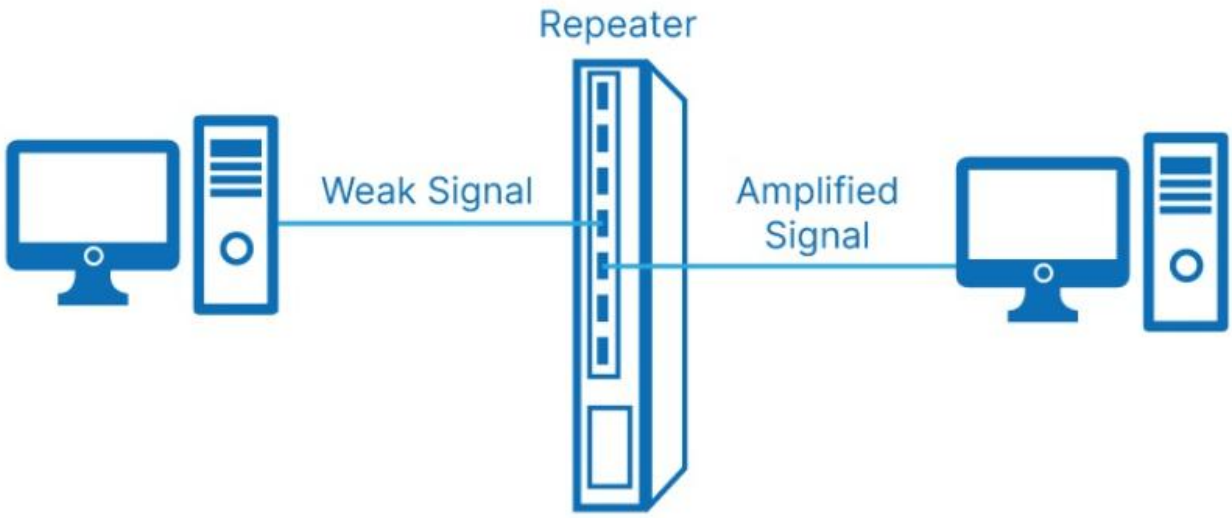
CNND MAY 2024 Answers

Q1

a) Explain Repeater, Hub, Bridge, Switch, and Gateway.

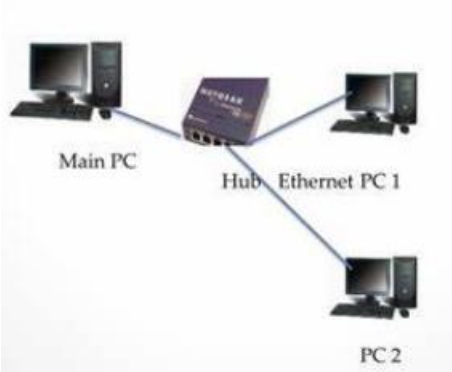
1. Repeater:

- An electrical device that receives, cleans, regenerates, and retransmits signals.
- Helps signals travel longer distances without degradation.
- Required for twisted-pair Ethernet networks with cable lengths over 100 meters.



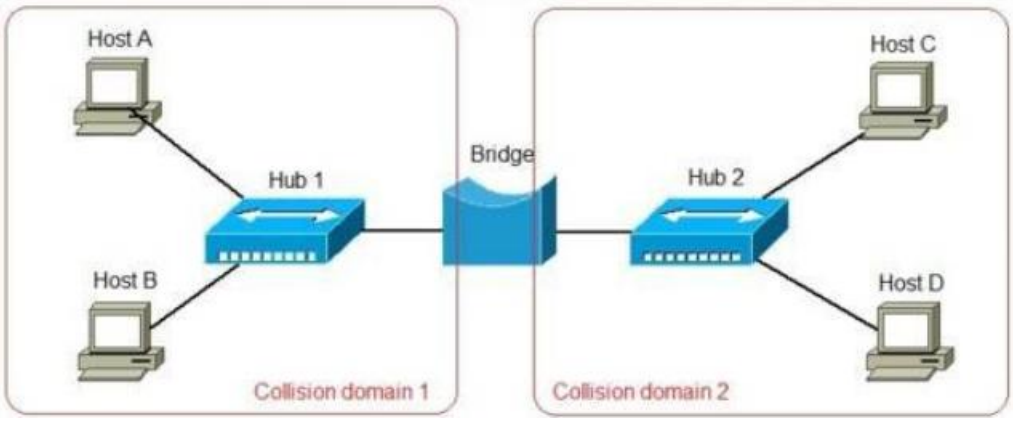
2. Hub:

- Connects multiple Ethernet devices and creates a single network segment.
- Acts as a **multiport repeater**, broadcasting packets to all ports.
- Does not control traffic, leading to packet collisions.



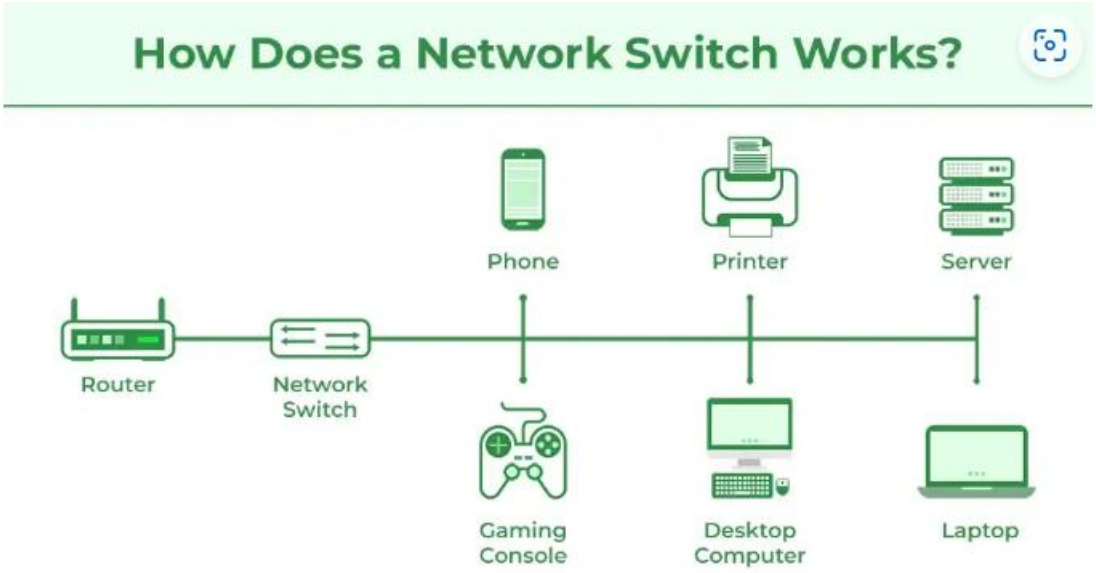
3. Bridge:

- Broadcasts data to all ports except the one that received the transmission.
- Learns which MAC addresses are linked to specific ports.
- Unlike hubs, bridges **only forward traffic to relevant ports**.



4. Switch:

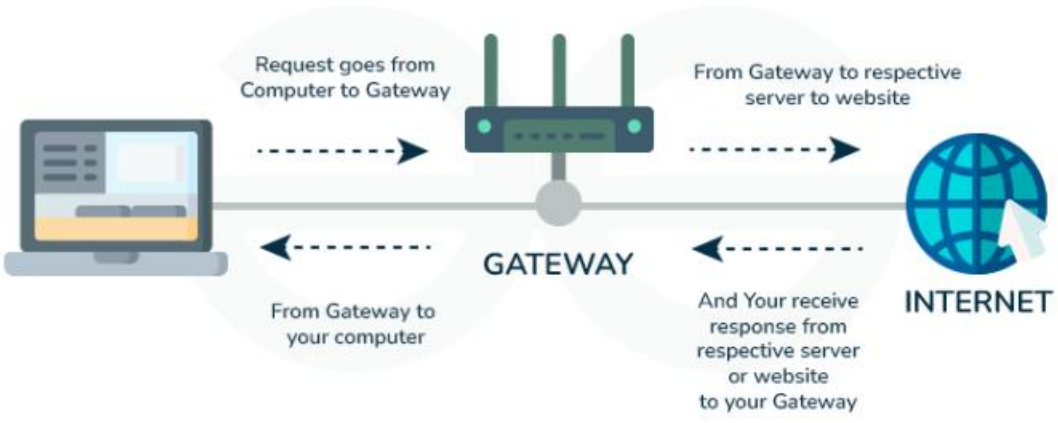
- Forwards frames **only to the intended ports**, reducing collisions.
- Breaks the collision domain but remains part of the broadcast domain.
- Makes forwarding decisions based on MAC addresses.



How Does a Network Switch Works?

5. Gateway:

- Provides system compatibility by using **protocol translators, rate converters, and signal translators**.
- Facilitates communication between networks using different protocols.
- Converts protocols as required to enable interoperability.



b) Explain Token passing controlled access protocol.

Definition:
Token passing is a controlled access protocol used in computer networks to avoid data collisions. It ensures that only one device can transmit data at a time on the network.

How It Works:

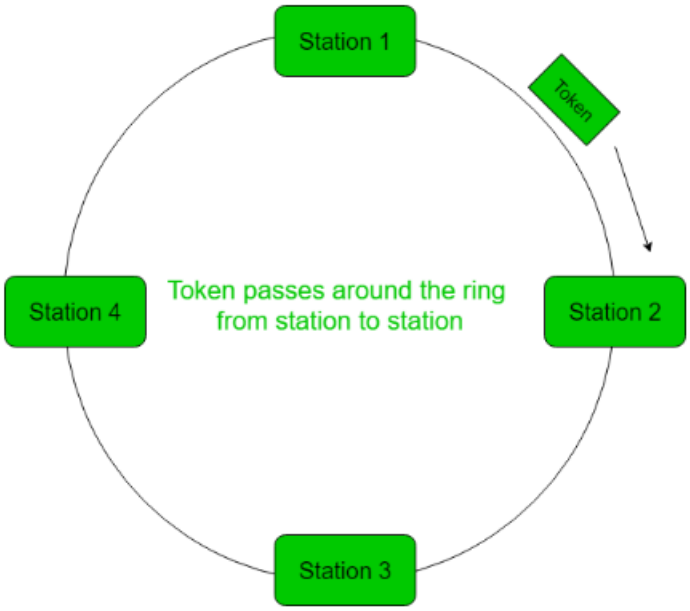
1. A special small data packet called a **"token"** is passed around the network in a logical sequence from one device (node) to another.
2. Only the device that **holds the token** is allowed to send data.
3. After sending the data, the device **releases the token**, which is then passed to the next device in line.
4. If a device does not have any data to send, it simply **passes the token** to the next device.

Key Features:

- **Collision-free:** Since only one token exists, no two devices can transmit at the same time, avoiding data collisions.
- **Deterministic:** Each device gets a turn, making the system predictable and fair.
- **Efficient under heavy load:** Performs well when many devices need to communicate.

Example:

- **Token Ring Network (IEEE 802.5):** A classic example where token passing is used. Devices are connected in a ring topology, and the token circulates around the ring.



c) Explain in detail Network Address Translation.

Network Address Translation (NAT) is a technique used in computer networks to translate private IP addresses into public IP addresses and vice versa. This allows devices in a private network to access the internet using a single public IP address. It plays a crucial role in conserving IP addresses and enhancing network security.

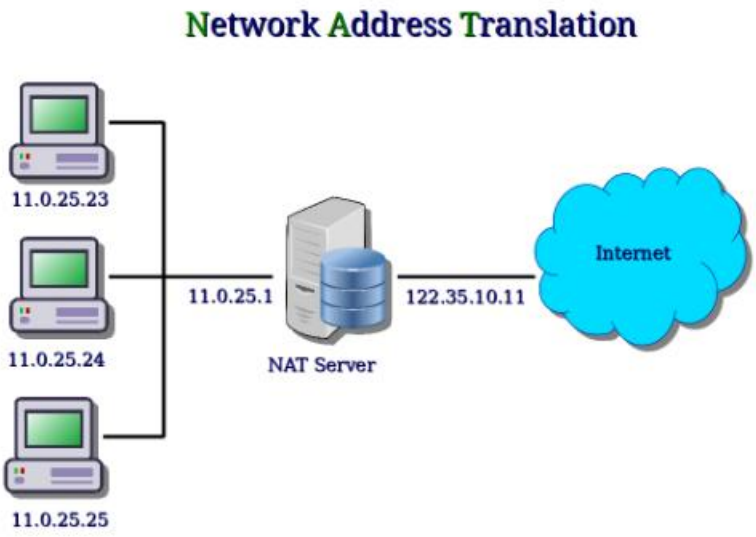
Working of NAT:

1. **Outbound Communication**:
   - When a device in a private network sends a request to the internet, NAT replaces the source private IP address with the router's public IP address.
   - The router keeps a mapping of private IPs and their corresponding port numbers.

2. **Inbound Communication**:
   - The router receives a response from the internet on its public IP address.
   - NAT uses the stored mappings to forward the data to the appropriate private IP address and port.

Advantages of NAT

1. **IP Address Conservation**: NAT reduces the demand for public IP addresses, especially useful with the limited IPv4 address space.
2. **Security**: NAT hides the internal network structure, making it harder for external entities to identify private devices.



Disadvantages of NAT

1. **Compatibility Issues**: Certain applications, such as online gaming or VoIP, may face challenges due to NAT.
2. **End-to-End Connectivity**: NAT breaks the direct connection between devices, which can complicate certain protocols.

Real-World Applications

- **Corporate Networks**: Businesses use NAT to provide internet access while securing internal systems.
- **Data Centers**: NAT is used to route traffic efficiently between internal and external servers.

d) Compare connection oriented and connectionless lossy protocols.

Feature	Connection-Oriented Protocol	Connectionless Lossy Protocol
Connection Setup	Requires connection to be established before data transfer	No connection setup required
Reliability	More reliable (uses acknowledgments, retransmissions)	Less reliable (packets may be lost, no guarantee)
Data Delivery Order	Ensures data is delivered in correct order	Data may arrive out of order or not at all
Overhead	Higher (due to connection setup, error checking, etc.)	Lower (no setup or tracking of data)
Example Protocol	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Use Case	File transfer, emails, web browsing	Video streaming, online gaming, VoIP
Acknowledgments	Yes, uses acknowledgments for received data	No acknowledgments
Error Handling	Built-in error detection and correction	Minimal or no error handling

e) Explain Image compression GIF and JPEG.

Image compression reduces the size of image files, making them more efficient for storage and transmission while maintaining acceptable visual quality. **GIF (Graphics Interchange Format)** and **JPEG (Joint Photographic Experts Group)** are two popular image formats that use different compression methods.

1. GIF (Graphics Interchange Format)

- **Type of Compression**: GIF uses **lossless compression** based on the **Lempel-Ziv-Welch (LZW)** algorithm. This means no data is lost during compression, ensuring that the image remains identical to the original after decompression.

- **Characteristics**:
  - Limited to **256 colors** (8-bit color depth), making it suitable for simple graphics like logos, icons, and animations.
  - Supports **transparency** and **animations** through frames.

- **Applications**:
    - Web graphics like banners, buttons, and memes.
    - Short, looping animations.

1. **JPEG (Joint Photographic Experts Group)**

- **Type of Compression**: JPEG uses **lossy compression**, which reduces file size by permanently discarding less noticeable details. The compression level can be adjusted to balance quality and size.

- **Characteristics**:
    - Supports **16.7 million colors** (24-bit color depth), making it ideal for detailed images like photographs.
    - Does not support transparency or animation.

- **Applications**:
    - Digital photography.
    - Web images requiring small file sizes with acceptable quality.

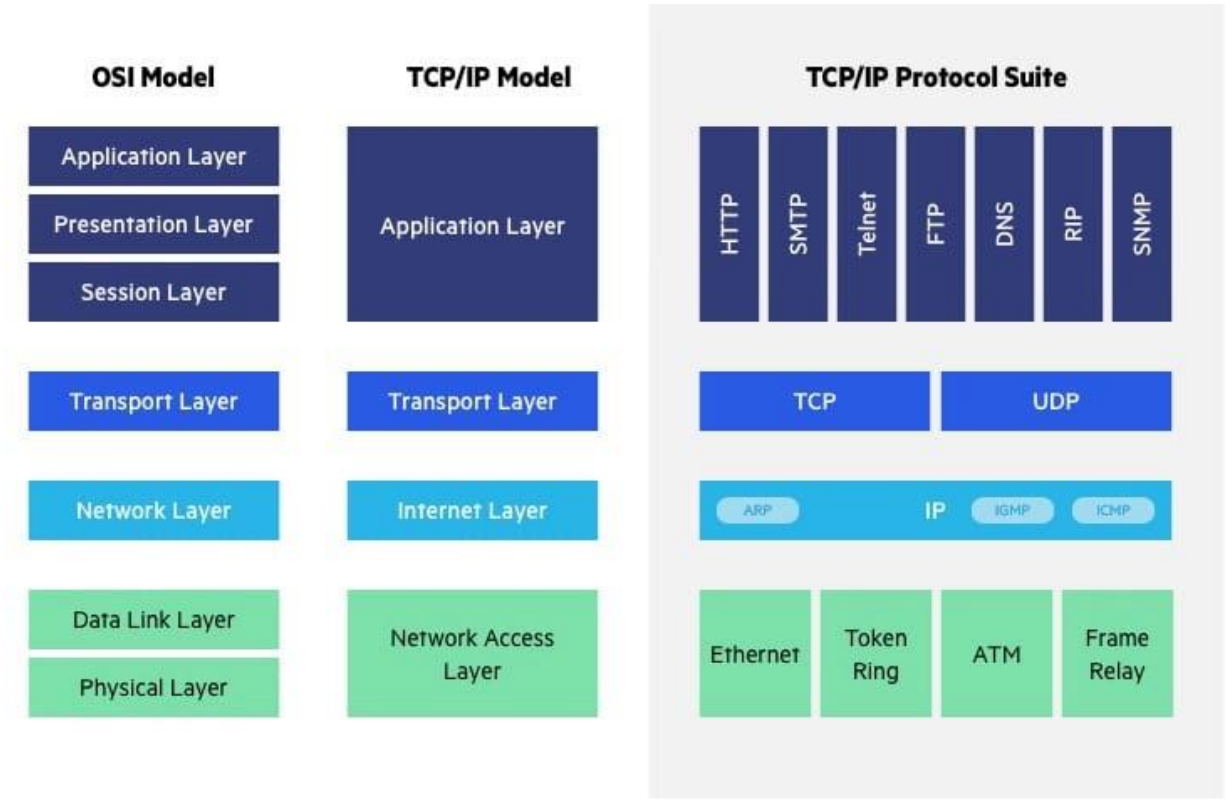
Q2

a) Draw and Explain OSI reference model with neat diagram

OSI Model

The **Open System Interconnection (OSI) Model** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer. It consists of **seven layers**, each performing a specific network function.

The OSI model was developed by the **International Organization for Standardization (ISO)** in 1984 and is now considered an architectural model for inter-computer communications. It divides the entire network communication process into **seven smaller and manageable tasks**, with each layer assigned a particular role. Each layer is **self-contained**, ensuring that tasks can be performed independently.



Layers of the OSI Model

1. Physical Layer

The **Physical Layer** defines the **hardware components** of the network, including cables, switches, and signal transmission methods.

Key Functions:

- **Modulation and bit synchronization**
- **Transmission of raw binary data** over a physical medium

Examples of Technologies:

- **Fiber Optics** - High-speed data transmission
- **Wi-Fi** - Wireless network connectivity

2. Data Link Layer

The **Data Link Layer** ensures **node-to-node data transfer** and handles **error detection and correction**. It manages **MAC (Media Access Control) addresses** and is divided into two sublayers:

1. **Logical Link Control (LLC)** - Error checking and flow control
2. **Media Access Control (MAC)** - Assigns MAC addresses and manages data transmission

Examples of Protocols & Technologies:

- **Ethernet** - Defines LAN data transmission rules
- **PPP (Point-to-Point Protocol)** - Direct connections between network nodes

3. Network Layer

The **Network Layer** is responsible for **data routing, forwarding, and addressing**. It determines the best path for data to reach its destination.

Key Functions:

- **Logical addressing** using IP addresses
- **Packet forwarding and routing**

Examples of Protocols:

- **IP (Internet Protocol)** - Routing and addressing
- **ICMP (Internet Control Message Protocol)** - Diagnostic and error reporting
- **RIP (Routing Information Protocol)** - Manages network data routing

4. Transport Layer

The **Transport Layer** ensures **end-to-end communication** between hosts, providing **error recovery, flow control, and complete data transfer**.

Key Functions:

- **Segmentation and reassembly** of data for efficient transmission
- **Error detection and correction** mechanisms

Examples of Protocols:

- **TCP (Transmission Control Protocol)** - Connection-oriented, reliable transmission
- **UDP (User Datagram Protocol)** - Connectionless, faster but less reliable (used in streaming and gaming)

5. Session Layer

The **Session Layer** manages and controls connections between computers. It establishes, maintains, and terminates sessions for organized and efficient data exchange.

Key Functions:

- Session **establishment, maintenance, and termination**
- **Checkpointing and recovery** to resume sessions after interruptions

Examples of Protocols:

- **Remote Procedure Call (RPC)** - Executes procedures on remote hosts
- **NetBIOS & SQL session protocols** - Manage network communication

6. Presentation Layer

Also known as the **Syntax Layer**, the **Presentation Layer** translates data between the application layer and the network format, ensuring interoperability between different systems.

Key Functions:

- **Data translation** (e.g., ASCII to EBCDIC conversion)
- **Encryption** for data security during transmission
- **Compression** for efficient data transfer

7. Application Layer

The **Application Layer** serves as the interface between end-user applications and network services. It provides protocols and services that allow applications to communicate across the network.

Key Functions:

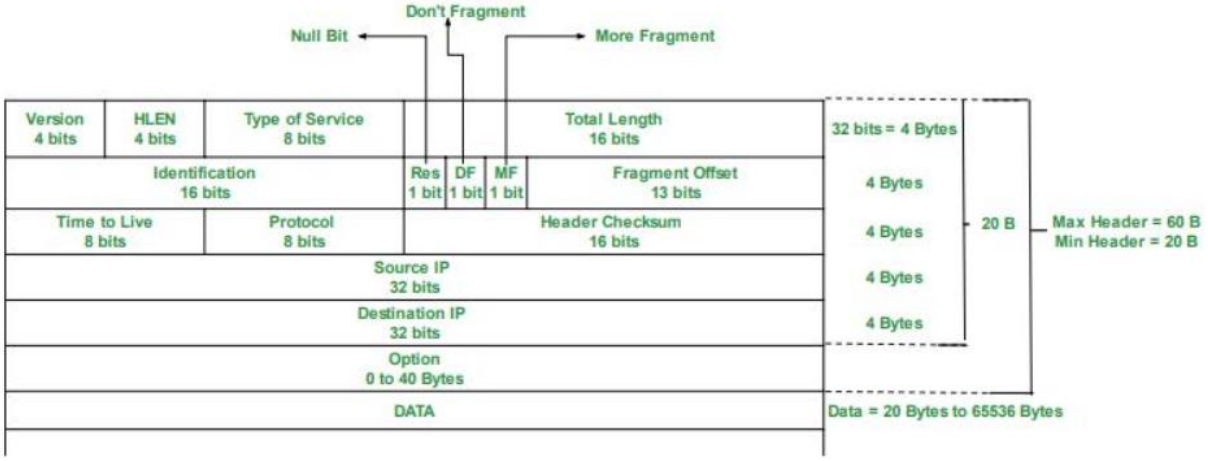
- Resource sharing and remote file access
- Network management and communication services

Examples of Protocols:

- **HTTP** (Hypertext Transfer Protocol) - Web browsing
- **FTP** (File Transfer Protocol) - File transfers
- **SMTP** (Simple Mail Transfer Protocol) - Email services
- **DNS** (Domain Name System) - Resolving domain names to IP addresses.

b) Explain IPV4 Headers format with diagram

The **IPv4 Header** is a crucial part of the IPv4 protocol, providing necessary information for the transmission of packets across networks. It is 20 to 60 bytes long (depending on options) and is structured into several fields.



IPv4 Datagram Header

Explanation of IPv4 Header Fields:

1. **Version (4 bits):** Indicates the IP version. For IPv4, this value is **4**.

2. **IHL (Internet Header Length) (4 bits):** Specifies the **length of the header** in 32-bit words. Minimum value is 5 (i.e., 20 bytes).

3. **Type of Service (ToS) (8 bits):** Used to specify **priority and quality** of the packet.

4. **Total Length (16 bits):** Specifies the **total size** of the packet (header + data) in bytes. Maximum value: **65,535 bytes**.

5. **Identification (16 bits):** Used to **identify fragments** of a single IP datagram.

6. **Flags (3 bits):**
   Control flags:
   - Bit 0: Reserved
   - Bit 1: Don't Fragment (DF)
   - Bit 2: More Fragments (MF)

7. **Fragment Offset (13 bits):** Indicates the **position** of a fragment in the original packet.

8. **Time to Live (TTL) (8 bits):** Limits the **lifetime** of the packet in the network. Prevents looping.

9. **Protocol (8 bits):** Specifies the **higher-layer protocol** (e.g., 6 for TCP, 17 for UDP).

10. **Header Checksum (16 bits):** Used for **error-checking** of the header.

11. **Source IP Address (32 bits):** IP address of the **sender**.

12. **Destination IP Address (32 bits):** IP address of the **receiver**.

Q3

a) Explain CSMA protocols. Explain how collisions are handled in CSMA / CD

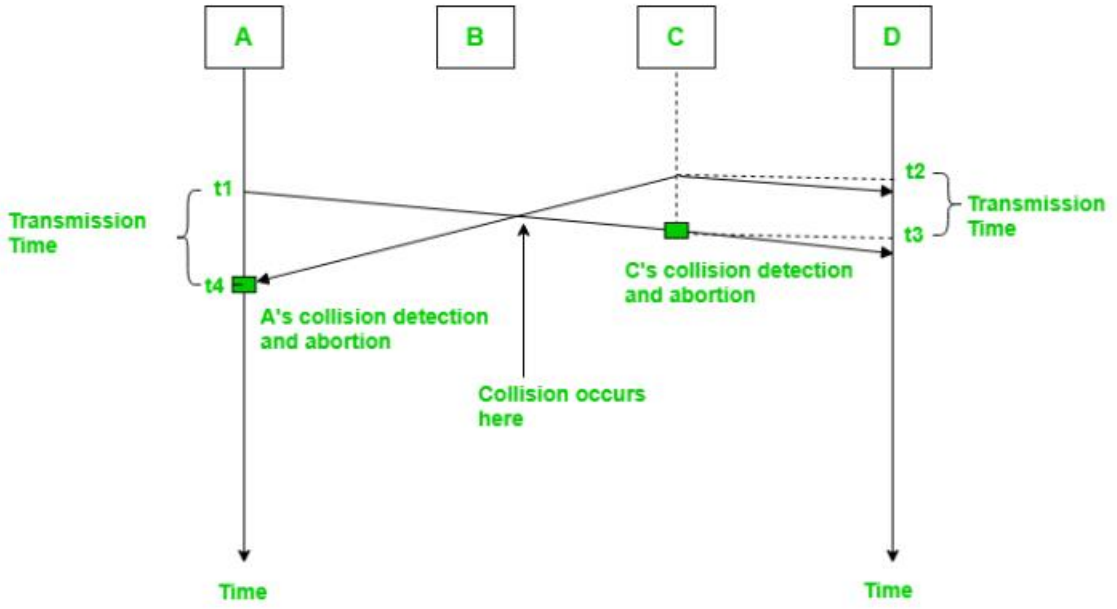
Definition:
CSMA (Carrier Sense Multiple Access) is a network protocol used to control access to a shared communication channel. Before sending data, a device **"listens"** to the channel to check if it is free or busy.

Types of CSMA Protocols:

1. **Persistent CSMA**
2. **Non-persistent CSMA**
3. **P-persistent CSMA (used in slotted channels)**

CSMA/CD – Collision Detection

CSMA/CD stands for **Carrier Sense Multiple Access with Collision Detection**. It is an extension of CSMA used to detect and handle **collisions** during data transmission.



Collision Handling in CSMA/CD:

1. **Sense the Channel**:
   Device checks if the channel is idle before sending.
2. **Start Transmission**:
   If the channel is free, it starts transmitting data.
3. **Collision Detection**:
   While transmitting, the device keeps checking the channel to detect any interference or collision.
4. **Jam Signal**:
   If a collision is detected, a **jam signal** is sent to notify all devices about the collision.
5. **Backoff Algorithm**:
   After sending the jam signal, devices stop transmitting and wait for a **random time** before trying again (called **exponential backoff**).

Used In:

- **Ethernet (Wired LAN)** uses CSMA/CD.

Q4

a) Explain following transmission media - Twisted pair, Coaxial Cable, Fiber Optic.

1. Twisted Pair Cable

Twisted pair cable consists of two insulated copper wires twisted around each other. The twisting helps reduce electromagnetic interference and crosstalk.

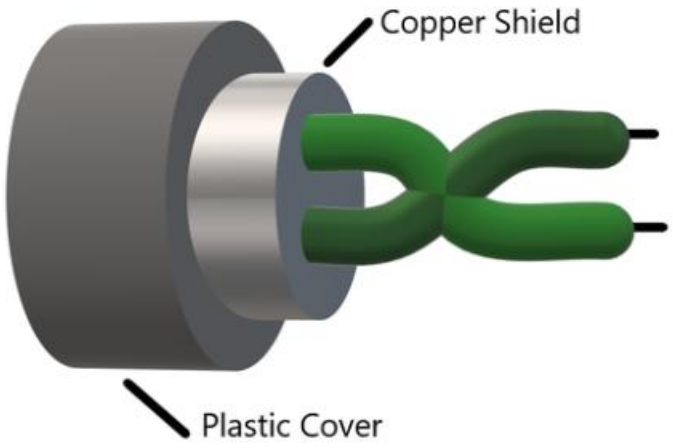
Types of Twisted Pair Cable

a) Unshielded Twisted Pair (UTP)

- Most commonly used in LANs (Ethernet networks).
- Lacks additional shielding, making it more susceptible to interference.
- Cheaper and easier to install.
- Used in telephone networks, computer networks, and DSL connections.

b) Shielded Twisted Pair (STP)

- Has additional shielding (metallic foil or braiding) to reduce interference.
- More expensive than UTP.
- Used in industrial environments with high interference.



Advantages of Twisted Pair

✅ Low cost and easy to install.
✅ Effective for short-distance communication (up to 100m for Ethernet).

Disadvantages of Twisted Pair

❌ Susceptible to electromagnetic interference.

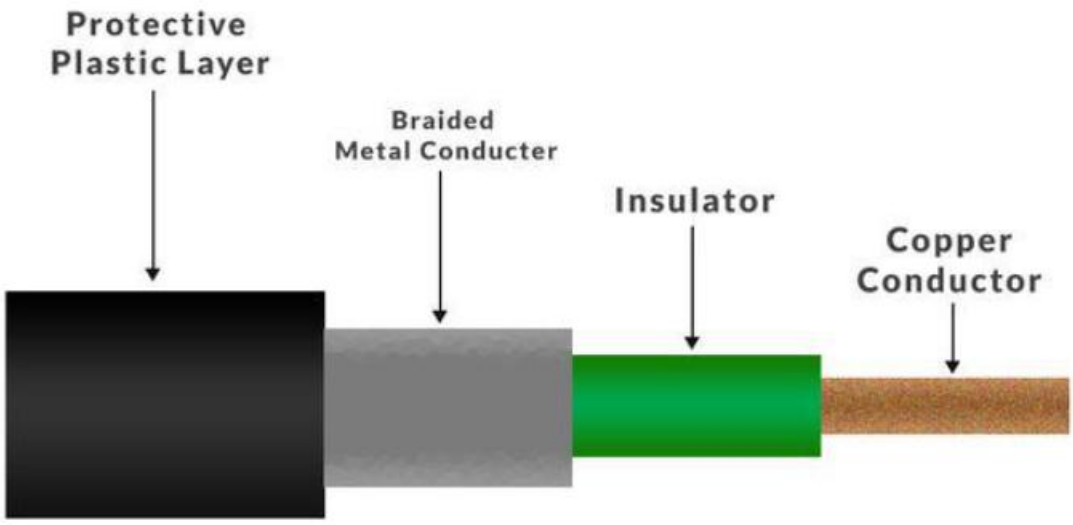
❌ Signal degradation over long distances.

2. Coaxial Cable

Coaxial cable consists of a central copper conductor surrounded by an insulating layer, metallic shield, and an outer protective cover. It is commonly used for cable television and broadband internet.

Types of Coaxial Cable

1. **RG-6**: Used for cable TV and internet.
2. **RG-59**: Used for CCTV and analog video transmission.
3. **RG-11**: Used for long-distance connections.



Coaxial cable

Advantages of Coaxial Cable

✅ Higher bandwidth than twisted pair (up to 10Gbps).

✅ Better resistance to interference.

Disadvantages of Coaxial Cable

❌ More expensive and bulkier than twisted pair.

❌ Difficult to install and maintain.

3. Fiber Optic Cable

Fiber optic cables use light signals to transmit data, making them the fastest and most reliable transmission medium. They consist of a glass or plastic core surrounded by cladding and protective layers.

Types of Fiber Optic Cable

a) Single-Mode Fiber (SMF)

- Uses a single light path.
- Supports long-distance communication (up to 100 km).
- Used in telecom and high-speed internet backbone networks.

b) Multi-Mode Fiber (MMF)

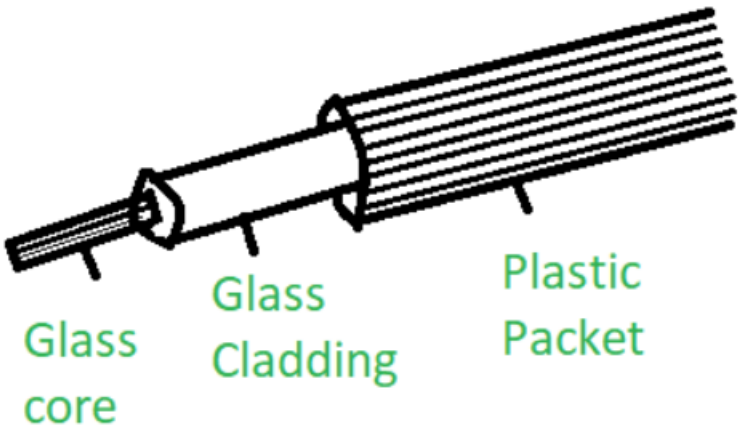
- Uses multiple light paths.
- Suitable for short distances (up to 2 km).
- Used in LANs, data centers, and short-haul communication.

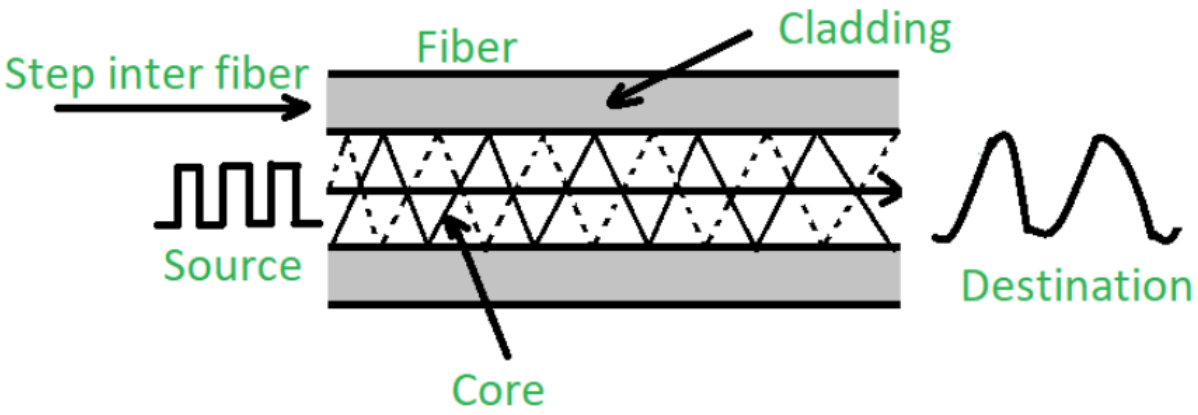
Advantages of Fiber Optic Cable

✅ Extremely high bandwidth (up to several Tbps).
✅ Immune to electromagnetic interference.
✅ Supports very long distances without significant signal loss.

Disadvantages of Fiber Optic Cable

❌ Expensive installation and maintenance.
❌ Difficult to repair.





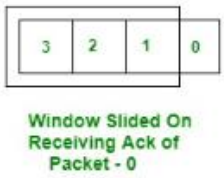
b) Explain concept of sliding protocol? Compare the performance of Go-back-N and Selective Repeat protocol.

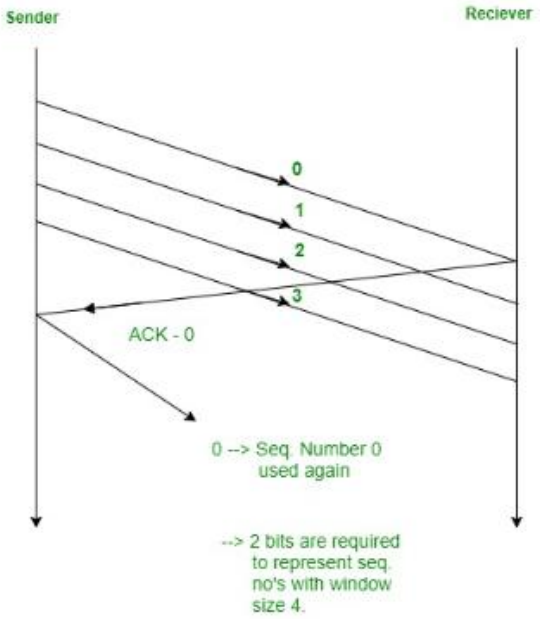
Sliding Window Protocol

The **Sliding Window Protocol** is a flow control mechanism used in data transmission to efficiently manage the sending and receiving of packets between two devices. It ensures reliable and orderly data transfer, especially in networks where packets can be lost or delayed.

Key Features:

- Allows multiple packets to be sent before requiring an acknowledgment.
- Uses a "window" (a range of sequence numbers) to control the number of outstanding (unacknowledged) frames.
- Two types of windows: **Sender Window** (controls how many frames can be sent) and **Receiver Window** (controls how many frames can be received).





Comparison of Go-Back-N and Selective Repeat Protocols

Feature	Go-Back-N (GBN)	Selective Repeat (SR)
Window Size	Sender: **N**	Sender: **N**, Receiver: **N**
Acknowledgment	Cumulative ACK (acknowledges all previous frames)	Individual ACK for each frame
Retransmission	If an error occurs, retransmit all frames from the error onwards	Only the erroneous/lost frames are retransmitted
Buffering	Receiver only buffers frames in order	Receiver buffers out-of-order frames
Efficiency	Less efficient (more retransmissions)	More efficient (fewer retransmissions)
Complexity	Simple to implement	More complex (requires more memory and processing)
Bandwidth Utilization	Lower (due to unnecessary retransmissions)	Higher (less redundancy)
Best Used When	Low error rate networks	High error rate networks

Q5

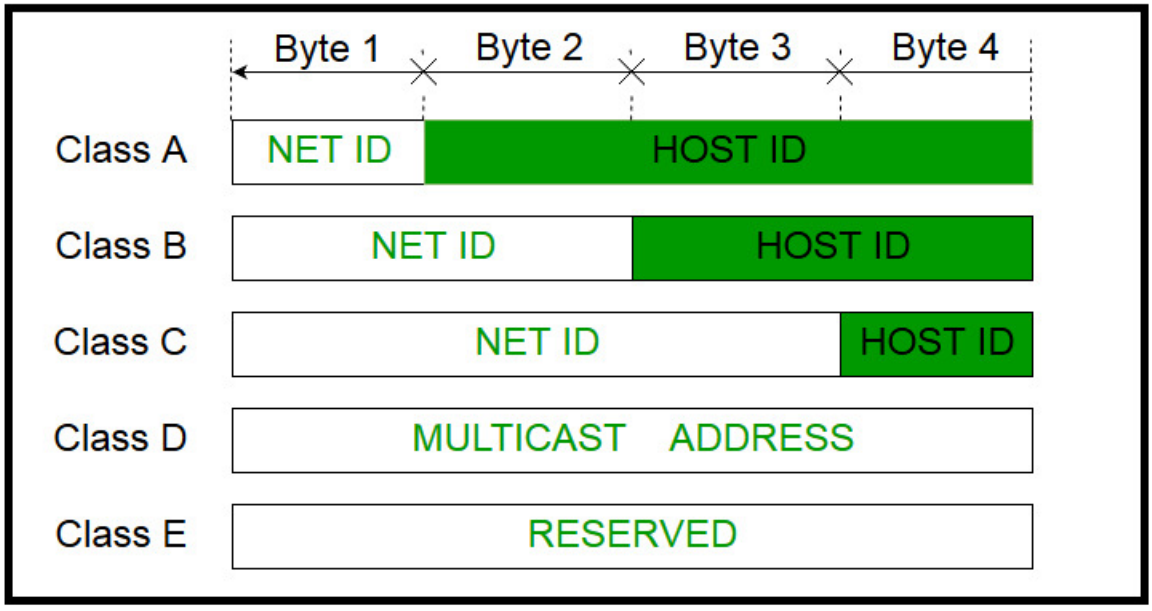
a) What is IP addressing? Explain in detail Classful and Classless IP addresses.

IP (Internet Protocol) addressing is a method used to uniquely identify devices on a network and enable communication between them. An IP address is a **32-bit** (IPv4) or **128-bit** (IPv6) number assigned to each device on a network.

It consists of two parts:
1. **Network ID** – Identifies the network.
2. **Host ID** – Identifies a specific device (host) in that network.

Example of an IPv4 address: 192.168.1.1

Classful IP Address



Classful Addressing

Key Characteristics of Classful Addressing

✅ Simple to understand and implement.
✅ Fixed division between network and host portions.

❌ **Wastage of IP addresses** (e.g., Class A assigns millions of addresses even if only a few are needed).
❌ **Does not support subnetting or efficient IP allocation.**

Structure of Classful Addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

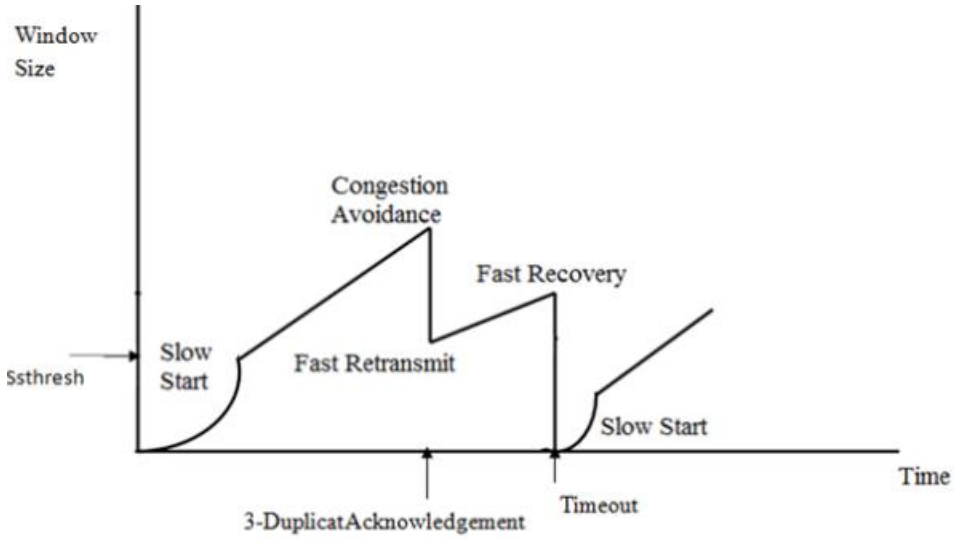
Classless IP Addressing (CIDR - Classless Inter-Domain Routing)
To overcome the limitations of classful addressing, **Classless Inter-Domain Routing (CIDR)** was introduced.

Key Features of CIDR
✅ **No fixed class boundaries** – The network can be of any size.
✅ Uses a **subnet mask** (e.g., /24 instead of 255.255.255.0).
✅ Allows **efficient allocation** of IP addresses.
✅ Reduces **IP wastage** and enables **subnetting and supernetting**.

CIDR Notation
- CIDR uses **variable-length subnet masking (VLSM)** to allocate IPs efficiently.
- Example: 192.168.1.0/26
    - /26 means the first **26 bits** are for the **network**, and the remaining **6 bits** are for hosts.
    - This allows 2^6 - 2 = 62 hosts (subtracting 2 for network and broadcast addresses).

b) Explain in detail TCP congestion control mechanism

Transmission Control Protocol (TCP) is a reliable transport layer protocol that ensures data is delivered without loss. However, in a network, congestion occurs when too many data packets compete for the same resources, causing delays or packet drops. To address this, TCP employs congestion control mechanisms to regulate the flow of data and prevent network congestion.



Phases of TCP Congestion Control

1. **Slow Start**:
   - TCP starts with a small **Congestion Window (CWND)**, typically set to one Maximum Segment Size (MSS).
   - For each acknowledgment (ACK) received, the CWND size doubles (exponential growth) until it reaches a threshold known as the **Slow Start Threshold (SSTHRESH)** or network congestion occurs.
   - Purpose: To quickly ramp up the transmission rate to detect the available bandwidth.

2. **Congestion Avoidance**:
   - Once CWND exceeds the SSTHRESH, TCP shifts to a more conservative growth approach.

- CWND increases linearly (one MSS per RTT) to avoid overwhelming the network.
- This phase ensures that the transmission rate grows steadily without causing congestion.

3. **Congestion Detection (Loss Detection)**:
   - TCP detects congestion via packet loss, which is identified in one of two ways:
     - **Timeout**: If an acknowledgment for a packet is not received within the timeout period.
     - **Duplicate ACKs**: If multiple duplicate ACKs are received, it indicates possible packet loss.
   - Upon detecting congestion, TCP reduces the CWND to mitigate network overload.

4. **Fast Recovery**:
   - Instead of reducing CWND drastically after duplicate ACKs, TCP adopts fast recovery to maintain data flow.
   - CWND is halved and grows linearly (congestion avoidance) rather than restarting from one MSS.
   - This phase is designed to recover from minor congestion without triggering slow start.

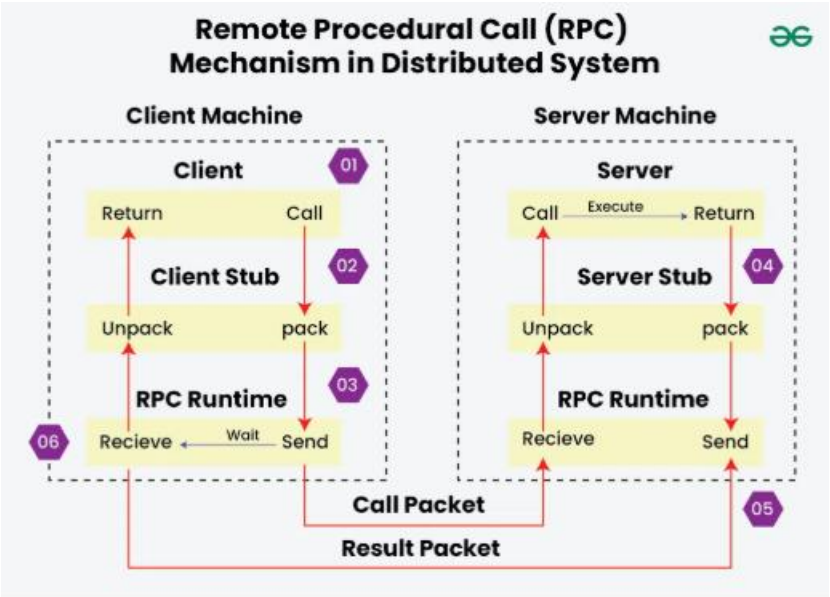
Q.6) Write a short note on:

1. RPC

Remote Procedure Call (RPC) is a powerful mechanism in distributed computing that allows a program to execute a procedure (function) on a remote server as if it were executing locally. This enables seamless communication between different systems in a network.

Key Features of RPC

1. **Transparency**: Abstracts the complexities of network communication, making remote calls appear like local calls.
2. **Interoperability**: Supports communication between applications running on different platforms or programming languages.
3. **Efficiency**: Simplifies distributed system design and allows for modular architectures.



Remote Procedural Call (RPC) Mechanism

How RPC Works

1. The client sends a request to the server specifying the procedure to be executed and its parameters.
2. The server processes the request, executes the procedure, and sends the response back to the client.
3. RPC typically involves stub code to handle communication and data serialization (marshalling) between client and server.

Applications

- Used in distributed systems for inter-process communication.
- Common in network services, such as file sharing and database querying.

2. DNS

The **Domain Name System (DNS)** is a hierarchical and distributed naming system in computer networks that translates human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.0.2.1). This allows users to access websites and services without memorizing numerical IP addresses.

Key Features

1. **Name Resolution**: Converts domain names into IP addresses for network communication.
2. **Distributed Structure**: Operates through a network of servers worldwide, ensuring efficiency and scalability.
3. **Caching**: Stores previously resolved queries to speed up future requests.

How DNS Works

1. The user enters a domain name in the browser.
2. The DNS client sends a request to a DNS server to resolve the name.
3. The server provides the corresponding IP address, allowing the user to access the desired resource.

Applications

- Essential for web browsing, email delivery, and internet services.
- Enables seamless communication between humans and computer networks.

3. VLAN

Definition:

A **VLAN (Virtual Local Area Network)** is a logical grouping of devices within a network, created to segment the network **regardless of physical location**. It allows devices in different physical locations to communicate as if they are on the same LAN.

Key Features:

- **Improves security** by isolating traffic between groups.
- **Reduces broadcast traffic** and improves performance.

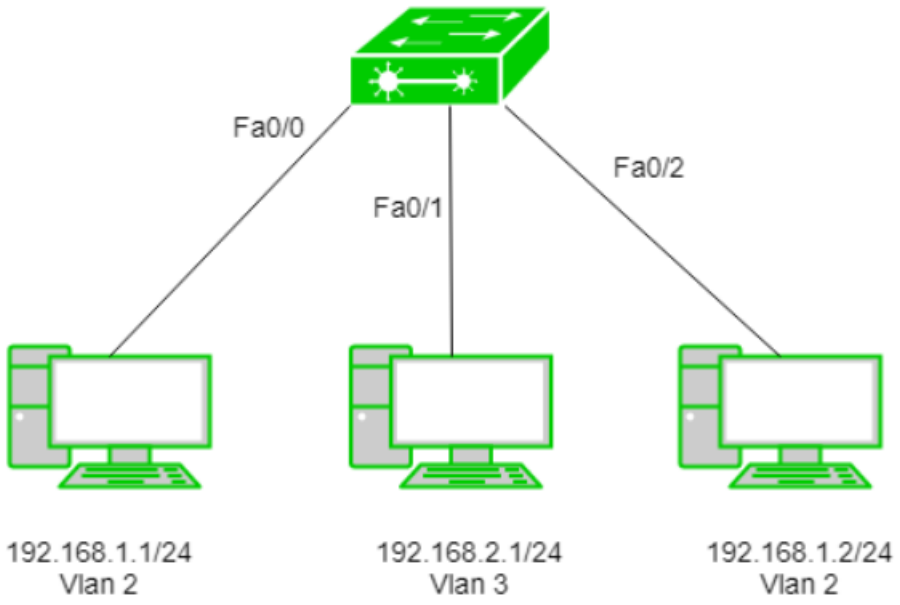
- **Flexible**: Devices can be moved to different VLANs without changing physical connections.

How it works:

- VLANs are configured on **network switches**.
- Each port on a switch can be assigned to a specific VLAN.
- VLAN tags (as per **IEEE 802.1Q** standard) are added to Ethernet frames to identify VLAN membership.

Example Use Case:

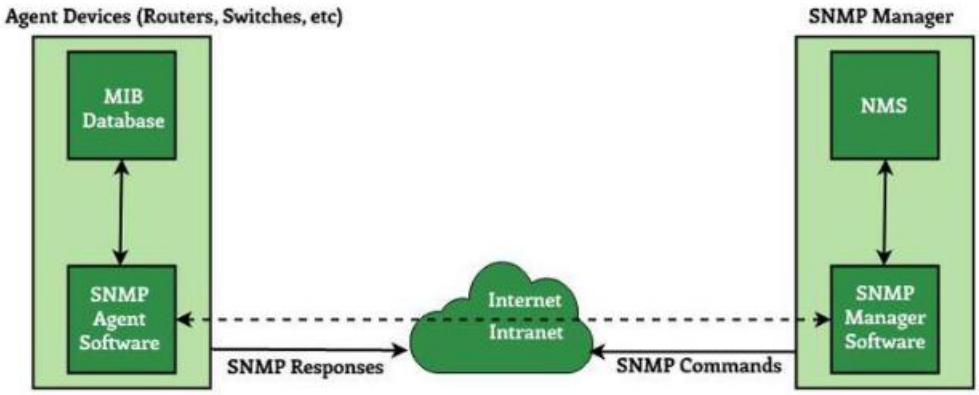
- Separating departments like **HR**, **Finance**, and **IT** into different VLANs even if they are on the same physical switch.



4. SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol designed for managing and monitoring network devices such as routers, switches, servers, and printers. It is widely used in network management systems to track the performance, detect faults, and configure devices within a network.

SNMP Architecture



Key Features

1. **Lightweight Protocol**:
   - Operates over UDP (port 161 for requests and port 162 for traps), ensuring minimal overhead.

2. **Device Management**:
   - Collects data on device performance, status, and configuration.

3. **Real-time Alerts**:
   - Supports "traps" that notify administrators about specific events or issues.

How SNMP Works

1. A **Manager** (central system) communicates with **Agents** (devices being monitored).
2. The Manager retrieves or sets device data using SNMP commands.
3. The Agent stores this data in a Management Information Base (MIB), a standardized database structure.

Applications

- Troubleshooting network issues.
- Automating configuration updates for devices.

5. OSPF

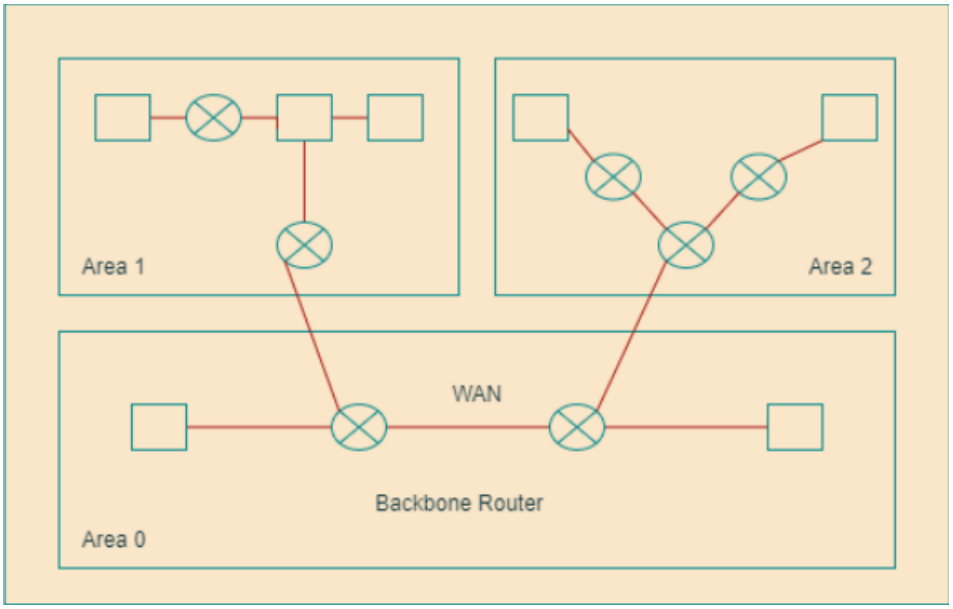
Open Shortest Path First (OSPF) is a link-state routing protocol used to determine the best path for data packets within a network. It operates within an Autonomous System (AS), typically in large enterprise networks, and ensures efficient and dynamic routing.

Key Features

1. **Dynamic Routing**:
    - OSPF adapts to changes in network topology by recalculating paths in real time.

2. **Link-State Advertisements (LSAs)**:
    - Routers share information about their connections and status, enabling a global view of the network.

3. **Shortest Path Calculation**:
    - OSPF uses Dijkstra's algorithm to compute the optimal route for data packets.



Applications

- Used in enterprise and large-scale networks for dynamic and efficient routing.
- Commonly employed in LAN and WAN environments.