Transport Layer, TCP and Floods

Ali Ghaffarian

December 1, 2024

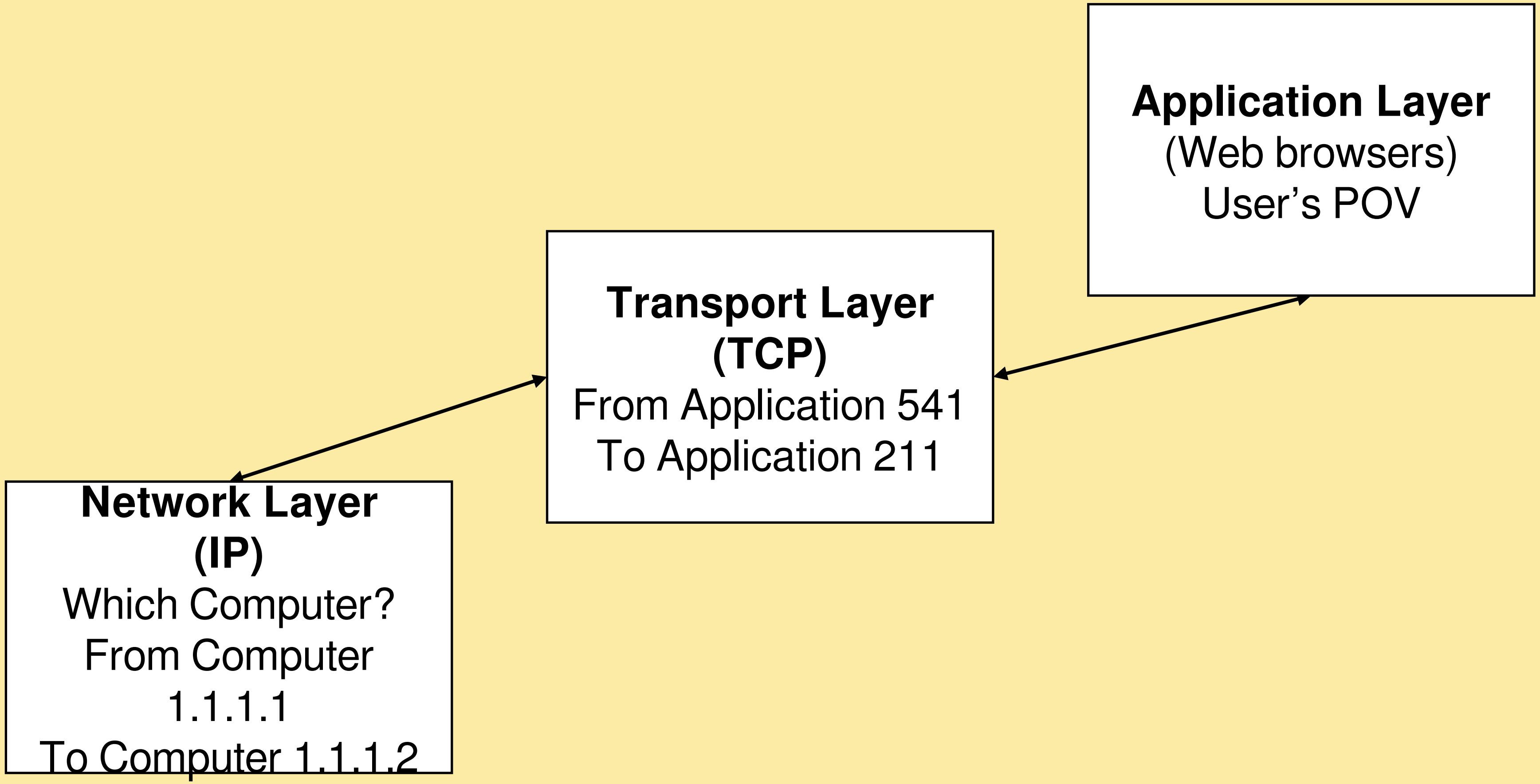
About Me

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

Table of contents

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

Transport Layer in TCP/IP Stack

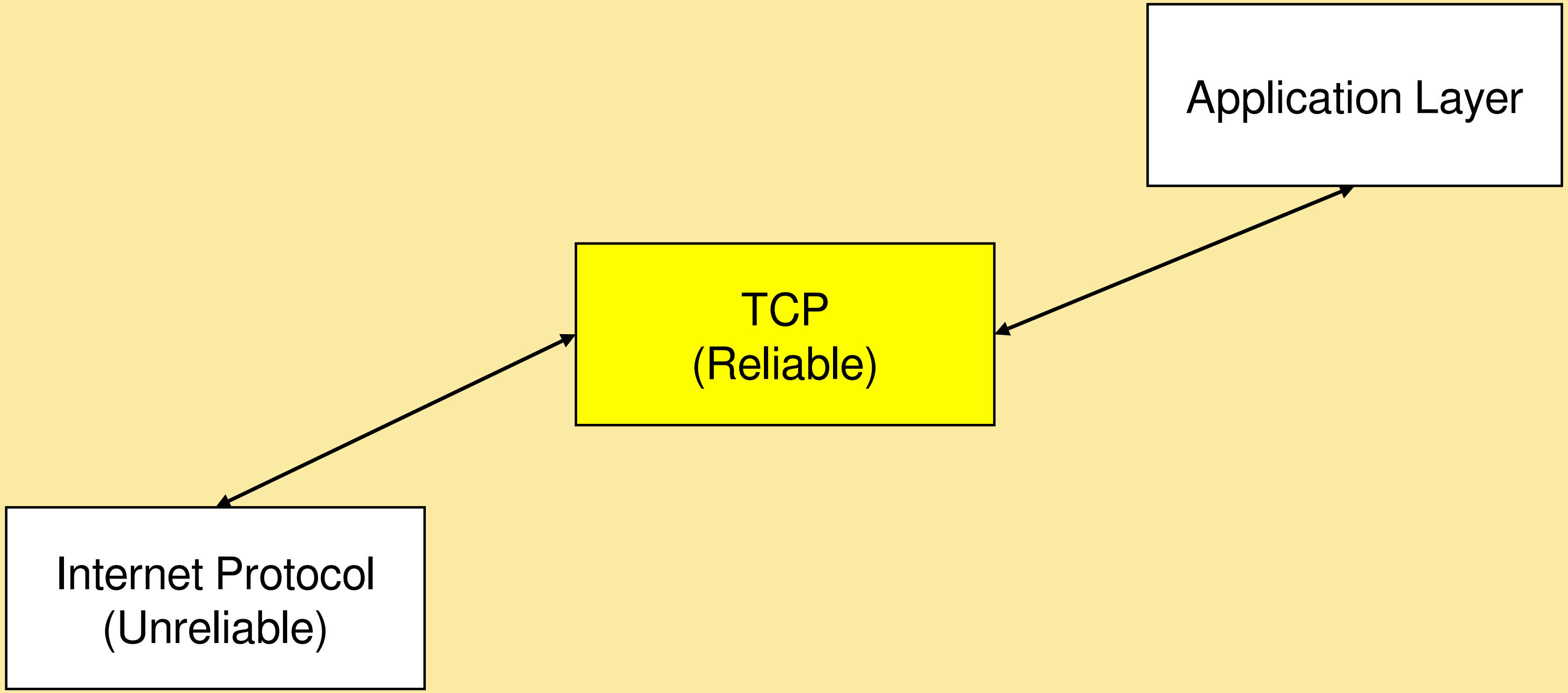


Application Layer
(Web browsers)
User's POV

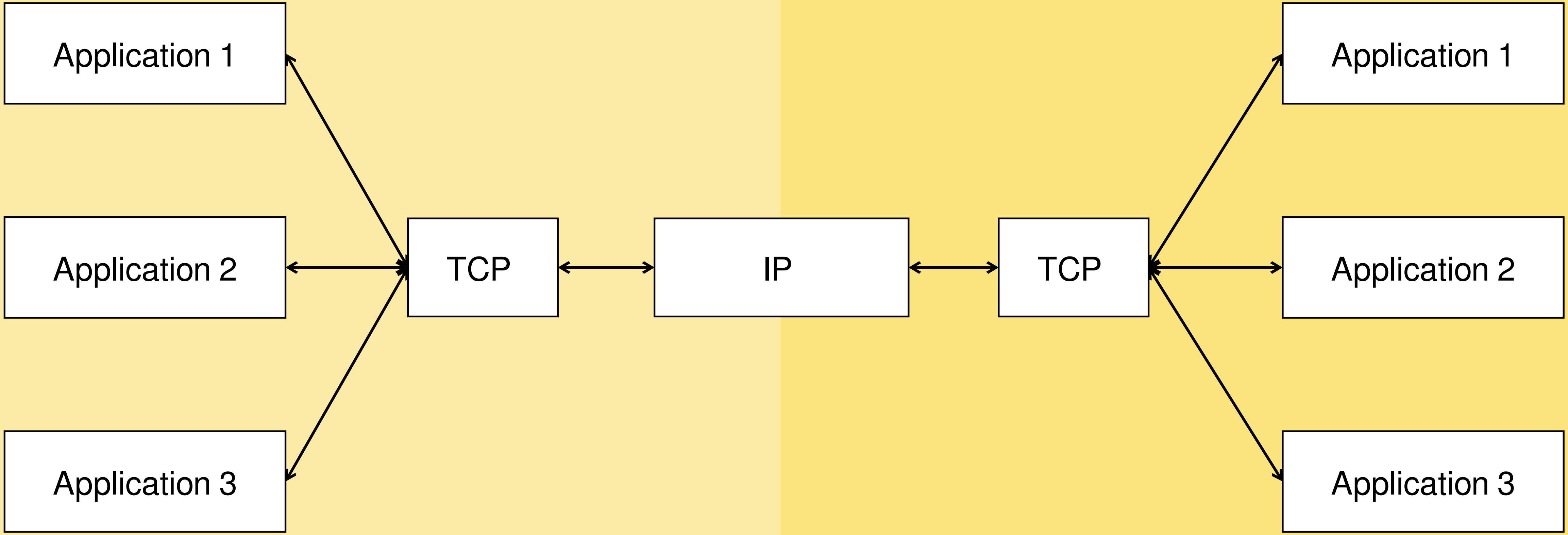
Transport Layer (TCP)
From Application 541
To Application 211

Network Layer (IP)
Which Computer?
From Computer 1.1.1.1
To Computer 1.1.1.2

TCP


Application Layer
TCP
(Reliable)
Internet Protocol
(Unreliable)

Multiplexing / Demultiplexing

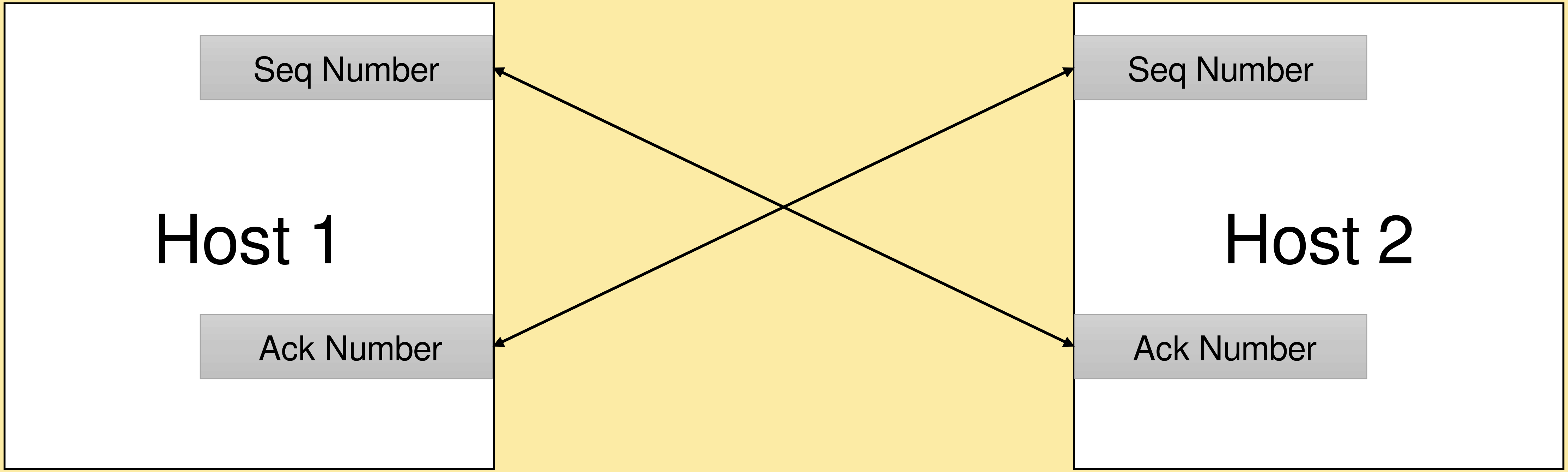


In Order Delivery

TCP’s Fields

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

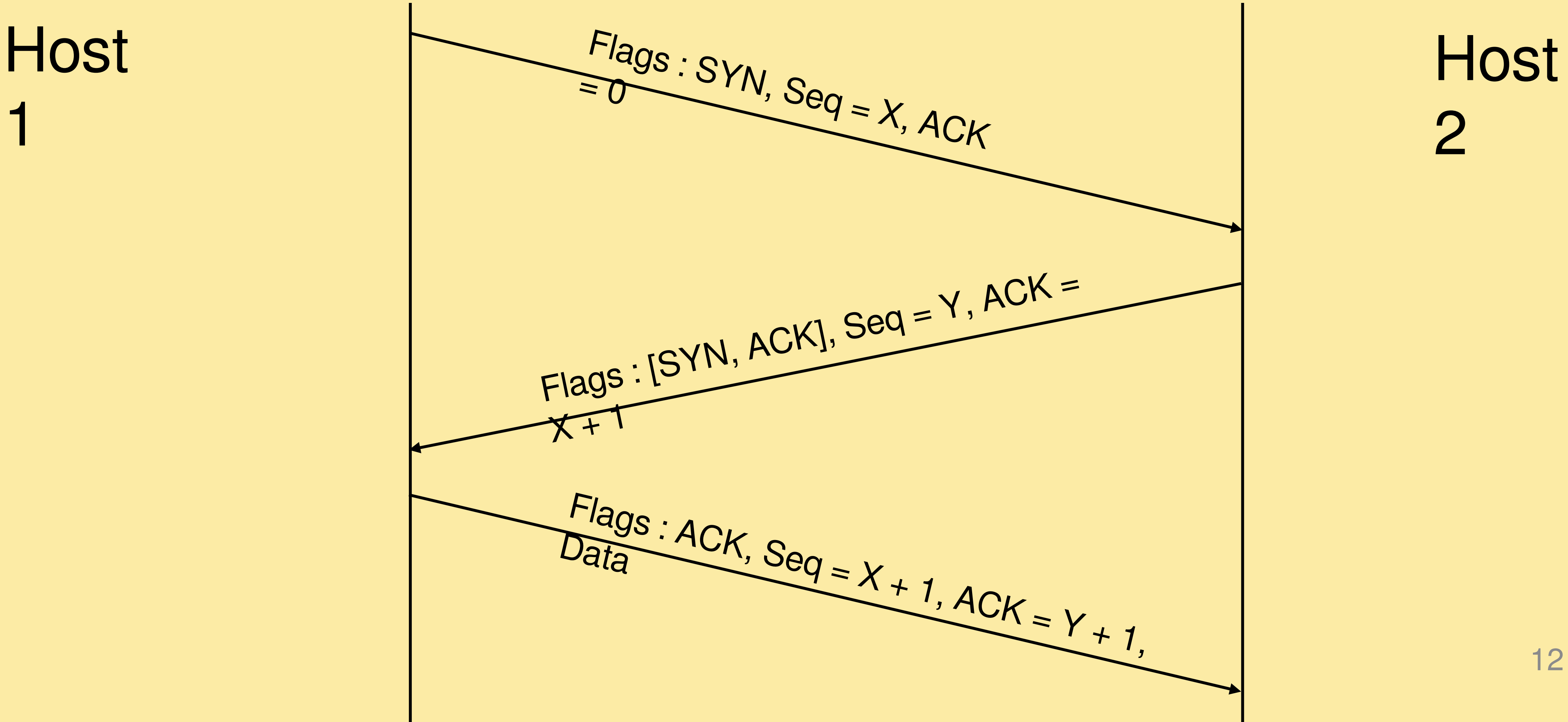
Sequence And Acknowledgement Number



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 Three Way Handshake



Host 1

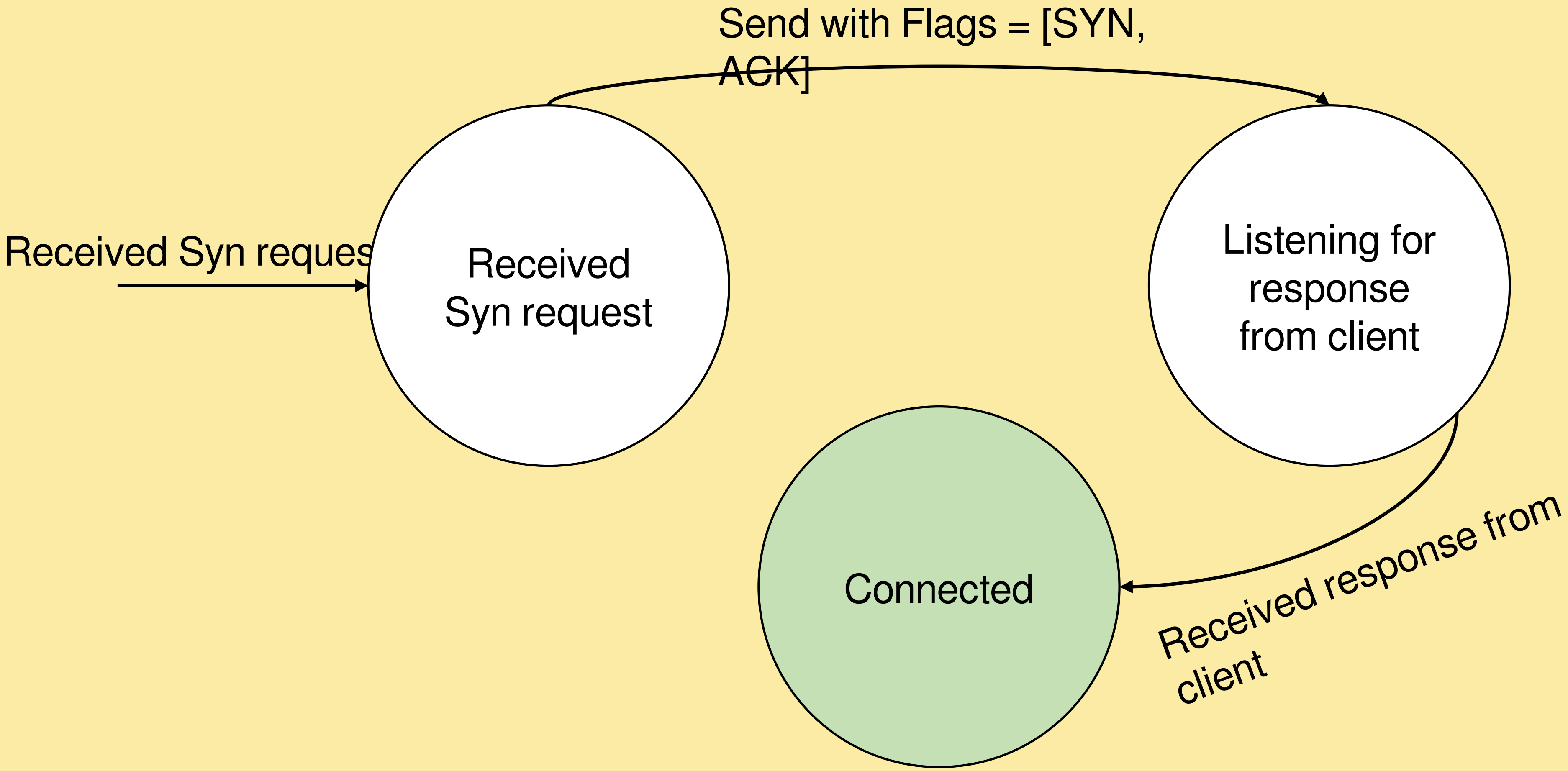
Host 2

Flags : SYN, Seq = X, ACK = 0

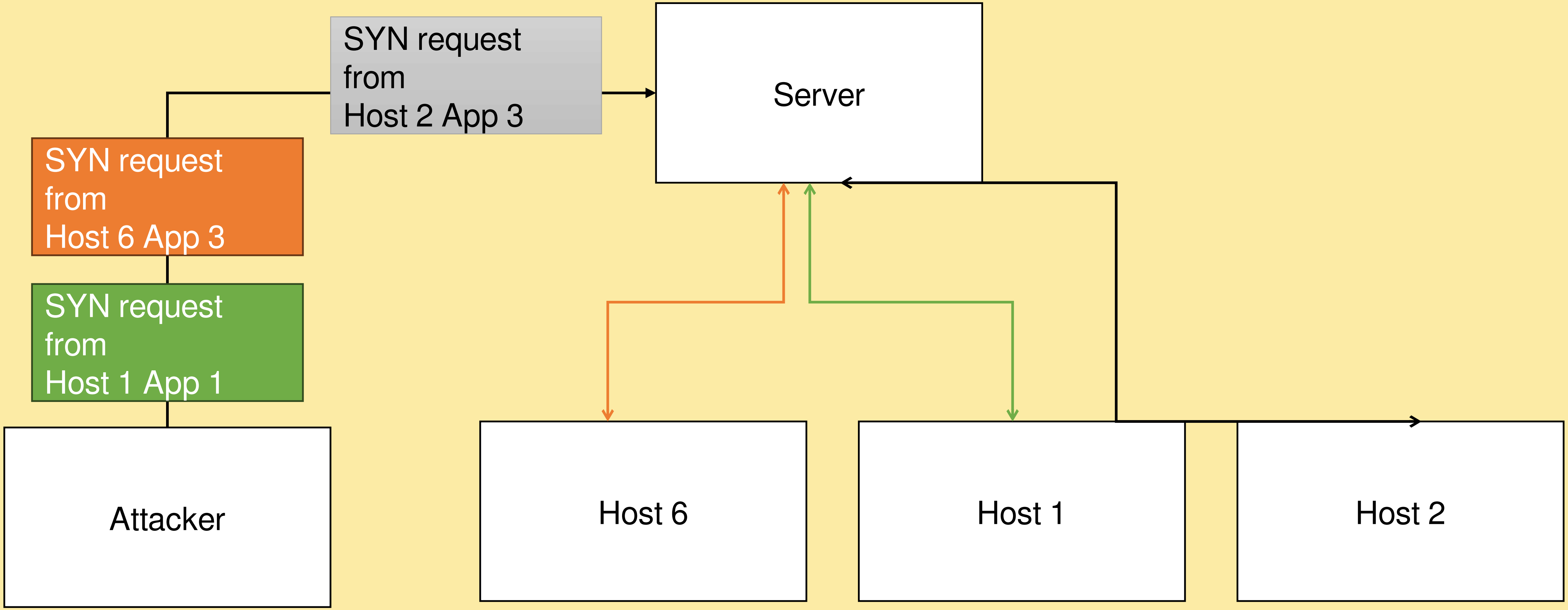
Flags : [SYN, ACK], Seq = Y, ACK = X + 1

Flags : ACK, Seq = X + 1, ACK = Y + 1, Data

State Machine of a TCP Server

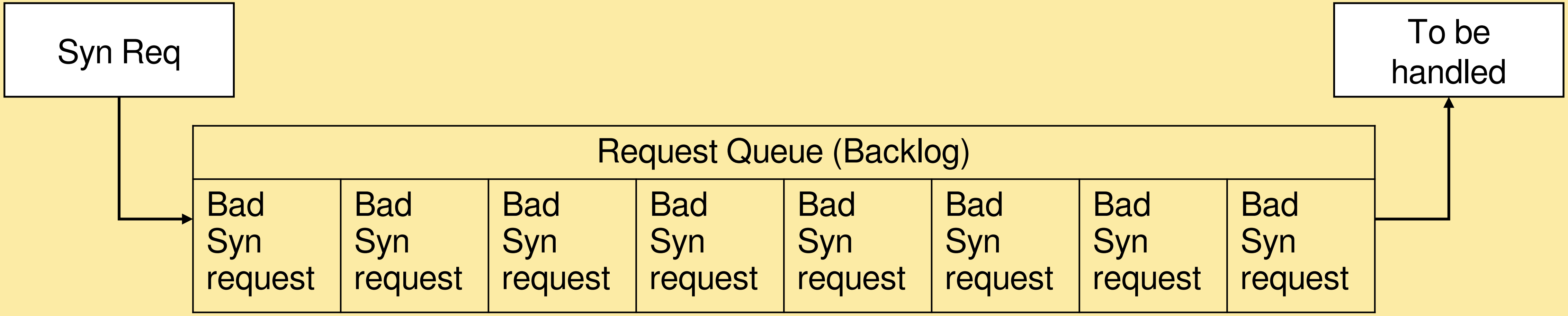

Send with Flags = [SYN, ACK]
Received Syn request
Received Syn request
Listening for response from client
Connected
Received response from client

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



Syn Req

To be handled

Request Queue (Backlog)

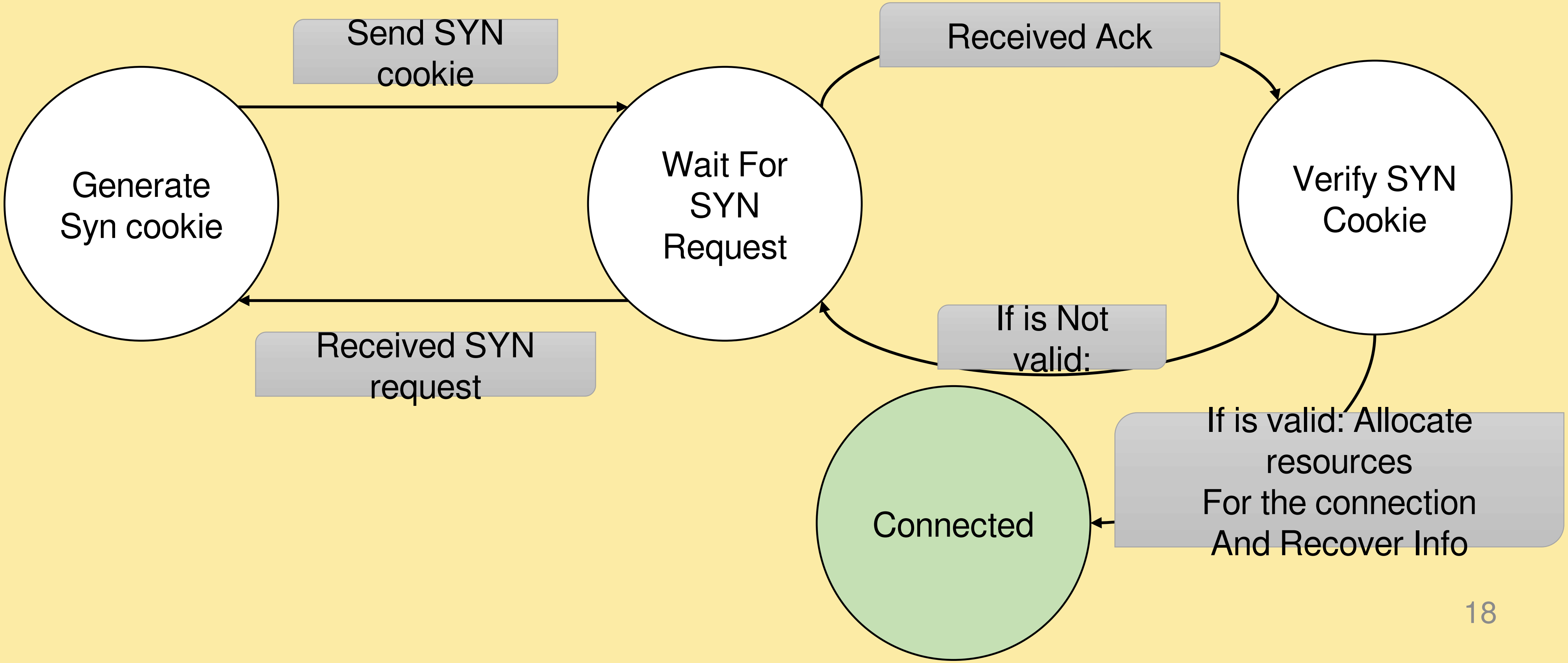
Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request	Bad Syn request

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 and Client’s IP Address
- Server and Client’s Sequence Number
- Server and Client’s Port
- Server and Client Maximum Segment Size (MSS)
- 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`

Questions

Presentation Files:
github.com/AliGhaffarian/university_thingies