

REGULAR/BACK EXAM-2080 BHADRA\

1. What is internet? Explain classification of computer network.

The **Internet** is a **global system of interconnected computer networks** that use standardized communication protocols (TCP/IP) to link billions of devices worldwide. It is a **network of networks** that enables the sharing of information, resources, and services across geographical boundaries.

Classification of Computer Networks

Computer networks can be classified based on geographical coverage, ownership, topology, and transmission medium. Let's go deep into each category:

1. Based on Geographical Area

- LAN (Local Area Network)
- Covers a small area such as an office, school, or building.
- High speed (up to 1 Gbps or more), low cost.
- Example: College computer lab network, office intranet.
- MAN (Metropolitan Area Network)
- Covers a city or metropolitan area.
- Connects multiple LANs using high-speed fiber optics.
- Example: Cable TV networks, city-wide Wi-Fi, metro rail communication systems.
- WAN (Wide Area Network)
- Covers large geographical areas (country, continent, world).
- Uses satellite links, leased lines, and public telecommunication systems.
- Internet is the largest WAN.
- Example: Banking networks, multinational company networks, the global Internet itself.

2. Based on Ownership

- Private Network
- Owned and managed by a single organization.
- Provides secure communication within the organization.
- Example: Corporate intranet, university campus network.
- Public Network
- Accessible to the general public.
- Managed by ISPs and government agencies.
- Example: Internet, public Wi-Fi hotspots.

3. Based on Topology

Topology refers to the physical or logical arrangement of nodes in a network.

- Bus Topology
- All devices connected to a single backbone cable.
- Simple and cost-effective, but prone to collisions.
- Star Topology
- Devices connected to a central hub/switch.
- Easy to manage, scalable, but hub failure disrupts the network.
- Ring Topology
- Devices connected in a circular loop.
- Data travels in one direction; failure of one node can affect the whole ring.

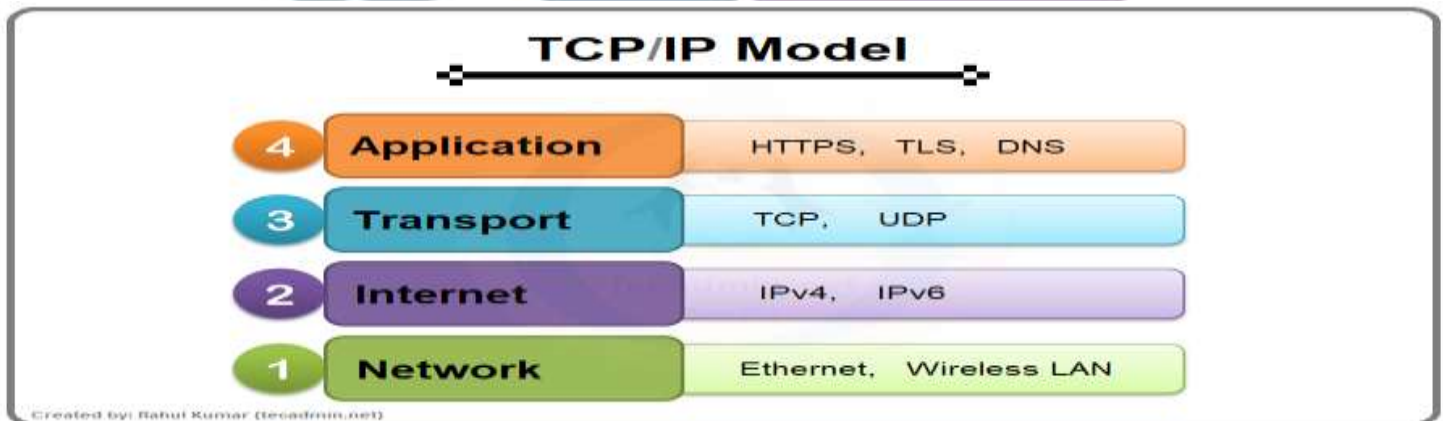
- Mesh Topology
- Devices interconnected with multiple paths.
- Provides redundancy and reliability, but costly to implement.

4. Based on Transmission Medium

- Wired Networks
- Use cables such as Ethernet, coaxial, or fiber optics.
- High speed, secure, but limited mobility.
- Wireless Networks
- Use radio waves, infrared, or satellite communication.
- Examples: Wi-Fi, Bluetooth, cellular networks (3G/4G/5G).
- Provide mobility but are more prone to interference and security risks..

2. What is internet Protocol (IP)? Explain TCP/IP model.

Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite (commonly known as TCP/IP) for relaying datagrams (packets of data) across network boundaries. Its routing function enables internetworking — hence the name "Internet Protocol".



The TCP/IP Model

The TCP/IP model, or [Internet Protocol Suite](#), is the conceptual framework for modern networking, developed by the U.S. Department of Defense in the 1970s. It operates through four functional layers:

1. **[Application Layer \(Top Layer\)](#)**: Handles high-level protocols, issues of representation, encoding, and dialogue control. Examples include HTTP, FTP, SMTP, and DNS.
2. **[Transport Layer](#)**: Manages end-to-end communication, flow control, segmentation, and error correction. The primary protocols are TCP (reliable) and UDP (fast, unreliable).
3. **[Internet Layer](#)**: Responsible for logical addressing (IP addresses) and routing packets across multiple networks. This is where the Internet Protocol (IP) resides.
4. **[Network Access/Link Layer \(Bottom Layer\)](#)**: Manages physical transmission, addressing, and framing of data on the physical network medium (e.g., Ethernet, Wi-Fi).

How TCP/IP Works

Data is packaged, addressed, and routed through these layers, starting from the Application layer down to the Network Access layer for transmission, and reversed at the destination.

3. Explain IEEE 802.3 and IEEE 802.4. Explain (CSMA/CD) LAN architecture.

IEEE 802.3 (Ethernet / CSMA/CD Standard)

IEEE 802.3 is the IEEE standard that defines **wired Ethernet** networks. It specifies the **physical layer** (PHY) and **media access control** (MAC) sublayer of the data link layer for **local area networks (LANs)** and some metropolitan/wide area applications.

- **Developed** — Based on the original Ethernet (DIX standard by DEC, Intel, Xerox in 1980), standardized by IEEE in 1983.
- **Access method** — **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** — for shared/half-duplex media (early versions).
- **Topology** — Originally bus (coaxial cable), now mostly star (twisted pair with switches/hubs).
- **Speeds** — Evolved from 10 Mbps (10BASE5/10BASE2) → 100 Mbps (Fast Ethernet) → 1 Gbps → 10/25/40/100/400 Gbps today.
- **Key features** — Uses frames with preamble, destination/source MAC addresses, length/type field, data, FCS (CRC). Modern Ethernet is full-duplex (no collisions) on switched networks, so CSMA/CD is rarely used except in legacy/shared media.
- **Current status** — Dominant wired LAN technology worldwide; IEEE 802.3-2022 is the latest consolidated version (supports up to 400 Gb/s and beyond).

Main use — Office networks, data centers, home networks, industrial Ethernet.

IEEE 802.4 (Token Bus Standard)

IEEE 802.4 is the IEEE standard for **Token Bus** networks (released around 1985, now withdrawn/archived).

- **Access method** — **Token passing** on a logical ring over a physical bus/tree topology.
- **Topology** — Physical: Bus or tree (coaxial cable or fiber). Logical: Virtual ring (stations form a sequence, token circulates in order).
- **How it works** — A special "token" frame circulates. Only the station holding the token can transmit data. After transmission (or timeout), it passes the token to the next station in the logical ring sequence.
- **Speeds** — 1, 5, 10 Mbps (phase-coherent FSK or broadband); some fiber variants up to 20 Mbps.
- **Key features** — Deterministic access (predictable wait time, good for real-time/industrial), priority levels, no collisions (token ensures only one transmitter).
- **Main use** — Industrial/manufacturing automation (e.g., General Motors' MAP — Manufacturing Automation Protocol in 1980s).
- **Current status** — Obsolete/withdrawn by IEEE; replaced by modern Ethernet (IEEE 802.3) in industrial settings.

Why 802.4 existed — In 1980s, Ethernet's probabilistic CSMA/CD couldn't guarantee max wait time for real-time factory control → token bus provided bounded delay.

CSMA/CD LAN Architecture (IEEE 802.3 Style)

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is the **media access control (MAC) protocol** originally used in IEEE 802.3 Ethernet on shared (half-duplex) media like coaxial bus or early hubs.

Architecture & How CSMA/CD Works (Step-by-Step)

1. **Carrier Sense** Before transmitting, a station listens ("senses") the shared medium (cable/bus) to check if it's idle (no carrier signal). If busy → wait (defer transmission).
2. **Multiple Access** All stations share the same medium → any can transmit when idle → possible simultaneous starts.
3. **Transmission** If idle → station starts sending frame (preamble + data).
4. **Collision Detection** While transmitting, station continues monitoring the medium. If it detects interference (higher voltage/signal mismatch = collision) → collision occurred (two+ stations transmitted at once).
5. **Collision Handling**
 - Stop transmitting immediately.
 - Send a **jam signal** (short bit pattern) to ensure all stations detect collision.
 - Wait random backoff time (truncated binary exponential backoff algorithm) to avoid repeated collisions.

- Retry after backoff (up to 16 attempts).

Typical LAN Architecture Using CSMA/CD (Classic/Original)

- **Bus topology** — All stations connected to single coaxial cable (e.g., 10BASE5 thicknet or 10BASE2 thinnet).
- **Shared medium** — Half-duplex → transmit OR receive at a time.
- **Repeaters/hubs** — Extend cable or connect segments (still shared collision domain).
- **Collision domain** — All devices that can collide (entire bus or hub segment).
- Modern replacement → Switched full-duplex Ethernet (no shared medium, no collisions, CSMA/CD not needed).

Advantages of CSMA/CD — Simple, low cost, fair access in low traffic. **Disadvantages** — Inefficient in high traffic (many collisions), non-deterministic delay.

4. What is transmission media? Explain its types with example.

Transmission media refers to the physical or logical pathways through which data is transmitted from one device to another in a computer network. It acts as the carrier of information in the form of electrical signals, light pulses, or electromagnetic waves.

Guided Media (Wired / Bounded)

In Guided Media, the signals are directed and confined within a physical path. These are cables that physically connect devices.

A. Twisted Pair Cable

It consists of two insulated copper wires twisted together to reduce electromagnetic interference. It is the most common cable used in local networks.

- **Example: Ethernet cables** (like Cat5 or Cat6) used to connect your PC to a router.

B. Coaxial Cable

This cable has a central copper conductor surrounded by an insulating layer and a braided metallic shield. It can carry higher-frequency signals than twisted pair.

- **Example: The TV cable** (dish cable) used to connect your television to the setup box or antenna.

C. Fiber Optic Cable

It uses thin strands of glass or plastic to transmit data as pulses of **light**. It offers extremely high speeds and is immune to electrical noise.

- **Example: High-speed internet backbones** used by ISPs (like WorldLink or Vianet) to provide fiber internet to homes.

2. Unguided Media (Wireless / Unbounded)

Unguided Media transmits electromagnetic waves through the air, vacuum, or water without using a physical conductor.

A. Radio Waves

These are electromagnetic waves that are omnidirectional, meaning they travel in all directions. They can easily penetrate walls.

- **Example: Wi-Fi** networks, Bluetooth, and AM/FM Radio.

B. Microwaves

Microwaves are unidirectional waves that require a "Line of Sight." This means the sender and receiver antennas must be perfectly aligned with each other.

- **Example: Satellite communication** (like GPS) and terrestrial microwave towers used for long-distance phone signals.

C. Infrared

These are high-frequency waves used for very short-range communication. They cannot pass through solid objects like walls.

- **Example: Your TV Remote control** or wireless computer mouse.

5. What is data link layer? Explain different data link layer protocols.

The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model, positioned between the Physical Layer and the Network Layer. It is responsible for node-to-node delivery of data frames over a physical medium.

Different Data Link Layer Protocols

1. Ethernet (IEEE 802.3)

This is the most widely used protocol for wired LANs. It uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) algorithm to manage how multiple computers share a single cable. It is known for its simplicity and efficiency in local environments.

2. Point-to-Point Protocol (PPP)

PPP is used to establish a direct connection between two nodes (e.g., connecting your home router to your ISP's server). It provides authentication (making sure you are who you say you are), encryption, and data compression. It is commonly used over phone lines, cellular networks, and fiber links.

3. High-Level Data Link Control (HDLC)

HDLC is a bit-oriented protocol used for both point-to-point and point-to-multipoint links. It ensures that data is transmitted reliably by using "bit stuffing" to mark the beginning and end of frames. It was the basis for many later protocols like PPP.

4. Frame Relay

Frame Relay is an efficient technology used mainly in Wide Area Networks (WANs). It is "packet-switched" and designed for cost-effective data transmission between intermittent traffic across digital networks. It skips most error-correction to achieve higher speeds, assuming the underlying fiber lines are already reliable.

5. Token Ring (IEEE 802.5)

In this protocol, all computers are connected in a logical ring. A small frame called a **token** circulates around the ring. A computer can only send data if it catches the token. This prevents collisions entirely, making it very predictable (deterministic).

6. ATM (Asynchronous Transfer Mode)

ATM uses small, fixed-size cells (53 bytes) rather than variable-length frames. This allows the network to handle both voice and data very smoothly with low "jitter" or delay. It was very popular in core telecommunications networks.

6.. Explain the necessity of IPv6. Differentiate between IP and MAC address.

Necessity of IPv6.

1. Address Exhaustion
 - IPv4 addresses are limited and almost fully allocated.
 - IPv6 uses 128-bit addresses, providing 3.4×10^{38} unique addresses (virtually unlimited).
2. Support for IoT
 - Billions of IoT devices require unique IP addresses.
 - IPv6 ensures scalability for future growth.
3. Improved Security
 - IPv6 has IPSec (Internet Protocol Security) built-in for authentication and encryption.
4. Better Performance
 - Simplified packet headers improve routing efficiency.
 - Supports multicasting (sending data to multiple devices simultaneously).

5. Auto-Configuration

- IPv6 supports stateless address autoconfiguration (SLAAC), allowing devices to configure themselves automatically.

6. End-to-End Connectivity

- Eliminates the need for NAT (Network Address Translation), restoring direct communication between devices.

7. Future-Proofing

- IPv6 ensures the internet can continue expanding without address limitations.

. Differentiate between IP and MAC address.

S.N.	Feature	IP Address (Internet Protocol)	MAC Address (Media Access Control)
1	Full Form	Internet Protocol Address.	Media Access Control Address.
2	Address Type	It is a Logical Address implemented in software.	It is a Physical Address implemented in hardware.
3	OSI Layer	Operates at the Network Layer (Layer 3).	Operates at the Data Link Layer (Layer 2).
4	Persistence	Temporary/Dynamic. It changes whenever a device connects to a different network.	Permanent/Static. It is "burned" into the Network Interface Card (NIC) during manufacturing.
5	Address Size	32-bit (IPv4) or 128-bit (IPv6).	48-bit.
6	Format	Written in decimal (e.g., 192.168.1.1) or hexadecimal for IPv6.	Written in hexadecimal (e.g., 00-14-22-01-23-45).
7	Assignment	Assigned by the Network Administrator or Internet Service Provider (ISP).	Assigned by the manufacturer of the device's hardware.
8	Function	Used for routing data between different networks across the world.	Used for delivering data to the specific device within a local network (LAN).
9	Configuration	Can be configured manually (Static) or automatically via DHCP.	Usually cannot be changed (though it can be "spoofed" via software).
10	Hierarchy	It is a Hierarchical address , containing a Network ID and a Host ID.	It is a Flat address , meaning it has no inherent geographical or network structure.

7. What is cryptography? Explain its types in detail.

Answer: **Cryptography is the practice and study of techniques for secure communication in the presence of adversaries.** It ensures confidentiality, integrity, non-repudiation, and authentication of data.

Types of Cryptography

There are three main types of cryptography used in modern computing, categorized by how they use "keys" to lock (encrypt) and unlock (decrypt) data.

1. Symmetric Key Cryptography (Private Key)

In this type, the **same single key** is used for both encryption and decryption. Both the sender and the receiver must have a copy of this secret key.

- **How it works:** If Alice wants to send a message to Bob, she locks it with a "Secret Key." Bob then uses that exact same "Secret Key" to unlock it.
- **Pros:** It is extremely fast and efficient for large amounts of data.
- **Cons:** The biggest challenge is "Key Distribution"—how do you get the key to the other person securely without someone else stealing it?
- **Examples:** AES (Advanced Encryption Standard), DES (Data Encryption Standard).

2. Asymmetric Key Cryptography (Public Key)

This type uses a **pair of keys**: a **Public Key** (which everyone can see) and a **Private Key** (which is kept secret by the owner).

- **How it works:** If Alice wants to send a message to Bob, she looks up Bob's Public Key to encrypt the message. However, once locked with the Public Key, **only Bob's Private Key** can unlock it. Even Alice cannot unlock the message once she sends it.
- **Pros:** Highly secure; there is no need to share secret keys.
- **Cons:** It is much slower and requires more "mathematical" power than symmetric encryption.
- **Examples:** RSA (Rivest-Shamir-Adleman), **Digital Signatures**, **SSL/TLS certificates**.

3. Hash Functions

Hash functions are different because they **do not use keys**. Instead, they use a mathematical algorithm to transform any length of data into a fixed-length string of characters (called a "Hash" or "Fingerprint").

- **How it works:** It is a **one-way process**. You can turn a message into a hash, but you can never turn a hash back into the original message. If even one letter in the message changes, the entire hash becomes completely different.
- **Pros:** Excellent for verifying the **integrity** of data.
- **Cons:** Cannot be used for communication (since it can't be decrypted).
- **Examples:** **SHA-256** (used in Bitcoin), **MD5**.

8. Explain client server model. Why security is essence in the server?

The Client-Server Model Explained

In this model, the relationship is based on a **Request-Response** cycle:

- **The Client:** This is usually a user-facing device or application (like a web browser, a mobile app, or your laptop). The client does not share any of its resources but requests content or service from a server.
- **The Server:** This is a powerful machine or software program that manages access to a centralized resource (like a database, a website, or a file storage system). It "serves" the requests sent by clients.

- **The Network:** The communication between the two happens over a network (like the Internet or a LAN) using protocols such as **HTTP** for web pages or **FTP** for files.

Example: When you type `www.google.com` into your browser:

1. Your browser (the **Client**) sends a **Request** for the homepage.
2. Google's computer (the **Server**) processes that request.
3. The server sends the website data back as a **Response**.

Why Security is the Essence in the Server

The server is the central point of communication and storage in the client–server model. Since it holds critical data and services, security is essential for the following reasons:

1. Data Protection

- Servers store sensitive information (user data, financial records, business secrets).
- Without proper security, data breaches can occur, leading to loss of confidentiality.

2. Authentication & Authorization

- Servers must verify user identities and enforce access control.
- Prevents unauthorized users from accessing restricted resources.

3. Integrity of Data

- Ensures that data is not altered maliciously during transmission or storage.
- Techniques like hashing and digital signatures are used.

4. Availability

- Servers must remain available to clients.
- Security measures like firewalls and intrusion detection prevent Denial of Service (DoS) attacks.

5. Protection Against Malware & Attacks

- Servers are prime targets for hackers.
- Security mechanisms (patching, antivirus, intrusion prevention) safeguard against threats.

6. Compliance & Legal Requirements

- Many industries (healthcare, banking) require strict compliance with data protection laws (GDPR, HIPAA).
- Server security ensures organizations meet these standards.

7. Trust & Reliability

- Clients rely on servers for accurate and safe responses.
- A secure server builds trust among users and ensures smooth business operation

9. Define routing. Write differences between switch, hub, repeater and router.

Routing is the process of selecting a path for data packets to travel across a network from the source to the destination. It is performed by routers using routing algorithms and protocols.

Routing ensures efficient, reliable, and correct delivery of data across interconnected networks (LANs, WANs, Internet).

S.N.	Feature	Repeater	Hub	Switch	Router
1	OSI Layer	Physical Layer (Layer 1).	Physical Layer (Layer 1).	Data Link Layer (Layer 2).	Network Layer (Layer 3).
2	Primary Function	Regenerates electrical signals to cover long distances.	Connects multiple devices in a LAN; acts as a multiport repeater.	Connects devices in a LAN and filters data based on MAC addresses.	Connects different networks (e.g., LAN to Internet).
3	Data Form	Bits.	Bits.	Frames.	Packets.
4	Intelligence	Not intelligent; just boosts signal.	Not intelligent; broadcasts data to everyone.	Intelligent; sends data only to the specific destination.	Highly intelligent; finds the best path using IP addresses.
5	Transmission Mode	Half-duplex.	Half-duplex (One talks at a time).	Full-duplex (Everyone can talk at once).	Full-duplex.
6	Broadcast vs. Unicast	Broadcasts everything.	Broadcasts everything to all ports.	Uses Unicast (Point-to-point) after learning MACs.	Uses Unicast or Routing to specific networks.
7	Collisions	High chance of collisions.	High chance of collisions (One collision domain).	Reduces collisions (Every port is a separate domain).	No collisions between networks.
8	Device Address	No address used.	No address used.	Uses MAC Addresses .	Uses IP Addresses .
9	Speed	Slow.	Slow (Shared bandwidth).	Fast (Dedicated bandwidth per port).	Fast (Depends on routing tables).
10	Usage Example	Extending a long Ethernet cable.	Small, old home networks.	Modern office or school LANs.	Connecting your home to your ISP/Internet.

10. Define SMTP. Explain FTP in detail.

SMTP (Simple Mail Transfer Protocol) is a standard protocol used for sending and receiving email messages over the internet. It works at the Application Layer of the OSI model and uses TCP port 25 (or 587 for secure transmission).

Explain FTP (File Transfer Protocol) in Detail

FTP is a standard network protocol used for the transfer of computer files between a client and a server on a computer network. It is built on a **Client-Server architecture**.

How FTP Works (The Dual-Connection System)

Unlike many other protocols, FTP uses **two separate connections** to complete a task:

1. **Control Connection (Port 21):** This is used for sending "commands" and "responses." When you log in with your username and password, that information travels over this connection. It stays open during the entire session.
2. **Data Connection (Port 20):** This is the actual "heavy lifting" connection. It opens only when a file is being transferred and closes as soon as the transfer is finished.

Types of FTP Access

- **Anonymous FTP:** Users can download files without needing an account or password. This is common for public software archives.
- **Authenticated FTP:** Users must provide a valid username and password to access, upload, or download files. This is used for private website management.

FTP Modes of Operation

- **Active Mode:** The client opens a port and waits for the server to connect to it to start the data transfer. (Often blocked by modern firewalls).
- **Passive Mode:** The server opens a port and tells the client to connect to it. This is the more common method today as it is "firewall-friendly."

Pros and Cons of FTP

- **Pros:** It allows for the transfer of very large files, supports "resuming" interrupted transfers, and is highly organized for directory management.
- **Cons:** Standard FTP is **insecure** because it sends your username and password in plain text. (This led to the creation of **SFTP** and **FTPS**, which add encryption).

11. Write short notes on.

a. DNS (Domain Name System)

The **Domain Name System (DNS)** is often called the "Phonebook of the Internet." Its primary job is to translate human-readable domain names (like `www.google.com`) into machine-readable IP addresses (like `142.250.190.46`).

- **How it works:** Computers communicate using numbers (IP addresses), but humans find it hard to remember them. When you type a URL in your browser, your computer queries a **DNS Server** to ask, "What is the IP for this name?"
- **The Process:** It follows a hierarchy starting from the **Root Servers**, then **Top-Level Domains** (.com, .org), and finally the **Authoritative Name Server** that holds the specific record.
- **Caching:** To speed up the process, your computer and your ISP store recently visited IP addresses in a "cache" so they don't have to ask the DNS server every single time.

b. Firewalls

A **Firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network (like the Internet).

- **Packet Filtering:** Most firewalls inspect "packets" of data. If a packet violates a rule (e.g., coming from a blocked IP or using a forbidden port), the firewall drops it.
- **Types:**
 - **Hardware Firewalls:** Physical devices placed between the router and the internet connection (used by businesses).
 - **Software Firewalls:** Programs installed on individual computers (like Windows Firewall).
- **Function:** They prevent unauthorized access (hackers) and stop malicious software from spreading from the internet into your private network.

c. Wi-Fi (IEEE 802.11)

Wi-Fi is a wireless networking technology that allows devices such as computers, smartphones, and tablets to interface with the Internet. It is based on the **IEEE 802.11** family of standards.

- **Radio Waves:** Wi-Fi uses radio waves to transmit information across a network. It typically operates on the **2.4 GHz** or **5 GHz** frequency bands.
- **WLAN (Wireless Local Area Network):** Wi-Fi is the most common technology used to create a WLAN. A device called a **Wireless Access Point (WAP)** or Router broadcasts the signal.
- **CSMA/CA:** Unlike wired Ethernet which uses Collision Detection (CD), Wi-Fi uses **Collision Avoidance (CA)**. Because it's wireless, devices "handshake" and wait for a clear channel before sending data to avoid interference.
- **Security:** To protect data traveling through the air, Wi-Fi uses encryption protocols like **WPA2** or **WPA3**.

Regular/Back Exam-2079, Bhadra/Ashwin

Diploma in Computer Engineering

1. What is computer network? Explain OSI model.

A **computer network** is a collection of interconnected computing devices (such as PCs, servers, smartphones, and routers) that communicate with each other to share resources and exchange data. These connections can be established via cables (wired) or radio waves (wireless).



The OSI Model (7 Layers)

The OSI model is a theoretical framework that breaks down the complex process of network communication into seven distinct layers. Developed by the ISO, it helps engineers troubleshoot problems and ensures interoperability between different vendors.

1. Physical Layer

This is the bottom layer that deals with the physical connection between devices. It is responsible for transmitting raw bits (0s and 1s) over a physical medium.

- **Deals with:** Cables, connectors, voltages, and bit rates.
- **Device:** Hub, Repeater.

2. Data Link Layer

This layer provides node-to-node data transfer. It takes data from the Network layer and organizes it into **Frames**. It handles physical addressing and error detection.

- **Deals with:** MAC Addresses.
- **Device:** Switch, Bridge.

3. Network Layer

The Network layer is responsible for packet forwarding and **Routing**. It finds the best physical path for the data to reach its destination.

- **Deals with:** IP Addresses and Packets.
- **Device:** Router.

4. Transport Layer

This layer handles "End-to-End" communication. It ensures that data is delivered reliably, in the correct order, and without errors. It breaks large data into **Segments**.

- **Protocols:** TCP (Reliable) and UDP (Fast).

5. Session Layer

This layer manages the "dialogue" between computers. It establishes, maintains, and terminates sessions (connections) between applications. It acts like a "manager" that keeps different data streams separate.

6. Presentation Layer

Often called the "Translator" layer. It formats and encrypts data to ensure that the application layer can understand it.

- **Functions:** Data compression, Encryption/Decryption, and Translation (e.g., ASCII to EBCDIC).

7. Application Layer

This is the top layer that the user interacts with directly. It provides network services to application software (like browsers or email clients).

- **Protocols:** HTTP (Web), SMTP (Email), FTP (Files)

2. What is a network protocol? Differentiate between a connection oriented and connectionless services.

A network protocol is a set of rules, standards, and conventions that define how data is transmitted and communicated across a computer network. It ensures that devices from different manufacturers can communicate effectively.

Differentiate between a connection oriented and connectionless services.

S.N.	Feature	Connection-Oriented Service	Connectionless Service
1	Analogy	Like a Telephone Call .	Like the Postal Service (Snail Mail).
2	Handshake	Requires a "Three-Way Handshake" to establish a connection before sending data.	No prior connection is established; data is just sent.
3	Reliability	High . It guarantees that data will reach the destination.	Low . It is "best-effort" and does not guarantee delivery.
4	Data Order	Data packets arrive in the exact same order they were sent.	Packets may arrive out of order via different routes.
5	Acknowledgment	Sends an "ACK" (Acknowledgment) back to the sender for every packet received.	No acknowledgment is sent back to the sender.
6	Retransmission	If a packet is lost, it is automatically re-sent.	If a packet is lost, it is simply gone.
7	Speed	Slower , due to the overhead of managing the connection and checks.	Faster , as there is no overhead for setup or checking.
8	Resource Use	High (requires memory to track the state of the connection).	Low (the network doesn't track the "state").
9	Example Protocol	TCP (Transmission Control Protocol).	UDP (User Datagram Protocol) or IP .
10	Typical Use Case	Web browsing, Email, File transfers (where accuracy is vital).	Video streaming, Online gaming, VoIP (where speed is vital).

3. Explain IEEE 802.3 and IEEE 802.4. Explain CSMA/protocol.

1. IEEE 802.3 (Ethernet)

IEEE 802.3 is the international standard for **Wired Ethernet**. It is the most common technology used for Local Area Networks (LANs) today.

- **Mechanism:** It uses a "contention-based" system. This means all devices compete for the chance to use the network.
- **Physical Layer:** It defines the types of cables used (like Twisted Pair or Fiber Optics) and the speed (10 Mbps, 100 Mbps, 1 Gbps).
- **Media Access:** It uses **CSMA/CD** (explained below) to manage how data is sent.
- **Usage:** Standard office and home wired networks.

2. IEEE 802.4 (Token Bus)

IEEE 802.4 is the standard for **Token Bus** networks. While it uses a physical bus layout (one long cable), it acts logically like a ring.

- **Mechanism:** It uses **Token Passing**. A small data packet called a "token" is passed from one computer to the next in a specific sequence.
- **Rule:** A computer can only transmit data if it is currently "holding" the token. Once it finishes, it passes the token to the next device.
- **Advantage:** There are **zero collisions**. This makes it "deterministic," meaning you can predict exactly when a machine will get to talk.
- **Usage:** Mainly used in industrial automation and factories where timing is critical.

3. Explaining CSMA Protocol

CSMA stands for **Carrier Sense Multiple Access**. It is a set of rules used in 802.3 (Ethernet) to decide how devices share the network. Think of it like a group of polite people in a dark room trying to have a conversation.

A. Carrier Sense (CS)

Before a device sends data, it "listens" to the cable (the carrier) to see if any electrical signal is present.

- If it hears someone else talking, it waits.
- If it hears silence, it starts transmitting.

B. Multiple Access (MA)

This means that many devices are connected to the same shared medium and all have equal rights to access it once it is free.

C. Collision Detection (CD)

In **IEEE 802.3**, the protocol is specifically **CSMA/CD**.

1. **Detection:** While a device is talking, it continues to listen.
2. **Collision:** If two devices hear silence and start talking at the exact same time, their signals "collide" and become garbled.
3. **Jam Signal:** As soon as they detect the collision, they stop talking and send a "Jam Signal" to warn everyone else.
4. **Backoff:** Each device waits for a **random** amount of time before trying to listen again. The randomness prevents them from colliding again immediately.

4. What are transmission media? Explain any two types. Discuss flow control in data link Layer.

Transmission media are the physical pathways or channels through which data signals travel from a sender to a receiver in a network. They can be broadly classified into guided (wired) and unguided (wireless) media.

Explanation of Any Two Types (with Examples)

Here are explanations of two important types — one from guided and one from unguided media:

1. Twisted Pair Cable (Guided Media)

- **Description:** Consists of two insulated copper wires twisted around each other to reduce electromagnetic interference (crosstalk) and noise.
- **Types:**
 - **UTP** (Unshielded Twisted Pair) — no extra shielding, most common.
 - **STP** (Shielded Twisted Pair) — has metallic shielding for better protection.
- **Categories** (for Ethernet): Cat5e, Cat6, Cat6a, Cat7 (higher categories support higher speeds and longer distances).
- **Examples of Use:**
 - Local Area Networks (LANs) — Ethernet cables connecting computers to switches/routers.
 - Telephone lines (traditional PSTN).
- **Advantages:** Inexpensive, easy to install, widely available.
- **Disadvantages:** Limited distance (usually up to 100 meters for Ethernet), susceptible to interference over long runs.

2. Fiber Optic Cable (Guided Media)

- **Description:** Uses thin strands of glass or plastic (fibers) to transmit data as pulses of light (via total internal reflection).
- **Types:**
 - **Single-mode fiber** — one light path, very long distance, high speed (used in backbones).
 - **Multi-mode fiber** — multiple light paths, shorter distance, cheaper.
- **Examples of Use:**
 - High-speed internet backbone networks.

- Data centers and long-distance telecommunication links.
- Undersea cables connecting continents.
- **Advantages:** Extremely high bandwidth (up to terabits per second), very long transmission distance (tens to hundreds of km without repeaters), immune to electromagnetic interference (EMI), secure (hard to tap).
- **Disadvantages:** Higher cost, difficult to install/terminate, fragile.

2. Flow Control in the Data Link Layer

Flow Control is a technique that coordinates the rate of data transmission between a sender and a receiver. It prevents a fast sender from "overwhelming" a slow receiver with more data than it can process or store in its buffer.

The Two Main Methods of Flow Control:

A. Stop-and-Wait Flow Control

This is the simplest form of flow control.

1. The sender sends one frame.
 2. The sender then **stops and waits** for an acknowledgment (ACK) from the receiver.
 3. Only after receiving the ACK does the sender send the next frame.
- **Pros:** Simple and easy to implement.
 - **Cons:** Very inefficient, especially over long distances, because the link stays idle while waiting for the ACK.

B. Sliding Window Flow Control

This is a much more efficient method used in modern networks (like TCP).

1. Both sender and receiver agree on a **Window Size** (e.g., 5 frames).
 2. The sender can send up to 5 frames without waiting for an acknowledgment.
 3. As the receiver sends back ACKs, the "window" slides forward, allowing the sender to transmit more frames.
- **Pros:** High efficiency; it keeps the "pipe" full of data.
 - **Cons:** More complex to manage as frames must be numbered (sequence numbers).

5. What is channel bandwidth? Explain the concept of sub-netting. Define inter-network.

Answer: **Channel bandwidth**

Channel bandwidth is the range of frequencies used for transmission of a signal over a specific channel. It measures the maximum data transfer rate of a network or internet connection, typically expressed in bits per second (bps) or Hertz (Hz). A higher bandwidth allows for faster data transmission.

The Concept of Sub-netting

Sub-netting is the process of logically dividing a single IP network into multiple smaller network segments. This is a critical skill for network administrators to manage IP address space efficiently.

How Sub-netting Works (The Logic)

Every IP address (IPv4) consists of 32 bits. These bits are divided into two parts: the **Network Address** and the **Host Address**.

- In sub-netting, we "borrow" bits from the Host portion and reassign them to the Network portion.
- The **Subnet Mask** is used by the router to determine which part of the IP address represents the network/subnet and which part represents the host.

The Mathematical Rule

To find the number of possible subnets and hosts:

1. **Number of Subnets:** 2^n , where n is the number of bits borrowed.
2. **Number of Hosts per Subnet:** $2^h - 2$, where h is the number of bits remaining for hosts. (We subtract 2 for the Network ID and the Broadcast Address).

Advantages of Sub-netting:

- **Reduced Network Traffic:** Broadcast packets stay within the subnet, reducing overall congestion.
- **Enhanced Security:** It is easier to apply security policies (ACLs) between subnets.
- **Organizational Hierarchy:** Different departments (Finance, HR, Tech) can have their own isolated networks.

Define Inter-network

- **Internetwork (or inter-network):** a collection of two or more distinct networks connected together so that hosts in one network can communicate with hosts in another (the Internet is the largest internetwork).

6. Explain transaction of IPV4 to IPV6. Explain how packets are formed and functions of network layer.

Transition from IPv4 to IPv6

Since IPv6 is not backward compatible with IPv4, three main strategies are used to bridge the gap:

- **Dual Stack:** This is the most common method. Every network device (routers, switches, servers) is configured with both an IPv4 and an IPv6 address. If the destination supports IPv6, it uses that; otherwise, it falls back to IPv4.
- **Tunneling:** This is used when two IPv6 networks need to communicate but are separated by an IPv4-only network. The IPv6 packet is "encapsulated" (wrapped) inside an IPv4 packet at the entry point and "decapsulated" at the exit point.
- **NAT-PT (Network Address Translation - Protocol Translation):** This allows IPv6-only devices to communicate with IPv4-only devices by translating the IP headers between the two formats.

How Packets are Formed (Encapsulation)

In the Network Layer, data is organized into **Packets** (or Datagrams). This process is called **Encapsulation**.

1. **Data Reception:** The Network Layer receives a "Segment" from the Transport Layer above it.
2. **Header Attachment:** It adds a header to the segment. This header contains critical information like:
 - **Source IP Address:** Where the data is coming from.
 - **Destination IP Address:** Where the data is going.
 - **Protocol:** Which protocol is being used (TCP or UDP).
 - **TTL (Time to Live):** A counter that prevents the packet from circling the network forever.
3. **Result:** The combination of the Transport Layer's segment and the Network Layer's header is called an **IP Packet**.

Functions of the Network Layer

The Network Layer (Layer 3 of the OSI model) is the "Post Office" of the network. Its main responsibilities include:

- **Routing:** This is the most important function. It determines the best physical path for a packet to travel from the sender to the receiver across multiple networks using a routing table.
- **Logical Addressing:** While the Data Link Layer uses MAC addresses for local delivery, the Network Layer uses **IP Addresses** to identify devices globally.
- **Fragmentation and Reassembly:** Different physical networks have different limits on packet size (MTU). If a packet is too large for a specific network, the Network Layer breaks it into smaller pieces (fragmentation) and reassembles them at the destination.
- **Error Reporting:** It uses protocols like ICMP to send messages back to the sender if a destination is unreachable or a packet is dropped.
- **Congestion Control:** It monitors the number of packets in the network to prevent bottlenecks that could slow down transmission.

7. Write short notes on.

a. DNS (Domain Name System)

The **Domain Name System (DNS)** is the "Phonebook of the Internet." It is a hierarchical and decentralized naming system for computers, services, and other resources connected to the Internet or a private network.

- **Core Function:** It translates human-friendly domain names (e.g., `www.merajob.com`) into numerical **IP addresses** (e.g., `104.21.32.189`) that computers use to identify each other.
- **How it Works:** When you enter a URL, a **DNS Resolver** (usually provided by your ISP) queries a series of servers—**Root Servers**, **Top-Level Domain (TLD) Servers** (like `.com` or `.np`), and **Authoritative Name Servers**—until it finds the correct IP address.
- **Caching:** To improve speed, DNS results are stored locally in a "cache" so the system doesn't have to look up the same address repeatedly.
- **Port:** It typically operates on **Port 53** using UDP.

b. Firewall

A **Firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network (like the Internet).

- **Mechanism:** It inspects **Packets** of data. Based on its rule set, it will either "Allow," "Block," or "Drop" the packet.
- **Types of Firewalls:**
 - **Packet Filtering:** Filters based on IP addresses and port numbers.
 - **Stateful Inspection:** Tracks the state of active connections to determine which network packets are allowed through.
 - **Proxy Firewall:** Acts as a gateway between networks for a specific application.
- **Purpose:** Its primary goal is to prevent unauthorized access, "hacking," and the spread of malware while allowing legitimate communication to pass through.

c. VPN (Virtual Private Network)

A **VPN** is a service that creates a secure, encrypted connection (often called a "tunnel") over a less secure network, such as the public Internet.

- **Encryption:** The most critical feature of a VPN is encryption. It scrambles your data so that even if a hacker or ISP intercepts it, they cannot read it.
- **IP Masking:** When you connect to a VPN, your actual IP address is hidden, and you appear to have the IP address of the VPN server. This provides **Anonymity**.
- **Remote Access:** It is widely used by corporate employees to safely access private company servers from home or while traveling.
- **Protocols:** Common VPN protocols include **OpenVPN**, **L2TP/IPsec**, and **WireGuard**.

d. WWW (World Wide Web)

The **World Wide Web (WWW)** is an information system where documents and other web resources are identified by **URLs** (Uniform Resource Locators), interlinked by hypertext links, and accessible via the Internet.

- **The Difference:** It is important to note that the WWW is a *service* that runs on the Internet; it is not the Internet itself. The Internet is the infrastructure of cables and hardware.
- **Core Components:**
 - **HTML:** The formatting language for web pages.
 - **HTTP/HTTPS:** The protocol used to transfer data between the server and the browser.
 - **Web Browsers:** Software (like Chrome or Firefox) used to display the web pages.
- **Architecture:** It follows the **Client-Server Model**, where your browser is the client requesting pages from a web server.

8. Explain two protocols of transport layer? Why does need flow control in transport layer?

Two Protocols of the Transport Layer

The two most widely used protocols at this layer are **TCP** and **UDP**. They serve different purposes based on whether the user needs accuracy or speed.

A. TCP (Transmission Control Protocol)

TCP is a **connection-oriented** protocol. It ensures that data is delivered reliably and in the correct order.

- **Three-Way Handshake:** Before sending data, TCP establishes a connection using a SYN, SYN-ACK, ACK sequence.
- **Reliability:** It uses acknowledgments. If a sender doesn't receive a "receipt" (ACK) for a packet, it retransmits the data.
- **Sequencing:** It adds sequence numbers to segments so the receiver can put them back in the correct order.
- **Usage:** Web browsing (HTTP), Email (SMTP), and File Transfers (FTP).

B. UDP (User Datagram Protocol)

UDP is a **connectionless**, "best-effort" protocol. It sends data without establishing a connection or checking if it arrived.

- **Speed:** Because it doesn't wait for acknowledgments or perform error recovery, it is much faster than TCP.
- **No Overhead:** It has a very small header, which saves bandwidth.
- **Unordered:** Data may arrive out of order, and lost packets are not re-sent.
- **Usage:** Live video streaming, Online gaming, and VoIP (Voice over IP).

2. Why Flow Control is Needed in the Transport Layer

Flow Control is the process of managing the rate of data transmission between two nodes. Without it, a fast sender could easily overwhelm a slow receiver.

Here is why it is essential:

1. **Preventing Buffer Overflow:** Every receiver has a limited amount of memory (a "buffer") to store incoming data before the CPU processes it. If the sender sends data faster than the receiver can process it, the buffer overflows, and data is lost.
2. **Matching Different Speeds:** A powerful server might be able to send data at 1 Gbps, but the receiving smartphone might only be able to process data at 50 Mbps. Flow control synchronizes these speeds.
3. **Reducing Retransmissions:** If data is lost due to buffer overflow, the sender has to retransmit it (in TCP). This wastes network bandwidth and increases latency. Proper flow control prevents this loss from happening in the first place.
4. **Congestion Management:** While "Congestion Control" protects the network as a whole, "Flow Control" protects the specific end-to-end connection, ensuring the smooth delivery of data.

9.Explain client server model. Why security is a field of computer networks? Discuss.

The Client-Server Model

The Client-Server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service (**Servers**) and service requesters (**Clients**).

How it Works:

- **The Client:** This is the service requester. It is usually a PC, smartphone, or web browser. The client initiates communication by sending a **request** to the server for a specific resource (like a webpage or a file).
- **The Server:** This is a high-performance machine that hosts, delivers, and manages most of the resources. It remains in a "passive" state, listening for incoming requests. When a request arrives, the server processes it and sends a **response** back to the client.
- **The Network:** The connection between them is managed by protocols (like **HTTP** for web browsing or **SMTP** for email).

Key Characteristics:

- **Centralization:** Resources and data are stored in a central location (the server), making it easier to manage.
- **Scalability:** You can easily add more clients to the network without needing to change the server's core software.
- **Backup and Recovery:** Since data is central, it is much easier to perform regular backups than in a decentralized Peer-to-Peer network.

• Why Security is a Field of Computer Networks

- Security is not just an "extra feature" of networking; it is the **foundation** of modern connectivity. As our world becomes more connected, the risks associated with networking grow. Here is a discussion on why security is a dominant field in this domain:
- **A. Protection of Centralized Data**
- In the client-server model, the server is the "vault." It stores sensitive information like passwords, credit card details, and personal records. Because all clients connect to it, a single security flaw in the server can lead to a data breach affecting thousands or millions of users at once.
- **B. Ensuring Network Availability (The CIA Triad)**
- Networks are prone to **DDoS (Distributed Denial of Service)** attacks, where attackers overwhelm a server with fake traffic to crash it. Network security focuses on ensuring "Availability"—making sure the network remains "up" for legitimate users.
- **C. Preventing Data Tampering (Integrity)**
- When data travels across a network, it passes through many routers and switches. Security protocols (like **SSL/TLS**) ensure that the data is not modified or tampered with by a "man-in-the-middle" while it is in transit.
- **D. Authentication and Access Control**
- Networking is essentially about "access." Security is the field that defines **who** can access **what**. Without robust authentication (passwords, biometrics) and authorization, a network would be open to any malicious actor.
- **E. Privacy and Encryption**
- With the rise of wireless networks (Wi-Fi) and public hotspots, data is literally traveling through the air. The field of network security uses **Cryptography** to ensure that even if someone "sniffs" the data packets,

10. How confidentiality, integrity and availability is maintained in a computer network?

Confidentiality (Keeping Data Secret)

Confidentiality ensures that sensitive information is accessed only by authorized people and is hidden from everyone else.

- **How it's maintained:**

- **Encryption:** This is the primary tool. Data is scrambled using algorithms (like AES) so that even if a hacker "sniffs" the packets, they cannot read the content.
- **Access Control:** Using usernames, passwords, and Two-Factor Authentication (2FA) to verify identity.
- **Physical Security:** Locking server rooms and securing network cables.

2. Integrity (Keeping Data Accurate)

Integrity ensures that data is not modified, deleted, or tampered with during transmission from the sender to the receiver.

- **How it's maintained:**

- **Hashing:** A mathematical "fingerprint" is created for a file or message (using algorithms like SHA-256). If even one bit of the data is changed, the hash will not match, alerting the receiver.
- **Digital Signatures:** Used to verify that the message actually came from the claimed sender and hasn't been altered.
- **Checksums:** Used at the Data Link and Transport layers to detect electrical noise or errors during transmission.

3. Availability (Keeping the Network Up)

Availability ensures that the network resources and services are accessible to authorized users whenever they are needed.

- **How it's maintained:**

- **Redundancy:** Having backup servers, multiple power supplies, and extra routers so that if one fails, another takes over (Failover).
- **DDoS Protection:** Using firewalls and specialized hardware to filter out "fake" traffic meant to crash the server.
- **Regular Maintenance:** Keeping hardware updated and software patched to prevent crashes and vulnerabilities.

11. Classify computer networks. Write down the differences between repeater and router.

Classification of Computer Networks

Networks are primarily classified based on the geographical area they cover:

a. Personal Area Network (PAN)

- **Range:** Very small (within a room/person's reach).
- **Usage:** Connecting a smartphone to a smartwatch or wireless headphones.
- **Technology:** Bluetooth, Zigbee.

b. Local Area Network (LAN)

- **Range:** Within a building, office, or campus.
- **Usage:** High-speed data sharing between computers in a school or home.
- **Technology:** Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11).

c. Metropolitan Area Network (MAN)

- **Range:** Across a city.
- **Usage:** Connecting multiple LANs across a town (e.g., a cable TV network or a city-wide bank branch network).

d. Wide Area Network (WAN)

- **Range:** Large distances, countries, or the entire globe.
- **Usage:** The Internet is the most famous example. It uses fiber optics, satellites, and leased lines to connect devices worldwide.

S.N.	Feature	Repeater	Router
1	OSI Layer	Operates at the Physical Layer (Layer 1).	Operates at the Network Layer (Layer 3).
2	Data Unit	Works with raw Bits (0s and 1s).	Works with Packets (Data + IP Header).
3	Intelligence	A "dumb" device; it doesn't read any addresses.	A "smart" device; it reads and understands IP addresses.
4	Primary Function	Regenerates and amplifies signals to extend cable length.	Routes data between different networks using the best path.
5	Address Used	Does not use any addressing (MAC or IP).	Uses Logical Addressing (IP Addresses) .

S.N.	Feature	Repeater	Router
6	Collision Domain	Extends the collision domain (collisions travel through it).	Breaks collision domains into smaller segments.
7	Broadcast Domain	Forwards all broadcasts (does not break them).	Breaks broadcast domains (stops broadcasts from spreading).
8	Connectivity	Connects two segments of the same network.	Connects different networks (e.g., your LAN to the Internet).
9	Routing Table	Does not maintain any table or record.	Maintains a Routing Table to store network paths.
10	Filtering	Cannot filter traffic; it sends everything it receives.	Can filter traffic using Access Control Lists (ACLs) and security rules.

Regular/Back Exam-2078, Kartik/Mangsir Diploma in Computer Engineering

1. What is computer Network? Explain the advantages and disadvantages of computer Network.

Computer Network is a group of two or more computer systems and other hardware devices (like printers and servers) linked together through communication channels. These connections allow them to share resources, exchange files, and communicate electronically.

Advantages of Computer Networks

Using a network provides several powerful benefits for both individuals and businesses:

- **Resource Sharing:** This is the biggest advantage. Multiple users can share physical hardware like printers and scanners, or software resources like databases, reducing costs significantly.
- **Easy Communication:** Networks enable instant communication through email, video conferencing, and instant messaging, regardless of geographical location.
- **Data Sharing & File Transfer:** Instead of using physical drives to move data, users can transfer files instantly across the network. Centralized storage (like a File Server) allows everyone to access the same version of a document.
- **Cost-Effectiveness:** Sharing expensive software and hardware across a network is much cheaper than buying individual copies or devices for every user.
- **Increased Storage Capacity:** Networks allow users to access storage on other machines or central servers (Cloud storage), meaning an individual computer doesn't need a massive hard drive.

Disadvantages of Computer Networks

While networks are incredibly useful, they also come with certain risks and challenges:

- **Security Issues:** Because computers are linked, a hacker who gains access to one device may be able to access the entire network. This makes networks vulnerable to data theft and unauthorized access.
- **Virus and Malware Spread:** If one computer on a network is infected with a virus, it can spread very quickly to all other connected devices.
- **High Setup Costs:** Setting up a large network requires expensive hardware (routers, switches, hubs) and cabling, along with professional installation.
- **Dependency on the Main Server:** In a Client-Server network, if the central server crashes, the entire network may stop working, leaving all users unable to perform their tasks.
- **Requirement of Technical Staff:** Managing a complex network often requires a dedicated "Network Administrator" to handle troubleshooting, updates, and security patches.

2. Explain the OSI reference model. Differentiate it with TCP/IP reference model.

The **OSI (Open Systems Interconnection)** model is a conceptual framework developed by the ISO to standardize the functions of a telecommunication or computing system. It breaks down the complex process of data communication into seven distinct layers.

The 7 Layers of OSI Model

1. **Physical Layer (Layer 1)**
 - Deals with hardware transmission of raw bits.
 - Defines cables, connectors, voltages, frequencies.
 - Example: Ethernet cables, hubs.
2. **Data Link Layer (Layer 2)**
 - Ensures error-free transfer of frames between two nodes.
 - Provides MAC addressing, framing, and error detection.
 - Example: Switches, Ethernet protocol.
3. **Network Layer (Layer 3)**
 - Responsible for routing and logical addressing (IP addresses).
 - Determines the best path for data packets.
 - Example: Routers, IP protocol.

4. Transport Layer (Layer 4)
 - Provides end-to-end communication and reliability.
 - Ensures error checking, sequencing, and flow control.
 - Example: TCP, UDP.
5. Session Layer (Layer 5)
 - Manages sessions (dialogues) between applications.
 - Handles session establishment, maintenance, and termination.
 - Example: Remote login, video conferencing sessions.
6. Presentation Layer (Layer 6)
 - Responsible for data translation, encryption, and compression.
 - Ensures data is in a format understandable by the application.
 - Example: JPEG, MP3, SSL/TLS encryption.
7. Application Layer (Layer 7)
 - Closest to the user. Provides network services to applications.
 - Example: HTTP, FTP, SMTP..

S.N.	Feature	OSI Model	TCP/IP Model
1	Full Form	Open Systems Interconnection.	Transmission Control Protocol/Internet Protocol.
2	Number of Layers	It has 7 layers .	It has 4 layers (some versions show 5).
3	Development	Developed by ISO (International Organization for Standardization) in 1984.	Developed by the DoD (Department of Defense) in the 1970s.
4	Nature	It is a Reference Model (Theoretical).	It is an Implementation Model (Practical).
5	Approach	Follows a Vertical approach.	Follows a Horizontal approach.
6	Strictness	Layers are strictly defined; functions don't overlap.	Layers are more flexible; some functions overlap.
7	Protocols	Protocols were hidden; the model was defined before protocols.	Protocols came first; the model was built around existing protocols.
8	Session/Presentation	Includes separate Session and Presentation layers.	No separate layers; these functions are part of the Application Layer .
9	Physical/Data Link	Separate Physical and Data Link layers.	Combines them into a single Network Access Layer .

3. What is firewall? Explain different types of firewall.

A **Firewall** is a network security device (either hardware or software) that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies

Different Types of Firewalls

Firewalls have evolved significantly over the years. Here are the most common types categorized by how they filter data:

1. Packet Filtering Firewall

This is the oldest and most basic type of firewall. It acts as a checkpoint at a router or switch.

- **How it works:** It examines each packet in isolation and tests it against a set of rules (ACLs). It checks the source and destination IP addresses, protocol, and port numbers.
- **Pros:** Very fast and efficient; low impact on system performance.
- **Cons:** It doesn't look at the actual content of the data (the payload), making it easy to bypass with sophisticated attacks.

2. Stateful Inspection Firewall

Unlike basic packet filters, these firewalls keep track of the state of active connections.

- **How it works:** It remembers if a connection was already established (a "handshake"). If a packet arrives claiming to be part of an existing conversation but the firewall has no record of that session, it drops the packet.
- **Pros:** Much more secure than simple packet filtering.
- **Cons:** Requires more memory and processing power to track all active sessions.

3. Proxy Firewall (Application Level Gateway)

This firewall acts as an intermediary between the internal user and the external server.

- **How it works:** When a client requests a webpage, the request goes to the Proxy Firewall first. The firewall then goes out and gets the data itself, inspects it for malware at the application layer, and then hands it to the client.
- **Pros:** It completely hides your internal network's IP address and provides deep content filtering.
- **Cons:** Can significantly slow down network performance because it has to process every bit of data.

4. Next-Generation Firewall (NGFW)

This is the modern standard for business security.

- **How it works:** It combines traditional firewall features with advanced capabilities like **Deep Packet Inspection (DPI)**, encrypted traffic inspection, and integrated **Intrusion Prevention Systems (IPS)**.
- **Pros:** It can actually "see" what an application is doing (e.g., it can tell the difference between "Facebook browsing" and "Facebook file uploading").

4. What is Transmission Media? Explain about various guided transmission media with examples.

Transmission Media is the physical "pathway" or "channel" used to carry information from a sender to a receiver in a computer network. Data is transmitted via electromagnetic signals, and the medium determines the speed, quality, and distance the data can travel.

Guided Transmission Media

Guided media (also known as bounded media) use a physical conductor to "guide" the signal from one point to another. Here are the three most common types used in modern networking:

1. Twisted Pair Cable

This is the most common type of cabling used in local networks. It consists of pairs of copper wires twisted together to reduce **crosstalk** (electromagnetic interference from adjacent pairs).

- **Types:**
 - **Unshielded Twisted Pair (UTP):** The standard cable used in home and office Ethernet.
 - **Shielded Twisted Pair (STP):** Has a foil covering to protect against external interference (used in industrial areas).
- **Examples:** LAN cables (Cat5e, Cat6) used to connect your PC to a router.

2. Coaxial Cable

A coaxial cable has a central copper conductor surrounded by an insulating layer, which is then encased in a braided metal shield and an outer plastic jacket.

- **Key Feature:** The metal shield prevents external noise from interfering with the signal, allowing it to carry data over longer distances than twisted pair.
- **Examples:** The thick black cable used for **Cable TV (CATV)** and high-speed cable internet connections.

3. Fiber Optic Cable

Fiber optic cables are the "gold standard" of transmission media. Instead of electricity, they use **light pulses** to transmit data through thin strands of glass or plastic.

- **Key Feature:** Since it uses light, it is incredibly fast and completely immune to electromagnetic interference. It can carry data for miles without the signal losing strength.
- **Structure:** Consists of a **Core** (where light travels) and **Cladding** (which reflects light back into the core).
- **Examples:** **Backbone internet cables** connecting continents under the ocean and high-speed Fiber-to-the-Home (FTTH) services

5. Describe the role of router and switch in Networks with their definition.

The Switch (The Internal Connector)

Definition

A **Switch** is an intelligent networking device that connects multiple devices (computers, printers, servers) within a single **Local Area Network (LAN)**. It uses "packet switching" to receive, process, and forward data to the specific destination device.

The Role and Functions of a Switch

- **MAC Address Management:** The switch maintains a **MAC Address Table** (also known as a CAM table). When a frame arrives, the switch looks at the destination hardware address and sends it only to the port where that device is connected.
- **Collision Domain Reduction:** Unlike a Hub, which shares bandwidth, a switch provides a dedicated path for each pair of communicating devices. This "breaks" the collision domain, significantly increasing network speed.
- **Layer 2 Operation:** It operates at the **Data Link Layer** of the OSI model.
- **Frame Filtering:** It checks the integrity of incoming data (Error Checking) before forwarding it.

2. The Router (The External Gateway)

Definition

A **Router** is a sophisticated networking device that connects two or more different networks (e.g., connecting a home LAN to the Internet). It acts as a "dispatcher," choosing the best path for information to travel across the vast web of connected networks.

The Role and Functions of a Router

- **Path Determination (Routing):** This is the primary role. Using **Routing Protocols** (like OSPF, RIP, or BGP), the router determines the most efficient path for a packet to reach its destination.
- **Logical Addressing:** It operates using **IP Addresses**. It reads the "Network ID" part of an IP address to move data between different subnets.
- **Broadcast Domain Control:** Routers do not forward broadcast traffic. This prevents a "broadcast storm" in one network from crashing another.
- **Security and NAT:** Routers often perform **Network Address Translation (NAT)**, allowing an entire private network to share one public IP address, and act as a basic Firewall.

Layer 3 Operation: It operates at the **Network Layer** of the OSI model.

6. Explain IEEE 802.3 (CSMA/CD) LAN Architecture

The **IEEE 802.3** standard, commonly known as **Ethernet**, defines the physical and data link layers for wired Local Area Networks (LANs). A core part of this architecture is the **CSMA/CD** protocol, which manages how multiple computers share a single communication channel without data overlapping.

1. What is CSMA/CD?

In early Ethernet networks, all devices shared the same wire. **CSMA/CD** stands for **Carrier Sense Multiple Access with Collision Detection**. It acts like a "traffic cop" to ensure data is transmitted orderly.

- **Carrier Sense (CS):** Before sending data, a station "listens" to the cable. If it senses a signal (the carrier), it waits. If it hears silence, it proceeds.
- **Multiple Access (MA):** Many stations are connected to the same medium and have equal rights to use it.
- **Collision Detection (CD):** If two stations "listen," hear silence, and send data at the same time, their signals collide and become corrupted. The protocol detects this and stops the transmission immediately.

2. How the Process Works (Step-by-Step)

1. **Listen (Sensing):** The device checks if the medium is busy.
2. **Transmit:** If the medium is free, the device starts sending its frame.
3. **Monitor:** While sending, the device continues to monitor the wire to see if any other signal interferes with its own.
4. **Collision:** If a collision is detected, the device sends a "**Jam Signal**" to warn all other stations to stop transmitting.
5. **Back-off:** To prevent the same two computers from crashing again, each one waits for a **random amount of time** (Binary Exponential Back-off) before trying to sense the carrier again.

3. Physical Components of 802.3

The IEEE 802.3 standard specifies different physical layers, often recognized by their shorthand names:

- **10Base5 (Thicknet):** The original version using thick coaxial cable.
- **10Base-T:** Uses Twisted Pair cables and hubs/switches (the most common foundation for modern LANs).
- **100Base-TX (Fast Ethernet):** Increases speed to 100 Mbps.
- **1000Base-T (Gigabit Ethernet):** The current standard for most high-speed wired office networks.

4. Why CSMA/CD is less common today

In modern networks, we use **Switches** instead of Hubs.

- **Full-Duplex:** Modern switches allow devices to send and receive data at the same time.
- **Collision-Free:** Since each device has its own dedicated path to the switch, collisions are physically impossible. Therefore, CSMA/CD is largely disabled in modern "Full-Duplex" Ethernet, though it remains a fundamental part of the 802.3 standard for backward compatibility.

7. Explain public key and private key cryptography.

(Private Key) Cryptography

Symmetric encryption is all about **efficiency and obfuscation**. It treats data like a block of clay that needs to be mangled beyond recognition and then perfectly smoothed back out.

The AES Standard (Advanced Encryption Standard)

The world runs on **AES-256**. When you hear "military-grade encryption," this is usually what they mean. It works through a series of "rounds":

1. **Substitution:** Replacing specific bytes with others based on a lookup table (S-box).
2. **Transposition:** Shifting rows of data and mixing columns.
3. **Key Addition:** Combining the data with a portion of the secret key.

Because both parties have the key, the computer just runs these steps in reverse to get the original data. It is so fast that modern CPUs have "AES-NI" instructions built directly into the hardware to do this math instantly.

(Public Key) Cryptography

The genius of asymmetric cryptography is the **One-Way Function**. These are mathematical problems that are easy to do in one direction but nearly impossible to reverse without a "trapdoor" (the private key).

The RSA Method (Prime Factorization)

RSA is based on the fact that if I give you two prime numbers, $p=61$ and $q=53$, it's easy to calculate $n = p \times q = 3233$.

However, if I give a computer the number 3233 and tell it to find the two prime factors, it has to guess. For small numbers, that's easy. For a **2048-bit key**, the number is so large that all the computers on Earth working together would take billions of years to factor it.

The ECC Method (Elliptic Curve Cryptography)

This is the modern successor to RSA. Instead of giant prime numbers, it uses the algebraic structure of elliptic curves.

- **The Benefit:** You get the same level of security as RSA but with much smaller keys. A 256-bit ECC key is as strong as a 3072-bit RSA key.
- **Why it matters:** Smaller keys mean less battery drain on your phone and faster website loading times. This is what **WhatsApp** and **Signal** use for end-to-end encryption

8. What do you mean by routing? Explain the various routing algorithms.

Answer: **Routing is the process of path selection for data packets in a network.** Various algorithms, broadly categorized as static (non-adaptive) and dynamic (adaptive), are used to determine the optimal path.

Routing Algorithms

Routing algorithms generally fall into three "families" based on how they calculate the best path.

1. Distance Vector Routing (The "Rumor" Method)

In this algorithm, each router shares its entire routing table with its immediate neighbors at regular intervals. It doesn't know the whole map of the internet; it only knows how far away a destination is (distance) and which direction to send it (vector).

- **Metric:** Usually **Hop Count** (how many routers are in the way).
- **Algorithm:** Bellman-Ford Algorithm.
- **Real-world Example:** **RIP** (Routing Information Protocol).
- **Analogy:** It's like following signs at a crossroad. You don't have a map, but the sign says "New York: 50 miles this way."

2. Link-State Routing (The "Map" Method)

Instead of just listening to neighbors, every router in a Link-State system builds a complete, identical map of the entire network topology.

- **How it works:** Each router broadcasts the status of its own links (up/down, speed, delay) to **everyone** in the network. Once every router has the same data, they each run a calculation to find the shortest path.
- **Algorithm:** **Dijkstra's Shortest Path First (SPF).**
- **Real-world Example:** **OSPF** (Open Shortest Path First).
- **Pros:** Very fast convergence (it reacts to changes instantly) and less prone to routing loops.

3. Path Vector Routing (The "Policy" Method)

This is used for the "big" internet. While OSPF and RIP work *inside* a company, Path Vector is used to route data *between* Internet Service Providers (like moving data from AT&T to Comcast).

- **How it works:** It doesn't just look at distance; it looks at the specific "Autonomous Systems" (AS) a packet must travel through. It allows for "policies"—for example, a provider might refuse to route data through a specific country for security or political reasons.
- **Real-world Example:** **BGP** (Border Gateway Protocol). This is the "glue" that holds the entire global internet together
-

9. How does client server architecture differ from peer-to-peer architecture? Explain.

Client–Server Architecture

Definition

In this model, the network is divided into clients (requesters) and servers (providers). Clients send requests for services, while servers process these requests and return responses. The server is a centralized authority that manages resources, data, and security.

Working

1. A client (e.g., a web browser) sends a request to the server.
2. The server processes the request (e.g., fetches a webpage or database record).
3. The server sends the response back to the client.

Features

- Centralized control: Server manages data, security, and resources.
- Scalability: Easy to add more clients without major changes.
- Security: Stronger because data is centrally managed.
- Reliability: If the server is well-maintained, services are consistent.

Advantages

- Centralized management of data and security.
- Easy to scale by adding more clients.
- Efficient for large organizations.
- Provides backup and recovery options.

Disadvantages

- Server failure can disrupt the entire network.
- Higher cost (dedicated hardware, maintenance).
- Potential bottleneck if server is overloaded.

Examples

- Web browsing (browser = client, web server = server).
- Email systems (Outlook client, mail server).
- Banking systems, cloud services.

2 Peer-to-Peer (P2P) Architecture

Definition : In this model, all computers (peers) have equal status. Each peer can act as both a client and a server simultaneously. There is no central authority; resources are distributed among peers.

Working

1. A peer requests a resource (e.g., a file).
2. Another peer provides the resource directly.
3. Communication is decentralized; peers can join or leave freely.

Features

- Decentralized control: No dedicated server; resources are shared among peers.
- Flexibility: Peers can join or leave without disrupting the network.
- Cost-effective: No need for expensive server hardware.

- **Resilience:** Even if one peer fails, others can continue sharing.

Advantages

- Low cost, no need for dedicated servers.
- Flexible and resilient (peers can join/leave easily).
- Suitable for file sharing and decentralized applications.

Disadvantages

- Difficult to enforce security and data consistency.
- Limited scalability; performance decreases with many peers.
- No centralized backup or control.

Examples

- File-sharing networks (BitTorrent).
- Blockchain systems (Bitcoin, Ethereum).
- Small office/home networks.

10. Differentiate between:

a) Circuit switching and packet switching

Basis of Comparison	Circuit Switching	Packet Switching
Path Allocation	A dedicated physical path is reserved between sender and receiver.	No dedicated path; data is divided into packets that find their own way.
Bandwidth	Bandwidth is fixed and reserved for the entire duration.	Bandwidth is shared dynamically among all users.
Efficiency	Low. Resources are wasted if the line is silent/idle.	High. Resources are used only when there is data to send.
Latency (Delay)	No waiting once the path is set. Very consistent.	Packets may face "queuing delays" at routers.
Congestion	Happens at setup. If no lines are free, the call is blocked.	Happens during transmission. Packets get delayed or dropped if the network is busy.
Data Order	Data always arrives in the exact order it was sent.	Packets may take different routes and arrive out of order.
Best Use Case	Traditional Telephone systems (Landlines).	Modern Internet (Web, Email, File transfer).

b) Connection-Oriented vs. Connectionless Service.

Basis of Comparison	Connection-Oriented (TCP)	Connectionless (UDP)
Handshake	Requires a "Three-way Handshake" to establish a connection.	No handshake; data is sent immediately to the destination.
Reliability	Guaranteed. The receiver sends Acknowledgments (ACK) for every packet.	Not Guaranteed. It is a "best-effort" delivery service.
Retransmission	Lost or corrupted packets are automatically resent.	Lost packets are simply ignored or missed.
Sequencing	Ensures data is reassembled in the correct order.	No sequence control; packets arrive as they come.
Speed/Overhead	Slower due to the extra "chatter" of confirming packets.	Faster because there is no overhead or waiting for ACKs.
Analogy	A Phone Call (must connect before talking).	A Postcard (send it and hope it arrives).
Primary Protocol	TCP (Transmission Control Protocol).	UDP (User Datagram Protocol).
Best Use Case	Web Browsing (HTTP), Email (SMTP), File Transfer (FTP).	Video Streaming, Online Gaming, VoIP, DNS.

Regular/Back Exam-2076, Pun/Cha**Diploma in Computer Engineering/ Information Technology****1. What is computer Network? Explain the various applications of computer Network.**

A computer network is a system where two or more computers are connected together to share resources, exchange data, and communicate. These connections can be through cables (wired) or wireless technologies (Wi-Fi, Bluetooth, etc.).

Applications of Computer Networks

1. Resource Sharing
 - Printers, scanners, and storage devices can be shared among multiple users.
2. File Sharing & Data Communication
 - Users can easily transfer files, documents, and multimedia across computers.
3. Internet Access
 - Networks provide connectivity to the internet for browsing, emails, and cloud services.
4. Remote Access
 - Users can log in to systems or servers from distant locations (e.g., work from home).
5. Communication Services
 - Email, instant messaging, video conferencing, and VoIP rely on networks.
6. E-Commerce & Online Services
 - Online banking, shopping, and digital payments are possible through networks.
7. Collaboration & Education
 - Online classes, group projects, and shared platforms (Google Docs, LMS) use networks.
8. Entertainment & Media Streaming
 - Platforms like YouTube, Netflix, and online gaming depend on computer networks.

2. Explain the TCP/IP reference model. Differentiate it with OSI reference model.**TCP/IP Reference Model**

The **TCP/IP reference model** is the foundation of the Internet. It was developed by DARPA in the 1970s for ARPANET and later became the standard for global networking. It defines how data is transmitted from one computer to another across networks.

♦ **Layers of TCP/IP Model****1. Application Layer**

- Closest to the user.
- Provides services like email (SMTP), file transfer (FTP), web browsing (HTTP/HTTPS), and remote login (Telnet, SSH).
- Combines OSI's Application, Presentation, and Session layers into one.

2. Transport Layer

- Ensures reliable communication between processes.
- Uses **TCP** (connection-oriented, reliable, error-checked) and **UDP** (connectionless, faster, less reliable).
- Handles segmentation, flow control, and error detection.

3. Internet Layer

- Responsible for logical addressing and routing.
- Protocols: **IP (IPv4/IPv6), ICMP, ARP.**
- Ensures packets reach the correct destination across multiple networks.

4. Network Access Layer (Link Layer)

- Deals with physical transmission of data.
- Includes Ethernet, Wi-Fi, PPP, device drivers.
- Handles framing, MAC addressing, and actual hardware communication.

Comparison between TCP/IP and OSI Reference Models

S.N.	Basis of Comparison	TCP/IP Model	OSI Model
1	Full Form	Stands for Transmission Control Protocol / Internet Protocol.	Stands for Open Systems Interconnection.
2	Number of Layers	Consists of 4 layers (Application, Transport, Internet, Network Access).	Consists of 7 layers (Application, Presentation, Session, Transport, Network, Data Link, Physical).
3	Development	Developed before the protocols were designed; it is protocol-dependent.	Developed after the protocols; it is a generic, protocol-independent model.
4	Usage	It is the practical model used for the actual internet today.	It is a theoretical model used as a guide for teaching and understanding.
5	Approach	Follows a Vertical approach (Bottom-up).	Follows a Horizontal approach (Top-down).
6	Services & Protocols	Does not clearly distinguish between services, interfaces, and protocols.	Provides a clear distinction between services, interfaces, and protocols.
7	Layer Combination	Combines Session and Presentation layers into the Application layer.	Has separate layers for Session and Presentation.
8	Reliability	Primarily relies on the Transport layer (TCP) to ensure data is delivered.	Reliability is built into multiple layers (Data Link and Transport).

3. What is propagation time and transmission time? Differentiate between Client server and Peer to Peer Network Architecture.

Propagation Time (Definition)

Propagation time refers to the total time taken by a signal to travel from the sender to the receiver across the transmission medium. It is purely dependent on the distance between the two communicating devices and the speed at which the signal propagates through the medium (which is usually close to the speed of light in fiber optics or slightly slower in copper cables).

Transmission Time (Definition).

Transmission time refers to the time required to push all the bits of a message or data packet into the transmission medium. Unlike propagation time, transmission time depends on the size of the data and the bandwidth (data rate) of the channel.

Differentiate between Client server and Peer to Peer Network Architecture.

Client-Server Architecture	Peer-to-Peer (P2P) Architecture
One central machine (Server) provides services; others (Clients) consume them.	Every machine acts as both a server and a client simultaneously.
Strict hierarchy; the Server is the superior node in the network.	No hierarchy; all nodes (peers) have equal status and power.
Data is stored centrally on a high-capacity server.	Data is distributed across all participating nodes in the network.
Requires expensive, dedicated server hardware to handle many requests.	Can run on standard, low-cost desktop or laptop computers.
As more clients join, the server can become a bottleneck (performance may drop).	As more peers join, the network often gets faster (more sources for data).
If the central server crashes, the entire network goes down (Single Point of Failure).	Highly resilient; if one node fails, the rest of the network continues to function.
Managed centrally by a professional Network Administrator.	Managed by individual users; no central administration exists.
Easier to secure because all data and access rules are in one place.	Harder to secure; every peer is a potential entry point for security risks.
High initial cost due to server hardware, software licenses, and maintenance.	Low cost as it uses existing resources and doesn't require a dedicated server.
Used for banking, web hosting, and corporate email systems.	Used for file sharing (BitTorrent), Blockchain, and small home LANs.

4. Define transmission media. Mention about the types of transmission media with its major attributions.

Transmission Media is the physical path or communication channel between the transmitter (sender) and the receiver through which data is sent in the form of signals. It is the "bridge" that carries information from one machine to another.

Types of Transmission Media

Transmission media is broadly classified into two categories: **Guided** (Wired) and **Unguided** (Wireless).

1. Guided Media (Wired / Bounded Media)

In this type, signals are directed or "guided" along a solid physical path (cables).

- **Twisted Pair Cable:** Consists of two insulated copper wires twisted together to reduce electromagnetic interference (EMI). It is cheap and widely used in LANs (Ethernet).
- **Coaxial Cable:** Features a central copper conductor surrounded by an insulating layer, a metallic shield, and an outer jacket. It has higher bandwidth than twisted pair and is used for Cable TV and older internet setups.
- **Fiber Optic Cable:** Made of glass or plastic threads. It transmits data as "pulses of light." It is the fastest medium, supports huge bandwidth, and is immune to electrical interference.

2. Unguided Media (Wireless / Unbounded Media)

In this type, data is transmitted through the air or space using electromagnetic waves without any physical cables.

- **Radio Waves:** These waves are omnidirectional (travel in all directions). They are used for FM radio, television, and mobile communication.
- **Microwaves:** These travel in a straight line (Line-of-Sight). They require antennas to be visible to each other. They are used for satellite and terrestrial (tower-to-tower) communication.
- **Infrared:** Used for very short-range communication. It cannot pass through solid objects like walls. A common example is a TV remote control.

Major Attributions (Characteristics)

When evaluating transmission media, these four factors are key:

1. **Bandwidth:** The data-carrying capacity of the medium (how much data it can send per second).
2. **Attenuation:** The loss of signal strength as it travels over a distance.
3. **EMI (Electromagnetic Interference):** How much external electrical noise affects the signal.
4. **Cost:** The price of the cable/equipment and the difficulty of installation.

5. Define Network device. Describe Router and Repeater.

Network devices are hardware components used to connect computers, printers, phones, and other electronic devices within a network. They help in transmitting, directing, and managing data across the network. These devices can be simple (like repeaters) or complex (like routers, switches, and gateways). Without network devices, communication between multiple systems would not be possible.

Router

- **Definition.**

A router is a network device that connects multiple networks together and forwards data packets between them based on their IP addresses. It works at the Network Layer (Layer 3) of the OSI model. Routers are considered intelligent devices because they use routing tables and algorithms to determine the most efficient path for data to travel.

- **Functions:**

- Connects LANs to WANs and provides internet access.
- Uses IP addressing to identify source and destination.
- Performs Network Address Translation (NAT) to allow multiple devices to share a single public IP.
- Can act as a firewall, filtering traffic for security.
- Supports dynamic routing protocols (RIP, OSPF, BGP) for automatic path selection.

- **Attributes:**

- Provides connectivity between different networks.
- Ensures efficient packet delivery.
- Can be hardware (home Wi-Fi router) or software (virtual router).

- **Example:**

A home Wi-Fi router connects laptops, phones, and smart devices to the internet while also managing local traffic between them.



Repeater

- **Definition.**

A repeater is a network device that regenerates, amplifies, and retransmits signals to extend the distance of communication. It works at the Physical Layer (Layer 1) of the OSI model. Unlike routers, repeaters are not intelligent; they do not analyze or filter data. Their sole purpose is to strengthen weak signals so that data can travel longer distances without loss or distortion.

- **Functions:**

- Receives a weak or distorted signal and regenerates it to its original strength.
- Extends the range of wired or wireless networks.
- Prevents data loss due to attenuation (signal weakening).
- Commonly used in long-distance communication lines (fiber optics, satellite links).

- **Attributes:**

- Simple device, low cost.
- No routing or filtering capability.
- Works only at the physical level.

- **Example:**

A Wi-Fi range extender acts as a repeater by boosting the wireless signal from a router so that devices farther away can still connect.

6.Explain IEEE 802.4 (Token Bus) Lan Architecture.

IEEE 802.4 (Token Bus) LAN Architecture

◆ Overview

- IEEE 802.4 defines the Token Bus LAN standard.
- It was developed for industrial automation and manufacturing systems, where guaranteed access time is critical.
- The physical medium is a bus or tree topology (commonly coaxial cable).
- A logical ring is formed over the bus, and the token is passed sequentially among stations.

◆ Working Principle

1. Token Concept
 - A token is a special control frame that grants permission to transmit.
 - Only the station holding the token can send data, preventing collisions.
2. Logical Ring Formation
 - Although the physical layout is a bus, stations are arranged in a logical ring.
 - Each station knows the address of its predecessor and successor.
3. Token Passing
 - The token circulates in a fixed order.
 - If a station has data, it transmits while holding the token, then passes it on.
 - If no data, the token is simply forwarded.
4. Deterministic Access
 - Maximum waiting time for transmission is predictable.
 - This makes Token Bus suitable for real-time industrial control systems.

◆ Features / Attributes

- Collision-free communication (only one station transmits at a time).
- Deterministic access → predictable delay, unlike CSMA/CD in Ethernet.
- Supports priority levels → urgent messages can be transmitted earlier.
- Physical medium → coaxial cable, bus/tree topology.
- Logical structure → virtual ring for token circulation.
- Applications → manufacturing plants, process control, industrial automation.

7.For an IP address 192.168.100.0/27, Calculate the following: a) Required subnet mask b) Network address c) Broadcast address d) Usable host range in a network..

a) Required Subnet Mask

The /27 notation means there are 27 "1"s in the binary subnet mask.

- **Binary:** 11111111.11111111.11111111.11100000
- **Calculation:** The first three octets are all 1s (255.255.255). For the fourth octet, we add the place values of the three "1"s: $128 + 64 + 32 = 224$.
- **Answer: 255.255.255.224**

b) Network Address

To find the network address, we look at the block size. Since 5 bits are left for hosts ($32 - 27 = 5$), the block size is $2^5 = 32$.

- Subnets for this network would start at .0, .32, .64, etc.
- Since the given address ends in 0, it is already the starting point of the subnet.
- **Answer: 192.168.100.0**

c) Broadcast Address

The broadcast address is the very last address in the current subnet, just before the next subnet starts.

- The next subnet starts at 192.168.100.32
- The address immediately before that is 192.168.100.31.
- **Answer: 192.168.100.31**

d) Usable Host Range

The usable host range consists of all addresses between the Network Address and the Broadcast Address.

- **First Usable Host:** Network Address + 1 = 192.168.100.1
- **Last Usable Host:** Broadcast Address - 1 = 192.168.100.30
- **Answer: 192.168.100.1 to 192.168.100.30**

8. Define static and dynamic routing. Explain the various classes of IP address.

Dynamic Routing .

Dynamic routing is an automatic routing technique where routers use routing protocols to discover, select, and update routes. Unlike static routing, dynamic routing adapts to changes in the network topology, such as link failures, congestion, or new devices.

Static Routing.

Static routing is a manual routing technique where the network administrator configures routes in the routing table by hand. In this method, the path that data packets should follow from source to destination is fixed and predetermined.

Classes of IP Address.

An IP address is a 32-bit logical address used to uniquely identify devices on a network. To organize and allocate addresses efficiently, IPv4 addresses are divided into five classes (A, B, C, D, E) based on the first octet value. Each class has a different default subnet mask, network size, and purpose.

◆ Class A

- Range: 0.0.0.0 – 127.255.255.255
- Default Mask: 255.0.0.0 (/8)
- Network/Host: 8 bits for network, 24 bits for hosts.
- Usage: Very large organizations (millions of hosts).
- Example: 10.0.0.1

◆ Class B

- Range: 128.0.0.0 – 191.255.255.255
- Default Mask: 255.255.0.0 (/16)
- Network/Host: 16 bits for network, 16 bits for hosts.
- Usage: Medium-sized organizations (thousands of hosts).
- Example: 172.16.0.1

◆ Class C

- Range: 192.0.0.0 – 223.255.255.255
- Default Mask: 255.255.255.0 (/24)
- Network/Host: 24 bits for network, 8 bits for hosts.
- Usage: Small networks (up to 254 hosts).
- Example: 192.168.1.1

◆ Class D

- Range: 224.0.0.0 – 239.255.255.255
- Usage: Reserved for multicasting (sending data to multiple hosts simultaneously).
- Example: 224.0.0.1

◆ Class E

- Range: 240.0.0.0 – 255.255.255.255
- Usage: Reserved for experimental and research purposes.
- Example: 250.1.1.1

9. Write down the function of application layer. Describe about RIP and ICMP.

Functions of Application Layer .

The Application Layer is the topmost layer of the OSI model. It provides the interface between the user and the network. Its main role is to enable communication services directly for end-users and applications.

◆ Functions:

1. User Interface: Provides services like email, file transfer, web browsing, and remote login.
2. Data Representation: Ensures data is presented in a format understandable to both sender and receiver (often combined with Presentation layer in TCP/IP).
3. Resource Sharing: Allows multiple users to access shared resources such as files, printers, and applications.
4. Communication Services: Supports protocols like HTTP, FTP, SMTP, DNS, and Telnet for user-level communication.
5. Directory Services: Provides name resolution and directory lookup (e.g., DNS).
6. Network Virtualization: Enables applications to run independently of hardware/network details.

■ Routing Information Protocol (RIP)

- Definition: RIP is a distance-vector dynamic routing protocol used in IP networks.
- Working:
- Uses hop count as the metric to determine the best path.
- Maximum hop count = 15 (16 = unreachable).
- Routers exchange routing tables periodically (every 30 seconds).
- Features:
- Simple and easy to configure.
- Suitable for small networks.
- Limited scalability due to hop count restriction.
- Versions:
- RIP v1: Classful routing (no subnet info).
- RIP v2: Classless routing (supports subnet masks, authentication).

■ Internet Control Message Protocol (ICMP).

- Definition: ICMP is a network layer protocol used for error reporting and diagnostic functions in IP networks.
- Functions:
- 1. Reports errors in packet delivery (e.g., destination unreachable, time exceeded).
- 2. Provides diagnostic tools like ping and traceroute.
- 3. Helps in congestion control and network troubleshooting.
- Attributes:
- Works alongside IP (part of the Internet Layer in TCP/IP).
- Does not carry user data, only control messages.
- Essential for network management and fault detection.

10. a) Difference Between Switch and Hub.

Hub	Switch
A "dumb" device with no processing power.	An "intelligent" device that learns MAC addresses.
Uses Broadcasting (sends data to everyone).	Uses Unicasting (sends data to a specific device).
Operates at the Physical Layer (Layer 1).	Operates at the Data Link Layer (Layer 2).
Bandwidth is shared among all connected ports.	Each port has its own dedicated bandwidth.
High chance of data collisions.	Collisions are almost eliminated.
Supports only Half-Duplex (one way at a time).	Supports Full-Duplex (two-way simultaneous).
Low security (everyone can see the data).	Higher security (data only goes to the target).
Inefficient for large networks.	Highly efficient for busy or large networks.

b) Connection-Oriented vs. Connectionless Service

Connection-Oriented Service	Connectionless Service
Requires a formal Handshake before data transfer.	No setup required; data is sent immediately.
Highly reliable; guarantees data delivery.	"Best-effort" delivery; no guarantee of arrival.
Primarily uses TCP (Transmission Control Protocol).	Primarily uses UDP (User Datagram Protocol).
Uses ACK to confirm data was received.	No acknowledgement is sent back to the sender.
Data packets arrive in the correct sequence.	Packets may arrive out of order.
Slower due to the overhead of managing the link.	Faster because there is no overhead or waiting.
Lost packets are automatically resent.	Lost packets are not resent and are simply lost.
Used for Web browsing (HTTP) and Email (SMTP).	Used for Video Streaming and VoIP calls.

11. Write short notes on.

a) TCP vs. UDP

These are the two primary protocols used at the **Transport Layer**.

- **TCP (Transmission Control Protocol):** It is a **connection-oriented** protocol. Before sending data, it performs a "three-way handshake" to ensure the receiver is ready. It is highly reliable because it uses acknowledgments and resends any data that gets lost. It is used for tasks where accuracy is vital, like web browsing (HTTP) and email (SMTP).
- **UDP (User Datagram Protocol):** It is a **connectionless** protocol. It sends data immediately without checking the receiver's status. While it is "unreliable" (no guarantees), it is much faster than TCP because it has less overhead. It is perfect for real-time applications like video streaming, online gaming, and VoIP calls.

b) Subnetting

Subnetting is the process of dividing a single large physical network into several smaller, logical sub-networks (subnets).

- **Purpose:** It is used to reduce network traffic by minimizing broadcast domains and to improve network security.
- **Efficiency:** It helps in the efficient use of IP addresses. Without subnetting, many IP addresses in a large block might go to waste if a company only has a few dozen computers.
- **How it works:** An administrator "borrows" bits from the Host portion of an IP address to create a Network portion, identified by a **Subnet Mask**.

c) IPv6 and its Necessity

IPv6 (Internet Protocol version 6) is the latest version of the IP protocol, designed to replace IPv4.

- **Structure:** While IPv4 uses 32-bit addresses (e.g., 192.168.1.1), IPv6 uses **128-bit addresses** written in hexadecimal (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Necessity:**
 1. **Address Exhaustion:** The world has run out of IPv4 addresses due to the massive number of smartphones and IoT devices. IPv6 provides 3.4×10^{38} addresses.
 2. **Security:** IPv6 was designed with IPSec (security) built-in by default.
 3. **Efficiency:** It simplifies routing and eliminates the need for NAT (Network Address Translation).

d) Cloud Computing

Cloud Computing is the on-demand delivery of computing services—including servers, storage, databases, and software—over the internet ("the cloud").

- **Key Features:** Instead of owning their own physical data centers and servers, companies can rent access to anything from applications to storage from a cloud service provider (like AWS, Google Cloud, or Azure).
- **Models:** It is typically categorized into three types: **IaaS** (Infrastructure as a Service), **PaaS** (Platform as a Service), and **SaaS** (Software as a Service, like Google Docs).
- **Benefits:** It offers faster innovation, flexible resources, and economies of scale (you only pay for what you use).

Regular/Back Exam-2075, Falgun/Chaitra

Diploma in Information Technology

1. Define computer network. Explain TCP/IP reference model.

A **computer network** is a collection of interconnected computing devices (computers, servers, routers, switches, etc.) that can communicate and share resources with each other using established data communication protocols over digital connections.

TCP/IP Reference Model

The **TCP/IP (Transmission Control Protocol/Internet Protocol)** model is the practical framework used to design and implement the modern internet. Unlike the theoretical OSI model, TCP/IP was developed based on a specific set of protocols.

It is organized into **four functional layers**:

Layer 1: Network Access Layer

This is the lowest layer, combining the functions of the OSI Physical and Data Link layers. It defines how data is physically sent through the network, including hardware addressing (MAC addresses) and the physical transmission of bits over cables or radio waves.

Layer 2: Internet Layer

This layer is responsible for logical addressing and routing. Its main job is to send packets from any network to any destination network.

- **Key Protocol: IP (Internet Protocol).**
- **Function:** It handles the movement of packets across the network using IP addresses.

Layer 3: Transport Layer

The Transport layer provides end-to-end communication services. It ensures that data packets arrive in the correct order and without errors.

- **Key Protocols:**
 - * **TCP:** Provides reliable, connection-oriented communication (guarantees delivery).
 - **UDP:** Provides fast, connectionless communication (no guarantee, used for streaming).

Layer 4: Application Layer

The highest layer where user-facing applications reside. It provides the protocols that allow software to interact with the network.

- **Key Protocols:** **HTTP** (web browsing), **FTP** (file transfer), **SMTP** (email), and **DNS** (domain name resolution).

2. Define network protocol. Explain OSI reference model with its diagram.

A **network protocol** is a formal set of **rules, conventions, and standards** that govern how data is transmitted, received, and processed across a network. These protocols ensure that devices from different manufacturers and with different operating systems can communicate effectively by defining:

The OSI Reference Model

The **Open Systems Interconnection (OSI)** model is a theoretical framework developed by the ISO. It divides network communication into **seven distinct layers**. This modular approach allows different manufacturers to create hardware and software that can work together.

The 7 Layers (Top to Bottom)

7. Application Layer

This is the only layer that interacts directly with the user software. It provides network services like email, file transfers, and web browsing.

- **Protocols:** HTTP, FTP, SMTP.

6. Presentation Layer

This layer acts as a translator. It ensures that data is in a usable format and handles **encryption**, compression, and data representation (like converting EBCDIC to ASCII).

5. Session Layer

It manages the "dialogue" between computers. It starts, maintains, and ends the communication sessions between applications on different devices.

4. Transport Layer

This layer is responsible for end-to-end communication. It breaks large data into smaller **segments**, handles error correction, and ensures data arrives in the correct order.

- **Protocols:** TCP, UDP.

3. Network Layer

The Network layer handles logical addressing and routing. It decides the best physical path for data to take from the source to the destination. Data here is called **packets**.

- **Device:** Router.

2. Data Link Layer

This layer provides physical addressing (MAC addresses) and handles error detection from the physical layer. It organizes data into **frames**.

- **Device:** Switch, Bridge.

1. Physical Layer

The lowest layer deals with the actual physical connection. It defines the electrical, mechanical, and functional specifications for transmitting raw bits over cables or radio waves.

- **Device:** Hub, Repeater, Cables.

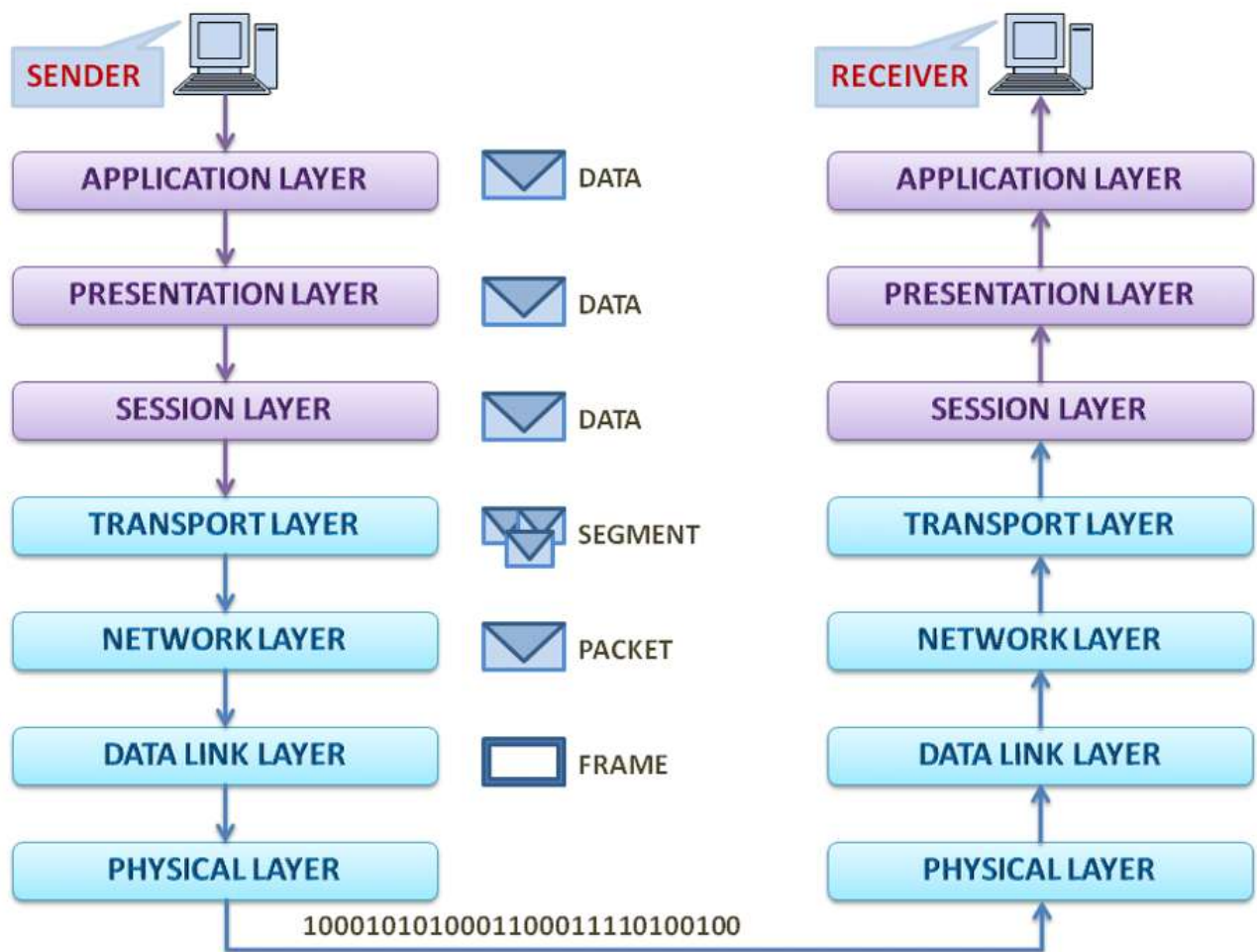


Figure 1: Layers of OSI Reference Model



3. Briefly explain client-server network architecture and explain briefly about the Router and Switch.

Client-Server Network Architecture

In a **Client-Server** architecture, the network roles are clearly divided between two types of entities:

1. **The Server:** A powerful, central computer that manages and provides resources, services, or data. It stays "on" and waits for requests.
2. **The Client:** Less powerful machines (PCs, laptops, smartphones) that request services or resources from the server.

Key Characteristics:

- **Centralization:** All data and security settings are stored in one place (the server), making it easy to manage and back up.
- **Scalability:** It is easy to add more clients to the network without affecting the data structure.
- **Performance:** Servers are built with high-end hardware to handle multiple requests simultaneously.
- **Single Point of Failure:** If the central server goes down, the entire network stops working for the clients.

Networking Devices: Router and Switch

While both devices connect computers, they operate at different layers of the OSI model and have different levels of "intelligence."

1. Router

A **Router** is an intelligent device that operates at the **Network Layer (Layer 3)**. Its main job is to connect different networks (for example, connecting your home network to the global Internet).

- **Function:** It uses **IP addresses** to determine the best and fastest path for a data packet to reach its destination.
- **Routing Table:** It maintains a "map" of the network called a routing table to direct traffic efficiently.
- **Security:** Routers often include firewalls to protect the internal network from outside threats.

2. Switch

A **Switch** is a smart device that operates at the **Data Link Layer (Layer 2)**. It is used to connect multiple devices (PCs, printers, servers) within a single Local Area Network (LAN).

- **Function:** Unlike a "dumb" Hub, a Switch learns the **MAC addresses** (physical addresses) of all connected devices.
- **Efficiency:** When it receives data, it sends it only to the specific port where the destination device is plugged in, rather than broadcasting it to everyone.
- **Performance:** By directing traffic only where it is needed, it reduces network congestion and prevents data collisions.

4. What do you mean by line coding? Explain line coding of digital signal with examples. Define Attenuation and Noise.

Line Coding is the process of converting digital data (binary 0s and 1s) into a digital signal (voltage levels). It is a critical step because while computers store data as 0s and 1s, those bits must be transformed into electrical pulses or waveforms to travel through a physical wire.

Line Coding of Digital Signals with Examples

There are several schemes used to represent bits as signals. Here are the most common examples:

1. **Unipolar (NRZ - Non-Return to Zero):**

- This is the simplest form.
- **Rule:** A binary "1" is represented by a high voltage (+V) and a binary "0" is represented by zero voltage (0V).
- **Example:** For the bit stream 1011, the signal stays high for the first bit, drops to zero for the second, and stays high for the next two.

2. **Polar (RZ - Return to Zero):**

- In this scheme, the signal uses positive, negative, and zero volts.
- **Rule:** The signal changes during the middle of every bit interval and "returns to zero" before the next bit begins. This helps the receiver stay synchronized with the sender.
- **Example:** A "1" might be represented by a transition from positive to zero, while a "0" goes from negative to zero.

3. **Manchester Encoding:**

- Used in standard Ethernet LANs.
- **Rule:** There is always a transition in the middle of each bit period. A "0" is a transition from High to Low, and a "1" is a transition from Low to High. This constant movement makes it very reliable for timing.

Noise.

Noise is any unwanted electrical or electromagnetic energy that interferes with the transmitted signal and distorts the original information. It is a major limiting factor in communication systems because it reduces the signal-to-noise ratio (SNR) and increases the probability of errors.

Attenuation.

Attenuation refers to the gradual reduction in the strength (amplitude or power) of a signal as it travels through a transmission medium. It is an unavoidable physical phenomenon that occurs due to the resistance, distance, and properties of the medium.

5. Define private IP address. Briefly explain framing and error control issues in the data link layer.

A private IP address is an IP address reserved for use within private networks (such as homes, schools, or offices) and is not routable on the public Internet. These addresses are used to identify devices inside a local area network (LAN) and allow them to communicate with each other. To access the Internet, devices with private IPs must use Network Address Translation (NAT), which maps private addresses to a public IP.

Framing in the Data Link Layer

Framing is the process of breaking the bit stream received from the Network layer into manageable units called **Frames**. It is essentially adding a "header" and a "trailer" to the data.

Why is it an issue?

The physical layer just sends a continuous stream of bits. Without framing, the receiver wouldn't know where one message ends and the next one begins.

Methods of Framing:

- **Character Count:** The header specifies the total number of characters in the frame. (Issue: If the count gets corrupted, the entire stream is lost).
- **Flag bytes with Byte Stuffing:** Special characters (flags) are placed at the start and end of the frame. If the data itself contains a flag character, an "escape" character is added so the receiver doesn't get confused.
- **Bit Stuffing:** A specific pattern of bits (like 01111110) marks the boundaries. If five consecutive '1's appear in the data, the sender automatically inserts a '0' to prevent it from looking like a flag.

3. Error Control in the Data Link Layer

Error Control refers to the methods used to detect and correct errors that occur during the transmission of frames (such as bits being flipped from 0 to 1 due to noise).

Key Issues and Mechanisms:

A. Error Detection

The receiver needs to know if the data arrived correctly. Common methods include:

- **Parity Check:** Adding an extra bit to make the total number of '1's even or odd.
- **Checksum:** Adding the numerical values of the data and sending the sum.
- **Cyclic Redundancy Check (CRC):** A powerful mathematical division used to detect errors in high-speed networks.

B. Error Correction

Once an error is detected, the layer must handle it.

- **Forward Error Correction (FEC):** The sender includes enough redundant data so the receiver can figure out and fix the error on its own.
- **Automatic Repeat Request (ARQ):** If the receiver detects an error, it sends a request back to the sender to retransmit that specific frame.

C. Flow Control Coordination

Error control is closely linked to flow control. If a receiver is overwhelmed and drops a frame, the error control mechanism must treat it as a "lost frame" and trigger a retransmission.

6. For the network 192.168.100.0/25, find the following:

a. The Subnet Mask

b. The number of Subnet

c. Range of valid hosts in each subnet

d. The network address and broadcast address of each subnet.

a. The Subnet Mask

The /25 notation means there are 25 "1"s in the binary subnet mask.

- **Binary Representation:** 11111111.11111111.11111111.10000000
- **Decimal Conversion:** The first three octets are all 1s (\$255.255.255\$). In the fourth octet, the first bit has a decimal value of \$128\$ (\$2^7\$).
- **Subnet Mask:** \$255.255.255.128\$

b. The Number of Subnets

Since 192.168.100.0 is a **Class C** address, the default mask is /24. To reach /25, we have borrowed **1 bit** from the host portion.

- **Formula:** 2^n (where n is the number of borrowed bits).
- **Calculation:** $2^1 = 2$.
- **Total Subnets:** 2

c. & d. Network Address, Broadcast Address, and Valid Host Range

To find the ranges, we use the **Block Size** (Magic Number).

- **Block Size:** $256 - 128 = 128$. This means our subnets start at intervals of 128.

Details	Subnet 1	Subnet 2
Network Address	\$192.168.100.0\$	\$192.168.100.128\$
First Valid Host	\$192.168.100.1\$	\$192.168.100.129\$
Last Valid Host	\$192.168.100.126\$	\$192.168.100.254\$
Broadcast Address	\$192.168.100.127\$	\$192.168.100.255\$

7.What do you mean by routing? Why is it necessary.Differentiate between static and dynamic routing.

Routing is the process of selecting the best path for data packets to travel from a source on one network to a destination on a different network. This process is performed by a **Router**, which operates at the **Network Layer (Layer 3)** of the OSI model.

Why is it Necessary?

1. **Inter-network Communication:** Without routing, a computer could only talk to other computers on its own local cable. Routing allows data to jump between different networks (e.g., your home Wi-Fi and the Google server).
2. **Path Optimization:** In a vast network like the Internet, there are thousands of ways to get from Point A to Point B. Routing ensures data takes the most efficient (fastest or shortest) path.
3. **Congestion Control:** Routers can detect if a specific path is "clogged" with too much traffic and redirect data through a clearer route.
4. **Traffic Isolation:** It prevents local traffic from unnecessarily flooding other networks, keeping the overall system efficient.

Static vs. Dynamic Routing

In an exam, presenting this as a table is the best way to get full marks.

Static Routing	Dynamic Routing
Routes are manually configured by a network administrator.	Routes are automatically discovered and updated by protocols.
Simple to configure in very small networks.	Complex to set up but manages itself once running.
Cannot adapt to network changes (if a link fails, the path stays dead).	Automatically reroutes data if a link or router fails.
Does not use routing protocols.	Uses protocols like RIP, OSPF, or BGP .
Uses almost no CPU or RAM on the router.	Requires CPU and RAM to process protocol updates.
High (only the admin can change the paths).	Lower (protocols can be "fooled" by malicious updates).
Best for small, stable networks.	Best for large, growing, or changing networks.

8. What do you mean by connection oriented and connectionless service in the transport layer? Briefly explain segmentation and reassembly.

Connection-Oriented vs. Connectionless Service

Connection-Oriented Service

This service is designed for reliability. Before any data is actually sent, the sender and receiver must perform a **handshake** to establish a dedicated logical connection.

- **Mechanism:** It uses the "Three-Way Handshake" (SYN, SYN-ACK, ACK). It tracks every packet and ensures they arrive in order.
- **Reliability:** Highly reliable; if a packet is lost, the receiver asks for a retransmission.
- **Protocol Example: TCP** (Transmission Control Protocol).
- **Analogy:** Like a phone call—you dial, wait for the other person to say "hello," and then start talking.

Connectionless Service

In this service, data is sent immediately without checking if the receiver is ready or even online. Each packet (or "datagram") is handled independently.

- **Mechanism:** No handshake occurs. The sender simply pushes the data onto the network.
- **Reliability:** "Best-effort" delivery. There is no guarantee that the data will arrive or arrive in the correct order.
- **Protocol Example: UDP** (User Datagram Protocol).
- **Analogy:** Like sending a postcard—you drop it in the mailbox and hope it reaches its destination; you don't wait for a "ready" signal.

2. Segmentation and Reassembly

Because networks have limits on how much data can be sent at once (called the Maximum Transmission Unit or MTU), the Transport Layer must manage the "size" of the data.

Segmentation (at the Sender)

When an application sends a large file, it is too big to fit into a single network packet. The Transport Layer breaks this large data into smaller pieces called **Segments**.

- Each segment is assigned a **Sequence Number**.
- This allows the network to handle smaller, more manageable chunks of data.

Reassembly (at the Receiver)

Once the segments arrive at the destination, they may arrive out of order because they took different paths through the network.

- The receiver's Transport Layer uses the **Sequence Numbers** to put the pieces back together in the correct order.
- If any segment is missing, the reassembly process pauses, and the receiver (in TCP) requests the missing piece.

9. Write Short Notes on.

a) IPv6 (Internet Protocol Version 6)

IPv6 is the most recent version of the Internet Protocol, designed by the IETF to replace the aging IPv4.

- **Address Space:** While IPv4 uses 32-bit addresses (4.3 billion total), IPv6 uses **128-bit addresses**, providing 3.4×10^{38} addresses. This effectively solves the problem of IP address exhaustion.
- **Format:** It is written in **hexadecimal**, divided into eight groups of four digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Key Benefits:**
 1. **Auto-configuration:** Devices can automatically generate their own IP address (Plug-and-Play).
 2. **Built-in Security:** It was designed with IPsec (encryption and authentication) as a mandatory requirement.
 3. **Efficiency:** It has a simplified header that allows routers to process packets more quickly.

b) DNS (Domain Name System)

DNS is often called the "phonebook of the Internet." It is an Application Layer protocol used to translate human-readable names into machine-readable IP addresses.

- **How it works:** When you type www.google.com into your browser, a DNS query is sent to a **DNS Resolver**. This server looks up the specific IP address (like 142.250.190.46) associated with that name.
- **Hierarchy:** DNS works in a tree-like structure, starting from **Root Servers**, moving to **TLD (Top-Level Domain) Servers** (like .com or .org), and finally reaching **Authoritative Nameservers**.
- **Caching:** To speed up the process, your computer and your ISP store recently visited IP addresses in a local "cache" so they don't have to look them up every single time.

c) VPN (Virtual Private Network)

A VPN creates a safe and encrypted connection over a less secure network, such as the public internet.

- **Tunneling:** A VPN works by "tunneling" your data. It wraps your data packets inside another set of packets, hiding the original content from anyone watching the network.
- **Encryption:** All data traveling through this tunnel is encrypted. Even if a hacker intercepts the data, they cannot read it without the decryption key.
- **Key Uses:**
 1. **Remote Access:** Allows employees to securely connect to their office network from home.
 2. **Privacy:** Hides the user's actual IP address and location from websites and ISPs.
 3. **Security:** Protects users on public Wi-Fi networks (like at a cafe) where data theft is common.

Regular/Back Exam Chaitra, 2070

Diploma in Computer /IT Eng.(New)

1. Explain computer Network. Write on OSI reference model.

A **Computer Network** is a collection of interconnected computing devices (nodes) that exchange data and share resources using a common set of communication protocols. These connections are established using either wired media (like twisted pair or fiber optics) or wireless media (like Wi-Fi or microwave)

The OSI Reference Model

The **Open Systems Interconnection (OSI)** model is a conceptual framework developed by the ISO to standardize network communication. It divides the complex process of networking into **seven distinct layers**.

The Seven Layers

7. Application Layer

The topmost layer that interacts directly with the user. It provides network services to the applications (like browsers or email clients).

- **Functions:** Resource sharing, remote file access.
- **Protocols:** HTTP, FTP, SMTP, DNS.

6. Presentation Layer

Acts as a data translator. It ensures that the data sent by the application layer of one system is readable by the application layer of another.

- **Functions:** Encryption/Decryption, Compression, and Translation (ASCII to EBCDIC).

5. Session Layer

Responsible for establishing, maintaining, and terminating "sessions" between applications.

- **Functions:** Dialogue control (half-duplex/full-duplex) and synchronization (checkpoints).

4. Transport Layer

Ensures end-to-end delivery of the message. It is responsible for error-free delivery and flow control.

- **Functions:** Segmentation (breaking data into smaller chunks), Reassembly, and **Error Control**.
- **Protocols:** TCP, UDP.

3. Network Layer

Manages the delivery of data between different networks. It handles logical addressing and chooses the best path for data.

- **Data Unit:** Packets.
- **Device:** Router.
- **Protocol:** IP (IPv4/IPv6).

2. Data Link Layer

Provides reliable transmission of data across the physical link. It deals with physical (MAC) addressing.

- **Data Unit:** Frames.
- **Device:** Switch, Bridge.
- **Functions:** Framing, Error Detection (CRC), and Flow Control.

1. Physical Layer

The lowest layer, dealing with the actual physical connection between devices. It defines the electrical and mechanical specifications.

- **Data Unit:** Bits.
- **Device:** Hub, Repeater, Cables.
- **Functions:** Bit synchronization and physical topology (Bus, Star, etc.)

2. Describe client server architecture. Explain any four network devices.

Client-Server Architecture

Client-Server Architecture is a network model where the workload is distributed between the providers of a resource or service (called **Servers**) and service requesters (called **Clients**).

How it Works:

- **The Request-Response Cycle:** The client sends a request (e.g., "Show me this webpage") to the server over the network. The server processes the request, retrieves the necessary data, and sends a response back to the client.
- **The Server:** A high-powered computer that stays active 24/7. It manages centralized resources like databases, files, and applications.
- **The Client:** User devices (PCs, laptops, smartphones) that access the services provided by the server.

Key Advantages:

- **Centralization:** Data is stored in one location, making backups and security management much easier.
- **Scalability:** You can add more clients or upgrade the server's power without disrupting the rest of the network.
- **Security:** Access rights and permissions are managed centrally by the server.

2. Network Devices

Network devices are the hardware components used to connect computers or other electronic devices together so that they can share files or resources.

I. Hub

A Hub is a basic networking device that operates at the **Physical Layer (Layer 1)**. It is used to connect multiple segments of a LAN.

- **How it works:** When a hub receives a packet of data at one of its ports, it **broadcasts** (copies) that data to all other ports.
- **Limitation:** It is a "dumb" device because it does not filter data or know which specific device the data is meant for, often leading to network traffic congestion.

II. Switch

A Switch is a more intelligent device that operates at the **Data Link Layer (Layer 2)**.

- **How it works:** It uses **MAC addresses** to identify devices. When it receives data, it sends it only to the specific port of the intended recipient.
- **Advantage:** This significantly reduces collisions and increases the efficiency and speed of the network compared to a hub.

III. Router

A Router is a sophisticated device that operates at the **Network Layer (Layer 3)**. Its primary job is to connect different networks (e.g., connecting your home LAN to the Internet).

- **How it works:** It uses **IP addresses** to determine the best path (routing) for data to travel across multiple networks.
- **Function:** It maintains a routing table and acts as a gateway for all outgoing and incoming external traffic.

IV. Gateway

A Gateway is a node that serves as an "entrance" to another network. It can operate at **all seven layers** of the OSI model.

- **How it works:** Its main role is to translate protocols between two different network architectures (e.g., connecting a TCP/IP network to an older AppleTalk or IPX/SPX network).
- **Analogy:** If a router is like a bridge between two towns, a gateway is like an international border crossing where you have to translate your language and currency to enter.

3. What is transmission media? Differentiate between guided and unguided media.

Transmission Media is the physical path between a transmitter and a receiver in a data communication system. It carries the data in the form of electromagnetic signals (electrical voltage, light pulses, or radio waves).

Differentiate between guided and unguided media.

Guided (Wired)	Unguided (Wireless)
Physical (Copper/Glass)	Non-physical (Air/Vacuum)
Defined/Constrained	Undefined/Broadcasted
Required	Not Required
Ethernet, Coaxial, Fiber	Wi-Fi, Radio, Bluetooth
High (Hard to tap)	Low (Easy to intercept)
Very High (up to Gbps)	Lower (affected by distance)
Cables pass through walls	Walls block/reflect signals
Magnetic (EMI)	Atmospheric (Rain/Fog)
Fixed (No movement)	Mobile (Work anywhere)
High (Physical breaks)	Low (No physical wear)

4. What are the different functions of data link layer? Explain them.

Functions of Data Link Layer (DLL)

The Data Link Layer is the second layer of the OSI model. It is responsible for reliable communication between two directly connected nodes over a physical medium. It acts as a bridge between the Physical Layer (raw bits) and the Network Layer (logical addressing). Here are the major functions explained in detail:

1. Framing

- Meaning: The DLL takes raw bits from the Physical Layer and organizes them into frames (structured packets of data).
- Purpose: Frames make it easier to identify the start and end of a message.
- How it works:
 - Adds headers (source/destination MAC address, control info).
 - Adds trailers (error detection codes like CRC).
- Example: In Ethernet, a frame contains preamble, source MAC, destination MAC, data, and CRC.

2. Physical Addressing

- Meaning: DLL uses MAC addresses (unique hardware addresses) to deliver frames to the correct device within a LAN.
- Purpose: Ensures that data reaches the intended recipient on the same network.
- Example: When a computer sends data in a LAN, the frame contains the destination MAC address so only the intended device accepts it.

3. Error Detection and Control

- Meaning: Ensures that transmitted data is received correctly.
- Techniques:
 - Parity bits (simple error check).
 - Checksum (adds up values to detect errors).
 - CRC (Cyclic Redundancy Check) (powerful error detection method).
- Control: If errors are detected, DLL requests retransmission.
- Example: Ethernet uses CRC to detect corrupted frames.
- Exam Note: DLL detects errors, but correction is often handled by higher layers.

4. Flow Control

- Meaning: Prevents a fast sender from overwhelming a slow receiver.
- Purpose: Maintains smooth communication between devices with different speeds.
- Methods:
 - Stop-and-Wait Protocol: Sender waits for acknowledgment before sending next frame.
 - Sliding Window Protocol: Sender can send multiple frames before needing acknowledgment.
- Example: In reliable communication, flow control ensures no buffer overflow at the receiver..

5. Access Control (Media Access Control – MAC)

- Meaning: Determines which device can use the communication channel when multiple devices share the same medium.
- Techniques:
 - CSMA/CD (Carrier Sense Multiple Access with Collision Detection) → used in wired Ethernet.
 - CSMA/CA (Collision Avoidance) → used in Wi-Fi.

5 Explain the CSMA/CD LAN architecture.

CSMA/CD: The Breakdown

1. Carrier Sense (CS)

Before a device sends data, it "listens" to the cable (the carrier) to check for a signal.

- **Idle:** If the line is quiet, the device starts transmitting.
- **Busy:** If it senses a signal, it waits until the line is free.

2. Multiple Access (MA)

This refers to the fact that many devices are connected to the same physical medium (the wire) and all have equal right to access it.

3. Collision Detection (CD)

Even with "listening," two devices might sense the line is idle at the same time and both start sending. This results in a **Collision**, which garbles the data.

- If a collision is detected, the transmitting devices immediately stop sending the frame.
- They send a **Jam Signal** to notify all other devices on the network that a collision has occurred.

The Working Process (Step-by-Step)

1. **Listen:** A station listens to the medium.
2. **Transmit:** If the medium is idle, it sends the data.
3. **Monitor:** While sending, it continues to listen for a collision.
4. **Collision:** If a collision is detected:
 - Stop transmission.
 - Send a **Jam Signal**.
5. **Back-off:** The station waits for a **random amount of time** (using the Binary Exponential Back-off algorithm) before trying to send again. This randomness ensures the two devices don't collide again immediately.

Key Characteristics for the Exam

- **Standard:** IEEE 802.3.
- **Layer:** Data Link Layer (MAC Sublayer).
- **Topology:** Mostly used in **Bus** and **Star** topologies with Hubs.
- **Efficiency:** It works very well under low-to-medium traffic, but efficiency drops if too many devices are trying to talk at once (high collision rate).

6. Write on circuit switching and packet switching. Define routing and state basic difference between static and dynamic routing.

Circuit Switching.

Circuit switching is a method of communication in which a dedicated physical path (circuit) is established between the sender and receiver before data transmission begins. This path remains reserved exclusively for the two parties throughout the communication session, regardless of whether data is being transmitted continuously or not.

- Phases:
 1. Setup phase – A circuit is established.
 2. Data transfer phase – Information flows continuously.
 3. Termination phase – Circuit is released.
- Key Features:
 - Guaranteed bandwidth and consistent quality.
 - No delay once the circuit is established.
 - Inefficient because resources remain occupied even during silence.
- Example: Traditional telephone networks where a line is reserved for the entire call.

2. Packet Switching

Packet switching is a communication technique where data is divided into small packets, each containing source and destination addresses. These packets are transmitted independently across the network and may take different routes to reach the destination, where they are reassembled into the original message.

- Process:
 1. Data broken into packets.
 2. Each packet routed independently.
 3. Destination reassembles packets.
- Key Features:
 - Efficient use of bandwidth (no dedicated path).
 - Supports multiple users simultaneously.
 - Packets may arrive out of order or with delay, requiring reassembly.
- Example: Internet communication (emails, browsing, file transfer).

Routing.

Routing is the process of selecting the best path for data packets to travel from source to destination across a network. Routers use routing tables and algorithms to determine the most efficient path based on factors like distance, cost, congestion, and network topology.

difference between static and dynamic routing.

S.N.	Feature	Static Routing	Dynamic Routing
1	Configuration	Manually entered by the Administrator.	Automatically discovered by Routing Protocols.
2	Adaptability	Does not adapt to network changes or failures.	Automatically adapts and reroutes during failures.
3	Protocols	No routing protocols are required.	Uses protocols like RIP, OSPF, or BGP.
4	Routing Table	Table is created once and stays fixed.	Table is updated periodically or when a change occurs.
5	Resource Usage	Very low (uses minimal CPU, RAM, and bandwidth).	Higher (consumes CPU/RAM to process updates).
6	Security	Higher security ; paths are hidden and controlled.	Lower; routing updates can be spoofed or intercepted.
7	Best For	Small, simple, and stable networks.	Large, complex, and growing networks.
8	Path Choice	Admin defines the path based on personal choice.	Router calculates the "Best Path" based on metrics.

7. What is dynamic routing protocols? Explain about Rip

Definition.

Dynamic routing protocols are network protocols that automatically discover, maintain, and update routing information between routers. Instead of manually configuring routes (as in static routing), dynamic protocols allow routers to communicate with each other, share information about network topology, and adjust routes when changes occur (like link failures or congestion).

RIP (Routing Information Protocol)

RIP is one of the oldest and simplest dynamic routing protocols. It is categorized as a **Distance-Vector Routing Protocol**.

How RIP Works:

1. **Metric (Hop Count):** RIP uses "Hop Count" as its only metric to find the best path. A "hop" is simply a router. If Path A has 2 routers and Path B has 3 routers, RIP will always choose Path A.
2. **Max Hops:** The maximum number of hops allowed is **15**. A distance of **16** is considered unreachable (this limits RIP to small networks).
3. **Periodic Updates:** Every **30 seconds**, a router sends its *entire* routing table to all its neighbors, even if nothing has changed.
4. **Routing Table:** It builds a map based on the information it hears from neighbors ("I heard from Router B that Network X is 2 hops away").

Advantages of RIP:

- **Simple to Configure:** Very easy to set up on small networks.
- **Low Complexity:** Does not require powerful hardware (low CPU/RAM usage).
- **Universal:** Supported by almost all routers regardless of the manufacturer.

Disadvantages of RIP:

- **Slow Convergence:** It takes a long time for all routers to learn about a network change.
- **Bandwidth Waste:** Sending the whole table every 30 seconds creates unnecessary traffic.
- **Limited Size:** Cannot be used in large networks due to the 15-hop limit.
- **Doesn't Consider Speed:** RIP will choose a slow 56kbps line with 1 hop over a fast 1Gbps fiber link with 2 hops because it only cares about the number of routers.

8. Explain the duties of transport layer, Write on the uDP (User Datagram Protocol).

Transport Layer – Duties

The Transport Layer is the fourth layer of the OSI model. Its main responsibility is to ensure end-to-end communication between applications running on different hosts. It provides reliable or unreliable delivery depending on the protocol used (TCP or UDP).

Major Duties of Transport Layer

1. Segmentation and Reassembly
 - Breaks large messages from the application layer into smaller segments for transmission.
 - At the destination, reassembles segments into the original message.
 - Example: A large file is divided into smaller chunks before sending.
2. End-to-End Communication
 - Provides logical communication between processes on different machines.
 - Uses port numbers to identify applications (e.g., HTTP uses port 80).
3. Error Detection and Correction
 - Ensures data integrity by detecting errors.
 - TCP provides error correction, while UDP only detects errors but does not correct them.
4. Flow Control
 - Prevents a fast sender from overwhelming a slow receiver.
 - TCP uses mechanisms like sliding window for flow control.
5. Connection Control
 - Can establish, maintain, and terminate connections.
 - TCP is connection-oriented, while UDP is connectionless.
6. Multiplexing and Demultiplexing
 - Multiplexing: Multiple applications can send data simultaneously over the same network.
 - Demultiplexing: At the receiver, data is directed to the correct application using port numbers.

User Datagram Protocol (UDP)

Definition

UDP is a connectionless transport layer protocol that provides fast but unreliable communication. It is often called a “best-effort” protocol because it does not guarantee delivery, order, or error correction.

Characteristics of UDP

1. Connectionless
 - No need to establish a connection before sending data.
 - Each packet (datagram) is independent.
2. Unreliable Delivery
 - No acknowledgment of received packets.
 - Packets may be lost, duplicated, or arrive out of order.
3. Lightweight Protocol
 - Minimal overhead (only 8-byte header).
 - Faster than TCP because it skips reliability checks.
4. Error Detection Only
 - Uses checksum for error detection.
 - No retransmission or correction.
5. Port Numbers
 - Uses source and destination port numbers to identify applications.

Structure of UDP Header

- Source Port (16 bits)
- Destination Port (16 bits)
- Length (16 bits)
- Checksum (16 bits)

Applications of UDP

- Streaming media (video/audio) → speed more important than reliability.
- Online gaming → real-time communication.
- VoIP (Voice over IP) → low latency required.

9. What is sub-netting? Subnet the network IP 192.168.0.0/24 into four subnet.

Definition

Subnetting is the process of dividing a large network (IP block) into smaller, manageable sub-networks (subnets). Each subnet functions as an independent network, but all belong to the same larger IP range.

Subnetting 192.168.0.0/24 into 4 Subnets

To divide a network into 4 subnets, we need to "borrow" bits from the Host portion and give them to the Network portion.

Step 1: Find the number of bits to borrow

We use the formula $2^n \geq \text{Number of subnets required}$.

- Here, we need 4 subnets.
- $2^2 = 4$.
- Therefore, we must borrow **2 bits** from the host part.

Step 2: Determine the New Subnet Mask

- The original mask is /24, which is 255.255.255.0.
- In binary, the last octet was 00000000.
- After borrowing 2 bits, it becomes 11000000.
- Binary 11000000 is **192** in decimal.
- **New Subnet Mask: 255.255.255.192 (or /26).**

Step 3: Determine the Block Size (Magic Number)

- Subtract the last non-zero octet from 256:
- $256 - 192 = 64$.
- The networks will increment by **64**.

Step 4: Create the Subnet Table

Subnet #	Network ID	First Usable IP	Last Usable IP	Broadcast ID
1	192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
2	192.168.0.64	192.168.0.65	192.168.0.126	192.168.0.127
3	192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
4	192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255

10: Write short notes on

(a) DHCP (Dynamic Host Configuration Protocol)

DHCP is an Application Layer protocol used to automatically assign IP addresses and other network configurations to devices on a network.

- **How it works:** It follows the **DORA** process:
 1. **Discover:** Client searches for a DHCP server.
 2. **Offer:** Server offers an IP address.
 3. **Request:** Client requests to use that IP.
 4. **Acknowledge:** Server confirms and "leases" the address.
- **Purpose:** It eliminates the need for manual IP configuration (Static IP), preventing IP conflicts and saving time for network administrators.
- **Components:** It assigns the **IP Address, Subnet Mask, Default Gateway, and DNS Server** details automatically.

(b) Encryption and Decryption

These are the primary functions of the **Presentation Layer (Layer 6)** used to ensure data security and privacy.

- **Encryption:** The process of converting plain, readable text (Plaintext) into an unreadable, scrambled format (Ciphertext) using a mathematical algorithm and a "key."
- **Decryption:** The reverse process of converting Ciphertext back into Plaintext so the receiver can understand the message.
- **Types:**
 1. **Symmetric:** Uses the same key for both encryption and decryption.
 2. **Asymmetric:** Uses a "Public Key" to encrypt and a "Private Key" to decrypt (much more secure).

(c) Firewall

A Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

- **Function:** It acts as a barrier between a trusted internal network (like your office LAN) and an untrusted external network (like the Internet).
- **Types:**
 1. **Packet Filtering:** Inspects individual packets based on IP address or Port number.
 2. **Proxy Firewall:** Acts as an intermediary between two systems so they never connect directly.
- **Key Goal:** To prevent unauthorized access (hackers/malware) from entering the private network.

(d) DNS (Domain Name System)

DNS is the "Phonebook of the Internet." It translates human-friendly domain names into machine-friendly IP addresses.

- **Function:** When you type `www.google.com`, DNS translates it to an IP like `142.250.190.46`.
- **Hierarchy:** It works in a hierarchical structure starting from Root Servers, then TLD (Top Level Domain like `.com`), and finally Authoritative servers.
- **Benefit:** Users don't have to memorize complex strings of numbers (IPs) for every website they want to visit.

IT 2081/2082

1. Explain Transmission impairment. Describe the block diagram of communication system.

Transmission Impairment

Transmission impairment means when a signal gets messed up or damaged while traveling from one place to another. Think of it like sending a message through a long telephone line — by the time it reaches the other end, it might sound unclear or distorted.

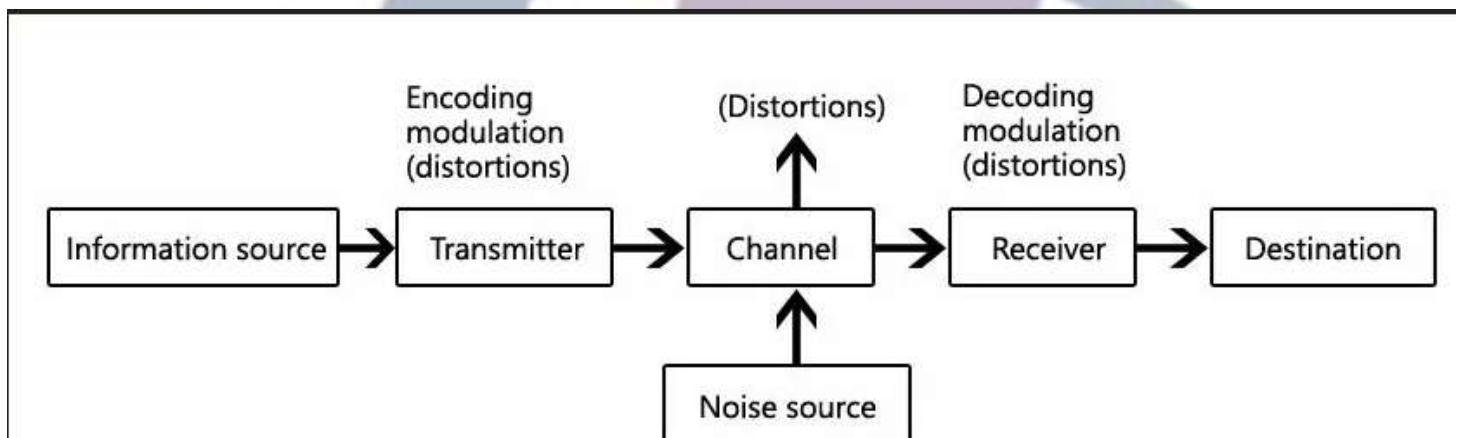
What Causes Transmission Impairment?

Attenuation — This is when the signal gets weaker as it travels. Imagine shouting across a long distance; the farther away someone is, the quieter your voice becomes. The same thing happens with electrical signals in wires or light signals in fiber optic cables. Long distances require special equipment to boost the signal back up.

Distortion — Sometimes different parts of the signal travel at different speeds through the medium, so the signal shape gets messed up. If you send a clean, clear wave through a cable, it might come out the other end looking bumpy or deformed. It's like sending a picture through a filter that changes how it looks.

Noise — This is basically interference or unwanted signals that mix with your original signal. Imagine trying to listen to someone talk in a loud, crowded room — there's so much background noise that you can't hear them clearly. In data transmission, this noise comes from electrical equipment nearby, heat in the wires, or signals from other cables running close by.

Dispersion — In fiber optic cables especially, different colors of light travel at slightly different speeds. Over long distances, this causes the signal to spread out and become unclear.



Communication System Block Diagram - Component Description

Looking at your diagram, here's what each component does:

Information Source

This is where the message or data comes from. It could be a microphone (for voice), a camera (for video), a computer (for data), or any device that creates the original information that needs to be sent. The source produces the raw message.

Transmitter

The transmitter takes the message from the source and prepares it for traveling through the channel. It does three main things:

- **Encoding** — Converts the message into a format that can be sent (like changing sound into electrical signals)
- **Modulation** — Changes the signal so it can travel through the channel properly (like putting it on a radio wave)
- **Amplification** — Makes the signal strong enough to travel long distances

The distortions mentioned here mean the signal might get slightly damaged or changed during these processes.

Channel (Transmission Medium)

This is the path that carries the signal from transmitter to receiver. It could be telephone wires, fiber optic cables, air (for radio/wireless), or any medium. The channel is where the signal travels, but it's also where problems happen.

Noise Source

Noise is unwanted signals that interfere with your message while it travels through the channel. Common sources include:

- Electrical interference from nearby equipment
- Weather and atmospheric conditions
- Other signals nearby (crosstalk)
- Heat in the wires

Noise makes the received signal unclear and can cause errors.

Receiver

The receiver catches the signal from the channel and tries to recover the original message. It does:

- **Amplification** — Boosts the weak signal so it's stronger
- **Demodulation** — Removes the carrier wave to get back the actual message
- **Decoding** — Converts the signal back into the original format (like electrical signals back to sound)

Again, distortions can happen here too, meaning the signal might not be perfectly recovered.

Destination

This is the final endpoint where the message arrives. It could be a speaker playing sound, a screen showing video, a printer printing data, or a person receiving the information. The destination receives the decoded message and uses it.

Overall Process

Information flows like this: The source creates a message → the transmitter encodes and sends it → it travels through the channel (where noise interferes) → the receiver catches and decodes it → the destination receives the final message.

2. Differentiate between MAN and WAN. Explain OSI reference model.

MAN vs WAN - Detailed Comparison Table

#	Feature	Remote Work	Office Work
1	Commute	Zero; more sleep or personal time.	Can be long and stressful.
2	Flexibility	High; easier to manage chores/life.	Structured; fixed start/end times.
3	Socializing	Mostly digital; can feel isolating.	In-person chats and team bonding.
4	Environment	Personalized (pajamas allowed!).	Professional and standardized.
5	Distractions	Household chores or family.	Chatty coworkers or loud meetings.
6	Collaboration	Scheduled via video calls/Slack.	Spontaneous "watercooler" ideas.
7	Costs	Saves money on gas and lunch.	Higher spending on travel and attire.
8	Boundaries	Harder to "switch off" from work.	Clear physical separation of life/work.

OSI Reference Model (7 Layers)

Layer 7: Application Layer

What it does: This is the top layer where users interact with the network. It provides services like email, web browsing, file transfer, and messaging.

Devices/Protocols: Web browsers (Chrome, Firefox), email (Gmail, Outlook), FTP (file transfer), HTTP/HTTPS (websites)

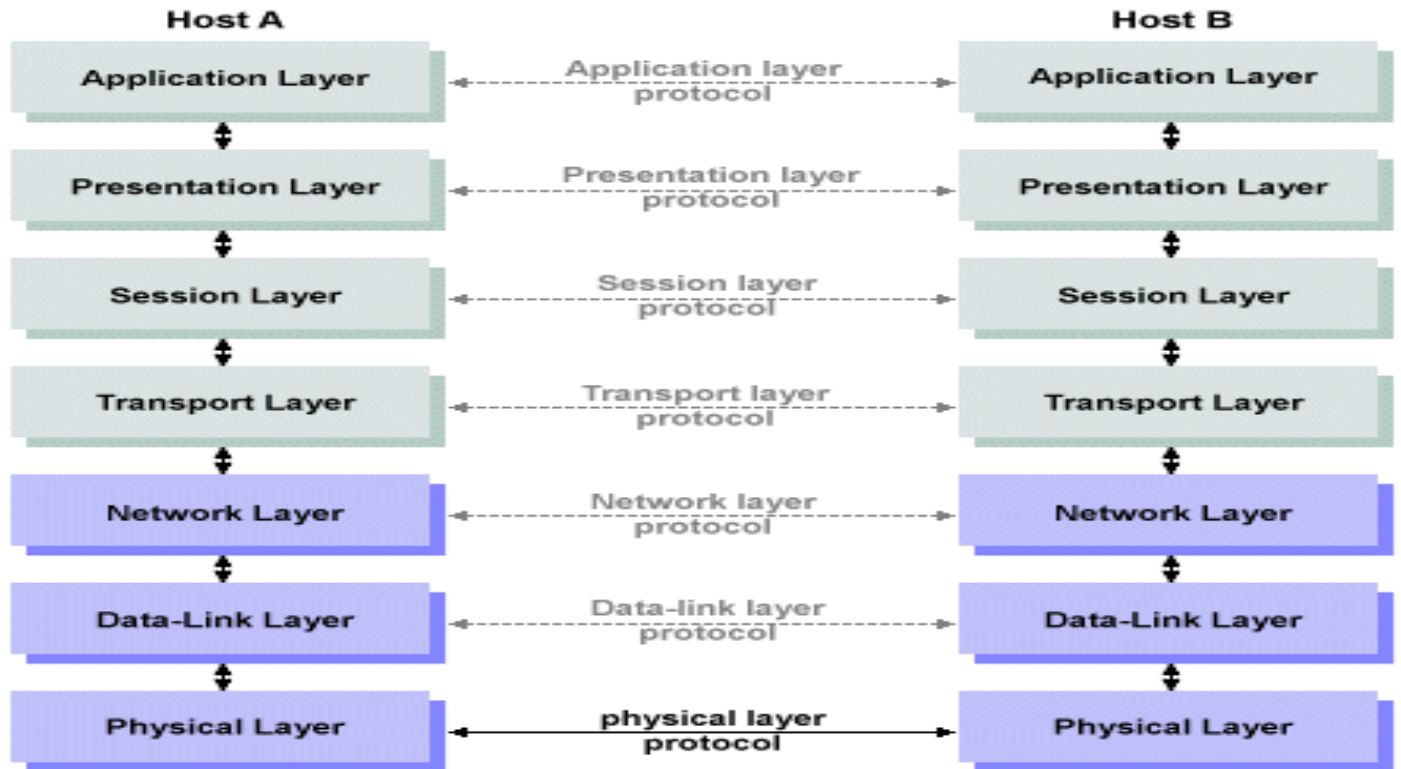
Examples: When you open Facebook or Gmail, you're using the Application Layer

Layer 6: Presentation Layer

What it does: This layer prepares data for the user. It translates, encrypts, and compresses data so it looks nice on your screen.

Job: Encryption, decryption, compression, translation (like converting between different formats)

Examples: Converting a file from one format to another, encrypting passwords, showing images properly on your screen



Layer 5: Session Layer

What it does: This layer manages conversations between computers. It starts, maintains, and ends connections.

Job: Opens and closes conversations, keeps track of who's talking to whom, manages login sessions

Examples: When you log into a website, this layer manages your session. If the connection breaks, it can reconnect.

Layer 4: Transport Layer

What it does: This layer makes sure data gets to the right place reliably and in order. It's like a delivery service.

Protocols: TCP (reliable, checks for errors), UDP (fast but doesn't check for errors)

Examples: When you download a file, TCP makes sure every piece arrives correctly. When you play online games, UDP is used for speed.

Layer 3: Network Layer

What it does: This layer decides the best path for data to travel from one computer to another across the network. It's like a GPS for data.

Protocols: IP (Internet Protocol) — assigns addresses to computers

Job: Routing (finding the best path), addressing (IP addresses like 192.168.1.1)

Examples: Your computer's IP address, routers that direct data to the right destination

Layer 2: Data Link Layer

What it does: This layer handles direct communication between devices on the same network. It makes sure data frames are sent correctly between neighbors.

Protocols: Ethernet, WiFi, MAC addresses

Job: Adds physical addresses (MAC addresses), error checking, framing

Examples: Your computer's MAC address, switching between devices on your home network

Layer 1: Physical Layer

What it does: This is the actual hardware — the physical cables, wires, and signals that carry the data. It's the lowest and most basic layer.

Hardware: Ethernet cables, WiFi antennas, fiber optic cables, switches, hubs, modems

Job: Transmits raw bits (1s and 0s) through cables

Examples: The copper wire connecting your computer to the router, the WiFi signal in the air

3. What is a public switched telephone network? Explain fiber optic cable with its applications.

PSTN is the traditional telephone network that connects telephones together so people can make voice calls to each other. It's the system that has been used for over 100 years to allow people around the world to talk to each other over long distances.

Explain fiber optic cable with its applications.

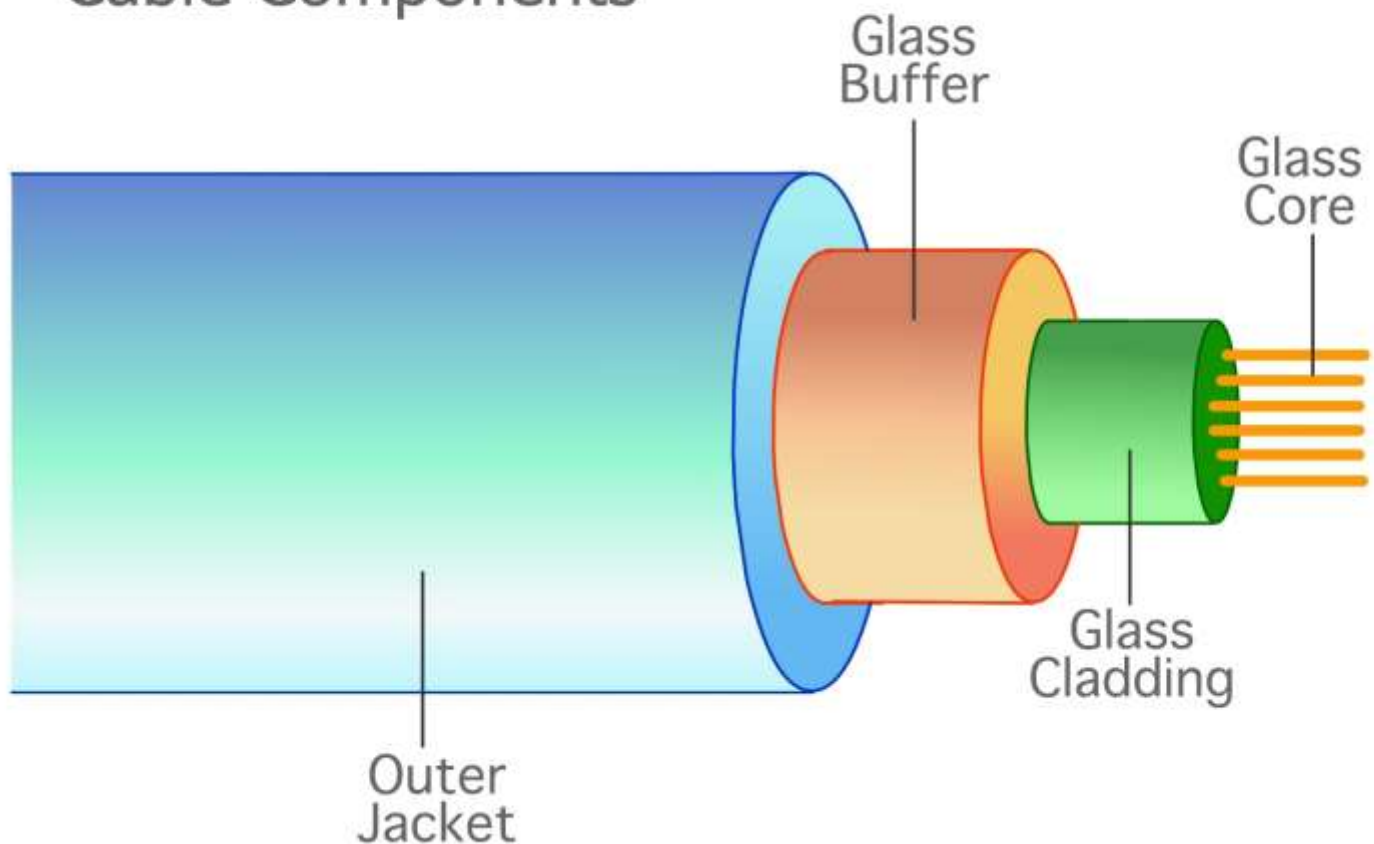
Fiber optic cable is a modern type of cable that uses thin strands of glass or plastic to transmit data using light signals instead of electrical signals. It's much faster and more reliable than traditional copper wires.

How Fiber Optic Cable Works

A fiber optic cable contains hair-thin glass fibers. Data is converted into light pulses, which travel through these fibers at the speed of light. The light bounces off the walls of the fiber (through a process called total internal reflection) and reaches the destination where it's converted back into electrical signals that computers can understand.

Think of it like this: Instead of sending electricity through copper wires (like traditional phone lines), you're sending light beams through glass tubes. Light travels much faster and doesn't get interfered with easily.

Fiber Optic Cable Components



Types of Fiber Optic Cable

Single-Mode Fiber (SMF):

- Has a very thin core (8-10 micrometers)
- Light travels in one path
- Longer distances (up to 100+ km)
- More expensive
- Used for long-distance telephone lines and Internet backbone

Multi-Mode Fiber (MMF):

- Has a thicker core (50-62.5 micrometers)
- Light travels in multiple paths
- Shorter distances (up to 2 km)
- Less expensive
- Used in building networks, LANs, and short-distance connections

Applications of Fiber Optic Cable

1. Telecommunications

- Long-distance telephone lines connecting cities and countries
- International submarine cables under the ocean connecting continents
- Backbone of the Internet infrastructure

2. Internet and Data Networks

- High-speed Internet connections (fiber-to-home, fiber-to-business)
- Data center networks where huge amounts of data transfer quickly
- Corporate networks that need very fast internal communication

3. Medical Applications

- Endoscopes (cameras for looking inside the human body)
- Laser surgery equipment
- Medical imaging systems

4. Military and Defense

- Secure communications that can't be easily intercepted
- Military command networks
- Submarine communication systems

5. Industrial Applications

- Monitoring systems in factories
- Remote sensing and measurement
- Control systems in hazardous environments

6. Television and Cable

- Cable TV distribution
- Broadcasting signals to homes
- Video transmission over long distances

7. Local Area Networks (LANs)

- Connecting buildings on a campus
- High-speed office networks
- Data center connections

8. Aerospace and Aviation

- Aircraft communication systems
- Navigation systems

4. What is framing? Explain the issues of data link layer

Framing is the process of organizing raw data into structured units called **frames** at the data link layer. A frame is a logically organized block of information consisting of a header, payload (actual data), and a trailer. Think of it like packaging a letter inside an envelope—the envelope provides structure and contains addressing information, while the letter is the actual content.

Issues in the Data Link Layer

Building a reliable bridge between hardware and software isn't easy. The Data Link Layer has to juggle several major challenges:

1. Frame Synchronization

The biggest hurdle is making sure the receiver can stay "in sync" with the sender. If the timing is off by even a fraction of a bit, the entire message becomes gibberish. Engineers use techniques like **Bit Stuffing** or **Byte Stuffing** (adding special "flag" sequences) to mark the boundaries of a frame.

2. Error Control

Physics is messy. Signal interference or thermal noise can flip a 0 to a 1 during transmission. The Data Link Layer must:

- **Detect Errors:** Using parity bits or Cyclic Redundancy Checks (CRC).
- **Correct/Recover:** Either by asking the sender to retransmit the data (ARQ) or using specialized codes to fix the bit on the fly.

3. Flow Control

Imagine a firehose trying to fill a tea cup. If a high-speed server sends data faster than a slow receiver can process it, the receiver's buffer will overflow, and data will be lost.

- **Stop-and-Wait:** The sender waits for an acknowledgment after every frame.
- **Sliding Window:** The sender can send multiple frames before needing an acknowledgment, which is much more efficient.

4. Media Access Control (MAC)

When multiple devices are on the same network (like a shared Wi-Fi channel), they can't all talk at once, or their signals will "collide." The layer must decide **who gets to speak and when**.

- In Ethernet, we use **CSMA/CD** (Collision Detection).
- In Wi-Fi, we use **CSMA/CA** (Collision Avoidance).

5. What is Ethernet? Explain ALOHA and VLAN.

Ethernet is a widely-used local area network (LAN) technology that defines standards for how devices physically connect and communicate within a network. It operates at the data link layer (Layer 2) and specifies how data is formatted, transmitted, and received over a shared medium—typically copper twisted-pair cables or fiber optics

ALOHA

ALOHA is a media access control protocol developed in the 1970s at the University of Hawaii for wireless network communication. It was one of the earliest protocols for managing shared medium access and served as a foundation for modern protocols like Ethernet's CSMA/CD.

How ALOHA works: Devices can transmit whenever they have data, without listening to the medium first (pure ALOHA). After sending a frame, the device waits for an acknowledgment from the receiver. If no acknowledgment arrives within a timeout period, the device assumes a collision occurred and retransmits after a random delay.

Slotted ALOHA: An improvement where time is divided into slots, and devices can only transmit at the start of a time slot, reducing collisions.

Issues with ALOHA:

- High collision rates, especially under heavy traffic
- Low efficiency (pure ALOHA achieves only about 18% maximum throughput; slotted ALOHA achieves about 37%)
- Wasted bandwidth due to collisions and retransmissions
- No mechanism to listen before transmitting (unlike CSMA/CD in Ethernet)

Despite its limitations, ALOHA demonstrated important concepts in random access protocols and influenced the development of better protocols like CSMA/CD and modern WiFi standards.

VLAN (Virtual Local Area Network)

A VLAN is a logical grouping of network devices that allows them to communicate as if they're on the same physical network segment, even though they may be physically separated or connected to different switches. VLANs operate at Layer 2 (data link layer) and Layer 3 (network layer).

How VLANs work: Network devices are assigned to VLANs through switch configuration, typically using VLAN IDs (1-4094). When devices on the same VLAN communicate, frames are tagged with the VLAN ID (using 802.1Q tagging standard). Switches use this tag to determine which ports should receive the frame. Devices on different VLANs cannot directly communicate without routing through a Layer 3 device.

Key benefits of VLANs:

- **Network Segmentation:** Divides a single physical network into multiple logical networks for better organization and security
- **Improved Security:** Isolates sensitive traffic (like finance or HR data) from general network traffic
- **Bandwidth Management:** Reduces broadcast traffic, since broadcasts are contained within a VLAN
- **Flexibility:** Devices can be moved or added to different VLANs through software configuration rather than physical rewiring
- **Cost Efficiency:** Allows organizations to use fewer physical switches while maintaining logical separation

Common VLAN applications:

- Departmental segregation (Sales VLAN, IT VLAN, HR VLAN)
- Guest network separation (keeping guest Wi-Fi isolated from corporate traffic)
- Voice and video separation (separate VLANs for VoIP and video conferencing)
- Server isolation (DMZ VLANs for web servers).

6. Calculate network address, usable host address, number of subnets and broadcast address for a network of 192.168.1.20/26.

Step 1: Understand the Subnet Mask

/26 indicates:

- Network bits = 26
- Host bits = $32 - 26 = 6$ bits
- Total addresses per subnet = $2^6 = 64$

Subnet Mask Calculation:

- Binary: 11111111.11111111.11111111.11000000
- Decimal: 255.255.255.192

Step 2: Calculate Network Address

To find the network address, we need to determine which /26 subnet block contains 192.168.1.20

Last octet calculation:

- With 6 host bits, subnet blocks are in increments of 64
- Block ranges: 0-63, 64-127, 128-191, 192-255
- The IP 192.168.1.20 falls in the 0-63 block (since $20 < 64$)
- Therefore, the first address (network address) = 0

Network Address = 192.168.1.0/26

Step 3: Calculate Broadcast Address

The broadcast address is the last address in the subnet block where all host bits are set to 1.

- Subnet block range: 0-63
- Last address in block = 63

Broadcast Address = 192.168.1.63

Step 4: Calculate Usable Host Addresses

Total addresses in subnet = 64

Usable host addresses = Total addresses - 2 (subtract network and broadcast addresses)

Number of Usable Host Addresses = $64 - 2 = 62$

Usable Host Range: 192.168.1.1 to 192.168.1.62

Step 5: Calculate Number of Subnets

The original network class is Class C (192.168.1.0/24)

Original subnet bits = 24 Current subnet bits = 26 Additional subnet bits = $26 - 24 = 2$ bits

Number of subnets = $2^2 = 4$ subnets

The 4 subnets are:

1. 192.168.1.0/26 (0-63)
2. 192.168.1.64/26 (64-127)
3. 192.168.1.128/26 (128-191)
4. 192.168.1.192/26 (192-255)

7.Explain quality of service. Differentiate between TCP and UDP.

Explain Quality of Service (QoS).

Quality of Service (QoS) is a set of techniques and technologies used to manage network resources and guarantee a certain level of performance for data transmission. It ensures that critical applications receive prioritized treatment and adequate bandwidth while maintaining acceptable performance standards for all network traffic.

Key Parameters of QoS:

- **Bandwidth:** The data rate provided to an application.
- **Latency (Delay):** The time it takes for a packet to travel from source to destination.
- **Jitter:** The variation in the delay of received packets (critical for smooth audio/video).
- **Packet Loss:** The percentage of packets that fail to reach the destination.

Applications Requiring QoS:

- **VoIP (Voice over IP):** Requires low latency (< 150 ms) and minimal jitter
- **Video Streaming:** Needs high bandwidth and consistent delivery
- **Video Conferencing:** Requires low latency and high reliability

Benefits of QoS:

- Ensures critical applications perform optimally
- Prevents network congestion and bottlenecks
- Improves user experience for real-time applications
- Enables efficient use of limited bandwidth

TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection-oriented: Establishes a session before sending data.	Connectionless: Sends data directly without a pre-established session.
Reliable: Guarantees that data reaches the destination.	Unreliable: Does not guarantee delivery; packets may be lost.
Uses a 3-way handshake (SYN, SYN-ACK, ACK) to start.	No handshake is performed.
Sequenced: Rearranges packets if they arrive out of order.	Unsequenced: Data is processed in the order it arrives.
Extensive error checking and retransmission of lost data.	Basic error checking (checksum), but no retransmission .
Slower due to the overhead of headers and acknowledgments.	Faster and more efficient for real-time applications.
Larger header (typically 20 bytes).	Smaller, lightweight header (8 bytes).
Provides flow and congestion control to prevent buffer overflow.	No flow control ; it just "fires and forgets."

7. What is PoP3? Differentiate between HTTP and HTTPS.

POP3 (Post Office Protocol version 3) is an application layer protocol used for retrieving (downloading) email messages from a mail server to a client computer or device. It is one of the most commonly used protocols for receiving emails.\

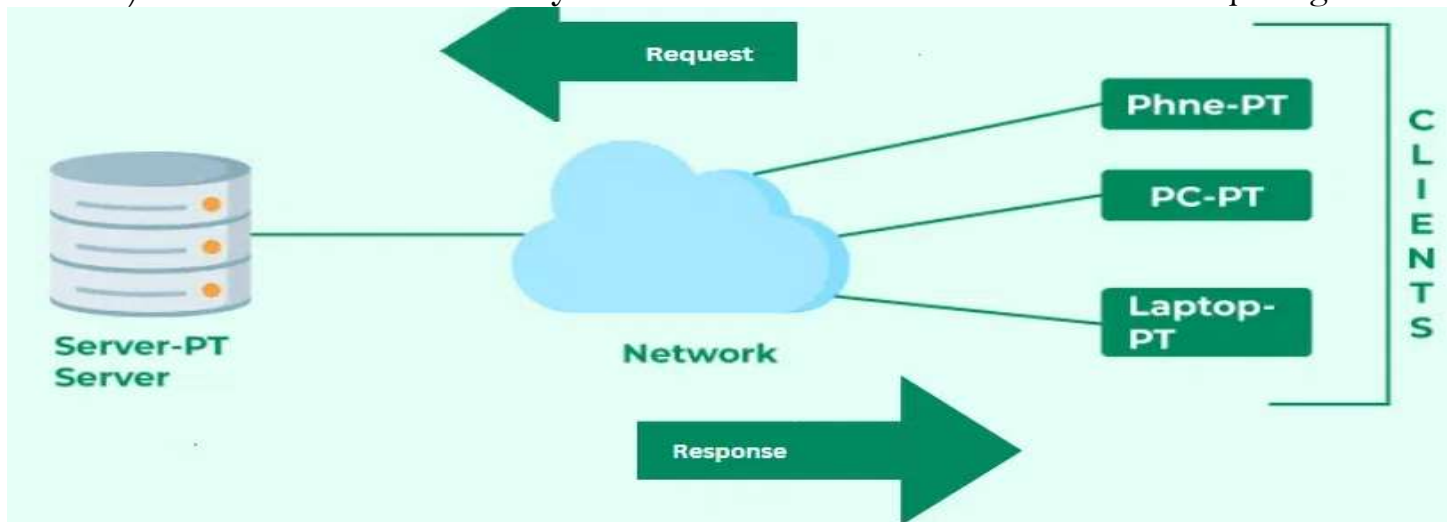
S.N.	Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
1	Full Form	It stands for Transmission Control Protocol.	It stands for User Datagram Protocol.
2	Connection Type	Connection-oriented: It must establish a connection before sending any data.	Connectionless: It sends data directly without waiting for a connection.
3	Reliability	Highly Reliable: It guarantees that the data reaches the destination safely.	Unreliable: It does not guarantee delivery; data may be lost in transit.
4	Handshaking	Uses a 3-way handshake (SYN, SYN-ACK, ACK) to start communication.	It has no handshaking process; it simply "fires and forgets."
5	Data Ordering	Ordered: It ensures that packets arrive and are read in the correct sequence.	Unordered: Packets can arrive in any order and are not rearranged.
6	Speed	Slower: Because it spends time checking for errors and acknowledgments.	Faster: It is very quick and efficient because it has very little overhead.
7	Error Control	Performs extensive error checking; if data is lost, it is retransmitted .	Performs basic error checking but never retransmits lost data.
8	Header Size	The header is larger and more complex, typically 20 bytes .	The header is small and simple, fixed at only 8 bytes .
9	Flow Control	It uses flow and congestion control to prevent the sender from overwhelming the receiver.	It has no flow control ; it sends data at the speed it is generated.

9a. What is a Router? Describe the Client-Server Model with figure.

A Router is a networking device that connects multiple networks together and forwards data packets between them based on their destination IP addresses. It operates at Layer 3 (Network Layer) of the OSI model and is essential for internet communication.

Describe the Client-Server Model with figure.

Client-Server Model is a distributed computing architecture where computing tasks are divided between clients (users or user machines) and servers (computers that provide services). It is one of the most widely used network architectures in modern computing.



Key Components:

1. **Client:** The device or program that requests a service. For example, a web browser (Chrome) on your phone is a client that asks for a webpage.
2. **Server:** The high-powered machine that provides the service or data. It stays "listening" for requests and sends the appropriate response back.
3. **Network:** The medium (like the Internet or a LAN) through which the client and server communicate.

How Does the Client-Server Model Work?

Client: A client is any device or software that initiates communication by requesting data or services from a server. Common client applications include:

Web browsers (e.g., Chrome, Firefox)

Email apps (e.g., Gmail, Outlook)

Server: A server is a powerful systems that listens for and responds to client requests by delivering data or performing tasks. Servers often handle multiple simultaneous client requests. Common server applications include:

- Web Servers (e.g., Apache, Nginx)
- Email Servers
- Database servers

Characteristics:

- **Centralization:** Data is stored in one central location (the server), making it easier to manage and back up.
- **Scalability:** You can add more clients easily, or upgrade the server's hardware to handle more traffic.
- **Security:** Since the server controls the data, it can enforce strict access rule

b. What is IP Address? List the types of IP Address.

IP Address (Internet Protocol Address) is a unique numerical identifier assigned to every device connected to a network that uses the Internet Protocol for communication. It serves as the device's address on the network, enabling data packets to be routed to the correct destination.

Types of IP Addresses:

- **Public IP Address:** The main address associated with the entire network, used to connect to the internet.
- **Private IP Address:** Assigned to individual devices within a private network (e.g., home/office) by a router.
- **Dynamic IP Address:** Automatically assigned by a network (via DHCP) and changes periodically.
- **Static IP Address:** Manually assigned and remains constant, typically used for servers or business purposes.
- **IPv4 (Internet Protocol version 4):** A 32-bit address, currently the most common format.
- **IPv6 (Internet Protocol version 6):** A 128-bit address created to replace IPv4 due to address exhaustion.

10. Write short notes on.

a. DNS (Domain Name System)

1. DNS stands for **Domain Name System**.
2. It converts **domain names into IP addresses**.
3. DNS makes internet usage **easy and user-friendly**.
4. It works like a **telephone directory** of the internet.
5. DNS reduces the need to remember IP numbers.
6. It improves **speed of website access**.
7. DNS uses a **hierarchical structure**.
8. Example: www.google.com → 142.250.183.14.

b. HDLC (High-Level Data Link Control)

1. HDLC is a **Data Link Layer protocol**.
2. It is used for **reliable data transmission**.
3. HDLC works in **point-to-point and multipoint links**.
4. It uses **frames** for data transmission.
5. HDLC provides **error detection**.
6. It supports **flow control**.
7. HDLC is commonly used in **WAN**.
8. It ensures **efficient and secure data transfer**.

c. Guided Media

1. Guided media is a **wired communication medium**.
2. Data travels through **physical cables**.
3. It provides **high data transmission speed**.
4. It is **less affected by noise**.
5. Guided media offers **better security**.
6. Examples include **twisted pair, coaxial, and optical fiber**.
7. It is commonly used in **LAN networks**.

8. Installation cost is **higher than wireless media**.

d. Analog Data Transmission

1. Analog data transmission uses **continuous signals**.
2. Data is represented in the form of **waves**.
3. Signal amplitude or frequency changes with data.
4. It is **highly affected by noise**.
5. Signal quality reduces over long distances.
6. Used in **radio and telephone communication**.
7. It is less secure than digital transmission.
8. Mostly used in **old communication systems**.

e. Properties of Secure Communication

1. **Confidentiality** ensures data privacy.
 2. **Integrity** prevents unauthorized data modification.
 3. **Authentication** verifies user identity.
 4. **Authorization** controls access rights.
 5. **Non-repudiation** prevents denial of communication.
 6. **Availability** ensures data is always accessible.
 7. **Encryption** protects data during transmission.
 8. **Security protocols** maintain safe communication
- 

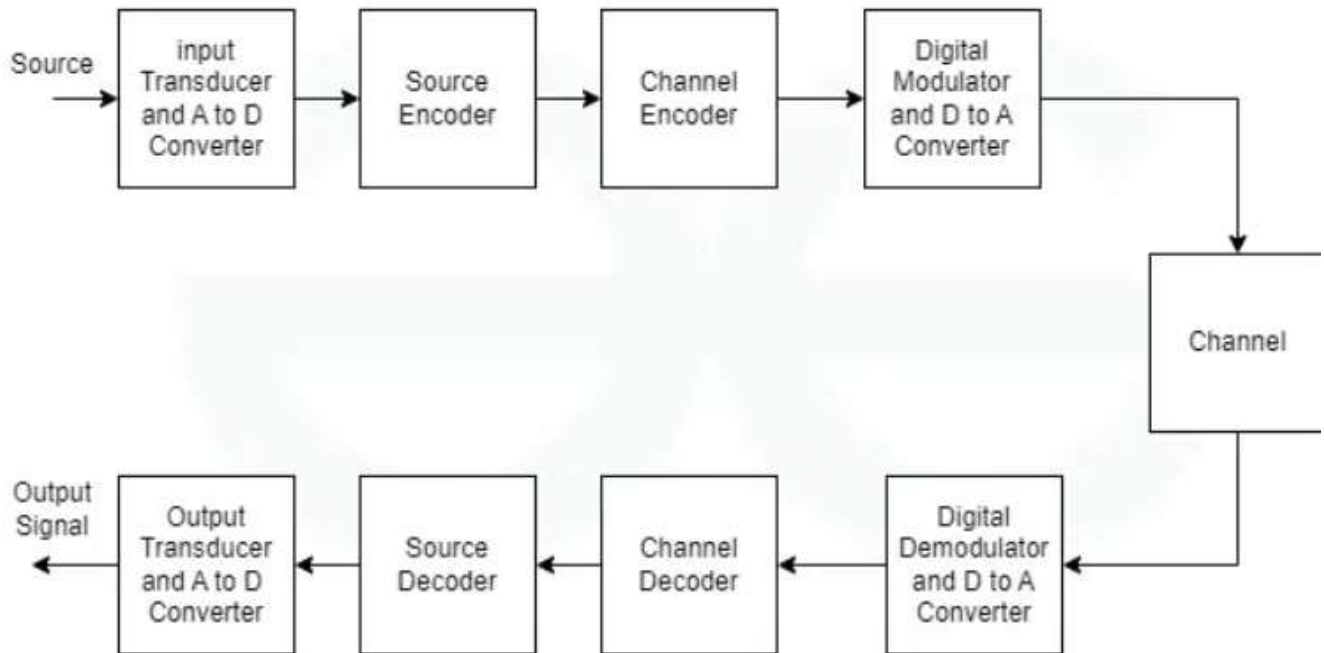
Regular Exam - 2081 Jestha/Ashadh

Diploma in Information Technology/

1. . What is transmission impairment? Draw the block diagram of digital communication system and explain.

Transmission impairment refers to any degradation or distortion of a signal as it travels from the transmitter to the receiver through a communication channel. These impairments affect the quality and reliability of data transmission, potentially causing errors in received data.

Components of Digital Communication



- **Source:** A source is the device that feeds the input signal into the system for processing. This can be a microphone, signal generator, or any other device capable of producing a signal.
- **Transducer:** The [transducer](#) is a device needed for generating electrical signals from the input signal. These electronic signals are important since data can't be transferred in any form and needs to be converted into some sort of signal.
- **Source Encoder:** A Source Encoder is used for encoding data by compressing it into bits that can help in reducing the bandwidth needed for transmission.
- **Channel Encoder:** During the transmission of data, errors are bound to get introduced therefore, a channel [encoder](#) is needed to eliminate errors due to noise. It intentionally adds some redundant bits that can be removed at the end.

- **Digital Modulator:** The modulation of the signal is performed by a Digital Modulator. This is necessary to convert the signal into a format that can be easily transmitted in a medium.
- **Channel:** This is the midway component in the system that helps to pass the signal from the transmitter end to the receiver end.
- **Digital Demodulator:** Once the signal has reached the receiver end, the signal needs to be converted from digital to analog form. This reconstruction of a signal is known as [demodulation](#) and is performed by the demodulator.
- **Channel Decoder:** Just like the channel encoder, the Channel Decoder is used for correction of errors at the receiver end. These errors are corrected using the redundant bits added.
- **Source Decoder:** This step is necessary to obtain a proper digitized signal therefore steps like sampling and quantizing are performed in the source [decoder](#).
- **Output Transducer:** This part involves the conversion of an electronic signal into a physical form that can be perceived by the device. Loudspeakers are a type of output [transducer](#).
- **Output Signal:** The final step is the collection of Output Signal that is generated after the entire process.

2. What are the function of network device? Explain any two of them.

Explain OSI reference model.

Network devices are hardware components that connect, manage, and control communication between computers and other devices in a network. Their main functions include:

- **Data transmission:** Forwarding data packets across the network.
- **Segmentation:** Dividing networks into manageable sections.
- **Filtering:** Controlling which data enters or leaves a network.
- **Conversion:** Translating signals between different formats (digital ↔ analog).
- **Security:** Protecting against unauthorized access.

Two Examples:

1. Router

- **Function:** Connects multiple networks (e.g., home network to the internet).
- **Role:** Determines the best path for data packets using IP addresses.
- **Example:** Your Wi-Fi router at home directs traffic between your devices and the ISP.

2. Switch

- **Function:** Connects multiple devices within a local area network (LAN).
- **Role:** Uses MAC addresses to forward data only to the intended device.
- **Example:** In an office, a switch connects all PCs and ensures efficient communication.

. Explain OSI reference model.

OSI Reference Model

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a communication system into seven layers. It was developed by the International Organization for Standardization (ISO) to help different systems communicate with each other.

The Seven Layers (from bottom to top):

Layer 1 - Physical Layer deals with the actual physical transmission of data. It defines the electrical, mechanical, and procedural specifications for activating and maintaining physical links between systems. Examples include cables, connectors, hubs, and repeaters. Data is transmitted as raw bits (1s and 0s).

Layer 2 - Data Link Layer handles direct link communication between adjacent nodes. It organizes data into frames and uses MAC addresses for local network delivery. Switches and network interface cards operate here. It also manages error detection and handles collision avoidance in shared media networks.

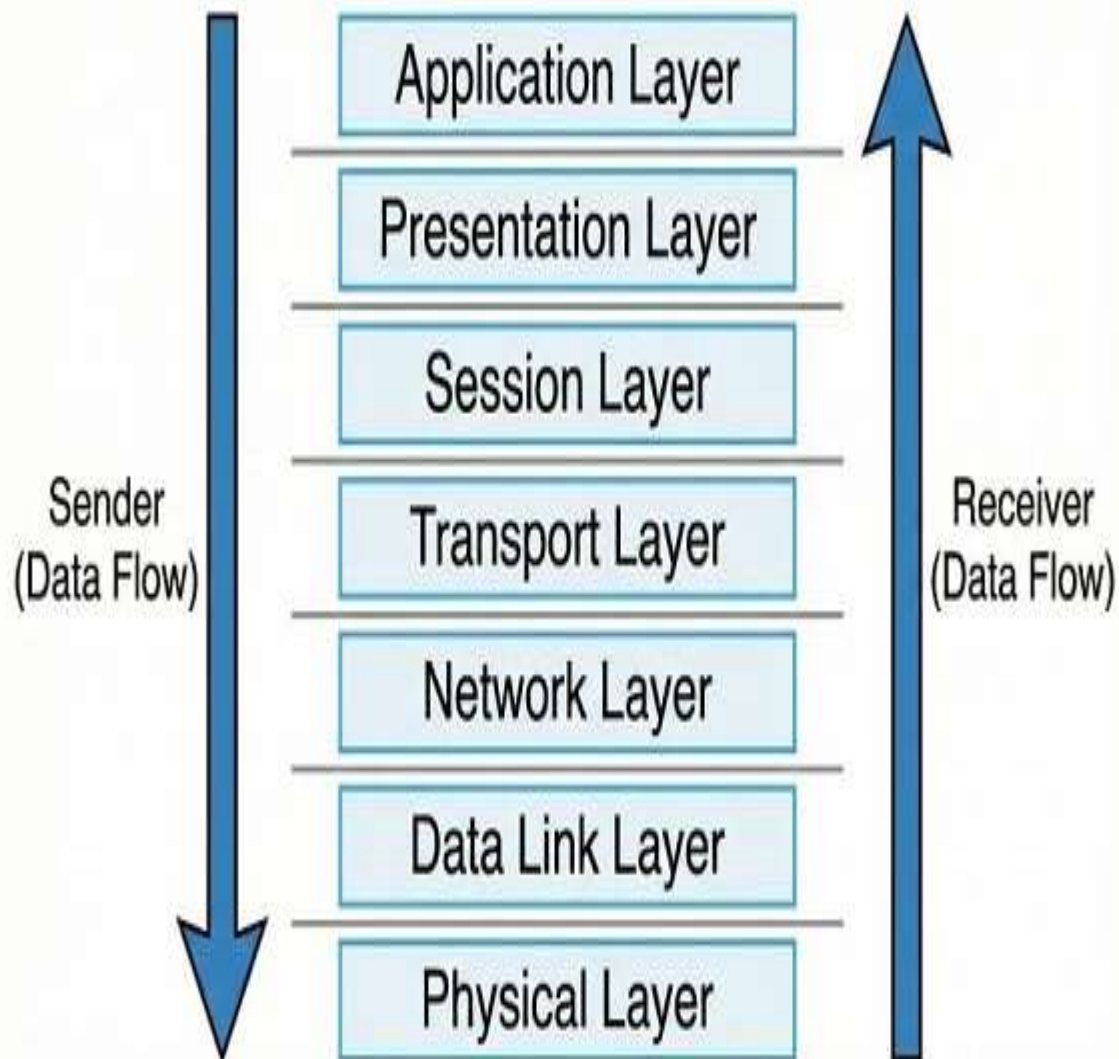
Layer 3 - Network Layer manages routing and logical addressing using IP addresses. Routers operate at this layer, determining paths for data packets across different networks. It handles congestion control and quality of service decisions.

Layer 4 - Transport Layer ensures reliable or unreliable end-to-end communication. TCP (reliable, connection-oriented) and UDP (fast, connectionless) protocols operate here. It manages flow control, error recovery, and multiplexing.

Layer 5 - Session Layer establishes, maintains, and terminates communication sessions between applications. It handles dialog control, determining who transmits and when, and synchronization of data exchange.

Layer 6 - Presentation Layer translates, encrypts, and compresses data into a format that the application layer can understand. It handles character encoding, data encryption, and compression algorithms.

Layer 7 - Application Layer provides network services directly to user applications. Email, web browsing, file transfer, and other user-facing services operate here. It includes protocols like HTTP, SMTP, FTP, and DNS.

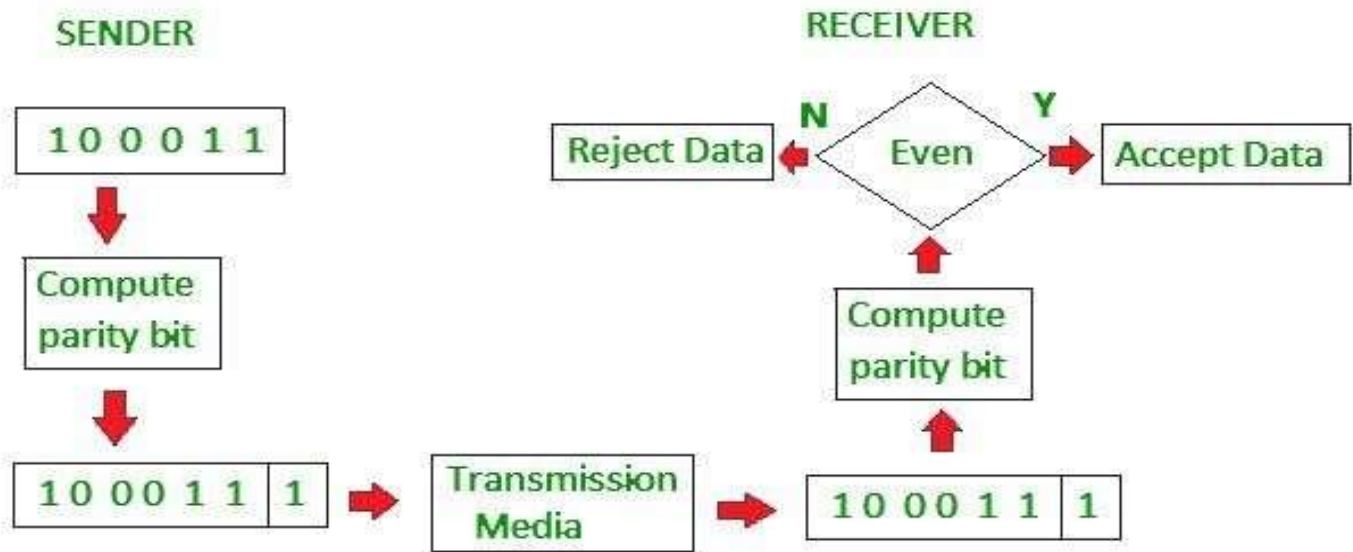


4. Discuss the error correction and error detection method in error correction detail.

Error Detection Methods

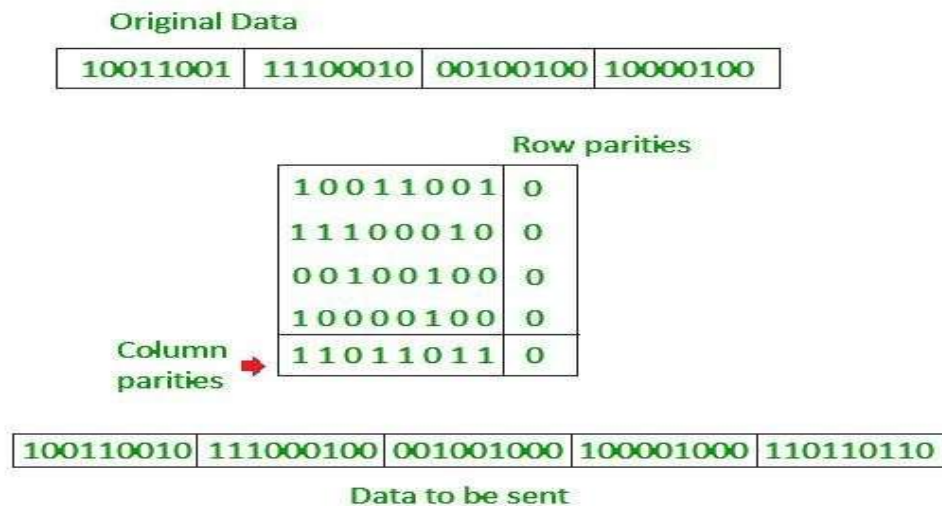
Simple Parity Check: Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's



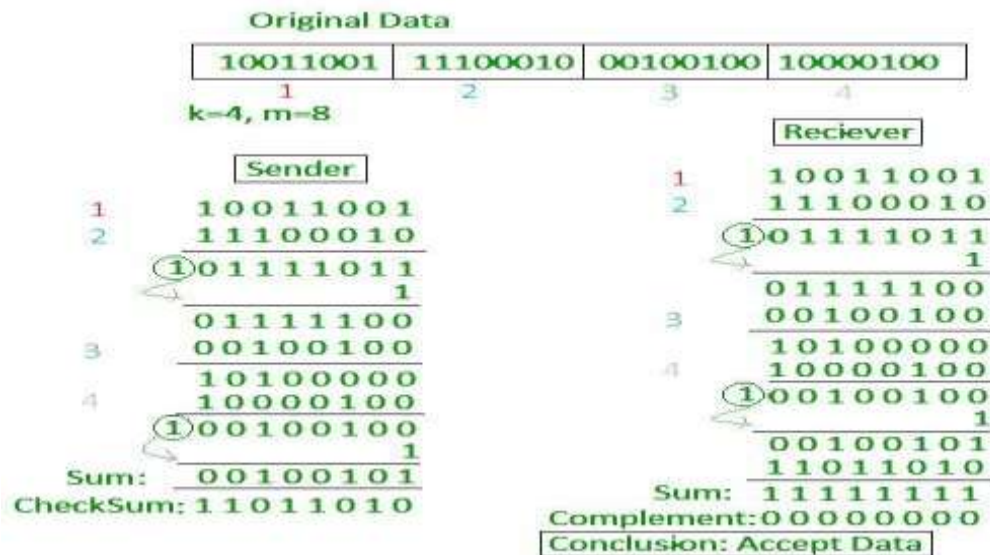
Two-dimensional Parity Check

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



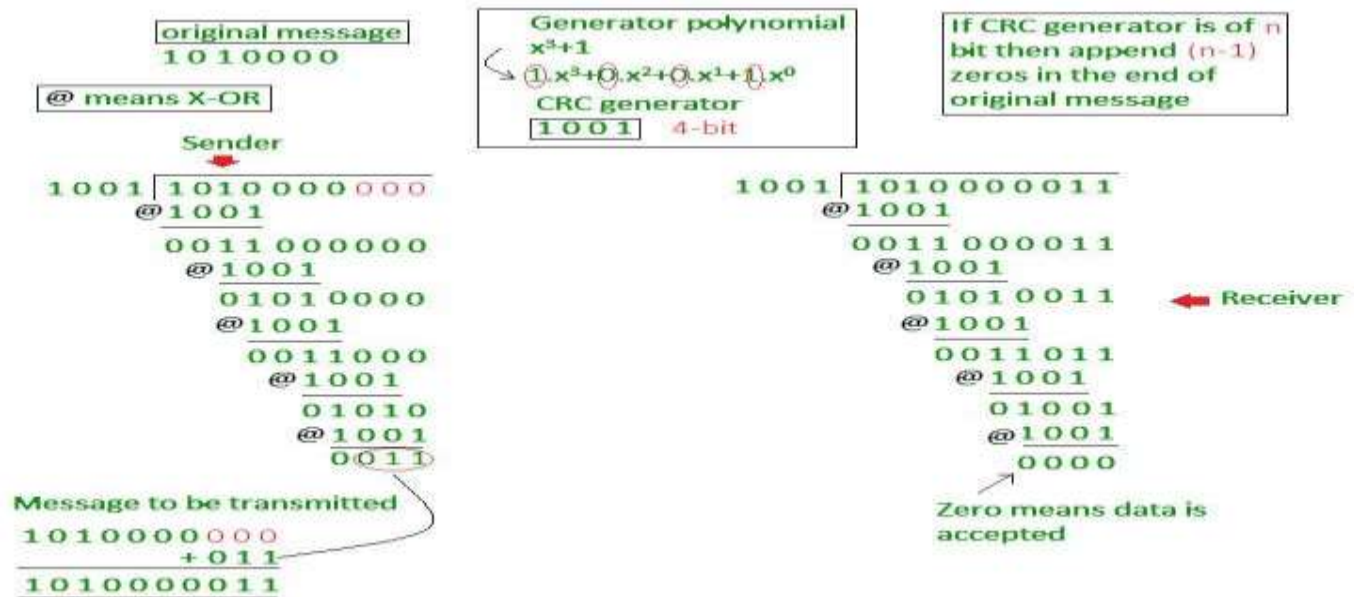
Checksum:

Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.



Cyclic Redundancy Check (CRC)

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



Error Correction:

In the digital world, error correction can be done in two ways

Backward Error Correction: When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit

Forward Error Correction: When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

. Hamming Code is also error correction method to used

.3 What is transmission media? Write short notes on optical fiber and satellite communication..

Transmission media are the physical pathways through which data signals travel from one device to another in a network. They form the backbone of communication systems and can be classified into two main categories: guided media (bounded) and unguided media (unbounded).

Optical Fiber (Short Note)

- Optical fiber is a **guided transmission media** that uses **light signals** to transmit data.
- It is made of **very thin strands of glass or plastic**.
- Data is transmitted using **total internal reflection** of light.
- It provides **very high data transmission speed**.
- Optical fiber has **very low signal loss**, even over long distances.
- It is **immune to electromagnetic interference (EMI)**.
- It is widely used in **internet backbone, cable TV, and long-distance communication**.
- It is **secure** and difficult to tap compared to copper cables.

Satellite Communication (Short Note)

- Satellite communication is an **unguided (wireless) transmission media**.
- It uses **artificial satellites** placed in space to transmit signals.
- The satellite receives signals from an earth station and **retransmits them** back to another station.
- It covers a **very large geographical area**.
- It is used for **TV broadcasting, mobile communication, GPS, and internet services**.
- Satellite communication supports **long-distance and international communication**.
- It is useful in **remote and rural areas** where cables are not available.
- It may suffer from **signal delay and weather effects**

5. Explain the architecture of LAN network with their advantages and disadvantages. Define ALOHA and token ring.

Answer: A Local Area Network (LAN) connects devices within a limited area like a building, enabling resource sharing and high-speed data transfer.

A LAN consists of interconnected devices such as computers, printers, servers, and switches, using physical cables (Ethernet) or wireless connections (Wi-Fi). The network architecture is often based on specific topologies (like star, bus, or ring) and utilizes protocols such as Ethernet or Token Ring.

Key aspects include:

- **Limited Coverage:** LANs cover a small geographic area, typically a single building or campus.
- **Resource Sharing:** Devices can easily share resources like files, printers, and internet connections.
- **High Data Transfer Speeds:** LANs offer fast data transfer rates.
- **Security:** As private networks, LANs offer better control over access.

Advantages and disadvantages of LANs include:

- **Advantages:**
 - **Resource Sharing:** Efficient sharing of expensive peripherals like printers and servers.
 - **Cost-Effective:** Sharing resources reduces the need for individual devices for each user.
 - **High Speed:** Provides fast communication between connected devices.
- **Disadvantages:**
 - **Setup Cost:** Initial setup can be expensive.
 - **Management:** Requires administration and maintenance.
 - **Security Risks:** While generally secure, improper configuration can lead to vulnerabilities.

• **ALOHA**

- A random access protocol where devices can transmit data whenever they have packets, without waiting for permission or coordination. If a collision occurs (two devices transmit simultaneously), both devices detect it by not receiving acknowledgment and retransmit after a random delay. It's simple but inefficient with only ~18% channel utilization due to frequent collisions.

• **TOKEN**

- A special data frame that circulates around a network, controlling which device has permission to transmit. Only the device possessing the token can send data; after transmission, it passes the token to the next device in sequence. This ensures collision-free, orderly access but requires more complex implementation than ALOHA.

6 Explain circuit switching and differentiate with packet switching.

Packet Switching

Packet switching divides data into small units called packets and sends them independently through the network. Each packet contains addressing information and can take different routes to reach the destination, where they're reassembled in order.

How it works:

- Data is segmented into packets before transmission
- Each packet is independently routed through the network
- Packets may travel different paths based on network conditions
- Packets are reassembled at the destination in the correct sequence
- Network resources are shared dynamically among multiple users
- No setup phase required before transmission

Examples: The Internet, email, web browsing, file transfer, modern data networks (TCP/IP)

Advantages:

- Efficient use of bandwidth—resources used only when packets are sent
- No connection setup delay—immediate transmission
- Excellent scalability—supports millions of simultaneous users
- Robust—if one path fails, packets can reroute
- Cost-effective for bursty traffic patterns

Disadvantages:

- Variable delays and unpredictable delivery times
- Packets may arrive out of order or be lost
- Overhead from packet headers containing address information
- No guaranteed quality of service

• Circuit Switching vs Packet Switching - Comparison Table

Circuit Switching	Packet Switching
Requires connection establishment before data transmission	No setup phase required; immediate transmission
Resources reserved exclusively for the connection	Resources allocated dynamically as needed
Single fixed path for entire communication	Each packet may take different routes
Dedicated bandwidth reserved; wasteful if idle	Shared bandwidth; efficient utilization
Consistent and predictable delay	Variable and unpredictable delay
Guaranteed QoS once connected	Best-effort delivery; no guarantees
Higher (resources reserved continuously)	Lower (pay per packet used)
Poor; limited concurrent users	Excellent; supports millions of users
Cannot reroute; must re-establish connection	Automatic rerouting around failures
N/A (continuous stream)	Packets may arrive out of order; reassembled at destination

7. Explain the necessity of IPV6. Differentiate between static routing and dynamic routing.

Necessity of IPv6

For decades, we relied on **IPv4** (Internet Protocol version 4). You've likely seen these addresses before: they look like 192.168.1.1. However, IPv4 uses a 32-bit addressing scheme, which limits the total number of possible addresses to about **4.3 billion**.

In 2026, with the explosion of IoT (Internet of Things) and mobile devices, 4.3 billion addresses are nowhere near enough. Here is why **IPv6** is necessary:

- **Address Scarcity:** IPv6 uses 128-bit addresses (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). This provides $3.4 * 10^{38}$ addresses—essentially an infinite supply for the foreseeable future.
- **Built-in Security:** IPv6 was designed with IPsec (Internet Protocol Security) in mind, making end-to-end encryption and authentication more standardized.
- **Better Efficiency:** It simplifies the packet header, which allows routers to process data faster and improves "Quality of Service" (QoS) for things like lag-free gaming and clear video calls.
- **No More NAT:** Because addresses are so abundant, we no longer need Network Address Translation (NAT), which was a "hack" used in IPv4 to allow multiple devices to share one public IP.

Static Routing	Dynamic Routing
Manually configured by a network administrator.	Automatically configured using routing protocols.
Cannot adapt to network changes or link failures.	Automatically reroutes data if a path goes down.
No complex algorithms; uses simple direct entries.	Uses complex algorithms (like Dijkstra or Bellman-Ford).
Very low; requires no CPU or RAM for pathfinding.	Higher; requires CPU, RAM, and bandwidth to talk to other routers.
Not scalable; becomes unmanageable in large networks.	Highly scalable; ideal for large, growing networks like the Internet.
High; only an admin can change the route.	Slightly lower; routing updates could potentially be spoofed.
Small, simple networks with only one or two routers.	Large, complex networks with multiple redundant paths.
Admin must know the entire network topology.	Routers discover the topology automatically from neighbors.

8. What is flow control? Explain the different types of IP address classes.

Flow control is a mechanism that manages the transmission rate of data between two devices to prevent the sender from overwhelming the receiver. It ensures that data is sent at a pace the receiver can handle, preventing packet loss, buffer overflow, and network congestion.

Explain the different types of IP address classes

IP Address Classes

IP addresses are 32-bit addresses in IPv4, divided into four octets (each 8 bits). Addresses are classified into five classes (A through E) based on the first few bits.

Class A Addresses

Range: 1.0.0.0 to 126.255.255.255

First octet: 1-126

Default subnet mask: 255.0.0.0 (/8)

Structure:

- First bit: 0
- First octet identifies network
- Remaining three octets identify hosts

Number of networks: 126 ($2^7 - 2$)

Hosts per network: 16,777,214 ($2^{24} - 2$)

Characteristics:

- Designed for very large networks
- Used by large organizations and governments
- Each Class A address can support millions of hosts
- Examples: IBM, Apple, GE, AT&T

Private range: 10.0.0.0 to 10.255.255.255

Class B Addresses

Range: 128.0.0.0 to 191.255.255.255

First octet: 128-191

Default subnet mask: 255.255.0.0 (/16)

Structure:

- First two bits: 10
- First two octets identify network
- Last two octets identify hosts

Number of networks: 16,384 (2^{14})

Hosts per network: 65,534 ($2^{16} - 2$)

Characteristics:

- Designed for medium-sized networks
- Suitable for organizations with thousands of hosts
- Balance between network and host addresses
- Commonly used by universities, large companies, and ISPs

Private range: 172.16.0.0 to 172.31.255.255

Class C Addresses

Range: 192.0.0.0 to 223.255.255.255

First octet: 192-223

Default subnet mask: *255.255.255.0 (/24)*

Structure:

- First three bits: 110
- First three octets identify network
- Last octet identifies hosts

Number of networks: *2,097,152 (2^{21})*

Hosts per network: *254 ($2^8 - 2$)*

Characteristics:

- Designed for small networks
- Most commonly deployed class
- Limited hosts per network
- Used by small businesses, schools, and home networks

Private range: *192.168.0.0 to 192.168.255.255*

Class D Addresses

Range: *224.0.0.0 to 239.255.255.255*

First octet: *224-239*

Purpose: Multicast addresses

Characteristics:

- Reserved for multicasting (one-to-many communication)
- Not assigned to individual hosts
- Packets sent to Class D address go to all members of the multicast group
- Examples: 224.0.0.1 (all hosts), 224.0.0.5 (OSPF routers)

Class E Addresses

Range: *240.0.0.0 to 255.255.255.255*

First octet: *240-255*

Purpose: Reserved for experimental and future use

Characteristics:

- Never assigned for public use
- Reserved by IANA for research and development
- *255.255.255.255* is the broadcast address

9. What is firewall? Explain active and passive attack in network.'

A firewall is a network security device or software that acts as a barrier between trusted internal networks and untrusted external networks (like the internet). It monitors and controls incoming and outgoing network traffic based on predetermined security rules, allowing legitimate traffic while blocking potentially harmful traffic.

Passive Attacks

Definition

A passive attack is when an attacker eavesdrops on network traffic without modifying, altering, or disrupting it. The attacker gains unauthorized access to information but does not change the data or disrupt network operations.

Characteristics

- **Non-disruptive:** Network continues operating normally
- **Hard to detect:** No obvious signs of attack; normal traffic appears unchanged
- **Information theft:** Attacker gains confidential information
- **No damage:** Original data remains intact
- **Reconnaissance:** Often used to gather information before launching active attack

Types:

1. **Eavesdropping:** Listening to communications
2. **Packet Sniffing:** Capturing network packets
3. **Wiretapping:** Intercepting communication lines
4. **Traffic Analysis:** Observing communication patterns
5. **Shoulder Surfing:** Watching someone's screen

Prevention: Encryption (HTTPS, VPN, SSH)

Active Attacks

Definition.

An active attack is when an attacker modifies, alters, disrupts, or destroys network data or services. The attacker actively participates in the attack by changing information or disrupting normal network operation.

Characteristics

- **Disruptive:** Affects network operation and data integrity
- **Detectable:** Usually leaves traces or causes noticeable impact
- **Data modification:** Original information is changed or corrupted
- **Service disruption:** Network or services become unavailable
- **Malicious intent:** Clear intent to harm or compromise

Types:

1. **Spoofing:** Impersonating legitimate user/system
2. **DoS/DDoS:** Flooding system with traffic to disable services
3. **Man-in-the-Middle:** Intercepting and altering messages between parties
4. **Replay Attack:** Resending captured messages for unauthorized access
5. **Message Modification:** Altering intercepted messages
6. **Brute Force:** Trying numerous passwords/keys
7. **Malware Injection:** Inserting malicious code
8. **Session Hijacking:** Taking over established sessions

Prevention: Firewalls, IDS/IPS, strong authentication, digital signatures, rate limiting, patching.

10. Write short notes on.

a. DHCP (Dynamic Host Configuration Protocol)

1. DHCP is a **network protocol** used to automatically assign **IP addresses** to devices.
2. It eliminates the need to **manually configure IP addresses**.
3. DHCP assigns IP addresses **temporarily** (lease) and can renew or release them.
4. It also provides other network details like **subnet mask, gateway, and DNS servers**.
5. Makes **network management easier** in large networks.
6. Operates using a **client-server model**.
7. Reduces **IP address conflicts**.
8. Widely used in **home networks, offices, and ISPs**.

b. Cryptography

1. Cryptography is the **science of securing data** by converting it into unreadable form.
2. It ensures **confidentiality, integrity, and authenticity** of data.
3. Data is transformed using **encryption algorithms**.
4. The original data can be restored using **decryption**.
5. Two main types: **Symmetric (same key)** and **Asymmetric (public/private key)**.
6. Used in **online banking, emails, and secure communication**.
7. Helps prevent **unauthorized access and hacking**.
8. Modern cryptography uses **complex mathematical algorithms** like AES, RSA.

c. Network Topology

1. Network topology is the **physical or logical layout** of devices in a network.
2. Types: **Bus, Star, Ring, Mesh, Tree, Hybrid**.
3. Defines how devices are **connected and communicate**.
4. Star topology: central device controls all communication.
5. Bus topology: single backbone cable connects all devices.
6. Ring topology: devices connected in a **closed loop**.
7. Mesh topology: every device is **connected to every other device**.
8. Choice depends on **cost, scalability, and fault tolerance**.

d. Subnet Mask and Subnetting

1. Subnet mask separates **network and host portion** of an IP address.
2. Example: $255.255.255.0 \rightarrow$ first 24 bits are network, last 8 bits are host.
3. Subnetting divides a **large network into smaller sub-networks**.
4. Helps in **efficient IP address management**.
5. Reduces **network congestion**.
6. Each subnet has its **own network address and broadcast address**.
7. Common in **corporate networks and ISPs**.
8. Example: $192.168.1.0/24$ can be divided into **4 subnets with /26 mask**.

e. Framing

1. Framing is the process of **dividing data into frames** for transmission in data link layer.
2. Each frame has a **header, data, and trailer**.
3. It helps in **error detection and control**.
4. Methods: **Character count, Flag bytes, Byte stuffing, Bit stuffing**.
5. Frames provide **synchronization between sender and receiver**.
6. Essential for **reliable communication over networks**.
7. Prevents data from being **lost or mixed during transmission**.

