Transport Layer

- The transport layer's job is to ensure that data is not incorrectly received by the receiver and that traffic is correctly directed to the specific application on the device. The main protocols are TCP and UDP
    - UDP
        - The header has the source port, destination port, length, and checksum
        - The port is a logical port, which is owned by TCP and UDP. Provides a rental address for the program to run.
        - Ports can be formed as 2 to the power of 16, depending on the range. 0-1023 Common port, 1024-49151 registered port, 49152-655535 temporary port.
        - Well-known ports are not often used by applications, and access on Unix requires superuser privileges.
        - Registered ports are more flexible to use, and there are no restrictions on how applications can use them.
        - Temporary ports are automatically required by the system for applications to respond to messages.
        - When machine A and machine B access the browser at the same time, one machine will temporarily rent A port to make it the source port. When a response is received, the data is forwarded to the application and the temporary port releases its hold.
    - NAT(network address translation)
        - Going back to the network layer, the problem is that you have a rented IP address if you have multiple devices in your home. How does a router route traffic to devices? It's all through NAT.
        - The combination of preserving the local IP address space and overload ports allows multiple devices to share a single IP address.
        - The packet contains source IP, destination IP, source port and destination port. When a machine sends a packet to a website, the router rents a new IP address and source port to replace the packet. But the original information is saved in the NAT list. When the site returns a packet, the router returns the original IP address and source port based on the NAT list.
    - Transmission Control Protocol (TCP)
        - It provides reliable, orderly, and error checking on hosts communicating over IP networks.
        - TCP is structured by :Destination port: indicates the destination port of the traffic
          Source port: The port to which replies should be directed.
          Serial number and confirmation number: Used together to ensure delivery of data.
          Data offset: Indicates the starting position of data.

Resources: Reserved

Flags: indicates the type of TCP Segment (see Flags)

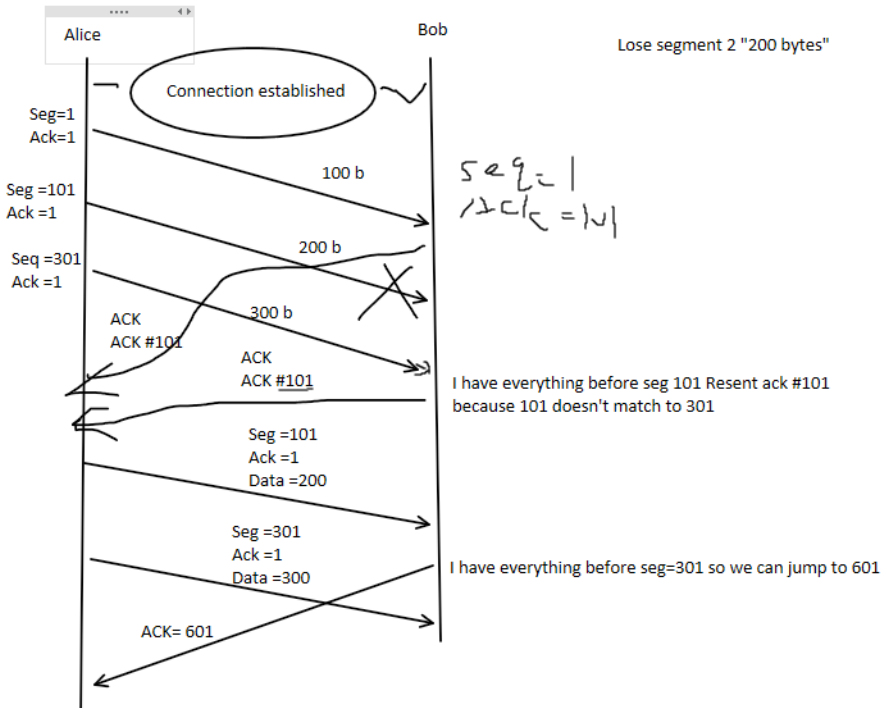
Window size: Used for congestion control to tell the sender how much data (in bytes) this device can receive at a point in time.

Checksum: Provides data integrity.

I personally don't think data integrity is necessary because the data link layer is also responsible for it, but there are objections on the network 3

Emergency pointer (not important to us) : Intended to allow segment priority. (out of date)

Options (not important to us) : Contains optional fields such as maximum segment size, window scaling, selective validation, and timestamp

- [SYN] is used to establish the connection for the first time, [No symbol] is used to encode the data segment of the data block, [ACK]Acknowledgment used to indicate receipt of data,[FIN]The end segment used to indicate a request to terminate a connection
- TCP is duplex, with each side having two sets of serial numbers and confirmation numbers
- Notify each other of the transmission speed by resize the window
- The connectionless datagram service provided by UDP reduces latency but not reliability. Perform any error recovery necessary to prevent the program from completely failing. For example, in online multiplayer games, characters are delayed after wrong location, and corrected after reconnection.
- 

    - Bob will ack back depend on losing which data from Alice.