Module -1

• Explain is the OSI reference model?

The **OSI (Open Systems Interconnection)** model is a conceptual framework used to understand and describe how different networking protocols work together to enable communication between devices over a network. It divides the networking process into **7 layers**, each with specific responsibilities:

* **Layer 1 (Physical Layer)**: Deals with the physical connection between devices, such as cables, switches, and the transmission of raw data bits.
* **Layer 2 (Data Link Layer)**: Ensures reliable communication over a physical link by handling error detection, frame synchronization, and MAC (Media Access Control) addressing.
* **Layer 3 (Network Layer)**: Handles routing of data packets between different devices on different networks. This layer uses IP addresses to route data.
* **Layer 4 (Transport Layer)**: Responsible for providing reliable data transfer between devices. It includes protocols like TCP and UDP that handle flow control, error checking, and data segmentation.
* **Layer 5 (Session Layer)**: Manages sessions or connections between devices, ensuring that communication remains open and organized.
* **Layer 6 (Presentation Layer)**: Deals with data format translation, encryption, and compression, ensuring that data can be understood by both the sender and receiver.
* **Layer 7 (Application Layer)**: The topmost layer that directly interacts with the end-user applications. It includes protocols like HTTP, FTP, and SMTP.

• What is a Network?

A **network** is a collection of devices (computers, servers, routers, etc.) connected together to share data, resources, and services. Networks can vary in size, from a local area network (LAN) connecting devices within a building to a wide-area network (WAN) covering large geographical areas. Networks enable communication and data transfer using various communication protocols.

• What are Routers?

A **router** is a network device that forwards data packets between computer networks. Routers operate at the **Network Layer (Layer 3)** of the OSI model and use IP addresses to determine the best path for forwarding packets. They connect multiple networks and can route data between different subnets, or between local networks and the internet.

• Explain Encapsulation.

**Encapsulation** is the process of adding headers and trailers to data as it moves down through the layers of the OSI model. Each layer of the model adds its own header or trailer to the data to provide necessary control information for that layer. The encapsulation process begins at the **Application Layer** and continues until the **Physical Layer**, where the data is transmitted over the network. When data reaches its destination, the reverse process (decapsulation) occurs, with headers and trailers being removed at each layer.

• Peer-to-Peer Communication.

**Peer-to-Peer (P2P)** communication refers to a decentralized network model where each device (or "peer") can act as both a client and a server. Peers can directly communicate with each other without needing a central server. Examples of P2P networks include file-sharing services like BitTorrent and communication apps like Skype.

• What is TCP and UDP?

 **TCP (Transmission Control Protocol)**: A connection-oriented protocol that ensures reliable data delivery. It breaks data into packets, assigns sequence numbers, and performs error-checking and retransmission if packets are lost or corrupted. TCP is used for applications requiring reliable data delivery, such as web browsing (HTTP) or email (SMTP).

 **UDP (User Datagram Protocol)**: A connectionless protocol that does not ensure reliable data delivery. It sends packets without checking for errors or ensuring they reach the destination. UDP is used for applications where speed is more important than reliability, such as video streaming or online gaming.

• What is Internetwork Operating System software?

**Internetwork Operating System (IOS)** is the software used on Cisco routers and switches to enable them to operate and manage network traffic. It provides the necessary protocols and commands for routing, switching, security, and network management.

• Explain LAN and draw any example.

A **LAN (Local Area Network)** is a network of devices connected in a limited geographical area, such as a home, office, or building. It typically uses Ethernet and Wi-Fi for communication. LANs allow devices to share resources like printers, files, and internet access.

**Example:** A simple LAN setup might include a router, several computers, and a printer, all connected to the router via wired or wireless connections.

• Explain Network Device - Router Switch and Hub.

 **Router**: A device that connects different networks (e.g., a LAN to the internet). It routes data between networks based on IP addresses.

 **Switch**: A device used within a network to forward data between devices (e.g., computers or printers) on the same local network. It operates at the Data Link Layer and uses MAC addresses to forward frames.

 **Hub**: A basic network device that connects multiple devices in a network, but unlike a switch, it broadcasts data to all devices, regardless of the destination. Hubs are less efficient than switches and operate at the Physical Layer.

• Describe Router and switch connection in LAN.

In a typical LAN, **routers** connect the local network to the outside world (such as the internet), while **switches** are used within the LAN to interconnect devices. Here's how they work together:

* The **router** connects to the internet (or other networks).
* The **switch** connects multiple devices (computers, printers, etc.) on the local network.
* The router provides an IP address to each device on the LAN (via DHCP) and forwards data packets between devices in the LAN and external networks.

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

Ethernet cables come in different categories, each supporting different speeds and uses:

* **Cat5 (Category 5)**: Supports speeds up to 100 Mbps and is used for older networks.
* **Cat5e (Category 5 enhanced)**: An improved version of Cat5, supporting speeds up to 1 Gbps (Gigabit Ethernet).
* **Cat6 (Category 6)**: Supports speeds up to 10 Gbps over short distances (up to 55 meters).
* **Cat6a (Category 6 augmented)**: Supports speeds up to 10 Gbps over longer distances (up to 100 meters).
* **Cat7 (Category 7)**: Supports speeds up to 10 Gbps and has better shielding to reduce interference.

• Explain TCP/IP -List of Protocol and port Number.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** is the suite of protocols that enable communication across the internet and other networks. Some common protocols and their default port numbers include:

* **HTTP (HyperText Transfer Protocol)**: Port 80
* **HTTPS (Secure HTTP)**: Port 443
* **FTP (File Transfer Protocol)**: Port 21
* **SMTP (Simple Mail Transfer Protocol)**: Port 25
* **DNS (Domain Name System)**: Port 53
* **IMAP (Internet Message Access Protocol)**: Port 143
* **POP3 (Post Office Protocol 3)**: Port 110
* **SSH (Secure Shell)**: Port 22
* **Telnet**: Port 23

• Explain Node(backborn) and Physical layer.

 **Node (Backbone)**: A **node** is any device connected to a network, such as a computer, router, or switch. The **backbone** refers to the high-capacity network infrastructure that interconnects various nodes or sub-networks. It carries the bulk of the network traffic and often operates at higher speeds than the rest of the network.

 **Physical Layer**: The **Physical Layer (Layer 1)** in the OSI model is responsible for transmitting raw data bits over physical media (such as cables, fiber optics, or wireless signals). It defines electrical, mechanical, and procedural aspects of data transmission, such as voltage levels, pin configurations, and data rates.

Module – 2

• Describe IPv4 address range and explain example of subnetting.

**Pv4 addresses** are 32-bit addresses divided into four octets (8 bits each), typically represented in dotted decimal format, like 192.168.1.1.

The **IPv4 address range** is from 0.0.0.0 to 255.255.255.255.

**Subnetting** is the process of dividing a larger IP network into smaller subnetworks (subnets). Each subnet will have its own range of IP addresses

• List of private address.

**Private IP addresses** are reserved for use within private networks and are not routable over the public internet. The following are the private IP address ranges:

* **Class A**: 10.0.0.0 - 10.255.255.255
* **Class B**: 172.16.0.0 - 172.31.255.255
* **Class C**: 192.168.0.0 - 192.168.255.255

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

**Routing** is the process of forwarding data packets from one network to another, ensuring that data reaches its correct destination. Routers are devices responsible for this process. They analyze the destination IP address of the packet and use routing tables or routing protocols to determine the best path.

* **Router**: A router connects different networks, either within an organization or between networks and the internet. It determines the optimal path for data using routing tables.
* **Routing Protocols**: These are protocols used by routers to exchange information about network paths. Examples include:
  + **RIP (Routing Information Protocol)**.
  + **OSPF (Open Shortest Path First)**.
  + **EIGRP (Enhanced Interior Gateway Routing Protocol)**.

• Which software we are use for routing and switching.

 **Cisco IOS (Internetwork Operating System)** is the most commonly used software for routing and switching on Cisco devices.

 Other vendors may use different operating systems such as **Juniper's Junos OS**, **Arista EOS**, or **Huawei's VRP**.

• Explain Basic command.

Basic network device commands (especially for Cisco routers/switches) include:

* **show ip interface brief**: Displays a brief summary of the router's interfaces.
* **ping**: Tests connectivity to another device.
* **traceroute**: Shows the path data takes to reach a destination.
* **show running-config**: Displays the current running configuration of the device.
* **configure terminal**: Enters configuration mode for making changes.

• Types of Routing – example of Static routing.

**Static Routing**: Involves manually configuring the routes on routers. The router’s administrator specifies the next hop and destination network. It is typically used for smaller, simple networks.

• Explain Dynamic routing.

**Dynamic Routing** uses routing protocols to automatically adjust and find optimal routes based on network changes. Dynamic routing protocols like RIP, EIGRP, and OSPF update routing tables dynamically as the network topology changes (such as device failures or new network additions).

• Deference btw RIP EIGRP and OSPF.

 **RIP (Routing Information Protocol)**:

* Distance-vector protocol.
* Uses hop count as the metric (max 15 hops).
* Updates every 30 seconds.
* Simpler but less scalable.

 **EIGRP (Enhanced Interior Gateway Routing Protocol)**:

* Advanced distance-vector protocol (Cisco proprietary).
* Uses a combination of distance-vector and link-state features.
* Faster convergence and more scalable than RIP.
* Supports variable-length subnet masks (VLSM) and classless inter-domain routing (CIDR).

 **OSPF (Open Shortest Path First)**:

* Link-state protocol.
* Scalable and faster convergence.
* Uses a more complex algorithm (Dijkstra).
* Supports large networks and hierarchical design (areas).
* Open standard and widely used.

• Perform Example of RIP EIGRP and OSPF with different area concept.

**RIP Example**: Router 1 (R1) can have RIP configured with router rip command and adding the network using network <network\_address>.

**EIGRP Example**: Configure EIGRP with router eigrp <AS\_number> and use network <network\_address> to specify which networks to advertise.

**OSPF Example**: Router 1 (R1) configured for OSPF with router ospf <process\_id> and define areas using network <network\_address> <wildcard\_mask> area <area\_id>. For example, for Area 0:

• Example of Default routing.

**Default Routing** is used when there is no specific route in the routing table for a destination. It's commonly used in edge routers that connect to the internet.

• Explain Autonomous system number.

An **Autonomous System Number (ASN)** is a unique identifier assigned to a collection of IP networks and routers under the same administrative control. ASNs are used in **BGP (Border Gateway Protocol)** to identify and route traffic between different networks.

* **Private ASNs**: Ranges from 64512 to 65535.
* **Public ASNs**: Assigned by the IANA and typically range from 1 to 64511.

• What is switching explain VLAN?

**Switching** is the process of forwarding data frames between devices on the same network, based on MAC addresses. A **VLAN (Virtual Local Area Network)** is a logical grouping of devices on different physical networks but treated as if they are on the same network. VLANs help segment networks for better performance, security, and management.

* **VLAN Example**: VLAN 10: 192.168.1.0/24 VLAN 20: 192.168.2.0/24 Devices in VLAN 10 can communicate with each other, and the same goes for VLAN 20. However, communication between different VLANs requires a **router** or **Layer 3 switch**.

• What is Access port and trunk port?

**Access Port**: A switch port that is assigned to a single VLAN. It connects end devices (like computers) to the network. For example, port 1 on a switch may be assigned to VLAN 10.

**Trunk Port**: A switch port used to carry traffic for multiple VLANs between switches or other network devices. It allows the transmission of tagged VLAN frames. For example, a port between two switches will typically be a trunk port, passing multiple VLANs.

• List of basic SHOW command.

**show ip interface brief**: Displays brief information about the router’s interfaces and their status.

**show running-config**: Displays the current configuration of the device.

**show ip route**: Displays the router's routing table.

**show vlan brief**: Displays information about VLANs on a switch.

**show version**: Displays system information, including hardware, software version, and uptime.

**show interfaces**: Displays detailed information about a specific interface, such as packets transmitted/received and errors.

Explain of Layer 2 and Layer 3 switch.

 **Layer 2 Switch**: A **Layer 2 switch** operates at the **Data Link Layer** (Layer 2) of the OSI model. It makes forwarding decisions based on MAC addresses, which are used to identify devices within the same network. Layer 2 switches are primarily used to connect devices within a local area network (LAN) and do not have routing capabilities. They create a **MAC address table** to forward frames between devices.

* **Example**: A Layer 2 switch receives data frames from one device and forwards them to another device within the same VLAN using MAC addresses.

 **Layer 3 Switch**: A **Layer 3 switch** operates at the **Network Layer** (Layer 3) of the OSI model. It has the ability to make forwarding decisions based on **IP addresses**, not just MAC addresses, and can route traffic between different VLANs (known as **Inter-VLAN Routing**). Layer 3 switches combine the functionality of both routers and switches.

* **Example**: A Layer 3 switch can route traffic between multiple VLANs (subnets) without needing a separate router.

• Example – VLAN Access port and trunk port.

**VLAN Access Port**: An **access port** is used to connect a device to a single VLAN. It is assigned to one VLAN and carries traffic for only that VLAN.

* **Example**:
  + Port GigabitEthernet0/1 on a switch is configured as an access port and assigned to **VLAN 10**.

• Example of inter VLAN routing.

**Inter-VLAN routing** allows devices in different VLANs to communicate with each other. This is typically done using a **Layer 3 switch** or a **router**.

* **Example**: Assume you have two VLANs:
  + **VLAN 10**: 192.168.10.0/24
  + **VLAN 20**: 192.168.20.0/24

On a **Layer 3 switch**, you can configure **SVIs (Switched Virtual Interfaces)** for each VLAN to enable routing between them:

interface Vlan10

ip address 192.168.10.1 255.255.255.0

no shutdown

interface Vlan20

ip address 192.168.20.1 255.255.255.0

no shutdown

After configuring the SVIs, the switch will perform routing between VLAN 10 and VLAN 20.

On the router or Layer 3 switch, the default gateway for devices in VLAN 10 will be 192.168.10.1 and for VLAN 20, it will be 192.168.20.1.

• Explain switching method and VTP.

 **Switching Methods**:

* **Store and Forward**: In this method, the switch receives the entire frame, checks for errors (CRC), and then forwards it to the appropriate port. It ensures that only error-free frames are forwarded.
* **Cut-Through**: In this method, the switch forwards the frame as soon as it has read the destination MAC address, without waiting to receive the entire frame. This results in faster forwarding but can propagate errors.
* **Fragment-Free**: This method is a hybrid between Store and Forward and Cut-Through. It begins forwarding the frame after receiving the first 64 bytes to ensure no collision has occurred.

 **VTP (VLAN Trunking Protocol)**: **VTP** is a Cisco proprietary protocol used to manage VLANs across multiple switches in a network. It allows VLAN configuration changes (such as adding or deleting VLANs) to be propagated automatically to other switches in the same VTP domain.

• What is spanning Tree – Mention spanning tree protocol and algorithm.

**Spanning Tree Protocol (STP)** is a network protocol used to prevent **loops** in Ethernet networks. STP ensures that there is only one active path between two devices by dynamically blocking redundant paths. It uses an algorithm to elect a **root bridge** and then calculates the **best path** for traffic.

* **Spanning Tree Algorithm**:
  + **Root Bridge Election**: The switch with the lowest **Bridge ID** (based on MAC address and priority) becomes the root bridge.
  + **Path Selection**: Once the root bridge is elected, the algorithm calculates the shortest path from each switch to the root bridge.

**STP Protocols**:

* + **IEEE 802.1D**: The original standard for STP.
  + **RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w)**: An enhancement to STP, designed to reduce convergence time.
  + **MSTP (Multiple Spanning Tree Protocol, IEEE 802.1s)**: A protocol that allows multiple spanning trees within a network, helping with load balancing and efficiency.

• Example of Per VLAN spanning tree.

**Per VLAN Spanning Tree (PVST)** is a Cisco proprietary protocol that runs a separate instance of STP for each VLAN in the network. It allows different VLANs to have different root bridges and topologies.

• What is IPv6? Explain types and ip address range.

**IPv6 (Internet Protocol version 6)** is the most recent version of the IP protocol, designed to address the limitations of IPv4, including address space and network performance.

* **IPv6 Address Format**: IPv6 addresses are **128 bits** long, written as 8 groups of 4 hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
* **Types of IPv6 Addresses**:
  + **Unicast**: Refers to a single sender and a single receiver.
  + **Multicast**: Refers to a single sender and multiple receivers.
  + **Anycast**: Refers to a single sender and the nearest of multiple possible receivers.
* **IPv6 Address Ranges**:
  + **Global Unicast**: 2000::/3 (Publicly routable addresses).
  + **Link-Local**: fe80::/10 (Used for communication within a local network segment).
  + **Multicast**: ff00::/8 (Used for one-to-many communication)

• Example of Ipv6 – RIP

**RIPng (Routing Information Protocol next generation)** is the version of RIP used with IPv6. It works similarly to RIP for IPv4, exchanging routing information using a distance-vector approach.