**CCNA**

**Module-1**

**Assignment – 6**

1. OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

Physical Layer:

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

Key Aspects: Transmission of raw bit streams over a physical medium. It includes electrical, mechanical, and procedural specifications.

Examples: Ethernet cables, USB, and RS-232.

Data Link Layer:

Function: Provides node-to-node data transfer and handles error correction from the physical layer.

Key Aspects: Framing, physical addressing (MAC addresses), and error detection and correction.

Examples: Ethernet, PPP (Point-to-Point Protocol), and MAC (Media Access Control).

Network Layer:

Function: Manages device addressing, tracks the location of devices on the network, and determines the best way to move data.

Key Aspects: Logical addressing (IP addresses), routing, and packet forwarding.

Examples: IP (Internet Protocol), ICMP (Internet Control Message Protocol), and routers.

Transport Layer:

Function: Ensures complete data transfer and provides error recovery and flow control.

Key Aspects: Segmentation, acknowledgments, and retransmission of data.

Examples: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Session Layer:

Function: Manages sessions or connections between applications.

Key Aspects: Establishing, maintaining, and terminating connections.

Examples: NetBIOS, PPTP (Point-to-Point Tunneling Protocol), and session establishment in RPC (Remote Procedure Call).

Presentation Layer:

Function: Translates data between the application layer and the network format. It is responsible for data encryption, compression, and translation.

Key Aspects: Data encoding, encryption, and compression.

Examples: SSL/TLS (Secure Sockets Layer/Transport Layer Security), JPEG, and ASCII.

Application Layer:

Function: Provides network services directly to user applications.

Key Aspects: Interface between network services and end-user applications.

Examples: HTTP, FTP, SMTP (Simple Mail Transfer Protocol), and DNS (Domain Name System).

1. A network is basically a collection of computers and other devices that are linked together to exchange data.
2. A router is a device that connects two or more packet-switched networks or subnetworks.
3. Encapsulation is a concept used in object-oriented programming to bundle data and methods into easy-to-use units.
4. Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session.
5. Transmission control protocol (TCP) and user datagram protocol (UDP) are foundational pillars of the internet, enabling different types of data transmission from a network source to the destination. TCP is more reliable, while UDP prioritizes speed and efficiency.
6. Cisco IOS (Internetwork Operating System) is a collection of proprietary operating systems (OSes) that run on Cisco Systems hardware, including routers, switches and other network devices.
7. A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
8. Routers connect multiple networks and determine the best path for data transmission based on IP addresses.

* Switches connect devices within a network and enable efficient data transfer using MAC addresses.
* Hubs, on the other hand, simply broadcast data to all connected devices.

1. Just as a switch connects multiple devices to create a network, a router connects multiple switches, and their respective networks, to form an even larger network. These networks may be in a single location or across multiple locations. When building a small business network, you will need one or more routers.
2. Category Max. Data Rate Usage

Category 5 100 Mbps 100BaseT Ethernet

Category 5e 1 Gbps 100BaseT Ethernet, residential homes

Category 6 1 Gbps Gigabit Ethernet, commercial buildings

Category 6a 10 Gbps Gigabit Ethernet in data centers and commercial buildings

1. The TCP/IP protocol suite is the fundamental communication architecture of the Internet and many private networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol and encompasses a suite of communication protocols used to interconnect network devices on the internet.

Protocols and Ports

* HTTP: 80
* HTTPS: 443
* FTP: 21 (command), 20 (data)
* SMTP: 25
* IMAP: 143
* POP3: 110
* DNS: 53
* Telnet: 23
* SSH: 22
* TFTP: 69
* SNMP: 161
* RDP: 3389

1. A node in a network refers to any device or point that can send, receive, or forward information. Nodes can be computers, servers, switches, routers, or other networking devices. In the context of a backbone network, nodes play a critical role in ensuring data is transmitted efficiently across the network.

* Physical Layer:- The Physical Layer is the first layer of the OSI (Open Systems Interconnection) model. It is responsible for the physical connection between devices and the transmission and reception of raw binary data over a physical medium.

**Module – 2**

1. IPv4 Address Range

IPv4 (Internet Protocol version 4) addresses are 32-bit numerical labels used to identify devices on a network. They are written in the form of four decimal numbers separated by dots, known as "dotted-decimal" notation. Each of the four numbers can range from 0 to 255. An example of an IPv4 address is 192.168.1.1.

Address Classes

IPv4 addresses are categorized into five classes (A, B, C, D, and E), based on the leading bits of the address:

Class A: 1.0.0.0 to 126.0.0.0 (0.0.0.0 to 0.255.255.255 and 127.0.0.0 to 127.255.255.255 are reserved)

Class B: 128.0.0.0 to 191.255.0.0

Class C: 192.0.0.0 to 223.255.255.0

Class D: 224.0.0.0 to 239.255.255.255 (Multicast)

Class E: 240.0.0.0 to 255.255.255.255 (Experimental)

Subnetting

Subnetting is a process of dividing a larger network into smaller, more manageable sub-networks (subnets). This is done by extending the default subnet mask.

Example

Determine the number of bits to borrow:

4 subnets require 2 bits because 2^2 = 4.

New subnet mask:

The default subnet mask is 255.255.255.0 (/24).

Borrowing 2 bits, the new subnet mask becomes 255.255.255.192 (/26).

Calculate the subnets:

Each subnet will have 64 addresses (2^(32-26) = 64).

However, each subnet will have 62 usable addresses (64-2 for network and broadcast addresses).

Subnet ranges:

Subnet 1: 192.168.1.0 - 192.168.1.63 (192.168.1.0 network address, 192.168.1.63 broadcast address)

Subnet 2: 192.168.1.64 - 192.168.1.127 (192.168.1.64 network address, 192.168.1.127 broadcast address)

Subnet 3: 192.168.1.128 - 192.168.1.191 (192.168.1.128 network address, 192.168.1.191 broadcast address)

Subnet 4: 192.168.1.192 - 192.168.1.255 (192.168.1.192 network address, 192.168.1.255 broadcast address)

1. the ranges of private IPv4 addresses:

Class A Private Address Range: 10.0.0.0 to 10.255.255.255

Class B Private Address Range: 172.16.0.0 to 172.31.255.255

Class C Private Address Range: 192.168.0.0 to 192.168.255.255

1. Routing is the process of selecting paths in a network along which to send network traffic. This is done by routing devices such as routers, which analyze information about the destination of a data packet and determine the best path for it to take through the network to reach its destination.

How Routers Work:

Receiving Data: Routers receive data packets from various sources, whether from a local device within the same network or from another network.

Analyzing Destination: They examine the destination IP address of the incoming packet to determine where it needs to go.

Routing Decision: Routers consult their routing tables, which contain information about available network paths, to determine the best path for the packet to take.

Forwarding: Once the best path is determined, the router forwards the packet to the next hop along that path. This next hop could be another router or the final destination device.

Repeat: This process is repeated at each router along the path until the packet reaches its final destination.

Routing Protocols:

Routing protocols are sets of rules that routers use to communicate with each other and share information about network paths. They help routers build and maintain accurate routing tables, ensuring efficient routing of data packets.

1. Cisco IOS (Internetwork Operating System): Cisco routers typically run Cisco IOS, a proprietary operating system designed for Cisco networking devices. It provides routing, switching, and security features.

Cisco IOS (Cisco Catalyst Switches): Cisco Catalyst switches typically run Cisco IOS or Cisco IOS XE, offering advanced switching functionalities along with routing features in some models.

1. Two main types:

static routing and dynamic routing.

Example of Static Routing

Consider a small network with three routers connected in a linear topology:

Router A is directly connected to Router B.

Router B is directly connected to Router C.

Each router is assigned IP addresses as follows:

Router A: 192.168.1.1/24

Router B: 192.168.1.2/24 and 10.0.0.1/24

Router C: 10.0.0.2/24

1. Dynamic routing, also called adaptive routing, is a process where a router can forward data via a different route for a given destination based on the current conditions of the communication circuits within a system.
2. RIP (Routing Information Protocol):

Distance Vector Protocol: RIP is a distance vector routing protocol.

Metric: RIP uses hop count as its metric. Each hop between routers adds one to the hop count.

Convergence Time: RIP has slower convergence compared to other routing protocols because it relies on periodic updates and does not support triggered updates.

Scaling: RIP is suitable for small to medium-sized networks but can become inefficient in large networks due to its limitations.

Compatibility: RIP is a simple and widely supported protocol, making it suitable for basic network configurations.

EIGRP (Enhanced Interior Gateway Routing Protocol):

Advanced Features: EIGRP is an advanced distance vector routing protocol with features of link-state protocols.

Metric: EIGRP uses a composite metric based on bandwidth, delay, reliability, load, and MTU.

Convergence Time: EIGRP has faster convergence compared to traditional distance vector protocols because it supports triggered updates and maintains a topology table.

Scalability: EIGRP is suitable for medium to large networks and provides efficient use of bandwidth and scalability.

Cisco Proprietary: EIGRP is a Cisco proprietary protocol, meaning it's primarily used in Cisco environments.

OSPF (Open Shortest Path First):

Link-State Protocol: OSPF is a link-state routing protocol.

Metric: OSPF uses cost as its metric, which is based on the bandwidth of the link.

Convergence Time: OSPF has faster convergence compared to distance vector protocols because it uses triggered updates and maintains a detailed database of the network topology.

Scalability: OSPF is highly scalable and suitable for large networks, including enterprise and service provider networks.

Standard Protocol: OSPF is an open standard protocol, meaning it's not vendor-specific and is widely supported by various networking vendors.

1. Routing Protocol Examples:

RIP:

All routers in the network are configured with RIP.

Routers exchange routing updates every 30 seconds.

All routers maintain the same routing table with the same routes.

EIGRP:

Routers A and B belong to Area 0 and use EIGRP AS 100.

Router C belongs to Area 1 and uses EIGRP AS 200.

Routers in Area 0 share routes with each other and routers in Area 1.

Routers in Area 1 share routes with each other and routers in Area 0.

EIGRP calculates routes based on the composite metric (bandwidth, delay, reliability, load, and MTU).

OSPF:

Routers A and B belong to Area 0 (Backbone Area) and use OSPF.

Router C belongs to Area 2 and uses OSPF.

Routers in Area 0 share routes with each other and routers in other areas.

Routers in other areas (e.g., Area 1) can reach routes in Area 0 via OSPF.

OSPF uses different types of LSAs to exchange routing information between routers in the same area and routers in different areas.

1. A default route identifies the gateway IP address to which the threat defense device sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0. 0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.
2. An autonomous system number is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems.
3. Switching is a networking technique used to forward data packets between devices within a local area network (LAN). A network switch is a device that operates at the data link layer (Layer 2) of the OSI model and uses MAC addresses to forward data frames to their destination devices. Switches are essential components in modern network infrastructures, providing efficient and high-speed connectivity between devices.

VLAN (Virtual Local Area Network):

A VLAN is a logical segmentation of a physical LAN into multiple virtual LANs. VLANs allow network administrators to group devices together logically, regardless of their physical location, and isolate traffic between different groups. Each VLAN operates as a separate broadcast domain, meaning that broadcast traffic within one VLAN does not propagate to devices in other VLANs.

1. Access Port:

An access port is a switch port configured to carry traffic for a single VLAN. Devices connected to access ports are typically end-user devices such as computers, printers, IP phones, or other network devices that do not need to communicate with multiple VLANs.

Trunk Port:

A trunk port is a switch port configured to carry traffic for multiple VLANs simultaneously. Trunk ports are used to interconnect switches or to connect switches to routers or other network devices that need to carry traffic for multiple VLANs.

1. Layer 2 Switch:

A Layer 2 switch operates at the data link layer (Layer 2) of the OSI model. Its primary function is to forward frames based on the MAC (Media Access Control) addresses of devices connected to it.

Layer 3 Switch:

A Layer 3 switch operates at the network layer (Layer 3) of the OSI model. In addition to the functions of a Layer 2 switch, a Layer 3 switch can perform routing functions, making forwarding decisions based on IP addresses.

1. VLAN Configuration:

Access Port Configuration:

Let's configure an access port on the switch for a specific VLAN (VLAN 10) to which a computer is connected.

Example

Switch(config)# interface GigabitEthernet0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Trunk Port Configuration:

Let's configure a trunk port on the switch to connect to a router, allowing traffic for multiple VLANs (VLAN 10 and VLAN 20) to pass through.

Example

Switch(config)# interface GigabitEthernet0/24

Switch(config-if)# switchport mode trunk

1. Inter-VLAN routing allows communication between devices in different VLANs by routing traffic between VLANs. Here's an example scenario demonstrating inter-VLAN routing using a router with subinterfaces and a Layer 2 switch with VLANs configured:

Example Scenario:

Router: A router capable of inter-VLAN routing, connected to a Layer 2 switch.

Layer 2 Switch: A switch with VLANs configured and multiple devices connected to it.

Devices: Several end-user devices connected to the switch, grouped into different VLANs (VLAN 10 and VLAN 20)

1. Switching Methods:

Switching methods refer to the techniques used by network switches to forward data frames from source devices to destination devices within a local area network (LAN).

VLAN Trunking Protocol (VTP):

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used to manage VLAN configurations across a network of switches. VTP simplifies VLAN management by allowing VLAN information to be automatically propagated to all switches within the same VTP domain.

1. Spanning Tree Protocol (STP):

STP operates on bridges and switches to prevent loops by creating a loop-free topology. The protocol elects a root bridge, selects designated and root ports on each switch, and blocks non-designated ports to ensure that only one active path exists between any pair of switches. STP uses Bridge Protocol Data Units (BPDUs) to exchange information between switches and determine the network topology.

Spanning Tree Algorithm:

The original Spanning Tree Algorithm (STA) was developed by Dr. Radia Perlman in the 1980s. The algorithm works as follows:

Root Bridge Election:

Each switch in the network participates in the election process to determine the root bridge.

The switch with the lowest Bridge ID (a combination of the Bridge Priority and MAC addess) is elected as the root bridge.

Root Port Selection:

Each non-root bridge selects one root port, which is the port that provides the shortest path to the root bridge.

The root port is the port on the non-root bridge with the lowest path cost to the root bridge.

Designated Port Selection:

Each network segment has one designated port, which is responsible for forwarding traffic to the root bridge.

The switch with the lowest Bridge ID on each segment is elected as the designated bridge, and its port facing the root bridge becomes the designated port.

Blocking Port State:

After root and designated ports are selected, non-designated ports are placed in a blocking state to prevent loops.

Blocking ports do not forward traffic but remain active to monitor the network for changes.

1. Per VLAN Spanning Tree (PVST) is a Cisco proprietary extension of the Spanning Tree Protocol (STP) that allows for the creation of a separate spanning tree instance for each VLAN. This enables finer control over network traffic and redundancy for different VLANs. Here's an example scenario demonstrating PVST:

Example Scenario:

Switches: Multiple Cisco switches supporting PVST.

Devices: End-user devices connected to the switches, grouped into different VLANs (VLAN 10, VLAN 20, and VLAN 30).

Topology: A simple network topology with multiple switches interconnected via trunk links.

1. IPv6, or Internet Protocol version 6, is the most recent version of the Internet Protocol (IP) designed to replace IPv4. IPv6 addresses the limitations of IPv4, such as address space exhaustion, by introducing a significantly larger address space, improved header format, and enhanced features

Types of IPv6 Addresses:

Unicast Address: Identifies a single interface on a network. Types of unicast addresses include:

Global Unicast Address: Equivalent to public IPv4 addresses, routable on the Internet.

Link-Local Address: Used for communication within the same subnet or link.

Multicast Address: Represents a group of interfaces, allowing one-to-many or many-to-many communication.

Anycast Address: Identifies multiple interfaces, but the packet is delivered to the nearest (in terms of routing distance) interface.

1. Example Scenario:

Router: A router running IPv6 RIP.

Network Segments: The network is divided into several segments, and the router connects these segments.