Module 1: Data Communication and Computer Networks

---

2 Marks Questions

1. What is Data Communication and discuss the characteristics of data communication.

Data communication is the process of transmitting digital or analog data between two or more computer systems or devices. It involves the transfer of information from a source to a receiver via a transmission medium. The key characteristics of data communication are:

- **Delivery:** Data must be delivered to the correct destination.
- **Accuracy:** Data must be delivered accurately without corruption.
- **Timeliness:** Data must be delivered in a timely manner.
- **Jitter:** The variation in the packet arrival time should be minimal.

2. Discuss the type of data flow of communication with an example.

The type of data flow, or **transmission mode**, describes the direction of signal flow between two devices. There are three types:

- **Simplex:** Communication is unidirectional, like a one-way street. (e.g., Radio broadcasting)
- **Half-duplex:** Communication is two-way but not simultaneously. (e.g., Walkie-talkie)
- **Full-duplex:** Communication is two-way and simultaneous. (e.g., Telephone call)

3. Specify the Network criteria.

A network must meet certain criteria to be effective. These include:

- **Performance:** Measured by throughput and delay.
- **Reliability:** Measured by the frequency of failures.
- **Security:** Protecting data from unauthorized access and damage.

4. Write the advantages and disadvantages of Star topology.

- **Advantages:** It is easy to install, manage, and scale. A single node failure does not affect the entire network.

- **Disadvantages:** It requires a lot of cabling and is expensive. The entire network depends on the central hub/switch, which is a single point of failure.

5. Write the advantages and disadvantages of Bus topology.

- **Advantages:** It is easy to install and requires less cabling compared to star or ring topologies, making it cost-effective.
- **Disadvantages:** It is difficult to troubleshoot and a break in the main cable can bring down the entire network. Performance degrades with more devices.

6. Write the advantages and disadvantages of Ring topology.

- **Advantages:** It provides equal access for all nodes and is relatively easy to manage. Data is transmitted in a single direction, which prevents data collisions.
- **Disadvantages:** A single node failure can break the entire network. It's difficult to add or remove nodes without disrupting network operation.

7. Write the advantages and disadvantages of Mesh topology.

- **Advantages:** It provides high reliability and security due to multiple paths for data transmission. A failure in one link doesn't affect the network's operation.
- **Disadvantages:** It's very expensive and complex to install and manage due to the extensive cabling required. The number of connections needed can be very high.

8. Describe any two common network topologies.

- **Star Topology:** All devices are connected to a central hub, switch, or server. This is the most common topology used in modern LANs due to its simplicity and fault tolerance.
- **Bus Topology:** All devices are connected to a single coaxial cable. Data is broadcast to all nodes, and a terminator is used at each end of the cable to prevent signal reflection.

9. Differentiate between OSI and TCP/IP Model.

Feature	OSI Model	TCP/IP Model
Layers	7 layers	4 layers
Nature	Conceptual framework	Practical, implemented model
Development	Developed by ISO	Developed by Department of Defense (DoD)
Protocols	Protocols are hidden from layers	Protocols are built into the model

10. What is line configuration and mention its types.

Line configuration refers to the way two or more communication devices are connected. The two main types are:

- **Point-to-point:** A dedicated link is established between two devices. (e.g., TV remote control)
- **Multipoint:** A single cable links multiple devices. (e.g., Bus topology)

11. What is flow control and error control in the transport layer?

- **Flow control** is a mechanism to manage the data transmission rate between a sender and receiver to prevent the receiver from being overwhelmed. The transport layer uses techniques like the sliding window protocol.
- **Error control** ensures reliable data delivery by detecting and correcting errors that occur during transmission. This is achieved through mechanisms like checksums and retransmission.

12. Mention the layers of TCP/IP model and explain any one layer.

The four layers of the TCP/IP model are:

1. **Application Layer**
2. **Transport Layer**
3. **Internet Layer**
4. **Network Access Layer**

The **Transport Layer** provides communication services to the application layer. It's responsible for the end-to-end delivery of the entire message and ensures that data is received in the correct sequence. It uses protocols like TCP and UDP.

13. Mention the layers of OSI model and explain any one layer.

The seven layers of the OSI model are:

1. **Physical Layer**
2. **Data Link Layer**
3. **Network Layer**
4. **Transport Layer**
5. **Session Layer**
6. **Presentation Layer**
7. **Application Layer**

The **Physical Layer** is the lowest layer and is responsible for the physical transmission of raw data bits over a communication medium. It defines hardware specifications, cabling, and the signaling method (voltage levels, frequency).

14. Write the difference between logical addressing and physical addressing.

Feature	Logical Addressing	Physical Addressing
Layer	Network Layer (OSI), Internet Layer (TCP/IP)	Data Link Layer (OSI), Network Access Layer (TCP/IP)
Address	IP Address	MAC Address
Scope	Unique across the internet	Unique to a specific network segment
Purpose	Used for routing data across different networks	Used for identifying devices within a local network

15. What is guided media and mention its types.

Guided media (also known as wired or bounded media) are transmission media that confine the signal to a specific path. The three main types are:

- **Twisted-pair cable:** Consists of two insulated copper wires twisted together.
- **Coaxial cable:** Has a central conductor surrounded by an insulating layer and a metallic shield.
- **Fiber-optic cable:** Transmits data using light signals through thin glass or plastic fibers.

16. What is unguided media and mention its types.

Unguided media (also known as wireless or unbounded media) are transmission media that do not guide the signal along a specific path. The signal is broadcast through the air. The three main types are:

- **Radio waves:** Used for broadcasting over large areas.
- **Microwaves:** Used for point-to-point communication.
- **Infrared waves:** Used for short-range communication.

17. Mention the categories of transmission media with diagram.

Transmission media can be broadly categorized into two types:

1. **Guided Media:** Signals are contained within a physical medium.
2. **Unguided Media:** Signals are propagated through the air.

18. Mention the factors to be considered while choosing the transmission medium.

The choice of transmission medium depends on several factors:

- **Data Rate:** The required speed of data transfer.
- **Cost:** The cost of the cable and its installation.
- **Distance:** The length of the link.
- **Attenuation:** The signal loss over distance.
- **Noise Immunity:** The resistance to external interference.

19. A signal travels through a transmission medium and its power reduces to half of its original value i.e., P2=(1/2)P1. Calculate the attenuation (loss of power) in the transmission medium.

The attenuation in decibels (dB) is calculated using the formula:

Attenuation (dB)=10log10P1P2

Given P2=21P1:

Attenuation (dB)=10log10P121P1=10log10(0.5)
Attenuation (dB)≈−3.01 dB

The attenuation is approximately **3.01 dB**. The negative sign indicates a loss of power.

20. The power of a signal is 10mW and the power of the noise is 1µW; what are the values of SNR and SNRdB?

Signal-to-Noise Ratio (SNR) is the ratio of signal power to noise power.

- Signal Power (Psignal) = 10 mW = 10×10−3 W
- Noise Power (Pnoise) = 1 µW = 1×10−6 W

  SNR=PnoisePsignal=1×10−610×10−3=10×103=10000

  SNRdB=10log10(SNR)=10log10(10000)=10×4=40 dB

  The SNR is **10,000**, and the SNR in decibels is **40 dB**.

21. Mention the functions of the physical layer.

The physical layer is responsible for the physical transmission of data bits. Its functions include:

- **Bit representation:** Defining the type of encoding for data bits.
- **Data rate:** Defining the transmission rate.
- **Synchronization:** Ensuring the sender and receiver have synchronized clocks.
- **Line configuration:** Point-to-point or multipoint.
- **Physical topology:** Defining the network's physical layout.

22. What are the types of twisted pair cable?

There are two main types of twisted-pair cables:

- **Unshielded Twisted-Pair (UTP):** The most common type, it consists of pairs of twisted wires without any additional shielding. It is inexpensive and easy to install.

- **Shielded Twisted-Pair (STP):** It has an extra metallic shield around the twisted pairs to protect against electromagnetic interference (EMI) and noise. It is more expensive and bulkier than UTP.

23. A signal travels through an amplifier, and its power is increased 10 times. This means that P2=10P1. In this case, calculate amplification (gain of power).

The gain in decibels (dB) is calculated using the formula:

Gain (dB)=10log10P1P2

Given P2=10P1:

Gain (dB)=10log10P110P1=10log10(10)
Gain (dB)=10×1=10 dB

The amplification gain is **10 dB**.

24. What is data rate limits and mention the two categories of the data rate limits.

Data rate limits refer to the maximum speed at which data can be transmitted over a communication channel. The two main categories are:

- **Data rate limit for a noiseless channel:** Governed by the **Nyquist theorem**, which calculates the maximum data rate based on the number of signal levels and bandwidth.
- **Data rate limit for a noisy channel:** Governed by the **Shannon capacity theorem**, which determines the theoretical maximum data rate based on bandwidth and SNR.

25. What is Nyquist theorem and Shannon capacity theorem.

- **Nyquist Theorem:** It defines the maximum data rate for a **noiseless** channel. The formula is: C=2Blog2L, where C is the channel capacity, B is the bandwidth, and L is the number of signal levels.
- **Shannon Capacity Theorem:** It defines the theoretical maximum data rate for a **noisy** channel. The formula is: C=Blog2(1+SNR), where C is the channel capacity, B is the bandwidth, and SNR is the signal-to-noise ratio.

26. Calculate the max. bit rate for a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels.

Using the Nyquist Theorem for a noiseless channel:

- C=2Blog2L
- B=3000 Hz
- L=2 signal levels

$C=2\times3000\times\log22=6000\times1=6000$ bps

The maximum bit rate is **6000 bps**.

27. Assume that we need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Using the Nyquist Theorem:

- $C=2B\log2L$
- $C=265$ kbps = 265,000 bps
- $B=20$ kHz = 20,000 Hz
- $L = ?$

$265000=2\times20000\times\log2L$

$265000=40000\times\log2L$

$\log2L=40000265000=6.625$

$L=26.625\approx98.74$

Since the number of signal levels must be an integer, we need to choose the next higher power of 2, which would be $27=128$ levels, or simply round up to the nearest integer, which would be **99 signal levels**.

28. Assume that we have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What are the appropriate bit rate and signal level?

First, calculate the maximum bit rate (channel capacity) using the Shannon capacity theorem for a noisy channel:

- $C=B\log2(1+SNR)$
- $B=1$ MHz = 106 Hz
- $SNR=63$

$C=106\times\log2(1+63)=106\times\log2(64)=106\times6=6\times106$ bps

The maximum bit rate is **6 Mbps**.

Next, find the appropriate number of signal levels (L). We use the Nyquist formula and assume a similar bit rate is achieved.

- $C=2B\log2L$
- $C=6\times106$ bps
- $B=106$ Hz

$6 \times 106 = 2 \times 106 \times \log 2L$

$\log 2L = 2 \times 1066 \times 106 = 3$

$L = 23 = 8$

The appropriate bit rate is **6 Mbps**, and the number of signal levels is **8**.

---

10 Marks Questions

1. What is a network? Explain the data flow of communication with a neat diagram.

A **network** is a set of devices (nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and receiving data. The links connecting these nodes can be wired (e.g., cables) or wireless (e.g., radio waves).

Data flow of communication refers to the direction in which data can move between two connected devices. As discussed in the 2-mark section, there are three primary modes:

- **Simplex Mode:** In this mode, communication is unidirectional. Only one device can transmit, and the other can only receive. This is like a one-way road where traffic flows in a single direction. A good example is a traditional radio or TV broadcast where the station transmits and the audience receives.
- **Half-Duplex Mode:** This mode allows for two-way communication, but not simultaneously. The devices take turns transmitting and receiving. It's like a single-lane bridge with a traffic light on each side; only one direction can cross at a time. The communication channel is shared, so when one device is sending, the other must be in receiving mode. The best real-world example is a **walkie-talkie**.
- **Full-Duplex Mode:** This mode allows simultaneous two-way communication between devices. Both devices can send and receive data at the same time. This is like a two-way street. The channel's capacity is shared by signals traveling in both directions. The common example is a **telephone conversation**.

2. Explain different types of network topologies and list their advantages and disadvantages.

A **network topology** is the physical or logical arrangement of nodes and connections in a computer network. The choice of topology affects performance, reliability, and cost.

1. Mesh Topology

In this topology, every device is connected to every other device on the network. There are dedicated point-to-point links.

- **Diagram:** * **Advantages:**
    - **High Reliability:** The network is very robust; if one link fails, there are many other paths for data to travel.
    - **Security:** Dedicated links make communication more secure and private.
    - **Fault Identification:** It's easy to locate a fault as the connection is point-to-point.
- **Disadvantages:**
    - **High Cost:** Requires extensive cabling, making it the most expensive topology.
    - **Complexity:** The installation and management are very complex due to the number of connections.
    - **Scalability:** Adding new devices can be difficult and disruptive.

2. Star Topology

In a star topology, all devices are connected to a central hub, switch, or server. The central device acts as a relay for all data.

- **Diagram:** * **Advantages:**
    - **Easy to Install:** Setting up the network is straightforward.
    - **Fault Isolation:** If a link to a single device fails, only that device is affected.
    - **Simple Management:** Easy to add, remove, or modify a node.
- **Disadvantages:**
    - **Single Point of Failure:** If the central hub/switch fails, the entire network goes down.
    - **High Cabling Cost:** Requires more cables than bus or ring topologies.
    - **Performance Dependency:** The network's performance depends on the central device's capacity.

3. Bus Topology

In a bus topology, all devices are connected to a single main cable, known as the backbone or bus. Data signals travel along the bus in both directions.

- **Diagram:** * **Advantages:**
    - **Cost-Effective:** Uses less cabling, making it cheaper to install.
    - **Easy to Install:** Relatively simple to set up a small network.
- **Disadvantages:**
    - **Single Point of Failure:** A break in the main cable can bring down the entire network.
    - **Difficult to Troubleshoot:** It's challenging to locate a fault.
    - **Performance Issues:** Network performance degrades significantly with high traffic and a large number of devices.

4. Ring Topology

In a ring topology, each device is connected to exactly two other devices, forming a circular ring. Data travels in one direction (unidirectional ring) or both directions (bidirectional ring).

- **Diagram:** * **Advantages:**
    - **No Collisions:** Unidirectional data flow eliminates the possibility of data collisions.
    - **Equal Access:** Every device has an equal opportunity to transmit.
    - **Better Performance:** Can handle higher network load than bus topology.
- **Disadvantages:**
    - **Single Point of Failure:** A failure of a single node or link can break the entire ring.
    - **Difficult to Add/Remove Nodes:** Adding or removing a device requires temporarily shutting down the network.

3. Explain with a neat diagram TCP/IP model.

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is a four-layer architectural model that describes how data is transmitted between computers over the internet. It is the de facto standard for all networking communications.

The Four Layers of the TCP/IP Model

1. **Application Layer:**
    - **Function:** This is the top layer and interacts directly with applications. It provides high-level protocols that enable specific services for user applications.
    - **Protocols:** HTTP, FTP, SMTP, DNS, etc.

- **Explanation:** When you open a web browser, the HTTP protocol is at work in the application layer, fetching web pages. Email clients use SMTP to send mail. This layer is what the user sees and interacts with.

2. **Transport Layer:**
   - **Function:** Responsible for end-to-end communication and providing reliable data delivery between hosts. It segments data from the application layer and adds control information.
   - **Protocols:**
     - **TCP (Transmission Control Protocol):** A connection-oriented protocol that ensures reliable, ordered, and error-checked delivery of a stream of data. It establishes a connection before transmitting data.
     - **UDP (User Datagram Protocol):** A connectionless protocol that provides an unreliable, fast delivery service. It does not perform error checking or sequencing, making it suitable for applications where speed is more critical than reliability (e.g., streaming).
   - **Explanation:** The transport layer is like a postal service that sorts and packs letters (data segments) into envelopes, ensuring they get from the source to the destination host. TCP is the "registered mail" service, while UDP is the "standard mail."
3. **Internet Layer (Network Layer):**
   - **Function:** Responsible for logical addressing and routing of data packets across different networks. It handles the movement of data from a source host to a destination host, possibly across multiple interconnected networks.
   - **Protocols:** IP (Internet Protocol), ICMP, etc.
   - **Explanation:** The Internet layer is the "GPS" of the network. It adds source and destination IP addresses to data packets and determines the best path for them to travel to their destination. The core protocol here, IP, is the heart of the internet.
4. **Network Access Layer (Data Link + Physical Layers):**
   - **Function:** This layer combines the functions of the OSI model's Data Link and Physical layers. It deals with the hardware aspects of networking, including the physical connection, addressing, and error detection on a single network segment.
   - **Protocols:** Ethernet, Wi-Fi (802.11), etc.
   - **Explanation:** This layer is like the "local road system" that a vehicle (data packet) uses to travel between two points on the same street. It provides a physical address (MAC address) for a device on the local network and manages the actual transmission of bits over the cable or airwaves.

4. Explain with a neat diagram OSI model.

The **OSI (Open Systems Interconnection) model** is a conceptual framework that standardizes the functions of a communication system into seven logical layers. Developed by the International Organization for Standardization (ISO), it provides a clear, layered approach to understanding how network protocols interact.

The Seven Layers of the OSI Model

1. **Physical Layer (Layer 1):**
    - **Function:** Deals with the physical transmission of raw bit streams over a communication medium. It defines hardware, cabling, and signal characteristics (voltage, frequency).
    - **Example:** Ethernet cables, optical fiber, wireless signals.
2. **Data Link Layer (Layer 2):**
    - **Function:** Provides reliable data transfer over a single link. It organizes the raw bit stream into logical units called **frames**, performs error detection and correction, and handles physical addressing (**MAC address**).
    - **Example:** Ethernet, Wi-Fi.
3. **Network Layer (Layer 3):**
    - **Function:** Responsible for logical addressing and routing of data packets from a source to a destination across a network. It adds source and destination **IP addresses** to the data.
    - **Example:** IP (Internet Protocol).
4. **Transport Layer (Layer 4):**
    - **Function:** Manages end-to-end communication between hosts. It ensures reliable, ordered, and error-free data delivery using protocols like **TCP** and **UDP**. It also handles segmentation and reassembly of data.
    - **Example:** TCP, UDP.
5. **Session Layer (Layer 5):**
    - **Function:** Establishes, manages, and terminates communication sessions between applications. It provides services like synchronization, dialog control, and checkpointing.
    - **Example:** NetBIOS, RPC.
6. **Presentation Layer (Layer 6):**
    - **Function:** Responsible for data translation, encryption, and compression. It ensures that the data format is readable by the receiving application.
    - **Example:** JPEG, MPEG, ASCII, SSL/TLS.
7. **Application Layer (Layer 7):**
    - **Function:** This is the top layer and provides a user interface to the network. It supports a variety of services for user applications.
    - **Example:** HTTP, FTP, SMTP, DNS.

5. Compare and contrast the TCP/IP model with the OSI model, highlighting their similarities and differences.

Both the **OSI (Open Systems Interconnection) model** and the **TCP/IP model** are conceptual frameworks used to describe network communication. While they serve a similar purpose, they have distinct structures and approaches.

Similarities

- **Layered Architecture:** Both models use a layered approach, where each layer performs a specific function and communicates with the layers directly above and below it. This modularity simplifies network design and troubleshooting.
- **Protocol Stacks:** Both models define a stack of protocols that provide communication services.
- **End-to-End Delivery:** The transport layer in both models is responsible for end-to-end data delivery.
- **Addressing:** Both models use logical (network layer) and physical (data link/network access layer) addressing to identify devices and route data.

Differences

Feature	OSI Model	TCP/IP Model
Number of Layers	7 layers	4 layers
Development	Theoretical and conceptual model developed by ISO.	Practical, a de facto standard developed by the U.S. Department of Defense.
Protocol Dependency	Protocols are separate from the model itself. The model was developed before the protocols.	Protocols are an integral part of the model. The model was developed around existing protocols.
Layer Combination	Separates the Presentation, Session, and Application layers.	Combines the Presentation, Session, and Application layers into a single Application layer.
Strictness	A rigid framework, with clear boundaries between layers.	A more flexible model that is easier to implement.
Troubleshooting	Easier to troubleshoot due to the strict separation of functions.	Can be more complex to troubleshoot due to the merged layers.
Physical/Data Link	Has separate Physical and Data Link layers.	Combines the Physical and Data Link layers into a single Network Access layer.

6. What is Transmission media and explain in brief the categories of the Transmission media.

Transmission media refers to the physical path or medium through which data is transmitted from a sender to a receiver.It can be a physical conductor or an open-air medium. The choice of medium depends on factors such as cost, data rate,distance, and environmental conditions.

There are two main categories of transmission media:

1. Guided Media (Wired)

Guided media, also known as wired or bounded media, provides a physical conduit for signals. The signal is contained and directed along a specific path.

- **Twisted-Pair Cable:** The most common type of guided media, it consists of two insulated copper wires twisted together to reduce electromagnetic interference (EMI).
    - **Types: Unshielded Twisted-Pair (UTP)** (commonly used in Ethernet networks) and **Shielded Twisted-Pair (STP)** (has an additional metallic shield for better noise immunity).
- **Coaxial Cable:** This cable has a central copper conductor surrounded by an insulating layer, a metallic shield, and an outer insulating jacket. This structure makes it more resistant to noise than UTP.
    - **Uses:** Used for cable TV and older Ethernet networks.
- **Fiber-Optic Cable:** Transmits data using light pulses through thin strands of glass or plastic. It offers significantly higher bandwidth and is immune to electromagnetic interference, making it ideal for long-distance, high-speed communication.
    - **Types: Single-mode** (for very long distances) and **Multimode** (for shorter distances).

2. Unguided Media (Wireless)

Unguided media, also known as wireless or unbounded media, propagates signals through the air without any physical conductor. The signal is broadcast, and the receiving antenna captures it.

- **Radio Waves:** These waves are omnidirectional and can travel long distances, even passing through walls. They are used for radio and television broadcasting, as well as cellular communication.
- **Microwaves:** These are highly directional waves that require line-of-sight communication between a sender and a receiver. They are used for satellite communication and terrestrial point-to-point links.

- **Infrared Waves:** These waves are used for short-range communication in a closed area, like a room. They are blocked by walls and other objects.
    - **Uses:** TV remote controls, short-range wireless keyboards.

7. Illustrate causes of Transmission impairment with neat diagram.

Transmission impairment is the degradation of a signal as it travels through a transmission medium. This can cause the received signal to be different from the transmitted signal. The three main causes are:

- **Attenuation:**
    - **Cause:** Attenuation is the loss of signal strength (energy) as it travels over a distance. The longer the distance, the more the signal loses its power. This can be caused by the medium's resistance, scattering, or absorption.
    - **Effect:** A weak signal may not be strong enough to be interpreted correctly by the receiver. Amplifiers and repeaters are used to compensate for this loss.
    - **Diagram:**
- **Distortion:**
    - **Cause:** Distortion occurs when the signal's shape or form changes. This is most common in composite signals where different frequency components travel at different speeds, arriving at the receiver at different times.
    - **Effect:** The received signal is a distorted version of the original, making it difficult to decode accurately.
    - **Diagram:**
- **Noise:**
    - **Cause:** Noise is an unwanted signal that interferes with the original data signal. It can be introduced by various sources, both internal and external to the system.
    - **Types of Noise:**
        - **Thermal Noise:** Caused by the random motion of electrons in a conductor.
        - **Impulse Noise:** A non-continuous, short-duration high-amplitude spike, often caused by power lines or lightning.
        - **Crosstalk:** The effect of signals from one cable or circuit interfering with another.
    - **Effect:** Noise corrupts the original signal, leading to errors in data transmission.
    - **Diagram:**

8. Define multiplexing. Explain different types of multiplexing with diagram.

Multiplexing is a technique that allows multiple data signals to be combined and transmitted over a single communication channel or medium. This significantly improves the efficiency of a network by maximizing the use of a shared resource. At the sending end, a device called a **multiplexer** combines the signals, and at the receiving end, a **demultiplexer** separates them.

There are two main types of multiplexing:

1. Frequency Division Multiplexing (FDM)

- **Concept:** FDM divides the available bandwidth of a single transmission medium into multiple, non-overlapping frequency bands. Each user or channel is assigned a unique frequency band for the duration of the communication.
- **How it works:** Each signal is modulated onto a different carrier frequency. These modulated signals are then combined and sent over the shared medium. At the receiver, filters are used to separate the signals based on their carrier frequencies.
- **Example:** Radio and television broadcasting, where multiple channels are transmitted simultaneously over a single antenna using different frequencies.
- **Diagram:**

2. Time Division Multiplexing (TDM)

- **Concept:** TDM divides the shared communication channel into time slots. Each user or channel is allocated a specific, recurring time slot to transmit its data. All signals use the entire bandwidth, but only for their assigned time slot.
- **How it works:** Data from each input is sent in a specific sequence, one after another, in a round-robin fashion. The multiplexer interleaves the data from different sources into a single data stream. The demultiplexer at the other end synchronizes with the multiplexer to correctly separate the data.
- **Types:**
    - **Synchronous TDM:** Each source is given a time slot, regardless of whether it has data to send. This can be inefficient if a source is idle.
    - **Statistical TDM:** Time slots are allocated dynamically to only those sources that have data to send, making it more efficient than synchronous TDM.
- **Example:** TDM is widely used in telephone systems and cellular networks.
- **Diagram:**

9. Define spread spectrum and explain its primary goal. Discuss two spread spectrum techniques commonly used in networking to ensure effective communication.

Spread spectrum is a wireless communication technique that spreads a narrow-band signal over a much wider frequency band. The primary goal of spread spectrum is to improve the signal's resistance to interference, increase its security, and allow multiple users to share the same frequency band without interfering with each other. This is achieved by making the signal "look like" random noise to any receiver not specifically designed to receive it.

The two most common spread spectrum techniques are:

1. Frequency Hopping Spread Spectrum (FHSS)

- **Concept:** The carrier frequency of the transmitted signal is rapidly changed or "hopped" across a wide range of frequencies, according to a pre-defined sequence known as a pseudo-random code.
- **How it works:**
  - The sender and receiver must use the same hopping sequence, which is synchronized.
  - The data signal is transmitted on one carrier frequency for a short duration (a "hop").
  - It then quickly switches to another carrier frequency for the next hop.
  - This rapid change makes the signal difficult for an unauthorized listener to intercept, and it effectively avoids interference since the signal only spends a brief time on any single frequency that might be experiencing interference.
- **Diagram:**

2. Direct Sequence Spread Spectrum (DSSS)

- **Concept:** The data stream is combined with a higher-rate bit sequence called a "chipping code" or "spreading code." This process spreads the data signal across a much wider frequency band.
- **How it works:**
  - Each bit of data is multiplied by the spreading code. For example, a data bit '1' might be represented by a sequence like "10110111," and a data bit '0' by "01001000."
  - The resulting signal is transmitted.
  - At the receiver, the same spreading code is used to "despread" the signal and recover the original data.Signals that do not have the correct spreading code are effectively rejected and appear as random noise.
- **Advantages:** DSSS provides better resistance to interference and more security than FHSS.
- **Diagram:**

10. This question is a duplicate of the previous one (Question 9). Please refer to the answer for Question 9.

11. You are working as a network administrator in a company that is setting up a new communication system based on the OSI Model. The company wants to ensure proper implementation and troubleshooting at each layer of the model to optimize network performance. Explain how each of the seven layers of the OSI Model would be applied in this network setup.

As a network administrator, applying the OSI model provides a structured framework for the entire network lifecycle,from initial design to ongoing maintenance and troubleshooting. Here's how each layer would be applied:

- **Layer 1 (Physical Layer):**
  - **Implementation:** Select and install the physical medium (e.g., Cat6 Ethernet cables for high-speed LAN,fiber optic cables for backbone). Ensure proper termination and physical connections for all devices (computers, servers, printers). Install network devices like hubs, repeaters, and power over Ethernet (PoE) switches.
  - **Troubleshooting:** Use a cable tester to check for breaks or shorts. Visually inspect cables and connectors.Verify link lights on devices are on and stable.
- **Layer 2 (Data Link Layer):**
  - **Implementation:** Configure switches to connect devices within the same local network. The switch uses **MAC addresses** to forward frames to the correct destination on the local network. Set up VLANs (Virtual LANs) to segment the network for security and performance.
  - **Troubleshooting:** Check the switch's MAC address table. If a device cannot communicate on the local network, check for a duplicate MAC address or a misconfigured VLAN.
- **Layer 3 (Network Layer):**
  - **Implementation:** Assign **IP addresses** to all devices. Configure routers to direct traffic between different subnets (e.g., between the employee network and the server network). Set up static or dynamic routing protocols (like OSPF) to ensure packets find the optimal path to their destination.
  - **Troubleshooting:** Use `ping` and `traceroute` commands to test connectivity and trace the path of packets.Check routing tables on routers to ensure they have the correct routes.
- **Layer 4 (Transport Layer):**
  - **Implementation:** Ensure that the right protocol is used for applications (e.g., **TCP** for reliable data transfer like file transfers, and **UDP** for real-time applications like video conferencing). Implement firewall rules to control traffic flow based on port numbers.
  - **Troubleshooting:** Check for dropped packets and connection timeouts. Verify that services are listening on the correct ports. Use tools like `netstat` to view active connections.
- **Layer 5 (Session Layer):**
  - **Implementation:** Ensure proper configuration of session management for client-server applications. This might involve configuring servers to handle a certain

number of simultaneous connections or setting up VPN tunnels for secure remote access.
    - **Troubleshooting:** Monitor application logs for session-related errors, such as a session that cannot be established or is unexpectedly terminated.
- **Layer 6 (Presentation Layer):**
    - **Implementation:** Configure network services to handle different data formats, such as ensuring that the web server serves data in a compatible format (e.g., UTF-8 encoding). Implement encryption protocols like SSL/TLS for secure communication.
    - **Troubleshooting:** Check for compatibility issues between different software versions. For encrypted traffic,check the certificate chain and ensure key exchange is working correctly.
- **Layer 7 (Application Layer):**
    - **Implementation:** Install and configure end-user applications and services, such as a mail server (SMTP,IMAP), a web server (HTTP), or a file server (FTP). Configure DNS to map domain names to IP addresses.
    - **Troubleshooting:** If a user can't access a website, check the DNS resolution. If an email fails to send, check the mail server logs. The administrator would directly interact with this layer when troubleshooting issues reported by users.

12. You are assigned the task of setting up a communication network for a small organization. The network will use the TCP/IP Model as its communication framework. Identify and briefly describe the layers of the TCP/IP Model, highlighting the key functions of each layer in ensuring effective communication within a network.

When setting up a network for a small organization using the TCP/IP model, you would work with four key layers to ensure smooth and effective communication.

- **Layer 1 (Network Access Layer):**
    - **Function:** This is the foundational layer responsible for the physical and logical link to the network. It handles the actual transmission of data over the physical medium and manages local addressing (**MAC addresses**).
    - **Application:** You would physically connect the computers using **Ethernet cables** to a **switch**. You would ensure the network interface cards (NICs) in each computer are working correctly and have a unique MAC address, allowing them to communicate on the local network segment.
- **Layer 2 (Internet Layer):**
    - **Function:** This layer is the "glue" that connects different networks. It's responsible for logical addressing (**IP addresses**) and **routing** data packets from a source to a destination, even if they are on different networks.
    - **Application:** You would assign a unique **IP address** to each device on the network. A **router** would be configured to manage traffic between the organization's local network and the outside world (the internet).The router uses the IP addresses to find the best path for each packet.
- **Layer 3 (Transport Layer):**

    - **Function:** This layer ensures reliable, end-to-end communication between applications on different devices.It segments data into smaller units and handles flow control and error checking.
    - **Application:** For a file server, you would use **TCP** to ensure that all data is transmitted and received correctly without errors. For voice or video calls, you would use **UDP** for its speed, as it doesn't require the overhead of error checking, which is less critical for real-time communication.
- **Layer 4 (Application Layer):**
    - **Function:** This is the topmost layer, where the network services and user applications reside. It provides the interface for users to interact with the network.
    - **Application:** You would configure services like a web server (**HTTP**), an email server (**SMTP, POP3, IMAP**), and a file transfer server (**FTP**). You would also set up a **DNS server** so that users can access websites by typing a domain name instead of a complex IP address. This layer is what the users directly interact with.