Transport Layer, TCP and Floods

Ali Ghaffarian

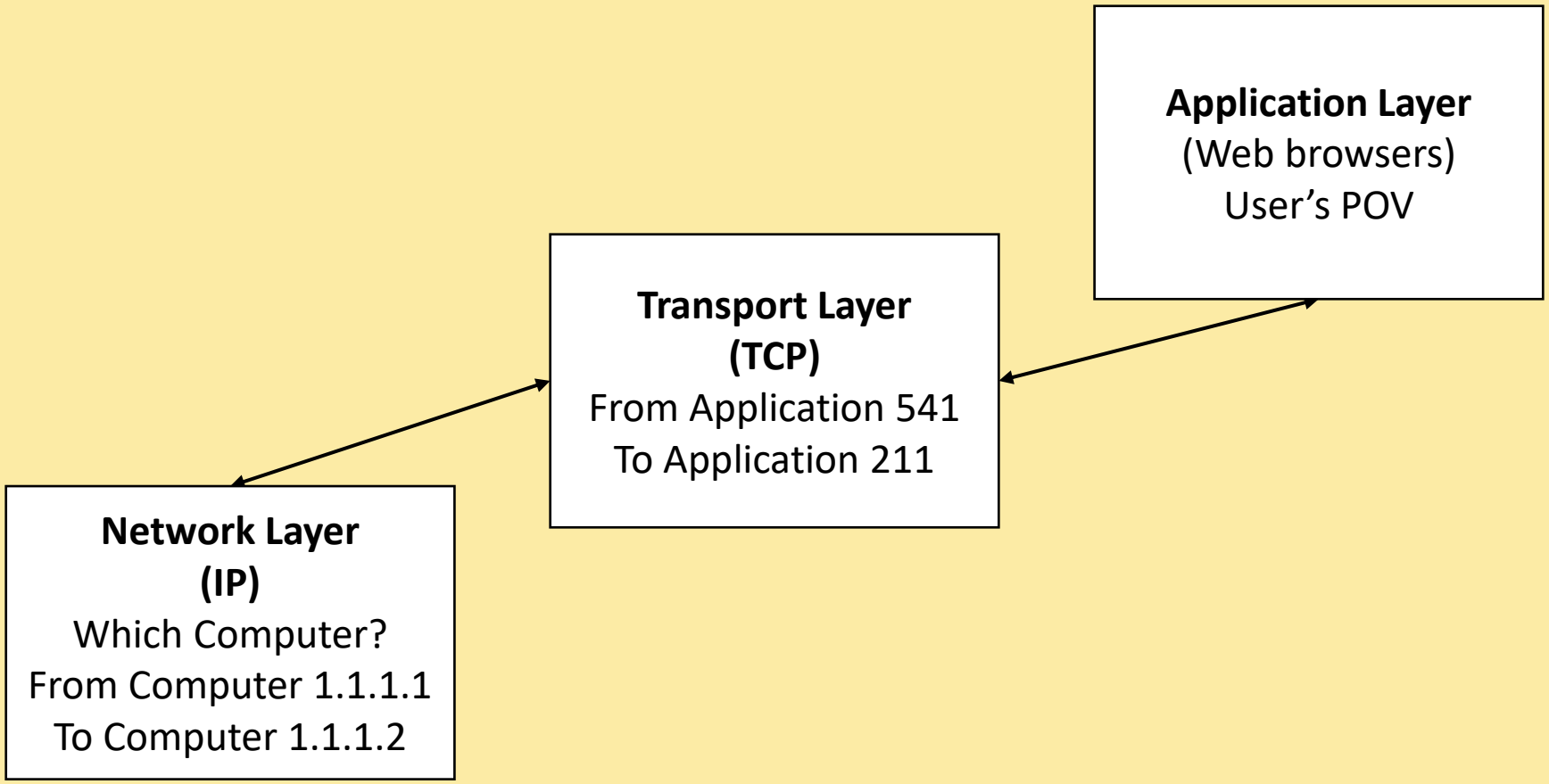
December 1, 2024

About Me

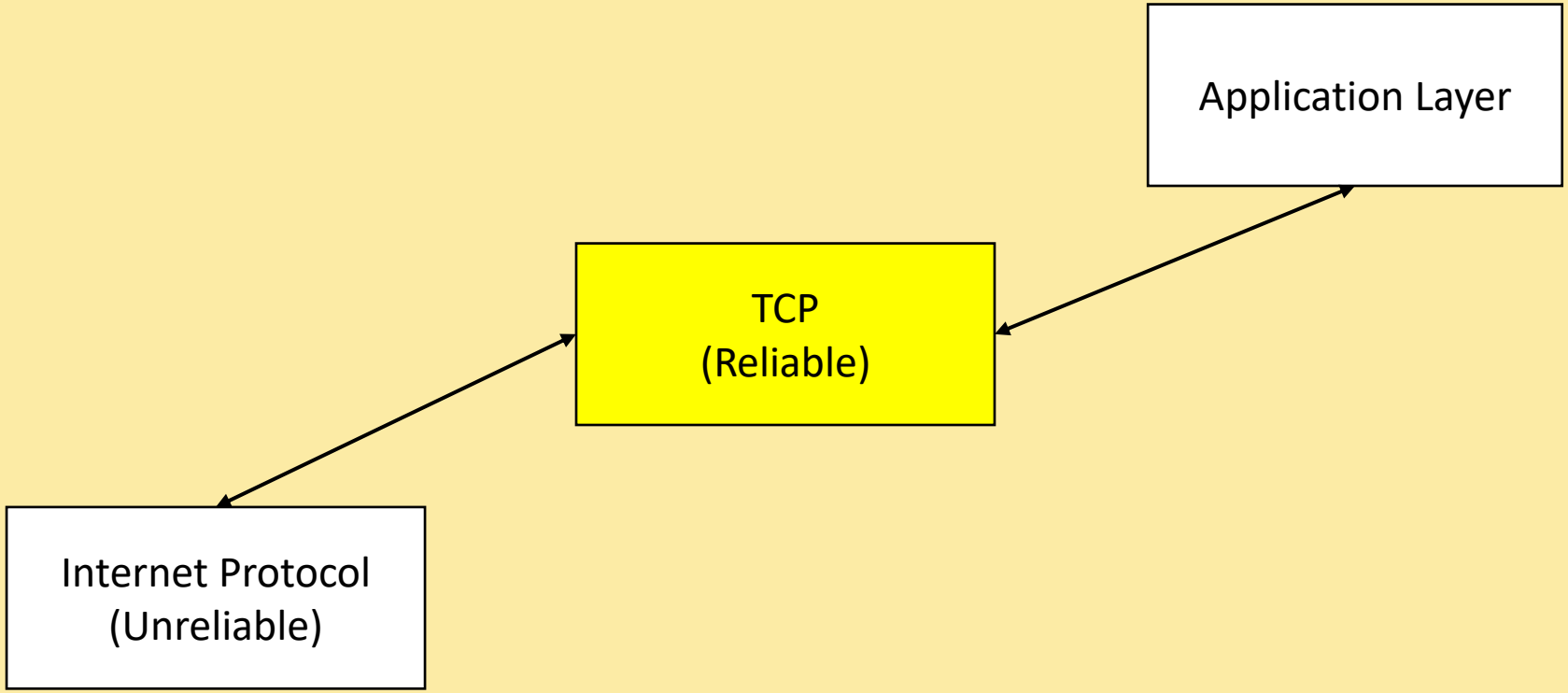
- Linux and Network Deep Diver
- Github: github.com/AliGhaffarian

Table of contents

Transport Layer in TCP/IP Stack



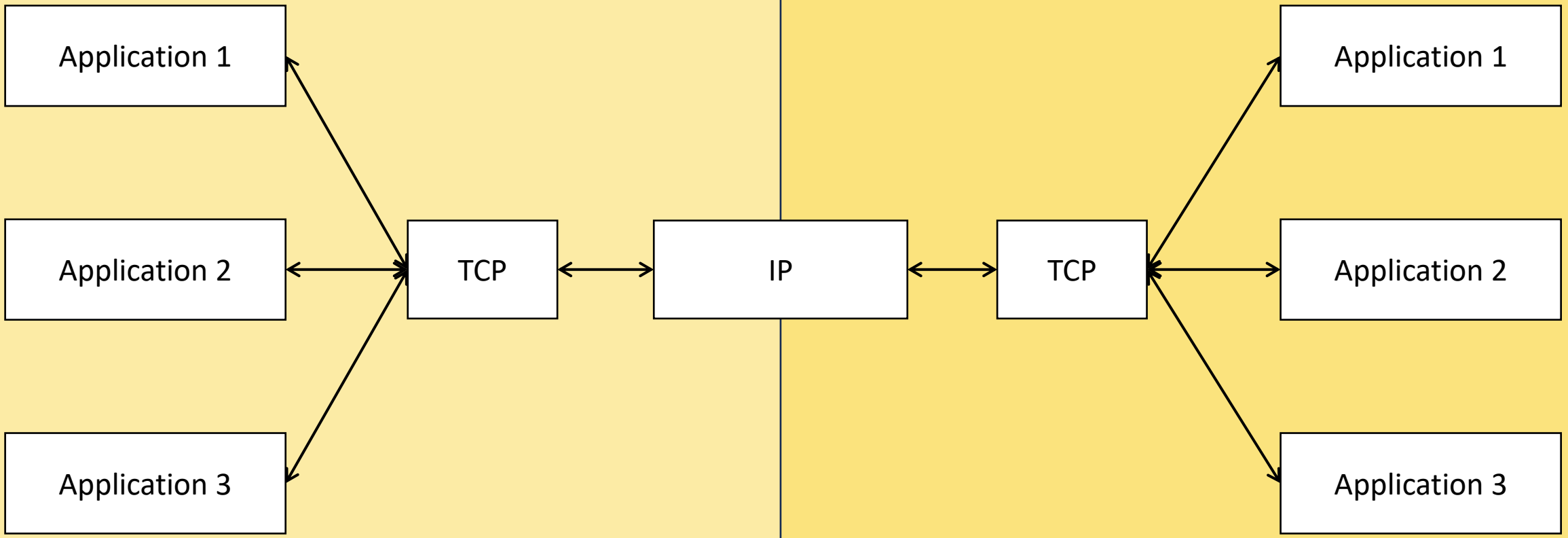
TCP


Application Layer
TCP
(Reliable)
Internet Protocol
(Unreliable)

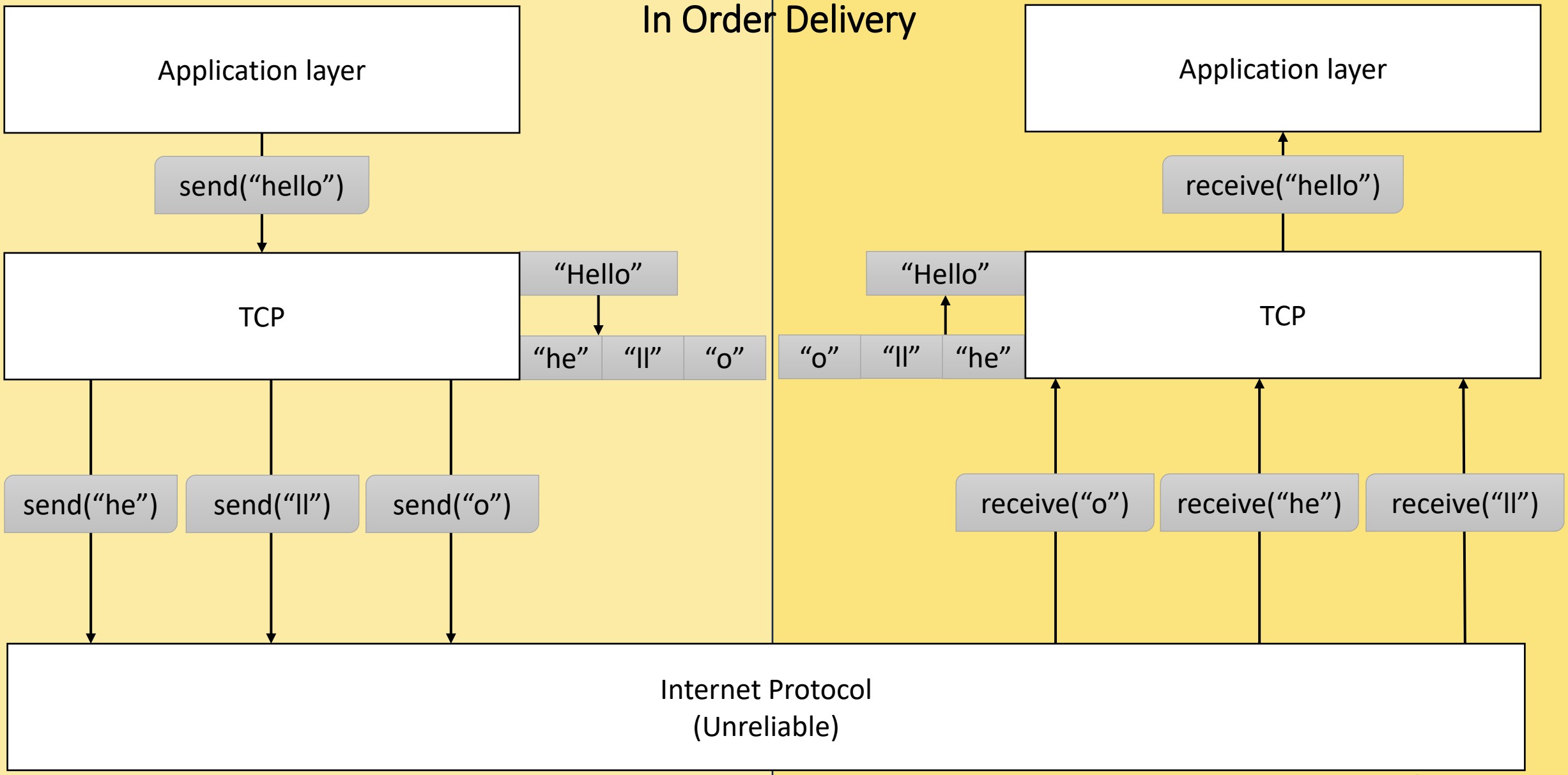
TCP’s Fields

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

Multiplexing / Demultiplexing



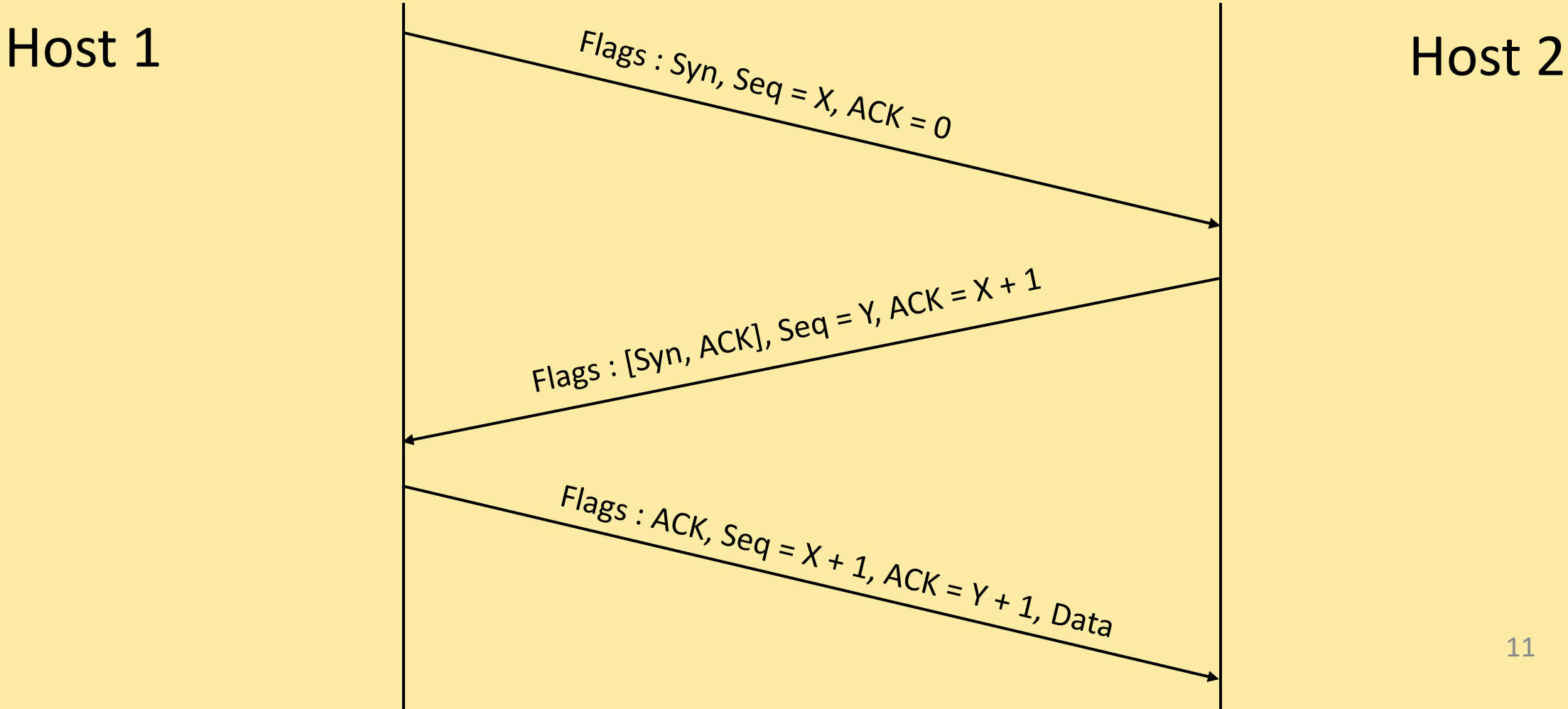
In Order Delivery



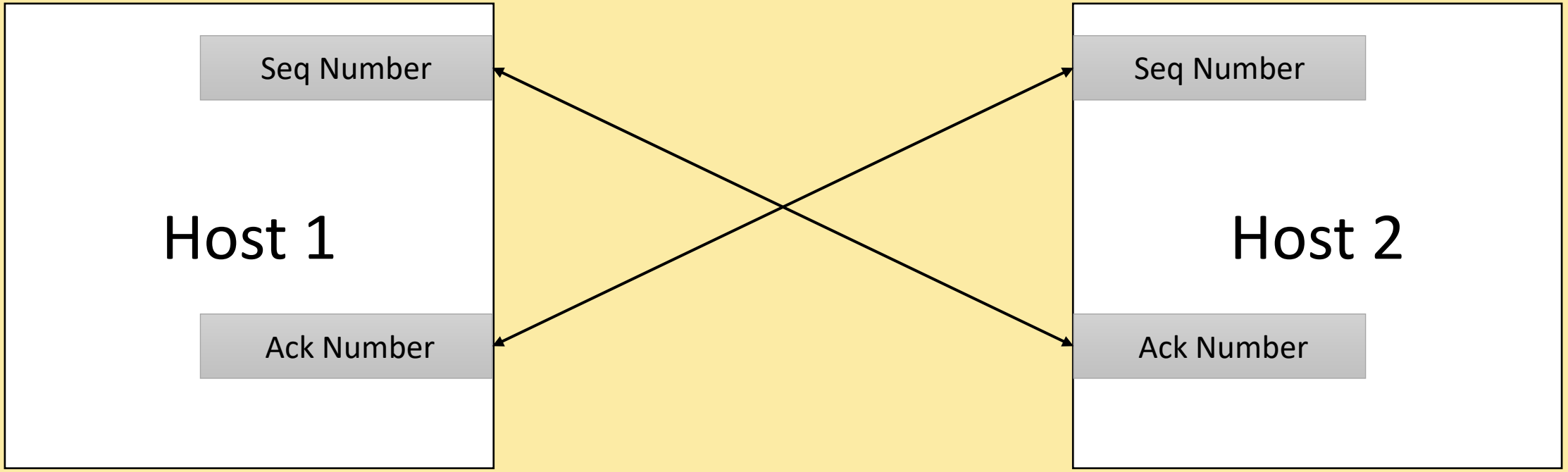
TCP Flags

```
000. .... .... = Reserved
...0 .... .... = Accurate ECN
.... 0... .... = Congestion Window Reduced
.... .0.. .... = ECN-Echo
.... ..0. .... = Urgent
.... ...0 .... = Ack
.... .... 0... = Push
.... .... .0.. = Reset
.... .... ..0. = Syn
.... .... ...0 = Fin
```

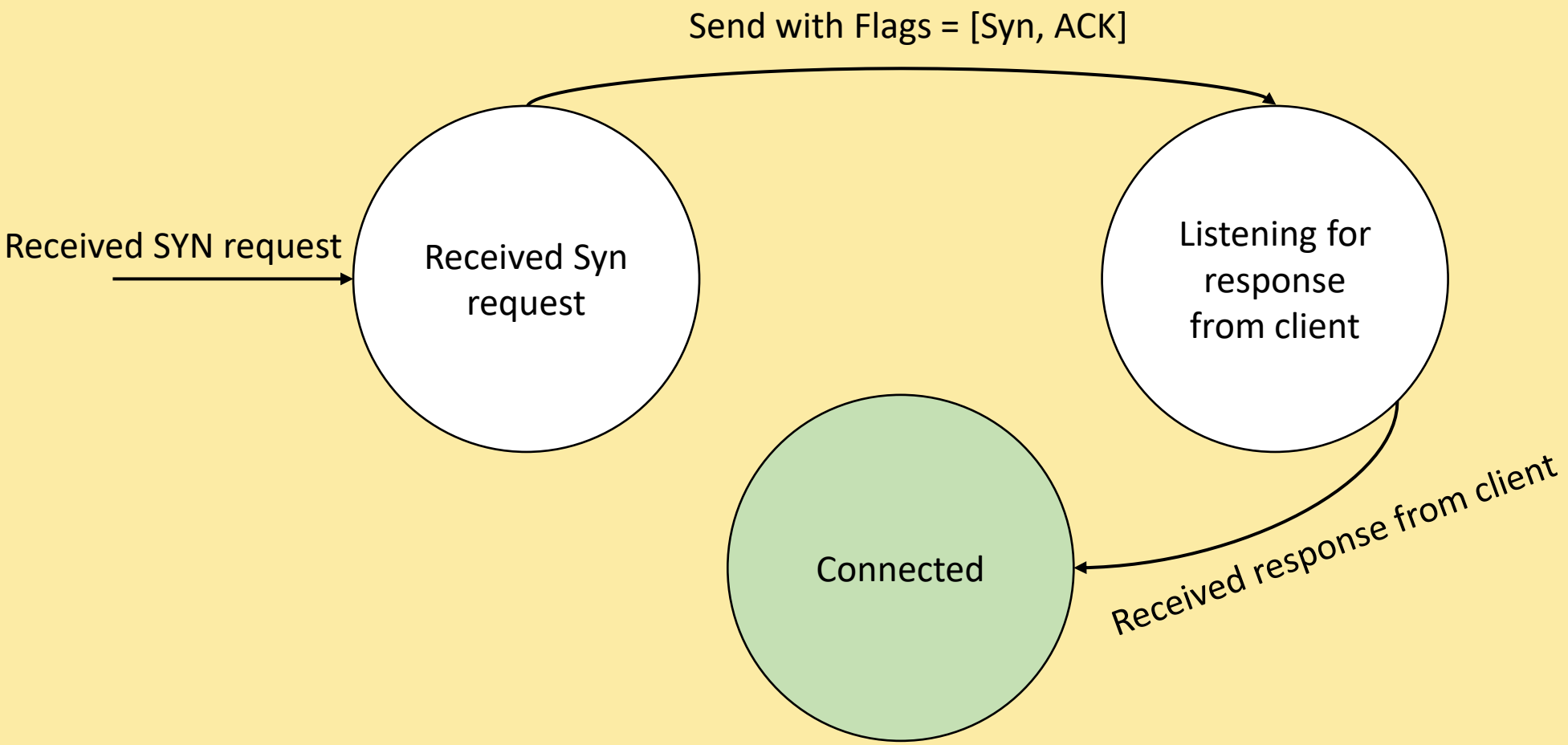
The Tree Way Handshake



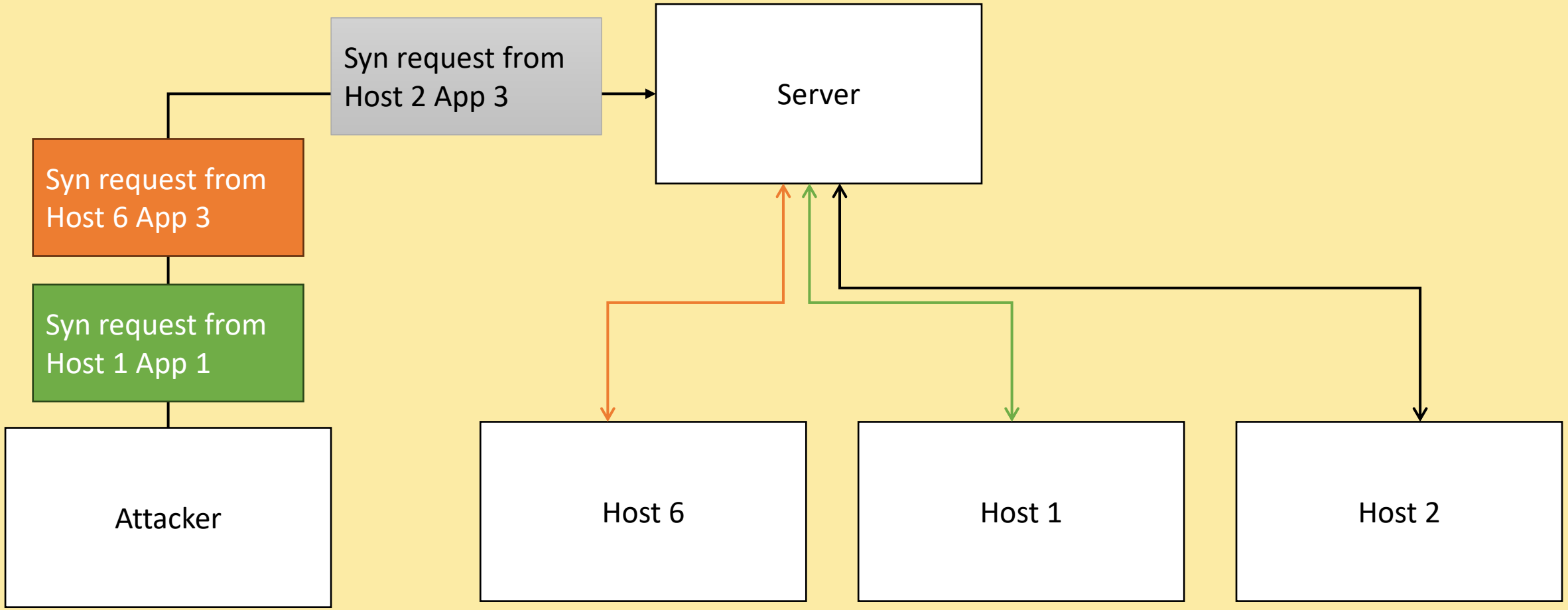
Sequence And Acknowledgement Number



State Machine of a TCP Server



SYN Floods


Syn request from
Host 2 App 3
Server
Syn request from
Host 6 App 3
Syn request from
Host 1 App 1
Attacker
Host 6
Host 1
Host 2

SYN Flooding is Cheap

Always Waiting on Non-Existing Clients

Request Queue (Backlog)							
Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request

Solution

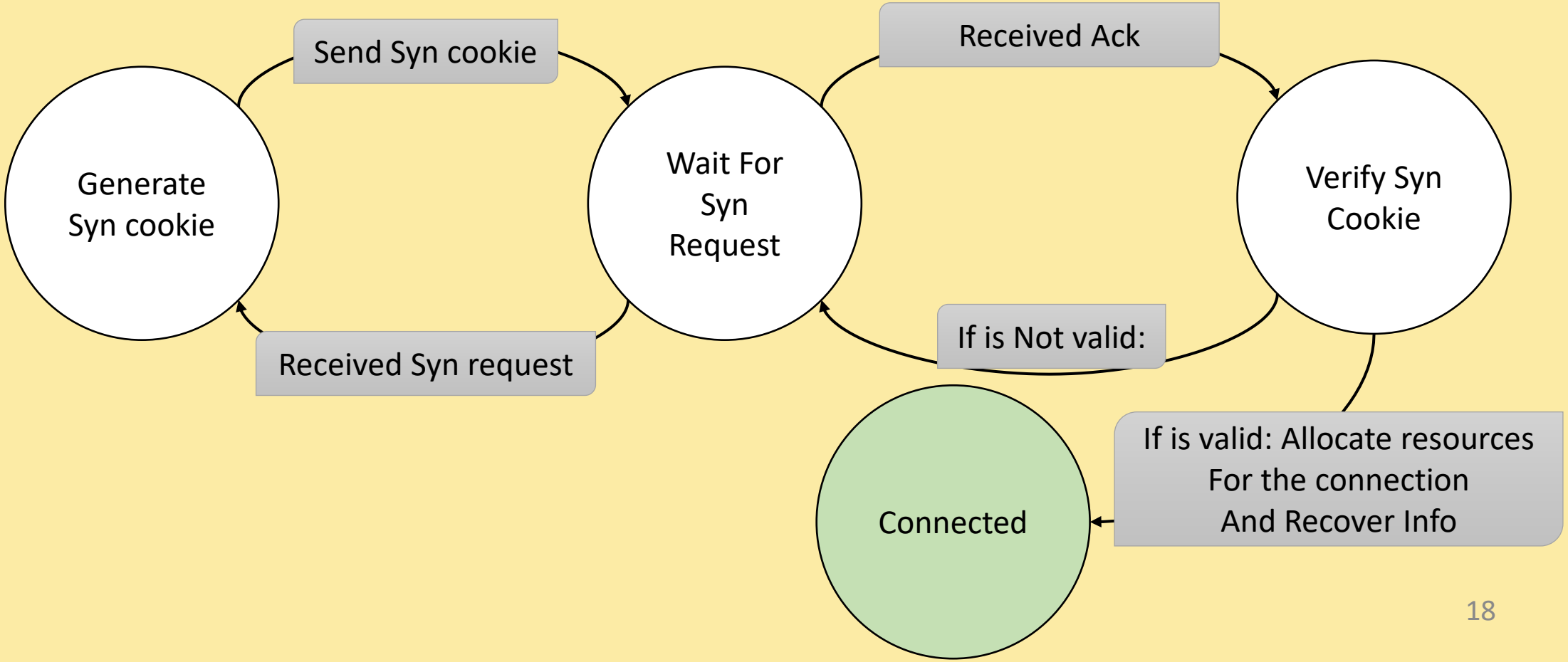
Break the Protocol?

Syn Cookies

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

How is it Done?

Forget the Connection But Not Really



Information to Recover

- Server’s IP Address
- Client’s IP Address
- Server’s Sequence Number
- Client’s Sequence Number
- Server’s Port
- Client’s Port
- TCP Options (Optional but Important)

Why Encoding Stuff?

- Preventing Against Connection Spoofing
- Being Flooded with Acks

Benefits and Drawbacks of Syn Cookies

- Higher Cost of Syn floods
- Lower Memory Usage
- No Direct Support For TCP Options
- Higher CPU Usage
- Complexity

Learn More

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