SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

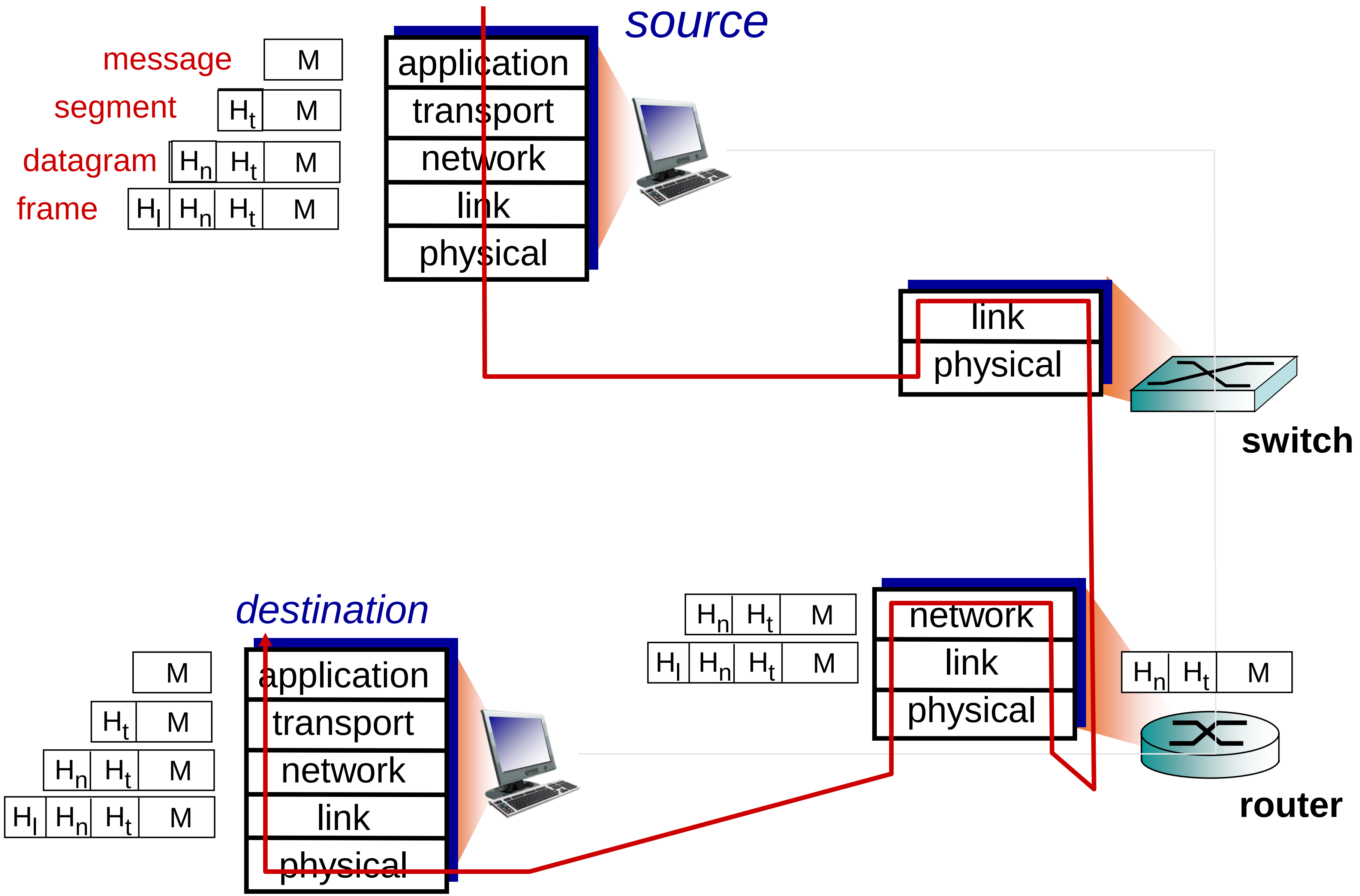
CMPT 479/980: Systems and Network Security

Spring 2020

TCP/IP Attacks

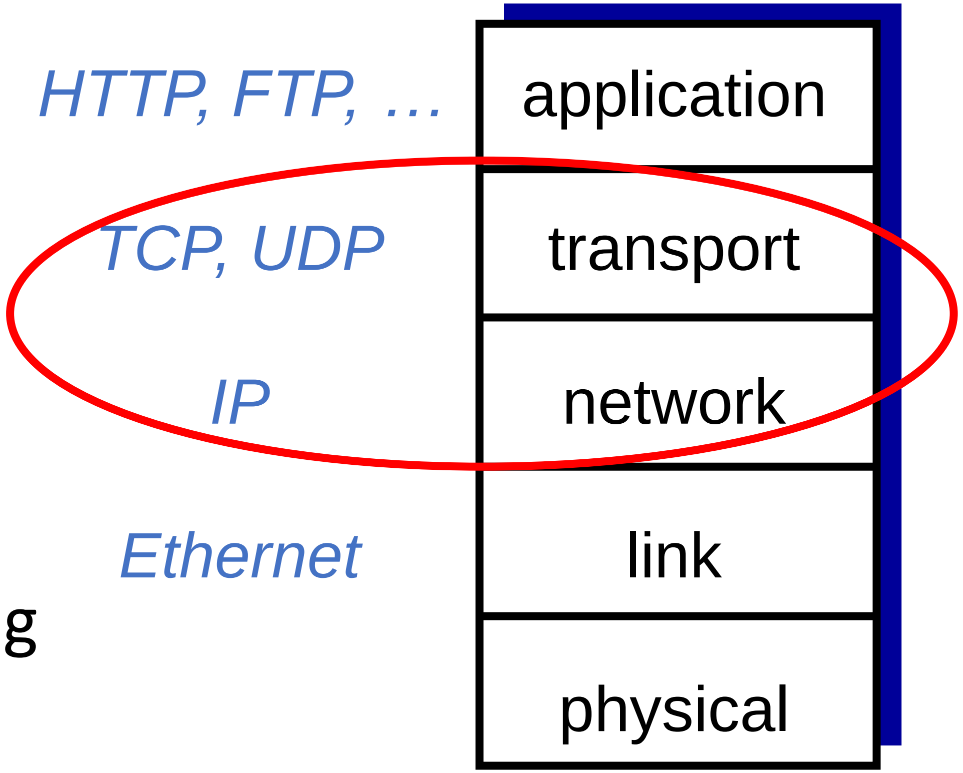
Instructor: Khaled Diab

Recall: Encapsulation



Recall: TCP/IP Protocol Suite

- *application:* supporting network applications
  - FTP, SMTP, HTTP
- *transport:* process-to-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits “on the wire”



Outline

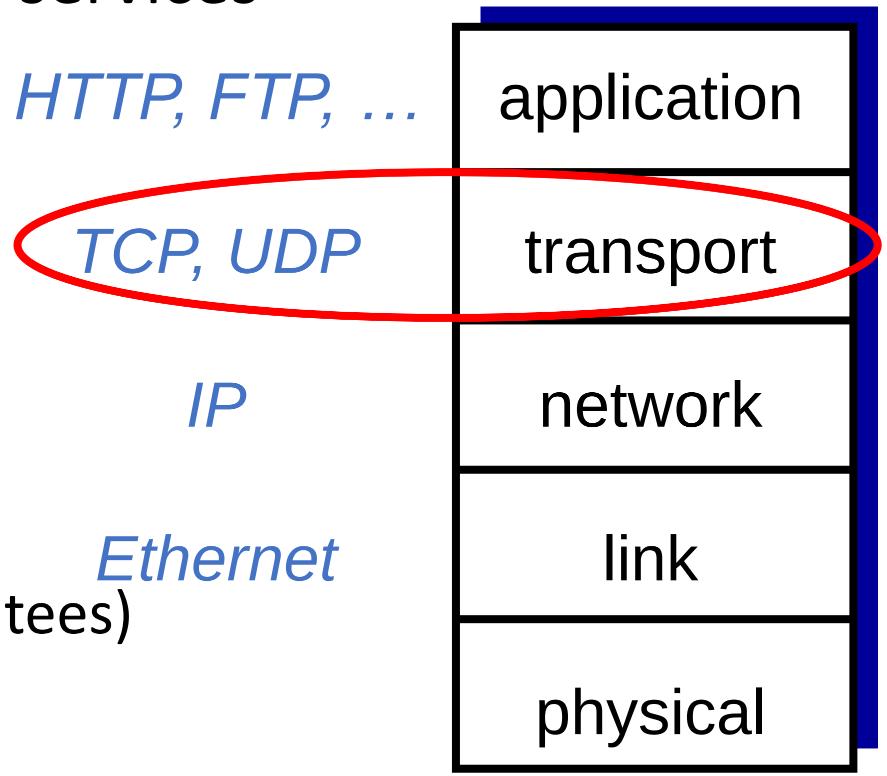
- How TCP works
- Attacks on TCP protocol:
  - SYN Flooding
  - TCP Reset
  - TCP Session Hijacking
  - TCP Sequence Number Prediction
- Attacks on IP protocol:
  - Source Routing

Transmission Control Protocol

A quick review

Recall: Transport Layer

- Provides process-to-process communication services
- User Datagram Protocol (UDP)
  - No delivery guarantees
  - Connectionless protocol
  - Low overhead
- Transmission Control Protocol (TCP)
  - Reliable transmission (but no bandwidth guarantees)
  - Connection-oriented
  - More overheads



Functional Overview

Client

❶ Create a socket

`SOCK_STREAM`

❷ Set destination info.

IP and port number

❸ Connect to the server

Logical and unique connection.

3-way handshake

❹ Send/Receive data

e.g., `write` and `read`

❺ Close the connection

Server

❶ Create two sockets

Listening and connection

❷ Bind to a port number

❸ Listen for connections

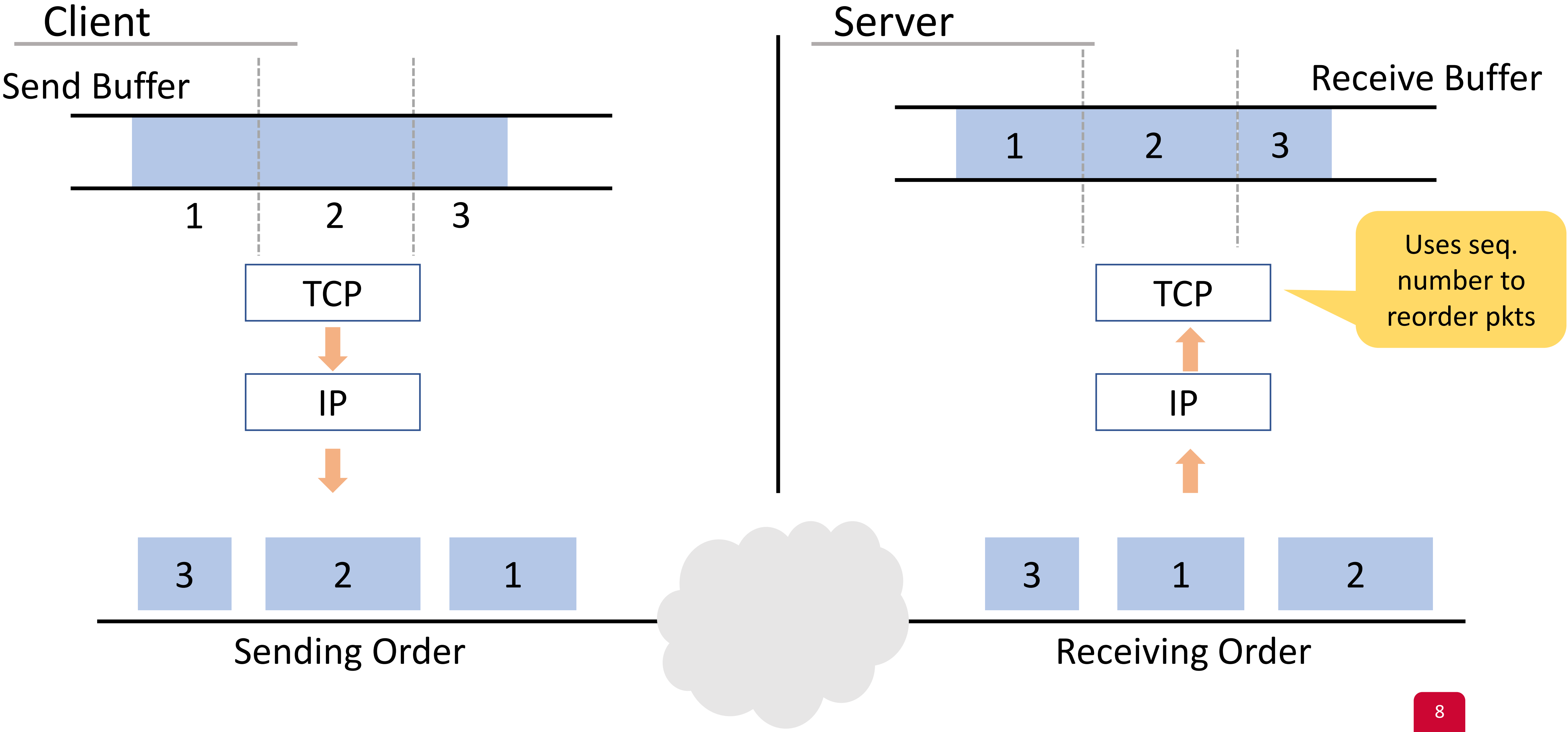
App is ready for receiving connection requests

❹ Accept a connection

Extracts the first connection request from the queue

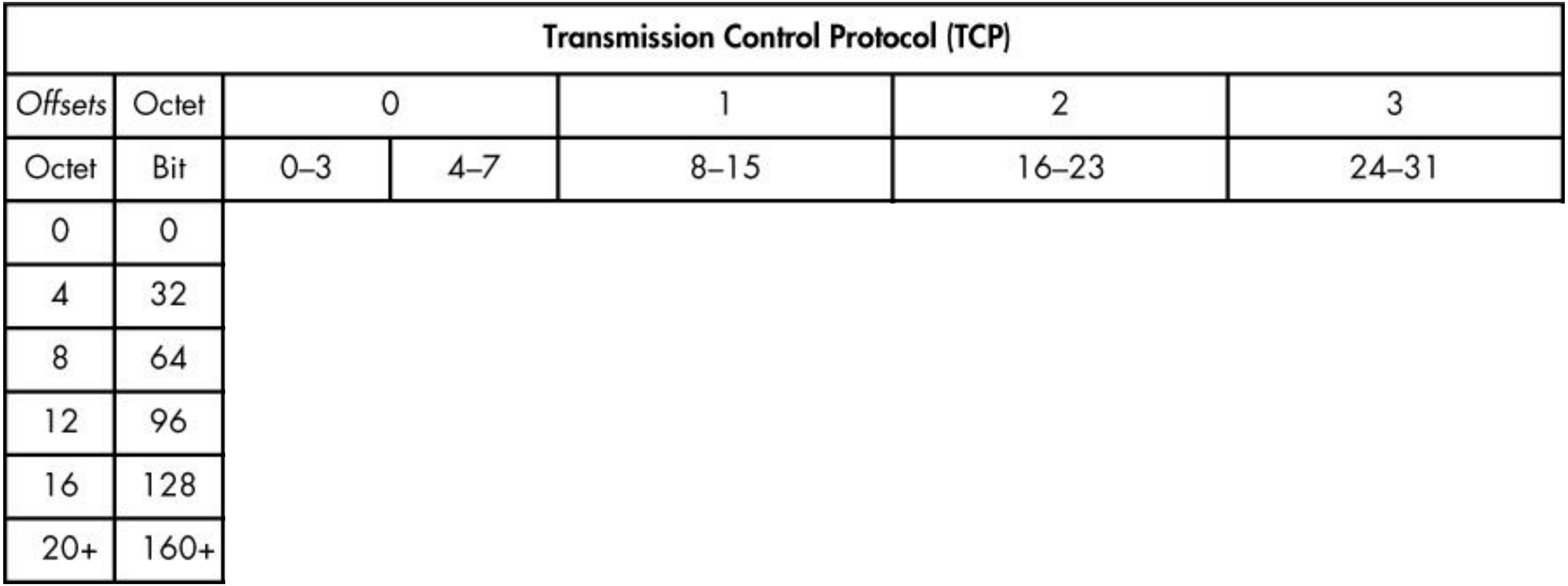
❺ Send/Receive data

Data Transmission



Uses seq. number to reorder pkts

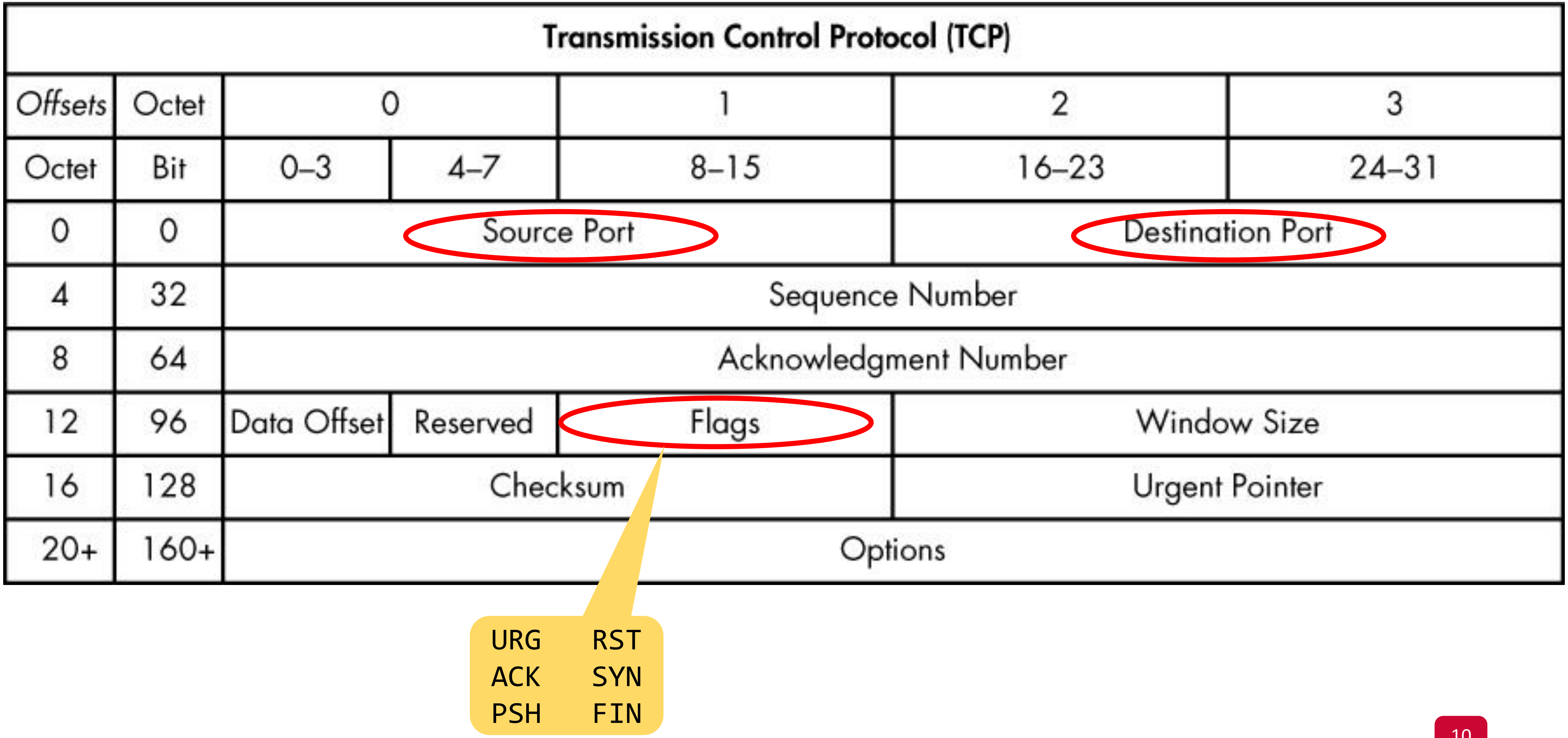
TCP Packet Diagram



Transmission Control Protocol (TCP)

Offsets	Octet	0		1	2	3
Octet	Bit	0–3	4–7	8–15	16–23	24–31
0	0					
4	32					
8	64					
12	96					
16	128					
20+	160+					

TCP Packet Diagram



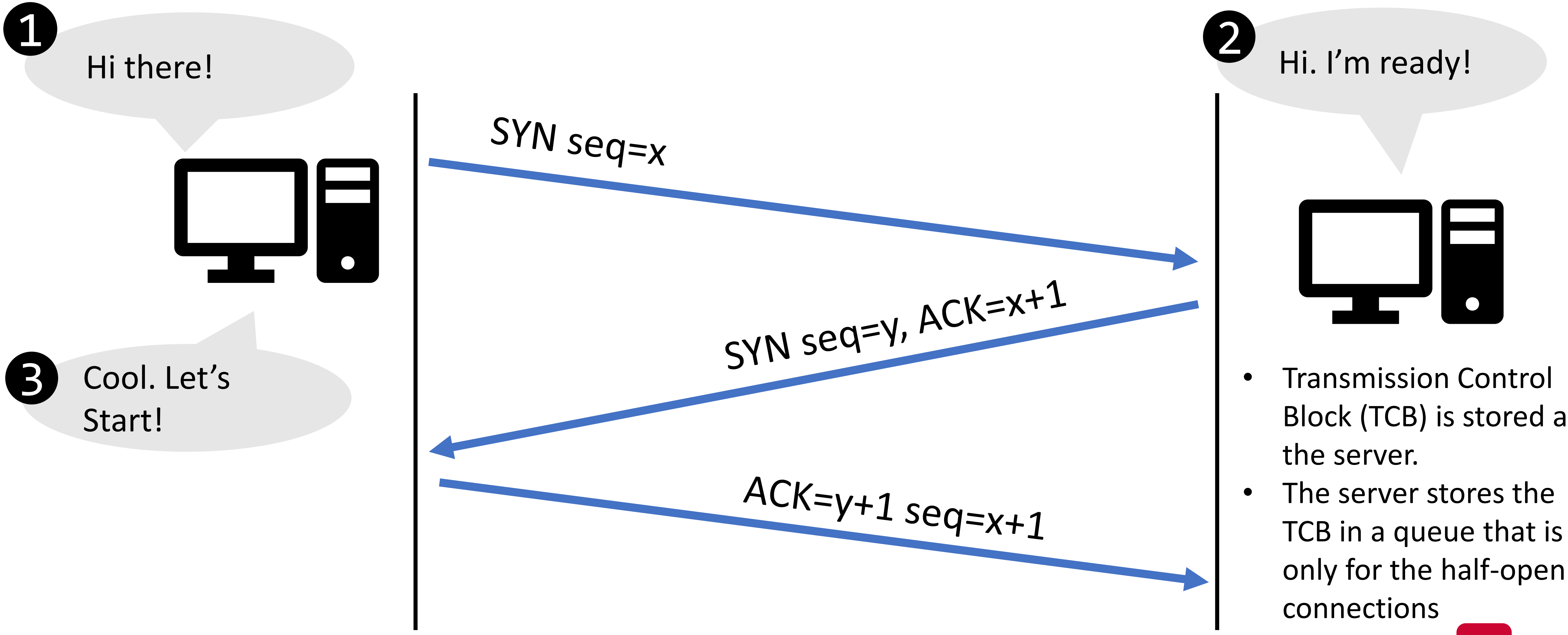
Transmission Control Protocol (TCP)						
Offsets	Octet	0		1	2	3
Octet	Bit	0–3	4–7	8–15	16–23	24–31
0	0	Source Port			Destination Port	
4	32	Sequence Number				
8	64	Acknowledgment Number				
12	96	Data Offset	Reserved	Flags	Window Size	
16	128	Checksum			Urgent Pointer	
20+	160+	Options				

URG RST
ACK SYN
PSH FIN

SYN Flooding

Recall: TCP Connection Establishment

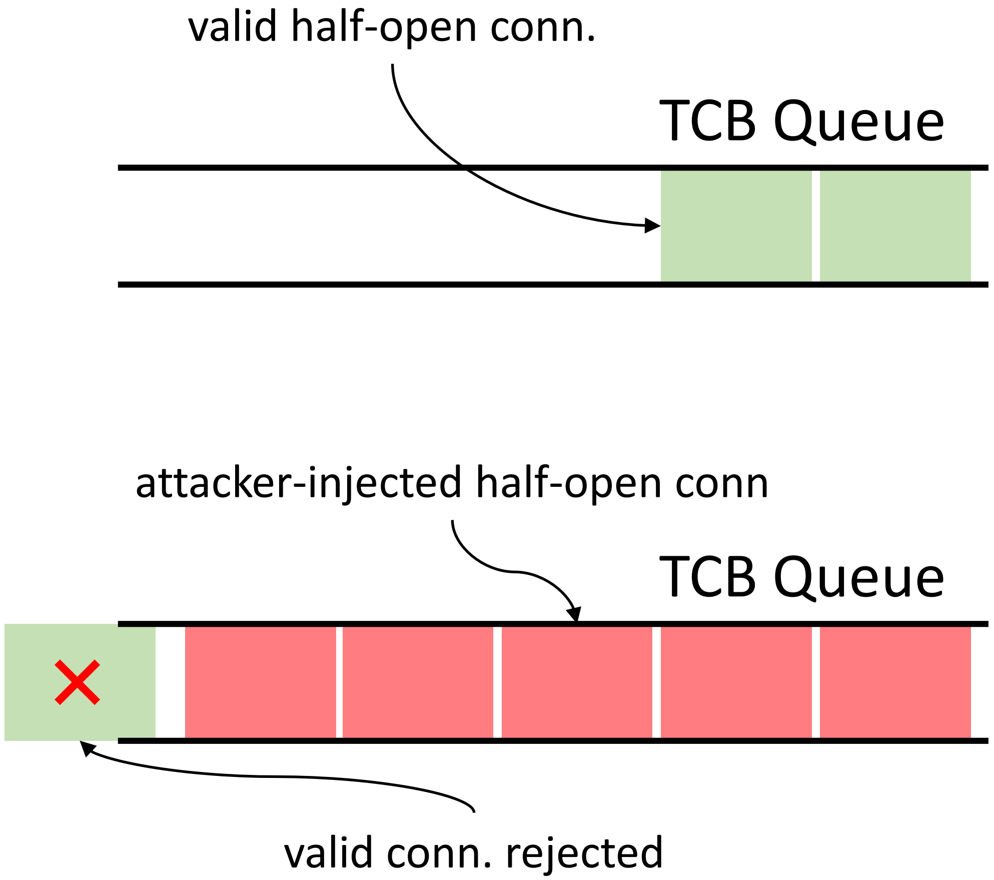
- Any TCP connection starts with a three-way handshake.



- Transmission Control Block (TCB) is stored at the server.
- The server stores the TCB in a queue that is only for the half-open connections

TCP SYN Flooding

- A denial-of-service attack
- The TCP server stores all the half-open connections in a queue
  - Before the three-way handshake is done
  - Recall: the queue has a limited capacity
  - What happens when the queue is full?
- The attacker attempts to fill up the TCB queue quickly
  - No more space for new TCP connections
- The server will reject new SYN packets
- The CPU may have not reached its capacity!



TCP SYN Flooding

- The attacker need to perform two steps:
  - Send a lot of SYN packets to the server (i.e., flooding)
  - Do not finish the third step of the three-way handshake protocol

- How does the attacker set the source IP address?
- Attacker needs to use random source IP addresses
  - Why?
- SYN-ACK packets may be:
  - Dropped in transit
  - Received by a real machine

Next Lecture

- SYN Flooding
- TCP Reset
- TCP Session Hijacking
- TCP Sequence Number Prediction
- Source Routing Attacks