Article 3 – TCP Handshake

**How Does It Work and Why Is It Important?**

The TCP three-way handshake is the process by which a client and server establish a reliable and connection-oriented session before the exchange of actual data.

1. SYN: The client sends a TCP segment with the SYN flag set and the Initial Sequence Number (ISN).

“Hi, I’d like to start a connection; here is my starting sequence number.”

1. SYN-ACK: The server responds with both the SYN and ACK flags set.

SYN – Carries its own ISN.

ACK – Acknowledges the receipt of the client’s SYN by setting ACK = SYN+1

“I’ll talk to you. Here’s my sequence number, and I got yours”.

1. ACK: The client finally responds with the ACK flag set and the server’s ISN as ACK = SYN+1.

“Great! I received your SYN. Let’s begin communicating”.

A three-way handshake is important for several reasons:

1. Allows sequence number synchronization. Ensures both endpoints are aware of where to start numbering bytes from for transmitting data. This prevents old or other data packets from interrupting the new session.
2. Sets the reliability foundation. Confirms that both sides are reachable and ready for communication; without it, neither side can be sure whether the other side is listening.

**Sequence Numbers: Labeling Every Byte**

Initial Sequence Number (ISN): When establishing the three-way handshake, both sides pick a random 32-bit ISN.

Byte-Offset Labeling: Every byte of data in the stream is assigned a unique sequence number in a sequential manner (1000, 1001, 1002,…)

**Acknowledgement Numbers: Confirmation Receipts**

The ACK field in a TCP segment indicates the next sequence number the receiver expects. This is known as a cumulative ACK, as it acknowledges every byte up to the sequence in the ACK has been received.