Redes de Computadores II

Universidade do Algarve

Semana 8

https://github.com/ncatanoc/redes_algarve

Néstor Cataño

nestor.catano@gmail.com

TCP (Transfer Control Protocol)

Goal:

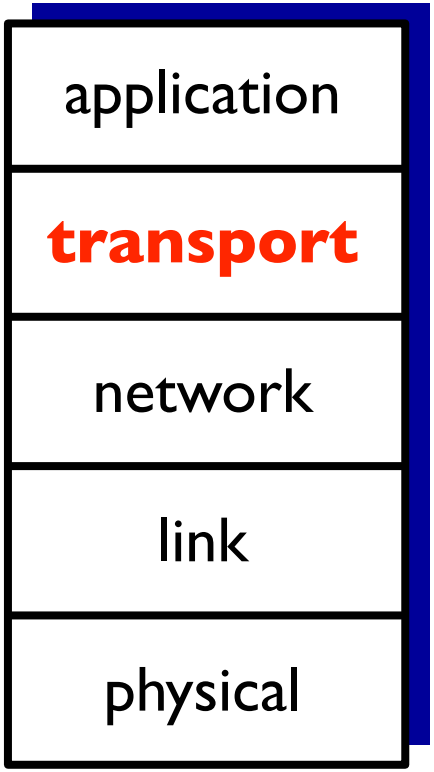
To understand the basic underpinnings of **TCP**, the transfer control protocol, and its relevance for network communications.

Roadmap

1. **TCP (Transfer Control Protocol)**
2. TCP security

TCP - transfer control protocol

- **TCP** fixes some issues related with UDP:
  - It is connection-oriented
  - It resends lost packets
  - It orders packets



the transfer control protocol

Why a new protocol?

- Messages constrained by packet size
- Out-of-order packet arrival
- Lost packets

How does TCP fix this?

- *Connections*: A connection must be established before sending any data.
- *Streaming*: An application can pass any amounts of data to the TCP layer, which will take care of packetization.
- *Reliability*: Packets are automatically ordered and retransmitted using sequence numbers.

the transfer control protocol - 2

What makes TCP reliable?

End-to-end principle: Transport issues are the responsibility of the endpoints.

Endpoints keep track of sequence numbers to order and retransmit packets when necessary.

Why do we even need UDP now?

- More lightweight.
- Speed $>$ reliability for some applications.

Quiz

Question

Check all application types where UDP is more suitable than TCP:

- ☐ Video chat
- ☐ On-demand video streaming
- ☐ Multiplayer first-person shooters
- ☐ Social media websites

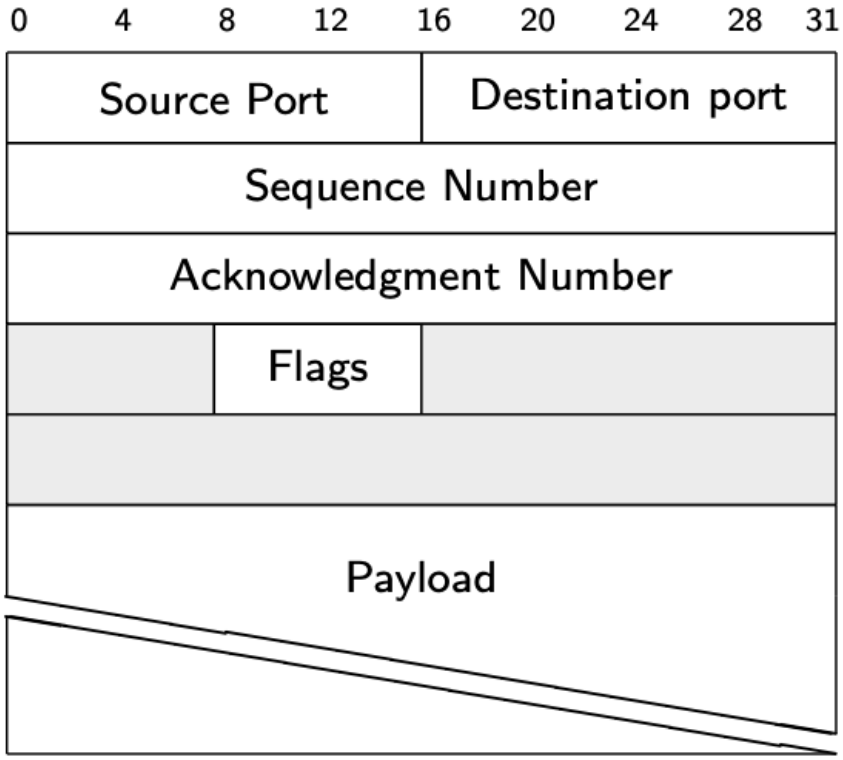
Quiz

Question

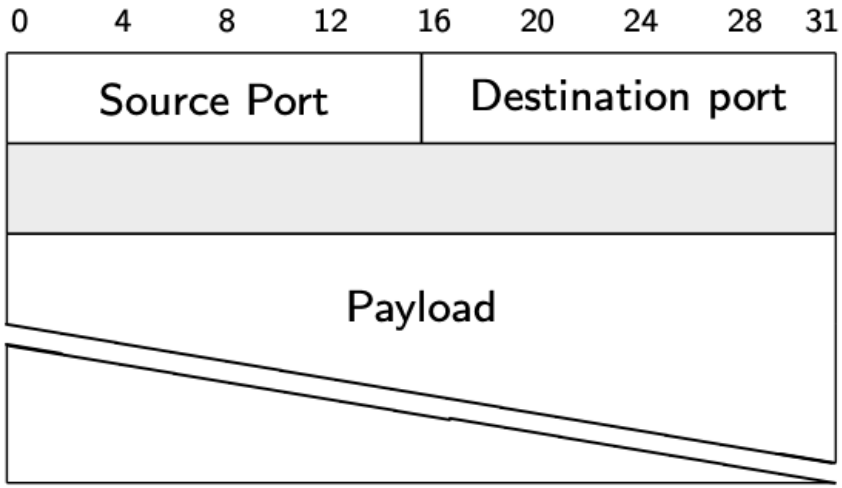
Check all application types where UDP is more suitable than TCP:

- [x] Video chat
- [ ] On-demand video streaming
- [x] Multiplayer first-person shooters
- [ ] Social media websites

TCP packet

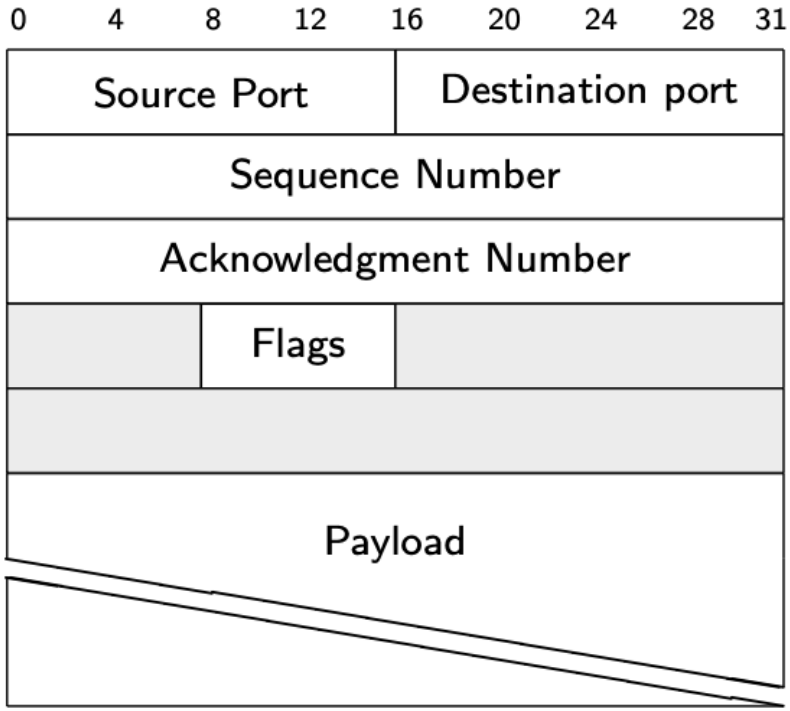


TCP Packet



UDP Packet

TCP packet



TCP Packet

Sequence Number

Position of packet contents in the overall stream.

Acknowledgment Number

Position up to which the stream has been completely received + 1; i.e., the next expected sequence number.

Flags

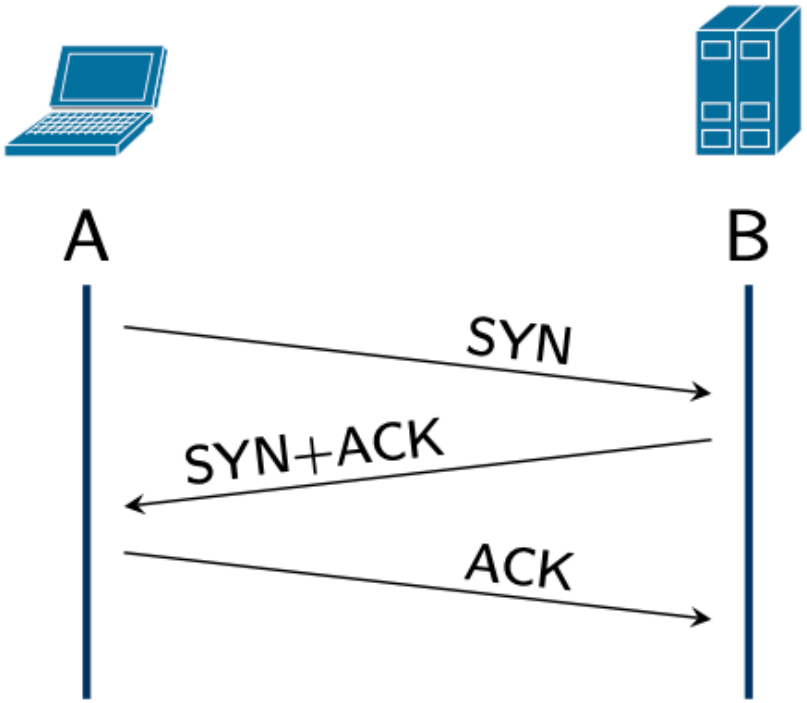
`SYN` Synchronize, i.e., initiate a new connection.

`ACK` Acknowledge receipt of previous packets. Set for all but the first packet.

`FIN` Finish, indicate no more data from sender.

`RST` Reset the connection.

TCP connection establishment



TCP three-way handshake

Quiz

Question

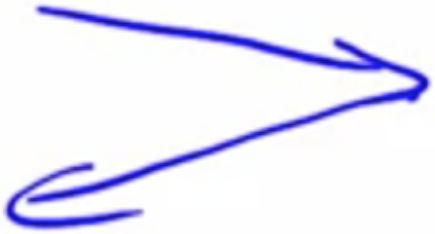
Assume sending a packet from A to B takes 100 ms.
How much time elapses until A can send data to B?

Answer

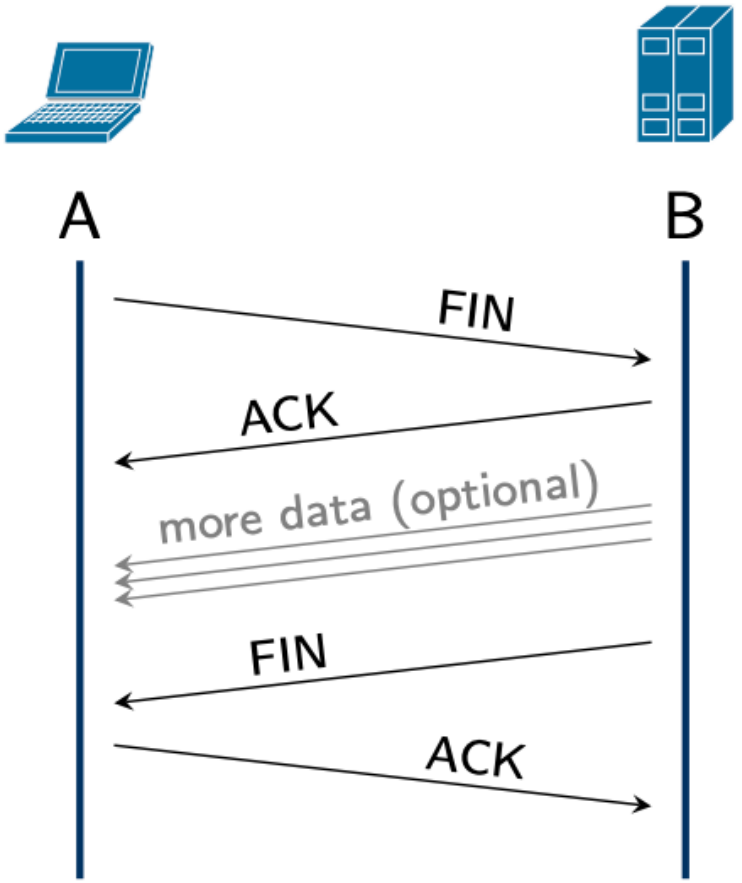
Question

Assume sending a packet from A to B takes 100 ms.
How much time elapses until A can send data to B?

700ms

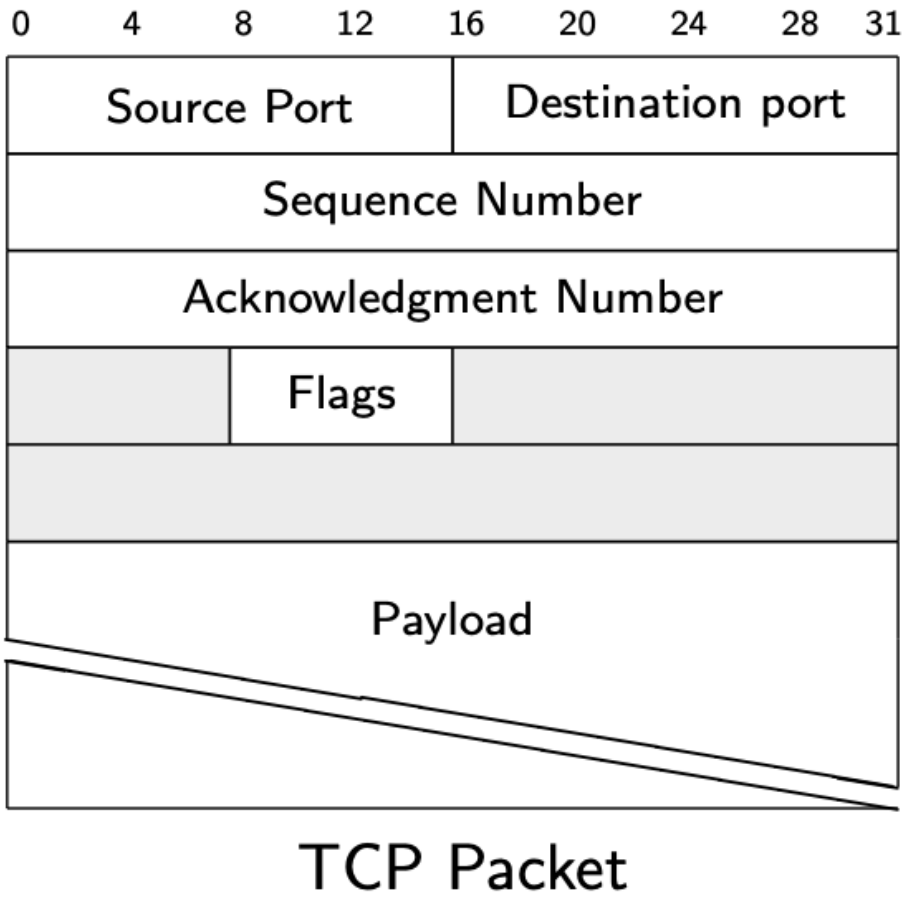


TCP connection closing



A typical TCP close.

sequence numbers



TCP Packet

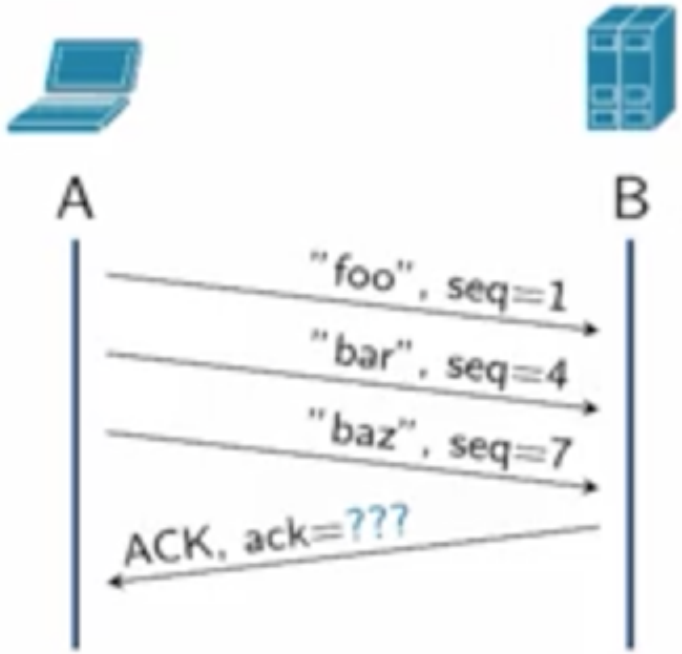
sequence numbers

	A sends	B sends
1	SYN, seq=0	
2		SYN+ACK, seq=0, ack=1
3	ACK, seq=1, ack=1	
4	"hello", seq=1, ack=1	
5		ACK, seq=1, ack=6
6	"world!", seq=6, ack=1	
7		"bye!", seq=1, ack=12
8		FIN, seq=5, ack=12
9	"bye!", seq=12, ack=6	
10	FIN, seq=16, ack=6	
11		ACK, seq=6, ack=17

Sequence numbers are idealized, see below.

Question

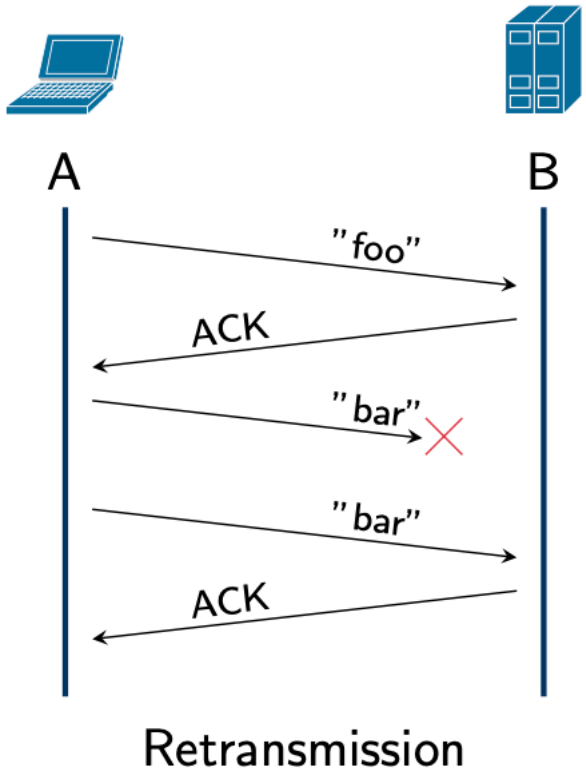
Given the following packet exchange,
what acknowledgment number should the server send?



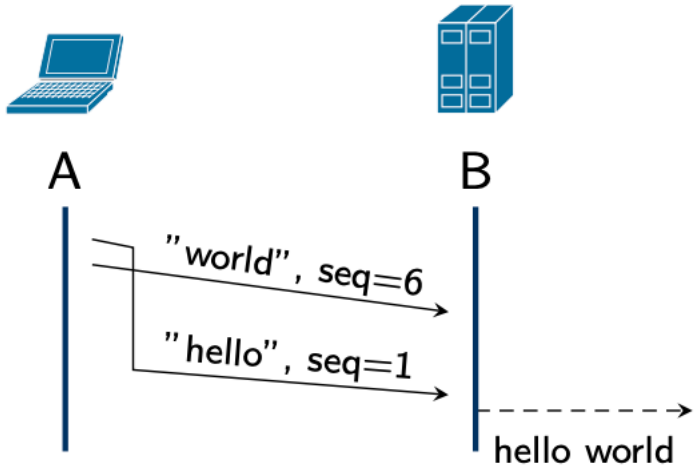
Question

Given the following packet exchange,
what acknowledgment number should the server send?

TCP reliability



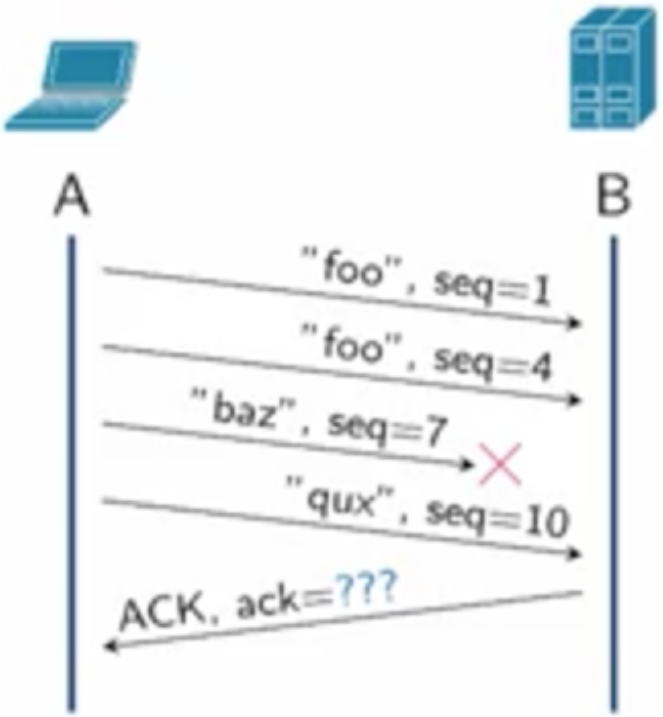
Retransmission



Reordering

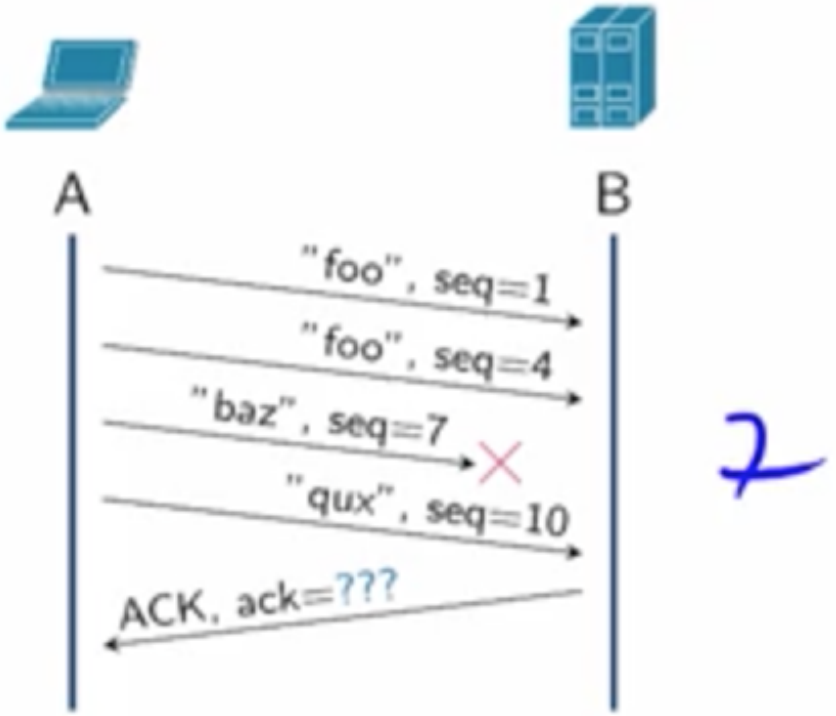
Question

Given the following packet exchange,
what acknowledgment number should the server send?



Question

Given the following packet exchange,
what acknowledgment number should the server send?



2

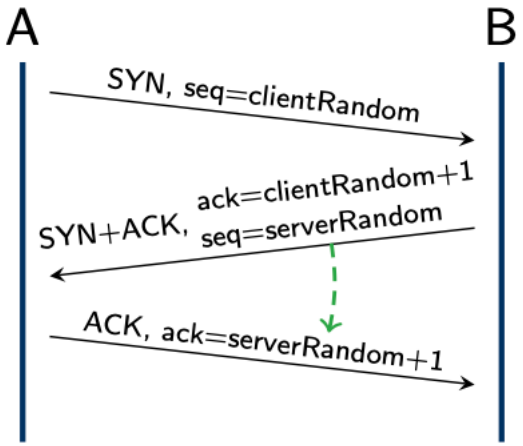
Roadmap

1. TCP (Transfer Control Protocol)
2. **TCP security**

IP spoofing

How can we make IP spoofing hard?

Start with unguessable sequence number.

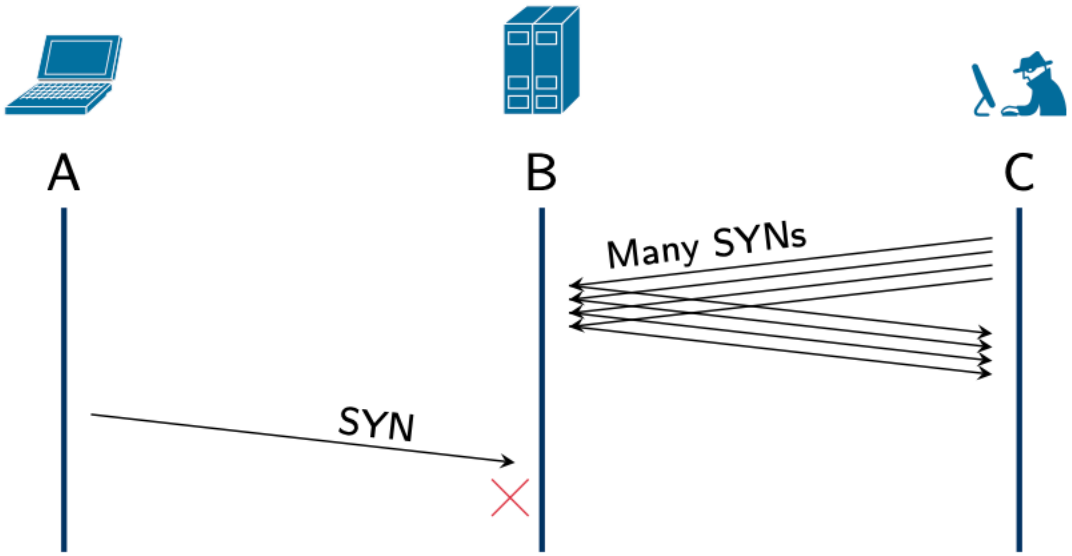


⇒ A needs to observe `SYN+ACK` before sending data.

⇒ IP spoofing can be done only by machines on the path between client and server.

SYN flooding

Server needs to keep state for each connection.



⇒ Attacker can flood `SYN`s to exhaust server resources.

security on the transport layer

- TCP is still plaintext.
- IP spoofing is hard, but still no sender authenticity.
- Target for man-in-the-middle attacks:

Security needs to be added at a higher layer.