Computer network Cheat Sheet

Q.1 Explain compare and draw OSI and TCP Model.

Ans.

Explanation :

1. **OSI model :**

OSI stands for Open Systems Interconnection. It has 7 layers Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer. Each layer performs its task independently. It was developed in 1984 by the International Organization for Standardization (ISO).

The layers manages a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments. Transport layer links the two groups

Physical Layer − Its function is to transmit individual bits from one node to another over a physical medium.

Data Link Layer − It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.

Network Layer − It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.

Transport Layer −It is responsible for delivery of the entire message from the source host to destination host.

Session Layer − It establishes sessions between users, and offers services like dialog control and synchronization.

Presentation Layer − It monitors syntax and semantics of transmitted information through translation, compression, and encryption.

Application Layer − It provides high-level APIs (application program interface) to the users

Advantages

- connection-oriented services and connectionless services are supported.
- It is quite flexible.
- All the layers work independently.

Disadvantages

- Setting up a model is a challenging task.
- Sometimes, it becomes difficult to fit a new protocol into this model.
- It is only used as a reference model.

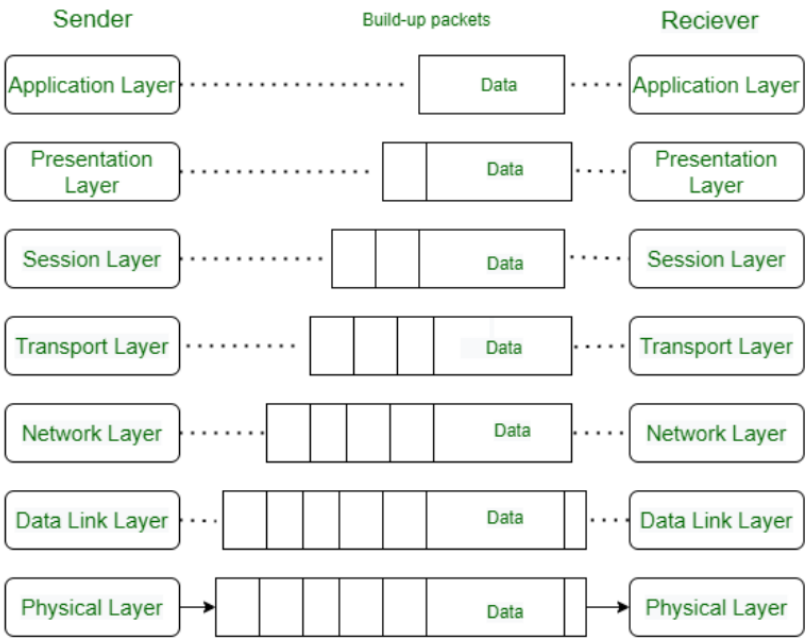
2. TCP model :

TCP/IP model was developed prior to the OSI model. The TCP/IP model is not exactly similar to the OSI model. **The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer**. The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer. TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality. It provides a full transport layer services to applications. It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission. TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded. At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message. At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Comparision :

Parameters	OSI Model	TCP/IP Model
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.

Draw :



Q.2 Explain draw and compare SMTP, MIME, SNMP, HTTP and FTP.

Ans.

Explanation :

1. SMTP :

Simple mail transfer protocol

The standard for e-mail transmissions across the Internet It is defined in RFC 821 It is a relatively simple, text-based protocol Port No is 25 It uses reliable connection to send mail. For the same it uses TCP connection.

o SMTP stands for Simple Mail Transfer Protocol.

o SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.

o It is a program used for sending messages to other computer users based on e-mail addresses.

o It provides a mail exchange between users on the same or different computers, and it also supports:

o It can send a single message to one or more recipients.

o Sending message can include text, voice, video or graphics. o It can also send the messages on networks outside the internet.

o The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

2. MIME :

Multipurpose Internet Mail Extensions

stands for Multipurpose Internet Mail Extensions. It is used to extend the capabilities of Internet e-mail protocols such as SMTP. The MIME protocol allows the users to exchange various types of digital content such as pictures, audio, video, and various types of documents and files in the e-mail. MIME was created in 1991 by a computer scientist named Nathan Borenstein at a company called Bell Communications.

Need of MIME Protocol : MIME protocol is used to transfer e-mail in the computer network for the following reasons:

1. The MIME protocol supports multiple languages in e-mail, such as Hindi, French, Japanese, Chinese, etc.

2. Simple protocols can reject mail that exceeds a certain size, but there is no word limit in MIME.

3. Images, audio, and video cannot be sent using simple e-mail protocols such as SMTP. These require MIME protocol.

4. Many times, emails are designed using code such as HTML and CSS, they are mainly used by companies for marketing their product. This type of code uses MIME to send email created from HTML and CSS.

3. SNMP :

SNMP stands for Simple Network Management Protocol.

o SNMP is a framework used for managing devices on the internet.

o It provides a set of operations for monitoring and managing the internet.

o SNMP has two components Manager and agent.

o The manager is a host that controls and monitors a set of agents such as routers.

o It is an application layer protocol in which a few manager stations can handle a set of agents.

o The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.

o It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways

4. HTTP :

The Hypertext Transfer Protocol (HTTP) is application-level protocol for collaborative, distributed, hypermedia information systems. It is the data communication protocol used to establish communication between client and server. HTTP is TCP/IP based communication protocol, which is used to deliver the data like image files, query results, HTML files etc on the World Wide Web (WWW) with the default port is TCP 80. It provides the standardized way for computers to communicate with each other.

The Basic Characteristics of HTTP (Hyper Text Transfer Protocol):

o It is the protocol that allows web servers and browsers to exchange data over the web.

o It is a request response protocol.

o It uses the reliable TCP connections by default on TCP port 80.

o It is stateless means each request is considered as the new request. In other words, server doesn't recognize the user by default.

Features :

HTTP is media independent: It specifies that any type of media content can be sent by HTTP as long as both the server and the client can handle the data content.

HTTP is connectionless: It is a connectionless approach in which HTTP client i.e., a browser initiates the HTTP request and after the request is sent the client disconnects from server and waits for the response.

HTTP is stateless: The client and server are aware of each other during a current request only. Afterwards, both of them forget each other. Due to the stateless nature of protocol, neither the client nor the server can retain the information about different request across the web pages.

5. FTP :

FTP stands for **File transfer protocol.**

o FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

o It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

o It is also used for downloading the files to computer from other servers.

Advantages :

o **Speed**: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.

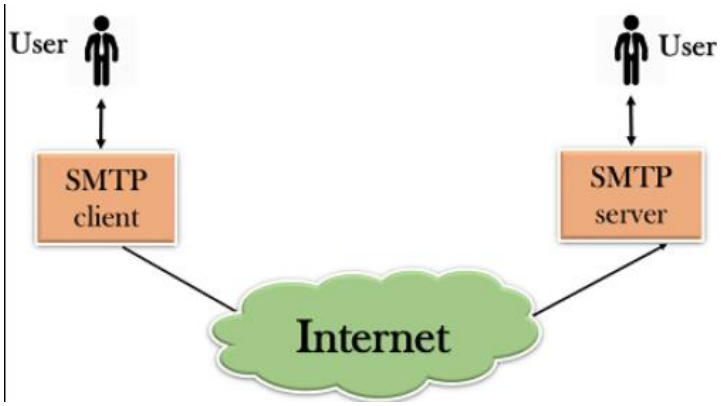
o **Efficient**: It is more efficient as we do not need to complete all the operations to get the entire file.
o **Security**: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

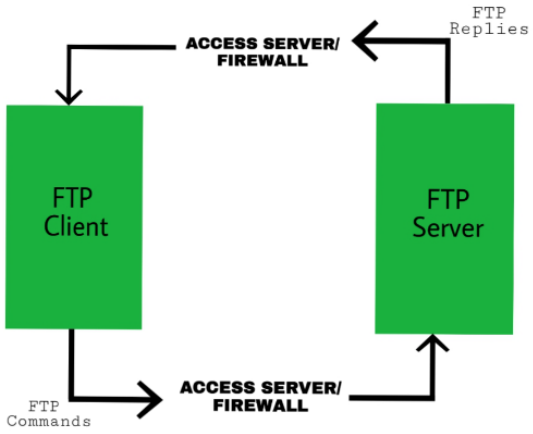
o **Back & forth movement**: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Comparison :

Parameter	HTTP	FTP	SMTP
Port number	80	20 and 21	25
Type of band transfer	In-band	Out-of-band	In-band
State	Stateless	Maintains state	–
Number of TCP connections	1	2 (Data Connection and Control Connection)	1
Type of TCP connection	Can use both Persistent and Non-persistent	Persistent for Control connection. Non-persistent for Data Connection	Persistent
Type of Protocol	Pull Protocol (Mainly)	–	Push Protocol (Primarily)
Type of Transfer	Transfer files between the Web server and Web client	Transfer directly between computers	Transfers mails via Mail Servers

Draw :





Q.3 Explain draw and compare SCTP, RTP, UDP and TCP

Ans.

1. SCTP :

SCTP stands for **Stream Control Transmission Protocol**.

It is a connection- oriented protocol in computer networks which provides a full-duplex association i.e., transmitting multiple streams of data between two end points at the same time that have established a connection in network. It is sometimes referred to as next generation TCP or TCPng, SCTP makes it easier to support telephonic conversation on Internet. A telephonic conversation requires transmitting of voice along with other data at the same time on both ends, SCTP protocol makes it easier to establish reliable connection.

SCTP is also intended to make it easier to establish connection over wireless network and managing transmission of multimedia data. SCTP is a standard protocol (RFC 2960) and is developed by Internet Engineering Task Force (IETF).

Advantages of SCTP :

1. It is a full- duplex connection i.e. users can send and receive data simultaneously.
2. It allows half- closed connections.
3. The message's boundaries are maintained and application doesn't have to split messages.
4. It has properties of both TCP and UDP protocol.
5. It doesn't rely on IP layer for resilience of paths.

2. RTP : Real Time Transport Protocol

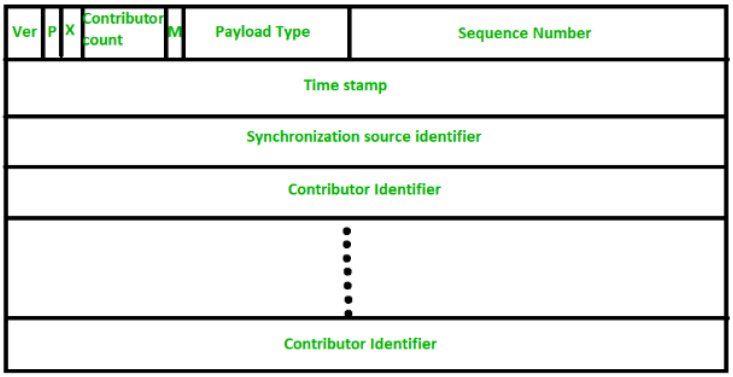
A protocol is designed to handle real-time traffic (like audio and video) of the Internet, is known as Real Time Transport Protocol (RTP). RTP must be used with UDP. It does not have any delivery mechanism like multicasting or port numbers. RTP supports different formats of files like MPEG and

MJPEG. It is very sensitive to packet delays and less sensitive to packet loss. History of RTP : This protocol is developed by Internet Engineering Task Force (IETF) of four members:

1. S. Casner (Packet Design)
2. V. Jacobson (Packet Design)
3. H. Schulzrinne (Columbia University)
4. R. Frederick (Blue Coat Systems Inc.)

RTP is first time published in 1996 and known as RFC 1889. And next it published in 2003 with name of RFC 3550. Applications of RTP :

1. RTP mainly helps in media mixing, sequencing and time-stamping.
2. Voice over Internet Protocol (VoIP)
3. Video Teleconferencing over Internet.
4. Internet Audio and video streaming.



3. UDP

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.The UDP enables process to process communication.

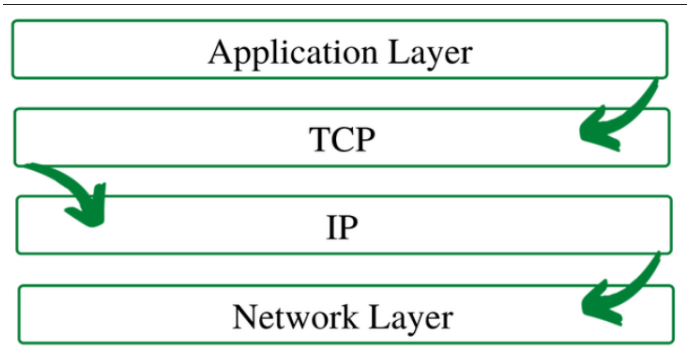
Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of the Internet services; provides assured delivery, reliability, and much more but all these services cost us additional overhead and latency. Here, UDP comes into the picture. For real-time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth.
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

UDP Header –

UDP header is an 8-bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contains all necessary header information and the remaining part consist of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.

4. TCP

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.



Working of TCP

To make sure that each message reaches its target location intact, the TCP/IP model breaks down the data into small bundles and afterward reassembles the bundles into the original message on the opposite end. Sending the information in little bundles of information makes it simpler to maintain efficiency as opposed to sending everything in one go.

After a particular message is broken down into bundles, these bundles may travel along multiple routes if one route is jammed but the destination remains the same.

Difference :

Protocol	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)	SCTP (Stream Control Transmission Protocol)
Reliability	Reliable data delivery with error detection, retransmission, and acknowledgement mechanisms	Unreliable data delivery without error recovery or acknowledgement	Reliable data delivery with error detection, retransmission, and acknowledgement mechanisms
Connection Type	Connection-oriented	Connectionless	Connection-oriented
Ordering	Guarantees ordered delivery of data packets	Does not guarantee the ordered delivery of data packets	Guarantees ordered delivery of data packets
Speed	Slower due to reliability mechanisms	Faster due to minimal overhead	Comparable to TCP, slower than UDP due to additional functionality
Overhead	Higher overhead due to additional headers and control mechanisms	Lower overhead due to minimal headers and control mechanisms	Moderate overhead due to additional headers and control mechanisms
Applications	Web browsing, email transfer, file transfer (FTP)	Real-time communication, video streaming, online gaming, DNS	Telecommunications, voice and video over IP, signalling transport
Congestion Control	Implements congestion control mechanisms to optimize network performance	No congestion control mechanisms	Implements congestion control mechanisms to optimize network performance
Error Recovery	Detects and retransmits lost or corrupted packets	No error recovery mechanisms	Detects and retransmits lost or corrupted packets
Message-Oriented Delivery	No	No	Yes, supports message-oriented delivery
Multi-streaming	No	No	Yes, supports the simultaneous transmission of multiple streams
Multi-homing	No	No	Yes, supports multiple IP addresses for fault tolerance and resilience

Q.4 TCP Collection Establishment and connection release with diagram and explanation.

Ans. TCP is a connection-oriented protocol and every connection-oriented protocol needs to establish a connection in order to reserve resources at both the communicating ends.

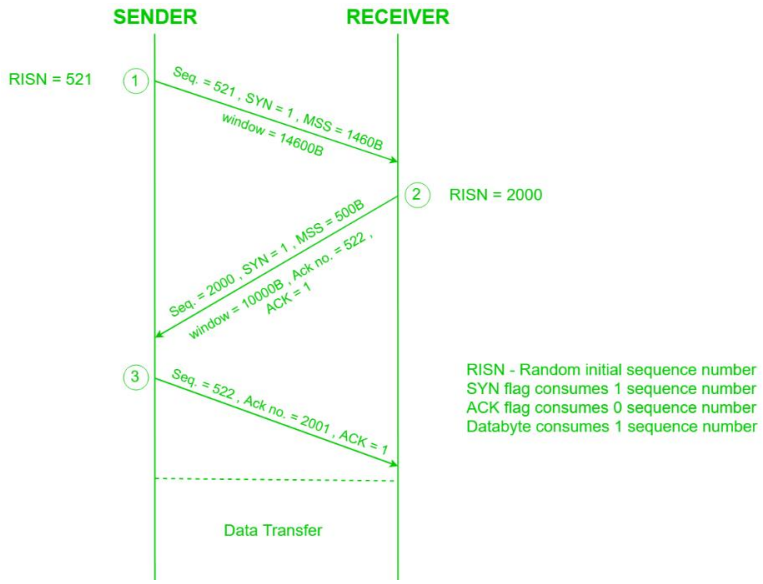
Connection Establishment –

1. Sender starts the process with the following:

- Sequence number (Seq = 521): contains the random initial sequence number generated at the sender side.
- Syn flag (Syn=1): request the receiver to synchronize its sequence number with the above-provided sequence number.
- Maximum segment size (MSS=1460 B): sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside Option field in TCP header.
- Window size (window=14600 B): sender tells about his buffer capacity in which he has to store messages from the receiver.

2. TCP is a full-duplex protocol so both sender and receiver require a window for receiving messages from one another.

- Sequence number (Seq = 2000): contains the random initial sequence number generated at the receiver side.
- Syn flag (Syn=1): request the sender to synchronize its sequence number with the above-provided sequence number.
- Maximum segment size (MSS=500 B): receiver tells its maximum segment size, so that sender sends datagram which won't require any fragmentation. MSS field is present inside Option field in TCP header.
  Since $MSS_{receiver} < MSS_{sender}$, both parties agree for minimum MSS i.e., 500 B to avoid fragmentation of packets at both ends.



Q.5 Transport layer responsibilities.

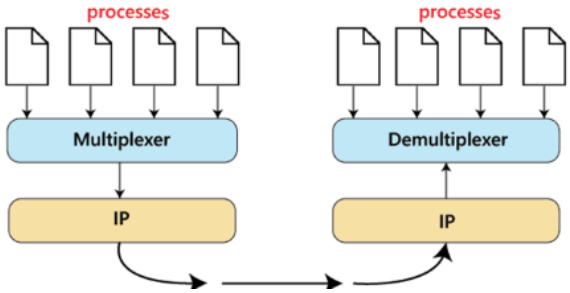
Ans.

Responsibilities of a Transport Layer

- The Process to Process Delivery
- End-to-End Connection between Hosts
- Multiplexing and Demultiplexing
- Congestion Control
- Data integrity and Error correction
- Flow control

1. The Process to Process Delivery

While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and the Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16-bit address used to identify any client-server program uniquely.



2. End-to-end Connection between Hosts

The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-orientated protocol that uses a handshake protocol to establish a robust connection between two end hosts. TCP ensures the reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol that ensures best-effort delivery. It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.

3. Multiplexing and Demultiplexing

Multiplexing(many to one) is when data is acquired from several processes from the sender and merged into one packet along with headers and sent as a single packet. Multiplexing allows the simultaneous use of different processes over a network that is running on a host. The processes are differentiated by their port numbers. Similarly, Demultiplexing(one to many is required at the receiver side when the message is distributed into different processes. Transport receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.

4. Congestion Control

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occurs. As a result, the retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open-loop congestion control to prevent congestion and closed-loop congestion control to remove the congestion in a network once it occurred. TCP provides AIMD – additive increases multiplicative decrease and leaky bucket technique for congestion control.

5. Data integrity and Error Correction

The transport layer checks for errors in the messages coming from the application layer by using error detection codes, and computing checksums, it checks whether the received data is not

corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.

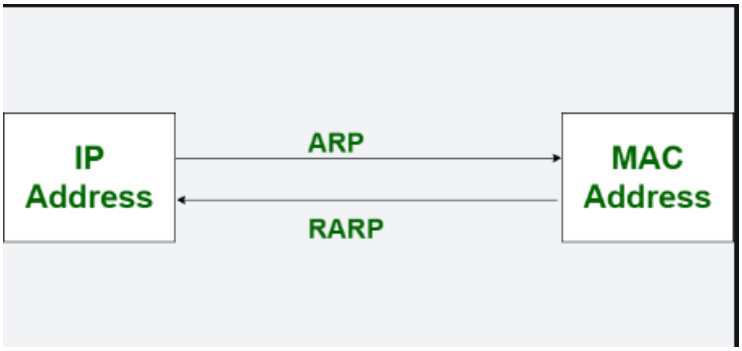
6. Flow Control

The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

Q.6 draw compare and explain ARP protocol and RARP .

Ans.

ARP : In Address Resolution Protocol (ARP), Receiver's MAC address is fetched. Through ARP, (32-bit) IP address mapped into (48-bit) MAC address. Whereas, In Reverse Address Resolution Protocol (RARP), IP address is fetched through server. Through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.



The **Reverse Address Resolution Protocol** (RARP) is a networking protocol that is used to map a physical (MAC) address to an Internet Protocol (IP) address. It is the reverse of the more commonly used Address Resolution Protocol (ARP), which maps an IP address to a MAC address.

RARP was developed in the early days of computer networking as a way to provide IP addresses to diskless workstations or other devices that could not store their own IP addresses. With RARP, the device would broadcast its MAC address and request an IP address, and a RARP server on the network would respond with the corresponding IP address.

While RARP was widely used in the past, it has largely been replaced by newer protocols such as DHCP (Dynamic Host Configuration Protocol), which provides more flexibility and functionality in assigning IP addresses dynamically. However, RARP is still used in some specialized applications, such as booting embedded systems and configuring network devices with pre-assigned IP addresses.

ARP	RARP
A protocol used to map an IP address to a physical (MAC) address	A protocol used to map a physical (MAC) address to an IP address
To obtain the MAC address of a network device when only its IP address is known	To obtain the IP address of a network device when only its MAC address is known
Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address	Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address
IP addresses	MAC addresses
Widely used in modern networks to resolve IP addresses to MAC addresses	Rarely used in modern networks as most devices have a pre-assigned IP address
ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.
Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.	Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.
In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
In Address Resolution Protocol, Receiver's MAC address is fetched.	While in RARP, IP address is fetched.
In ARP, ARP table uses ARP reply for its updation.	While in RARP, RARP table uses RARP reply for configuration of IP addresses .
Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks.	While RARP is used by small users having less facilities.
ARP is used in sender's side to map the receiver's MAC address.	RARP is used in receiver's side to map the sender's IP.

Q.7 Compare and explain Static and dynamic routing

Ans. Static Routing:

Static Routing is also known as non-adaptive routing which doesn't change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.

Dynamic Routing:

Dynamic routing is also known as **adaptive** routing which changes the routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing. When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.

S.NO	Static Routing	Dynamic Routing
1.	In static routing routes are user-defined.	In dynamic routing, routes are updated according to the topology.
2.	Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
3.	Static routing provides high or more security.	Dynamic routing provides less security.
4.	Static routing is manual.	Dynamic routing is automated.
5.	Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
6.	In static routing, additional resources are not required.	In dynamic routing, additional resources are required.
7.	In static routing, failure of the link disrupts the rerouting.	In dynamic routing, failure of the link does not interrupt the rerouting.
8.	Less Bandwidth is required in Static Routing.	More Bandwidth is required in Dynamic Routing.
9.	Static Routing is difficult to configure.	Dynamic Routing is easy to configure.
10.	Another name for static routing is non-adaptive routing.	Another name for dynamic routing is adaptive routing.

Q.8 Compare draw and explain IPV4 and IPV6

Ans. IPv4

IPv4 address consists of two things that are the network address and the host address. It stands for Internet Protocol version four. It was introduced in 1981 by DARPA and was the first deployed version in 1982 for production on SATNET and on the ARPANET in January 1983.

IPv4 addresses are 32-bit integers that have to be expressed in Decimal Notation. It is represented by 4 numbers separated by dots in the range of 0-255, which have to be converted to 0 and 1, to be understood by Computers. For Example, An IPv4 Address can be written as 189.123.123.90.

IPv6

IPv6 is based on IPv4 and stands for Internet Protocol version 6. It was first introduced in December 1995 by Internet Engineering Task Force. IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 Address Format

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29×10^{9} address space	The address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Q.9 Explain subnetting with example.

Ans. When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

Uses of Subnetting

1. Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
2. Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
3. Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
4. Subnetting is used in increasing network security.

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.

How Does Subnetting Work?

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

Example :

- **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus, the range of subnet 1 is: 193.1.2.0 to 193.1.2.127

Subnet id of Subnet-1 is : 193.1.2.0

The direct Broadcast id of Subnet-1 is: 193.1.2.127

The total number of hosts possible is: 126 (Out of 128,

2 id's are used for Subnet id & Direct Broadcast id)

The subnet mask of Subnet- 1 is: 255.255.255.128

Q.10 Explain CIDR, Mobile IP, ICMP

Ans.

CIDR :

CIDR stands for Classless Inter-Domain Routing. It is an IP address assigning method that improves the efficiency of address distribution. It is also known as supernetting that replaces the older system based on classes A, B, and C networks. By using a single CIDR IP address many unique IP addresses can be designated. CIDR IP address is the same as the normal IP address except that it ends with a slash followed by a number.

Characteristics of CIDR

It dynamically allocates the IP addresses by using CIDR blocks on the requirement of the user based on certain rules. The assignment of the CIDR block is handled by the Internet Assigned Number Authority (IANA). CIDR block consists of IP addresses and it consists of some rules:

- All IP addresses which are allocated to host must be continuous.
- The block size must be of power 2 and equal to the total number of IP addresses.
- The size of the block must be divisible by the first IP address of the block.

Advantages

- CIDR provide efficient address space allocation i.e. with CIDR addresses are allocated in sizes of any binary multiple.
- It eliminates the class imbalance, i.e. there are no more class networks so you can widely use some portion of the address space and neglect others.
- It allows efficient routing entries i.e. a Large number of networks can be represented by a small number of routing entries.

Mobile IP

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped.

Terminologies:

1. Mobile Node (MN) is the hand-held communication device that the user carries e.g. Cell phone.
2. Home Network is a network to which the mobile node originally belongs as per its assigned IP address (home address).
3. Home Agent (HA) is a router in-home network to which the mobile node was originally connected
4. Home Address is the permanent IP address assigned to the mobile node (within its home network).

5. Foreign Network is the current network to which the mobile node is visiting (away from its home network).
6. Foreign Agent (FA) is a router in a foreign network to which the mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node.
7. Correspondent Node (CN) is a device on the internet communicating to the mobile node.
8. Care-of Address (COA) is the temporary address used by a mobile node while it is moving away from its home network.
9. Foreign agent COA, the COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as a common COA.
10. Co-located COA, the COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.

ICMP

Internet Control Message Protocol (ICMP) is a network layer protocol used to diagnose communication errors by performing an error control mechanism. Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide error control.

ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information. For example, the requested service is not available or a host or router could not be reached.

Uses of ICMP

ICMP is used for error reporting if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error. For Example, whenever a device sends any message which is large enough for the receiver, in that case, the receiver will drop the message and reply back ICMP message to the source.

Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility.

Working

ICMP is the primary and important protocol of the IP suite, but ICMP isn't associated with any transport layer protocol (TCP or UDP) as it doesn't need to establish a connection with the destination device before sending any message as it is a connectionless protocol.

Q.11 Draw an explain sliding window protocol silly windows Syndrome.

Ans.

Sliding window protocol :

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

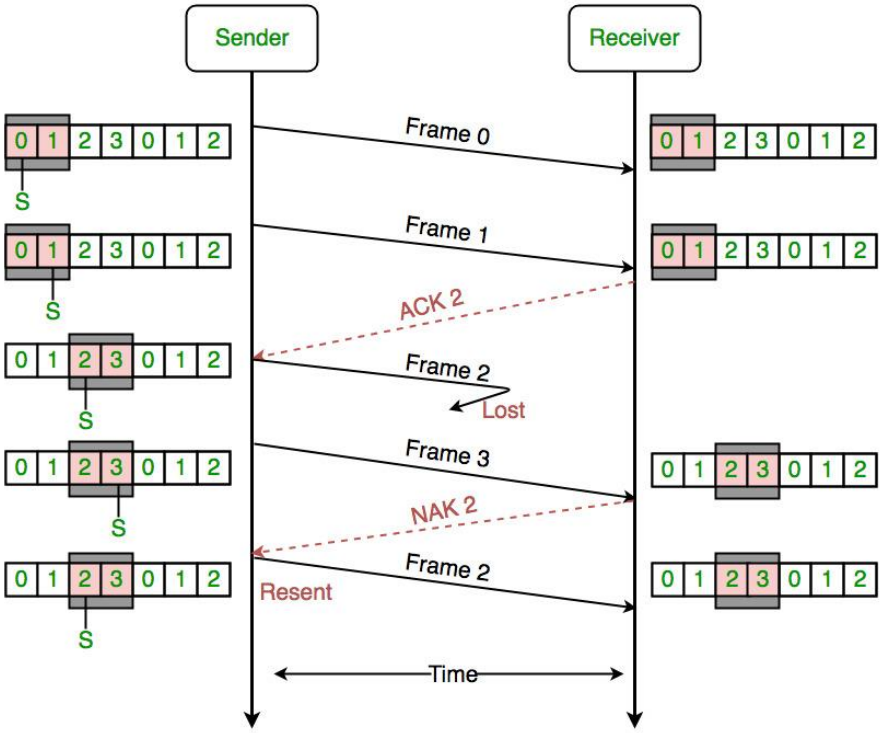
In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n–1. Consequently, the size of the sending window is 2^n–1. Thus in order to accommodate a sending window size of 2^n–1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.



Silly Window Syndrome is a problem that arises due to poor implementation of TCP. It degrades the TCP performance and makes the data transmission extremely inefficient. The problem is called so because:

1. It causes the sender window size to shrink to a silly value.
2. The window size shrinks to such an extent that the data being transmitted is smaller than TCP Header.

What are the causes?
The two major causes of this syndrome are as follows:

1. Sender window transmitting one byte of data repeatedly.
2. Receiver window accepting one byte of data repeatedly.

Cause-1: Sender window transmitting one byte of data repeatedly –
Suppose only one byte of data is generated by an application . The poor implementation of TCP leads to transmit this small segment of data.Every time the application generates a byte of data, the window transmits it. This makes the transmission process slow and inefficient.The problem is solved by Nagle's algorithm.

Nagle's algorithm suggests:

1. Sender should send only the first byte on receiving one byte data from the application.
2. Sender should buffer all the rest bytes until the outstanding byte gets acknowledged.
3. In other words, sender should wait for 1 RTT(Round Trip Time).

After receiving the acknowledgement, sender should send the buffered data in one TCP segment. Then, sender should buffer the data again until the previously sent data gets acknowledged.

Cause-2: Receiver window accepting one byte of data repeatedly –
Suppose consider the case when the receiver is unable to process all the incoming data.In such a case, the receiver will advertise a small window size.The process continues and the window size becomes smaller and smaller.A stage arrives when it repeatedly advertises window size of 1 byte.This makes receiving process slow and inefficient.The solution to this problem is Clark's Solution.

Clark's solution suggests:

1. Receiver should not send a window update for 1 byte.
2. Receiver should wait until it has a decent amount of space available.
3. Receiver should then advertise that window size to the sender

Q.12 Distance vector routing algorithm.

Ans. A distance-vector routing (DVR) protocol requires that a router inform its neighbours of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances, based on a chosen metric, are computed using information from the neighbours' distance vectors**.**

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbours in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbours.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbour containing different information than before.
    - It discovers that a link to a neighbour has gone down.

Q.13 Explain classfull addresses.

Ans. Classful addressing was an outdated system used in the early days of the internet to assign IP addresses in the IPv4 protocol. It divided the 32-bit address space into five classes (A, B, C, D, and E) based on the number of hosts and networks they could support. Each class had a predefined bitmask that determined the size of the network and host portions of the address.

Class A: These addresses were used for large networks with a massive number of hosts, typically assigned to governments, corporations, and universities. The first 8 bits were for the network ID, leaving 24 bits for hosts (a total of 16,777,214 hosts).

Class B: These addresses were for medium-sized networks with a moderate number of hosts, often assigned to businesses and organizations. The first 16 bits were for the network ID, leaving 16 bits for hosts (a total of 65,536 hosts).

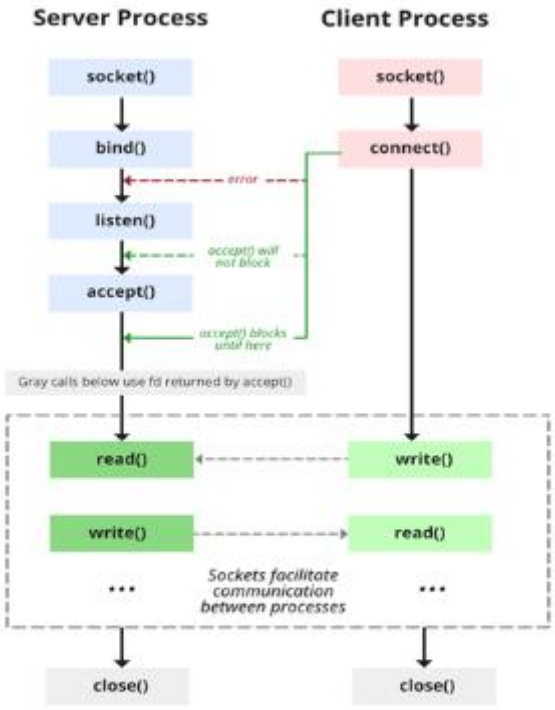
Class B: These addresses were for medium-sized networks with a moderate number of hosts, often assigned to businesses and organizations. The first 16 bits were for the network ID, leaving 16 bits for hosts (a total of 65,536 hosts).

Class D: These addresses were reserved for multicasting, a special type of communication where a single source sends data to a group of destinations simultaneously.

Class E: This class was originally reserved for future use but is currently not assigned.

Q.14 Explain socket programming.

Ans. Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while the other socket reaches out to the other to form a connection. The server forms the listener socket while the client reaches out to the server.



State diagram for server and client model of Socket

1. Socket creation:

- sockfd: socket descriptor, an integer (like a file-handle)
- domain: integer, specifies communication domain. We use AF_ LOCAL as defined in the POSIX standard for communication between processes on the same host. For communicating between processes on different hosts connected by IPV4, we use AF_INET and AF_I NET 6 for processes connected by IPV6.
- type: communication type
  SOCK_STREAM: TCP(reliable, connection oriented)
  SOCK_DGRAM: UDP(unreliable, connectionless)
- protocol: Protocol value for Internet Protocol(IP), which is 0. This is the same number which appears on protocol field in the IP header of a packet.(man protocols for more details)

2. Setsockopt:

This helps in manipulating options for the socket referred by the file descriptor sockfd. This is completely optional, but it helps in reuse of address and port. Prevents error such as: “address already in use.

3. Bind :

After the creation of the socket, the bind function binds the socket to the address and port number specified in addr(custom data structure). In the example code, we bind the server to the localhost, hence we use INADDR_ANY to specify the IP address.

4.**Listen** :

It puts the server socket in a passive mode, where it waits for the client to approach the server to make a connection. The backlog, defines the maximum length to which the queue of pending connections for sockfd may grow. If a connection request arrives when the queue is full, the client may receive an error with an indication of ECONNREFUSED.

5. Accept:

It extracts the first connection request on the queue of pending connections for the listening socket, sockfd, creates a new connected socket, and returns a new file descriptor referring to that socket. At this point, the connection is established between client and server, and they are ready to transfer data.

Q.15 Difference between TCP and UDP

Ans.

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is a message stream.
Overhead	Low but higher than UDP.	Very low.
Applications	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.	This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc.

Q.16 Draw explain and compare CSMA, WDMA, CSMA/CD, CSMA/CA

Ans.

CSMA : Carrier Sense Multiple Access

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station first check the state of the medium before sending.

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the transmission is finished, if not, the frame is sent again.

2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

Characteristics of CSMA/CA :

1. **Carrier Sense**: The device listens to the channel before transmitting, to ensure that it is not currently in use by another device.
2. **Multiple Access**: Multiple devices share the same channel and can transmit simultaneously.
3. **Collision Avoidance**: If two or more devices attempt to transmit at the same time, a collision occurs. CSMA/CA uses random backoff time intervals to avoid collisions.
4. **Acknowledgment (ACK)**: After successful transmission, the receiving device sends an ACK to confirm receipt.
5. **Fairness**: The protocol ensures that all devices have equal access to the channel and no single device monopolizes it.
6. **Binary Exponential Backoff**: If a collision occurs, the device waits for a random period of time before attempting to retransmit. The backoff time increases exponentially with each retransmission attempt.
7. **Interframe Spacing**: The protocol requires a minimum amount of time between transmissions to allow the channel to be clear and reduce the likelihood of collisions.
8. **RTS/CTS Handshake**: In some implementations, a Request-To-Send (RTS) and Clear-To-Send (CTS) handshake is used to reserve the channel before transmission. This reduces the chance of collisions and increases efficiency.
9. **Wireless Network Quality**: The performance of CSMA/CA is greatly influenced by the quality of the wireless network, such as the strength of the signal, interference, and network congestion.

WDMA : TDMA

Time Division Multiple Access (TDMA) is a complex technology, because it requires an accurate synchronization between the transmitter and the receiver. TDMA is used in digital mobile radio systems. The individual mobile stations cyclically assign a frequency for the exclusive use of a time interval.

In most of the cases, the entire system bandwidth for an interval of time is not assigned to a station. However, the frequency of the system is divided into sub-bands, and TDMA is used for the multiple access in each sub-band. Sub-bands are known as carrier frequencies. The mobile system that uses this technique is referred as the multi-carrier systems

Advantages of TDMA

Here is a list of few notable advantages of TDMA −

- Permits flexible rates (i.e. several slots can be assigned to a user, for example, each time interval translates 32Kbps, a user is assigned two 64 Kbps slots per frame).
- Can withstand gusty or variable bit rate traffic. Number of slots allocated to a user can be changed frame by frame (for example, two slots in the frame 1, three slots in the frame 2, one slot in the frame 3, frame 0 of the notches 4, etc.).
- No guard band required for the wideband system.
- No narrowband filter required for the wideband system.

Disadvantages of TDMA

The disadvantages of TDMA are as follow −

High data rates of broadband systems require complex equalization.

Due to the burst mode, a large number of additional bits are required for synchronization and supervision.

Call time is needed in each slot to accommodate time to inaccuracies (due to clock instability).

Electronics operating at high bit rates increase energy consumption.

Complex signal processing is required to synchronize within short slots**.**

S.NO	CSMA/CD	CSMA/CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).
7	It is the type of CSMA to detect the collision on a shared channel.	It is the type of CSMA to avoid collision on a shared channel.
8.	It is work in MAC layer.	It is also work in MAC layer.

Q.17 Explain binary exponential backoff algorithm.

Ans. Binary Exponential Backoff Algorithm Explained

Binary exponential backoff (BEB) is a powerful algorithm used in various situations to manage retries or retransmissions after failures. It's particularly common in network protocols and concurrent systems to handle collisions or resource contention. Here's how it works:

The Core Idea:

- When a failure occurs (e.g., a collision in a network), the entity (e.g., a device) involved waits for a random amount of time before retrying.
- This waiting time, called the backoff interval, is crucial to avoid further collisions and achieve efficient resource utilization.

- BEB makes the backoff interval grow exponentially with each consecutive failure. This discourages multiple entities from retrying at the same time, increasing the chance of successful retransmission.

How it Works:

1. Initial Backoff: After the first failure, the entity chooses a random number within a specific range (usually 0 to a small value, like 2).
2. Exponential Increase: If a retry fails again, the range for choosing the random backoff value is doubled. This means the potential wait time increases significantly.
3. Maximum Limit: Typically, there's an upper limit to the backoff interval to prevent excessive delays and wasted resources.

Benefits of BEB:

- Reduces collisions: By spreading out retries, BEB minimizes the chance of multiple entities trying to access the same resource at the same time, leading to fewer collisions and smoother operation.
- Fairness: Entities that experience more failures back off for longer, giving others a higher chance of success, promoting fair access to resources.
- Robustness: BEB adapts to changing conditions by automatically adjusting the backoff intervals based on the failure rate.

Applications of BEB:

- Ethernet: BEB is used in CSMA/CD (Carrier Sense Multiple Access with Collision Detection) to resolve collisions when multiple devices try to transmit data simultaneously.
- Distributed Systems: BEB is used in algorithms like Paxos and Raft to ensure consensus and avoid conflicts during leader election or data replication.
- Messaging Systems: BEB helps prevent message flooding and ensures efficient message delivery in systems like RabbitMQ or Kafka.

Q.18 Go-Back-N ARQ and selective repeat ARQ

Ans. Go back N ARQ

The Go-Back-N protocol is a sliding window protocol used for reliable data transfer in computer networks. It is a sender-based protocol that allows the sender to transmit multiple packets without waiting for an acknowledgement for each packet. The receiver sends a cumulative acknowledgement for a sequence of packets, indicating the last correctly received packet. If any packet is lost, the receiver sends a negative acknowledgement (NACK) for the lost packet, and the sender retransmits all the packets in the window starting from the lost packet. The sender also maintains a timer for each packet, and if an acknowledgement is not received within the timer’s timeout period, the sender retransmits all packets in the window.

The key features of the Go-Back-N (GBN) protocol include:

- Sliding window mechanism
- Sequence numbers
- Cumulative acknowledgements
- Timeout mechanism
- NACK mechanism
- Simple implementation.

Selective Repeat Protocol:

The Selective Repeat protocol is another sliding window protocol used for reliable data transfer in computer networks. It is a receiver-based protocol that allows the receiver to acknowledge each packet individually, rather than a cumulative acknowledgement of a sequence of packets. The sender sends packets in a window and waits for acknowledgements for each packet in the window. If a packet is lost, the receiver sends a NACK for the lost packet, and the sender retransmits only that packet. The sender also maintains a timer for each packet, and if an acknowledgement is not received within the timer's timeout period, the sender retransmits only that packet.

S.NO	Go-Back-N Protocol	Selective Repeat Protocol
1.	In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	In selective Repeat protocol, only those frames are re-transmitted which are found suspected.
2.	Sender window size of Go-Back-N Protocol is N.	Sender window size of selective Repeat protocol is also N.
3.	Receiver window size of Go-Back-N Protocol is 1.	Receiver window size of selective Repeat protocol is N.
4.	Go-Back-N Protocol is less complex.	Selective Repeat protocol is more complex.
5.	In Go-Back-N Protocol, neither sender nor at receiver need sorting.	In selective Repeat protocol, receiver side needs sorting to sort the frames.
6.	In Go-Back-N Protocol, type of Acknowledgement is cumulative.	In selective Repeat protocol, type of Acknowledgement is individual.
7.	In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.	In selective Repeat protocol, Out-of-Order packets are Accepted.
8.	In Go-Back-N Protocol, if Receives a corrupt packet, then also, the entire window is re-transmitted.	In selective Repeat protocol, if Receives a corrupt packet, it immediately sends a negative acknowledgement and hence only the selective packet is retransmitted.
9.	Efficiency of Go-Back-N Protocol is `N/(1+2*a)`	Efficiency of selective Repeat protocol is also `N/(1+2*a)`

Q.19 Design issues of data link layer.

Ans. Design issues with data link layer are :

1. Services provided to the network layer –
The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).

It provides three types of services:

1. Unacknowlwdged and connectionless services.
2. Acknowledged and connectionless services.
3. Acknowledged and connection-oriented services

Unacknowledged and connectionless services.

- Here the sender machine sends the independent frames without any acknowledgement from the sender.
- There is no logical connection established.

Acknowledged and connectionless services.

- There is no logical connection between sender and receiver established.
- Each frame is acknowledged by the receiver.
- If the frame didn't reach the receiver in a specific time interval it has to be sent again.
- It is very useful in wireless systems.

Acknowledged and connection-oriented services

- A logical connection is established between sender and receiver before data is trimester.
- Each frame is numbered so the receiver can ensure all frames have arrived and exactly once.

2. Frame synchronization –
The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.

3. Flow control –
Flow control is done to prevent the flow of data frame at the receiver end. The source machine **must** not send data frames at a rate faster than the capacity of destination machine to accept them.

4. Error control –
Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Q.20 AODV and IGMP

Ans. Ad hoc On-Demand Distance Vector routing(AODV) –
Since AODV is a reactive (or on-demand) MANET routing protocol, it only keeps routes that have a demand in the network. For reaching destinations, AODV holds a routing table with the next hop. If no packets are sent on a path, they will time out after a while. It only consists of information about its neighbor nodes so re-transferring the data frames might take more time.

Types of routing in AODV :
It consists of 3 types of routing messages as follows.

1. **RREQ: Route Request –**
   A node, Initiates to send/transmit a packet but doesn't know how to get there, it sends an RREQ multicast message to start the route discovery process. Neighboring nodes keep track of where the message originated and move it on to their neighbors before it reaches the destination node.

2. **RREP: Route Reply –**
   The destination node responds with an RREP, which returns to the source through the path taken by the RREQ. As the RREP returns to the source, forward routes are formed in the intermediate nodes. If an intermediate node knows the path to the destination, it may send an RREP in response to a received RREQ, allowing nodes to enter an established route. Communication between the source and the destination will begin once the RREP arrives at the source and the route is established.

3. **REER: Route Error –**
   AODV typically has less overhead as a reactive protocol (less route maintenance messages) than proactive. In the event of the connection interruption that the path no longer functions, i.e. messages cannot be sent, a RERR message is sent through a node detecting the link interruption. The message is re-cast by other nodes. The RERR message shows the unattainable destination. Message receiving nodes inactivates the route.

IGMP

IGMP is acronym for **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as IGMPv2 and MLDv2 is almost similar to IGMPv3. The communication protocol, IGMPv1 was developed in 1989 at Stanford University. IGMPv1 was updated to IGMPv2 in year 1997 and again updated to IGMPv3 in year 2002.

The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group. IGMP is a part of the IP layer and IGMP has a fixed- size message. The IGMP message is encapsulated within an IP datagram.

The IP protocol supports two types of communication:

- Unicasting- It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
- Multicasting: Sometimes the sender wants to send the same message to a large of receivers simultaneously. This process is known as multicasting which has one-to-many communication.