**Assignment**

**CCNA Assignment**

**By**

**Himanshu Kalambe**

**Guided by**

**Rohit Sir**

**MODULE 1**

1, Explain is the OSI reference model?

Ans, The OSI (Open Systems Interconnection) model is a way to understand how different computer systems communicate over a network. It breaks down the process into seven layers, each with a specific role:

**Physical Layer (Layer 1)**:

Function: Deals with the physical connection between devices, including the cables, switches, and other hardware.

Data Units: Bits.

Examples: Ethernet cables, fiber optics, physical aspects of network interfaces.

**Data Link Layer (Layer 2)**:

Function: Provides node-to-node data transfer and handles error correction from the physical layer. It ensures that data is transferred without errors.

Data Units: Frames.

Examples: MAC addresses, Ethernet, switches, bridges.

**Network Layer (Layer 3)**:

Function: Manages the delivery of packets across multiple networks. It handles routing and forwarding of packets.

Data Units: Packets.

Examples: IP addresses, routers, IPv4/IPv6.

**Transport Layer (Layer 4)**:

Function: Ensures complete data transfer. It provides end-to-end communication, error recovery, and flow control.

Data Units: Segments (TCP) or datagrams (UDP).

Examples: TCP (Transmission Control Protocol), UDP (User Datagram Protocol)

**Session Layer (Layer 5)**:

Function: Manages sessions between applications. It establishes, maintains, and terminates connections between the applications.

Data Units: Data.

Examples: Session establishment protocols, RPC (Remote Procedure Call).

**Presentation Layer (Layer 6)**:

Function: Translates data between the application layer and the network. It handles data encryption, compression, and translation.

Data Units: Data.

Examples: SSL/TLS (encryption), JPEG (image format), ASCII (text encoding).

**Application Layer (Layer 7)**:

Function: Provides network services directly to end-user applications. It facilitates user interaction and offers various network services.

Data Units: Data.

Examples: HTTP (web browsing), FTP (file transfer), SMTP (email).

2, What is a Network?

Ans: A network is a group of connected devices, such as computers, phones, and servers, that can communicate and share resources, like files and internet access. These connections can be made using cables, wireless signals, or other methods.

3, What are Routers?

Ans; Routers are devices that connect different networks together and direct data traffic between them. They determine the best path for data to travel from one device to another, ensuring it reaches its destination efficiently

4,Explain Encapsulation.

Ans; Encapsulation is the process of adding headers and sometimes trailers to data as it moves through the layers of a network. This ensures that the data is correctly formatted and can be properly understood when it reaches its destination.

5: Peer-to-Peer Communication.

Ans: Peer-to-peer (P2P) communication is a network model where each device (peer) can directly share resources and data with other devices without needing a central server.

6, What is TCP and UDP?

Ans;

**TCP (Transmission Control Protocol):**

Reliable: Ensures all data sent is received accurately and in order.

Connection-oriented: Establishes a connection between sender and receiver before data transfer.

Use cases: Web browsing (HTTP/HTTPS), email (SMTP), file transfers (FTP).

**UDP (User Datagram Protocol):**

Unreliable: Sends data without ensuring it arrives correctly or in order.

Connectionless: Sends data without establishing a dedicated connection.

Use cases: Streaming videos, online gaming, voice calls (VoIP), where speed is more critical than reliability.

7, What is Internetwork Operating System software?

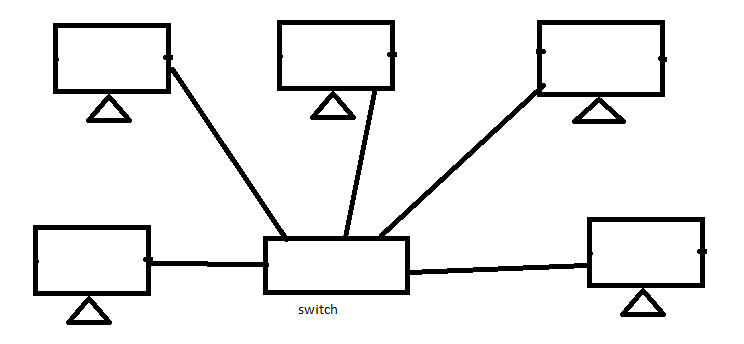
Ans: Internetwork Operating System (IOS) software is a network operating system used on many Cisco Systems routers and network switches. It provides the necessary functionality to manage network hardware, allowing devices to perform routing, switching, internetworking, and telecommunications functions

Routing and Switching: Handles data packet forwarding and management.

Security: Implements security protocols and features like firewalls and VPNs.

8, Explain LAN and draw any example.

Ans; A Local Area Network (LAN) is a network that connects computers and devices within a limited geographical area, such as a home, school, office building, or closely positioned group of buildings. LANs are used to share resources like files, printers, and internet access among connected devices.



9, Explain Network Device - Router Switch and Hub .

Ans; Router: Connects different networks and directs traffic between them.

Switch: Connects devices within a network and sends data directly to the intended device. Traffic avoidance using csma/cd technology .

Hub: Connects devices within a network but sends data to all devices, causing potential congestion.

10, Describe Router and switch connection in LAN.

Ans;

**Router-Internet Connection:**

The router connects the LAN to the internet. It serves as the gateway, managing traffic between the LAN and external networks.

The router is usually connected to a modem (or directly to an internet line), allowing devices within the LAN to access online resources.

**Switch-Device Connection:**

The switch connects devices within the LAN, such as computers, printers, and servers.

Each device is connected to a port on the switch, forming a local network where devices can communicate directly with each other.

Switches enable fast and efficient data transfer within the LAN by sending data only to the intended recipient device.

11.Types of Cable - explain types of Ethernets and speed

Ans: Ethernet cables are used to connect devices in a local area network (LAN). There are several types, each with different capabilities and speeds:

Cat 5e (Category 5e): Supports speeds up to 1 Gigabit per second (Gbps) over short distances. Commonly used in homes and small businesses.

Cat 6 (Category 6): Supports speeds up to 10 Gbps over short distances. Often used in larger networks and for higher bandwidth requirements.

Cat 6a (Category 6a): Supports speeds up to 10 Gbps over longer distances compared to Cat 6. Suitable for enterprise networks and data centers.

Cat 7 (Category 7): Supports speeds up to 10 Gbps over longer distances and offers better shielding against interference. Used in high-performance networks and environments where reliability is critical.

12.

Ans;

**IP (Internet Protocol)**:

Responsible for addressing and routing packets of data so they can travel across networks.

Versions include IPv4 and IPv6.

**TCP (Transmission Control Protocol**):

Provides reliable, connection-oriented communication between devices.

Ensures data delivery by handling error-checking, packet sequencing, and acknowledgment.

**UDP (User Datagram Protocol)**:

Provides connectionless, unreliable communication.

Used for applications where speed is more critical than reliability, like real-time audio/video streaming and online gaming.

**HTTP (Hypertext Transfer Protocol)**:

Used for transmitting web pages and other resources over the internet.

Standard protocol for browsing the web.

**HTTPS (Hypertext Transfer Protocol Secure)**:

Secure version of HTTP that encrypts data to ensure secure communication over the internet, commonly used for online transactions and sensitive information exchange.

**FTP (File Transfer Protocol)**:

Used for transferring files between a client and a server on a network.

Allows users to upload and download files.

**SMTP (Simple Mail Transfer Protocol):**

Used for sending emails between servers.

Responsible for the transmission of email messages over the internet.

**POP3 (Post Office Protocol version 3):**

Used by email clients to retrieve emails from a remote server.

Allows users to download emails to their devices.

**IMAP (Internet Message Access Protocol)**:

Similar to POP3, used by email clients to retrieve emails from a remote server.

Allows users to view and manage emails stored on the server without downloading them.

**TFTP (Trivial File Transfer Protocol):**

TFTP allows devices to transfer files, such as firmware or configuration files, over a network. It's commonly used for tasks like updating router firmware.

**DHCP (Dynamic Host Configuration Protocol)**

It assigns IP addresses dynamically or automatically to devices on a network, making it easier to manage large networks.

**DNS (Domain Name System)**:

Translates domain names (e.g., [www.example.com](http://www.example.com/" \t "https://chatgpt.com/c/_new)) into IP addresses.

**Port Numbers**:

HTTP: Port 80

HTTPS: Port 443

FTP: Port 20 (data transfer) and Port 21 (control)

SMTP: Port 25

POP3: Port 110

IMAP: Port 143

DHCP: port 67 (server) and 68 (client)

DNS : port 53

TFTP: port 69

1. Explain Node(backborn) and Physical layer.

Ans. **Node (Backbone)**:

Definition: A backbone node is a device that connects different parts of a network together.

Function: It helps in directing data traffic between different segments of the network.

Example: In a large office network, a backbone node might be a powerful router connecting different floors or departments.

**Physical Layer**:

Definition: The physical layer is responsible for transmitting data over the physical network medium.

Function: It handles the actual hardware connections, like cables and connectors, ensuring data is transmitted reliably.

Example: When you connect your computer to the internet with an Ethernet cable, the physical layer ensures the electrical signals travel between devices accurately.

**Module – 2**

1. Describe IPv4 address range and explain example of subnetting.

Ans; IPv4 addresses are 32-bit numerical addresses written in a dotted-decimal format (e.g., 192.168.1.1) and are used to uniquely identify devices on a network. The IPv4 address space is divided into several classes, and each class has a specific range of addresses.

Range

Class A ip range : 0-127

Class B ip range : 128- 191

Class c ip range : 192 - 223

Class d ip range : 224 - 239

1. List of private address.

Ans. Private IP addresses are reserved for use within private networks and are not routable over the public internet. The following ranges are designated as private IP address ranges according to RFC 1918:

Class A: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)

Class B: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)

Class C: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

1. What is routing? Explain work of Router and protocol.

Ans; Routing is like finding the best route on a map to get from one place to another. A router is like a traffic cop that decides which way data packets should go to reach their destination. It uses routing protocols to share information with other routers and figure out the fastest and most efficient paths for data to travel through a network.

**Distance Vector Protocols:**

Examples: RIP (Routing Information Protocol)

Based on hop count and periodically broadcast routing tables to neighboring routers.

**Link State Protocols:**

Examples: OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System)

Based on the complete topology of the network and calculate the shortest path to each destination.

**Hybrid Protocols**:

Examples: EIGRP (Enhanced Interior Gateway Routing Protocol)

Combines elements of both distance vector and link state protocols.

1. Which software we are use for routing and switching.

Ans. Cisco Packet tracer

1. • Types of Routing – example of Static routing.

Ans: There are two types of routing

1. Static Routing
2. Dynamic Routing

**static routing**, network administrators manually configure routing tables on routers.

Routes remain fixed unless manually changed by an administrator.

Suitable for small, simple networks where the network topology rarely changes.

Example: Configuring a router to send all traffic destined for a specific network through a particular interface.

1. Explain Dynamic routing

Ans: Dynamic routing protocols automatically update routing tables based on network topology changes.

Routers communicate with each other to share routing information and adapt to changes.

Suitable for larger, complex networks where network topology changes frequently.

Examples: OSPF (Open Shortest Path First), RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol).

1. Deference btw RIP EIGRP and OSPF

Ans;

| Feature | RIP | EIGRP | OSPF |
| --- | --- | --- | --- |
| Type | Distance Vector | Hybrid (Distance Vector + Link-State) | Link-State |
| Metric | Hop Count | Composite metric based on bandwidth, delay, reliability, and load | Shortest Path First |
| Updates | Periodic full updates | Partial updates based on changes | Periodic updates (LSAs) |
| Convergence | Slow | Faster than RIP, slower than OSPF | Fast |
| Complexity | Simple configuration | More complex than RIP, simpler than OSPF | More complex |
| Scaling | Limited scalability | Good scalability | Highly scalable |
| Example | RIP version 2 (RIPv2) | Proprietary to Cisco devices | OSPF version 2 |

1. Example of Default routing.

Ans:   
In default routing, also known as default gateway routing, a router is configured to forward all packets with destinations outside of its known routes to a specific next-hop router, often referred to as the default gateway.

Example:

Let's say you have a small office network with multiple computers connected to a router for internet access. The router's WAN interface is connected to the internet, and its LAN interface is connected to the office network.

1. Explain Autonomous system number

Ans; An Autonomous System Number (ASN) is a unique identifier assigned to a network or an organization that participates in the Border Gateway Protocol (BGP). BGP is a routing protocol used to exchange routing information between different autonomous systems on the internet

1. What is switching explain VLAN?

Ans; Switching: Sending data packets to the right device within a local network based on MAC addresses.

VLAN (Virtual Local Area Network): Creating virtual groups within a network to logically separate and manage traffic for better security and performance.

1. What is Access port and trunk port?

Ans. **Access Port:**

Purpose: Access ports are used to connect end devices, such as computers, printers, or IP phones, to a switch.

Functionality: Each access port is typically assigned to a single VLAN, and it carries traffic only for that VLAN.

**Trunk Port:**

Purpose: Trunk ports are used to interconnect switches or to connect switches to routers or other network devices.

Functionality: Trunk ports can carry traffic for multiple VLANs simultaneously by tagging each packet with a VLAN identifier.

1. List of basic SHOW command

Ans;

**show ip interface brief**:

Displays a brief summary of the IP interfaces configured on the router, including their IP addresses, status, and protocol.

**show running-config**:

Displays the current running configuration of the router, including interface configurations, routing protocols, and other settings.

**show ip route**:

Displays the routing table of the router, showing the known routes and their next-hop addresses.

**show interfaces**:

Displays detailed information about the interfaces on the router, including their status, configuration, and counters.

**show vlan brief**:

Displays a brief summary of VLAN configurations on a switch, showing VLAN IDs, names, and status.

show mac address-table:

Displays the MAC address table of a switch, showing MAC addresses and associated switch ports.

**show arp**:

Displays the ARP (Address Resolution Protocol) table, showing IP addresses and corresponding MAC addresses.

**show cdp neighbors**:

Displays information about neighboring Cisco devices discovered using the Cisco Discovery Protocol (CDP).

**show version**:

Displays information about the software version, hardware platform, and system uptime of the router or switch.

**show interfaces status**:

Displays the status of all interfaces on a switch, including their operational status, speed, and duplex mode.

1. Explain of Layer 2 and Layer 3 switch.

Ans; **Layer 2 Switch:**

Operates at: Data Link Layer (Layer 2) of the OSI model.

**Functionality:**

Forwards data packets based on MAC addresses.

Uses MAC address tables to make forwarding decisions.

Supports VLANs for network segmentation.

Provides basic switching functionalities such as MAC address learning, forwarding, and filtering.

Example Scenario: Connecting computers, printers, or IP phones within a LAN.

**Layer 3 Switch:**

Operates at: Network Layer (Layer 3) of the OSI model.

**Functionality:**

Performs routing functions in addition to switching.

Forwards data packets based on both MAC addresses and IP addresses.

Uses routing tables to make forwarding decisions.

Supports advanced routing protocols such as OSPF, EIGRP, and BGP.

Provides inter-VLAN routing and can perform Layer 3 switching between VLANs.

Example Scenario: Interconnecting multiple VLANs within a LAN and routing traffic between them.

1. Example of inter VLAN routing

Ans; **Spanning Tree Protocol (STP)**:

**Purpose**: Prevents loops in Ethernet networks to avoid broadcast storms and network instability.

**Operation**:

Elects a root bridge to serve as the reference point for the spanning tree.

Determines the best path from each switch to the root bridge.

Blocks redundant links to eliminate loops while maintaining network connectivity.

**Algorithm**: STP uses the following steps to build a loop-free topology:

**Root Bridge** : Each switch in the network determines its Bridge ID based on priority and MAC address. The switch with the lowest Bridge ID becomes the root bridge.

**Root Port Selection**: Each non-root switch selects the port with the lowest path cost to reach the root bridge as its root port.

**Designated Port Selection**: Each LAN segment selects one switch port as the designated port with the lowest path cost to the root bridge.

**Non-designated port** : Redundant ports are put into a blocking state to prevent loops, creating a loop-free tree structure.