Module 7 Network Fundamental

1. **Explain Network Topologies.**
    - Network topology refers to the physical arrangement of nodes, devices, and links in a computer network. They describe the structure and communication in the network. Here is a brief description of the network topology:

    - 1. Bus Topology: All devices connected to the network are called busses. Data travels along the bus, and each device receives and processes the data available for it.
    - 2. Star topology: All devices are connected to a central device such as a switch or hub. Information flows through the central device, enabling communication between devices.
    -
    - 3. Ring Topology: Devices are connected in a closed loop or ring, where each device is connected to two adjacent devices.
    - Data travels around the ring in one direction, passing through each device until it reaches its destination.

    - 4. Mesh topology: Every device in the network is connected to every other device. This creates more direct communication channels and increases reliability and repeatability.

    - 5.Tree topology: Devices are arranged in a tree-like hierarchical structure. Central nodes are connected to other nodes that are connected to other nodes. Information flows from higher levels to lower levels.

    - 6. Hybrid Topology: Combine two or more different topologies to create a more complex network.
    - For example, the network may have a combination of star and ring topologies.

    - Each network topology has advantages and disadvantages in terms of cost, capacity, security and performance. The choice of topology depends on the requirements and limitations of the network.

2. **Explain TCP/IP Networking Model.**
    - TCP/IP networking standard, also known as Internet Protocol Suite, is a standard for computer communication. It provides a way for devices to send and receive information over the Internet. The TCP/IP standard has four layers, each responsible for a specific communication function. Here is a brief description of each layer:

- 1. Application layer: This layer represents the interface between the network and the user application.It includes protocols that allow certain applications to communicate with each other, such as HTTP for web browsing, SMTP for email, and FTP for file transfer.

- Transport layer: this layer manages reliable data transfer between devices. It has two main protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP provides reliable and orderly transmission of data, while UDP provides faster connection and transmission.

- Internet Layer : This layer manages the location and routing of data packets across multiple networks. It uses Internet Protocol (IP) to assign unique IP addresses to devices and determine how data packets are sent from destination to destination over the Internet.

- Link Layer : Also called Network Interface Layer or Data Link Layer, this layer controls the physical transmission of data over the network medium.It consists of processes and technologies specific to physical connections, such as Ethernet or Wi-Fi, and is responsible for data encapsulation and error detection.

- The TCP/IP standard is layered, and each layer hosts a set of services provided by the layer below it. This architecture provides flexibility and interaction between different devices and different networks. The TCP/IP standard is the foundation of today's Internet and is used in all kinds of networks, from small local networks to the global Internet.

3. Explain LAN and WAN Network.

- LAN (Local Area Network) and WAN (Wide Area Network) are two types of computer networks that differ in area and connectivity.

- Local Area Network: ALocal Area Network is a network that covers a small area such as a home, office or school campus. It is designed to connect devices close to each other. In a LAN, devices such as computers, printers, servers, and switches communicate with each other using wired (Ethernet) or wireless (Wi-Fi) technology. LANs are often used for local data sharing, resource sharing, and internal communication within an organization.
- They offer high-speed and low-latency connections, making them suitable for tasks that require fast and direct communication.

- WAN:A WAN, on the other hand, is a network that spans a wide area and usually interconnects multiple LANs or other networks. It can cover a city, a country, or even an entire country. WANs use a variety of technologies to connect remote locations, including leased lines, fiber optics, satellite links, and public networks such as the Internet. WANs are usually operated and managed by service providers or telecommunications companies.It provides communication between different LANs, facilitates access to remote locations, and supports applications such as e-mail, video conferencing, and data center. WANs provide more services but may have higher latency and lower bandwidth than LANs.

4. Explain Operation of Switch

- The switch is a network device that operates at the data link layer (layer 2) of the TCP/IP network model. It is used to connect devices in a local area network (LAN) and facilitate data transfer between these devices. The operating principle of the switch is briefly explained below:

- MAC address learning: When the switch is turned on or connected to a new device, the switch will learn the MAC address of the device connected to its port. It does this by examining the MAC address of the incoming device and associates it with the relevant port.

- MAC address table: The variable maintains a table of MAC addresses, also known as the delivery table of content addressable memory (CAM).This message specifies the MAC address for the router connection. Initially the table is empty, but populated based on the changed MAC address.

- Routing decision: When a frame arrives at the switch, it checks the MAC address. If the MAC address is found in the MAC address table, the frame is forwarded only to the port associated with the MAC address. This is called unicast routing.

- Broadcast and multicast management: If the MAC address is a broadcast address (any address) or a multicast address, the frame is forwarded to all ports except the port from which it was received. This enables all devices on the LAN to receive broadcast or multiview.

- Switching and Filtering: A switch switches using the MAC address table to determine the appropriate port for each frame. It improves network performance by reducing unnecessary traffic by filtering out frames that are not suitable for connecting devices.

- Collision Domain Allocation: The switch creates a separate collision domain for each of its ports.This means that devices connected to different ports can send data at the same time without conflict, unlike shared media such as hubs.

- VLAN support: Switches generally support virtual LANs (VLANs) that allow communication networks to be created on the physical LAN. VLANs provide segmentation and increase security by separating traffic between different groups.

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

- Router: A router is an important device that connects multiple networks such as a LAN or WAN. Its main purpose is to send packets between networks based on IP addresses. Routers communicate between networks using routing tables to determine the best route to send data.

- switch: A switch is a device used to connect devices in a community. It works on the data link layer and transmits data according to the MAC address.Switches create independent collisions for connected devices, providing simultaneous and efficient communication. They also help create VLANs for network sharing and increased security.

- Firewall: A firewall is a network security device that monitors and controls network access. It acts as a barrier between internal networks (such as LANs) and other networks (such as the Internet). Firewalls enforce security policies, filter traffic according to defined rules, and block unauthorized access and threats.

- Wireless Access Point (WAP): A wireless access point supports wireless connections on a network. It acts as a central hub for wireless devices connecting to a wired network. WAP provides Wi-Fi access, identifies devices and manages their wireless settings, allowing devices to access the network without physical cables.

- Modem: A Modem (short for Modem) is a device that converts digital signals from a computer into analog signals suitable for communication transmission, such as telephone lines or electrical cables. It allows the device to connect with an Internet Service Provider (ISP) and access the Internet.

- Network Switches: Network switches are used to increase the number of network ports available on a LAN. They allow multiple devices to connect and communicate over a network by providing additional Ethernet ports.

- Network Load Balancer: A load balancer distributes network traffic across multiple servers or resources to improve performance, maximize availability, and increase capacity. They help distribute incoming requests evenly, prevent server overload, and increase the overall efficiency of the network.

- Network Hub: A hub is a primitive device that operates at the physical layer of a network.They only receive incoming packets and broadcast them to all connected devices. Hubs are less useful than wrenches as they create joint collisions and can cause joint damage.

6. **Make a list of the appropriate media, cables, ports, and connectors to connect switches to others.**
    - To connect switches to other devices, various media, cables, ports, and connectors can be used depending on the specific requirements and technologies involved. Here's a list of commonly used options:

    - **Media:**

    - Copper Wire: Utilizes twisted pair cables made of copper for data transmission. It is commonly used for Ethernet connections.

    - Fiber Optic: Utilizes optical fibers to transmit data as light signals. It provides higher bandwidth, longer distance capabilities, and immunity to electromagnetic interference.

    - **Cables:**

    - Ethernet Cable: Commonly used for wired connections. Options include:
    - Category 5e (Cat 5e): Supports speeds up to 1 Gigabit per second (Gbps).
    - Category 6 (Cat 6): Supports speeds up to 10 Gbps over shorter distances.
    - Category 6a (Cat 6a): Supports speeds up to 10 Gbps over longer distances.
    - Fiber Optic Cable: Offers high-speed and long-distance transmission. Options include:
    - Single-mode fiber (SMF): Designed for long-range communication.
    - Multimode fiber (MMF): Suitable for shorter distances.

- **Ports and Connectors:**

- Ethernet Ports: Most switches have Ethernet ports that support standard RJ-45 connectors for copper Ethernet cables.
- Fiber Optic Ports: Switches may have SFP (Small Form-factor Pluggable) or SFP+ (Enhanced Small Form-factor Pluggable) ports that can accept fiber optic transceivers. Transceivers with LC, SC, or ST connectors are commonly used.
- Console Port: A serial port found on switches for out-of-band management and configuration. It typically uses RS-232 or USB connectors.
- Uplink Ports: Some switches have dedicated uplink ports that provide higher bandwidth connections, such as Gigabit Ethernet or 10 Gigabit Ethernet, for connecting to other switches or network devices.
- Stacking Ports: In stackable switches, stacking ports are used to connect multiple switches together to form a logical unit with increased capacity and redundancy.

7. .Define Network devices and hosts.

- Network Devices: Network devices are physical or virtual devices that facilitate communication, connection and data transfer in a computer network. These tools are designed to perform specific tasks and to operate and manage the network. Some examples of network equipment include routers, switches, firewalls, wireless access points, modems, load balancers, and network centers. Network equipment plays an important role in ensuring efficient and secure data transmission, network connectivity and network management.

- host: In the context of a computer network, host refers to the end user or system connected to the network.The host can be a computer, server, laptop, smartphone, tablet, IoT device, or any device that can participate in networking. Hosts initiate and receive data sent over the network in relation to network services and applications and can be both the source and destination of the data. Hosts have unique identifiers, such as IP addresses, that allow them to address and access the network. Hosts rely on network equipment such as switches and routers to facilitate communication and connections with other hosts and network resources.

8. **What are Ethernet Standard (802.3) and Frame Formats?**
    - The Ethernet standard (IEEE 802.3) defines specifications for Ethernet networks, including physical announcements, guidelines, standards, and network access procedures. The Ethernet frame type provides a structure for data packets transmitted over Ethernet. The Ethernet II frame type, also known as DIX Ethernet or Ethernet version 2, is the most widely used. The preface includes the starting frame delimiter, destination and destination MAC address, EtherType or length field, payload information, and a frame check sequence (FCS) for errors.Ethernet frames are essential for reliable and efficient operation and transmission of data over Ethernet networks.

9. **Comparison between UTP, MM and SM Ethernet Cabling**

Feature	**UTP**	**MM Fiber optical**	**SM fiber optical**
Transmission speed	up to 10 gbps	up to 100 gbps	up to 100 gbps
Maximum Distance	up to 100 meters	up to 550 meters	up to 40 kilometer
Immunity to Emi	susceptible to emi	immune to emi	immune to emi
bandwidth	limited bandwidth	higher bandwidth	highest bandwidth
Cost	relatively inexpensive	moderate cost	higher cost
Installation	Easy to install	Require specialized termination	Require specialized termination
Cable Size	Thicker and bulkier	Thinner and more flexible	Thinner and more flexible
Use Cases	Local Area Network	Data center, sort range links	long range links, telecommunication

10. **Make Cross cable.**
    - Gather tools and consumables: You will need an Ethernet cable, wire cutters/stripers, an RJ-45 crimper and two RJ-45 connectors.

    - Stripping Outer Sheath: Using wire cutters/stripers, carefully strip approximately 1.5 inches (4 cm) of outer sheath from both ends of the Ethernet cable. Be careful not to damage the internal cables.Untwisted Pairs: You will find four twisted pairs in the cable.Dissolve and separate pairs by making them color coded based on negative.

- cable: at one end of the cable, arrange the cables from left to right: white orange, orange, white green, blue, white blue, green, white brown, brown.

- Cut the cables: Use cable cutters to cut the cables as long as possible, make sure they match and plug them into the RJ-45 connectors.

- Attaching Cables to Connectors: Plug each cable into a T568A model RJ-45 connector. Double check that the cables are seated properly.

- Crimp the Connectors: Use an RJ-45 crimping tool to crimp the connectors using firm pressure to secure the wires in place. Make sure the connector is connected to the cable.

- Repeat the procedure: Do the same on the other end of the cable, but this time prepare the cables according to the T568B model: White-green, Green, White-orange, Blue, White-Blue, Orange, White-Brown , Brown.

11.Make Straight-Through Cable.

- Gather tools and consumables: You will need an Ethernet cable, wire cutters/stripers, an RJ-45 crimper and two RJ-45 connectors.
- Stripping Outer Sheath: Using wire cutters/stripers, carefully strip approximately 1.5 inches (4 cm) of outer sheath from both ends of the Ethernet cable. Be careful not to damage the internal cables.
- Untwisted Pairs: You will find four twisted pairs in the cable.Dissolve and separate the pairs, making the color-coded wires intact.
- cable: At both ends of the cable, arrange the cables from left to right: orange white, orange, white green, blue, white blue, green, white brown, brown.
- Cut the cables: Use cable cutters to cut the cables as long as possible, make sure they match and plug them into the RJ-45 connectors.
- Attaching Cables to Connectors: Plug each cable into an RJ-45 connector on a T568A or T568B model. For consistency, it's important to use the same pattern on both ends of the cable.Double check that the cables are seated properly.
- Crimping the Connector: Use an RJ-45 crimping tool to crimp the connector applying firm pressure to secure the cable in place. Make sure the connector is connected to the cable.
- Repeat the procedure: Follow the same steps on the other end of the cable, join and crimp the cables in the same order.

12. Differentiate between LAN/WAN operation and features.

- **Function:**
- LAN: Work in a limited space such as home, office or school. Owned and managed by a company.
- WAN: Connects multiple LANs and remote sites over large areas. It uses public or private network infrastructure and often includes multiple service providers.

- **Service:**
- LAN: Usually covers a small area in a home or school.
- WAN: covers a large area such as a city, a country, or several countries.

- **distance:**
- LAN: Short range, usually up to several hundred meters.
- WAN: typically covers distances of thousands of miles or more.

- **Network Speed:**
- LAN: Provides high-speed connections, typically in the range of gigabits per second (Gbps) or higher.
- WAN: Provides lower bandwidth than LAN, ranging from kilobits per second (Kbps) to gigabits per second (Gbps), depending on technology and equipment.

- **Members:**
- LAN: Privately owned and operated by an organization.
- WAN: can be personal or provided by the service provider. It may involve collaboration between different organizations or service providers.

- **Connectivity:**
- LAN: Allow direct communication and sharing of devices by connecting devices in a limited area.
- WAN: Connect devices in different locations to realize long-distance communication and collaboration.

- **Reliability:**
- LAN: Most reliable as it is managed and controlled by an enterprise.
- WAN: Reliability may vary depending on the respective manufacturer and service provider. Backup and backup systems are often used to provide reliable connections.

- **Security:**
- LAN: Easy to use and manage security measures due to its location.
- WAN: Additional security measures are required due to the involvement of public networks and the possibility of exposure to external threats.

- **Cost:**
- LAN: Usually cheaper to install and maintain due to small network impact.
- WAN: Often involves higher costs due to the need for long distance connectivity, advanced network equipment, and potential service provider costs.

13. Explain ARP, ICMP and Domain name .

- ARP: Address Resolution Protocol (ARP) is a network protocol used to assign an IP address to a MAC address on a local network. When a device wants to send data to another device on the same network, it uses ARP to determine the device's MAC address. ARP maintains a table called ARP cache that stores IP-MAC address mappings for efficient communication.

- ICMP: Internet Control Message Protocol (ICMP) is a network protocol used for diagnostics and error reporting in IP networks. ICMP allows network devices to send error messages and control messages to each other about network events such as host failures or replication. Utilities such as Ping and Traceroute often use ICMP to check network connectivity and measure round-trip times between devices.

- Domain Name: A domain name is a human-readable and easy-to-remember tag used to identify a specific website or location on the Internet. It provides an easy way for users to access resources such as websites or email servers using their domain name instead of IP addresses. Domain names are organized hierarchically; top-level domains (TLDs) represent the top-level domain, followed by secondary domains and subdomains. The Domain Name System (DNS) is responsible for translating domain names into IP addresses and allows computers to communicate over the Internet.

14. Describe the components required for network and Internet communications.

- Network Interface Card (NIC): A network interface card, also known as a network adapter or network interface controller, is a hardware device that enables a computer or device to be connected to a network. It provides the necessary interface between devices and network environments such as Ethernet or Wi-Fi.

- Router: A router is a device that connects multiple networks and routes data between them. It acts as a central point for data traffic and determines the most efficient way for data files to reach their destination across multiple networks. Routers also perform functions such as network address translation (NAT) to allow multiple devices to share separate IP addresses.

- Switch: A switch is a network device that allows multiple devices in an area to communicate with each other. It operates on a data link layer network that uses MAC addresses to send packets to their destinations on the same network.

- Modem: A modem is a device that converts digital data into analog signals for transmission over a communication medium such as a telephone or cable. It enables devices to connect to the internet by converting the digital signals used by computers into a format suitable for the transmission of a certain communication channel.

- protocol: A protocol is a set of rules and standards that govern the formatting, exchange, and processing of data between devices on a network or the Internet.Examples of protocols include TCP/IP (Communication Control Protocol/Internet Protocol), which is the basis of Internet communication, and HTTP (Hypertext Transfer Protocol), which controls data transfer between web browsers and web servers.

- DNS Server: Domain Name System (DNS) servers are responsible for translating domain names into their own IP addresses. When a user enters a domain name on a website, the DNS server resolves the domain name to an IP address, allowing the device to establish a connection with the desired website or server.

15. Explain Encapsulation and DEcapsulation in OSI Reference model.

- Encapsulation: At each layer of the OSI model, a header specific to that layer is added to the data, creating a Data Package (PDU). This PDU becomes the payload for the next layer. It adds special features such as encapsulation, addressing, checking and error checking.

- Decapsulation: When the last is taken, the extra headers in each layer are removed and the rest is passed to the next layer. This action deletes the data and related data until the original data is retrieved in the application layer.

16. Explain network segmentation and basic traffic management concepts.

- Network partitioning divides a network into smaller, separate network segments or subnets, providing benefits such as improved performance, enhanced security, and better network management. Techniques such as VLANs, subnets, and DMZs are often used for network partitioning.

- Traffic management concepts are designed to manage and optimize network traffic. Quality of Service (QoS) technology prioritizes and manages traffic according to defined rules, providing differentiated service and efficient bandwidth allocation. Traffic management also includes techniques such as traffic scheduling, load balancing and congestion control to maintain network performance and reliability.

17.What is flow control and acknowledgment?

- Flow control and authentication are important concepts in computer communication:
-
- Flow control controls the data flow between the sender and the receiver to avoid data loss and interruption of received goods.
- Stop-wait and sliding window are two methods of flow control.
- Stop Waiting involves the sender sending data one at a time and waiting for confirmation before sending the next frame. The
- sliding window allows the sender to send multiple frames before they are acknowledged, depending on the capabilities of the receiver.
- Acknowledgment (ACK) is a response sent by the receiver to verify receipt of data.
- Acknowledgment gives feedback to the sender that the document has reached its destination without errors.
- The sender may cause data to be returned if no acknowledgment or negative acknowledgment (NAK) is received in a timely manner.
- traffic management and authentication work together to ensure that data is transferred efficiently and effectively across a computer network.

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

- **OSI model:**
- OSI model has seven layers, each layer is responsible for a specific function in network communication. From top to bottom, the layers are:

- **Application Layer:** This layer provides direct services to end users and applications. Protocols such as HTTP, FTP, SMTP, and DNS work on these protocols to support functions such as file transfer, email, web browsing, and name resolution.

- **presentation layer:** This layer ensures compatibility of input data between different systems. It performs functions such as data encryption, compression and formatting.
  Protocols such as SSL and TLS operate at this layer.

- **Session Layer:** Session layer creates, manages and terminates sessions between applications. Provides synchronization and dialog control. Protocols such as NetBIOS and SSH work on this layer.

- **Container Layer:** A transport mechanism that ensures reliable and controlled transmission of data across the network.It splits large files into smaller partitions and performs monitoring, error recovery and replication. The main protocol of this layer is TCP (Transmission Control Protocol).

- **Network Layer:** The network layer manages address and location information. It encapsulates data in packets and determines the best path for the package to be delivered. IP (Internet Protocol) runs on this layer.
- **Data Link Layer:** This layer provides reliable data transmission over physical links. It encapsulates packets into frames and performs error detection and correction. Protocols such as Ethernet and PPP operate at this layer.

- **Body System:** The body system works on the delivery of raw material through the body environment. Defines the electrical, mechanical and functional properties of the physical interface.
- Data flows from the application layer to the physical layer via the OSI model, and each layer adds its own header or trailing information during encapsulation. This process is reversed at the receiving end, stripping each layer of header or queue information.

- **TCP/IP standard:**
- TCP/IP standard, also known as the Internet Protocol Suite, is a simpler and more widely used network standard. It has four layers:

- **Application layer:** The application layer in the TCP/IP model, which corresponds to the application layer, presentation layer, and layer layer of the OSI model. It includes protocols for services such as e-mail (SMTP), file transfer (FTP), web browsing (HTTP), and domain name resolution (DNS).
- **Transport layer:** The transport layer in the TCP/IP model corresponds to the transport layer in the OSI model. It provides data transmission and provides end-to-end communication services. The main protocols of this layer are TCP and UDP (User Datagram Protocol).

- **Internet layer:** The Internet layer in the TCP/IP model corresponds to the network layer in the OSI model. It manages packet forwarding between different networks.

- The IP protocol works in this process along with protocols such as ICMP (Internet Control Message Protocol) for error notification and IGMP (Internet Group Management Protocol) for group management.
- **Network interface layer:** The network interface layer in the TCP/IP model, which corresponds to the data link layer and layer of the OSI model. It controls the physical transmission of data over network connections, including protocols specific to the network technology used, such as Ethernet, Wi-Fi, or DSL.
- Data flows in the TCP/IP model and the data request is packaged in a data packet at the application layer. These packets are then packaged in the transport layer section, which adds a TCP or UDP header.This section is also added to the IP packet at the Internet layer and an additional IP header. Finally, IP packets are packaged in frames at the network interface layer by adding data link headers and fragments specific to the network technology used.

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

- **Layer 1: Physical layer**
- The physical layer is the lowest layer of the OSI model. It involves physically transmitting the raw material over a physical medium such as copper wire, fiber optic cable or wireless signal. It describes the electrical, mechanical and physical interactions between devices. This layer is responsible for sending and receiving binary data without worrying about the meaning or format of the data.
- **Layer 2: Data Link Layer**
- Data Link Layer is responsible for improving data transfer between direct links over physical links.It provides error-free, sequential and flow-controlled transmission of data frames. This layer encapsulates the packets from the network layer into frames and adds the necessary control information for detection and correction.
- **Layer 3: Network Layer**
- Network Layer is responsible for addressing, routing and forwarding packets across multiple networks. It provides end-to-end packet delivery by determining the best path for data transmission. This process encapsulates the data in the transport layer into packets, adding the network header and the address (IP address) based path.
- **Layer 7: Application Layer**
- The application layer is the top layer of the OSI model. It provides direct service to end users and applications. This system consists of processes and connections that provide network communication and support functions such as data representation, encryption, compression, and session management.

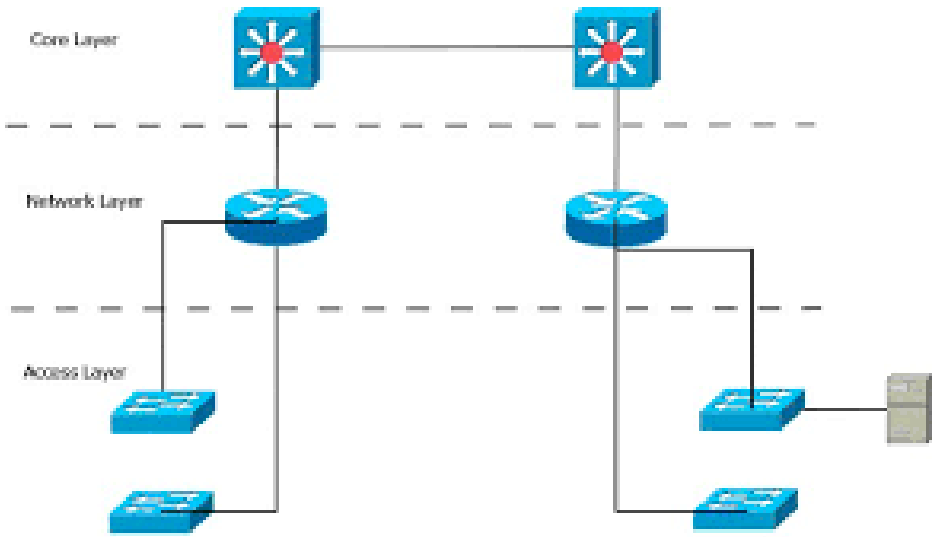
20.Explain CSMA/CD and CSMA/CA.

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection):
- CSMA/CD is a method used in traditional Ethernet networks, especially wired networks. It works by allowing network devices to identify the carrier (the medium that carries the data) before transmission. If the carrier is busy, it indicates that another device has sent it, the device waits for a different time and then tries again. If two devices are transmitting at the same time and collide, both stop transmitting and wait a different amount of time before trying to transmit again.
- CSMA/CD is based on the collision principle where the device listens to the network for any collisions during transmission.
- When a collision is detected, the device in question waits a different amount of time before exiting and trying again. This process allows only one device to transmit at a time, reducing the possibility of conflicts and maintaining efficient data transfer across the network.

- CSMA/CA (Carrier Sense Multiple Access with Collision Prevention):
- CSMA/CA is a widely used method in wireless networks such as Wi-Fi networks. Unlike CSMA/CD, which focuses on detecting and recovering from collisions, CSMA/CA aims to avoid collisions entirely. The
- CSMA/CA operates using the Request to Send (RTS) and Clear to Send (CTS) mechanisms.
- Before sending data, the device sends an RTS frame requesting permission to transmit to the receiving device. The receiving device responds with a CTS frame that allows transmission. This exchange ensures that other nearby devices are aware of the ongoing transmission and can delay their own transmission.

21.Explain this frame and find layer

-

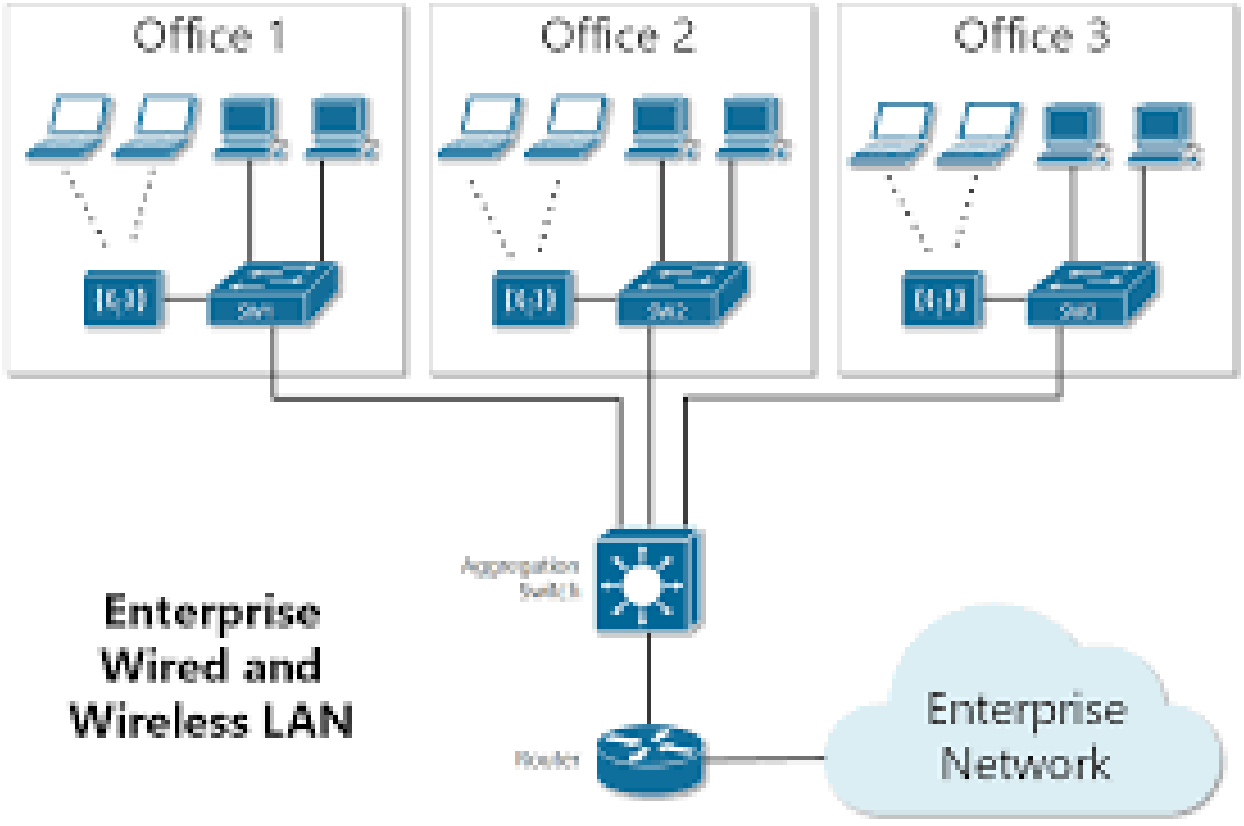


- **Access layer:** It is the layer where end devices such as computers, phones, printers and IoT devices are connected to the network. It provides an access point for users and acts as an interface between end devices and the rest of the network. This layer usually uses switches to connect and control network devices.

- **Distribution Layer:** Distribution layer acts as an intermediary between the access layer and the main layer. Its main function is to provide training, policy management and consolidation of the joint venture.It connects multiple access layers and distributes traffic between them. It can also manage security policies, Quality of Service (QoS), and VLANs (Virtual Local Area Networks).

- **Core Layer**: The core layer is responsible for fast data transmission and is the backbone of the network. It connects different protocols to provide fast and reliable data transmission in the network. Large systems often use routers to handle large amounts of traffic efficiently. Redundancies and violations such as link failure and link failure are often used by this layer to ensure the reliability of the network.

22.Drawing of a typical wired and wireless enterprise LAN



-

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

- **straight-through cable:**
- **Application:** Flat network cable is the most common type of network cable. They are used to connect different types of devices with different roles or functions in the network.
- Wiring Configuration: In a straight line, the configuration of the wires is the same from one end to the other. Pin 1 on one end of the cable connects to Pin 1 on the other end and so on. This configuration is called "T568B" or "T568A" wiring.
- Useful information:
- , connecting a computer or laptop to a switch or router.
- connects the switch to the router. The
- connects a network printer or network attached storage (NAS) device to a switch or router.

- **Crossover Ethernet Cable:**
- **Purpose:** Crossover cables are used to connect similar types of devices directly to each other without an intermediate device such as switches or routers.
- Wiring Configuration: In crossover cable, change the set configuration to allow direct connection between two similar things.
- The transmit (Tx) pins on one end of the cable switch to the receive (Rx) pins on the other end and vice versa. Mode
- Data Usage:
- connects two computers or computers directly together for data sharing or network gaming. The
- connects two switches directly together without using a router. It is worth noting that
- Modern Ethernet ports and devices usually have an MDI / MDI-X (Media Dependent Interface / Media Dependent Interface Pass-through) interface that can be controlled and adjusted for the type of cable used. This means that in most cases flat cables can be used for both connection types because the device adapts to the cabling accordingly.

24.Explain Layer 2 and Layer 3 Switch

- **Layer 2 switch:**
- Function: Layer 2 switch operates on the data link layer (layer 2) of the OSI model. Its main function is to send network traffic according to MAC (Media Access Control) address.
- MAC Address Learning: A Layer 2 switch creates and maintains a MAC address table by examining the MAC address of incoming frames. This allows them to associate MAC addresses with specific switches.
- MAC Address Forwarding: Once the MAC address table is populated, Layer 2 switches use this information to forward the frame only to the specific port with the MAC address.
- This leads to efficient and territorial communication in the network.

- VLAN support: Layer 2 switches generally support VLAN (Virtual Local Area Network) functionality, allowing network sharing and isolation of different VLANs.
- Low Routing Capability: Layer 2 switches cannot route IP packets between different subnets. They usually focus on exchanging and forwarding frames based on MAC addresses.

- **Layer 3 switch:**
- Function: Layer 3 switch operates at the network layer (layer 3) of the OSI model.It combines the features of a traditional Layer 2 switch with some functionality.
- Routing Capabilities: Layer 3 switches can perform IP routing using routing protocols such as OSPF (Open Shortest Path First) or static routing configurations. This allows them to decide to send by IP address.
- Inter-VLAN Routing: Layer 3 switches are usually capable of inter-VLAN routing and forwarding packets between them, enabling communication between different VLANs.
- Efficient Packet Forwarding: Layer 3 switches have hardware-based routing mechanisms that allow for faster and more efficient forwarding than traditional routers using software-based routing.
- Advanced features: May include additional features such as Layer 3 switches, access control lists (ACLs), quality of service (QoS) features, and multicast support.

25.Identifying Collision and Broadcast Domains

- Collision area: Collision area is the part of the network where the network devices share the same network environment. In this case, conflicts can occur when two or more devices try to send data at the same time. Collisions often occur in networks that use shared media, such as Ethernet hubs or half-duplex connections.

- Broadcast Domain: A broadcast domain is a domain on the network to which broadcast packets are sent. Broadcast packets are packets sent to all devices on the network to display services or transmit information.Broadcast is usually defined by routers or Layer 3 boundaries, as routers prevent broadcast from passing between different networks or subnets.

26.Explain Spanning Tree Protocol

- Spanning Tree Protocol (STP) is a protocol that protects circuits in Ethernet networks.
- STP selects the reference root bridge to calculate the shortest path for other switches.
- Path value is calculated based on connection speed or bandwidth.
- transmits data transmission units (BPDUs) for transmitting and exchanging network data. Switch
- determines the best path to the root bridge and marks the port as root or port.
- STP goes through blocking, listening, learning and transmitting phases to ensure there are no loops.

- STP constantly monitors the network for changes and recalculates the path to avoid loops. The
- STP prevents broadcast storms, network congestion, and other problems caused by Ethernet loops.

27. Explain unicast Multicast and Broadcast

- **Unicast Communication:**
- Unicast communication is a type of one-to-one communication in which messages are sent from a source to a specific destination.
- Unicast communication uses a device to address a specific destination using its MAC address or IP address.
- then send the message directly to the intended recipient.
- unicast communication is used for most client-server communications, such as when you visit a website or send an email.

- **Multicast Communication:**
- Multicast Communication is one-to-many communication in which messages are sent from one device to multiple destinations.
- The source device forwards the message to a set of multicast IP addresses instead of a specific IP address.
- A device wishes to receive a multicast message by registering with the corresponding multicast IP address and joining a multicast group.
- The network infrastructure then copies only the multicast messages and sends them to the devices that join the multicast group.
- Multicast communication is often used in applications such as multimedia streaming, online gaming, and video conferencing where multiple receivers need to receive the same information simultaneously.

- **Broadcast Communication:**
- Broadcast Communication is a type of one-to-one communication in which messages are sent from one device to all devices in a particular segment or broadcast.
- The device is used to forward messages to a specific broadcast destination, usually representing all devices in a particular segment or subnet.
- Network infrastructure broadcasts messages to all devices in the broadcast network, and all devices receive and process messages.
- broadcasts are often used for network discovery, such as Address Resolution (ARP) or Dynamic Host Configuration Protocol (DHCP) requests, where devices must find messages and interconnect with other devices on the same network.

28.. Explain CAM (Content Addressable Memory)

- Structure: The CAM has a set of tables or storage units, each associated with a specific content or data schema. Each memory cell has two parts: a data area and a parallel area.
- Data Storage: CAM stores content or schema data and associated data or results. For example, in an Ethernet switch, a CAM may store a MAC address and a port number that includes a specific MAC address.
- Content-Based Research: CAM is unique in its ability to handle content-based research.
- When starting a search, the content or data structure to be searched is presented as an input.
- Parallel Comparison: The CAM performs simultaneous parallel comparison of sent data with sample data stored in each memory. Checks the match between the input model and the object stored in each memory location.
- MATCH LINE ENABLE: If a match is found, the match line associated with the corresponding memory is activated. Active lines provide the address or location of the matching data in the CAM.
- Data recovery: When Matchline is enabled, relevant data or results stored in memory can be quickly recalled.

29.Explain CAM (Ternary Content Addressable Memory)

- Triple Content Addressable Memory (TCAM) is a type of advanced memory used for high speed integration and decision making in connected devices. Key points are:
- TCAM differs from Content Address Memory (CAM), which displays a mask and facilitates compliance.
- He has a mental memory containing information, masks and matches. TheTCAM performs content-based comparison by simultaneously comparing incoming data with stored models. Supports triple mapping by allowing external state onMask model.
- When a match is found, the corresponding match line is activated and relevant information can be retrieved quickly. The
- TCAM offers flexibility and choice in comparison models, making it suitable for difficult deployment-based decisions in network equipment.
- However, TCAM has higher cost, power consumption, and capacity limitations than other types of memory.

30.Which command use of Show MAC TABLE?

- **command : show mac address-table**