Introduction to Networking

Zane Ma
University of Illinois
CS 461 / ECE 422 - Fall 2019

Educational Objectives

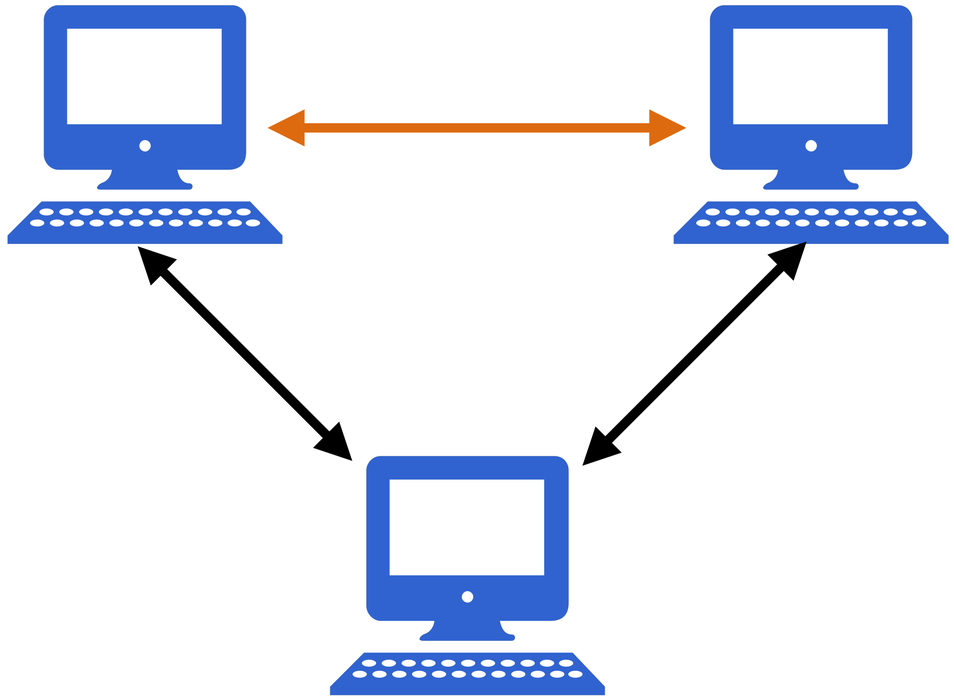
- Understand networking layer abstraction
- Introduction to packet headers to understand the concerns of each layer - more depth in CP2
- How to use Wireshark to visualize encapsulation, packet headers/ content
- How to perform dig / curl
- How to use scapy to send / receive SYN + SYN/ACK

First Things First

- Start downloading: https://uofi.box.com/v/cs461-netsec-vm
- We will use this for follow-along live demos for latter half of the discussion

What is Networking?

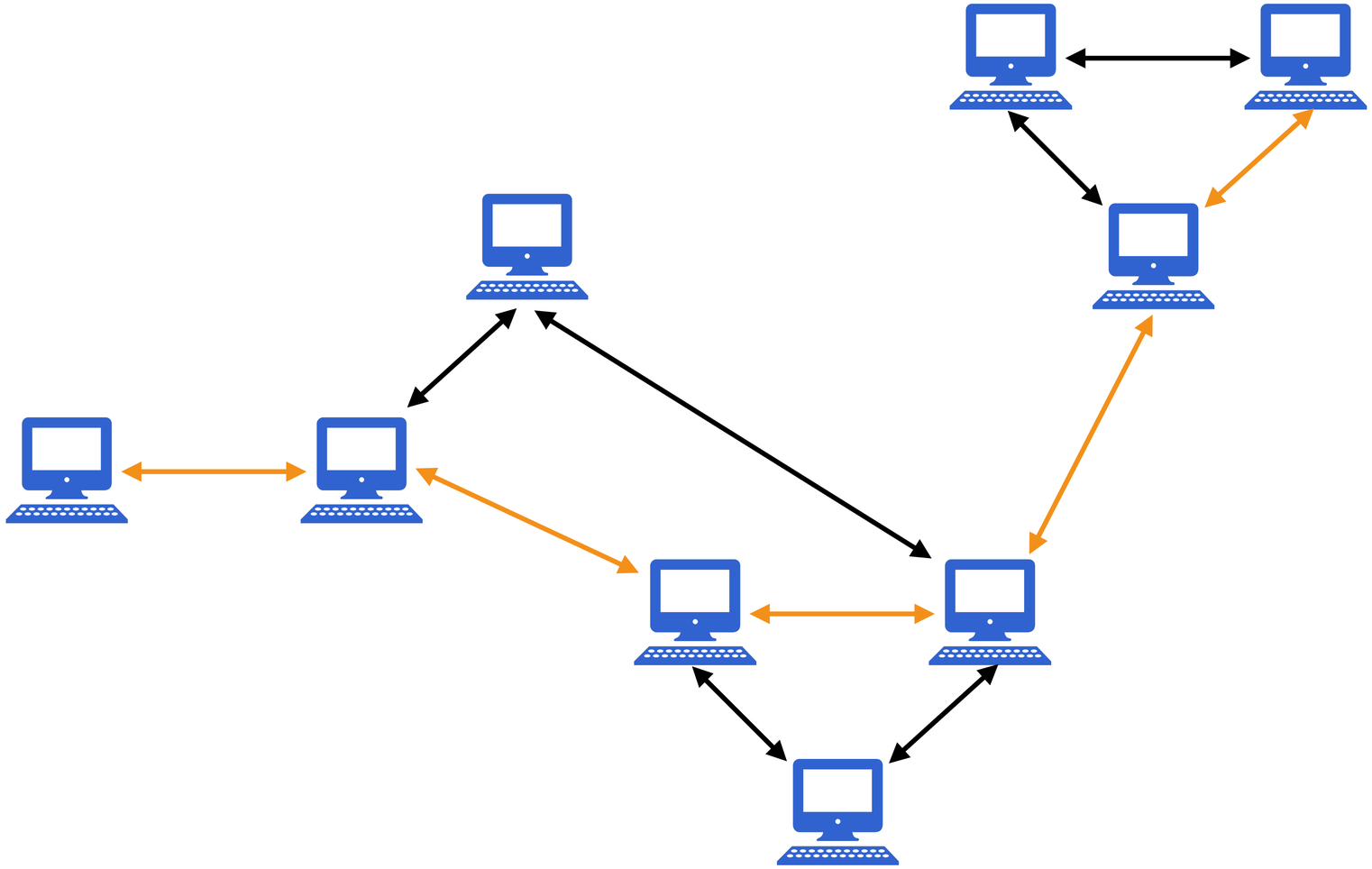
1950s - Simple networks



What is Networking?

1950s - Simple networks

1960s & 70s - Internet

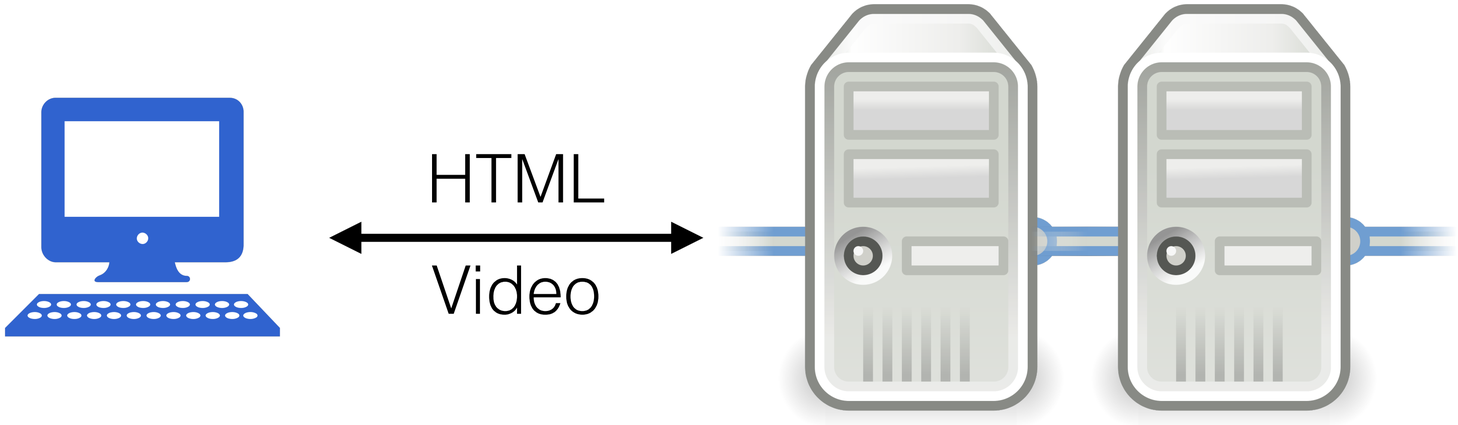


What is Networking?

1950s - Simple networks

1960s & 70s - Internet

1980s & 90s - Web



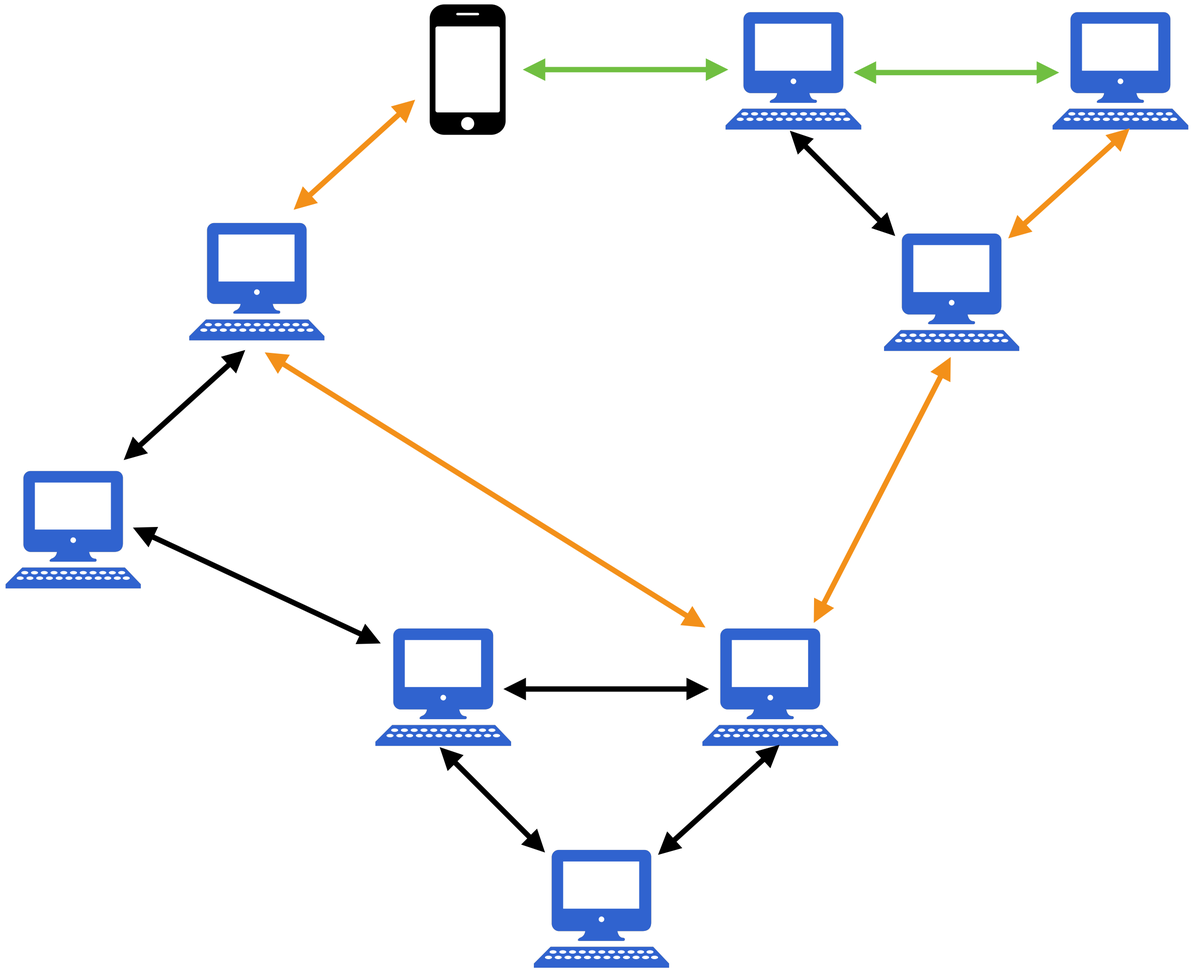
What is Networking?

1950s - Simple networks

1960s & 70s - Internet

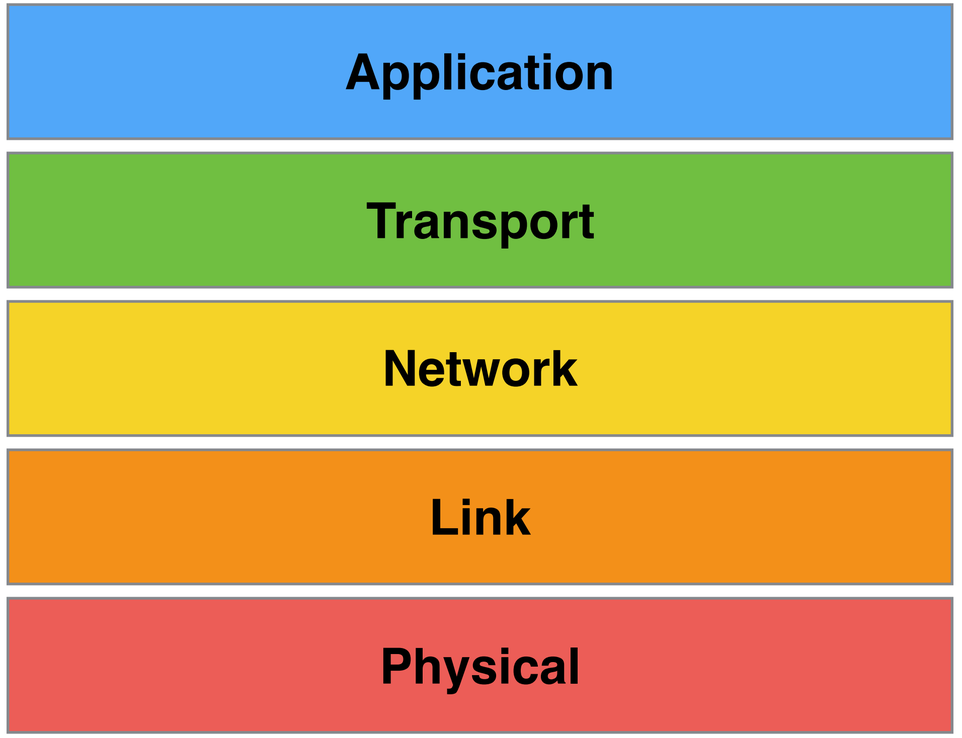
1980s & 90s - Web

2000s - Mobile

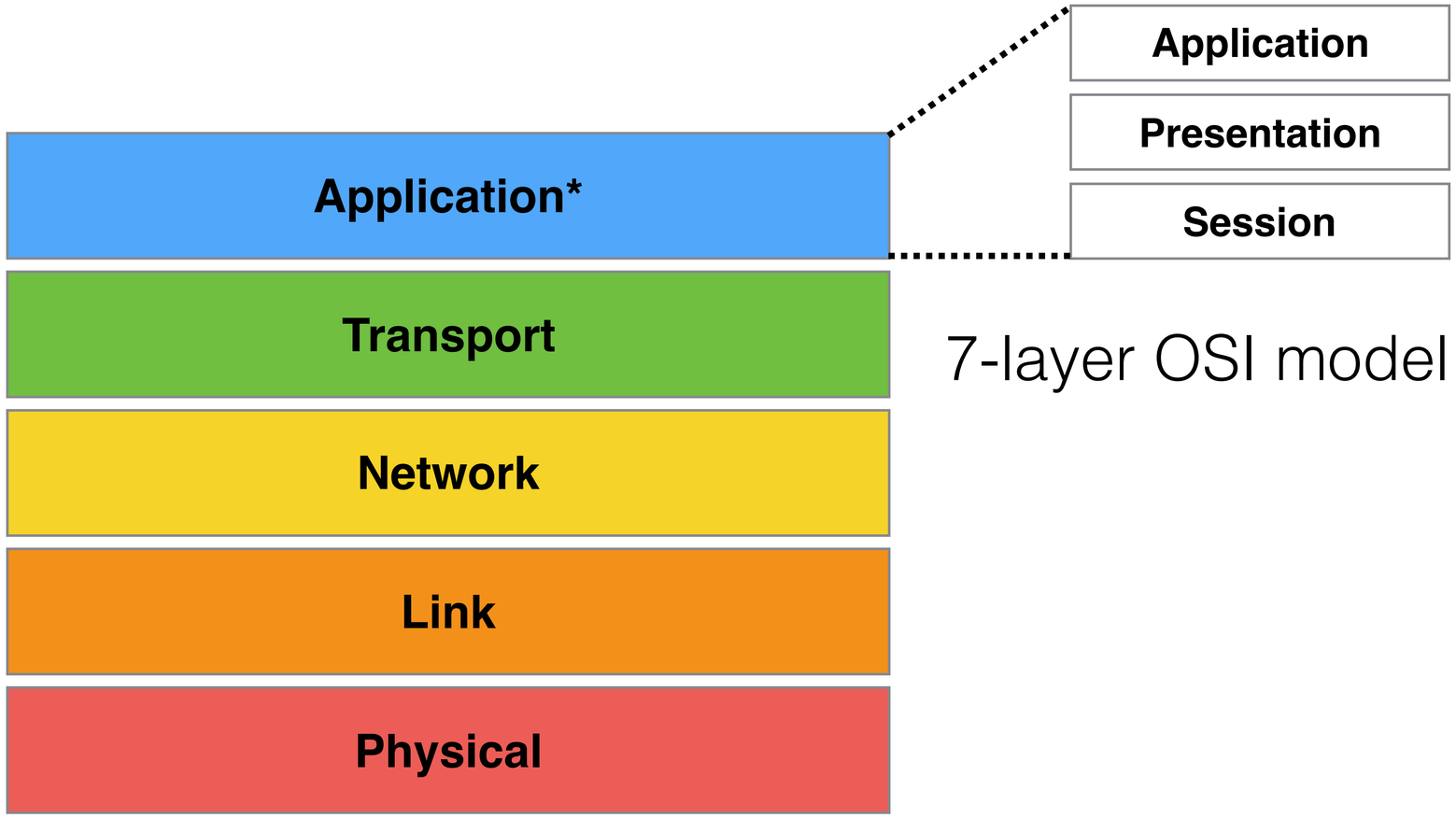


How Does Networking Work?

How Does Networking Work?



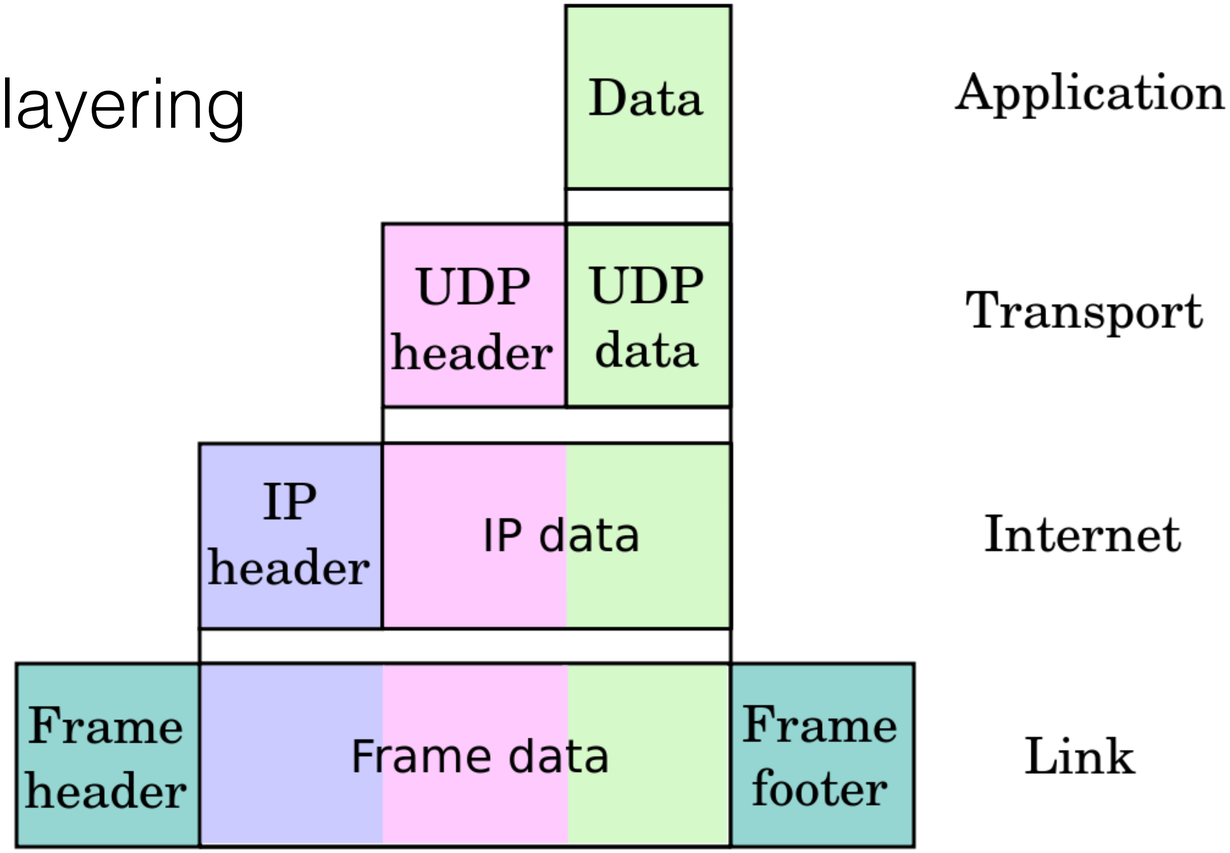
How Does Networking Work?



7-layer OSI model

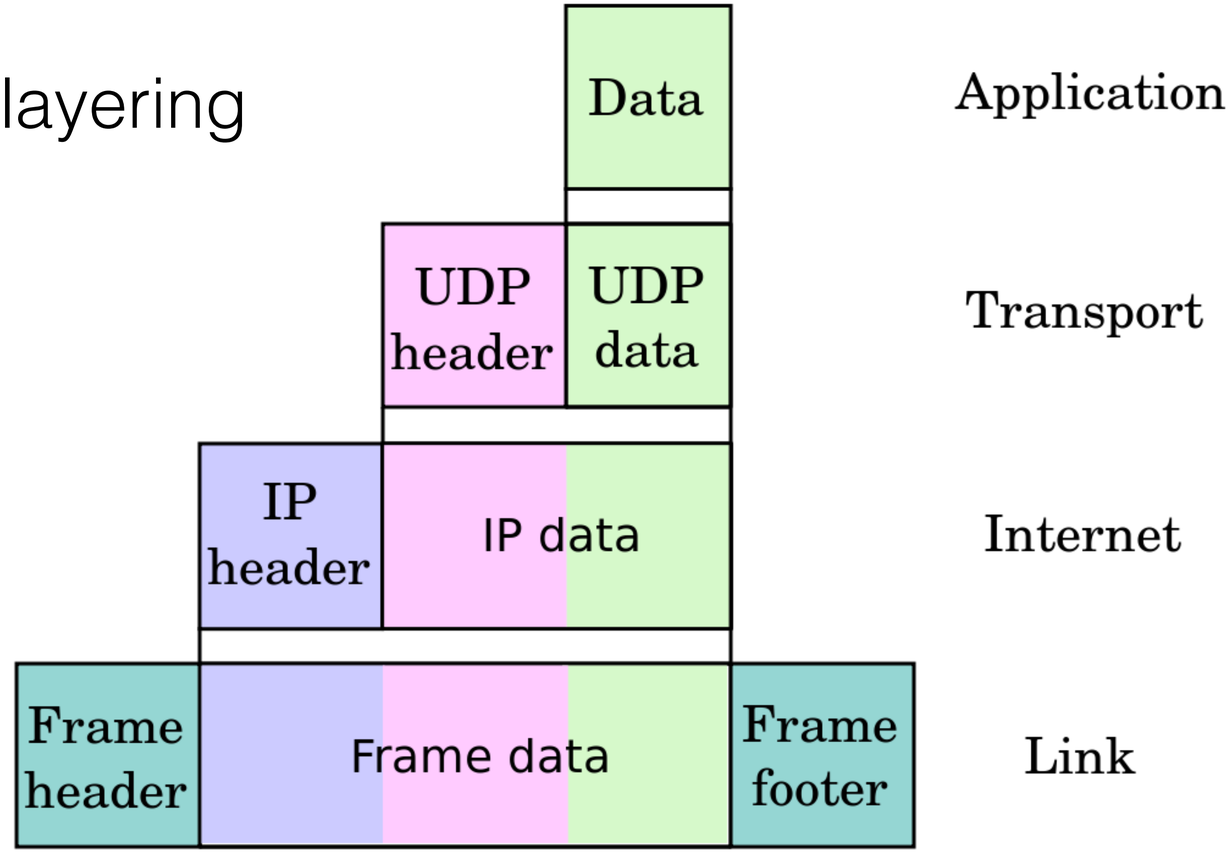
Encapsulation

Network packet layering



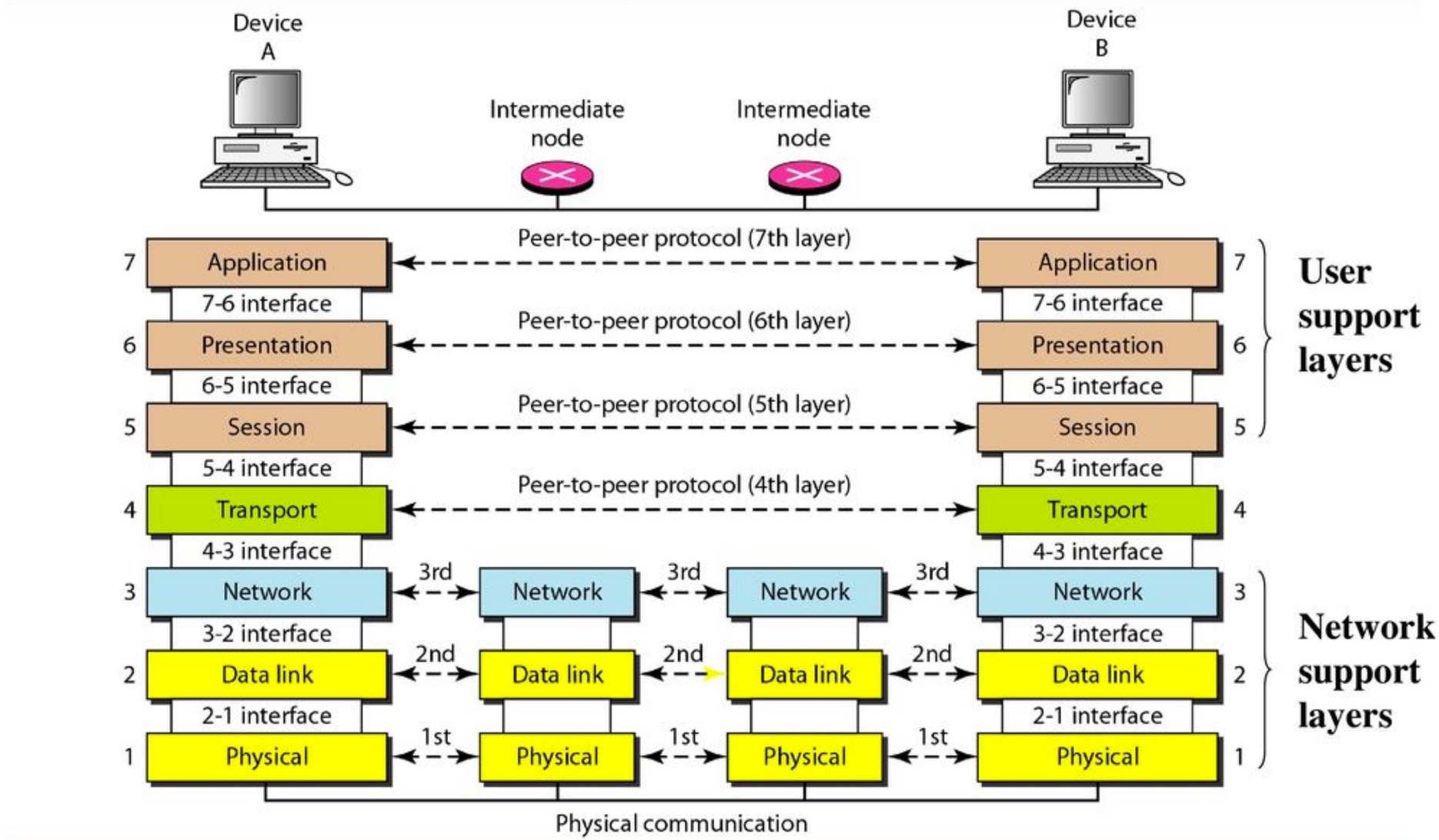
Encapsulation

Network packet layering

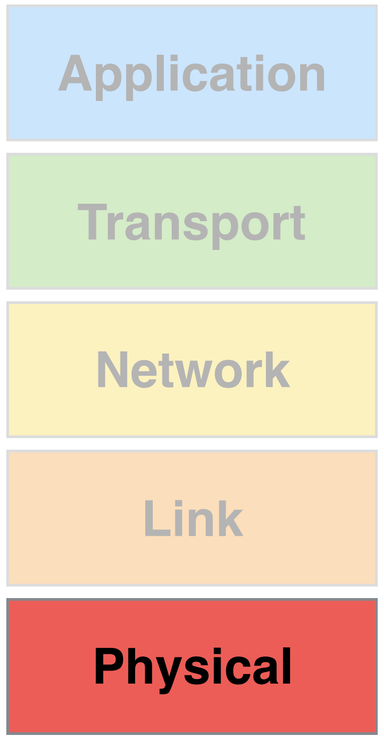


Counterintuitive: higher layers are more deeply nested

Encapsulation

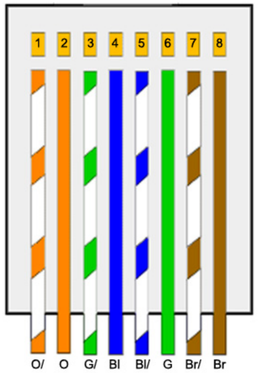


Physical Layer

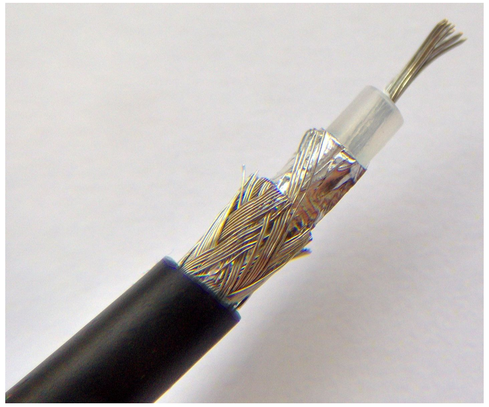


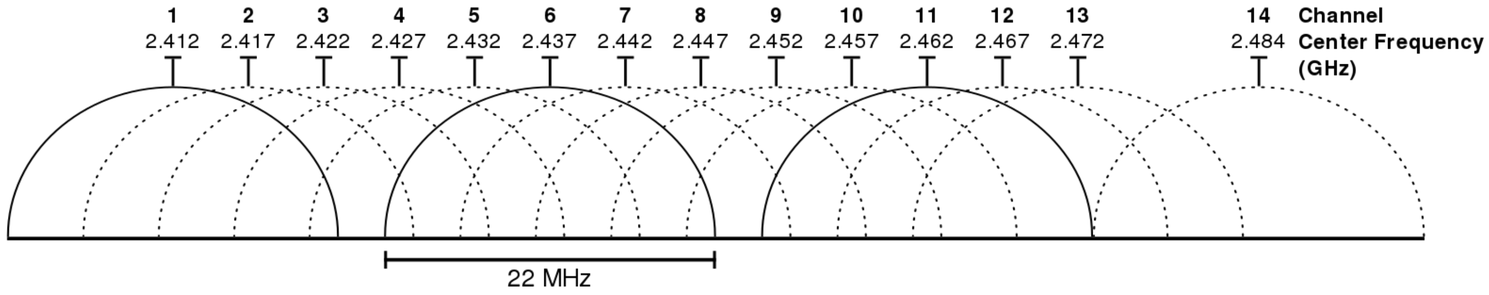
Physical Layer

- Application
- Transport
- Network
- Link
- **Physical**

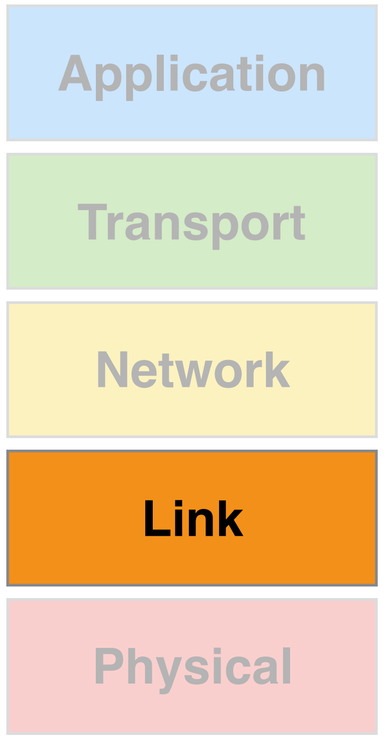


568B





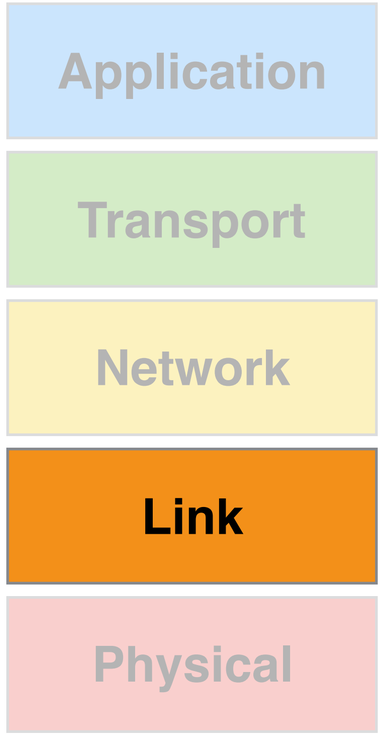
Link Layer



Physically connected node-to-node communication

MAC Address: unique ID for network interface controller

Link Layer



Physically connected node-to-node communication

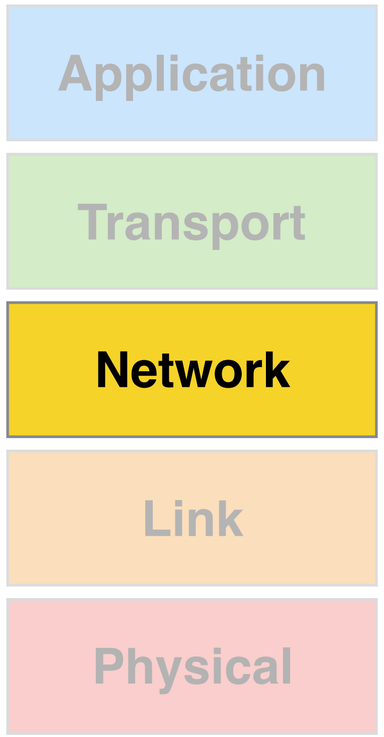
MAC Address: unique ID for network interface controller

WiFi (802.11)

Ethernet

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets

Network Layer



Indirectly connected nodes

IP Address: unique ID for network nodes

Network Layer

Application

Transport

Network

Link

Physical

Indirectly connected nodes

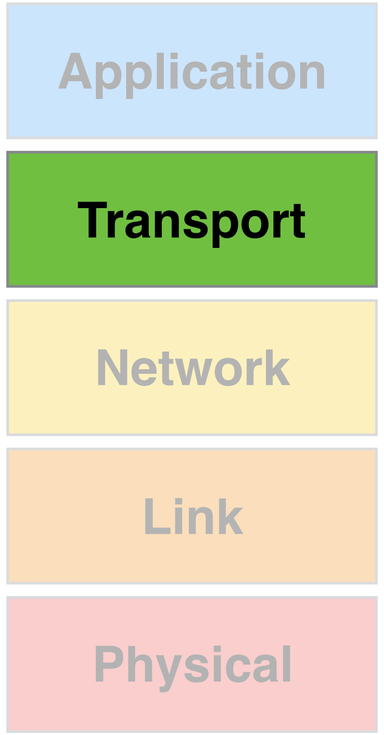
IP Address: unique ID for network nodes

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Data Payload

Transport Layer



Network layer: communication between hosts

Transport: communication between processes

Can also be used for reliability, flow control, multiplexing, connection-oriented communication

Transport Layer

Application

Transport

Network

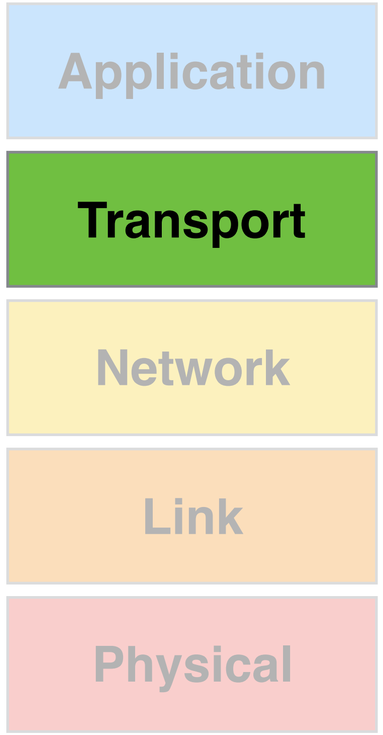
Link

Physical

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port														
4	32	Length																Checksum														

Transport Layer



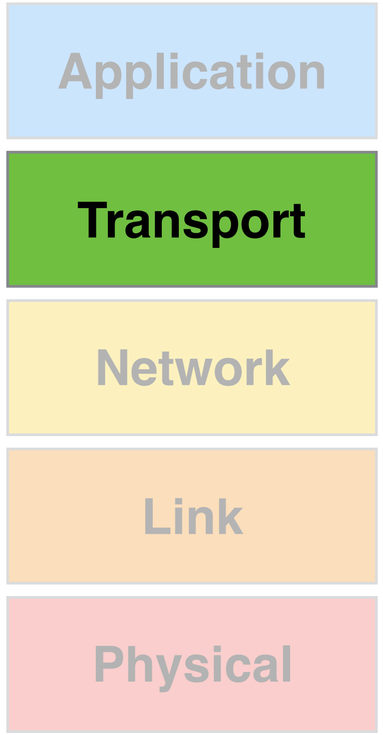
UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port														
4	32	Length																Checksum														

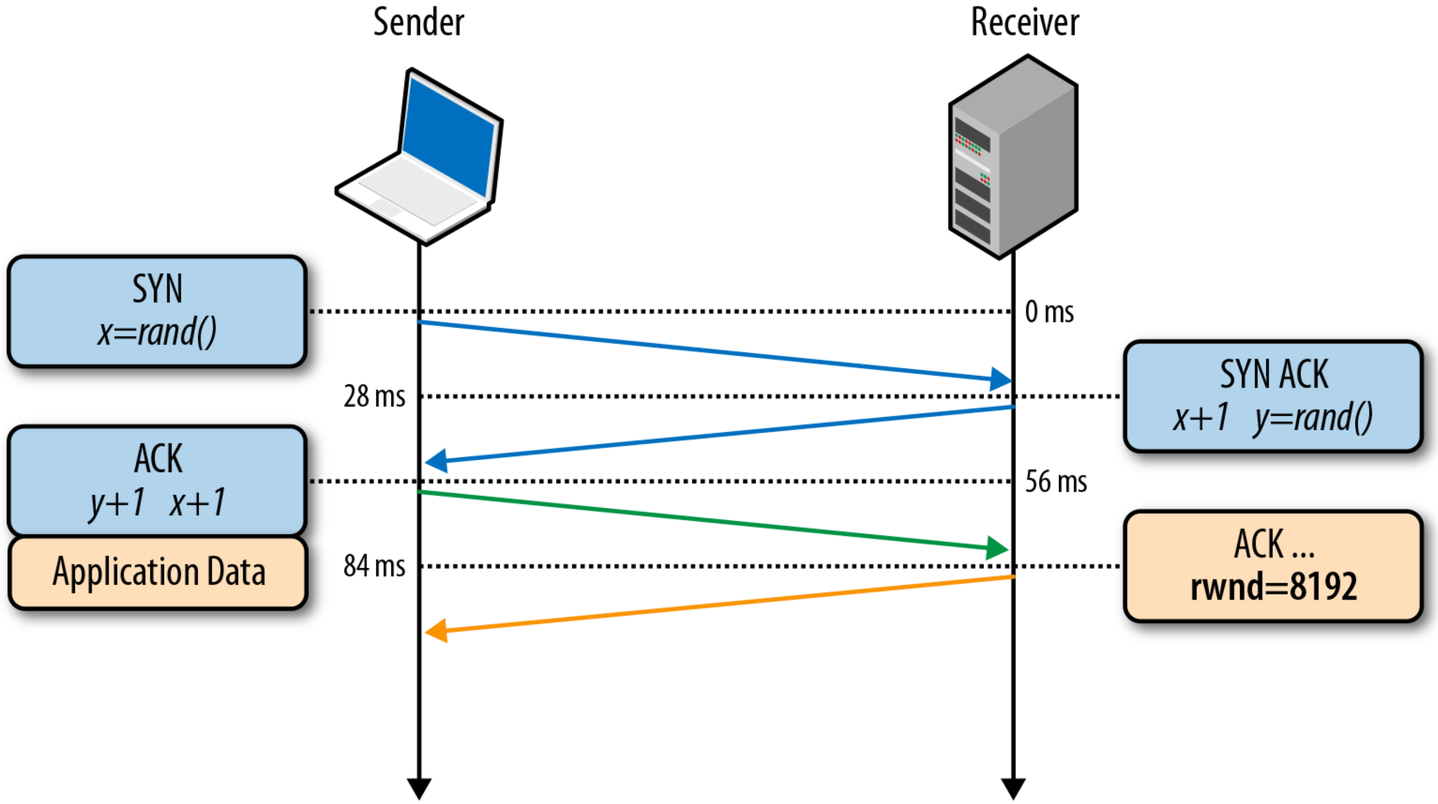
TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset			Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

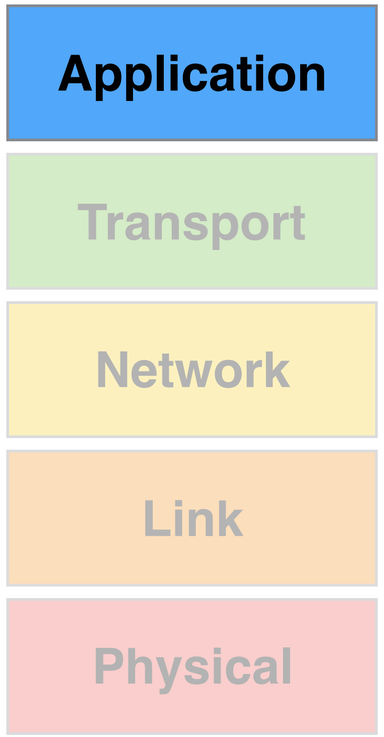
Transport Layer



TCP: Three-way handshake



Application Layer



Anything and everything!

WireShark Demo

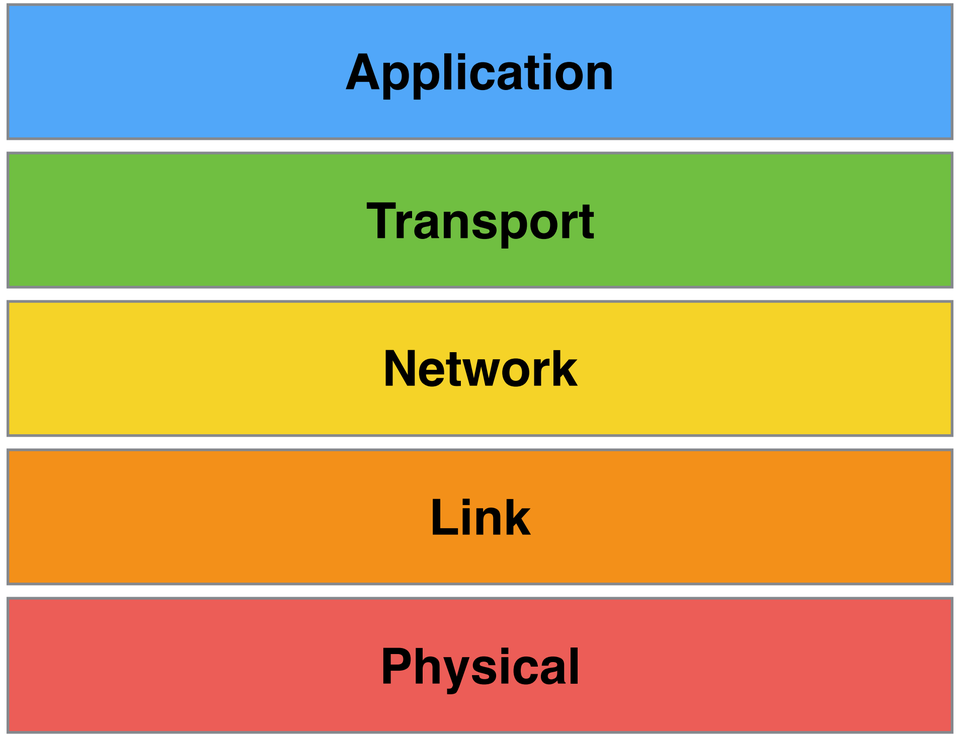
When in doubt (or not in doubt), use WireShark. Always use WireShark.

DNS Demo

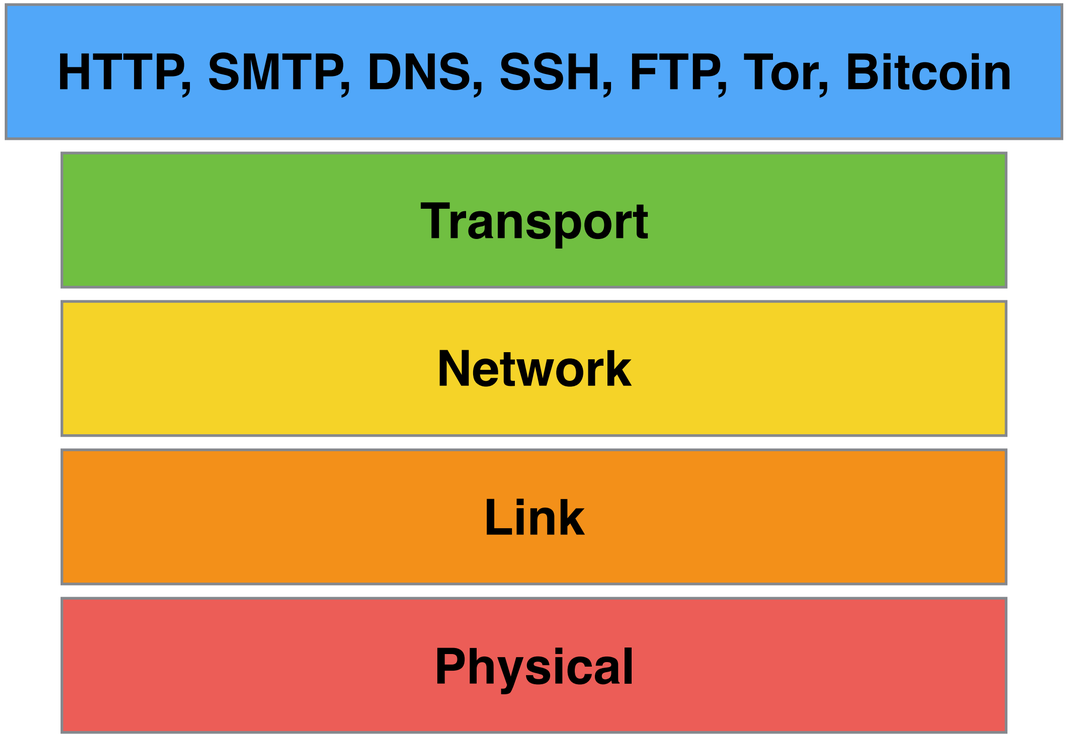
HTTP Demo

Scapy Demo

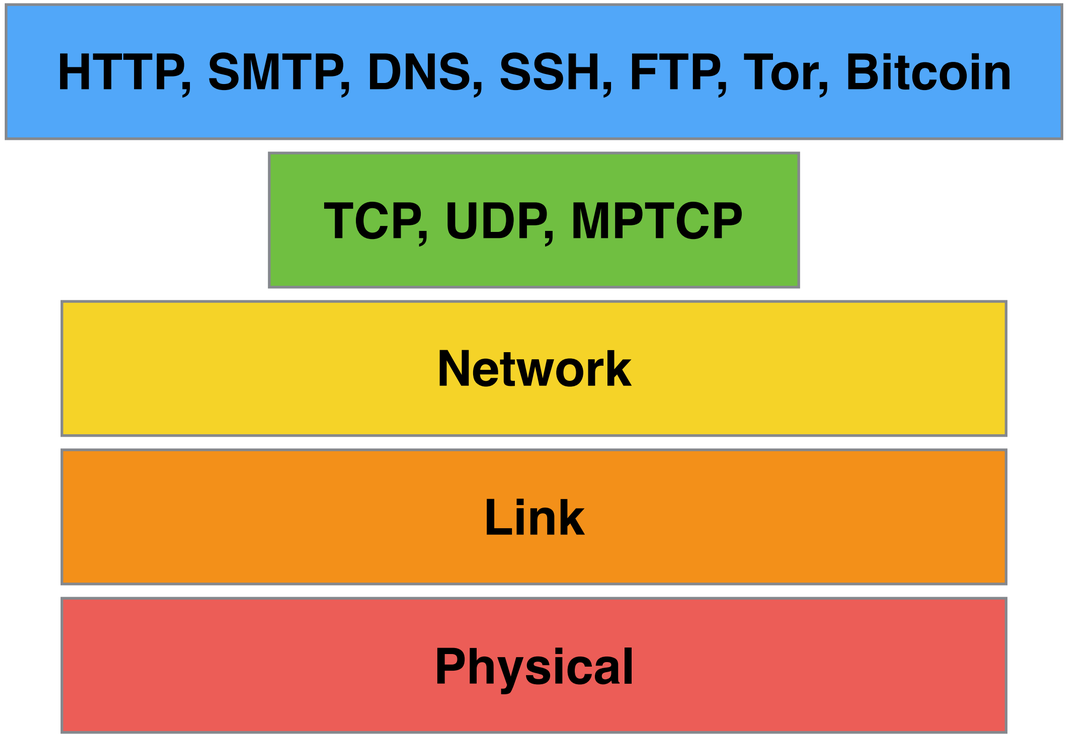
Narrow Waist



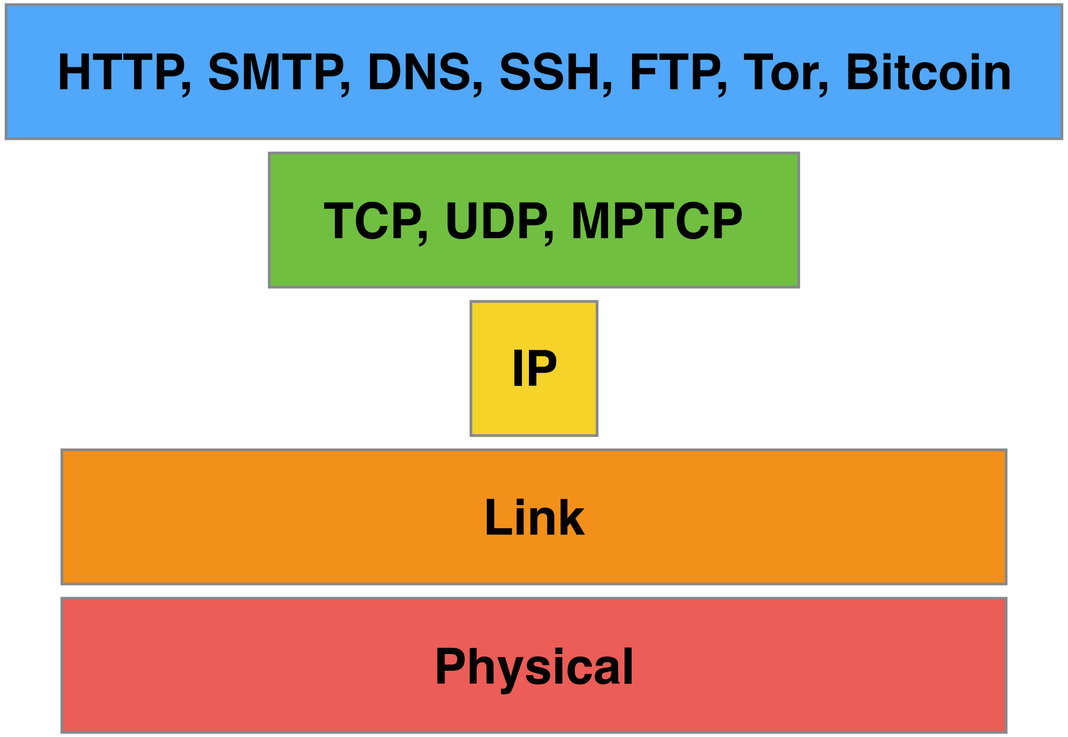
Narrow Waist



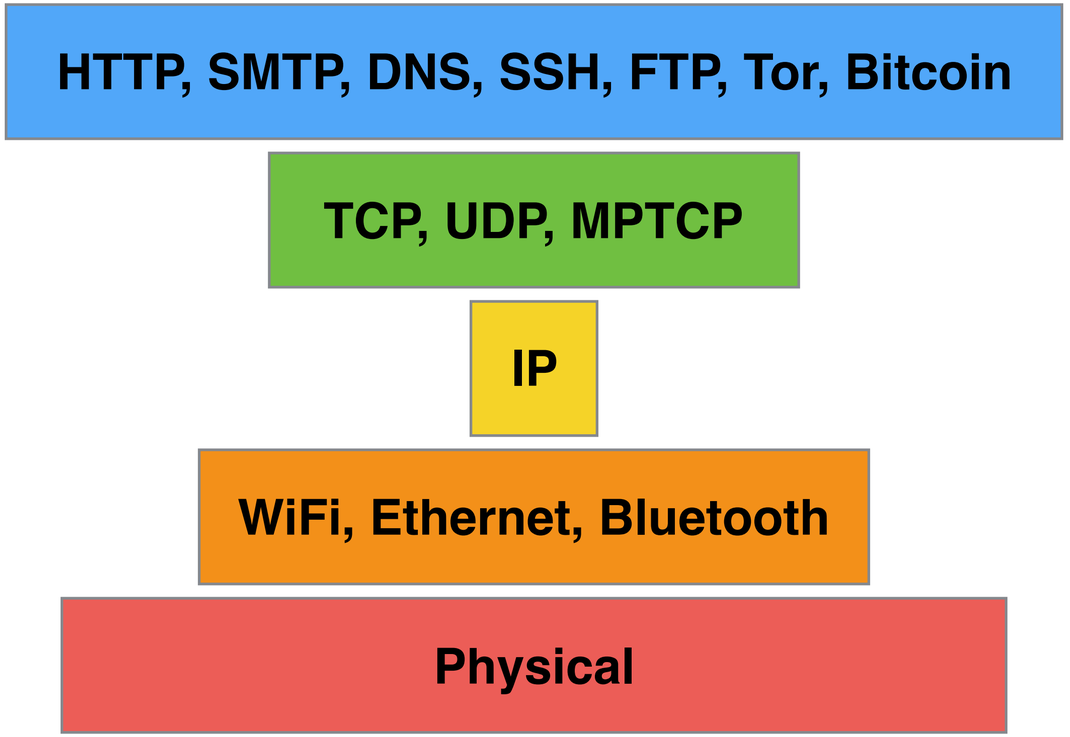
Narrow Waist



Narrow Waist



Narrow Waist



Narrow Waist