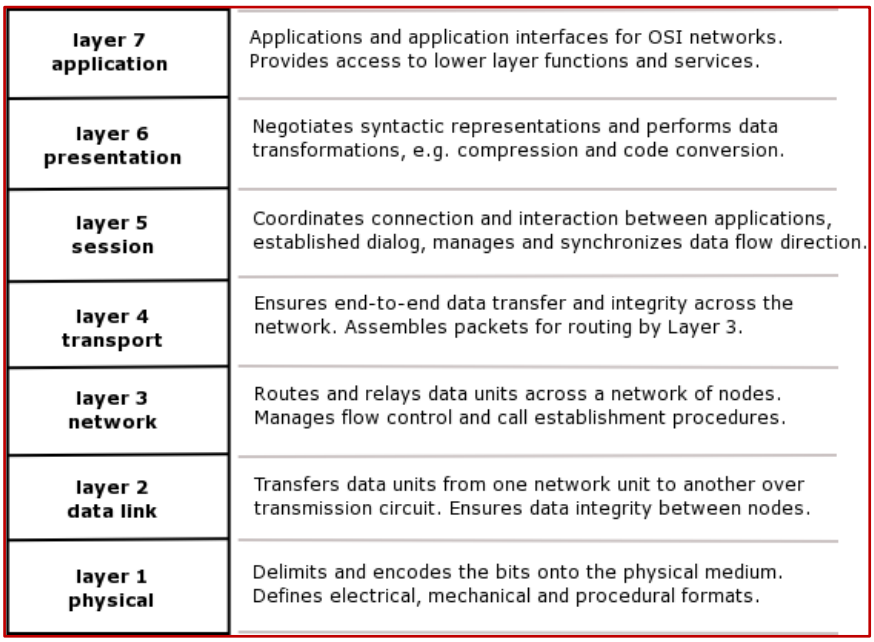
1 Basics:

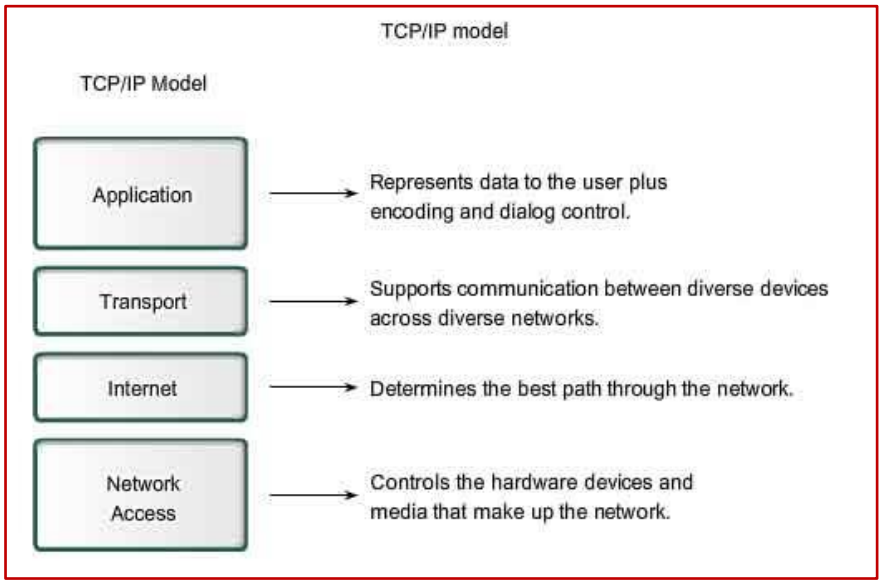
1. **What is difference between LAN, MAN and WAN?**

   LAN is a private network used in small offices or homes usually within 1km range with high speed transfer data rate and fulltime service connectivity in low cost. WAN covers a large geographical area for example, a country or a continent. Its data transfer data is usually low as compared to LAN, but it is compatible with a variety of access lines and has an advanced security. MAN covers an area bigger than LAN within a city or town and serves as an ISP for larger LAN. It uses optical fibers or wireless infrastructure to link the LANs therefore, providing high speed regional resource sharing.

2. **Explain OSI layers in detail**

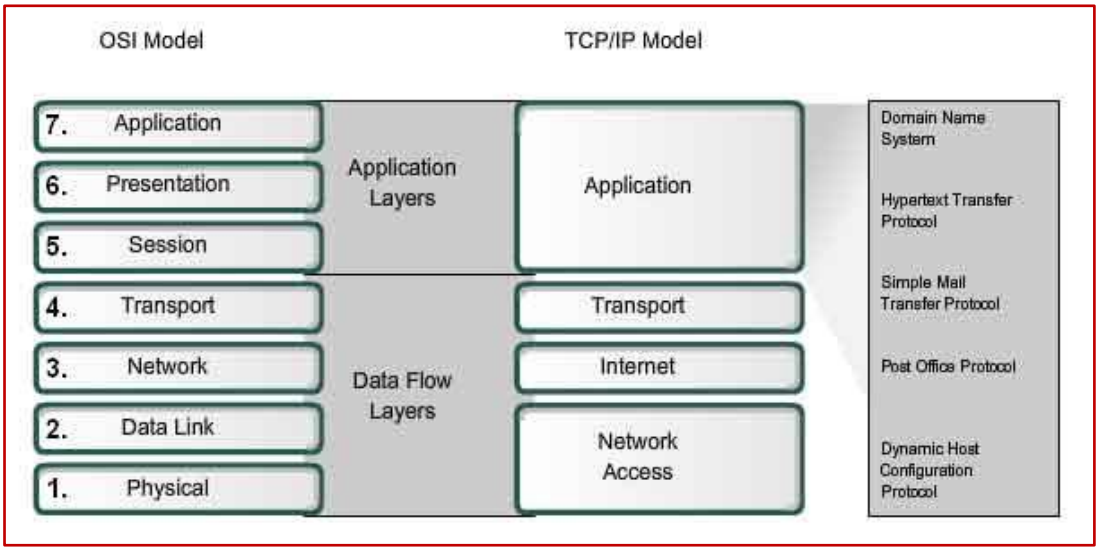


3. **Explain TCP/IP layers in detail**



4. **What is the fundamental difference between OSI model & TCP/IP model?**

   OSI model is a reference model, which mentions about functionality of each of the layers. TCP/IP model is a derived model from OSI, which practically implements the OSI functionalities.



5. **What other models you know other than TCP/IP that are derived based on OSI?**
   - AppleTalk
   - IPX
   - SNA
   - UMTS

6. **What are the differences between Hub / Switch / Router?**

   - **Hub**

   A network hub is designed to connect computers to each other with no real understanding of what it is transferring. When a hub receives a packet of data from a connected device, it broadcasts that data packet to all other connected devices regardless of which one ends up being the final destination. Working at layer 1 (Refer OSI model)

   - **Switch**

   A network switch also connects computers to each other, like a hub. Where the switch differs from a hub is in the way it handles packets of data. When a switch receives a packet of data, it determines what computer or device the packet is intended for and sends it to that computer only. Traditional switching operates at layer 2 but layer 3 switches also available

   - **Router**

   A network router is quite different from a switch or hub since its primary function is to route data packets to other networks, instead of just the local computers. A router is quite common to find in homes and businesses since it allows your network to communicate with other networks including the Internet. Operates at layer 3

2 TCP/IP addressing:

1. **What is a MAC address? What is its significance?**

   A media access control address (MAC address), also called physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most network technologies, including Ethernet and Wi-Fi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.
   MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware.

2. **What is an IP address? What is its significance?**

   An IP address is an identifier/address for a computer or device on a TCP/IP network. Where the networks using the TCP/IP protocol and route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255. For example, 192.168.32.12 could be an IP address. IP have two parts network and host part.

3. **What is port number? What is its significance?**

   A port number is the logical address of each application or process that uses a network or the Internet to communicate. A port number uniquely identifies a network-based application on a computer. Each application/program is allocated a 16-bit integer port number.
   Port numbers are mainly used in TCP and UDP based networks, with an available range of 0-65,535 for assigning port numbers. Although an application can change its port number, some commonly used Internet/network services are allocated with global port numbers such as Port Number 80 for HTTP, 23 for Telnet and 25 for SMTP.

4. **What are various classes of IP address?**

Class	Theoretical Address Range	Binary Start
A	0.0.0.0 to 127.255.255.255	0
B	128.0.0.0 to 191.255.255.255	10
C	192.0.0.0 to 223.255.255.255	110
D	224.0.0.0 to 239.255.255.255	1110

5. **What is a netmask? Explain its significance**

   A netmask is a 32-bit mask used to divide an IP address into subnets and specify the network's available hosts. In a netmask, two bits are always automatically assigned. For example, in 255.255.225.0, "0" is the assigned network address. In 255.255.255.255, "255" is the assigned broadcast address.

6. **What is IPv4 and IPv6 addresses? Explain their differences**

   An IP address is binary numbers but can be stored as text for human readers. For example, a 32-bit numeric address (IPv4) is written in decimal as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.
   IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this: 3ffe:1900:4545:3:200:f8ff:fe21:67cf

   Advantages of IPv6 over IPv4:

   - IPv6 simplified the router's task compared to IPv4.
   - IPv6 is more compatible to mobile networks than IPv4.
   - IPv6 allows for bigger payloads than what is allowed in IPv4.
   - IPv6 is used by less than 1% of the networks, while IPv4 is still in use by the remaining 99%.

7. **Explain differences between different types of ports.**

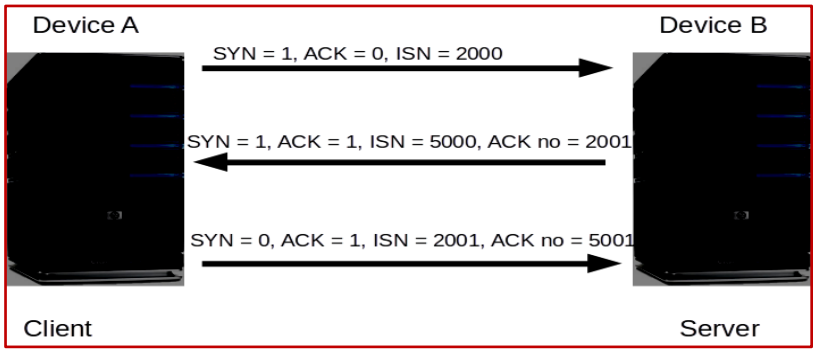
   - Well known ports
     Well known ports are used by system or processes run by root or with specific privileges. The port numbers range from 0 to 1023.
   - System ports
     Same as well-known ports
   - User ports /Registered ports
     The registered port numbers range from 1024-49151. Such ports are used by programs run by users in the system.

- Dynamic / Private ports
  Private ports are not assigned for any specific purpose. Its range are from range 49152-65535

8. **Explain importance of following Linux Networking commands:**
   - ifconfig
     To get IP address as well as MAC address of system interfaces.
   - Traceroute
     To get the route of each packet from source to destination
   - Nslookup / host
     To convert a domain name to IP address.
   - Netstat
     Current network status of application using network
   - ping
     To check connectivity between two system using ICMP protocol

9. **Explain TCP three-way handshake steps in detail**

   Before the sending device and the receiving device start the exchange of data, both devices need to be synchronized. During the TCP initialization process, the sending device and the receiving device exchange a few control packets for synchronization purposes. This exchange is known as Three-way handshake.



Step 1. Device A (Client) sends a TCP segment with SYN = 1, ACK = 0, ISN (Initial Sequence Number) = 2000. Refer TCP header

An Initial Sequence Number (ISN) is a random Sequence Number, allocated for the first packet in a new TCP connection.
The Active Open device (Device A) sends a segment with the SYN flag set to 1, ACK flag set to 0 and an Initial Sequence Number 2000 (For Example), which marks the beginning of the sequence numbers for data that device A will transmit. SYN is short for SYNchronize. SYN flag announces an attempt to open a connection.

Step 2. Device B (Server) receives Device A's TCP segment and returns a TCP segment with SYN = 1, ACK = 1, ISN = 5000 (Device B's Initial Sequence Number), Acknowledgment Number = 2001 (2000 + 1, the next sequence number Device B expecting from Device A).Refer TCP header

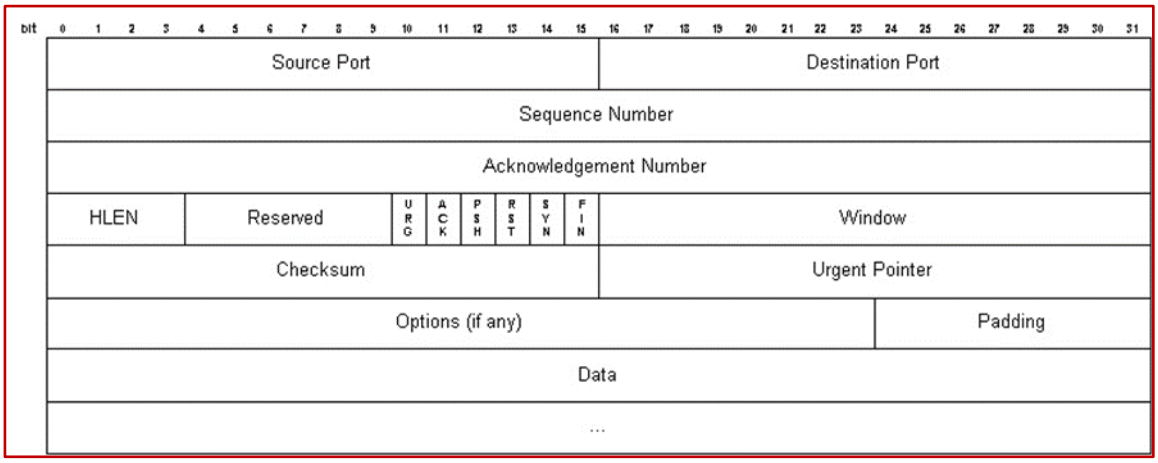
Step 3. Device A sends a TCP segment to Device B that acknowledges receipt of Device B's ISN, With flags set as SYN = 0, ACK = 1, Sequence number = 2001, Acknowledgment number = 5001 (5000 + 1, the next sequence number Device A expecting from Device B)

This handshaking technique is referred to as TCP Three-way handshake or SYN, SYN-ACK, ACK. After the Three-way handshake, the connection is open and the participant computers start sending data using the agreed sequence and acknowledge numbers.

10. What is the difference between TCP and UDP

TCP	UDP
• Connection oriented TCP • Reliable delivery • In-order guaranteed • Three way handshake • More network BW	• Connectionless UDP • Unreliable delivery • No-order guarantees • No notion of “connection” • Less network BW

11. Explain various fields of TCP header



Source Port: 16 bits
The source port number.

Destination Port: 16 bits
The destination port number.

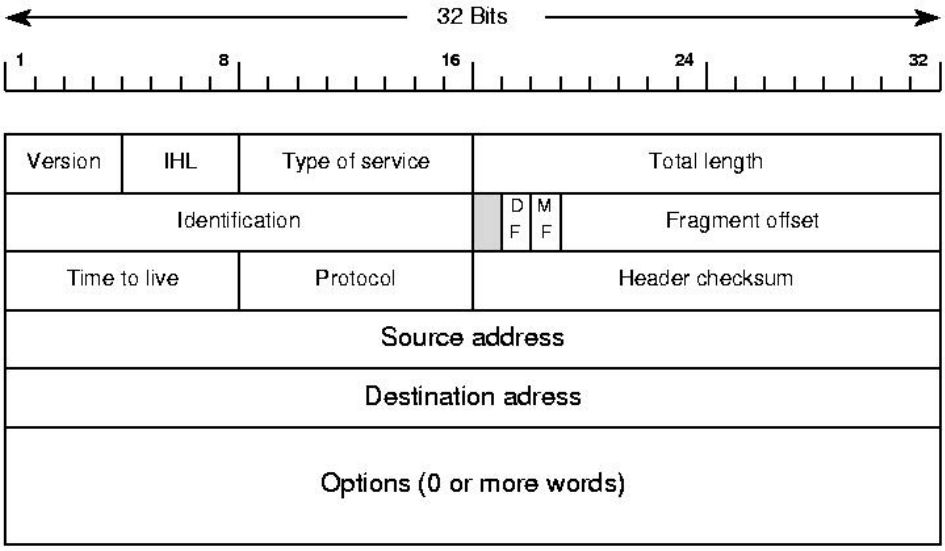
Sequence Number: 32 bits
The sequence number of the first data octet in this segment (except when SYN is present). If SYN is present the sequence number is the initial sequence number (ISN) and the first data octet is ISN+1.

Acknowledgment Number: 32 bits
If the ACK control bit is set this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.

Data Offset (Header len) : 4 bits
The number of 32 bit words in the TCP Header. This indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits long.

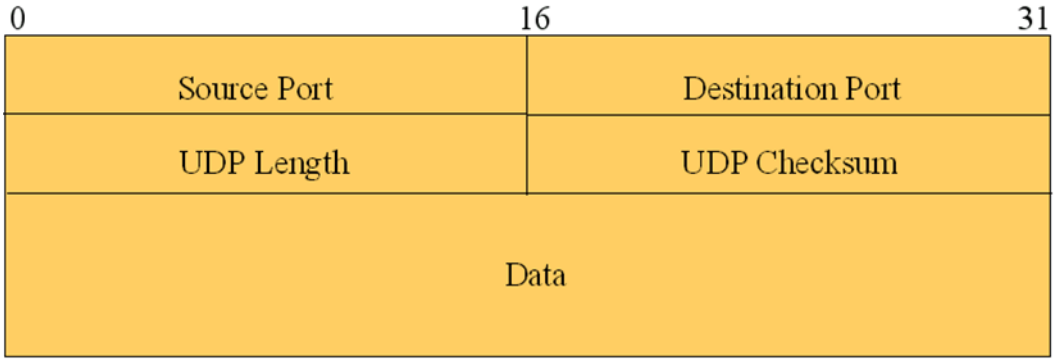
Control Bits: 6 bits (from left to right):
URG: Urgent Pointer field significant
ACK: Acknowledgment field significant
PSH: Push Function
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: No more data from sender

12. Explain various fields of IP header



Version:
IPv4 or IPv6
Source and destination IP address:
This fields store the source and destination address respectively. Since size of these fields will vary according to version (IPv4 – 32bit, IPv6 – 128 bit).

13. Explain various fields of UDP header



14. Given an application you need to choose between TCP and UDP. Compare them with respect to speed, cost and reliability

Refer Qn 10

15. Briefly explain how routing works?

Routing is the process of forwarding IP packets using routing table from one network to another. A router is a device that joins networks together and routes traffic between them.
A routing table is a **set** of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.

3 TCP/IP protocols – Brief working details:

1. SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.
SNMP is widely used in network management systems to monitor network-attached devices for

conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

2. **ICMP**

   ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages. ICMP is not a transport protocol that sends data between systems.

3. **ARP & RARP**

   The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP) [RFC826], specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer.
   The Reverse Address Resolution Protocol (RARP) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.

4. **DNS**

   The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address. Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. There is probably a DNS server within close geographic proximity to your access provider that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

5. **DHCP**

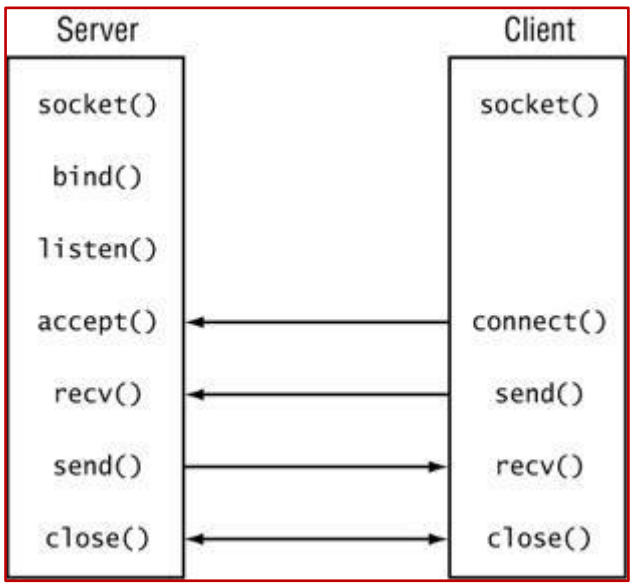
   DHCP (Dynamic Host Configuration Protocol) is a communications protocol that network administrators use to centrally manage and automate the network configuration of devices attaching to an Internet Protocol (IP) network. DHCP allows devices needing an IP address to request one when they are starting up, for example, rather than an address preassigned and manually configured on each device. With DHCP, if a device is moved from place to place, it will be assigned a new address in each location.

4 Socket programming

1. **What is a socket? How it is different compared to other system calls?**

   A socket is just a logical endpoint for communication. They exist on the transport layer. You can send and receive data on a socket. A socket is bind to a protocol, machine, and port.
   Using socket we can communicate between process in same system as well as process in different device over network.

2. Explain system calls used in TCP client and server.



3. **Explain TCP client and server system calls and three-way handshake**

   Three way handshake happens between connect and accept. Ref Qn 9

4. **Is bind() is mandatory in the client side? Justify your answer.**

   Bind is optional in client side. When we do a connect request from the client bind will happen automatically.

5. **What is host byte order and network byte order? Explain**

   Since machines will have different type of byte orders (little endian v/s big endian), it will create undesired issues in the network. In order to ensure consistency network (big endian) byte order to be used as a standard. There are multiple help functions (for conversion) available which can be used for this purpose.

   ```
   uint16_t htons(uint16_t host_short);
   uint16_t ntohs(uint16_t network_short);
   uint32_t htonl(uint32_t host_long);
   uint32_t ntohl(uint32_t network_long);
   ```

6. **What is control connection and what is data connection? Explain with respect to socket() and accept() system calls.**

   In server program of a TCP/IP connection we will get two socket fds.

   1. From socket system call, which we need to bind with IP and port number. This socket fd is called as control socket. We use this socket to accept connections from multiple clients. With one control socket we can accept any number of clients.
   2. When accept multiple connections we need one more fd to send/receive data with client. That fd we will receive from accept system call which called as data socket.

7. **What is the difference between send() and sendto()?**

   Send is using for TCP/IP connection where we only send data. Sendto using for UDP connection where we need send data as well as destination details (IP and PORT).

8. **Define iterative server and concurrent server. What are their advantages and disadvantages?**

Iterative server	Con-current server
Pros: - Simple - Reduced network overhead - Less CPU intensive - Higher single-threaded transaction throughput **Cons:** - Severely limits concurrent access - Server is locked while dealing with one client	**Pros:** - Concurrent access - Can run longer since no one is waiting for completion - Only one listener for many clients **Cons** - Increased network overhead - More CPU and resource intensive

9. **What is the importance of select () system call? Explain it in the context of synchronous I/O**

   Select is a system call which help to write a **concurrent** server in one process. It also used to examine the status of file descriptors of open input/output channels. The select system call is similar to the polling in operating systems. Select loop uses the select system call to sleep until a condition occurs on a file descriptor (e.g., when data is available for reading) or a timeout occurs. By examining the return parameters of the select call, the loop finds out which file descriptor has changed and executes the appropriate code to read/write to file descriptor.

10. **What is a RAW socket? Explain its importance**

    Using RAW packet we can read the packet directly from physical layer. Means it will by-pass transport and network layer and directly passed application layer.
    If you want implement your own protocols on top of physical layer, we can use RAW packet data.

5 Application specific:

1. **I type www.google.com in Chrome. Explain various protocols that helps to make browsing happen**

   - The browser extracts the domain name from the URL.
   - The browser queries DNS for the IP address of the URL. If neither the browser nor the OS have a cached copy of the IP address, then a request is sent off to the system's configured DNS server.
   - If that DNS server has the address for that domain, it will return it. Otherwise, it will forward the query along to DNS server it is configured to defer to.
   - The web browser then assembles an HTTP request, which consists of a header and optional content.
   - This HTTP request is sent off to the web server host (via TCP/IP/MAC layer protocols) as some number of packets, each of which is routed in the same way as the earlier DNS query. (The packets have sequence numbers that allow them to be reassembled in order even if they take different paths.)
   - In the routing side there are a set of routing protocols (RIP, IGMP, OSPF etc..) which routes the packet from the source (your machine) to the web-server. This follows complex routing algorithm
   - Once the request arrives at the webserver, it generates a response (this may be a static page, served as-is, or a more dynamic response, generated in any number of ways.) The web server software sends the generated page back to the client in the similar way.

2. **List of protocols that doesn't use IP address**
   DHCP, ICMP, IGRP, ARP etc