**Module 1**

**OSI Reference Model**

The OSI (Open Systems Interconnection) reference model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. These layers facilitate interoperability between different systems by defining clear communication protocols and functions for each layer. The layers are:

Physical Layer: Deals with the physical transmission of data over the network medium, such as cables, wires, or wireless signals.

Data Link Layer: Responsible for the reliable transmission of data frames between adjacent network nodes, including error detection and correction.

Network Layer: Manages the routing of data packets across interconnected networks, addressing, and logical network topology.

Transport Layer: Ensures reliable end-to-end data delivery between hosts, including segmentation, flow control, and error recovery.

Session Layer Establishes, maintains, and terminates connections between applications on different devices.

Presentation Layer: Translates data formats between application and network formats, handling data encryption, compression, and formatting.

Application Layer: Provides network services directly to end-users and applications, such as file transfer, email, and web browsing.

**Network**

A network is a collection of interconnected devices and systems that can communicate with each other to share resources and information. Networks can be classified based on their geographical scope, such as LANs (Local Area Networks), MANs (Metropolitan Area Networks), and WANs (Wide Area Networks). They can also be categorized by their architecture, such as peer-to-peer networks, client-server networks, and distributed networks

**Routers**

Routers are network devices that operate at the network layer (Layer 3) of the OSI model. They are responsible for forwarding data packets between different networks based on IP addresses. Routers analyse the destination IP address of incoming packets and determine the most efficient path for forwarding the packets to their destination. They help in directing traffic between interconnected networks and enable communication between devices on different networks.

**Encapsulation:**

Encapsulation is a process in networking where data is wrapped with additional information as it moves through the OSI layers. Each layer adds its own header (and sometimes trailer) to the data, creating a data packet at each layer. This process is essential for ensuring that data can be transmitted across different network technologies and protocols. Encapsulation also provides a structured format for data transmission and helps in error detection and correction.

**Peer to peer communication:**

Peer-to-peer communication is a decentralized model of network communication where devices, called peers, communicate directly with each other without the need for a central server. In this model, each peer can act as both a client and a server, exchanging data and resources with other peers on the network. Peer-to-peer networks are often used for file sharing, collaborative applications, and distributed computing.

**TCP and UDP**

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two transport layer protocols used for communication between devices over a network.

TCP provides reliable, connection-oriented communication by establishing a connection between sender and receiver, ensuring data delivery, and managing flow control and error recovery mechanisms.

UDP provides unreliable, connectionless communication by sending data packets without establishing a connection or ensuring delivery. UDP is used in applications where real-time data transmission and low overhead are more important than reliability, such as streaming media and online gaming.

**Internetwork Operating System software:**

Internetwork Operating System (IOS) software is a proprietary operating system developed by Cisco Systems for managing and operating Cisco networking devices, including routers and switches. IOS provides a command-line interface (CLI) for configuring, monitoring, and troubleshooting network devices, as well as features such as security, routing, and network management.

**LAN (Local Area Network):**

A LAN is a network that spans a small geographical area, such as a single building or campus. LANs typically use high-speed Ethernet connections to connect devices within the same physical location. An example of a LAN could be a network within an office building, connecting computers, printers, and servers to facilitate local communication and resource sharing.

**Network Devices - Router, Switch, and Hub**:

Router: A router is a networking device that forwards data packets between networks based on IP addresses. It operates at the network layer (Layer 3) of the OSI model and helps in directing traffic between interconnected networks.

Switch: A switch is a networking device that connects multiple devices within a single network. It operates at the data link layer (Layer 2) of the OSI model and uses MAC addresses to forward data packets to the appropriate destination device within the same network.

Hub: A hub is a basic networking device that connects multiple devices in a LAN. Unlike switches, hubs operate at the physical layer (Layer 1) of the OSI model and simply broadcast data packets to all connected devices, regardless of the intended destination. Hubs are less efficient than switches and are rarely used in modern networks.

**Router and Switch Connection in LAN:**

In a LAN, routers and switches are interconnected to facilitate communication between devices within the same network and between different networks.

Routers connect different LANs or LAN segments and manage traffic between them, ensuring that data packets are routed to the correct destination.

Switches connect devices within the same LAN and forward data packets directly to the intended destination device based on its MAC address, improving network performance and efficiency.

**Types of Cable - Types of Ethernets and Speed:**

Types of Ethernet cables commonly used in LANs include:

**Category 5e (Cat5e):** Supports speeds up to 1 Gbps and is suitable for most Ethernet applications.

**Category 6 (Cat6):** Supports speeds up to 10 Gbps and provides better performance and bandwidth compared to Cat5e.

**Category 6a (Cat6a):** Supports speeds up to 10 Gbps over longer distances and provides improved crosstalk and interference reduction compared to Cat6.

**Category 7 (Cat7):** Supports speeds up to 10 Gbps and provides even better performance and shielding against crosstalk and interference.

The choice of Ethernet cable depends on factors such as required speed, distance, and network environment.

**TCP/IP - List of Protocols and Port Numbers:**

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols used for transmitting data over networks, including the Internet.

Common TCP/IP protocols and their associated port numbers include:

**HTTP (Hypertext Transfer Protocol): Port 80**

**HTTPS (Hypertext Transfer Protocol Secure): Port 443**

**FTP (File Transfer Protocol): Port 21**

**SMTP (Simple Mail Transfer Protocol): Port 25**

**DNS (Domain Name System): Port 53**

**DHCP (Dynamic Host Configuration Protocol): Port 67/68**

**SSH (Secure Shell): Port 22**

**Telnet: Port 23**

**SNMP (Simple Network Management Protocol): Port**

**Module :2**

**IPv4 Address Range and Subnetting:**

IPv4 addresses are 32-bit numerical identifiers represented in dotted-decimal notation (e.g., 192.168.1.1). The IPv4 address space is divided into several classes, but the most commonly used method for subnetting is Classless Inter-Domain Routing (CIDR). CIDR allows for flexible allocation of IP addresses by specifying both the network prefix and the number of significant bits in the address. For example, in the address 192.168.1.0/24, the /24 indicates that the first 24 bits represent the network portion, leaving 8 bits for host addresses.

Private IP Address Range: Private IP addresses are reserved for use within private networks and are not routable over the public Internet. The following ranges are reserved for private use:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

**Routing and Routers:**

Routing is the process of selecting paths in a network along which to send network traffic. Routers are devices responsible for forwarding data packets between computer networks. They use routing tables to determine where to forward packets based on their destination IP addresses. Routing protocols, such as OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol), are used by routers to exchange routing information and make dynamic routing decisions.

**Software for Routing and Switching:**

Commonly used software for routing and switching include Cisco IOS (Internetwork Operating System) for Cisco devices, Juniper Junos for Juniper devices, and various open-source routing and switching software like Quagga and Open vSwitch.

Basic Commands: Some basic commands used in networking include:

**ping: Tests reachability to a host by sending ICMP echo requests.**

**tracert (Windows) / traceroute (Unix): Displays the route packets take to reach a destination.**

**ipconfig (Windows) / ifconfig (Unix): Displays network interface configuration.**

**show ip route: Displays the routing table on Cisco routers.**

Types of Routing: Static Routing: Involves manually configuring routing information into the router's routing table. It requires manual intervention and does not adapt to changes in the network topology automatically.

Dynamic Routing: Involves routers dynamically exchanging routing information using routing protocols. Dynamic routing protocols automatically update routing tables in response to network changes.

Difference between RIP, EIGRP, and OSPF: RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and OSPF are all routing protocols used to exchange routing information between routers. However, they differ in terms of their operation, scalability, and convergence speed.

RIP: A distance-vector routing protocol that uses hop count as its metric. Limited to small networks due to its slow convergence and limited scalability.

EIGRP: A Cisco proprietary routing protocol that combines aspects of both distance-vector and link-state routing protocols. It supports faster convergence and scalability compared to RIP.

OSPF: A link-state routing protocol that uses a shortest path first algorithm to calculate routes. It scales well and converges quickly, making it suitable for large networks.

Autonomous System Number (ASN): An Autonomous System (AS) is a collection of IP networks and routers under the control of one entity that presents a common routing policy to the Internet. Each AS is assigned a unique ASN by a regional Internet registry (RIR). ASNs are used by exterior routing protocols like BGP to identify individual networks on the Internet.

Switching and VLANs: Switching is the process of forwarding data frames between devices in a network. VLANs (Virtual Local Area Networks) are used to segment a single physical network into multiple logical networks, allowing for better network management, security, and traffic control.

Access Port and Trunk Port: An access port is a switch port that is assigned to a single VLAN and carries traffic only for that VLAN. A trunk port is a switch port that carries traffic for multiple VLANs, typically used to interconnect switches or connect a switch to a router.

Basic SHOW Commands: Some basic SHOW commands used in networking include:

**show interfaces: Displays information about interfaces on a device.**

**show ip route: Displays the routing table.**

**show vlan: Displays VLAN information.**

**show spanning-tree: Displays Spanning Tree Protocol (STP) information.**

Layer 2 and Layer 3 Switches: Layer 2 switches operate at the data link layer of the OSI model and forward traffic based on MAC addresses. Layer 3 switches operate at the network layer and can perform routing functions in addition to switching.

Inter-VLAN Routing: Inter-VLAN routing is the process of forwarding traffic between VLANs. This can be accomplished using a router or a Layer 3 switch.

Switching Methods and VTP: Switching methods include store-and-forward, cut-through, and fragment-free. VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used to manage VLAN configuration consistency across a network.

Spanning Tree Protocol (STP): STP is a network protocol that prevents loops in a switched network topology by dynamically disabling selected redundant links.

IPv6: IPv6 is the successor to IPv4, designed to address the exhaustion of IPv4 addresses and improve upon its features. IPv6 addresses are 128 bits long, allowing for a significantly larger address space. IPv6 addresses are typically represented in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Example of IPv6 – RIP: IPv6 supports routing protocols similar to IPv4, including RIPng (Routing Information Protocol next generation) for IPv6. RIPng operates similarly to RIP but uses IPv6 addresses and has support for larger networks.