

6 If you want to skip the handshake you could use UDP instead. – [Oznetverid](#) Nov 4 '15 at 22:20

5 @Mehrdad, if you have a question of your own, please use the [Ask Question](#) link at the top of the page to post your own. – [YLearn](#) ♦ Nov 4 '15 at 23:12

45 @YLearn: Sorry, it's not really a question of my own, but rather it was to motivate readers to give answers that dig a little deeper than what is literally stated in the question. – [user541686](#) Nov 5 '15 at 0:03

5 Don't forget about TCP Fast Open (RFC 7413) – [Alnitak](#) Nov 6 '15 at 23:25

## 9 Answers

Active	Oldest	Votes
--------	--------	-------



Break down the handshake into what it is really doing.

192



In TCP, the two parties keep track of what they have sent by using a Sequence number. Effectively it ends up being a running byte count of everything that was sent. The receiving party can use the opposite speaker's sequence number to acknowledge what it has received.

But the sequence number doesn't start at 0. It starts at the ISN (Initial Sequence Number), which is a randomly chosen value. And since TCP is a bi-directional communication, both parties can

"speak", and therefore both must randomly generate an ISN as their starting Sequence Number. Which in turn means, both parties need to notify the other party of their starting ISN.

So you end up with this sequence of events for a start of a TCP conversation between Alice and Bob:

```
Alice ---> Bob    SYNchronize with my Initial Sequence Number of X
Alice <--- Bob    I received your syn, I ACKnowledge that I am ready for [X+1]
Alice <--- Bob    SYNchronize with my Initial Sequence Number of Y
Alice ---> Bob    I received your syn, I ACKnowledge that I am ready for [Y+1]
```

Notice, four events are occurring:

1. Alice picks an ISN and **SYNchronizes** it with Bob.
2. Bob **ACKnowledges** the ISN.
3. Bob picks an ISN and **SYNchronizes** it with Alice.
4. Alice **ACKnowledges** the ISN.

In actuality though, the middle two events (#2 and #3) happen in the same packet. What makes a packet a SYN or ACK is simply a binary flag turned on or off inside each [TCP header](#), so there is nothing preventing both of these flags from being enabled on the same packet. So the three-way handshake ends up being:

```
Bob <--- Alice    SYN
Bob ---> Alice    SYN ACK
Bob <--- Alice    ACK
```

Notice the two instances of "SYN" and "ACK", one of each, in both directions.

So to come back to your question, why not just use a two-way handshake? The short answer is because a two way handshake would only allow one party to establish an ISN, and the other party to acknowledge it. Which means only one party can send data.

But TCP is a bi-directional communication protocol, which means either end ought to be able to send data reliably. Both parties need to establish an ISN, and both parties need to acknowledge the other's ISN.


So in effect, what you have is exactly your description of the two-way handshake, but *in each direction*. Hence, four events occurring. And again, the middle two flags happen in the same packet. As such three packets are involved in a full TCP connection initiation process.

Share Improve this answer Follow

edited Sep 6 '16 at 14:03

answered Nov 4 '15 at 16:56

 **Xavi**  
103 4

 **Eddie**  
13k 4 34 74

- 
- 7 Why do we need ISNs at all? Humans don't need it, why do computers? Is there a proof of this, or do we just have them because they're convenient? – [user541686](#) Nov 4 '15 at 20:52
- 
- 29 @Mehrdad: You need sequence numbers for retransmissions to work properly (or indeed at all). The ISN can't just be zero because of [sequence prediction attacks](#). – [Kevin](#) Nov 4 '15 at 21:04
- 
- 4 @Mehrdad The chat room doesn't necessarily have to be 'real time', we can leave messages for each other. The reason I thought to direct it elsewhere is because you are now asking a different question. The OP asked "why is it a 3 way handshake instead of 2", but now you questioning "why do we need Sequence numbers at all", which is different. Rather than derail this thread, I thought we should discuss the other question in chat. *Alternatively*, you can post a new question, I'm sure it will net some good answers. – [Eddie](#) Nov 4 '15 at 22:19
- 
- 5 Great, concise answer. Reading "ACK SYN" feels fundamentally wrong but you even explained that so +1. – [Lilienthal](#) Nov 5 '15 at 12:52
- 
- 3 According to [RFC 793, Transmission Control Protocol](#): "*The principle reason for the three-way handshake is to prevent old duplicate connection initiations from causing confusion.*" – [Ron Maupin](#) ♦ Nov 5 '15 at 18:05
- 



24

The three-way handshake is necessary because both parties need to **synchronize** their segment sequence numbers used during their transmission. For this, each of them sends (in turn) a SYN segment with a sequence number set to a random value  $n$ , which then is **acknowledged** by the other party via a ACK segment with a sequence number set to  $n+1$ .



Share Improve this answer Follow

answered Nov 4 '15 at 15:05

 **dr\_**  
1,240 1 9 18

---

Why is the acknowledgement needed? – [Paūlo Ebermann](#) Nov 4 '15 at 21:18