1.a)Wireless LAN b)Sensor networks

a)wireless LAN

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

Disadvantages of WLANs

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many

enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

b)Sensor networks

A **sensor network** is a group of sensors where each sensor monitors data in a different location and sends that data to a central location for storage, viewing, and analysis.

There are many applications for sensor networks, from monitoring a single home, to the surveillance of a large city, to earthquake detection for the whole world.

Home security

The primary goal of a home security sensor network is to detect an intruder. Many different types of sensors can help collect data towards that goal, such as magnetic open sensors on doors and windows, acoustic-based glass break sensors, security cameras, and motion detectors.

Environmental monitoring

Researchers, farmers, and governments need to monitor aspects of the natural environment such as air pollution, water quality, soil conditions, and weather metrics. The traditional approach to monitoring is to collect a sample, bring it back to a lab, analyze it, and record the results. Needless to say, that approach is slow and dependent on human labor, so traditional monitoring doesn't produce a lot of data.

A more automated and scalable approach is to use a sensor network. Sensors can be distributed across an area, collect the environmental data, and send it back to a central server for processing.

In the Great Lakes of the United States, dozens of buoys use sensors to collect data about wind speed, water temperature, air temperature, and wave height.

2.Methods for error detection and correction.

Error detection

Simple Parity Check

Data sent from the sender undergoes parity check :

- 1 is added as a parity bit to the data block if the data block has an **odd number of 1's**.
- 0 is added as a parity bit to the data block if the data block has an **even number of 1's**.

This procedure is used for making the **number of 1's even**. This is commonly known as even parity checking.

Disadvantage:

- Only **single-bit error** is detected by this method, it fails in multi-bit error detection.
- It can not detect an error in case of an error in **two bits**.

Two-Dimensional Parity Check

For every **row and column**, parity check bits are calculated by a simple method of parity check. Parity for both rows and columns is transmitted with the data sent from sender to receiver. At the receiver's side, parity bits are compared with the calculated parity of the data received.

Error Correction

When the data is sent from the **sender side** to the receiver's side it needs to be detected and corrected. So an error correction method is used for this purpose. Following are the two ways through which error correction can be handled:

Backward Error Correction

In this method, When any error is found in the data at the receiver's end. Then the request for resending the whole data unit is sent by the receiver.

Forward Error Correction

In this method, an error-correcting code is used by the receiver that automatically corrects the errors.

Error Correction Techniques

We can detect the error using a single additional bit but we cannot use this bit for the correction purpose. It is important to know the exact location of the error if we want to correct that error. For example, for finding out the **single-bit error**, the error detection code checks out that the error is actually in one of the seven bits. Let d represents the number of data bits and r represents the number of redundant bits. The formula below is used for finding the r number of redundant bits :

$2r>=d+r+12r>=d+r+1$

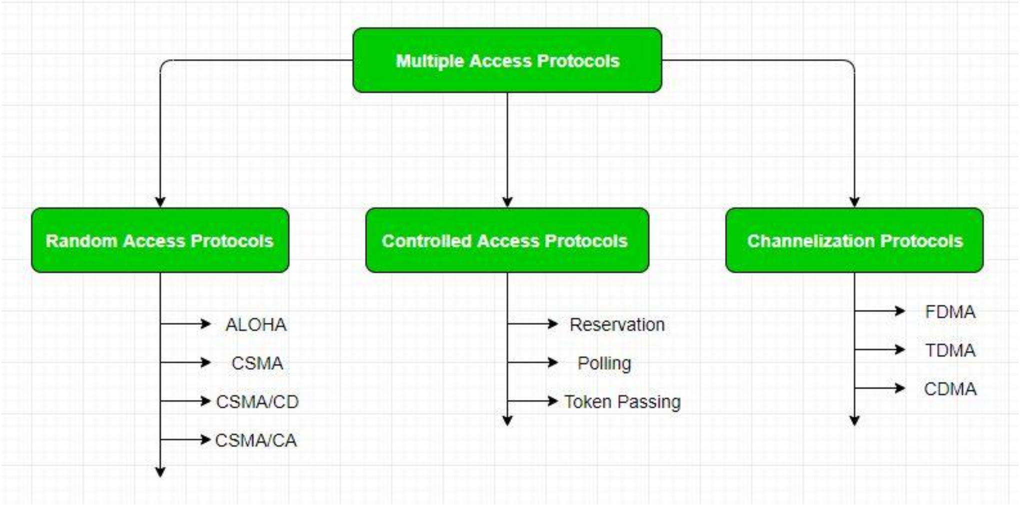
3.Multiple access protocols.

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

- Data Link Control
- Multiple Access Control

Data Link control –
The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.

Multiple Access Control –
If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.



.

Advantages :

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

Disadvantages :

- It is complex to implement
- It require the accurate information about the channel

Features of multiple access protocols:

Contention-based access: Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.

Carrier Sense Multiple Access (CSMA): CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.

Collision Detection (CD): CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.

4.Routing algorithm in network layer.

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm

Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into two parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

5.Transport layer connection estsblished and termination.

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.

Termination

1. **Graceful connection release –**
   In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.
2. **Abrupt connection release –**
   In an Abrupt connection release, either one TCP entity is forced to close the connection or one user closes both directions of data transfer.

Abrupt connection release :

An abrupt connection release is carried out when an RST segment is sent. An RST segment can be sent for the below reasons:

1. When a non-SYN segment was received for a non-existing TCP connection.

2. In an open connection, some TCP implementations send an RST segment when a segment with an invalid header is received. This will prevent attacks by closing the corresponding connection.

6.OSI reference model.

The Open Systems Interconnection (OSI) model is a conceptual framework that divides network communications functions into seven layers. Sending data over a network is complex because various hardware and software technologies must work cohesively across geographical and political boundaries. The OSI data model provides a universal language for computer networking, so diverse technologies can communicate using standard protocols or rules of communication. Every technology in a specific layer must provide certain capabilities and perform specific functions to be useful in networking. Technologies in the higher layers benefit from abstraction as they can use lower-level technologies without having to worry about underlying implementation details.

- Shared understanding of complex systems
- Faster research and development
- Flexible standardization

Physical layer

The physical layer refers to the physical communication medium and the technologies to transmit data across that medium. At its core, data communication is the transfer of digital and electronic signals through various physical channels like fiber-optic cables, copper cabling, and air. The physical layer includes standards for technologies and metrics closely related with the channels, such as Bluetooth, NFC, and data transmission speeds.

Data link layer

The data link layer refers to the technologies used to connect two machines across a network where the physical layer already exists. It manages data frames, which are digital signals encapsulated into data packets. Flow control and error control of data are often key focuses of the data link layer. Ethernet is an example of a standard at this level. The data link layer is often split into two sub-layers: the Media Access Control (MAC) layer and Logical Link Control (LLC) layer.

Network layer

The network layer is concerned with concepts such as routing, forwarding, and addressing across a dispersed network or multiple connected networks of nodes or machines. The network layer may also manage flow control. Across the internet, the Internet Protocol v4 (IPv4) and IPv6 are used as the main network layer protocols.

Transport layer

The primary focus of the transport layer is to ensure that data packets arrive in the right order, without losses or errors, or can be seamlessly recovered if required. Flow control, along with error control, is often a focus at the transport layer. At this layer, commonly used protocols include the Transmission Control Protocol (TCP), a near-lossless connection-based protocol, and the User Datagram Protocol (UDP), a lossy connectionless protocol. TCP is commonly used where all data must be intact (e.g. file share), whereas UDP is used when retaining all packets is less critical (e.g. video streaming).

Session layer

The session layer is responsible for network coordination between two separate applications in a session. A session manages the beginning and ending of a one-to-one application connection and synchronization conflicts. Network File System (NFS) and Server Message Block (SMB) are commonly used protocols at the session layer.

Presentation layer

The presentation layer is primarily concerned with the syntax of the data itself for applications to send and consume. For example, Hypertext Markup Language (HTML), JavaScipt Object Notation (JSON), and Comma Separated Values (CSV) are all modeling languages to describe the structure of data at the presentation layer.

Application layer

The application layer is concerned with the specific type of application itself and its standardized communication methods. For example, browsers can communicate using HyperText Transfer Protocol Secure (HTTPS), and HTTP and email clients can communicate using POP3 (Post Office Protocol version 3) and SMTP (Simple Mail Transfer Protocol).

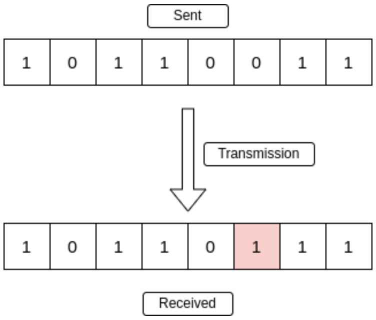
7.Error detecting codes with example.

Error is a condition when the receiver’s information does not match the sender’s information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits traveling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.
Data (Implemented either at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or get corrupted whenever a message is transmitted. To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

Types of Errors

Single-Bit Error

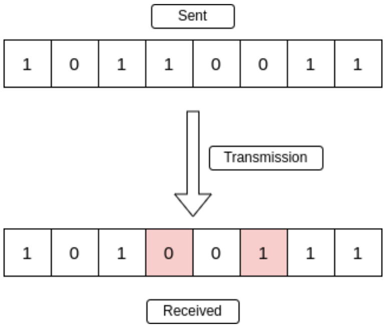
A single-bit error refers to a type of data transmission error that occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.



Single-Bit Error

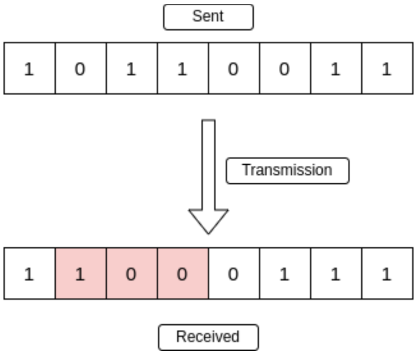
Multiple-Bit Error

A multiple-bit error is an error type that arises when more than one bit in a data transmission is affected. Although multiple-bit errors are relatively rare when compared to single-bit errors, they can still occur, particularly in high-noise or high-interference digital environments.



Burst Error

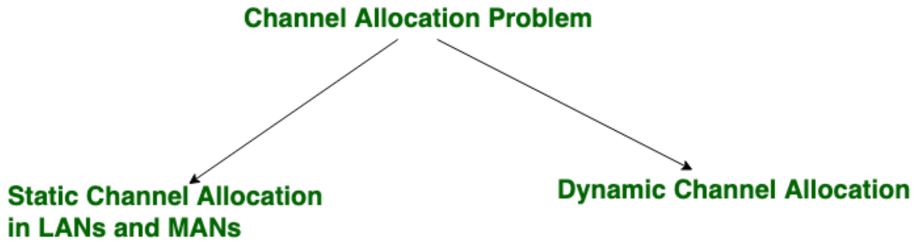
When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error. This error causes a sequence of consecutive incorrect values.



Burst Error

8.Channel allocation problem in medium access control sublayers.

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.
Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.


Channel Allocation Problem
Static Channel Allocation in LANs and MANs
Dynamic Channel Allocation

1. Static Channel Allocation in LANs and MANs:
It is the classical or traditional approach of allocating a single channel among multiple competing users using Frequency Division Multiplexing (FDM). if there are N users, the frequency channel is divided into N equal sized portions (bandwidth), each user being assigned one portion. since each user has a private frequency band, there is no interference between users.
However, it is not suitable in case of a large number of users with variable bandwidth requirements.
It is not efficient to divide into fixed number of chunks.

2. Dynamic Channel Allocation:
In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.
This allocation scheme optimises bandwidth usage and results is faster transmissions.
Dynamic channel allocation is further divided into:

1. Centralised Allocation
2. Distributed Allocation

Station Model:
Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

Single Channel Assumption: In this allocation all stations are equivalent and can send and receive on that channel.

Collision Assumption: If two frames overlap in time-wise, then that’s collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.

9.Three internet control protocols.

Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data. In order to understand it better, let’s take an example of a language. Any language has its own set of vocabulary and grammar which we need to know if we want to communicate in that language. Similarly, over the internet whenever we access a website or exchange some data with another device then these processes are governed by a set of rules called the internet protocols.

The internet and many other data networks work by organizing data into small pieces called packets. Each large data sent between two network devices is divided into smaller packets by the underlying hardware and software. Each network protocol defines the rules for how its data packets must be organized in specific ways according to the protocols the network supports.

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)
2. SMTP(Simple Mail Transfer Protocol)
3. PPP(Point-to-Point Protocol)

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)

These are a set of standard rules that allows different types of computers to communicate with each other. The IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination. The TCP is also known as a connection-oriented protocol.

2. SMTP(Simple Mail Transfer Protocol)

These protocols are important for sending and distributing outgoing emails. This protocol uses the header of the mail to get the email id of the receiver and enters the mail into the queue of outgoing mail. And as soon as it delivers the mail to the receiving email id, it removes the email from the outgoing list. The message or the electronic mail may consider the text, video, image, etc. It helps in setting up some communication server rules.

3. PPP(Point-to-Point Protocol)

It is a communication protocol that is used to create a direct connection between two communicating devices. This protocol defines the rules using which two devices will authenticate with each other and exchange information with each other. For example, A user connects his PC to the server of an Internet Service Provider and also uses PPP. Similarly, for connecting two routers for direct communication it uses PPP.

10.Two types of cryptographic.

Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can understand and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and the suffix "graphy" means "writing". In Cryptography, the techniques that are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

Types Of Cryptography

1. Symmetric Key Cryptography

It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric Key cryptography is faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely. The most popular symmetric key cryptography systems are Data Encryption Systems (DES) and Advanced Encryption Systems (AES).

2. Hash Functions

There is no usage of any key in this algorithm. A hash value with a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography

In Asymmetric Key Cryptography, a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is the RSA algorithm.

11.Communication satellities.

A communication satellite is an artificial satellite that acts as a large repeater in the sky. It receives signals from the source transmitter, amplifies using transponders, and relays them to the receiver. Thus, it creates a communication channel between locations of the earth that would not have been able to communicate due to long distance or obstruction by earth's curvature.

A **communication satellite** is a **microwave repeater station** in a space that is used for telecommunication, radio and television signals. A communication satellite processes the data coming from one earth station and it converts the data into another form and send it to the second earth station.

Communication satellites may be owned by government or private organizations. Presently, there are more than 2000 communication satellites in the sky. Some of its uses are −

- Internet
- Military operations
- Television
- Telephone
- Radio

Communication satellites are broadly categorized into three types depending upon the orbit in which they are placed.

- **Geostationary Satellite (GEO)** − They are at 36,000 km from the earth's surface. They have same orbital period as earth's rotation. So they appear to be still in the sky. At least 3 GEOs are needed for global coverage.
- **Medium Earth Orbit Satellite (MEO)** − They are placed between the two Van Allen belts, at a distance between 2,000 km to 36,000 km from the earth's surface. At least 10 MEOs are needed for global coverage.
- **Low Earth Orbit Satellite (LEO)** − They are situated below the Lower Van Allen belt. Their orbital altitude is 160 km to 2000 km. For global coverage, as high as 50 LEOs are required.

Advantages :

- Through satellite transmission, coverage over geographical area is quite large mainly for sparsely populated areas.
- High bandwidth and broadcast possibilities .
- Wireless and mobile communication applications can be easily established by satellite communication independent of location.

- It is used in wide variety of applications such as global mobile communication, private business networks, Long distance telephone transmission, weather forecasting, radio/TV signal broadcasting, gathering intelligence in military, navigation of ships and air crafts, connecting remote areas, television distribution etc.

Disadvantages :

- Design, development, investment, and insurance of satellite requires higher cost.
- There can be a congestion of frequencies.
- propagation issues and interference may arise.
- Launching satellites into orbit is an expensive process.
- To reach the satellite from Earth, time can vary between 270 milliseconds and return again to 320 milliseconds. This propagation delay can cause an echo over telephone connections
- Satellites are not easy to repair and maintain.

12.Elements of transport protocols.

To establish a reliable service between two machines on a network, transport protocols are implemented, which somehow resembles the data link protocols implemented at layer 2. The major difference lies in the fact that the data link layer uses a physical channel between two routers while the transport layer uses a subnet.

Following are the issues for implementing transport protocols−

Types of Service

The transport layer also determines the type of service provided to the users from the session layer. An error-free point-to-point communication to deliver messages in the order in which they were transmitted is one of the key functions of the transport layer.

Error Control

Error detection and error recovery are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis. To control errors from lost or duplicate segments, the transport layer enables unique segment sequence numbers to the different packets of the message, creating virtual circuits, allowing only one virtual circuit per session.

Flow Control

The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. The transport layer enables a fast process to keep pace with a slow one.

Acknowledgements are sent back to manage end-to-end flow control. Go back N algorithms are used to request retransmission of packets starting with packet number N. Selective Repeat is used to request specific packets to be retransmitted.

Connection Establishment/Release

The transport layer creates and releases the connection across the network. This includes a naming mechanism so that a process on one machine can indicate with whom it wishes to communicate. The transport layer enables us to establish and delete connections across the network to multiplex several message streams onto one communication channel.

Multiplexing/De multiplexing

The transport layer establishes a separate network connection for each transport connection required by the session layer. To improve throughput, the transport layer establishes multiple network connections. When the issue of throughput is not important, it multiplexes several transport connections onto the same network connection, thus reducing the cost of establishing and maintaining the network connections.

Addressing

Transport Layer deals with addressing or labelling a frame. It also differentiates between a connection and a transaction. Connection identifiers are ports or sockets that label each frame, so the receiving device knows which process it has been sent from. This helps in keeping track of multiple-message conversations. Ports or sockets address multiple conservations in the same location.

13.Guided transmittion media.

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

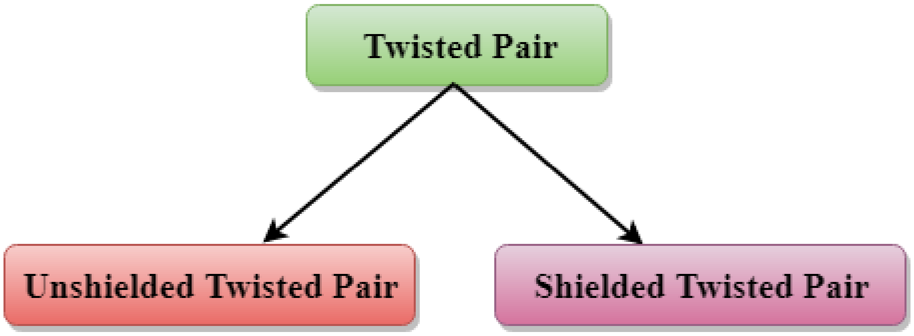
Types Of Guided media:

Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

14.Sliding window protocols.

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.

Types of Sliding Window Protocol

Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again.

Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame.

15.Congestion control algorithm.

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Congestion control algorithms

- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
- There are two congestion control algorithm which are as follows:

- Leaky Bucket Algorithm
- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.
Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

- Token bucket Algorithm
- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

16.Basic aspects of cryptography.

Nowadays, computing systems play a significant role in every aspect of human activity. Every marketing, software, banking, healthcare, and education application uses this computing technology. However, you might be curious about how businesses protect their data and maintain the privacy of their banking activities.

"Cryptography" is the answer to each of these questions. In today's connected world, sensitive information must be protected, which is why cryptography has influenced the current information age.

Additionally, Gmail data is secured using cryptography and is transmitted throughout Google data centers in an encrypted manner. Cryptography is therefore regarded as the essential component for protecting shared information.

Cryptography

Cryptography uses codes to protect data and communications so only the intended receivers can decode and understand them. Consequently, restricting access to information from outside parties.

"Crypto" indicates "hidden," and "graphy" indicates "writing," respectively. The techniques used in cryptography to secure data are based on mathematical principles and a set of rule-based calculations known as algorithms to modify signals in a way that makes them challenging to decode.

These algorithms generate cryptographic keys, create digital signatures, safeguard data privacy, enable online browsing on the Internet, and ensure the confidentiality of private transactions like credit and debit card payments.

History of Cryptography

Cryptography started with ciphers, the initial among which was the Caesar Cipher. Contrasted to modern algorithms for cryptography, ciphers were much simpler to decode, yet both employed plaintext and keys.Though simple, the earliest forms of encryption were ciphers. Modern cryptosystems and algorithms are considerably more advanced. They employ numerous iterations of ciphers and encrypt the ciphertext of messages to ensure the most secure data transportation and storage.

Purpose of cryptography

Cryptography aims to keep data and messages private and inaccessible to possible threats or bad actors. It frequently works invisibly to encrypt and decrypt the data you send through email, social media, applications, and website interactions.

- Payment applications and card transactions
- Random number generation
- Verify the sender's signature to be sure they are who they claim they are

There are several uses for asymmetric cryptography, including:

- Email messages
- SIM card authentication
- Web security
- Exchange of private keys