

Network Security I

Question 1 *Back to L_4 Basics*

(15 min)

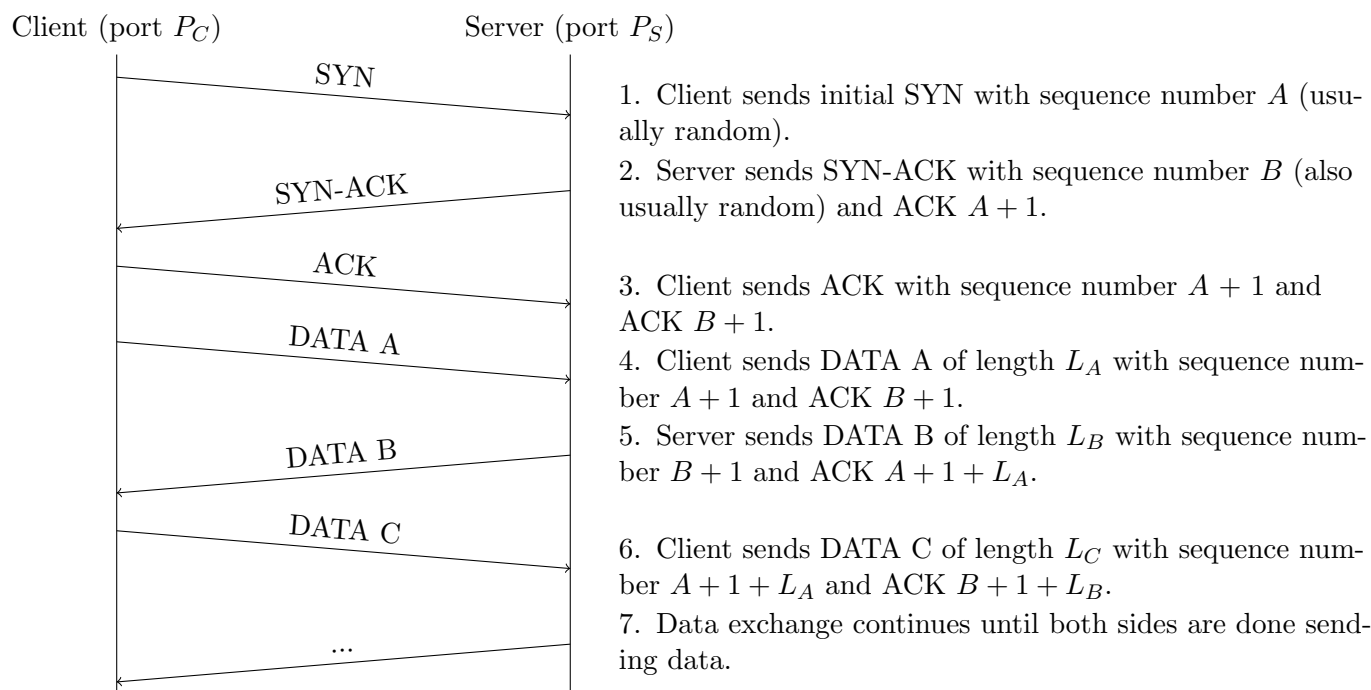
The transmission control protocol (TCP) and user datagram protocol (UDP) are two of the primary protocols of the Internet protocol suite.

- (a) How do TCP and UDP relate to IP (Internet protocol)? Which of these protocols are encapsulated within (or layered atop) one another? Could all three be used simultaneously?
- (b) What are the differences between TCP and UDP? Which is considered “best effort”? What does that mean?
- (c) Which is easier to spoof, and why?

Question 2 *Attack On TCP*

(35 min)

Suppose that a client connects to a server, and then performs the following TCP handshake and initial data transfer:



- (a) Assume that the next transmission in this connection will be DATA D from the server to the client. What will this packet look like?

Sequence number: _____ ACK: _____

Source port: _____ Destination port: _____

Length: L_D Flags: None

- (b) You should be familiar with the concept and capabilities of a *man-in-the-middle* as an attacker who **CAN observe** and **CAN intercept** traffic. There are two other types of relevant attackers in this scenario:

1. *On-path* attacker: **CAN observe** traffic but **CANNOT intercept** it.
2. *Off-path* attacker: **CANNOT observe** traffic and **CANNOT intercept** it.

Carol is an *on-path* attacker. Can Carol do anything malicious to the connection? If so, what can she do?

- (c) David is an *off-path* attacker. Can David do anything malicious to the connection? If so, what can he do?

- (d) The client starts getting responses from the server that don't make any sense. Inferring that David is attempting to hijack the connection, the client then immediately sends the server a **RST** packet, which terminates the ongoing connection. Can David successfully impersonate the client and establish a new connection with the server?

Assume that the server trusts the client's IP address as an identifier of the client.