Module 7 Network fundamentals

• Advance Question

1. Explain Network Topologies.

ANS: Network topologies refer to the physical or logical layout of a computer network, defining how different nodes or devices are connected and how data is transmitted between them.

Bus Topology: All devices share a single communication line or bus.

Star Topology: Devices are connected to a central hub or switch.

Ring Topology: Devices are connected in a circular fashion, forming a closed loop.

Mesh Topology: Every device is connected to every other device, providing multiple paths for data transmission.

Tree Topology: A hierarchical structure where devices are connected in a tree-like fashion, often with a main central node.

Hybrid Topology: A combination of two or more different topologies to meet specific network requirements.

2. Explain TCP/IP Networking Model

ANS: The TCP/IP (Transmission Control Protocol/Internet Protocol) networking model is a conceptual framework that standardizes the communication protocols used on the Internet. It four layers

Application Layer: Handles high-level communication and network services, such as HTTP for web browsing, SMTP for email, and FTP for file transfer.

Transport Layer: Responsible for end-to-end communication, ensuring reliable and error-checked data delivery. TCP (Transmission Control Protocol) operates at this layer, providing connection-oriented and reliable communication.

Internet Layer: Manages addressing and routing of data packets across the network. The Internet Protocol (IP) is a key protocol in this layer, allowing devices to locate and communicate with each other.

Link Layer: Deals with the physical connection between devices on the same local network. It includes protocols for data framing, error detection, and handling communication within a local network.

3. Explain LAN and WAN Network

ANS: **LAN (Local Area Network):**

A LAN is a network that is limited to a small geographic area, such as a single building, campus, or office. It allows connected devices, such as computers and printers, to share resources and communicate with each other at high speeds. LANs typically use Ethernet cables or Wi-Fi for connectivity.

WAN (Wide Area Network):
A WAN spans a larger geographic area and connects multiple LANs or other networks over long distances, often using public or private communication links, such as leased lines or the internet. WANs enable the interconnection of geographically dispersed networks, facilitating data exchange between different locations. Examples include global corporate networks and the internet itself.

4. Explain Operation of Switch

ANS: A switch operates at the data link layer of the OSI model and is designed to forward and filter data within a local area network .

It functions:

MAC Address Learning: Switches learn the MAC (Media Access Control) addresses of devices connected to their ports by observing the source addresses of incoming frames. This information is stored in a MAC address table.

Filtering and Forwarding: Based on the MAC address table, the switch makes informed decisions about where to forward data. If the destination MAC address is known, the switch forwards the data only to the specific port where the destination device is located, reducing unnecessary network traffic.

Broadcast and Unknown Unicast Handling: Switches forward broadcast frames to all connected devices within a broadcast domain, ensuring that devices receive essential broadcast messages. If the destination MAC address is unknown, the switch sends the frame to all ports except the source port.

Collision Avoidance: Unlike hubs, switches create separate collision domains for each connected device, preventing collisions and enhancing the overall efficiency of the network.

5. Describe the purpose and functions of various network devices.

1. **Router:**

- **Purpose:** Connects different networks and directs data between them.
- **Functions:** Manages IP addresses, makes routing decisions, and provides network layer connectivity.

2. **Switch:**

- **Purpose:** Connects devices within a local network, facilitating efficient data transfer.
- **Functions:** Learns MAC addresses, filters and forwards data based on MAC addresses, creates separate collision domains.

3. **Hub:**

- **Purpose:** Connects multiple devices in a LAN, but operates at the physical layer.
- **Functions:** Broadcasts incoming data to all connected devices, doesn't differentiate between devices.

4. **Firewall:**

- **Purpose:** Protects a network by controlling incoming and outgoing traffic based on predefined security rules.
- **Functions:** Monitors and filters network packets, blocks or allows traffic based on security policies.

5. **Modem:**

- **Purpose:** Converts digital data from a computer into a format suitable for transmission over communication lines (analog signals for traditional phone lines or digital signals for broadband).
- **Functions:** Modulates and demodulates signals for two-way communication over various types of networks.

6. **Access Point (AP):**

- **Purpose:** Connects wireless devices to a wired network using Wi-Fi.
- **Functions:** Transmits and receives wireless signals, bridges the gap between wired and wireless networks.

7. **Gateway:**

- **Purpose:** Connects different types of networks and translates data between them.
- **Functions:** Acts as an interface between networks with different communication protocols or technologies.

6. Make list of the appropriate media, cables, ports, and connectors to connect switches to other

ANS: **Media:**

Ethernet (for wired connections)
Wireless (for Wi-Fi connections)
Cables:

Ethernet cables (e.g., Cat5e, Cat6, Cat6a, or Cat7 for wired connections)
Fiber optic cables (for high-speed and long-distance connections)
Ports on Switches:

RJ45 ports for Ethernet connections
SFP (Small Form-Factor Pluggable) ports for fiber optic connections
Console port for management purposes (often using RS-232 or USB)
Connectors:

RJ45 connectors for Ethernet cables
LC, SC, or ST connectors for fiber optic cables
USB or RS-232 connectors for console connections

7. Define Network devices and hosts8. What are Ethernet Standard (802.3) and Frame Formats?

- **Network Devices:** Hardware or software components that facilitate communication and data exchange within a network. Examples include routers, switches, hubs, access points, and firewalls.
- **Hosts:** Devices on a network that generate or consume data. Examples include computers, printers, and servers. Hosts often have unique IP addresses and can be the source or destination of network traffic.

- **Ethernet Standard (802.3):** A set of standards defining the physical and data link layer specifications for wired Ethernet networks. It specifies aspects like frame format, signaling, and collision detection.

- **Ethernet Frame Format**: The structure of data packets transmitted over Ethernet networks. The typical Ethernet frame consists of:

- **Preamble:** Helps synchronize receiver and sender clocks.
- **Destination and Source MAC Addresses:** Identifies the source and destination devices.
- **Type or Length Field:** Indicates the upper-layer protocol or the length of the data.
- **Data Field:** Carries the actual payload or information.
- **Frame Check Sequence (FCS):** Contains error-checking information.

Ethernet Frame Types:

- **Ethernet II (DIX) Frame:** Commonly used in modern Ethernet networks, it includes a type field to identify the upper-layer protocol.
- **IEEE 802.3 Frame:** Incorporates a length field instead of a type field to specify the frame's size

• Intermediate Question

1. Comparison between UTP, MM and SM Ethernet Cabling

ANS:

Aspect	UTP	MM	SM
Transmission distance	Up to 100 meters	Up to a few hundred meter	Tens of kilometer or more
bandwidth	Varies by category	High	Highest bandwidth
Immunity to interface	Prone to interface	Immune to interface	Highly immune ideal for challenger

Size and weight	Light and flexible	Thick and less	Typically more expensive
Cost Installation and termination	Cost effective Easy ,RJ45 connector	flexible precise termination	Careful termination various connectors

2. Make Cross cable

Cross Cable:

Purpose: Connects similar devices directly without requiring an intermediary device.

Wire Configuration:

Pins 1 and 3 at one end connect to pins 2 and 6 at the other end.

Pins 2 and 6 at one end connect to pins 1 and 3 at the other end.

Uses T568A or T568B standards for both ends, but the wiring is crossed.

Typical Use Cases:

Connecting two computers directly.

Connecting two switches.

3. Make Straight-Through Cable.

ANS: **Straight-Through Cable**:

Purpose: Connects devices of different types, maintaining the same pin configuration at both ends.

Wire Configuration:

Both ends use the same wiring standard, either T568A or T568B.

Pins at one end match corresponding pins at the other end.

Typical Use Cases:

Connecting a computer to a switch.

Connecting a computer to a router.

4. Differentiate between LAN/WAN operation and features

ANS: **LAN (Local Area Network) Operation and Features:**

Operation: Limited to a small geographic area, like a single building or campus.

Features:

- High data transfer rates within the local network.
- Lower latency due to proximity.
- Typically uses Ethernet cables or Wi-Fi for connectivity.
- Managed by a single organization.
- Well-suited for resource-sharing within a localized environment.

WAN (Wide Area Network) Operation and Features:

Operation: Spans a larger geographic area, connecting multiple LANs or networks over long distances.

Features:

- Supports communication between distant locations.
- Involves higher latency due to longer transmission distances.
- Often uses leased lines, satellite links, or the internet for connectivity.
- May involve multiple organizations or service providers.
- Enables data exchange between geographically dispersed networks.

5. Explain ARP, ICMP and Domain name

ANS: **ARP (Address Resolution Protocol):**

Purpose: Maps an IP address to a corresponding MAC address on a local network.
Operation: When a device needs to communicate with another device on the same network, it uses ARP to discover the MAC address associated with the target device's IP address.
Example: Device A wants to send data to Device B. Device A uses ARP to find the MAC address corresponding to Device B's IP address.
ICMP (Internet Control Message Protocol):

Purpose: Handles error messages and communication between network devices.
Operation: Used for diagnostic functions such as ping, traceroute, and error reporting.
Example: Ping uses ICMP Echo Request and Echo Reply messages to test connectivity between devices.
Domain Name:

Purpose: Provides human-readable names for IP addresses.
Operation: Domain names, like www.example.com, are easier to remember than numerical IP addresses. DNS (Domain Name System) translates domain names into IP addresses.
Example: When you type a website URL, DNS resolves it to the corresponding IP address, allowing your device to connect to the correct server.

6. Describe the components required for network and Internet communications

ANS: **Network Devices:**

- Includes routers, switches, hubs, and access points.
- Facilitate communication within local networks.

End Devices:

- Computers, laptops, Smartphone’s, servers, and other devices.
- Generate or consume data in the network.

Network Cabling:

- Ethernet cables for wired connections.
- Fiber optic cables for high-speed and long-distance connections.
- Facilitate the physical transmission of data.

Wireless Connectivity:

- Wi-Fi technology for wireless communication.

- Enables device connection without physical cables.

Protocols:

- TCP/IP (Transmission Control Protocol/Internet Protocol) for standardization.
- Governs how data is transmitted and received in networks.

Internet Service Provider (ISP):

- Provides internet connectivity to homes and businesses.
- Offers access to the global internet infrastructure.

Domain Name System (DNS):

- Translates human-readable domain names to IP addresses.
- Essential for locating resources on the internet.

Firewall:

- Ensures network security by controlling incoming and outgoing traffic.
- Monitors and filters data based on predefined security rules.

Modem:

- Converts digital data from devices into a format suitable for transmission over communication lines.
- Essential for connecting to the internet via broadband or traditional phone lines.

Internet Backbone:

- High-speed, long-distance communication infrastructure.
- Connects ISPs and facilitates global internet connectivity.

7. Explain Encapsulation and DE capsulation in OSI Reference model.

ANS**: Encapsulation in OSI Reference Model:**

- **Definition:** The process of adding protocol-specific headers and trailers to data as it moves down the OSI layers.
- **Purpose:** Each layer adds its own header and potentially a trailer to the data, creating a protocol data unit (PDU) at that layer.
- **Example:** In TCP/IP, at the Transport Layer (Layer 4), data from the Application Layer (Layer 7) gets encapsulated with a TCP header.

De capsulation in OSI Reference Model:

- **Definition:** The process of stripping off the headers and trailers added by each layer as data moves up the OSI layers.
- **Purpose:** Ensures that the data is correctly interpreted and delivered to the appropriate application at the receiving end.

- **Example:** At the receiving end, the Transport Layer encapsulates the received data, removing the TCP header to expose the original data for the Application Layer.

8. Explain network segmentation and basic traffic management concepts.

ANS: **Network Segmentation:**

- **Definition:** Dividing a network into smaller, isolated segments to enhance performance, security, and manageability.
- **Purpose:**
- Reduces broadcast domains, minimizing network traffic.
- Enhances security by isolating different parts of the network.
- Improves performance by reducing collision domains and isolating network issues.

Traffic Shaping:

- Controls the rate of data transmission to manage network congestion.
- Smoothes outburst traffic and ensures a more consistent data flow.

Quality of Service:

- Prioritizes certain types of network traffic over others.
- Ensures that critical applications receive better performance and lower latency.

Management:

- Allocates available bandwidth to different applications or users.
- Prevents one user or application from consuming excessive network resources.

Load Balancing:

- Distributes network traffic across multiple paths or devices.
- Optimizes resource utilization and ensures even distribution of the network load.

Traffic Monitoring:

- Involves the continuous observation of network traffic.
- Helps identify potential issues, bottlenecks, or security threats in real-time.

9. What is flow control and acknowledgment**?**

ANS: **Flow Control:**

- **Definition:** Mechanism to manage the rate of data transmission between sender and receiver to prevent congestion and ensure data integrity.
- **Purpose:** Prevents the sender from overwhelming the receiver with data, ensuring a smooth and controlled flow of information.

Acknowledgment:

- **Definition:** Process where the receiving end informs the sender that it has successfully received a data packet.

- **Purpose:** Provides feedback to the sender about the successful delivery of data, allowing for error detection and retransmission if necessary.

• Advance question

1. Use the OSI and TCP/IP models and their associated protocols to explain how data
Flows in a network.

ANS: **Data Flow in a Network Using OSI Model**:

Application Layer:

- Data originates from an application, which formats it into a specific protocol.
- Examples: HTTP, FTP, SMTP.

Presentation Layer :

- Data undergoes translation, encryption, or compression.
- Examples: SSL/TLS, JPEG, GIF.

Session Layer :

- Establishes, manages, and terminates sessions between applications.
- Examples: NetBIOS, RPC.

Transport Layer :

- Segments data, adds headers for source/destination ports.
- Ensures reliable, ordered delivery.
- Examples: TCP, UDP.

Network Layer :

- Routes packets between devices using logical addresses (IP).
- Examples: IP, ICMP.

Data Link Layer :

- Frames are created with source/destination MAC addresses.
- Manages access to the physical medium.
- Examples: Ethernet, PPP.

Physical Layer :

- Transmits raw bits over the physical medium (cables, wireless).
- Examples: Ethernet cables, optical fibers.

Data Flow in a Network Using TCP/IP Model:

Application Layer:

- Similar to OSI's Application Layer, includes protocols for end-user services.
- Examples: HTTP, FTP, SMTP.

Transport Layer:

- Combines functions of OSI's Transport and Session Layers.
- Segments data, adds headers for source/destination ports.
- Examples: TCP, UDP.

Internet Layer:

- Similar to OSI's Network Layer, responsible for routing.
- Routes packets between devices using IP addresses.
- Examples: IP, ICMP.

Link Layer:

- Combines functions of OSI's Data Link and Physical Layers.
- Frames are created with source/destination MAC addresses.
- Manages access to the physical medium.
- Examples: Ethernet, PPP.

2. Identify and explain at layers 1, 2, 3, and 7 using a layered model approach

ANS**: Layer 1 - Physical Layer:**

- **Function:** Transmits raw bits over the physical medium.
- **Examples:** Ethernet cables, optical fibers.
- **Explanation:** This layer deals with the physical connection and transmission of data as electrical or optical signals.

Layer 2 - Data Link Layer:

Function: Frames are created with source/destination MAC addresses. Manages access to the physical medium.

Examples: Ethernet, PPP.

- **Explanation:** Responsible for error detection, addressing, and framing before sending data over the physical medium.

Layer 3 - Network Layer:

- **Function:** Routes packets between devices using logical addresses (IP).
- **Examples:** IP, ICMP.
- **Explanation:** Focuses on logical addressing, routing, and packet forwarding to ensure data reaches its destination across networks.

Layer 7 - Application Layer:

- **Function:** Provides end-user services and interfaces.
- **Examples:** HTTP, FTP, SMTP.
- **Explanation:** The closest layer to the end-user, responsible for application-specific communication and interactions.

3. Explain CSMA/CD and CSMA/CA

ANS: **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):**

- **Operation**: Used in Ethernet networks to manage access to a shared communication medium.
- **Process:** Devices listen for a clear channel before transmitting. If a collision is detected, devices stop transmitting, wait for a random backoff time, and then reattempt transmission.
- **Example**: Traditional Ethernet (e.g., 10BASE5, 10BASE2) uses CSMA/CD.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):

- **Operation**: Used in wireless networks to avoid collisions and manage access to the shared medium.
- **Process**: Devices listen for a clear channel before transmitting. If the channel is busy, they wait until it's clear. Also includes mechanisms like Request-to-Send (RTS) and Clear-to-Send (CTS) to avoid hidden node problems.
- **Example**: Wi-Fi networks (IEEE 802.11) use CSMA/CA.

4. Explain this frame and find layer

ANS:

5. Draw and explain Cisco hierarchical model

ANS: he Cisco Hierarchical Model, also known as the Cisco Three-Layer Architecture, is a design framework used for designing scalable, modular, and

efficient enterprise networks. The model consists of three layers: the Access Layer, Distribution Layer, and Core Layer.

1. Access Layer:

Function: Provides network access to end devices such as computers, printers, and IP phones.

Key Features:

Port security and VLANs for segmentation.
Connectivity to end devices.
Fast and efficient access to the network.

2. Distribution Layer:

Function: Aggregates traffic from the access layer and provides routing, filtering, and policy-based connectivity.

Key Features:

Routing between VLANs.
Policy enforcement (e.g., Access Control Lists - ACLs).
Aggregation of uplink bandwidth from the access layer.

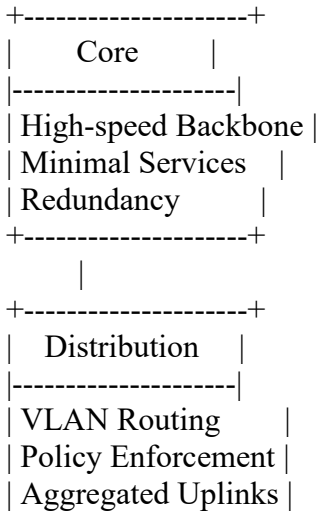
3. Core Layer:

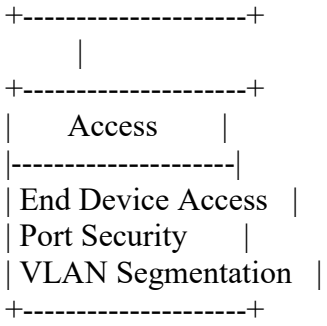
Function: High-speed backbone that facilitates fast and efficient data transport.

Key Features:

High-speed and low-latency forwarding of traffic.
Minimal services to maintain fast data transfer.
Redundancy and fault tolerance for high availability.

Diagram:



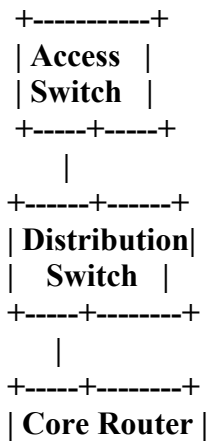


Explanation:

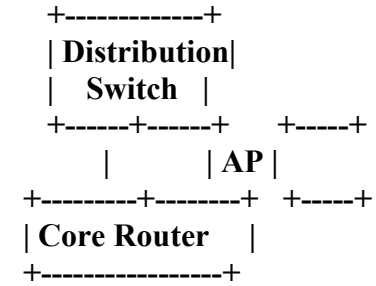
Traffic flows from the Access Layer to the Distribution Layer for aggregation and routing. Distribution Layer connects to the Core Layer, ensuring efficient and fast transport of data. Each layer has specific functions, promoting modularity, scalability, and ease of management in large networks.

6. Drawing of a typical wired and wireless enterprise LAN

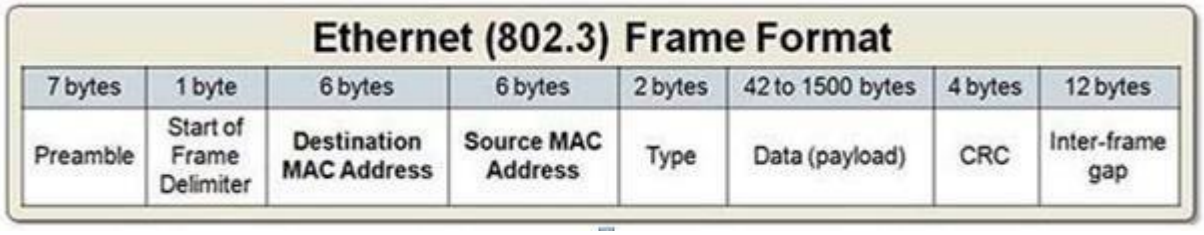
Wired Enterprise LAN:



Wireless Enterprise LAN:



7. Describe the uses of straight-through and crossover Ethernet cables



ANS: when you connect two devices of different types of

8. Explain Layer 2 and Layer 3 Switch

ANS: **Layer 2 Switch:**

Function: Operates at the data link layer (Layer 2) of the OSI model.
Key Features:

- Makes forwarding decisions based on MAC addresses.
- Segments network into collision domains.
- Supports VLANs for logical network segmentation.

Common protocols: Ethernet, ARP.

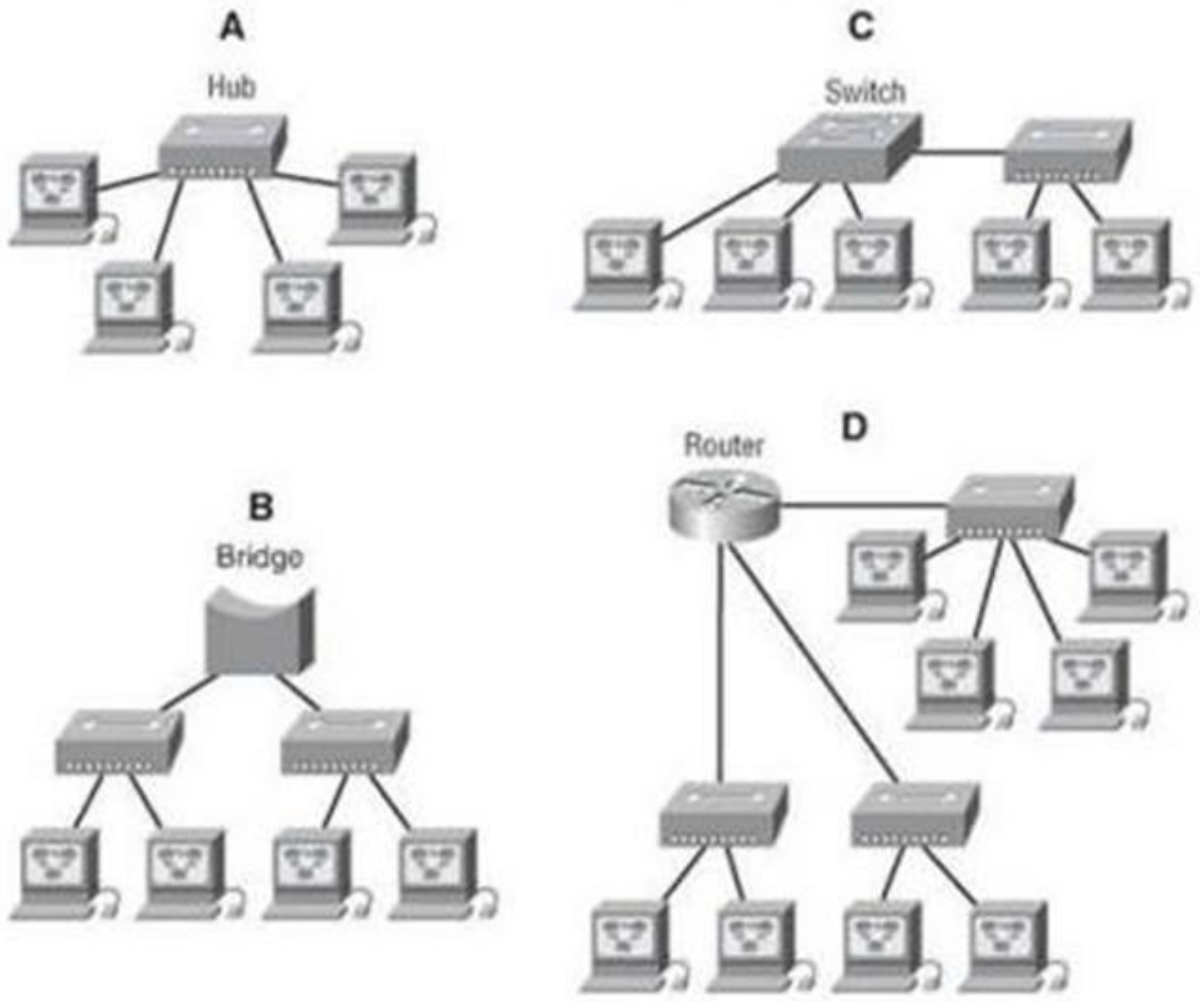
- Efficient for local traffic within the same network segment.

Layer 3 Switches:

Function: Operates at both the data link layer and the network layer of the OSI model.
Key Features:

- Combines switching and routing functionalities.
- Makes forwarding decisions based on both MAC and IP addresses.
- Routes between VLANs, enhancing network segmentation.
- Provides inter-VLAN routing.
- Efficient for routing between different network segments within the same device.

9. Identifying Collision and Broadcast Domains



9. Explain Spanning Tree Protocol

ANS: **Spanning Tree Protocol (STP):**

- **Function**: Prevents loops and ensures a loop-free topology in Ethernet networks.
- **Key Features:**

• Elects a root bridge as the central reference point.
• Designates one path as the active (forwarding) and others as blocked (discarding) to eliminate loops.
• Monitors network changes and dynamically adjusts the topology if needed.
• Ensures redundancy by providing an alternate path in case the active path fails.
• Common version: IEEE 802.1 D (STP) and its variants like Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) for faster convergence and improved efficiency.

10. Explain uncast Multicast and Broadcast

ANS: **Uncast**:

Definition: Communication between a single sender and a single receiver.
Characteristics:

- One-to-one communication.

- Data is sent from a source to a specific destination.

Multicast:

Definition: Communication between one sender and multiple specific receivers.
Characteristics:

- One-to-many communication.
- Data is sent from a source to a selected group of receivers who have expressed interest.

Broadcast:

Definition: Communication from one sender to all devices in the network.
Characteristics:

- One-to-all communication.
- Data is sent to all devices in the network, and devices decide whether to process the information based on their unique addresses.

11. Explain CAM (Content Addressable Memory)

ANS**: Content Addressable Memory (CAM):**

Function: Specialized type of memory used in network devices, such as switches, for MAC address table lookups.
Characteristics:

- Allows for quick searches based on the content (data) rather than memory addresses.
- Used in Layer 2 switches to efficiently store and retrieve MAC addresses.
- Supports high-speed table lookups, making it suitable for forwarding decisions in network switches.
- Enables fast and efficient retrieval of destination addresses during the switching process.

12. Explain CAM (Ternary Content Addressable Memory)

ANS: Ternary Content Addressable Memory (TCAM):

- **Function**: An advanced version of CAM used in networking devices for high-speed table lookups, particularly in routing and access control.

Characteristics:

- Allows for three matching states: 0, 1, or don't care (X).
- Enables more flexible and granular matching criteria in comparison to traditional CAM.
- Commonly used in routers and firewalls for access control lists (ACLs) and routing table lookups.
- Facilitates efficient processing of complex matching conditions in network forwarding decisions.

14. Which command use of Show MAC TABLE?

ANS: Command: show Mac address-table