Module 8 network access basic routing and advanced routing concept, switching concept

# Beginner Question

### 1. Explain Switch

A switch is a networking device that connects multiple devices on a local area network (LAN) and forwards data to the appropriate destination based on MAC addresses.

### 2. Explain Switch Boot Sequence

It's the process a switch goes through when powered on, including power-on self-test (POST), loading the bootstrap program, locating and loading the operating system, and initializing interfaces.

### 3. Explain Three Methods to access Switch Command Line Interface

Methods include using a console cable connected to the console port, accessing remotely via Telnet or SSH over the network, or accessing through a web-based interface using a web browser.

### 4. Explain and Configuring the Cisco Internet Operating System

It involves accessing the switch's command line interface, entering configuration mode, and using commands to configure settings such as interface configurations, VLANs, and security features.

### 5. Explain Switch Port

A switch port is a physical interface on a switch used to connect devices, such as computers or servers, to the network. It operates at Layer 2 of the OSI model and forwards frames based on MAC addresses

### 6. Configure Basic Password Settings on a switch - Done in lab

### 7. Configure Line Password Settings on a switch - Done in lab

### 8. Configure Password Settings on a switch - Done in lab

### 9. Configure IPv4 on a switch - Done in lab

### 10.Verifying IPv4 on a switch - Done in lab

### 11. Explain Basic V LAN

VLANs are logical groupings of devices on a network, allowing administrators to segment a physical network into multiple virtual networks. This segmentation enhances network security, performance, and management by isolating traffic within each VLAN.

Virtual LAN is logically created groups inside a LAN network.

### 12. Explain VTP

VTP is a Cisco proprietary protocol used to manage VLAN configurations across a network of switches. It allows VLAN information, such as VLAN IDs, names, and types, to be synchronized and propagated automatically to all switches within a VTP domain, simplifying VLAN management and configuration.

### 13. Explain CDP.

CDP is a proprietary Cisco protocol used to discover and gather information about directly connected Cisco devices. It operates at the data link layer of the OSI model and enables devices to learn about neighboring Cisco devices, including their device type, IP address, and capabilities. CDP facilitates network troubleshooting, device management, and topology mapping in Cisco environments.

### 14. Identifying VLAN - Done in lab

### 15.Describe the basic operation of STP

STP prevents network loops in Ethernet networks by selectively blocking redundant links between switches. It elects a root bridge and calculates the best paths to the root bridge, while blocking alternative paths to prevent loops.

### 16. Explain IPv4 subnetting.

Pv4 subnetting is the process of dividing a large IP network into smaller subnetworks, or subnets, to improve network efficiency and manageability. It involves borrowing bits from the host portion of an IP address to create network and host portions, allowing for better organization and allocation of IP addresses within a network.

### 17.What is subnet mask?

It's a numerical value used in IP networking to define the network portion and host portion of an IP address. It determines which part of the IP address is the network address and which part is the host address

### 18. Explain binary decimal hexadecimal with example

They are number systems used in computing. Binary uses 0s and 1s, decimal uses 0-9, and hexadecimal uses 0-9 and A-F. For example, the decimal number 10 is equivalent to binary 1010 and hexadecimal A.

### 19.Describe the Need for Public IPv4 and Private IP Addressing

Public IPs are used to identify devices on the internet, while private IPs are used within private networks. Private addressing conserves public IP addresses and provides security by hiding internal network topology.

### 20. Explain Subnet Prefix

It's a notation used in subnetting to specify the size of a subnet. It's represented by a forward slash (/) followed by a number indicating the number of bits used for the network portion of the IP address.

### 21. Explain How to Connect Router with Switch

Connect a router's Ethernet port to a switch port using an Ethernet cable. Configure router interfaces and switch ports with appropriate IP addresses and VLAN memberships to enable communication between them.

### 22. Explain Routing Basics with command

Use the "show ip route" command on a router to display the routing table, showing all known networks and how to reach them. Use "ip route" command to manually configure static routes, specifying destination networks and next-hop routers

### 23.Configuration basic IP address in fig. - Done in lab

### 24.Create Static Routes - Done in lab

### 25.Verifying IP Routing - Done in lab

### 26. Explain rip version 1 and rip version 2

RIP (Routing Information Protocol) Version 1 is a distance-vector routing protocol that uses hop count as the metric for path selection. RIP Version 2 is an updated version that supports CIDR (Classless Inter-Domain Routing), VLSM (Variable Length Subnet Masking), and includes support for authentication, but still relies on hop count as the metric.

### 27. Explain EIGRP

EIGRP is a Cisco proprietary routing protocol that combines features of both distance-vector and link-state routing protocols. It uses DUAL (Diffusing Update Algorithm) to calculate the shortest path to destinations and supports features like fast convergence, unequal-cost load balancing, and route summarization.

### 28. Explain OSPF Basics

OSPF is a link-state routing protocol used to determine the best path for routing packets in an IP network. It calculates the shortest path to each destination based on the cost of links and constructs a topology map of the network. OSPF routers exchange link-state advertisements (LSAs) to maintain network topology information.

### 29. Explain OSPF Area

OSPF networks are divided into areas to scale large networks and reduce routing overhead. Each area maintains its own link-state database and summarizes routing information to other areas. OSPF routers within the same area share a full routing table, while routers between areas only exchange summarized routes.

### 30. Explain DR/BR Selection

In OSPF, on multi-access networks like Ethernet, one router is elected as the DR and another as the BDR. The DR is responsible for exchanging routing information with other OSPF routers on the network, while the BDR acts as a backup in case the DR fails

### 31. Explain OSPF

OSPF is a link-state routing protocol used to determine the best path for routing packets in an IP network. It calculates the shortest path to each destination based on the cost of links and constructs a topology map of the network. OSPF routers exchange link-state advertisements (LSAs) to maintain network topology information.

### 32. Explain Describe IPv6 addresses

IPv6 addresses are 128-bit identifiers used to uniquely identify devices on an IPv6 network. They are represented as eight groups of four hexadecimal digits separated by colons. Examples include 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

### 33.What is 6to4 tunnel?

6to4 is an IPv6 transition mechanism that allows IPv6 packets to be encapsulated within IPv4 packets for transmission over an IPv4 network. It enables communication between IPv6 networks over an IPv4 infrastructure by automatically tunneling IPv6 traffic over IPv4.

### 34. Explain Wireless Technology

Wireless technology enables communication between devices without the need for physical wired connections. It uses radio waves to transmit data between devices, providing flexibility and mobility in network connectivity.

### 35. Explain Basic Wireless Devices

Basic wireless devices include wireless routers, access points, and wireless network interface cards (NICs). Routers and access points create wireless networks, while wireless NICs enable devices to connect to these networks wirelessly.

### 36. Explain Wireless Security

Wireless security measures protect wireless networks from unauthorized access and data breaches. They include encryption protocols like WPA (Wi-Fi Protected Access) or WPA2, MAC (Media Access Control) address filtering, and disabling SSID (Service Set Identifier) broadcasting.

### 37. Explain WPA or WPA2 Pre-Shared Key

WPA (Wi-Fi Protected Access) and WPA2 are security protocols used to secure wireless networks. They use a pre-shared key (PSK) or passphrase to authenticate and encrypt data transmitted between devices on the network, ensuring confidentiality and integrity of communications.

# Intermediate Question

### 1. Explain Logging into a Switch

Access a switch through a console port using terminal emulation software or remotely via SSH, Telnet, or web interface, providing appropriate credentials

### 2. Explain Switch User Mode, Enable (Privileged) Mode and Global Configuration Mode

User Mode provides limited access for basic monitoring and troubleshooting. Enable Mode grants privileged access for configuration changes. Global Configuration Mode allows modifying switch-wide settings.

### 3. Gathering Switch Basic information

Use commands like "show version" to display hardware and software information, "show interfaces" for interface status, and "show ip interface brief" for IP address information.

### 4. Explain SSH

SSH is a network protocol that allows secure remote access to network devices. It encrypts data transmission, providing confidentiality and integrity, and is commonly used for managing switches securely over a network.

### 5. Configure SSH Setting on a Switch - Done in lab

### 6. Explain Telnet Setting

Telnet settings involve configuring parameters for Telnet sessions on a network device. This includes setting Telnet access permissions, specifying timeout values, configuring authentication methods such as username/password or AAA (Authentication, Authorization, and Accounting), and enabling encryption for secure communication. Additionally, administrators may adjust Telnet session options like terminal type and character encoding to suit specific requirements.

### 7. Verifying Switch Interface Status - Done in lab

### 8. Configure VLAN - Done in lab

### 9. Verifying VLAN - Done in lab

### 10.Configure VLAN Trucking - Done in lab

### 11.Give Reasons for Using VLANs

VLANs help in improving network security, reducing broadcast domain size, optimizing network traffic, simplifying network management, and facilitating network scalability.

### 12. Static VLANs

Static VLANs involve manually assigning ports to specific VLANs, which remains unchanged unless manually reconfigured.

### 13.Dynamic VLANs

Dynamic VLANs assign VLAN membership to devices dynamically based on factors such as MAC addresses, allowing for more flexible and automated VLAN management.

### 14.Brief explain STP Timer

Spanning Tree Protocol (STP) timers control the behavior of the STP protocol. These timers include Hello Time, Forward Delay, and Max Age, which determine how quickly switches converge and adapt to changes in the network topology.

### 15. Explain how Switches Calculate Their Root Cost

Switches calculate the root cost based on the cumulative path cost to reach the root bridge in a spanning tree network. The root cost is determined by adding up the individual link costs along the path from the switch to the root bridge, with lower costs indicating better paths.

### 16.Configure STP on Switch - Done in lab

### 17.Verifying STP on a Switch - Done in lab

### 18.What is Port Security how to find Port with command?

Port security is a feature that restricts access to switch ports based on MAC address, limiting the number of devices that can connect to a port. To find ports with port security enabled, use the command "show port-security interface [interface]" on a Cisco switch.

### 19.Classified Default subnet mask for Class A, B, C, D

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Class D (Multicast): No default subnet mask (reserved for multicast addressing)

### 20. Explain ClasslessInter-Domain Routing

CIDR is a method for allocating IP addresses and IP routing. It allows for more efficient use of IP address space by using variable-length subnet masks (VLSM) and eliminating the strict class-based addressing of IPv4.

### 21.How to define subnetting address of class A, B, C, D

Subnetting addresses involve dividing a network into smaller subnetworks to improve efficiency and manageability. This can be done by borrowing bits from the host portion of the IP address to create subnet addresses with varying lengths.

### 22. Explain Classless and Class full Addressing

Classful addressing divides IP addresses into classes (A, B, C) with fixed subnet masks, while classless addressing allows for more flexible allocation of IP addresses using variable-length subnet masks (VLSM) and CIDR notation.

### 23.Details of VLSM (variable length Subnet Mask

VLSM allows for the allocation of IP addresses with varying subnet mask lengths within the same network, enabling more efficient use of IP address space by subnetting networks into smaller subnets.

### 24. Explain Static Routing

Static routing involves manually configuring routing tables on network devices to determine the path packets should take to reach their destination. It's often used in small networks or for specific routes where dynamic routing protocols are not required.

### 25. Explain Default Routing

Default routing involves configuring a router to forward packets with unknown destinations to a specific gateway, typically the next-hop router or the router's default gateway. It's used to provide a default path for outbound traffic when a specific route is not available in the routing table.

### 26.Configuring IP routing - Done in lab

### 27.Configure VLAN Routing - Done in lab

### 28.Routing Protocol Metric

A routing protocol metric is a value used by routing algorithms to determine the best path to a destination network. It represents the cost associated with traversing a particular route and can be based on factors like bandwidth, delay, reliability, and hop count.

### 29. Explain how OSPF calculates the cost for a route

OSPF calculates the cost for a route based on the formula: Cost = Reference Bandwidth / Interface Bandwidth. The default reference bandwidth is 100 Mbps, and the interface bandwidth is obtained from the speed configured on the interface. Lower bandwidth results in a higher OSPF cost.

### 30.Define Benefits and Uses of IPv6

IPv6 offers benefits such as a larger address space, improved security features, simplified network configuration (auto-configuration), and support for new technologies like IoT. It's used to address the limitations of IPv4, accommodate the growing number of internet-connected devices, and enable future network growth.

### 31.Define thisIPV6 Address

An IPv6 address is a 128-bit identifier used to uniquely identify devices on an IPv6 network. It's represented as eight groups of four hexadecimal digits separated by colons. Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

### 32. Explain IPv6 Routing Protocols

IPv6 routing protocols, such as OSPFv3, RIPng, and BGP4+, are designed to support IPv6 networks and enable routers to exchange routing information for forwarding IPv6 packets.

### 33. Explain Wireless Access Points

Wireless access points (APs) are networking devices that allow wireless devices to connect to a wired network. They transmit and receive wireless signals, provide network connectivity to wireless clients, and may include features like security settings and management capabilities.

### 34.Define IEEE 802.11 Transmissions

IEEE 802.11 defines standards for wireless local area network (WLAN) transmissions. It specifies protocols for physical and data link layers, including modulation techniques, frame formats, and media access control (MAC) procedures used in Wi-Fi networks.

### 35. Explain Independent Basic Service Set (Ad Hoc)

An Independent Basic Service Set (IBSS), also known as an ad hoc network, is a decentralized wireless network where devices communicate directly with each other without the need for a central access point. It's commonly used for peer-to-peer communication between devices in temporary or mobile networks.

### 36. Explain How to Secure Wireless Network

Secure wireless networks by enabling encryption (e.g., WPA2), using strong passwords, disabling SSID broadcasting, enabling MAC address filtering, updating firmware regularly, and implementing network segmentation and monitoring tools.

# Advance question

### 1. Setting administrative factions - Done in lab

### 2. Setting hostnames - Done in lab

### 3. Setting banners - Done in lab

### 4. Setting passwords - Done in lab

### 5. Viewing,saving, and erasing configurations - Done in lab

### 6. Configure an IP address on a switch - Done in lab

### 7. Configuring SSH - Done in lab

### 8. Configuring Telnet - Done in lab

### 9. Explain Layer 3 Switch

A Layer 3 switch combines features of traditional Layer 2 switches with routing capabilities found in routers. It can route traffic between different subnets or VLANs at wire speed, improving network performance and reducing the need for separate routers.

### 10.Describe Dynamic IP configuration with DHCP

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to devices on a network. DHCP servers manage a pool of IP addresses and lease them to client devices dynamically, along with other configuration parameters like subnet mask, default gateway, and DNS servers.

### 11. Explain 802.1q Protocol

IEEE 802.1Q is a protocol used for VLAN tagging in Ethernet networks. It inserts a VLAN tag into the Ethernet frame header, allowing switches to identify VLAN membership and route traffic accordingly. This enables the creation of virtual LANs within a physical network infrastructure.

### 12. Explain the Switch Port Mode Command

The switchport mode command configures the operational mode of a switch port. Common modes include access mode for connecting end devices, trunk mode for carrying traffic from multiple VLANs, and dynamic auto mode for automatically negotiating the mode with connected devices.

### 13. Explain the Removing Command of VLAN

To remove a VLAN from a Cisco switch, use the no vlan [vlan\_id] command in global configuration mode. This removes the VLAN configuration and any associated ports or interfaces from the switch's VLAN database.

### 14.Describe Inter VLAN Routing

Inter-VLAN routing allows communication between devices in different VLANs within the same network. It can be accomplished using a Layer 3 switch or a router, which routes traffic between VLANs based on their IP addresses.

### 15. Explain Dynamic Routing

Dynamic routing protocols allow routers to dynamically exchange routing information and adapt to changes in network topology. Examples include OSPF, EIGRP, and RIP, which use algorithms to calculate the best paths and share routing updates with neighboring routers.

### 16. Explain routing loop

A routing loop occurs when packets are continually forwarded between routers in a network due to incorrect routing information or misconfigured routing protocols. This can result in excessive network traffic, delays, and potential network instability. Routing loops are usually resolved by implementing mechanisms like route summarization, split horizon, and route poisoning.

### 17.Configure and verify inter switch connectivity - Done in lab

### 18.Configure and Verify VLAN Trucking - Done in lab

### 19. Explain and configure PAGP

Port Aggregation Protocol (PAgP) is a Cisco proprietary protocol used to automatically aggregate multiple physical links into a single logical link, known as an EtherChannel. PAgP negotiates the creation and maintenance of the EtherChannel between switches.

### 20.Configuring Ether Channel - Done in lab

### 21.Verifying Ether Channel - Done in lab

### 22. Explain PAGP and LACP

PAgP (Port Aggregation Protocol) and LACP (Link Aggregation Control Protocol) are protocols used for link aggregation, with PAgP being Cisco proprietary and LACP being an open standard allowing interoperability across different vendors.

### 23.Configure and Verifying IPv4 Addressing and Subnetting - Done in lab

### 24. Explain the Network Address and Broadcast Address

The network address identifies the network portion of an IP address, while the broadcast address is used to send data packets to all devices on a network.

### 25. Explain Classful Network

Classful networks are based on the original addressing scheme of IPv4, which divides IP addresses into classes (A, B, C, D, E) with fixed-length subnet masks. Each class has a predetermined range of IP addresses, and the subnet mask is determined by the class of the address. However, this addressing scheme has limitations in efficient address allocation and led to the development of Classless Inter-Domain Routing (CIDR).

### 26. 26. Practice Example #5B: 255.255.255.0 (/24) - Done in lab

### 27. 27. Practice Example #2A: 255.255.240.0 (/20) - Done in lab

### 28.Given the no of hosts as 126, 50, 20 and 5 Find IP address and subnet

### mask using class (192.168.1.0)

### 29. Explain this Network

### 30. Put right addressing in fig.

### 31. Explain Routed and Routable Protocol

Routed Protocol: A protocol that can carry data across networks and requires routing to reach its destination, e.g., IPv4, IPv6. Routable Protocol: A protocol that supports the routing of data packets across networks, allowing communication between different subnets or networks, e.g., IP.

### 32. Explain IGP

IGP is a routing protocol used within an autonomous system (AS) to exchange routing information between routers. Examples include OSPF and EIGRP.

### 33. Explain Distance Vector, link state and Hydride

Distance Vector: Routing algorithm where routers exchange information about their directly connected neighbors' distances to destinations. Example: RIP.

Link State: Routing algorithm where routers exchange information about the state of their links, allowing each router to build a detailed map of the network. Example: OSPF.

Hybrid: Combines characteristics of both distance vector and link state routing algorithms. Example: EIGRP.

### 34. Explain and Verifying OSPFv2

OSPFv2 is a link-state routing protocol used to exchange routing information within an autonomous system (AS). It calculates the shortest path to each destination based on link costs.

### 35. Explain Wildcard Mask

A wildcard mask is used in access control lists (ACLs) and routing protocols to specify a range of IP addresses. It is the inverse of a subnet mask and indicates which bits in an IP address are relevant for matching.

### 36. Explain Address Types and Special Addresses

Unicast: Addressed to a single destination host.

Broadcast: Addressed to all devices on a network segment.

Multicast: Addressed to a specific group of hosts.

Loopback: Special address (127.0.0.1) used to test the network interface.

Broadcast Address: Address used to send data to all devices on a network.

Network Address: Address representing a network as a whole, used for routing purposes.

Subnet Address: Address used to represent a subdivision of a larger network.

### 37.Configuring Cisco Routers with IPv6 - Done in lab

### 38. Explain RIPng, EIGRPv6, OSPFv3

RIPng (Routing Information Protocol Next Generation):

RIPng is an extension of RIP for IPv6 networks.

It operates similarly to RIP for IPv4 but supports IPv6 addresses and networks.

RIPng uses UDP as the transport protocol and operates on port 521.

It uses the hop count as the metric to determine the best path.

EIGRPv6 (Enhanced Interior Gateway Routing Protocol Version 6):

EIGRPv6 is an enhanced version of EIGRP that supports IPv6.

It is a Cisco proprietary routing protocol designed for IPv6 networks.

EIGRPv6 uses the Diffusing Update Algorithm (DUAL) to calculate the shortest path to destinations.

Like its IPv4 counterpart, EIGRPv6 supports features such as rapid convergence, unequal-cost load balancing, and route summarization.

OSPFv3 (Open Shortest Path First Version 3):

OSPFv3 is an extension of OSPF for IPv6 networks.

It is designed to support IPv6 addresses and networks.

OSPFv3 uses the same link-state database concept as OSPFv2 but includes modifications to accommodate IPv6 addressing.

It uses IPv6 multicast addresses for communication between OSPFv3 routers and supports features such as authentication, route summarization, and virtual links.

### 39.Creating a 6to4 tunnel - Done in lab

### 40. Explain 802.11 Committees and subcommittees

Various committees and subcommittees within the IEEE 802.11 Working Group are responsible for developing and maintaining the 802.11 standard, addressing specific aspects like security, throughput, and amendments.

### 41. Explain Wireless Topologies

Peer-to-Peer: Devices connect directly to each other without the need for a central node, facilitating easy communication but lacking scalability.

Bus: All devices share a single communication line, with data transmitted sequentially. Simple to implement but prone to single-point failures.

Ring: Devices are connected in a circular manner, passing data from one to the next until it reaches the intended recipient. Efficient but susceptible to disruptions if one device fails.

Mesh: Each device connects to multiple others, creating redundant paths for data transmission, ensuring reliability and fault tolerance.

Hybrid: Combines two or more different topologies to suit specific network requirements, offering flexibility and scalability.

Tree: Devices are organized hierarchically, with one central node connecting to multiple secondary nodes, forming a tree-like structure. Offers efficient data transmission but may suffer from bottleneck issues.