

# Transport Layer, TCP and Floods

Ali Ghaffarian

December 1, 2024



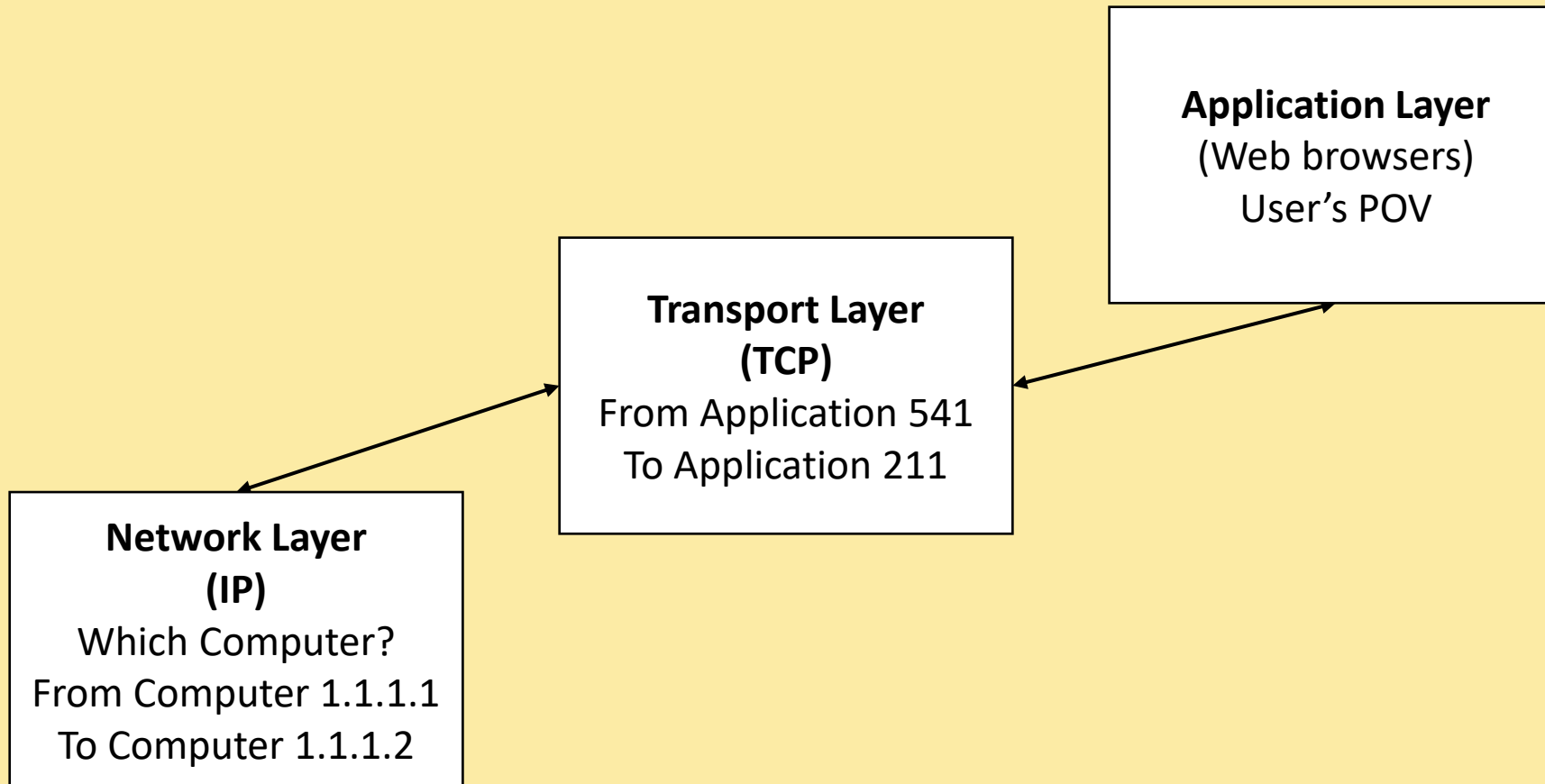
# About Me

- Linux and Network Deep Diver
- Github: [github.com/AliGhaffarian](https://github.com/AliGhaffarian)

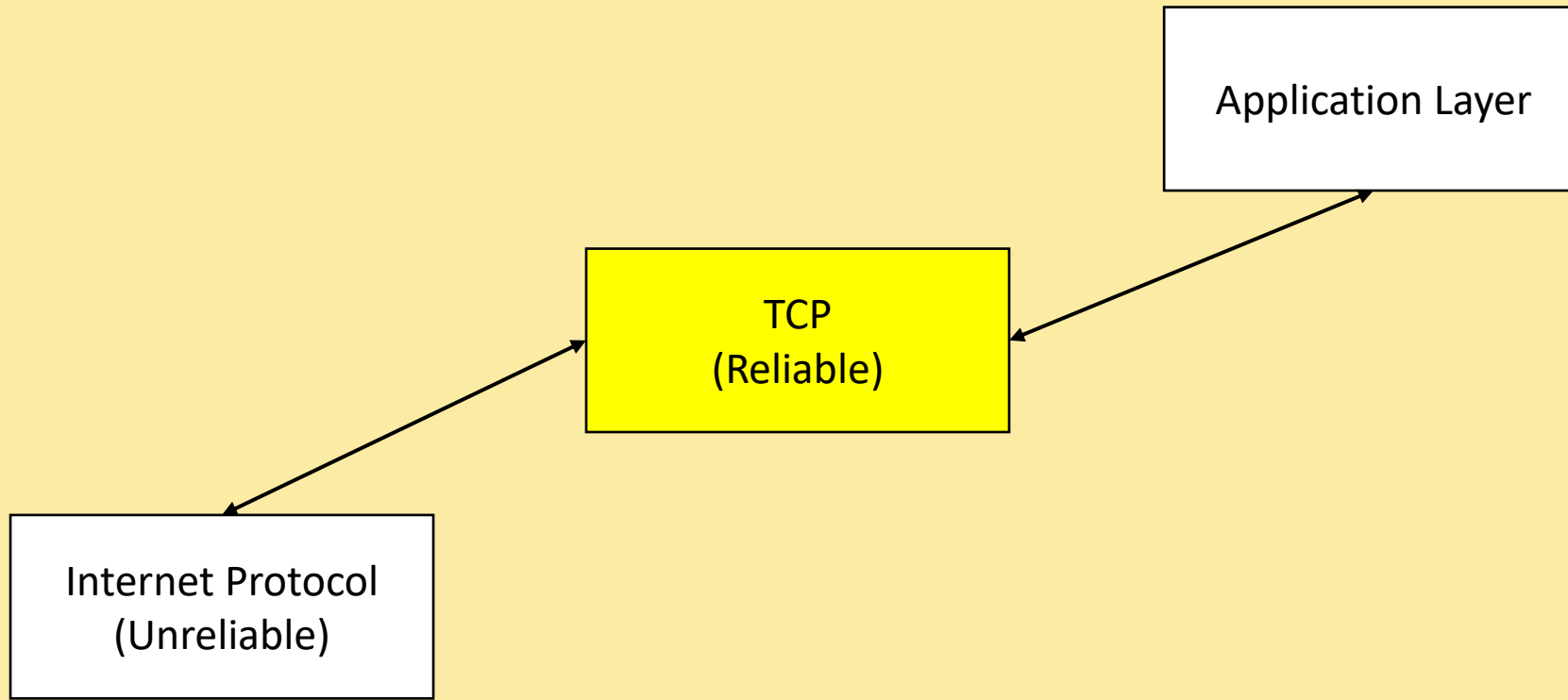
# Table of contents

- Transport Layer in TCP/IP Stack
- TCP
- The Three Way Handshake
- Syn Floods

# Transport Layer in TCP/IP Stack



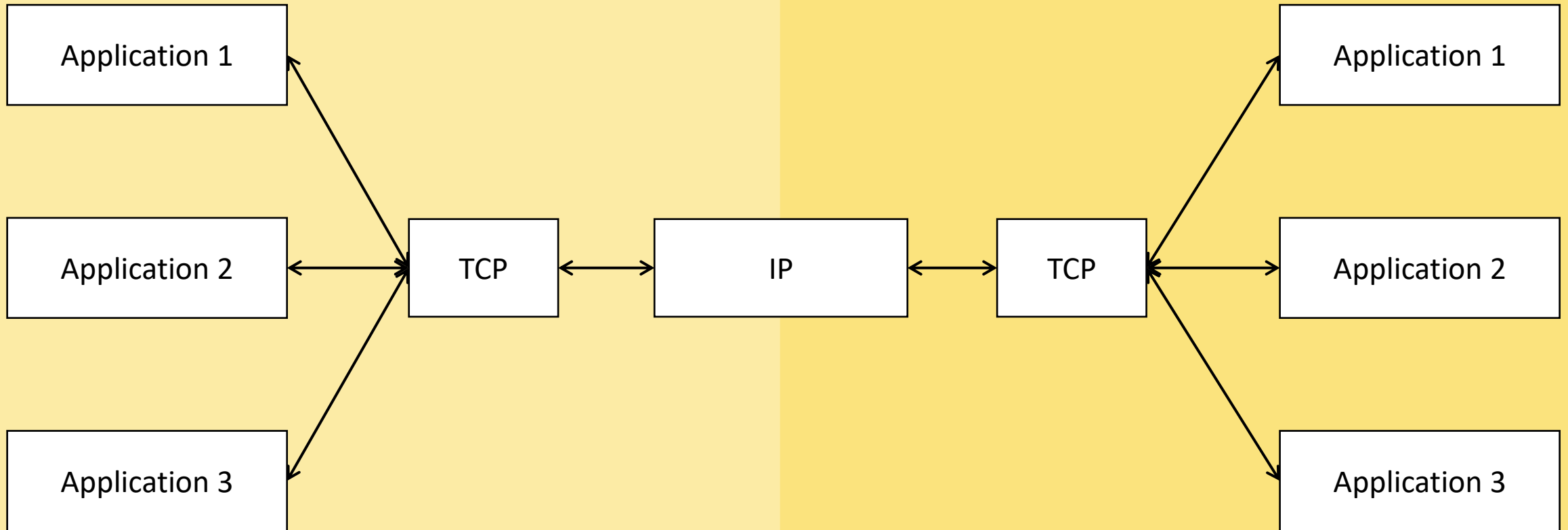
# TCP



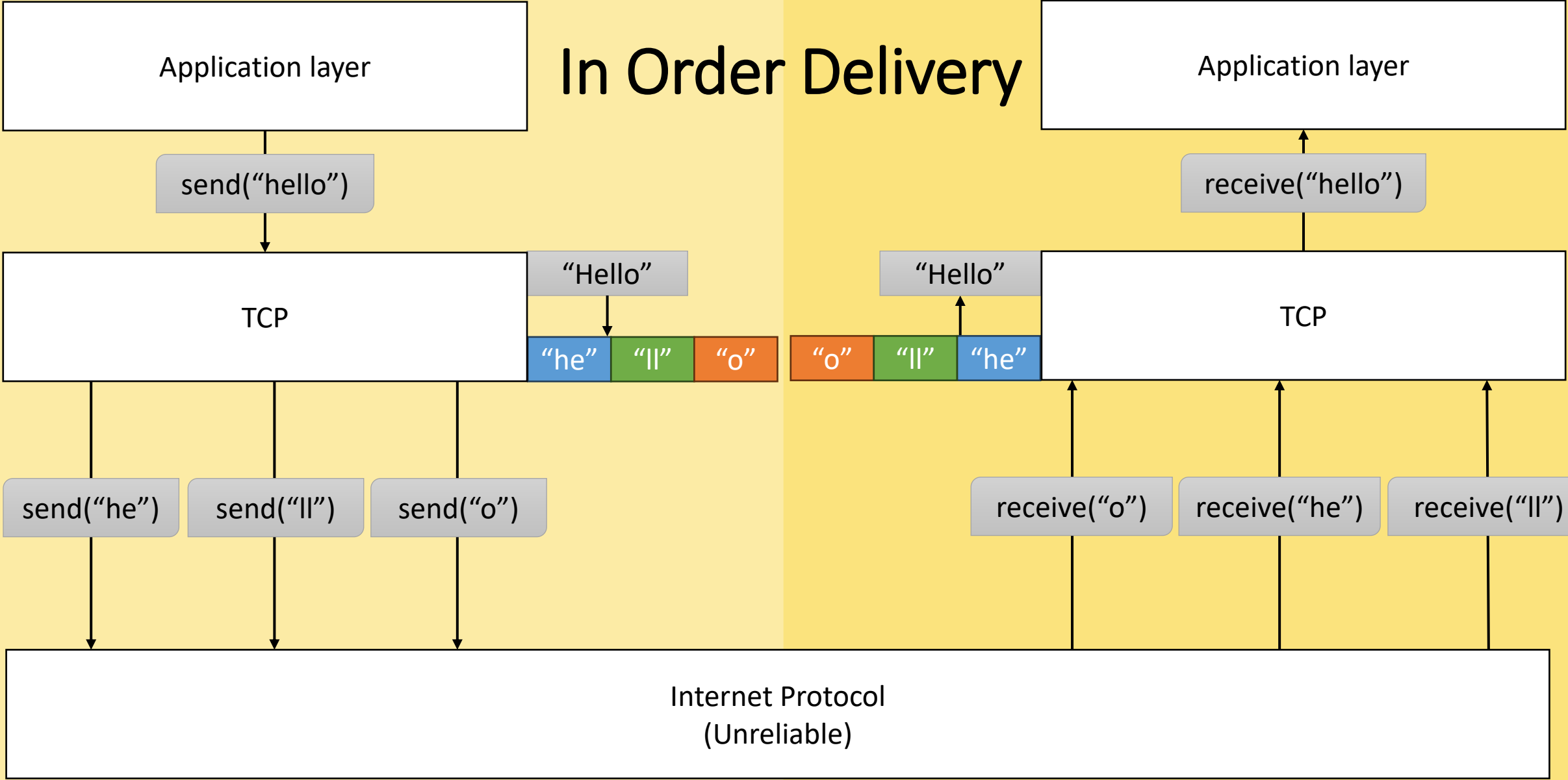
# TCP's Fields

- Source Port ( From Which Application )
- Destination Port ( To Which Application )
- Sequence Number
- Acknowledgement Number
- Flags
- ...

# Multiplexing / Demultiplexing



# In Order Delivery





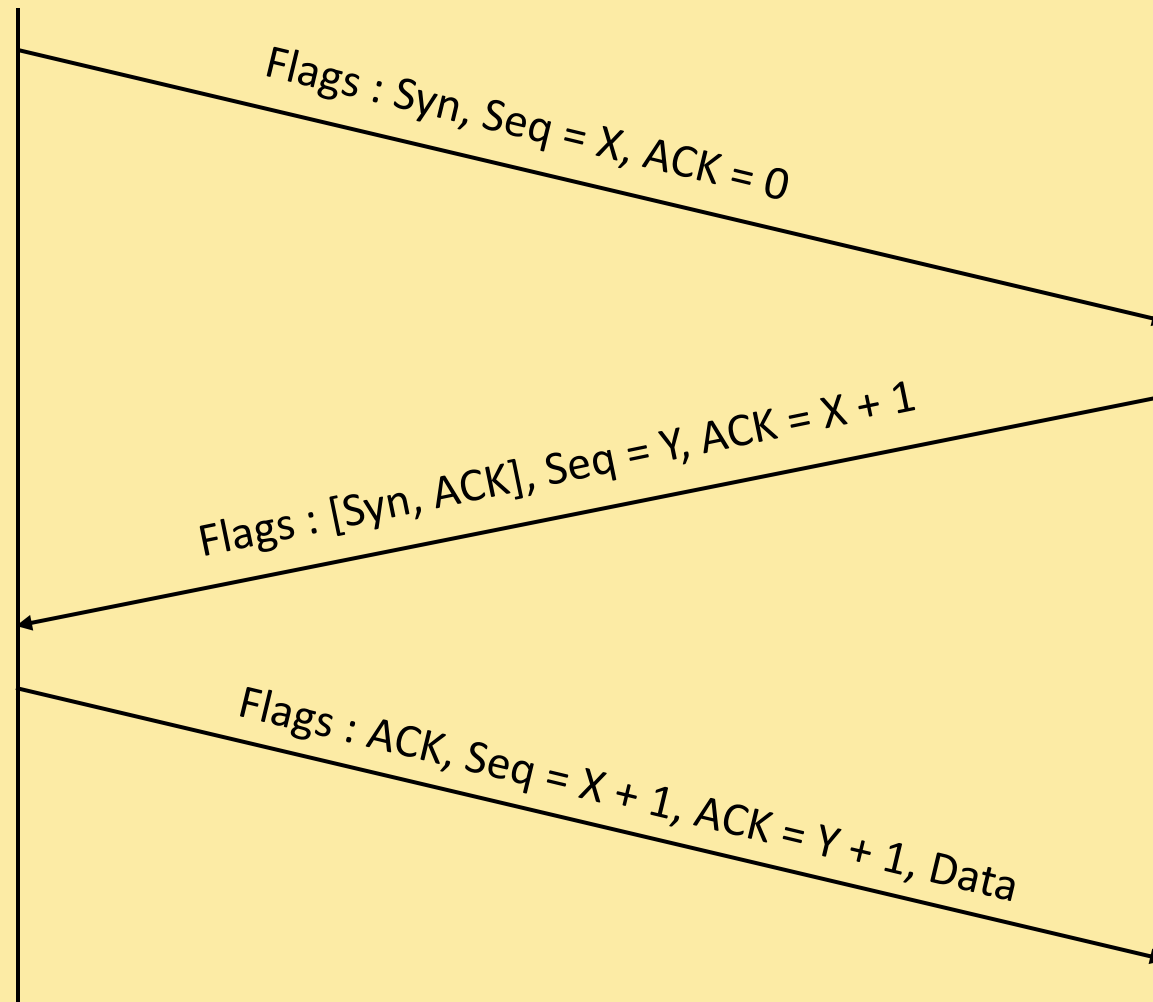
# TCP Flags

000.	....	....	= Reserved
...0	....	....	= Accurate ECN
....	0...	....	= Congestion Window Reduced
....	.0..	....	= ECN-Echo
....	..0.	....	= Urgent
....	...0	....	= <b>Ack</b>
....	....	0...	= Push
....	....	.0..	= Reset
....	....	..0.	= <b>Syn</b>
....	....	...0	= <b>Fin</b>

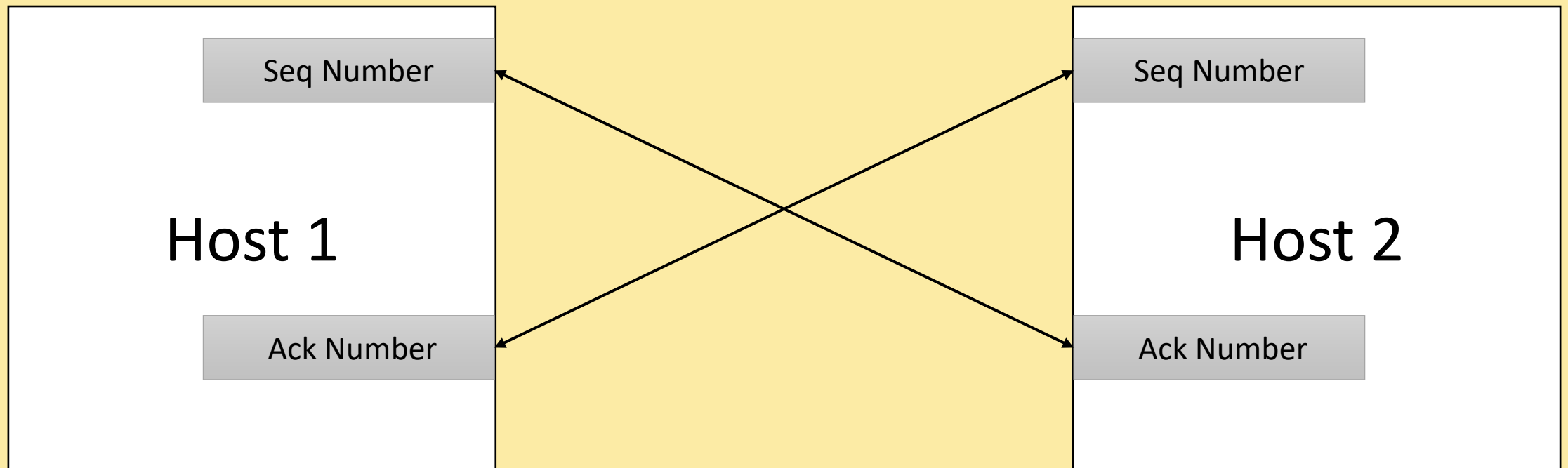
# The Tree Way Handshake

Host 1

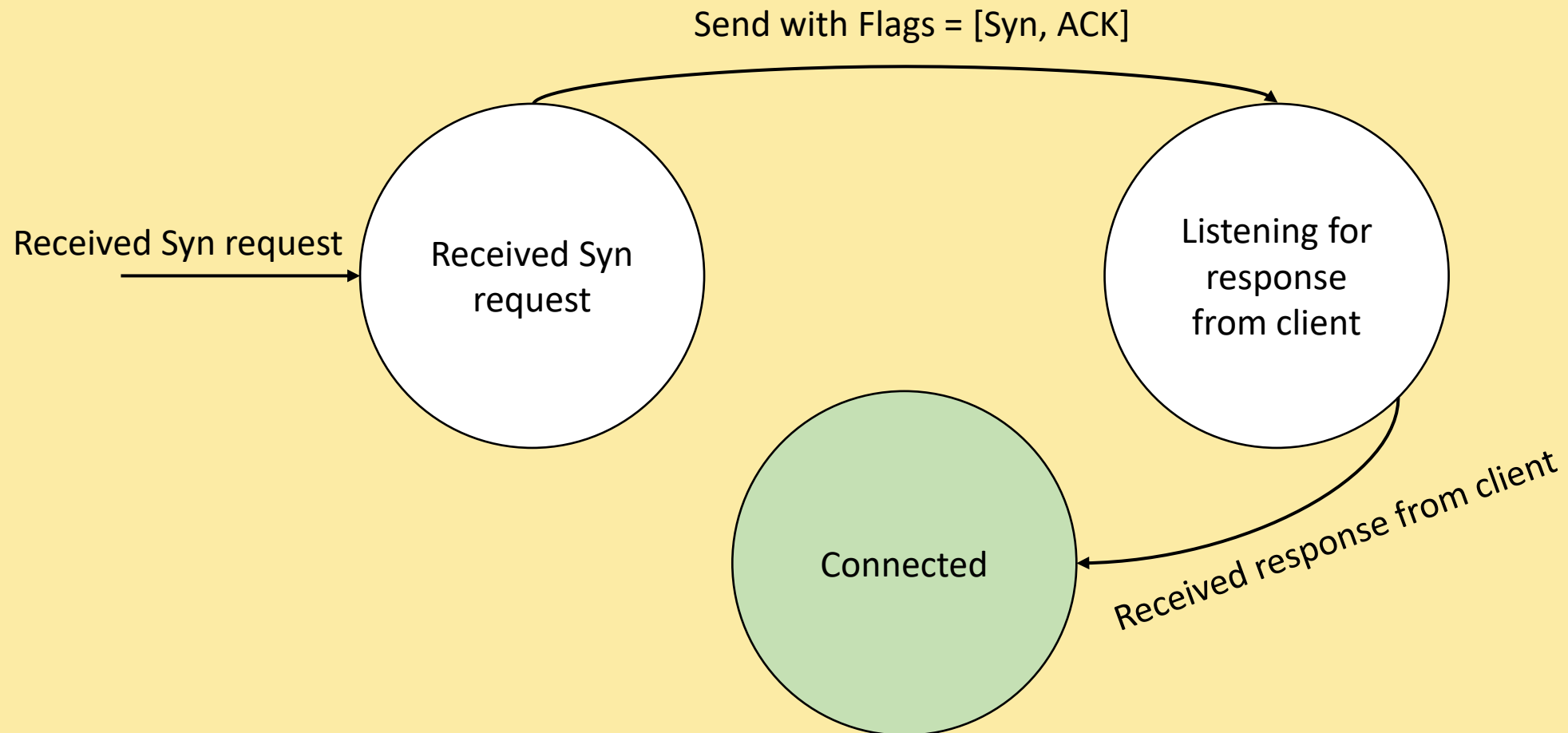
Host 2



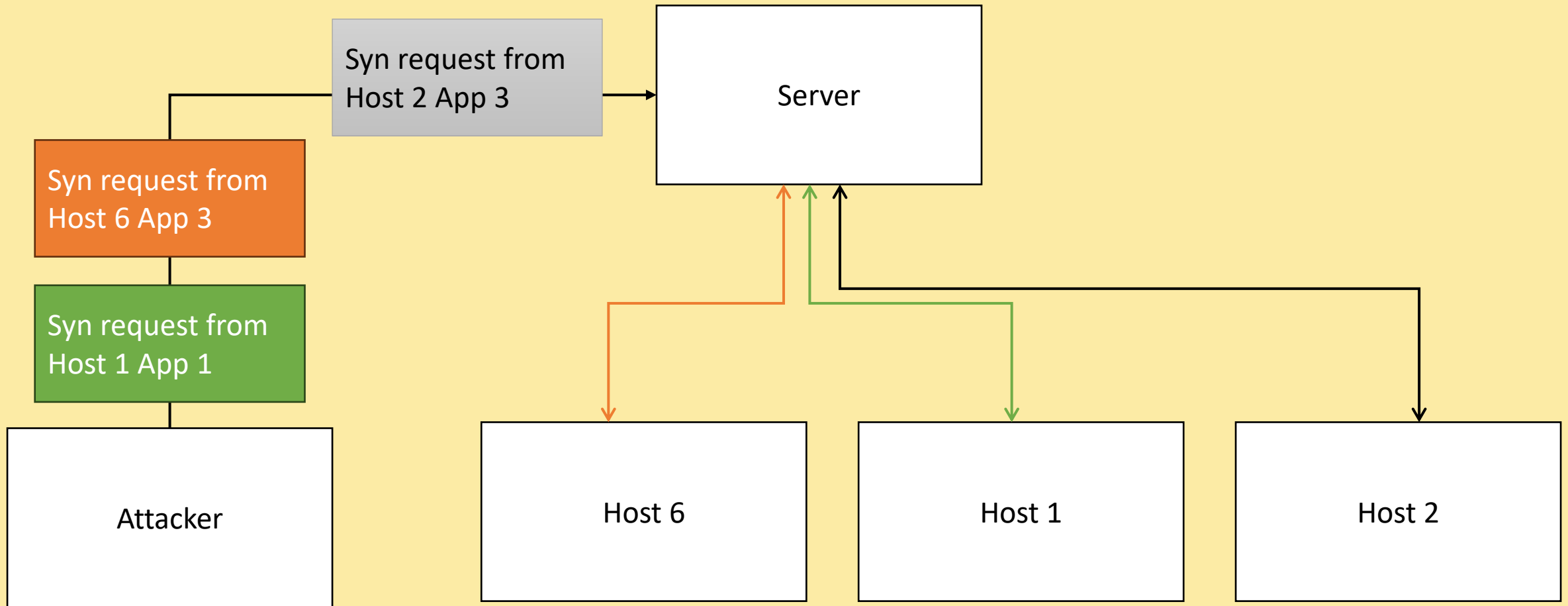
# Sequence And Acknowledgement Number



# State Machine of a TCP Server

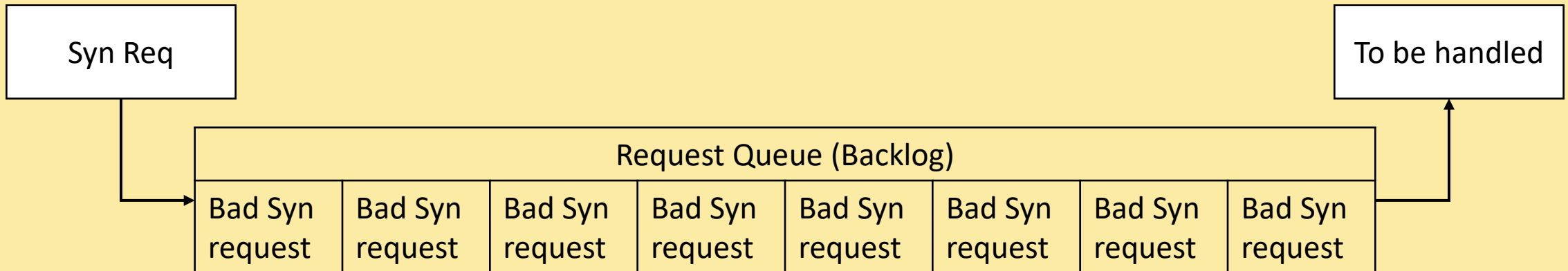


# SYN Floods



# SYN Flooding is Cheap

Always Waiting on Non-Existing Clients



# Syn Cookies

- Handle the Handshake Statelessly
- No More Request Queue (Backlog)
- Reconstructing the Connection

# Learn More

- `linux/net/ipv4/syncookies.c`
- `lwn.net/Articles/277146`



# Questions

Presentation Files:

[github.com/AliGhaffarian/university\\_thingies](https://github.com/AliGhaffarian/university_thingies)