# CN

# MOD1

## PART-A

**1.Assume the difference between circuit switching and packet switching. Assume the link's rate is 2 Mbps and users are generating data at a rate of 100 Kbps when busy. Users are busy only a. What is the maximum number of users that a circuit switching architecture can support simultaneously?**

In the given scenario, the link's rate is 2 Mbps and users are generating data at a rate of 100 Kbps when busy. This means that each user requires 100 Kbps of bandwidth when busy.

To calculate the maximum number of users that a circuit switching architecture can support simultaneously, we divide the total available bandwidth by the bandwidth required per user:

Maximum number of users = Total available bandwidth / Bandwidth required per user

Maximum number of users = 2 Mbps / 100 Kbps

Maximum number of users = 20

**2.With a network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?**

Given:

- Bandwidth of the network = 10 Mbps (10,000,000 bits per second)
- Average number of frames per minute = 12,000 frames
- Average number of bits per frame = 10,000 bits

Now, let's calculate the throughput:

Throughput = (12,000 frames/minute) × (10,000 bits/frame) / (60 seconds/minute)
Throughput = (120,000,000 bits/minute) / (60 seconds/minute)

To get the throughput in bits per second, we need to convert from bits per minute to bits per second:

Throughput = (120,000,000 bits/minute) / (60 seconds/minute) Throughput = 2,000,000 bits per second

So, the correct throughput of this network is 2,000,000 bits per second, which is equivalent to **2 Mbps.**

**3.Imagine a signal travels through a transmission medium and its power is reduced to half. This means p2 = (1/2) p1. Calculate Attenuation**

Attenuation can be calculated using the following formula:

Attenuation (dB) = 10 log10 (P1/P2)

where:

- P1 is the input power
- P2 is the output power

In this case, P2 is (1/2) P1, so we can plug this into the formula to get:

Attenuation (dB) = 10 log10 (P1 / ((1/2) P1))

Attenuation (dB) = 10 log10 (2)

Attenuation (dB) = 10 * 0.3010

Attenuation (dB) = 3.01 Db

4. Consider a telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communications. The signal-to-noise ratio is usually 3162. Calculate the channel capacity for this channel?

the calculation of the channel capacity for the given telephone line:

Channel capacity = Bandwidth * log2(1 + SNR)

Channel capacity = 3000 Hz * log2(1 + 3162)

Channel capacity = 34,881 bits/s

Therefore, the channel capacity for the given telephone line is **34,881 bits/s.**

5. Illustrate for a wavelength in vacuum of 1550 nm, the corresponding frequency is 193.4 THz. for a typical single mode fiber, the velocity of propagation is approximately v = 2.04 * 108. Find out Wavelength of the Fiber optic cable.

the calculation of the wavelength in the fiber optic cable:

λ = v / f

where:

λ is the wavelength in the fiber optic cable

v is the velocity of propagation in the fiber optic cable

f is the frequency of the light in vacuum

In this case, v = 2.04 * 10^8 m/s and f = 193.4 * 10^12 Hz. Plugging these values into the formula, we get:

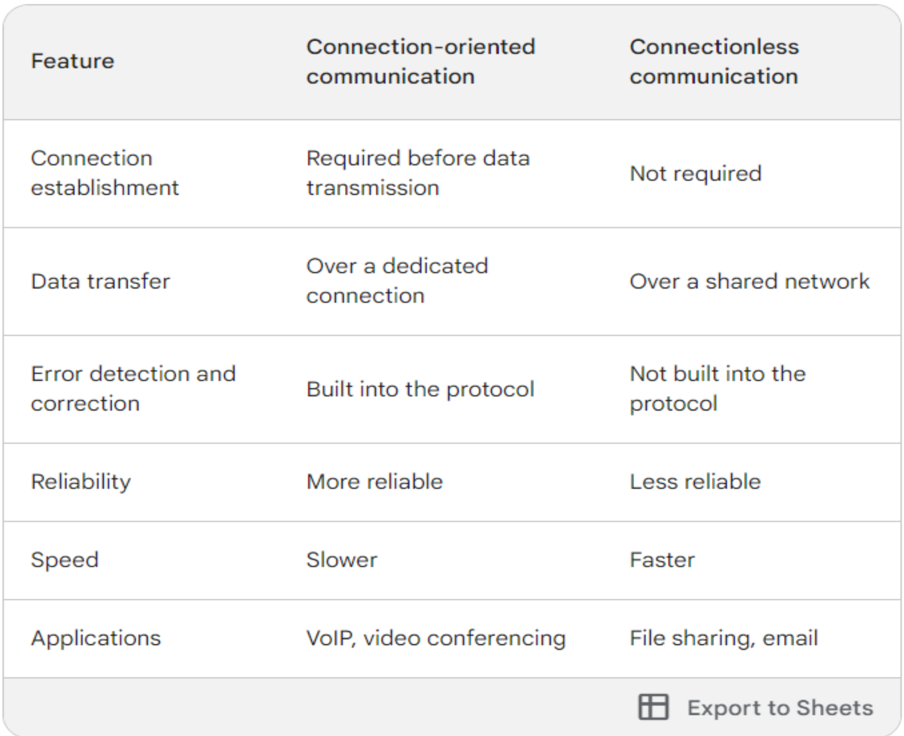
λ = (2.04 * 10^8 m/s) / (193.4 * 10^12 Hz)

λ = 1.054 * 10^-9 m

λ = 1054 nm

Therefore, the wavelength in the fiber optic cable is 1054 nm.

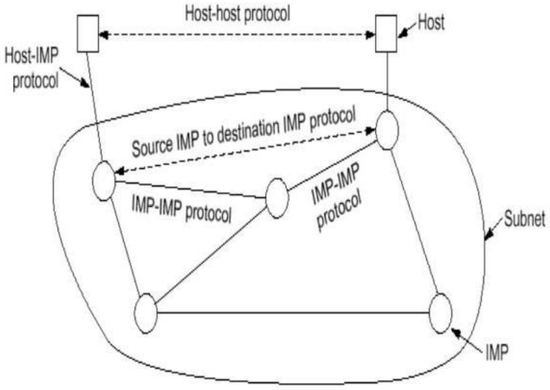
6. Explain the principle differences between connection-oriented communication and connectionless communication.



| Feature | Connection-oriented communication | Connectionless communication |
|---|---|---|
| Connection establishment | Required before data transmission | Not required |
| Data transfer | Over a dedicated connection | Over a shared network |
| Error detection and correction | Built into the protocol | Not built into the protocol |
| Reliability | More reliable | Less reliable |
| Speed | Slower | Faster |
| Applications | VoIP, video conferencing | File sharing, email |

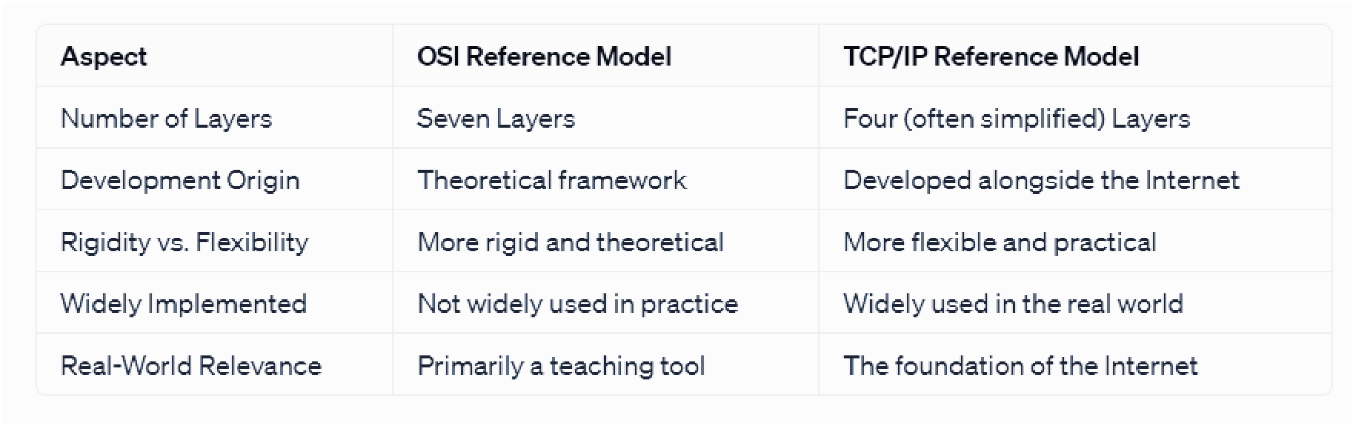
## 7.Discuss briefly about the original ARPANET design

The ARPANET was a revolutionary network that used packet switching to transmit data over a shared network. It was designed with distributed control, packet switching, and open architecture, making it resilient, efficient, and open to innovation. This groundbreaking network laid the foundation for the modern Internet we use today.



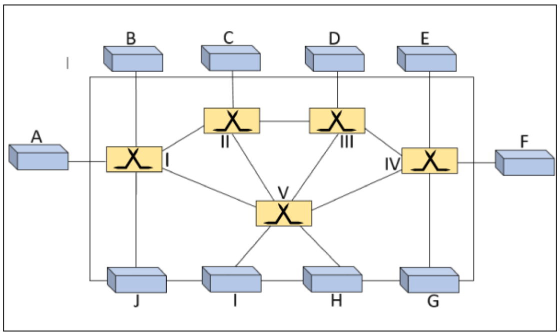
The original ARPANET was a pioneering, decentralized computer network designed for resource sharing using packet switching. It influenced the development of standardized protocols and laid the foundation for the modern Internet by enabling host-to-host communication and open standards. ARPANET began with four nodes in 1969 and rapidly expanded, ultimately evolving into the global Internet.

## 8. Differentiate OSI reference model with the TCP/IP reference model.



| Aspect | OSI Reference Model | TCP/IP Reference Model |
|---|---|---|
| Number of Layers | Seven Layers | Four (often simplified) Layers |
| Development Origin | Theoretical framework | Developed alongside the Internet |
| Rigidity vs. Flexibility | More rigid and theoretical | More flexible and practical |
| Widely Implemented | Not widely used in practice | Widely used in the real world |
| Real-World Relevance | Primarily a teaching tool | The foundation of the Internet |

## 9.Explain the significance of Switching? What are different switching techniques used in computer networks? Discuss.



Switching: Directing data packets along optimal paths for efficient transmission in computer networks.

### Significance of Switching:

1. **Efficiency:** Switching optimizes data transmission by forwarding data only to the intended recipient, reducing congestion.
2. **Resource Sharing:** It allows multiple devices to share network resources effectively.
3. **Scalability:** Supports network growth while maintaining low latency and high throughput.
4. **Security:** Isolates communication, enhancing privacy and reducing the risk of interception.
5. **Quality of Service (QoS):** Prioritizes critical traffic for multimedia and real-time services.
6. **Redundancy:** Enables redundant paths for network resilience.

### Different Switching Techniques:

1. **Circuit Switching:** Dedicates a communication path for the entire session, common in traditional telephony.
2. **Packet Switching:** Divides data into packets, shared resources, used in the Internet.
3. **Message Switching:** Stores and forwards entire messages, rarely used due to inefficiency.
4. **Cell Switching:** Uses fixed-sized cells for data transfer, found in ATM networks.
5. **Space-Division Switching:** Utilizes physical components for creating connections, common in high-capacity telephone exchanges.
6. **Time-Division Switching:** Shares a channel by dividing it into time slots, used in TDM and SONET/SDH networks.

## 10. .a) Write short notes on Wireless Transmission. b) Describe in detail about Lightwave transmission.

a) Wireless Transmission

Wireless transmission refers to the transmission of data or information using electromagnetic waves without the need for physical cables or wires. It has become increasingly popular in recent years due to its flexibility, convenience, and ability to connect devices over long distances without the limitations of physical infrastructure

- Applications: Wireless transmission is used in a wide variety of applications, including cellular networks, Wi-Fi, Bluetooth, satellite communication, and radio broadcasting.

b) Lightwave Transmission

Lightwave transmission, also known as optical fiber communication, is a type of telecommunication that uses light to transmit data. It is the most widely used method for long-distance communication due to its high bandwidth, low latency, and immunity to electromagnetic interference.

Principles of lightwave transmission:

- Light sources: Lasers or light-emitting diodes (LEDs) are used to generate light pulses that carry data.

- Optical fibers: Optical fibers are transparent cables that guide light pulses from the transmitter to the receiver.

- Photodetectors: Photodetectors convert the light pulses back into electrical signals that can be processed by computers and other devices.

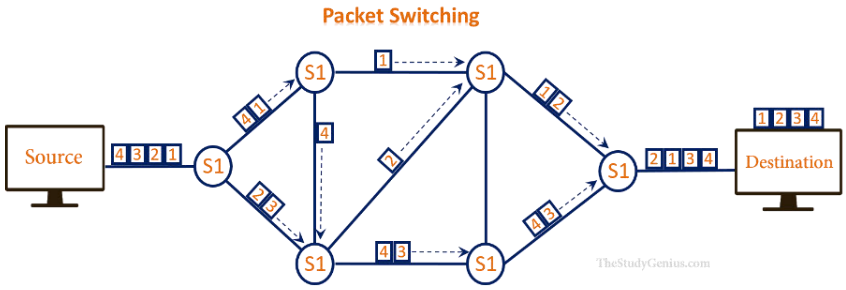
## PART-B

### 1.Define switching and Explain packet switching.

**Switching is a fundamental concept in computer networks that determines how data is forwarded from one device to another. It's like a traffic cop for data, deciding where to send information so it reaches its intended destination**

It involves examining the destination address of each packet and selecting the best available path for it to reach its intended destination. Switching is a crucial component of computer networks, as it enables efficient data transmission, network scalability, and reduced delays.

Packet switching is a type of switching that breaks down data into smaller packets, each with its own header containing addressing information. Packets are routed independently through the network, using different paths if necessary, and reassembled at the destination. Packet switching is the most commonly used switching technique in modern computer networks. Once all the packets arrive, they're reassembled to form the original message. It's like sending pieces of a puzzle through the network, and they come together at the other end. This method is efficient, as it allows multiple messages to share the network at the same time, and it's how the Internet works.

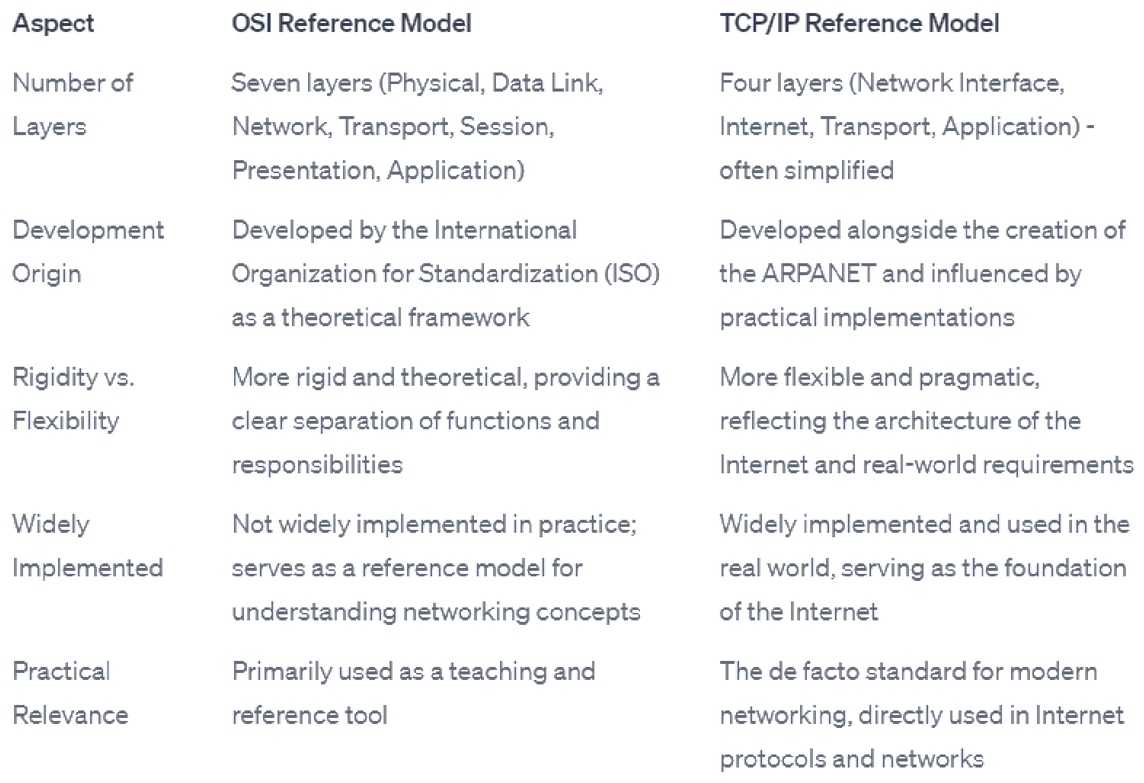


Here are some of the benefits of packet switching:

- Efficiency: Packet switching allows for more efficient use of network resources, as data packets from different sources can share the same physical path.
- Scalability: Packet switching networks can easily be scaled to handle increasing traffic demands by adding more nodes and links.
- Resiliency: Packet switching networks are more resilient to failures, as data packets can be rerouted around failed links.

## 2.Illustrate the differences between the OSI and TCP/IP Reference Models.

The Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP) model are two conceptual frameworks that are commonly used to describe the architecture of computer networks. They both describe how data should be formatted and transmitted across a network, but they differ in several key ways.

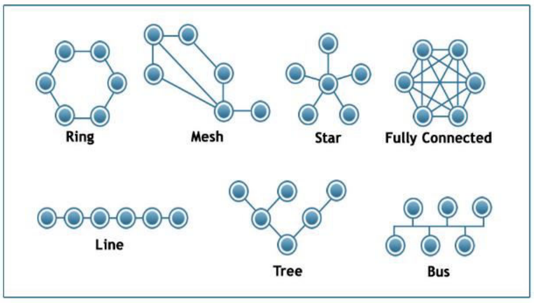


| Aspect | OSI Reference Model | TCP/IP Reference Model |
|---|---|---|
| Number of Layers | Seven layers (Physical, Data Link, Network, Transport, Session, Presentation, Application) | Four layers (Network Interface, Internet, Transport, Application) - often simplified |
| Development Origin | Developed by the International Organization for Standardization (ISO) as a theoretical framework | Developed alongside the creation of the ARPANET and influenced by practical implementations |
| Rigidity vs. Flexibility | More rigid and theoretical, providing a clear separation of functions and responsibilities | More flexible and pragmatic, reflecting the architecture of the Internet and real-world requirements |
| Widely Implemented | Not widely implemented in practice; serves as a reference model for understanding networking concepts | Widely implemented and used in the real world, serving as the foundation of the Internet |
| Practical Relevance | Primarily used as a teaching and reference tool | The de facto standard for modern networking, directly used in Internet protocols and networks |

## 3. Define computer networks? Describe various types of networks topologies in computer network. Also discuss various advantages and disadvantages of each topology.

**Computer Networks:** A computer network is a set of interconnected computers and other devices that can communicate and share resources with each other. These networks can be as small as a local area network (LAN) within a single building or as vast as the internet, connecting devices worldwide. Computer networks enable data exchange, communication, and resource sharing among connected devices.

Network topology refers to the arrangement of nodes and links that make up a network. It defines how these nodes and links are physically connected to each other.

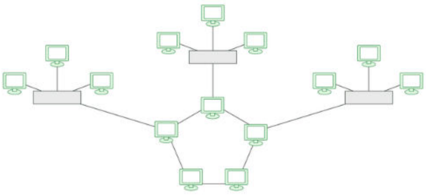


Various Types of Network Topologies:

1. Bus Topology:
    - In a bus topology, all devices are connected to a single central cable, called the bus.
    - **Advantages:** Simple to set up and cost-effective for small networks.
    - **Disadvantages:** Susceptible to cable failures, can experience data collisions, and limited scalability.
2. Star Topology:
    - In a star topology, each device is connected directly to a central hub or switch.
    - **Advantages:** Easy to install and manage, centralized control, and one device's failure doesn't affect others.
    - **Disadvantages:** Dependency on the central hub or switch, which, if it fails, can disrupt the entire network.
3. Ring Topology:
    - In a ring topology, devices are connected in a closed loop, where each device is connected to two others.
    - **Advantages:** Equal data distribution, simple and predictable design.
    - **Disadvantages:** Difficult to add or remove devices, a single cable failure can disrupt the entire network.
4. Mesh Topology:

- In a mesh topology, every device is connected to every other device, creating redundant connections.
- **Advantages:** High reliability, fault tolerance, and data can take multiple paths.
- **Disadvantages:** Complex, expensive to implement and manage, and a significant amount of cabling.

5. **Hybrid Topology:**



- A hybrid topology combines two or more of the above topologies within a network.
- **Advantages:** Offers flexibility, better fault tolerance, and scalability.
- **Disadvantages:** Complex to design and manage, and cost varies depending on the selected topologies.

## 4. Define switching. Explain circuit switching.

### Circuit Switching

Circuit switching is a type of switching that establishes a dedicated physical connection between two devices before any data transfer occurs. This connection remains dedicated throughout the communication session, ensuring uninterrupted data transmission.

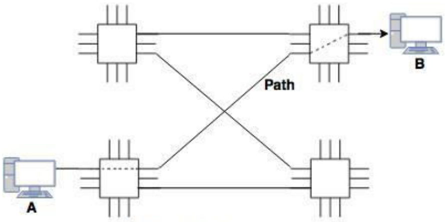


Fig: Circuit Switching

Key features and characteristics of circuit switching:

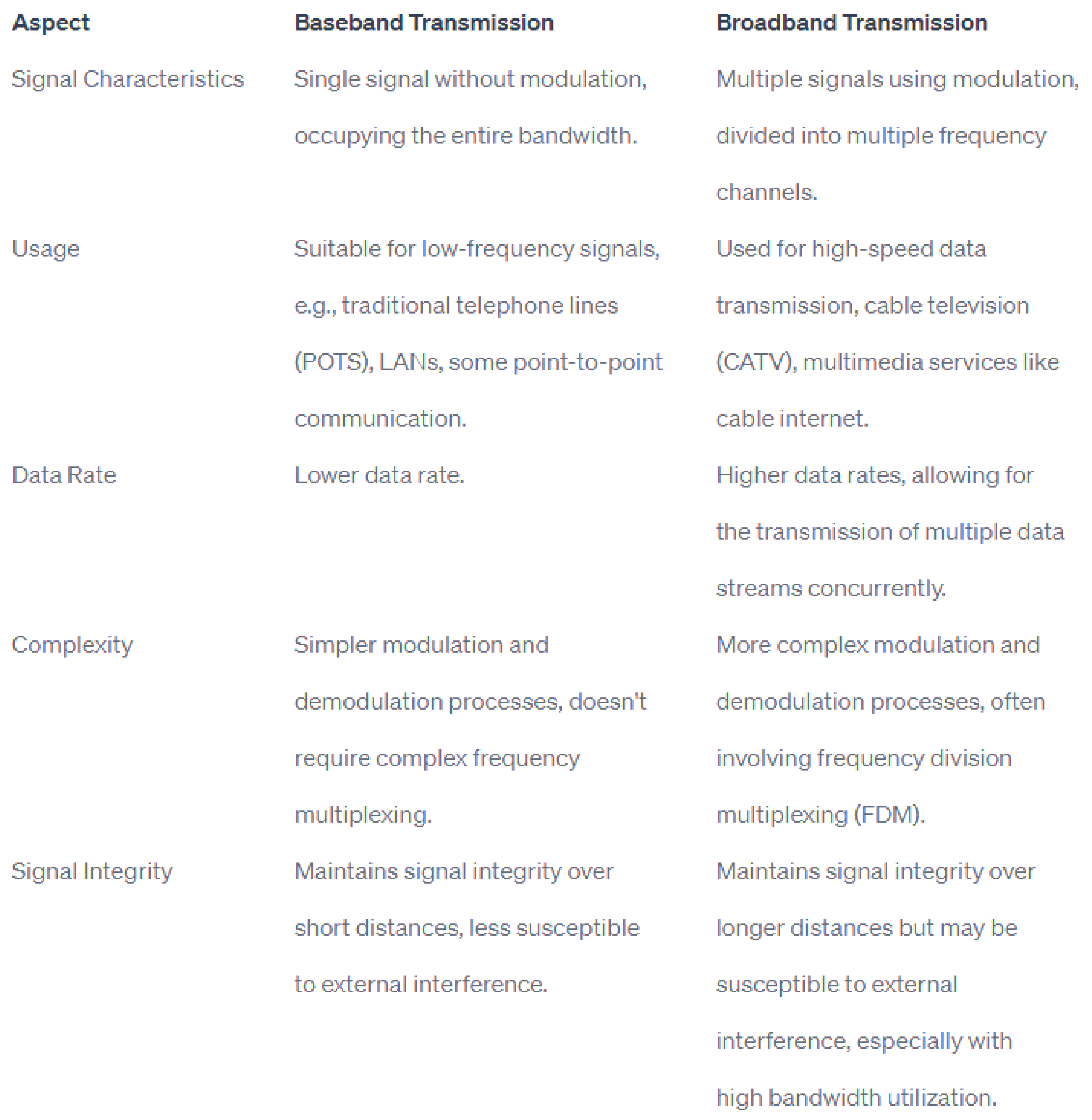
1. **Dedicated Connection:** When a call or data session is initiated, a dedicated circuit or connection is established between the sender and receiver. This connection remains open until the session is terminated.
2. **Suitability for Real-Time Communication:** Circuit switching is well-suited for real-time communication applications, such as traditional telephone calls, where a constant and predictable connection quality is essential.
3. **Fixed Bandwidth:** The allocated bandwidth for a circuit-switched connection remains fixed throughout the call, providing consistent quality but potentially wasting resources during periods of silence.
4. **Inefficient for Data Networks:** Circuit switching is not efficient for data communication networks where variable data rates and bursty traffic patterns are common.

### Applications of Circuit Switching

Circuit switching is commonly used in traditional telephony services, such as PSTN (Public Switched Telephone Network) and ISDN (Integrated Services Digital Network). It is also used in some specialized applications, such as video conferencing and ATM (Asynchronous Transfer Mode) networks.

- Advantages of Circuit Switching: Guaranteed bandwidth,Low latency,Circuit switching offers low latency,Quality of service (QoS)

## 5. Illustrate the differences between baseband transmission and broadband transmission.



| Aspect | Baseband Transmission | Broadband Transmission |
|---|---|---|
| Signal Characteristics | Single signal without modulation, occupying the entire bandwidth. | Multiple signals using modulation, divided into multiple frequency channels. |
| Usage | Suitable for low-frequency signals, e.g., traditional telephone lines (POTS), LANs, some point-to-point communication. | Used for high-speed data transmission, cable television (CATV), multimedia services like cable internet. |
| Data Rate | Lower data rate. | Higher data rates, allowing for the transmission of multiple data streams concurrently. |
| Complexity | Simpler modulation and demodulation processes, doesn't require complex frequency multiplexing. | More complex modulation and demodulation processes, often involving frequency division multiplexing (FDM). |
| Signal Integrity | Maintains signal integrity over short distances, less susceptible to external interference. | Maintains signal integrity over longer distances but may be susceptible to external interference, especially with high bandwidth utilization. |

## 6. Summarize TCP/IP Model. Explain the functions and protocols and services of each layer. Compare it with OSI Model.

TCP/IP Model:

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a concise networking framework used in the design and operation of the Internet. It consists of four layers:

1. Network Interface (Link) Layer: Handles the physical transmission of data over a network medium. It deals with hardware addressing, error detection, and access control.

2. Internet Layer: Manages routing and forwarding of data packets between devices across different networks. It enables addressing, packet switching, and routing.

3. Transport Layer: Manages end-to-end communication, ensuring data reliability and integrity. It segments and reassembles data and provides error detection and correction.

4. Application Layer: Supports application-level services and network applications. It deals with user interfaces, data exchange formats, and communication processes.

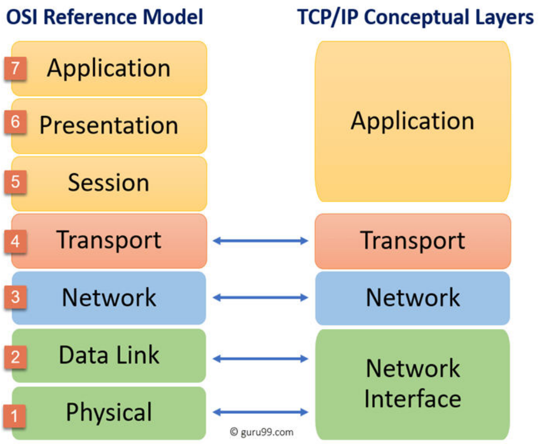
Comparison with OSI Model:

- Number of Layers: TCP/IP has four layers, OSI has seven.

- Development Origin: TCP/IP evolved with the Internet, while OSI is more theoretical.

- Layer Correspondence: TCP/IP layers do not directly correspond to OSI layers.

- Real-World Relevance: TCP/IP is the dominant model for practical networking, while OSI is primarily a reference model.



## 7.With a neat sketch and Explain ISO/OSI reference model.

The OSI model, or Open Systems Interconnection model, is a conceptual framework that describes this layered architecture of computer networks

1. Application Layer: The application layer provides network services to applications, such as file transfer, email, and web browsing. It is the layer that users interact with directly.

2. Presentation Layer: The presentation layer handles data representation and encryption. It ensures that data is formatted in a way that can be understood by both the sender and receiver.

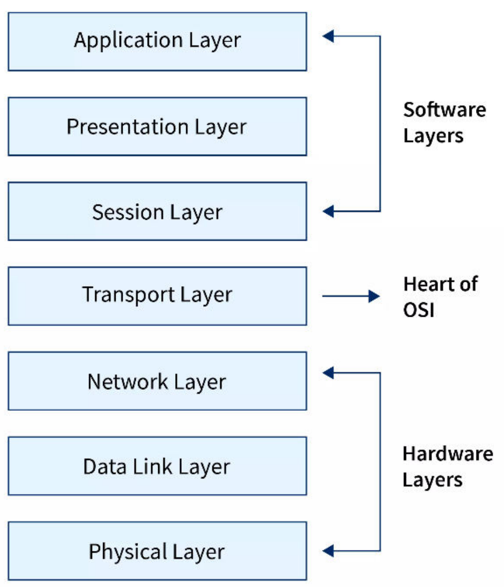
3. Session Layer: The session layer establishes, manages, and terminates sessions between applications. It creates a logical connection between two applications that can be used to exchange data.

4. Transport Layer: The transport layer provides reliable data transfer between applications. It breaks down data into packets, adds error-checking information, and ensures that packets are delivered correctly.

5. Network Layer: The network layer handles routing and addressing of data packets. It determines the best path for packets to take through the network and adds addressing information so that packets can be delivered to the correct destination.

6. Data Link Layer: The data link layer handles error detection and correction for data transmission over a physical link. It checks for errors in data transmission and retransmits data if necessary.

7. Physical Layer: The physical layer provides the physical and electrical characteristics of the network. It defines the physical connections between devices and the electrical signals that are used to transmit data.



**8.Define topology and Explain the various topologies of the network.- PART-B 3Q**

**9. Discuss and Compare various types of networks.**

Local Area Network (LAN): A small network connecting devices within a limited area, such as a home or office, using wired or wireless technologies.

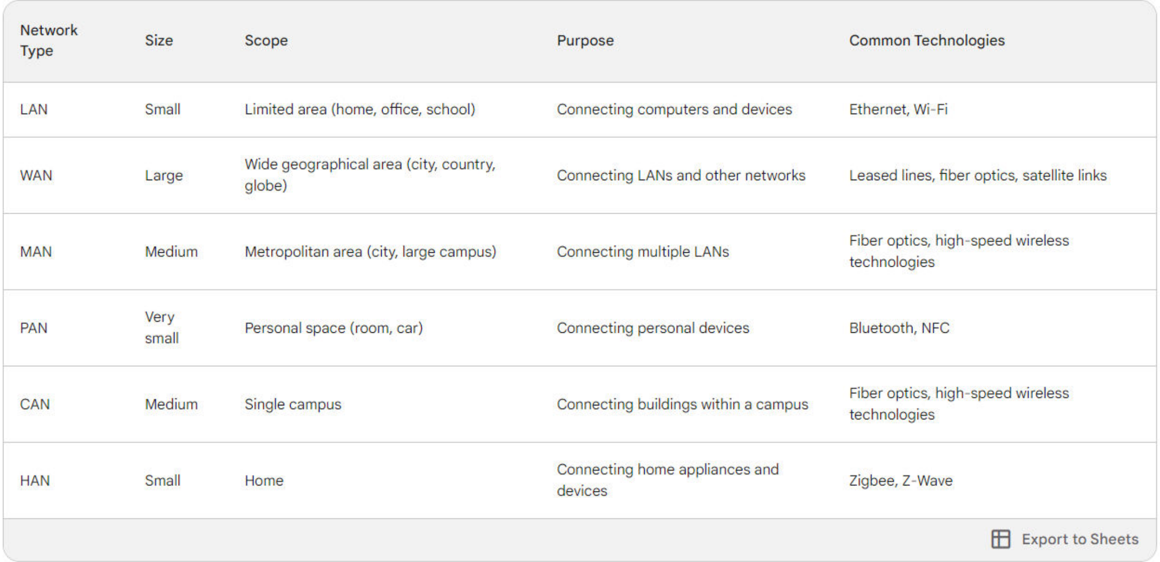
Wide Area Network (WAN): A large network connecting LANs over a wider geographical area, such as a city or country, using leased lines, fiber optics, or satellite links.

Metropolitan Area Network (MAN): A network connecting multiple LANs within a metropolitan area, providing higher bandwidth and advanced features.

Personal Area Network (PAN): A very small network connecting personal devices within a personal space, such as a room or car, using short-range wireless technologies.

Campus Area Network (CAN): A network connecting multiple buildings within a single campus, providing a balance between coverage and performance.

Home Area Network (HAN): A network connecting home appliances and devices within a home, enabling remote control and automation.



| Network Type | Size | Scope | Purpose | Common Technologies |
|---|---|---|---|---|
| LAN | Small | Limited area (home, office, school) | Connecting computers and devices | Ethernet, Wi-Fi |
| WAN | Large | Wide geographical area (city, country, globe) | Connecting LANs and other networks | Leased lines, fiber optics, satellite links |
| MAN | Medium | Metropolitan area (city, large campus) | Connecting multiple LANs | Fiber optics, high-speed wireless technologies |
| PAN | Very small | Personal space (room, car) | Connecting personal devices | Bluetooth, NFC |
| CAN | Medium | Single campus | Connecting buildings within a campus | Fiber optics, high-speed wireless technologies |
| HAN | Small | Home | Connecting home appliances and devices | Zigbee, Z-Wave |

## 10. List out and Explain the applications of Computer Networks.

list of the applications of computer networks, with brief explanations:

1. Communication: Computer networks enable users to communicate with each other through various means, including email, instant messaging, video conferencing, and VoIP (Voice over IP) calls.

2. Resource Sharing: Computer networks allow users to share resources, such as files, printers, and network storage, making them more accessible and efficient.

3. Information Access: Computer networks provide access to the World Wide Web, enabling users to browse websites, search for information, and access online databases and e-learning platforms.

4. E-commerce: Computer networks facilitate online shopping, banking, and electronic payment systems, enabling convenient and secure transactions.

5. Entertainment: Computer networks enable users to enjoy online gaming, streaming media, and social media interactions, providing a variety of entertainment options.

6. Remote Access: Computer networks allow users to access computers and data remotely, enabling flexible work arrangements and access from anywhere with an internet connection.

7. Network Security: Computer networks employ various security measures, such as firewalls and encryption, to protect data and systems from unauthorized access and cyber threats.

8. Network Management: Computer networks enable network administrators to monitor, manage, and troubleshoot network performance and ensure its stability and reliability.

9. Research and Collaboration: Computer networks facilitate research and collaboration by enabling scientists, researchers, and professionals to share data, communicate ideas, and work together remotely.

10. Education and Learning: Computer networks support online education, enabling students to access educational resources, participate in virtual classrooms, and connect with educators and peers.

### 11.Define OSI Model. Explain the functions and protocols and services of each layer.= PART-B 6Q

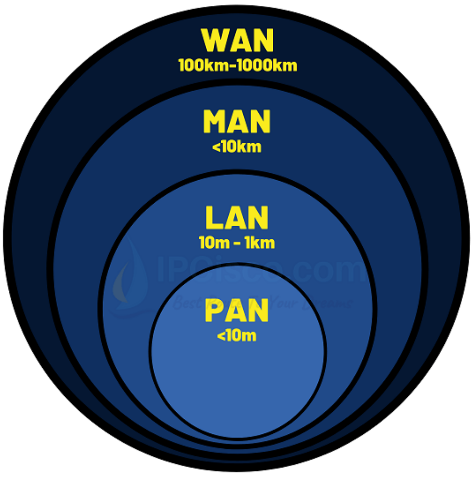
## 12. Explain the following:- a) LAN b) MAN c) WAN d) ARPANET

a) LAN (Local Area Network)

- Connects devices within a limited area, such as a home, office, or school.
- Typically interconnected using wired or wireless technologies.
- Characterized by high speeds, low latency, and ease of management.
- Common applications include file sharing, printer sharing, and network gaming.

b) MAN (Metropolitan Area Network)

- Connects multiple LANs within a metropolitan area, such as a city or large campus.
- Provides higher bandwidth and more advanced features than LANs.
- Suitable for applications that require high-speed data transfer and collaboration.
- Common applications include video conferencing, enterprise resource planning, and cloud computing.



c) WAN (Wide Area Network)

- Spans a large geographical area, such as a city, country, or even the entire globe.
- Connects LANs and other networks, enabling communication and resource sharing over long distances.
- Typically uses leased lines, fiber optics, or satellite links for data transmission.
- Common applications include internet access, corporate communication, and remote access.

d) ARPANET (Advanced Research Projects Agency Network)

- The first packet-switching network, developed in the 1960s by the U.S. Department of Defense.
- Laid the foundation for the modern internet, connecting researchers at different institutions.
- Pioneered the use of TCP/IP, the standard communication protocol suite for the internet.
- Was decommissioned in 1990 but its legacy lives on in the global internet we use today.

## 13. Discuss how OSI and ISO related to each other.

The Open Systems Interconnection (OSI) model and the International Organization for Standardization (ISO) are closely related entities that have played a significant role in the development of computer networking standards. Here's a discussion of their relationship:

### ISO

The International Organization for Standardization (ISO) is a non-governmental international organization that develops and publishes international standards. ISO is the world's largest developer of voluntary international standards. ISO standards cover a wide range of subjects, including technology, food safety, and environmental protection..

### OSI Model

The Open Systems Interconnection (OSI) model is a conceptual framework that describes the architecture of computer networks. It was developed by the International Organization for Standardization (ISO) in the 1980s. The OSI model is a seven-layer model that divides the network into seven abstraction layers, each of which performs a specific function. The OSI model provides a common framework for developing and understanding network protocols and technologies. The OSI model is a valuable tool for understanding and designing computer networks. It is widely used in industry and it is supported by a large body of documentation and tools.

### Relationship between ISO and OSI Model

The OSI model is a product of ISO's standardization efforts. ISO's Technical Committee on Open Systems Interconnection (ISO/TC 97) was responsible for the development of the OSI model. The model was published as an ISO standard in 1984, becoming ISO 7498.

The OSI model has had a significant impact on the development of computer networking. It has been widely adopted by network designers and implementers, and it has helped to ensure interoperability between different network devices and software.

- ✓ OSI is an ISO standard.
- ✓ ISO developed the OSI model.
- ✓ ISO promotes the use of the OSI model.

## 14. Illustrate some of the factors that determine whether a unification system is a LAN or WAN.

the factors that determine whether a unification system is a LAN or WAN:

Geographical area spanned:

- **LAN:** A LAN typically spans a limited geographical area, such as a home, office, or school.
- **WAN:** A WAN spans a large geographical area, such as a city, country, or even the entire globe.

Network topology:

- **LAN:** LANs typically use bus, star, or ring topologies.
- **WANs:** WANs typically use point-to-point, mesh, or star topologies.

Transmission medium:

- **LAN:** LANs typically use twisted-pair cables, coaxial cables, or fiber optic cables.
- **WANs:** WANs typically use leased lines, fiber optic cables, or satellite links.

Bandwidth:

- **LAN:** LANs typically have high bandwidth, allowing for fast data transfer.

- **WANs:** WANs typically have lower bandwidth than LANs, which can result in slower data transfer.

Latency:

- **LAN:** LANs typically have low latency, meaning there is little delay between sending and receiving data.
- **WANs:** WANs typically have higher latency than LANs, which can result in noticeable delays.

Cost:

- **LAN:** LANs are typically less expensive to set up and maintain than WANs.
- **WANs:** WANs can be more expensive to set up and maintain than LANs due to the cost of leased lines, fiber optic cables, or satellite links.

## 15. Discuss Shannon Capacity with example

### Shannon Capacity

In the realm of telecommunications, Shannon capacity, also known as channel capacity, refers to the maximum rate at which information can be transmitted reliably over a communication channel.

$$C = B * \log_2(1 + S/R)$$

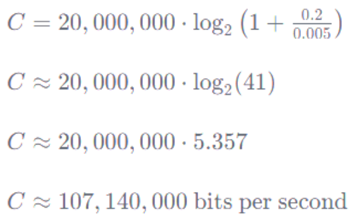
- *C* is the channel capacity in bits per second.
- *B* is the bandwidth of the channel in hertz.
- *S* is the signal power.
- *N* is the noise power.

Shannon capacity is measured in bits per second (bps) and is determined by two primary factors:

1. Channel bandwidth: The bandwidth of a channel represents the range of frequencies that can be transmitted over it. A wider bandwidth allows for more information to be transmitted per unit of time.

2. Signal-to-noise ratio (SNR): The SNR is a measure of the strength of the desired signal compared to the background noise. A higher SNR indicates a clearer signal and allows for more reliable transmission of information.

let's consider a practical example involving a Wi-Fi connection. Imagine you have a Wi-Fi router operating in a certain frequency band with a bandwidth (*B*) of 20 megahertz (20,000,000 hertz). The signal power (*S*) is 200 milliwatts, and the noise power (*N*) is 5 milliwatts.



$$C = 20,000,000 \cdot \log_2\left(1 + \frac{0.2}{0.005}\right)$$

$$C \approx 20,000,000 \cdot \log_2(41)$$

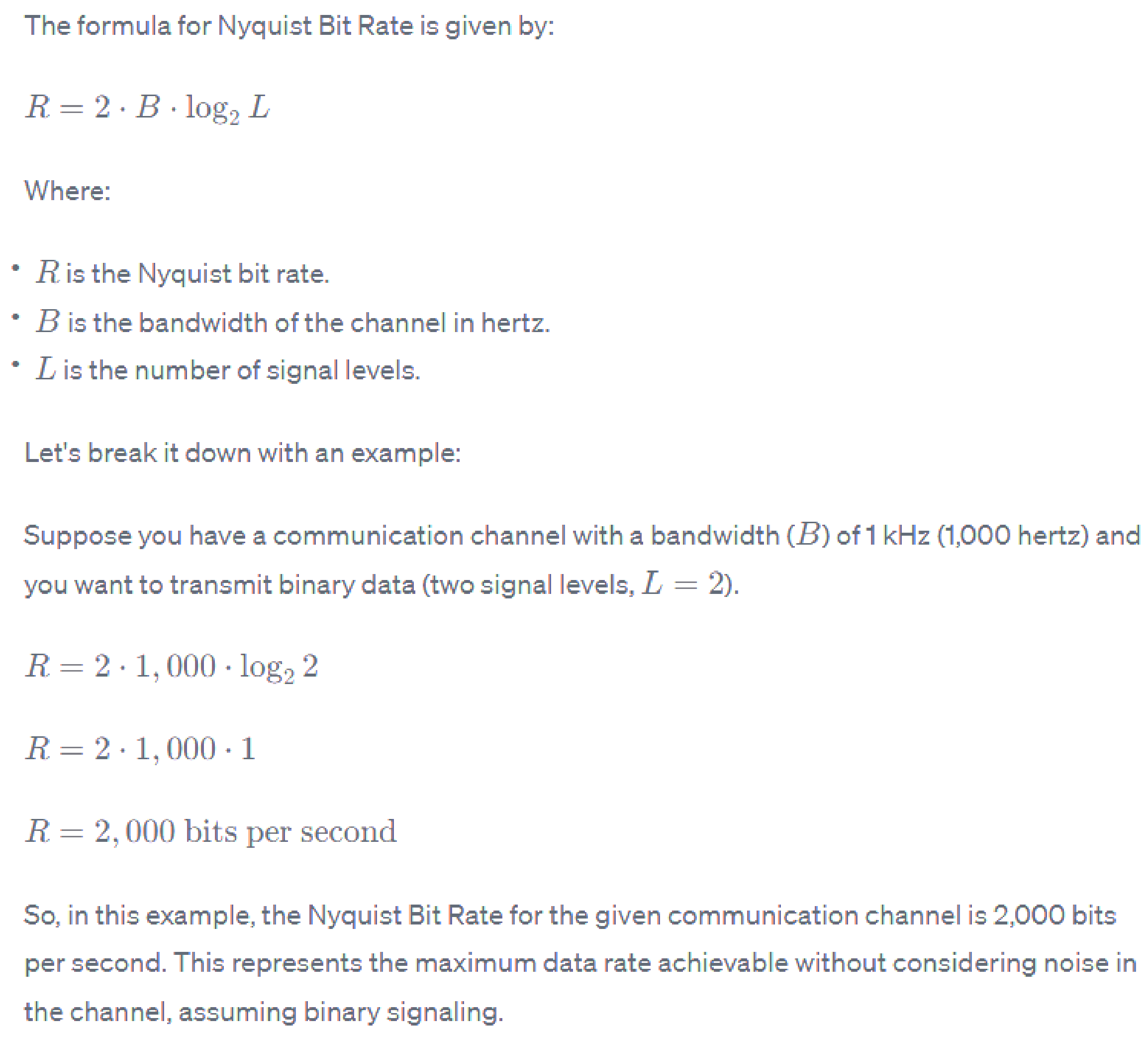
$$C \approx 20,000,000 \cdot 5.357$$

$$C \approx 107,140,000 \text{ bits per second}$$

In this example, the Shannon Capacity for your Wi-Fi channel would be approximately 107,140,000 bits per second.

## 16. Discuss Nyquist Bit Rate with example

Nyquist Bit Rate is a concept in digital communication that determines the maximum data rate (in bits per second) for a noise-free channel. It's named after Harry Nyquist, a pioneer in information theory.



The formula for Nyquist Bit Rate is given by:

$$R = 2 \cdot B \cdot \log_2 L$$

Where:

- $R$ is the Nyquist bit rate.
- $B$ is the bandwidth of the channel in hertz.
- $L$ is the number of signal levels.

Let's break it down with an example:

Suppose you have a communication channel with a bandwidth ($B$) of 1 kHz (1,000 hertz) and you want to transmit binary data (two signal levels, $L = 2$).

$$R = 2 \cdot 1,000 \cdot \log_2 2$$

$$R = 2 \cdot 1,000 \cdot 1$$

$$R = 2,000 \text{ bits per second}$$

So, in this example, the Nyquist Bit Rate for the given communication channel is 2,000 bits per second. This represents the maximum data rate achievable without considering noise in the channel, assuming binary signaling.

The Nyquist bit rate is a fundamental result in digital signal processing. It has had a profound impact on the development of telecommunications systems, and it is still used today to design and analyze digital communication systems.

## 17. Define bit rate and explain the factors that effects the bit rate

Bit Rate

In digital communications, bit rate, also known as data rate or transmission rate, refers to the number of bits of data that are transmitted or processed per unit of time. It is typically measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), gigabits per second (Gbps), or terabits per second (Tbps).

Bit rate plays a crucial role in determining the quality and speed of data transmission. Higher bit rates allow for faster data transfer and better quality of audio, video, and other multimedia content. However, higher bit rates also require more bandwidth, which can be a limiting factor for some networks.

Factors Affecting Bit Rate

Several factors can affect the bit rate of a digital transmission:

1. Bandwidth: Bandwidth is the range of frequencies that a communication channel can support. A wider bandwidth allows for higher bit rates.

2. Data Format: The format of the data being transmitted can also affect the bit rate. For example, compressed data typically has a lower bit rate than uncompressed data.

3. Encoding Scheme: The encoding scheme used to represent the data can also affect the bit rate. For example, different audio and video codecs have different bit rates for the same level of quality.

4. Error Correction: Error correction techniques can add redundancy to the data stream, increasing the bit rate to ensure data integrity.

5. Transmission Medium: The physical medium used for data transmission can also affect the bit rate. For example, fiber optic cables typically support higher bit rates than copper cables.

6. Signal-to-Noise Ratio (SNR): The SNR is the ratio of the desired signal to the background noise in a communication channel. A higher SNR allows for higher bit rates without sacrificing quality.

7. Transmission Distance: Longer transmission distances can lead to signal attenuation and interference, which may require lower bit rates to maintain data integrity.

8. Application Requirements: The specific application using the data transmission also influences the bit rate

## 18. Which characteristics affect the quality of service offered by a network? Justify your answer with proper example

Several characteristics affect the quality of service (QoS) offered by a network. These characteristics determine the performance and reliability of a network in delivering data and applications to users. Here are some of the key characteristics that influence QoS:

1. Bandwidth: Bandwidth is the amount of data that can be transmitted over a network per unit of time. It is typically measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), gigabits per second (Gbps), or terabits per second (Tbps). Adequate bandwidth is essential for supporting high-bandwidth applications like video conferencing, streaming media, and large file transfers.

Example: A network with insufficient bandwidth for a video conference call can result in choppy video, audio delays, and overall poor communication experience.

2. Latency: Latency, also known as network delay or lag, is the time it takes for a data packet to travel from its source to its destination. It is typically measured in milliseconds (ms). Low latency is crucial for real-time applications like online gaming, video conferencing, and voice over IP (VoIP) calls.

Example: High latency in an online game can lead to noticeable delays between player actions and the game's response, making it difficult to compete effectively.

3. Jitter: Jitter is the variation in latency between data packets. It is caused by factors such as network congestion, routing changes, and hardware limitations. Excessive jitter can disrupt the flow of data, causing audio and video playback to become choppy or distorted.

Example: Jitter in a video streaming service can lead to fluctuations in video quality, making it difficult to watch smoothly.

4. Packet Loss: Packet loss occurs when data packets fail to reach their destination due to network congestion, errors in transmission, or hardware failures. Packet loss can disrupt the flow of data, causing data corruption or application interruptions.

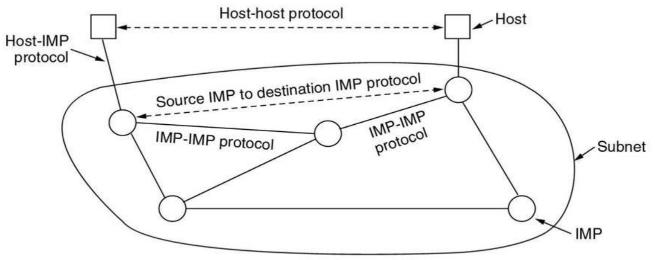
Example: Packet loss in a file transfer can lead to incomplete or corrupted files, requiring retransmissions and affecting overall transfer efficiency.

5. Security: Network security is the protection of network resources and data from unauthorized access, modification, or destruction. It involves implementing measures to prevent cyberattacks, data breaches, and other malicious activities.

Example: A network with weak security measures can be vulnerable to cyberattacks, potentially leading to data breaches, financial losses, and damage to an organization's reputation.

## 19. Discuss briefly about the original ARPANET design

The Advanced Research Projects Agency Network (ARPANET) was the first packet-switching network, developed in the 1960s by the U.S. Department of Defense. It is considered the precursor to the modern internet, and its design principles have had a profound impact on the development of computer networks.



The original ARPANET design.

Ch 1-4

The original ARPANET design was based on several key principles:

1. Distributed Control: The network was designed without a central controller. Instead, each node in the network was responsible for routing packets to their destination. This distributed approach made the network more resilient to failures, as any single node could go down without affecting the entire network.

2. Packet Switching: Data was broken down into small packets, each with its own routing information. This allowed for efficient use of network bandwidth, as packets could be sent independently of each other and take different routes through the network.

3. Adaptive Routing: Each node in the network maintained a routing table that was used to determine the best path for each packet. This routing table was updated dynamically based on the current state of the network, allowing the network to adapt to congestion and failures.

4. Error Detection and Correction: Each packet included error detection and correction codes to ensure data integrity. This allowed for reliable transmission of data even over unreliable communication links.

The original ARPANET design was a groundbreaking achievement that paved the way for the modern internet. Its principles of distributed control, packet switching, adaptive routing, and error detection and correction are still fundamental to the way computer networks operate today.

## 20. Explain the significance of Switching? What are different switching techniques used in computer networks? Discuss.

Switching is a fundamental process in computer networking that enables the transfer of data packets between different devices on a network. It plays a crucial role in connecting computers, routers, and other networking devices, allowing them to communicate and exchange information efficiently. The significance of switching lies in its ability to:

1. Improve Network Performance: Switching utilizes dedicated paths for data transmission, reducing congestion and allowing multiple data streams to flow simultaneously. This leads to faster data transfer speeds and improved network performance overall.

2. Enhance Network Efficiency: Switching eliminates the need for every device on the network to receive and process every data packet. Instead, data packets are only sent to the intended destination, reducing network overhead and improving network efficiency.

3. Increase Network Scalability: Switching enables the expansion of networks by allowing the addition of more devices without affecting the overall performance. This makes networks more scalable and adaptable to changing requirements.

4. Reduce Network Collision: In traditional bus-based networks, data collisions can occur when multiple devices attempt to transmit data simultaneously. Switching eliminates this issue by creating dedicated paths for data transmission, preventing collisions and ensuring reliable data transfer.

5. Enable Network Segmentation: Switching allows the division of large networks into smaller segments, making it easier to manage and isolate network traffic. This enhances network

### Switching Techniques

- **Circuit Switching:** Establishes a dedicated path before transmission, ensuring continuous data flow.
- **Packet Switching:** Divides data into packets, routed independently for efficient resource use.
- **Frame Switching:** Operates at the data link layer, using frames with error detection and correction.
- **Cell Switching:** Divides data into fixed-size cells, ideal for high-bandwidth applications.
- **Cut-through Switching:** Forwards packets upon receiving the destination address, reducing latency.
- **Store-and-forward Switching:** Buffers the entire packet before forwarding, allowing error detection.
- **Hybrid Switching:** Combines different techniques, leveraging strengths for specific network needs.