TCP VS UDP and Three-way handshake

Alright, my fellow hackers, it's time to dive into the heart of network communication – the TCP and UDP protocols. These two workhorses are the foundation upon which countless applications and services are built, and as hackers, understanding their intricacies is crucial for identifying potential vulnerabilities and executing successful attacks.

I have listed the difference between both of them in this nice looking table. So, let's go through each of the pointers one by one.

Let's start with the Connection Type - So the TCP requires an established connection between a client and the server before transmitting any data. If there is no connection, no data will be flowed, it is as simple as that. Talking about UDP on this, it is a connection-less protocol. Unlike TCP, no connection is needed to start or end a data transfer.

Next is the data sequence - In TCP, data is send in a sequential or specific order where as this is not the case in UDP.

After this we have Data Retransmission - If in case, a data packet is lost while transferring in TCP, it will re-transmit it while on the other hand, UDP doesn't care about all this extra work.

Next is Delivery - As we discussed earlier, TCP is connection-oriented protocol and also re-transmits wherever required, so the delivery of data is guaranteed whereas UDP does not guarantee anything, you are at your own risk.

Moving on we have Checking for errors - TCP gives us this but for UDP it depends on the mood.

And at last we have speed - Now in this particular comparison, we have been shitting on UDP but in this point, UDP is a clear winner. As we know TCP needs connection, it sometimes re-transmits and gurantee delivery but due to all these features, it comes slow sometimes. While on the other hand, UDP is all about speed.

You can think, TCP as a lovely supporting wife that mutually accepts your love and gives back with more. But on the other hand, UDP is like that one-sided crush who likes speedy dating and all you can do is to shower connectionless data packets to it with maximum speed with no guaranteed results.

Keeping the jokes aside, we can use TCP where we need gurateed deliery of data and speed is not the priority like while transferring funds from one bank account to another while on the other hand, UDP is used in scenario where speed of the data is in priority like Video Streaming and Conferencing, where delay can cause an inconsistent and unpleasant experience.

3 way handshake

To understand the working of TCP protocol, we have to understand the TCP 3 way handshake.

Imagine you want to have a conversation with someone over the phone, but you need to establish a proper connection first. The three-way handshake is like the initial back-and-forth you go through to set up the call.

- The first step is you calling the other person's number. This is like sending a "SYN" or synchronize message, saying "Hey, I'd like to start a conversation with you."
- If the other person is available, they will pick up the phone and respond with "SYN-ACK" or synchronize-acknowledge. This is them saying "Sure, I'm ready to talk. I heard your request to start a conversation."
- When you hear them pick up, you confirm by saying "ACK" or acknowledge. This final acknowledgement establishes the connection, and you can now start your conversation over the open line.

The three-way handshake ensures that both parties are ready to communicate and have acknowledged each other's initial sequence numbers before data transfer begins. It's like making sure you and the person you're calling have properly greeted each other before launching into the conversation.

This process prevents scenarios where one side thinks a connection is open while the other side thinks no connection has been made. The three steps make the connection setup more robust and reliable.

The handshake also allows both parties to negotiate parameters like the maximum data size they can send or receive in each chunk. It's like agreeing on how much you can say in one go during your conversation before pausing for the other person to respond.

So in simple terms, the three-way handshake is an initial exchange of messages that establishes a reliable data connection, similar to setting up a phone call properly before starting to speak.

Working of UDP

Imagine you are sending letters through the postal service, but you don't really care if some letters get lost or arrive out of order. UDP is like that unreliable postal service.

With UDP, you just keep writing letters data packets and putting them in outgoing mail without waiting for acknowledgement that the previous letters arrived safely. You simply send the datagrams out rapidly one after another.

You just keep writing letters and putting them in outgoing mail as fast as possible. It's a "best effort" approach - some letters may arrive quickly, some may arrive late, some may get lost, and some may arrive out of order. But you don't care, as long as most of the important information gets through without too much delay.

This works well for applications that can tolerate some data loss, like video streaming, online gaming, DNS lookups etc. It's much faster than a formal "connection-oriented" protocol like TCP that establishes a reliable communication channel first before transferring data.

The trade-off is that UDP is unreliable and unordered, but it's lightweight and super fast for time-sensitive data transfers where occasional data loss is acceptable. It's like a super speedy but unreliable postal worker who just keeps moving your letters along as quickly as possible!
