1. Layer 3 protocols:
   * IP:
     + Internet Protocol (IP) is a layer 3 protocol that provides mechanism to transport packets from source to destination based on IP address
     + They are designed to be efficient and scalable but at the cost of unreliable and connectionless delivery.
     + IP address is a best effort delivery service, meaning it attempts to deliver packets but does not guarantee delivery, order of delivery etc.
     + It lacks error detection as well as error correction
     + If there is some error, the packet is simply dropped and the matter is left to higher level protocols.
   * ICMP:
     + The ICMP(Internet Control Message Protocol) is designed to compensate the following deficiencies
       - Determine if a router is alive
       - The destination can’t be found or the TTL(Time To Live) hits 0.
     + There are two types of messages: error reporting message and query message
       - Error reporting message report problems that a device may encounter when processing the packet
       - Query message help a device get information of another device
     + It’s main job is to report errors to the original source, it does not correct them
     + There are 2 main tools under ICMP for debugging:
       - Ping: It is used to mainly find if a host is alive and responding. It has an echo request packet and an echo reply packet. If the reply packet reaches the original source, the router is alive and responding
       - Tracert: This tool is used to trace the route between the original source and destination. It sets its TTL value to 1 at the initial step to get a reply from the first hop. Then it increases the TTL value subsequently by 1 to get reply at every hop.
2. Layer 4 protocols:
   * Overview:
     + The data link layer is responsible for delivery fo frames between 2 nodes, hence it is called node-to-node delivery
     + The network layer is responsible for delivery of frames between 2 hosts, hence it is called host-to-host delivery
     + The transport layer is responsible for process-to-process delivery
   * UDP:
     + It is a connectionless, unreliable transport protocol with a simple overhead
     + It performs very minimal error correction
     + If a process want to send either a small packet that does not require error check or some very important packet like live video or audio which must be delivered as soon as possible, UDP is preferred as it does not consume much time unlike TCP
     + UDP headers are of a fixed size of 8 bytes and have the following fields:
       - Source Port: This is the port number used by the process running on source host
       - Destination Port: this is the port number used by the process running on the destination host
       - Length: it indicates the length of the entire datagram
   * TCP:
     + Transmission control Protocol is a process-to-process protocol.
     + It uses port numbers as well
     + TCP is connection oriented protocol; it creates a virtual connection between 2 TCPs
     + It also flow and error control mechanism
     + It uses a numbering system for each packet to keep the sequence in mind.
     + In a TCP, the host and destination TCP are involved in a 3 way handshake where when decide upon the number of packets to be transferred
     + Until and unless all the packets reach the destination, no further packets will be sent. This makes it a slow but efficient process
     + Structure of the segment header
       - Source port address
       - Destination port address
       - Sequence number
       - Acknowledgement number
       - Header length
       - Etc