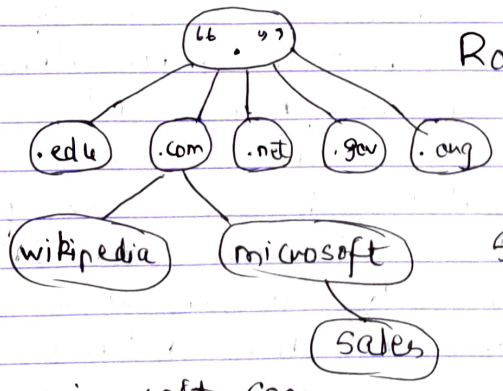
CN TT2 QB
Chp-6 Application Layer

1. Explain DNS in detail

Ans: Domain Name System (DNS) is a host name for an IP address translation ~~server~~ service.
Application layer protocol for message exchange between clients and servers.
It is a distributed db implemented in a hierarchy of name servers.
Requirement:
Every host is identified by a unique IP address. It is difficult for humans to remember numbers and also IP addresses are not static, hence some kind of mapping is required to change the domain name to IP address.
DNS is used to convert the domain name of websites to their IP addresses.

Domains :-
* Generic Domain — .com (commercial) .edu (educational) .net (similar to commercial) .org (organization).
* Country Domain — .in (India) .us, .uk
* Inverse Domain - DNS can provide both the mapping, IP to domain and domain to IP.



sales.microsoft.com

* DNS Record :- Domain Name, IP address, Validity, Time to live and other info related to domain name. Records are stored in tree like structures
* Namespace :- Set of possible names, flat or hierarchical. In flat, each name is a sequence of characters without structure. In hierarchical each name has several parts. First part - nature of org, second part - name of organization, third part - dept of org and so on.
* Name Server :- It is the implementation of resolution mechanism.

Name to Address Resolution :-
Host request the DNS name server to resolve the domain name.
Name server returns the IP address corresponding to the domain name.

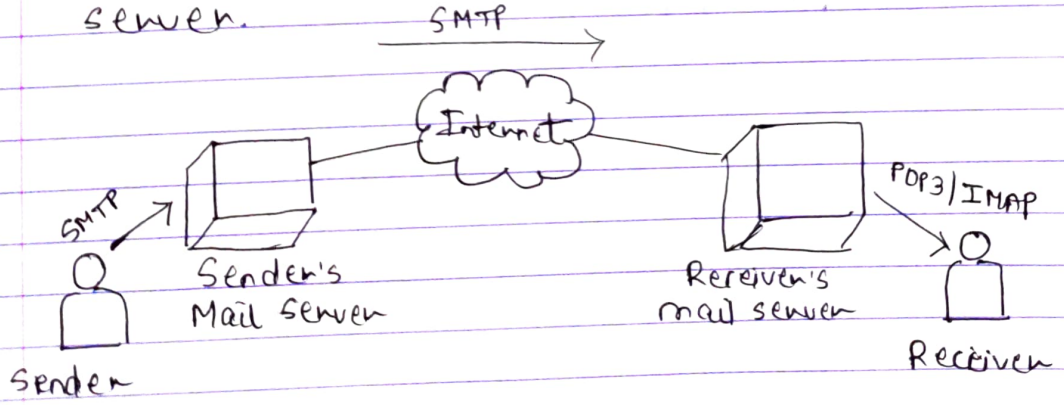
Hierarchy of Name Servers
* Root name servers :- Contacted by name servers that cannot resolve the name. Contains info about top level name servers.
* Top Level Name Servers :- Responsible for generic domains and ~~co~~ top level country domains. Contains info about authoritative name servers (name and IP address).
* Authoritative Name Servers :- This is the organization's DNS server, providing authoritative hostname to IP mapping. Maintained by organization or service provider. They will return the associative IP address.

Q 2. Write a short note on:- SMTP Protocol

Simple Mail Transfer Protocol
Application layer protocol
Used for sending emails efficiently and reliably over the Internet.
It is a push protocol
Used port number 25.
Uses TCP at the transport layer
Connection-oriented protocol
Stateless Protocol.

Working:-
SMTP server is always on a listening mode.
Clients initiates a TCP connection with the SMTP server.
SMTP server listens for a connection and establishes a connection on that port.
The connection is established.

Client informs the SMTP server that it would like to send a mail.
Assuming that the server is OK, the client sends the mail to its mail server.
With the help of DNS the client's mail server gets the IP address of the receiver's mail server.
Then, SMTP transfers the mail from the sender's mail server to the receiver's mail server.



While sending the mail SMTP is used twice
1.) Between the sender and the sender's mail server
2.) Between the sender's mail server and receiver's mail server.

To receive or download the mail, Another protocol is used between the receiver's mail server and the receiver. POP3 or IMAP.

Q 3. Write a short note on Telnet
Ans. Short for ~~Tet~~ Terminal Network.
Client-Server application that allows a user to log on to a remote computer and allows the user to ~~use~~ access any application on the remote computer.
Uses NVT (Network Virtual Terminal) system to encodes the characters on the local system.
On the remote system, NVT decodes the characters to a form acceptable to the remote machine.
Provides a general, bi-directional, 8 bit byte oriented communication facility.
Many ~~Co~~ application layer protocols are built on Telnet protocol
Uses Port Number 23.

Q4. Write a short note on DHCP Protocol

Dynamic Host Configuration Protocol is a network management tool to dynamically assign IP addresses to any device, node on a network so that they can communicate using IP.

There is no need to manually assign IP address to new devices.

It can be implemented on local networks as well as large enterprise networks.

Default protocol of most routers and networking equipment.

Manages the provision of all nodes or devices added or dropped from the network.

Maintains the unique IP address of the host using a DHCP server.

It sends a request to the DHCP Server whenever a client/node/device configured with DHCP connects to the network. The server acknowledges by providing an IP address to the client/node/device.

Runs at the application layer of the TCP/IP stack to dynamically assign IP addresses to the DHCP clients and to allocate TCP/IP configuration info (which include Subnet mask info, default gateway, IP addresses and DNS addresses).

Based on client-server protocol where the server maintains a pool of unique IP addresses and assign IP addresses out of those address pools.

Components of DHCP.

* DHCP server:- A networking device running DHCP service that holds a pool of IP addresses and other configuration information. Typically a server or a router but it could be anything that acts as a host such as ~~SD-WAN~~ SD-WAN appliance.
* DHCP client:- It is the endpoint that receives configuration information from the DHCP server. Devices like computer, Laptop, IOT devices that require connectivity to the network. Most of the devices are configured to receive DHCP info by default.
* IP address pool:- Range of addresses that are available to the DHCP clients. Handed out sequentially from lowest to highest.
* Subnet:- Partitioned segments of the IP network. Used to keep networks manageable.
* Lease:- Time for which the DHCP client holds the IP address information. When the lease expires it has to renew it.
* DHCP Relay:- A host or router that listens for client messages being broadcast on the network and ~~sends responses~~ and forwards them to the configured server. The server then sends responses back to the relay agent that passes them back to the client. It can be used to centralize DHCP servers instead of having a DHCP server on each subnet.

Chapter 4: Network Layer

Q1. Explain in detail the different classes of IPv4 addresses.

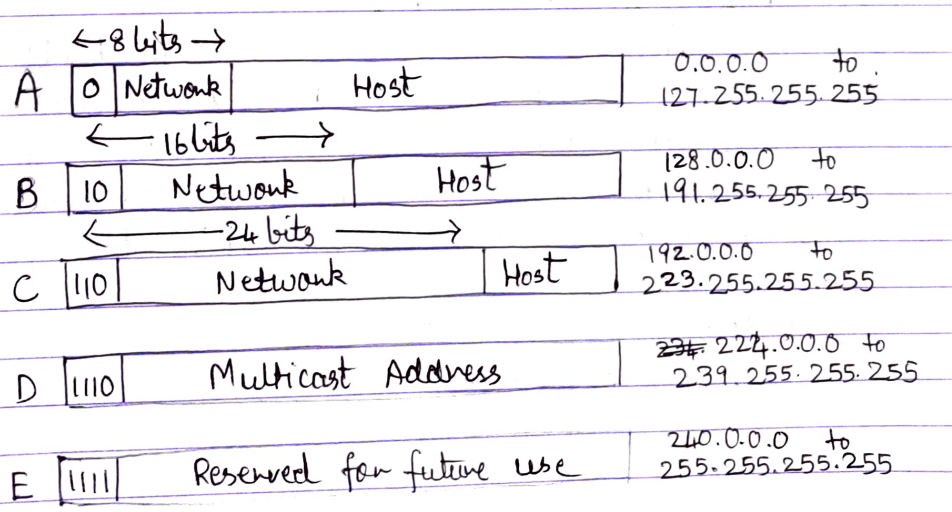
Ans 1. IP addresses are managed globally by IANA (Internet Assigned Numbers Authority) and RIR (Regional Internet Registries).
The 32 bit IP address is divided into 5 sub-classes.

Class A
Class B
Class C
Class D } Reserved for multicast and experimental purposes respectively
Class E }

IPV4 address is divided into two parts:-

i) Network ID
ii) Host ID.

The class of IP address determines the number of bits used for network ID and host ID and number of total networks and hosts possible in that particular class.
While finding the total number of host IP addresses two IP's are not counted, the first IP address is the network number and the last IP address which is the broadcast IP.



Class	Leading Bits	Net ID Bits	Host ID Bits	No. of networks	Addresses per network	Start Address	End Address
A	0	8	24	2^7	2^{24}	0.0.0.0	127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0	191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0	223.255.255.255
D	1110	N.D	N.D	ND	ND	224.0.0.0	239.255.255.255
E	1111	N.D	N.D	ND	ND	240.0.0.0	255.255.255.255

Range of special IP addresses.
169.254.0.0 - 169.254.0.16 - Link Local addresses
127.0.0.0 - 127.0.0.8 - Loop back addresses
0.0.0.0 - 0.0.0.8 : used to communicate within the current network.

Problems with classfull addressing:-
i) Millions of class A addresses are wasted, & many of class B addresses are wasted, and no. of class C addresses is so small that it cannot cater the needs of org.
ii) Class D addresses are used for multicast routing and class E addresses are reserved for experimental purposes.

Q 2. Compare and contrast - Virtual circuits Vs Datagram Networks.

Ans 2.

Virtual Circuits	Datagram Networks
* Virtual Circuit is a connection oriented service in which there is an implementation of resources like buffers, CPU, bandwidth for data transmission	It is a connection less service where no such resources are required for data transmission.

Virtual Circuit	Datagram Networks
* The path utilized or followed by the first data packet gets fixed and all other data packets will follow the same path and consume same resources	The path of data packets is not fixed as the packets are free to decide the path on any intermediary router by dynamically changing routing tables of routers.
* As the path is fixed all the packets use a common and same header.	Different headers with information of other data packets are used.
* Less complex	More complex
* More reliable due to fixed path and assurance of same resources	Less reliable due to dynamic path and dynamic resource allocation as they are prone to error.
* Costlier and mainly used in ATM networks (Asynchronous Transfer Mode) used for Telephone Calls.	Cheaper and mainly used for IP networks, used for Data services like Internet.

Q3. The address in the block is given as 73.25.16.27. Find the number of addresses in the block, the first address and the last address.

Number of addresses in the block = 2^{24}.
First Address = 73.0.0.0/8
Last Address = 73.255.255.255

Q 4 Explain the concept of subnetting and masking.

Ans 4 Subnetting

Dividing a large block of addresses into ~~smaller block of sub~~ several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting.

Also called subnet routing or subnet addressing.

Widely used when ~~classed~~ classless addressing is done to reduce the wastage of IP addresses.

We use host id bits as net id bits of classful IP addressing.

We give the IP address and define a number of bits for mask along with it.

Eg 192.168.1.1/28 where 28 out of ~~or~~ 32 bits are 1 and rest are 0 and so the subnet mask is 255.255.255.240.

Benefits of subnetting are-

i) Reduced network traffic
ii) Optimized network performance
iii) Simplified network management.

Masking

A process that extracts the address of the physical network from the IP address is called masking.

If we use subnetting, it extracts the subnet address from the ~~physical~~ IP address.

To find the subnet address two methods are used :-

i) Boundary Level Masking.
Mask number is 0 or 255

If mask number 255, IP address is repeated in the subnet address.
If mask number 0, 0 repeated in subnet address.

iii) Non-Boundary Level Masking
Mask number > 0 and < 255
If mask no. 255, IP address is repeated.
If mask no. 0, 0 is repeated.
For other values Bitwise AND operation is performed between each mask no (byte) and IP address (byte).

The default mask in different classes are:-
Class A:- 255.0.0.0
Class B:- 255.255.0.0
Class C:- 255.255.255.0

Q 7. Explain IPv4 Datagram Header in detail

← 16 bits →			← 16 bits →
Version (4 bits)	Header Length (4 bits)	Type of service (8 bits)	Total length (16 bits)
Identification (16 bits)		0	DF MF Fragment offset (13 bits)
Time to live (8 bits)	Protocol (8 bits)		Header checksum (16 bits)
Source IP Address (32 bits)			
Destination IP Address (32 bits)			
Options (0–40 bytes)			
Data			

* Version (4 bits)
  Indicates the version used. (IPv4 or IPv6)
  Only IPv4 uses the above ~~value~~ header, so this field is always set to ~~4~~ decimal value 4.
* Header Length (4 bits).
  Also known as Internet Header Length.
  Contains length of IP header, Range (0, 15)
  Helps in knowing from where the actual data begins.
  Header Length = Header Length field value × 4 bytes
* Type of Service (8 bits).
  Used for Quality of Service (QoS).
* Total Length (16 bits).
  Total length of datagram (in bytes)
  Total length = Header header + Payload length
  Min Total length = 20 bytes.
  Max Total length = 65535 bytes.
* Identification (16 bits).
  Identification of fragments of original IP datagram.
* IP Flags (3 bits).
  1st bit is always 0.
  2nd bit (Don't Fragment - DF) indicates that this packet should not be fragmented.
  3rd bit (More Fragments - MF) ~~indicates that~~ set on all fragmented packets except last one.
* Fragmented Offset (13 bits).
  Indicates position of fragmented datagram in original unfragmented IP datagram.
  1st fragmented datagram has a ~~off~~ fragmented offset of zero.
* Time to live (8 bits).
  Indicates maximum number of hops a datagram can take to reach the destination.
  main purpose to prevent IP datagram from looping around forever.

* Protocol (8 bits).
Tells the network layer at the destination host to which protocol the IP datagram belongs to.
Protocol no. of ICMP is 1 TCP is 6
IGMP is 2 UDP is 17
* Header Checksum (16-bits)
Store the checksum of the header.
Receiver can use this checksum to see if there are any errors in the header.
* Source IP address (32 bits)
* Destination IP address (32 bits)
* Options (0 to 40 bytes)
Used for several purposes – Record Route, Source Routing, Padding.

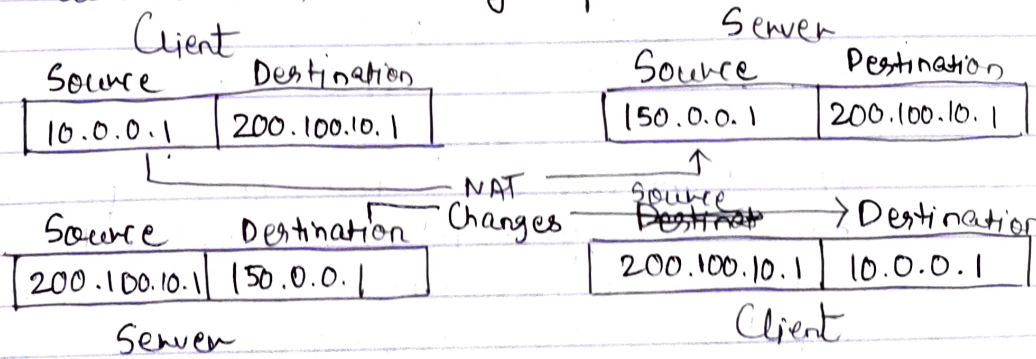
Q8. Explain NAT with its types and example
Network Address Translation (NAT) is used to map multiple local private addresses to a single public one before transferring the information.
NAT resulted in two types of addresses :- public and private.
The range of private addresses according to RFC 1918 are.
Class A:- 10.0.0.0 – 10.255.25.5.255
Class B:- 172.16.0.0 – 172.31.255.255
Class C:- 192.168.0.0 – 192.168.255.255.
NAT allows you to use these private addresses on your internal network.
You can assign unique addresses to all computers, servers using DHCP.
Another company can use the same set of private IP addresses as long as they are internal to the network.
So two companies can use the same set

of private IP addresses within their internal network without conflicting with each other.

When an internal host wants to communicate with the Internet, public address comes into picture. This address is purchased from the ISP is a routing public address, which would represent your network gateway. It is a unique address which no one can use.

Nat types :-

* Static NAT:
  Single private address is mapped with single public address. Used in Web Hosting.
* Dynamic NAT:
  Instead of choosing the same IP address, this NAT chooses from a pool of public IP addresses. This allows NAT device to get a different address each time the router translates the local address to a public address.
* PAT
  Port Address Translation. Type of dynamic NAT, binds several ~~public~~ local IP addresses to a single public one.



Q5. One of the addresses in the block is 167.199.170.82/27. Find no. of addresses in the network, 1st address and last address.

IP Address :- 167.199.170.82/27.
Subnet Mask :- 255.255.255.224.

No. of addresses is $2^5 = 32$.
First address = IP address AND Subnet Mask.
= 167.199.170.82 AND 255.255.255.224
= 167.199.170.64.

Last address = IP address OR (NOT Subnet Mask)
= 167.199.170.82 OR (NOT 255.255.255.224)
= 167.199.170.82 OR 0.0.0.31
= 167.199.170.95.

Q6. An organization is granted the block 130.34.12.64/26. The organization needs four subnetworks, each with an equal number of hosts. Design the subnetworks and find the information about each network.

IP Address :- 130.34.12.64/26.
Subnet Mask :- 255.255.255.192.
No. of addresses is $2^6 = 64$
No. of subnets is 4 so 16 addresses in each subnet.

Subnet 1	Subnet 2	Subnet 3	Subnet 4
S :- 130.34.12.64	S:- 132.34.12.80	S:- 132.34.1296	S:- 132.34.12.112
E:- 130.34.12.79	E:- 132.34.12.95	E:- 132.34.12.111	E:- 132.34.12.127.

Chapter 5: Transport Layer

Q 1. Explain in detail the services offered by Transport Layer.

Ans 1. The services offered by Transport Layer are:-

* End-to-end delivery:- Transmits the entire message to the destination. It ensures end-to-end delivery of an entire message from source to destination.
* Addressing:- Transport layer interacts with the functions of the session layer. Data generated by an application on one machine must be delivered to the correct application on another machine. Addressing is provided by the transport layer.
* Reliable delivery:- Transport layer provides reliable services by retransmitting the lost and damaged packets. Reliable delivery has four aspects:- Error Control, Sequence Control, Loss Control and Duplication Control.
* Flow Control:- Flow Control is used to prevent the sender from ~~overwhelming~~ overwhelming the receiver. If the receiver is overloaded with packets, it discards the packets and asks for retransmission. This increases network congestion, thus affecting the system performance. Thus transport layer is responsible for flow control. TL uses the sliding window protocol for efficient data transmission.
* Multiplexing:- Used for improving transmission efficiency. Two ways:-
  Upward Multiplexing:- Multiple ~~to~~ TL connections use the same network connection. To make cost-effective, the transport layer sends multiple transmission to the same destination on the same path.

Downward Multiplexing:- Single transport layer connection uses multiple network connections. Allows TL to split a connection among several paths to improve the throughput. Used when network have low or slow capacity.

Transport Layer Service Primitives

Primitive	TPDU Sent	Meaning
Listen	None	Block until some process tries to connect.
Connect	Connection Request	Actively attempt to establish connection.
Send	Data	Send data
Receive	None	Block until a data TPDU arrives.
Disconnect	Disconnect Request	Release the connection.

Q8 Explain Berkeley Sockets in detail.

Ans 8 Socket is a service provided by the TL. A socket is a endpoint of a two way communication link between 2 programs running on the network.
Berkeley socket is an API between Internet socket and UNIX domain socket.
Used for inter-process communication
Implemented as a library of linkable modules.
Primitive of Berkeley Socket
Socket - Create a new communication endpoint
Bind - Attach a local address to a socket
Listen - Shows willingness to accept a connection
Accept - Blocks the caller until a connection attempt arrives.

Connect :- Actively attempts to establish a connection.
Send :- Send data over the connection
Receive :- Receive data over the connection
Close :- Release the connection.

Q7. Explain different types of TCP timers :-
Ans 7. Timers used by TCP to avoid excessive delays during communication are called TCP timers.

i) Time-Out Timer :- Sender starts it when a TCP segment is transmitted to receiver.
If ACK received before timer, stop it.
If ACK not received before timer, TCP retransmission.
Sender retransmits, resets the timer.
Value of timer is dynamic, depends upon traffic in network.
Also known as Retransmission Timer

ii) Time Wait Timer :-
Senders starts this after transmitting ack for the second FIN segment.
It allows retransmission of final ack if it gets lost.
Prevents just closed port from reopening for some other application.
Ensures that segments forwarded to just closed port are discarded.
Value is set to twice of lifetime of TCP segment.

iii) Keep Alive Timer :- Each time server hears from client, it resets the timer to 2 hours.
If server does not hear within 2 hrs

it sends 10 probe segments at a gap of 75 seconds.
If it gets no response it assumes client is down.
Terminates the connection automatically.

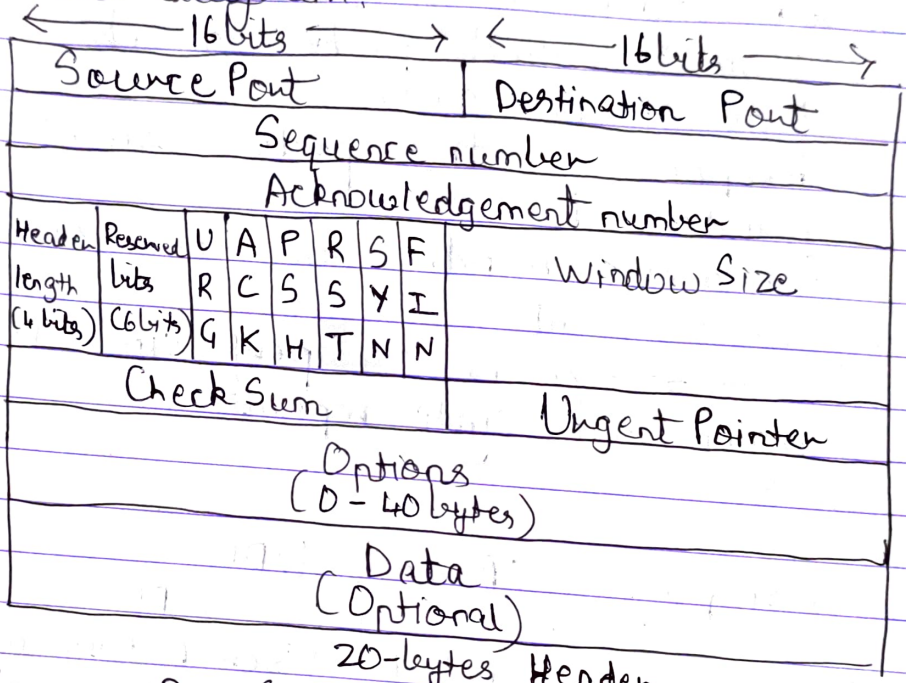
iv) Persistent Timer:-
Used to deal with zero-window-size deadlock situation.
Sender starts it on receiving ack with a 0 window size.
When timer goes off sender sends special segment called probe segment contains 1 byte of new data.
Response to this probe segment gives the window size.
If updated window size non-zero, data can be sent
If ~~0 s~~ size is 0, ~~perf~~ timer is set again and cycle repeats.

Q6. Compare TCP and UDP

TCP	UDP
* Transmission Control Protocol	User Datagram Protocol
* Connection Oriented Protocol	Connection less protocol
* Reliable protocol provides assurance for delivery of data	Unreliable protocol does not guarantee delivery of data.
* Slower as it performs, error checking, flow control	Faster
* Header size is 20 bytes.	Header size is 8 bytes.

TCP	UDP
* Provides error control by use of checksum and resends ~~of~~ lost data packets.	No error control and does not resend.
* Provides flow control mechanism.	No such mechanism.

Q4. Explain TCP header in detail with a neat diagram.



* Source Port (16 bits)
  Identifies the host process on sender m/c
* Destination Port (16 bits)
  Identifies the host process on receiver m/c
* Sequence Number (32 bits)
  Gives the sequence no of the first data byte in this segment. If SYN bit is 1, indicates sequence no is the intial sequence no and the 1st data byte is the initial sequence no. + 1.
* Ack no (32 bits).
  If ACK bit is 1, this field contains the value of next sequence no. receiver is expecting to receive.

* Header length (4 bits).
  Tells how many 32-bits words are present in the TCP
* Next 6 bits reserved for future use
* Flag Bits.
  URG: Set to 1 if the urgent pointer is in use
  ACK: Set to 1 indicates acknowledgement no is valid.
  PSH: Push Flag indicates pushed data
  RST: Reset the connection
  SYN: Establish the connection
  FIN: Set to 1 release the connection.
* Window Size (-16 bits)
  No of data bytes that the receiver is willing to accept
* Checksum (-16 bits).
  Used for error control.
  Sender adds CRC checksum to the checksum field before sending the data.
* Urgent Pointer (16-bits)
  Indicates how many bytes in the current segment from the 1st data byte is urgent
* Optional (0-40 bytes)
  Used for several purposes. - Time Stamp, Window size extension, Padding.

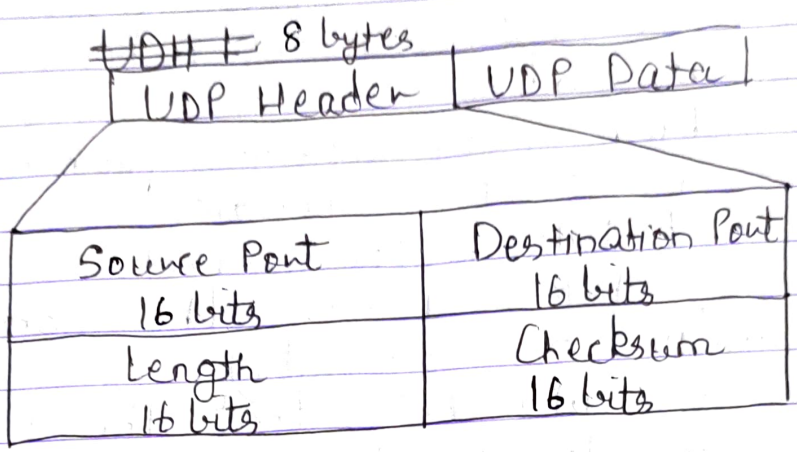
Q2. Explain features of UDP and also explain UDP Header in detail.

Ans. Features of UDP

i) Connectionless and unreliable protocol
ii) For real time services like computer gaming, video or voice communication.
iii) No error checking so it saves bandwidth.
iv) More efficient in terms of latency and bandwidth

v) UDP permits packets to be dropped instead of processing delayed packets for high performance

UDP Header (8 bytes)



* Source Port (2 bytes)
  Identify port number of source
* Destination Port (2 bytes)
  Identify port number of destination
* Length (2 bytes)
  Length of UDP header and including header and data
* Checksum (2 bytes).
  1's Complement of sum of UDP header, pseudo header of information from IP header and data, padded with zeroes zero octets at the end (if necessary) to make a multiple of two octets.

Q3: UDP header in hexadecimal form
06 32 00 0D 00 1C E2 17.
What is the
(a.) Source port number :- 1586
(b.) Destination port number :- 13
(c.) Total length of UDP :- 28 bytes
(d.) Length of data :- ~~28-2 = 26 bytes~~
= 28 - 8
= 20 bytes.

Q5. TCP header
00CD0018 00000EF1 00000D5D 5022 00D1
01BF0010

(a.) Source Port No :- 00CD
= 0000 0000 1100 1101
= 205

(b.) Destination Port No = 24.
(c.) Sequence Number = 3825
(d.) Acknowledgement Number = 3421.
(e.) Length of Header = 20 bytes
(f.) Type of Segment = SYN
(g.) What is window size = 209.

5022 00D1
0101 0000 0010 0010 0000 0000 1101 0001