TCP Connection

30/3/23

Step 1 Client sends a TCP Packet Known as SYN segment. Among the 6 flags in TCP segment, in SYN segment, only the SYN flag is set. SYN segment uses one sequence Number. No data in SYN segment.

Step 2

*The Server replies with a SYN+ACK segment In SYN+ACK segment. only two flags are set; SYN & ACK flags.

*The SYN segment is used for communication in Server ⟶ client direction.

The ACK flag is an acknowledgement of the first SYN sent by the client.

Step 3

The client replies to the SYN+ACK segment with a ACK segment. In the ACK segment only the ACK flag is set. The ACK segment does not use any Sequence number.

SYN flooding attack:-

1) Denial of service type.

2). Client sends multiple SYN segments using fake IP in the source address.

3) The server responds to each fake SYN segment by replying it with SYN+ACK segments & reserve resources for future communication.

4) As a result the resources of a server ~~on~~ be exhausted by using fake IP as source addresses.

Solutions: 1) Time based constraint
2) ~~Ident~~ Restricting IPs
3) Withholding resources.

Connection establishment
↓
Data Transfer
↓
Connection Termination

Step-1,2,3

1) Client sends a FIN segment, where the FIN flag is set. It might contain the last of data from client.

2) Server replies with FIN + ACK, where both FIN & ACK flags are set. FIN + ACK can carry the last of data from server side.

3) ~~The~~ Finally the client replies by ACK segment. It contains no data, hence does not need sequence number.

TCP Flow control:

TCP provides flow control & error control using

1) Sequence Number.
2) Acknowledgement Number.
3) Flow control Algorithms:-
ex:- Stop & Wait ARQ
Go back-N-ARQ
Sliding Window.