# LAB-08

## TCP Intro qanda

1. **What field in the TCP header determines the expected length of the header?**

Ans. Data offset (4 bits) Specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum are 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header.

2. **What is the minimum and maximum number of bytes a TCP header can have. Explain your reasoning.**

Ans. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header. This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data.

3. **It is not possible to have a 23-byte header, why not? What is used to pad the data?**

Ans. The header is **24 bytes** long and contains 15 fields, including 4 bytes for source IP address and 4 bytes for destination IP address

PAD stands for packet assembler-disassembler, is a telecommunications device that breaks a data stream into individual packets and formats the packet headers for asynchronous transmission over an X.25 network. It also accepts packets from the network and translates them into a data stream.

4. **What is required for a TCP segment to be considered valid for a given connection?**

Ans. TCP uses **a three-way handshake** to establish a reliable connection. The connection is full-duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other.

5. **Why does TCP have a three-way handshake?**

Ans. TCP uses a three-way handshake **to establish a reliable connection**. The connection is full-duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps: SYN, SYN-ACK, ACK.

6. **You notice a TCP SYN packet with the same 4-tuple occurring at regular intervals in a packet capture. Those time interval since the first packet sent seems to be 2s, 4s, 8s, 16s, 32s, and 64s. What is this behavior called?**

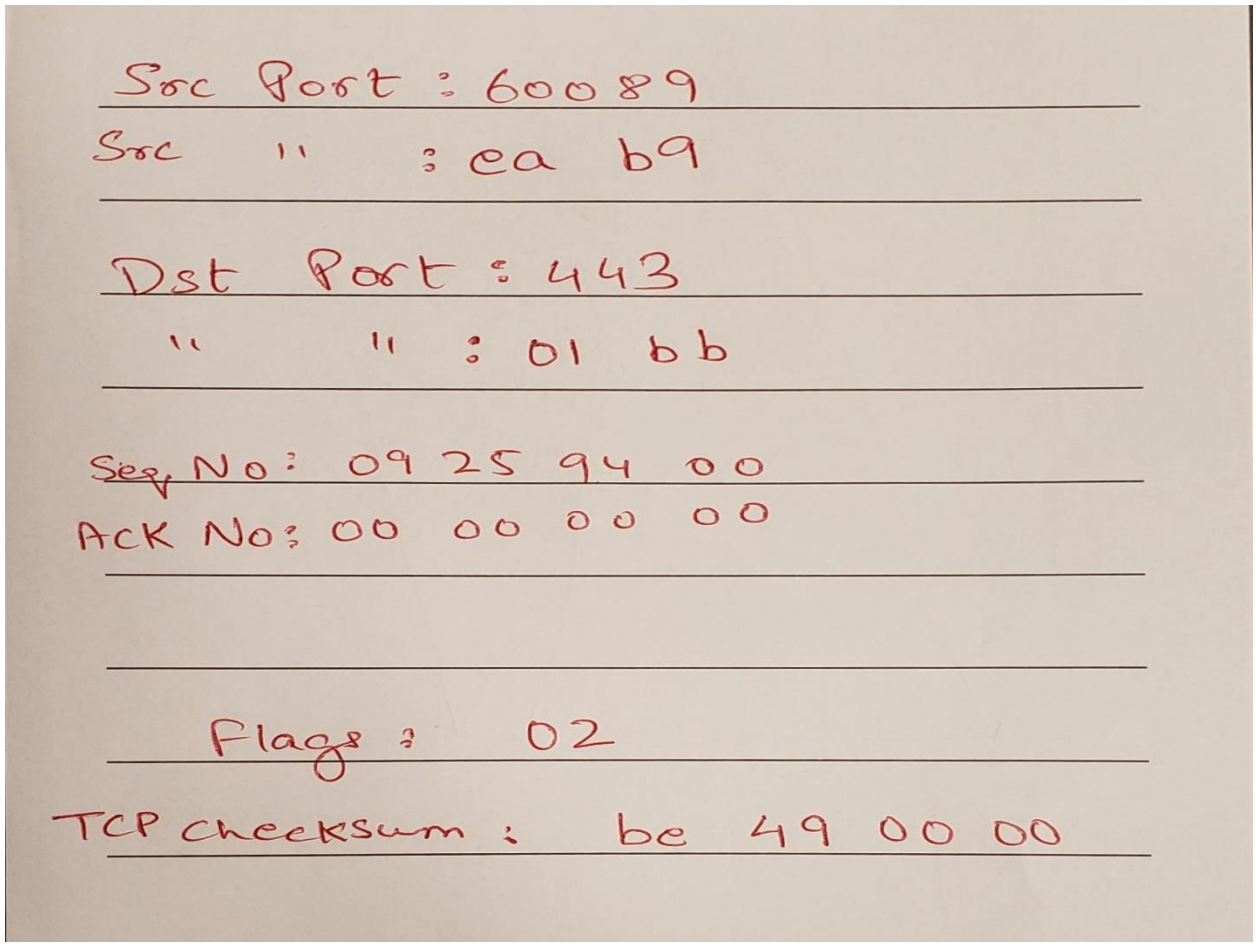
Ans. Three-Way Handshake.

**TCP Packet qanda**

**The link layer (14 bytes) and network layer (20 bytes) protocols occupy the first 34 bytes of the frame for all three of the packets capture in this printout. The printout contains a three-way handshake only.**

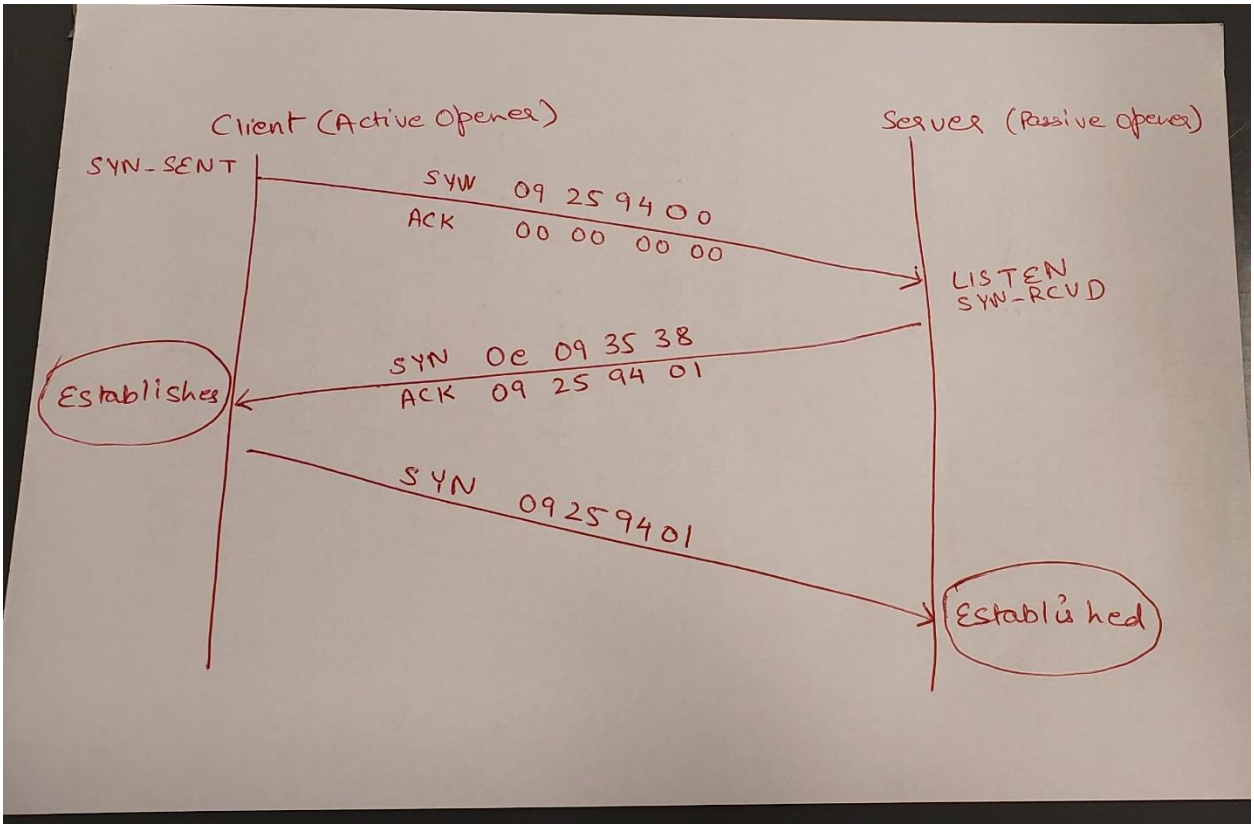
1. **Create a protocol diagram similar to *Figure 13-1* from the slides. Include the *actual* sequence numbers in the diagram.**

Ans.



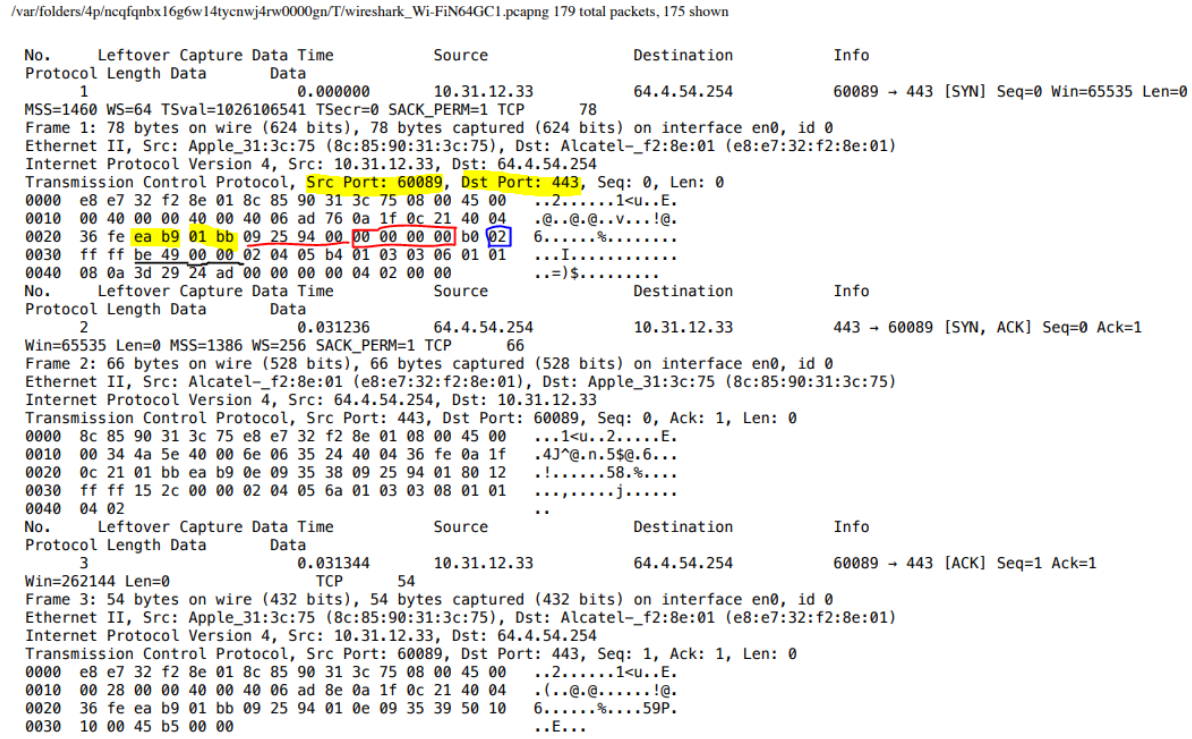
2. **Modify your diagram to include the TCP *state* that client/server are in.**

Ans.



**3. Highlight the source port, destination port, sequence number, acknowledgement number, flags and checksum in the *bytes* section for the client's SYN packet. Include a legend with your highlight mappings.**

Ans.



/var/folders/4p/ncqfqnbx16g6w14tycnwj4rw0000gn/T/wireshark_Wi-FiN64GC1.pcapng 179 total packets, 175 shown

```
No.     Leftover Capture Data Time           Source                Destination           Info
Protocol Length Data       Data
      1                    0.000000       10.31.12.33           64.4.54.254           60089 → 443 [SYN] Seq=0 Win=65535 Len=0
MSS=1460 WS=64 TSval=1026106541 TSecr=0 SACK_PERM=1 TCP      78
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
Ethernet II, Src: Apple_31:3c:75 (8c:85:90:31:3c:75), Dst: Alcatel-_f2:8e:01 (e8:e7:32:f2:8e:01)
Internet Protocol Version 4, Src: 10.31.12.33, Dst: 64.4.54.254
Transmission Control Protocol, Src Port: 60089, Dst Port: 443, Seq: 0, Len: 0
0000  e8 e7 32 f2 8e 01 8c 85 90 31 3c 75 08 00 45 00   ..2......1<u..E.
0010  00 40 00 00 40 00 40 06 ad 76 0a 1f 0c 21 40 04   .@..@.@..v...!@.
0020  36 fe ea b9 01 bb 09 25 94 00 00 00 00 00 b0 02   6.......%........
0030  ff ff be 49 00 00 02 04 05 b4 01 03 03 06 01 01   ...I............
0040  08 0a 3d 29 24 ad 00 00 00 00 04 02 00 00         ..=)$.........
No.     Leftover Capture Data Time           Source                Destination           Info
Protocol Length Data       Data
      2                    0.031236       64.4.54.254           10.31.12.33           443 → 60089 [SYN, ACK] Seq=0 Ack=1
Win=65535 Len=0 MSS=1386 WS=256 SACK_PERM=1 TCP      66
Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
Ethernet II, Src: Alcatel-_f2:8e:01 (e8:e7:32:f2:8e:01), Dst: Apple_31:3c:75 (8c:85:90:31:3c:75)
Internet Protocol Version 4, Src: 64.4.54.254, Dst: 10.31.12.33
Transmission Control Protocol, Src Port: 443, Dst Port: 60089, Seq: 0, Ack: 1, Len: 0
0000  8c 85 90 31 3c 75 e8 e7 32 f2 8e 01 08 00 45 00   ...1<u..2.....E.
0010  00 34 4a 5e 40 00 6e 06 35 24 40 04 36 fe 0a 1f   .4J^@.n.5$@.6...
0020  0c 21 01 bb ea b9 0e 09 35 38 09 25 94 01 80 12   .!......58.%....
0030  ff ff 15 2c 00 00 02 04 05 6a 01 03 03 08 01 01   ...,.....j......
0040  04 02                                             ..
No.     Leftover Capture Data Time           Source                Destination           Info
Protocol Length Data       Data
      3                    0.031344       10.31.12.33           64.4.54.254           60089 → 443 [ACK] Seq=1 Ack=1
Win=262144 Len=0              TCP      54
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_31:3c:75 (8c:85:90:31:3c:75), Dst: Alcatel-_f2:8e:01 (e8:e7:32:f2:8e:01)
Internet Protocol Version 4, Src: 10.31.12.33, Dst: 64.4.54.254
Transmission Control Protocol, Src Port: 60089, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
0000  e8 e7 32 f2 8e 01 8c 85 90 31 3c 75 08 00 45 00   ..2......1<u..E.
0010  00 28 00 00 40 00 40 06 ad 8e 0a 1f 0c 21 40 04   .(..@.@......!@.
0020  36 fe ea b9 01 bb 09 25 94 01 0e 09 35 39 50 10   6......%....59P.
0030  10 00 45 b5 00 00                                 ..E...
```