**Computer Network**

**Explain osi 7 layer model. With diagram**

(Diagram)

OSI stands for Open Systems Interconnection. It is a 7 layer architecture with each layer having specific functionality to perform

Physical layer: The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next

Data Link Layer:The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host

Network Layer: Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP address are placed in the header by the network layer.

Transport Layer: Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

Session Layer: This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

Presentation Layer: Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Application Layer: At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.  
Ex: Application – Browsers, Skype Messenger etc.

**2.Explain working of FDM with its limitations**

In FDM, the total bandwidth is divided to a set of frequency bands that do not overlap. Each of these bands is a carrier of a different signal that is generated and modulated by one of the sending devices. The frequency bands are separated from one another by strips of unused frequencies called the guard bands, to prevent overlapping of signals.

The modulated signals are combined together using a multiplexer (MUX) in the sending end. The combined signal is transmitted over the communication channel, thus allowing multiple independent data streams to be transmitted simultaneously

Limitations : All the frequency division multiplexing channels get affected due to wideband fading.

A large number of modulators and filters are required.

The communication channel must have a very large bandwidth.

The frequency division multiplexing suffers from the problem of crosstalk

**3.Briefly explain computer application**

business applications of computer networks:

1. Resource Sharing:

The goal is to make all programs, equipments(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

#### Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called **Servers** the employees have simple machines, called **Clients**, on their desks, using which they access remote data.

#### 3. Communication Medium:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

#### 4. eCommerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

Home Applications

1. Internet access provides home users with connectivity to remote computers. As with companies, home users can access information, communicate with other people and buy products and services with e-commerce. Access to remote information comes in many forms. It can be surfing the World Wide Web for information or just for fun
2. Many newspapers have gone online and can be personalized. The next step beyond newspapers is the online digital library. Electronic book readers and online libraries may make printed books obsolete
3. The peer to peer computing architecture contains nodes that are equal participants in data sharing. All the tasks are equally divided between all the nodes. The nodes interact with each other as required as share resources.
4. Entertainment: This has made huge strides in the home in recent years, with the distribution of music, radio and television programs, and movies over the Internet beginning to rival that of traditional mechanisms. Users can find, buy, and download MP3 songs and DVD-quality movies and add them to their personal collection.

4**. Explain the following**:

**Multiplexing**   
Gathering data from multiple application processes of sender, enveloping that data with header and sending them as a whole to the intended receiver is called as multiplexing.

**Demultiplexing**   
Delivering received segments at receiver side to the correct app layer processes is called as demultiplexing.

**Explain**

**LAN**: LAN is a network that connects computers and devices in a limited geographical area..The simplest form of LAN is to connect two computers together**.** Example: Home, school computer laboratory, office building or closely positioned group of buildings

Advantages of LAN:

 Easy to share devices such as printers, scanners etc.,

 Easy to share data such as pictures

Disadvantages of LAN:

Power-a good LAN is required to be all the times.

Security-each computer and device become another point of entry for undesirables

**MAN:**It is a high speed network that connects local area networks in a metropolitan area. Is larger than a LAN, but smaller than a WAN. Example: city or town handles the bulk of communication activity across that region.

Advantage

 Efficiency and shared access.

 All the computer-owing residents of the area have equal abiolity to go online.

Disadvantages:

 It can be costly.

 Security problem.

**WAN (**Wide area network):

 WAN is a network that covers a larger geographic area (such as a city, country, or world)

using a communications channel that combines many types of media such as telephone lines,

cables and radio waves. Example :internet

Advantages:

 Increased efficiency

 Ease of communication

 Lowered costs.

Disadvantages:

 Security problems.

 Training costs

 Maintenance problems.

**PAN** (Personal Area Network)

 PAN devices communicate over the range of a person.Used for data transmission among devices such as computers, telephones and personal digital assistants. The data cable is an example of PAN.

Example : blutooth, RFID tag

**Explain baseband and pass band transmission**

**Baseband Transmission** is a signaling technology that sends digital signals over a single frequency as discrete electrical pulses. The entire bandwidth of a baseband system carries only one data signal and is generally less than the amount of bandwidth available on a broadband transmission system.

The baseband signal is bidirectional so that a baseband system can both transmit and receive signals simultaneously.

NRZ (Non – Return to Zero)

NRZ is an unipolar coding scheme. Here, a high voltage represents 1, while a low voltage represents 0. Non-return to zero implies that the signal does not return to zero at the middle of the bit.

NRZ-I (NRZ Invert)

NRZ-I is an polar coding scheme. In NRZI, bit 1 is represented by a transition in voltage, while bit 0 is represented by no such transitions. It has an average signal rate of N/2 baud.

Manchester Encoding

Manchester encoding is a biphase coding scheme. Bit 1 is represented by a voltage transition from high to low, while bit 0 is represented by a voltage transition from low to high.

Bipolar Encoding

It is also called Alternate Mark Inversion or AMI. Three voltage levels are used here. Here, bit 0 is represented by no line signal, while bit 1 is represented by a positive or negative voltage level, alternating for successive ones

**passband transmission**, the amplitude, phase or frequency of the carrier signal is regulated to transmit the bits. The incoming data stream is modulated onto a carrier and then transmitted over a band-pass channel

Amplitude Shift Keying (ASK)

In ASK, the amplitude of the signal is varied to represent the signal levels, while frequency and phase remains constant

Frequency Shift Keying (FSK)

In FSK, the frequency of the signal is modulated to represent the signal levels, while amplitude and phase remains constant

Phase Shift Keying (PSK)

In PSK, the phase of the carrier signal is modulated to represent the signal levels, while amplitude and frequency remains constant

On packet-switched networks, which means that blocks of data (called frames at this level), not bit

streams, are exchanged between nodes. It is the network adaptor that enables the nodes to exchange

frames. There are several ways to address the framing problem.

**Binary Synchronous Communication (BISYNC)** is basically a character or byte-oriented form of communication which means that the groups of bits or bytes are the important elements of transmission rather than a stream of bits.

It generally includes characters and procedures for simply controlling the establishment or development of a valid connection and transmission of data. It is a half-duplex link protocol that has replaced the Synchronous transmit-receive (STR) protocol usually used with second-generation computers

1. **Error Detection Methods - Parity, Checksum, CRC (Sender & Receiver End)**

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the messag

Some popular techniques for error detection are:  
1. Simple Parity check  
2. Two-dimensional Parity check  
3. Checksum  
4. Cyclic redundancy check

**Simple Parity check**  
Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

* 1 is added to the block if it contains odd number of 1’s, and
* 0 is added if it contains even number of 1’s

This scheme makes the total number of 1’s even, that is why it is called even parity checking.

**Two-dimensional Parity check**  
Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data

**Checksum**

* In checksum error detection scheme, the data is divided into k segments each of m bits.
* In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.
* The checksum segment is sent along with the data segments.
* At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented.

**4. Cyclic redundancy check (CRC)**

* Unlike checksum scheme, which is based on addition, CRC is based on binary division.
* In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
* At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

**Error Correction Methods**

* **Backward Error Correction**  When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
* **Forward Error Correction**  When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

**Stop & Wait Protocol with various Scenarios**

Sender sends one data frame, waits for acknowledgement (ACK) from receiver before

proceeding to transmit next frame

– This simple flow control will break down if ACK gets lost or errors occur

→ Sender may wait for ACK that never arrives

For noisy link, pure stop and wait protocol will break down, and solution is to incorporate some error control mechanism

• Stop and wait with ARQ: Automatic Repeat request (ARQ), an error control method, is incorporated with stop and wait flow control protocol If error is detected by receiver, it discards the frame and send a negative ACK (NAK), causing sender to re-send the fram In case a frame never got to receiver, sender has a timer: each time a frame is sent, timer is set

→ If no ACK is received during timeout period, it re-sends the frame

Timer introduces a problem:

Suppose timeout and sender retransmits a frame but receiver actually received the previous transmission

→ Receiver has duplicated copies

– To avoid receiving and accepting

two copies of same frame, frames and

ACKs are alternatively labeled 0 or 1:

ACK0 for frame 1, ACK1 for frame 0

1. **Connection Oriented Service & Connectionless Service**
2. In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.
3. Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.
4. It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.
5. In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

**Virtual circuit**

**Virtual Circuit** is the computer network providing connection-oriented service. It is a connection-oriented network. In virtual circuit resource are reserve for the time interval of data transmission between two nodes. This network is a highly reliable medium of transfer.

**Working of Virtual Circuit:**

* In the first step a medium is set up between the two end nodes.
* Resources are reserved for the transmission of packets.
* Then a signal is sent to sender to tell the medium is set up and transmission can be started.
* It ensures the transmission of all packets.
* A global header is used in the first packet of the connection.
* Whenever data is to be transmitted a new connection is set up.

**Congestion control Mechanism**

**Congestion Control in Virtual Circuit:**  
Once the congestion is detected in virtual circuit network, closed-loop techniques is used. There are different approaches in this technique:

* **No new connection –**  
  No new connections are established when the congestion is detected. This approach is used in telephone networks where no new calls are established when the exchange is overloaded.
* **Participation of congested router invalid –**  
  Another approach to control congestion is allow all new connections but route these new connections in such a way that congested router is not part of this route.
* **Negotiation –**  
  To negotiate different parameters between sender and receiver of the network, when the connection is established. During the set up time, host specifies the shape and volume of the traffic, quality of service and other parameters.

Pv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device.

**IPv4 Header format**

**Diagram()**

***VERSION:****Version of the IP protocol (4 bits), which is 4 for IPv4*

***HLEN:****IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*

***Type of service:*** *Low Delay, High Throughput, Reliability (8 bits)*

***Total Length:****Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*

***Identification:****Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*

***Flags:****3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*

***Fragment Offset:****Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*

***Time to live:****Datagram’s lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*

***Protocol:****Name of the protocol to which the data is to be passed (8 bits)*

***Header Checksum:****16 bits header checksum for checking errors in the datagram header*

***Source IP address:****32 bits IP address of the sender*

***Destination IP address:****32 bits IP address of the receiver*

***Option:****Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

**Ipv6**

. IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes

In IPv6 representation, we have three addressing methods :

 Unicast

 Multicast

 Anycast

**Unicast Address:** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.  
**Multicast Address:** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.  
**Anycast Address:** Anycast Address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible).

**ARC Protocol**

The devices of the network peel the header of the data link layer from the **protocol data unit (PDU)** called frame and transfers the packet to the network layer (layer 3 of OSI) where the network ID of the packet is validated with the destination IP’s network ID of the packet and if it’s equal then it responds to the source with the MAC address of the destination, else the packet reaches the gateway of the network and broadcasts packet to the devices it is connected with and validates their network ID

The above process continues till the second last network device in the path to reach the destination where it gets validated and ARP, in turn, responds with the destination MAC address.

The important terms associated with ARP are : 

1. **ARP Cache:** After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table
2. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside
3. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not.
   1. The physical address of the sender.
   2. The IP address of the sender.
   3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1’s.
   4. The IP address of the receiver
4. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

**MODULE 4**

1. **UDP Datagram Format**

**User Datagram Protocol (UDP)** is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol**

For the realtime 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 save bandwidth.   
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

**UDP Header –**

UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long,

1. **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
2. **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.
3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one’s complement of the one’s complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

**Applications of UDP:** 

* Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
* It is suitable protocol for multicasting as UDP supports packet switching.
* UDP is used for some routing update protocols like RIP(Routing Information Protocol).

**Three Way Handshake for Connection Establishment and Termination**

The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model)

TCP provides reliable communication with something called **Positive Acknowledgement with Re-transmission(PAR)**. The Protocol Data Unit(PDU) of the transport layer is called segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver’s end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), then receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. You can realize from above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established.

* **Step 1 (SYN) :**In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with
* **Step 2 (SYN + ACK):**Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with
* **Step 3 (ACK) :**In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer

Termination ?

Increase the resources or decrease the load

• The most basic way to avoid congestion is to build a network that is well matched to the traffic

that it carries.

• These solutions are usually applied on different time scales to either prevent congestion or react to

it once it has occurred.

• The most basic way to avoid congestion is to build a network that is well matched to the traffic

that it carries.

• In a virtual-circuit network, new connections can be refused if they would cause the network to

become congested. This is called admission control.

**Throtelling traffic**

* When congestion is imminent, it must tell the senders to throttle back their transmissions and slowdown.

• Throttling traffic that can be used in both datagram networks and virtual-circuit networks.

**Choke Packets**

• A specialized packet that is used for flow control along a network.

• A router detects congestion by measuring the percentage of buffers in use, line utilization and

average queue lengths.

• When it detects congestion, it sends choke packets across the network to all the data sources

associated with the congestion.

**Explicit congestion notification**

When the network delivers the packet, the destination can note that there is congestion and inform

the sender when it sends a reply packet.

• The sender can then throttle its transmissions as before. This design is called ECN (Explicit

Congestion Notification) and is used in the Internet.

**Load Shedding**

Load shedding is a fancy way of saying that when routers are being in undated by packets that

they cannot handle, they just throw them away. The term comes from the world of electrical

power generation.

**Random Early Detection**

• Routers drop packets early, before the situation has become hopeless, there is time for the source

to take action before it is too late. A popular algorithm for doing this is called RED (Random

Early Detection)

**Explain sliding window protocol**

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. n this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver.

## Working Principle

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 2𝑛−1. Consequently, the size of the sending window is 2𝑛−1. Thus in order to accommodate a sending window size of 2𝑛−1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n.

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.

**Types od sliding window protocol**

* **Go – Back – N ARQ**

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

* **Selective Repeat ARQ**

This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

**TCP and UDP**

TCP UDP

|  |  |
| --- | --- |
| 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, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission. |
| 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. |
| TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgement of data. | UDP has only the basic error checking mechanism using checksums. |
| 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. |
| TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| 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). |
| TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| TCP is heavy-weight. | UDP is lightweight. |
| TCP doesn’t support Broadcasting. | UDP supports Broadcasting. |

**Describe with respect to Networking**

1. **Node:** A node is a connection point inside a network that can receive, send, create, or store data. Each node requires you to provide some form of identification to receive access, like an IP address. A few examples of nodes include **computers, printers, modems, bridges, and switches**.
2. **Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.
3. **A hub** is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices
4. **Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol.
5. [**Routers**](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/#Routers) – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together
6. **Distance Vector Routing Algorithm**
7. **Spanning Tree Algorithm**
8. **CIDR**
9. **Source-based congestion avoidance**
10. **Layering**
11. **Protocol**
12. **Encapsulation**
13. **Segment**
14. **Packet**
15. **Frames**