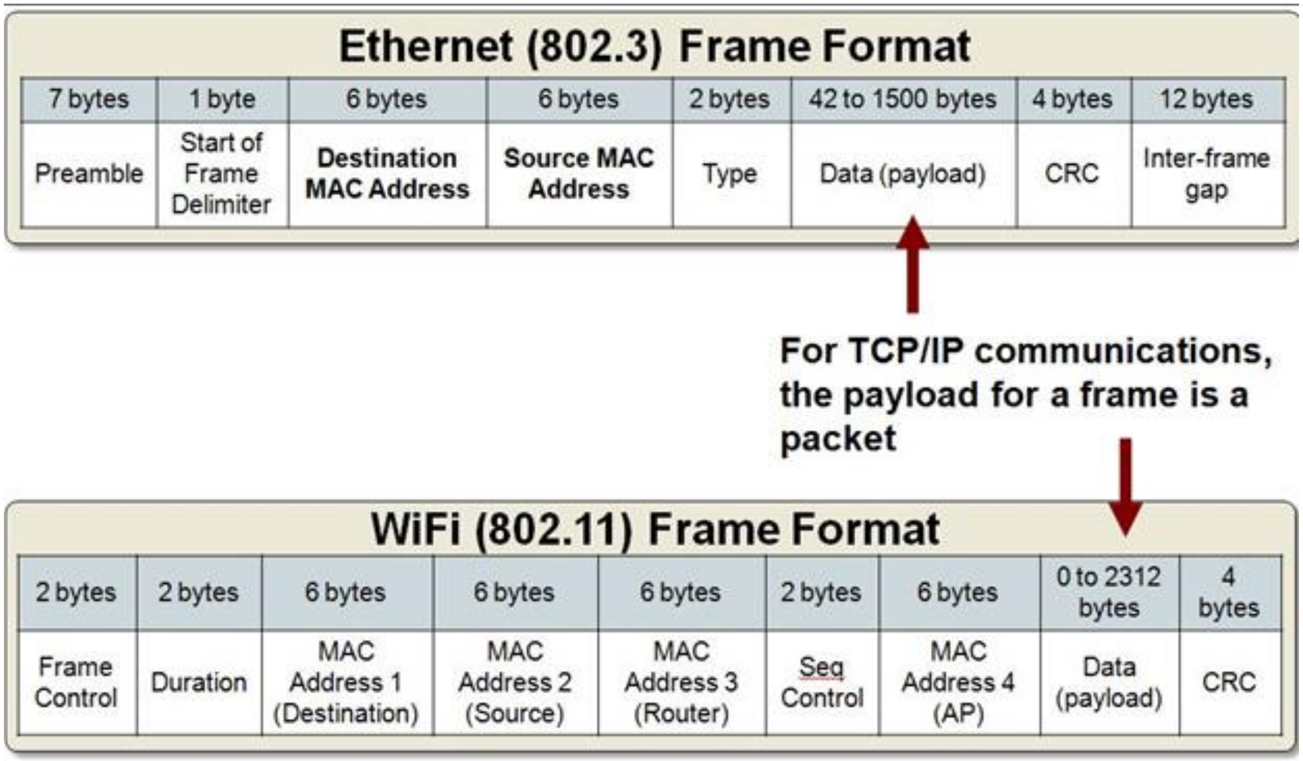
ACK

Initiator

Receiver

FIN

ACK



Ethernet (802.3) Frame Format

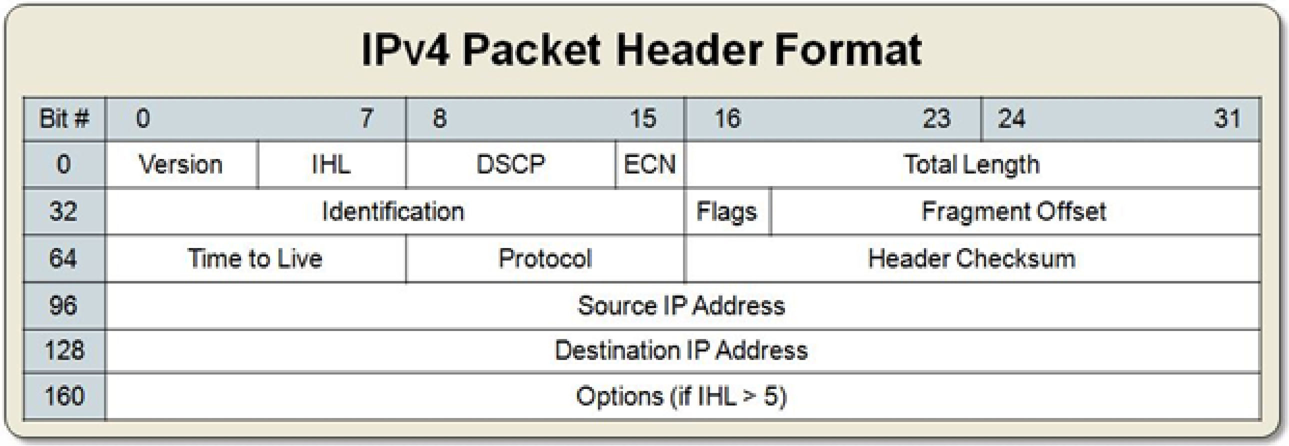
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

For TCP/IP communications, the payload for a frame is a packet

WiFi (802.11) Frame Format

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

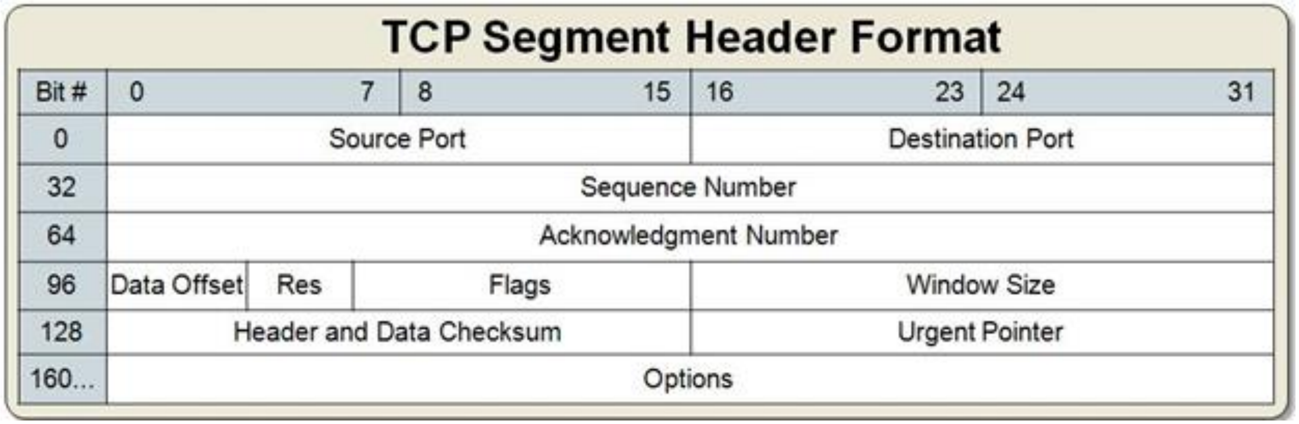
https://networkengineering.stackexchange.com/questions/25563/what-is-the-reason-for-the-different-order-of-the-source-and-destination-in-a-l2/25565



IPv4 Packet Header Format

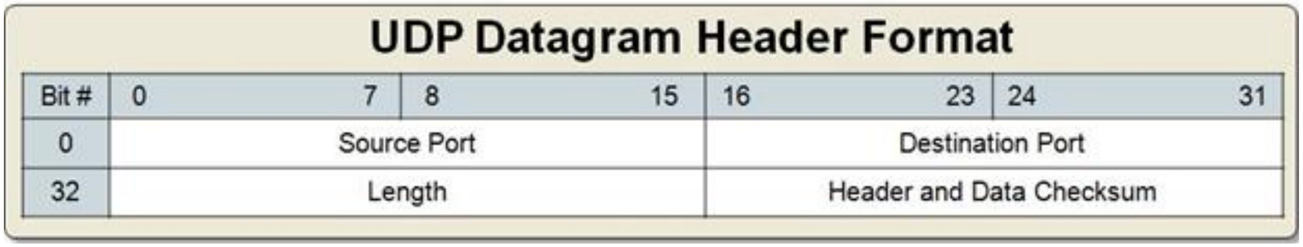
<table>
<tr><th>Bit #</th><th colspan="2">0 7</th><th colspan="2">8 15</th><th colspan="2">16 23</th><th>24 31</th></tr>
<tr><td>0</td><td>Version</td><td>IHL</td><td>DSCP</td><td>ECN</td><td colspan="3">Total Length</td></tr>
<tr><td>32</td><td colspan="4">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td>64</td><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td>96</td><td colspan="7">Source IP Address</td></tr>
<tr><td>128</td><td colspan="7">Destination IP Address</td></tr>
<tr><td>160</td><td colspan="7">Options (if IHL > 5)</td></tr>
</table>

https://networkengineering.stackexchange.com/questions/25563/what-is-the-reason-for-the-different-order-of-the-source-and-destination-in-a-l2/25565



TCP Segment Header Format

<table>
<tr><th>Bit #</th><th>0</th><th>7</th><th>8</th><th>15</th><th>16</th><th>23</th><th>24</th><th>31</th></tr>
<tr><td>0</td><td colspan="4">Source Port</td><td colspan="4">Destination Port</td></tr>
<tr><td>32</td><td colspan="8">Sequence Number</td></tr>
<tr><td>64</td><td colspan="8">Acknowledgment Number</td></tr>
<tr><td>96</td><td>Data Offset</td><td>Res</td><td colspan="2">Flags</td><td colspan="4">Window Size</td></tr>
<tr><td>128</td><td colspan="4">Header and Data Checksum</td><td colspan="4">Urgent Pointer</td></tr>
<tr><td>160...</td><td colspan="8">Options</td></tr>
</table>



UDP Datagram Header Format

<table>
<tr><th>Bit #</th><th>0</th><th>7</th><th>8</th><th>15</th><th>16</th><th>23</th><th>24</th><th>31</th></tr>
<tr><td>0</td><td colspan="4">Source Port</td><td colspan="4">Destination Port</td></tr>
<tr><td>32</td><td colspan="4">Length</td><td colspan="4">Header and Data Checksum</td></tr>
</table>

https://networkengineering.stackexchange.com/questions/25563/what-is-the-reason-for-the-different-order-of-the-source-and-destination-in-a-l2/25565