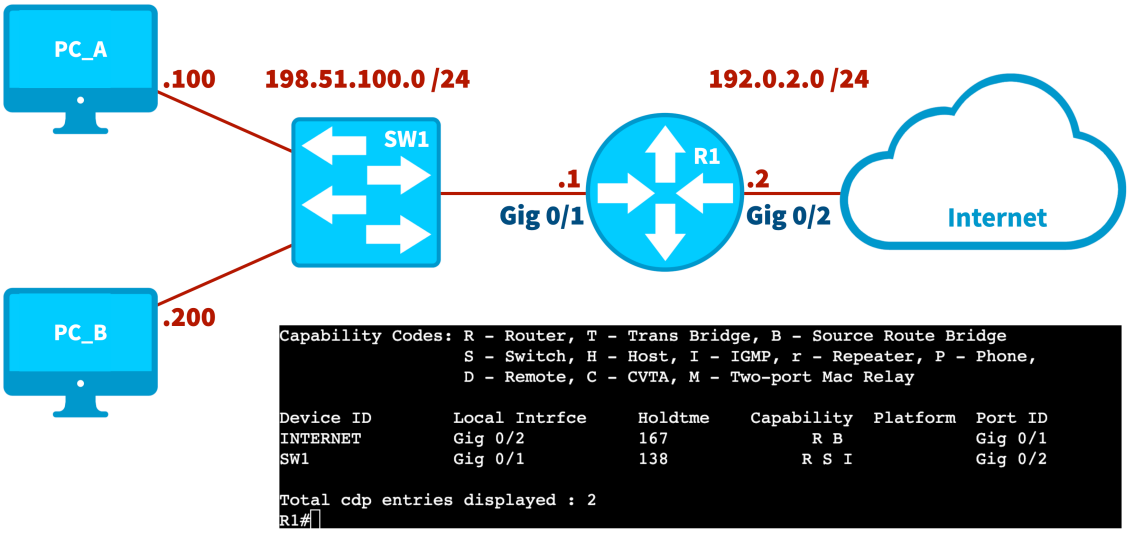
CCNA v1.1 (200-301) Video Training Series
Practice Exam #2

Questions

Q1. Consider the following topology and output. Which of the following commands produced the output?



A) show lldp neighbors
B) show cdp neighbors detail
C) show ip ospf neighbors
D) show cdp neighbors

Q2. Which WLAN design would you use if you need to extend wireless coverage to a remote location without direct Ethernet connectivity?

A) Infrastructure WLAN
B) Ad Hoc WLAN
C) Mesh WLAN
D) Peer-to-Peer WLAN

Q3. You are setting up a router that connects to the Internet but want to avoid maintaining a full Internet routing table. Which of the following should you configure?

A) Static route for each network
B) MAC address filtering
C) A default route
D) Egress interface designation

Q4. If a company wants to enable communication between a computer in the sales department (VLAN 10) and a computer in the engineering department (VLAN 20), which of the following components is essential?

A) A Layer 2 switch configured with VLANs 10 and 20
B) A dedicated firewall between the two VLANs
C) A router or a Layer 3 switch to route between VLANs
D) A Cisco Express Forwarding (CEF) configuration

Q5. Starting with which Wi-Fi standard can an access point both send and receive multiple spatial streams at the same time?

A) Wi-Fi 4 (802.11n)
B) Wi-Fi 5 (802.11ac)
C) Wi-Fi 6 (802.11ax)
D) Wi-Fi 7 (802.11be)

Q6. You are designing a network to include EtherChannel for higher bandwidth and redundancy. Which of the following is a benefit of utilizing EtherChannel in your network design?

A) EtherChannel reduces the number of IP addresses needed for the links between switches.
B) EtherChannel can aggregate up to eight links, providing increased bandwidth and redundancy without affecting the port channel port if a single link goes down.
C) EtherChannel allows for non-contiguous links to be logically bundled together, reducing physical cabling.
D) EtherChannel eliminates the need for Spanning Tree Protocol, thereby simplifying network configuration and management.

Q7. In the process of OSPF verification, you examine the OSPF database on a router. What would you expect to find in the Summary Net Link States section of the OSPF database?

A) Detailed topological information of all areas
B) A list of OSPF neighbors and their states
C) OSPF router IDs and their corresponding IP addresses
D) A listing of networks in other areas

Q8. You need to configure a network device with an IP address within the subnet 10.2.4.0 /23. Which of the following IP addresses would be considered valid for a device within this subnet?

A) 10.2.4.255
B) 10.2.5.0
C) 10.2.5.254
D) All of the above

Q9. What technology is represented by the IEEE 802.1s standard?

A) PVST
B) Rapid PVST+
C) RSTP
D) MSTP

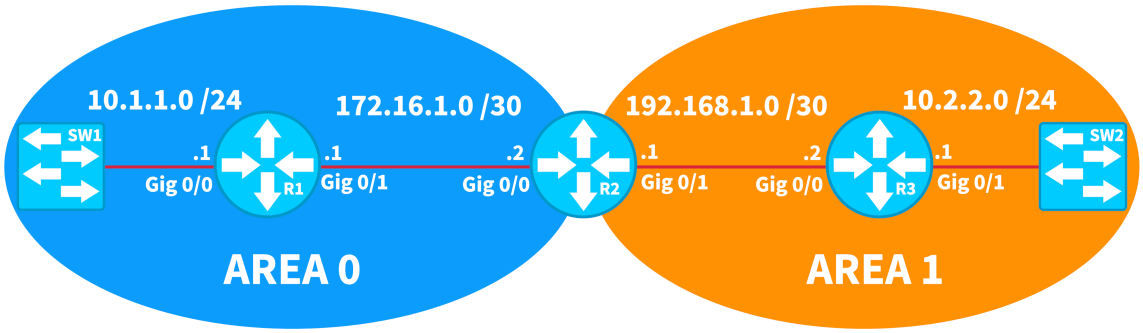
Q10. Why is UDP considered an unreliable protocol compared to TCP?

A) UDP does not establish a session before data transmission
B) UDP has a larger header than TCP
C) UDP uses dynamic or private ports for communication
D) UDP traffic is always encrypted for security

Q11. What purpose does the IPv6 solicited-node multicast address serve in the Duplicate Address Detection (DAD) process?

A) It ensures that the IPv6 address is routable on the Internet.
B) It allocates a unique MAC address to the IPv6 device.
C) It identifies the router's IPv6 address on the network.
D) It verifies that no other device on the network is using the same IPv6 address.

Q12. Consider the following topology. How many Type 3 LSAs are present in router R3's Link State Database (LSDB)?



A) 1
B) 2
C) 3
D) 4

Q13. In Cisco's Collapsed Core architecture model, which two layers are combined?

A) Access and Distribution
B) Distribution and User
C) Access and Core
D) Core and Distribution

Q14. Which SNMP version introduced significant security improvements such as encryption, integrity checking, and authentication?

A) SNMPv1
B) SNMPv2c
C) SNMPv1c
D) SNMPv3

Q15. Which type of cabling issue can result in hearing part of a voice conversation from another circuit?

A) Attenuation
B) Crosstalk
C) Jitter
D) Latency

Q16. Which Syslog severity level is the most severe?

A) Level 0 - Emergencies
B) Level 1 - Alerts
C) Level 2 - Critical
D) Level 3 - Errors

Q17. What is the directed broadcast address of a subnet containing an IP address of 172.16.1.10 /19?

A) 172.16.15.255
B) 172.16.31.255
C) 172.16.255.255
D) 172.16.95.255
E) 172.16.0.255

Q18. When a client attempts to obtain network information through Dynamic Host Configuration Protocol (DHCP), which unicast message from the client requests network addressing information from the server?

A) REQUEST
B) DISCOVER
C) OFFER
D) ACKNOWLEDGEMENT

Q19. What is the primary advantage of using Infrastructure as Code (IaC) with tools like Terraform?

A) It eliminates the need for network security.
B) It automates the creation and management of a virtual infrastructure.
C) It replaces the need for cloud service providers.
D) It physically installs and configures network hardware.

Q20. With which category of routing protocol is the Dijkstra Algorithm used?

A) Link-State
B) Distance-Vector
C) Path-Vector
D) Route-Vector

Q21. Which type of Wide Area Network (WAN) has built-in redundancy due to the ring topology used?

A) Metropolitan Area Network (MAN)
B) Multiprotocol Label Switching (MPLS)
C) Virtual Private Network (VPN)
D) Point-to-Multipoint

Q22. With IPv6 multicast communication, how many bits are dedicated to the group ID?

A) 64
B) 112
C) 107
D) 86

Q23. In the context of WPA2 wireless configuration, what does PSK stand for?

A) Private Secure Key
B) Public Shared Key
C) Pre-Shared Key
D) Protected Security Key

Q24. In the context of Network Address Translation (NAT), what terminology is used to describe the original, unaltered IP address of a device located inside the network, before any translation has occurred?

A) Inside Local
B) Inside Global
C) Outside Local
D) Outside Global

Q25. Which type of cabling would be used if required to run through a raised floor or above drop-ceiling tiles?

A) Unshielded Twisted-Pair
B) Shielded Twisted-Pair
C) Plenum-Rated
D) RG-58/U

Q26. Which fiber optic connector is known for its straight tip design and utilizes a bayonet-style attachment mechanism?

A) ST connector
B) LC connector
C) SC connector
D) MTRJ connector

Q27. A network administrator is implementing Cisco Catalyst Center in their enterprise network. Which of the following is NOT a primary feature offered by this SDN controller?

A) Network design and provisioning
B) Configuration monitoring and troubleshooting
C) Custom application development platform
D) Direct control of data center fabric switches

Q28. Which QoS mechanism, by default, drops traffic that exceeds a configured bandwidth limit?

A) Policing
B) Shaping
C) Queuing
D) Link Efficiency

Q29. Which type of network connection is used in a switched network where devices are able to communicate in full-duplex mode with one another?

A) Ethernet Bus
B) Shared Media Hub
C) Direct Connect
D) Point-to-Point

Q30. Which of the following statements is true about the order of rules in an ACL?

A) The rules can be in any order, because the router processes all rules simultaneously.
B) The more specific rules should be placed at the bottom of the list.
C) The order of rules is not important as there is no implicit deny at the end of the ACL.
D) The more specific rules should be placed at the top of the list to ensure they are evaluated first.

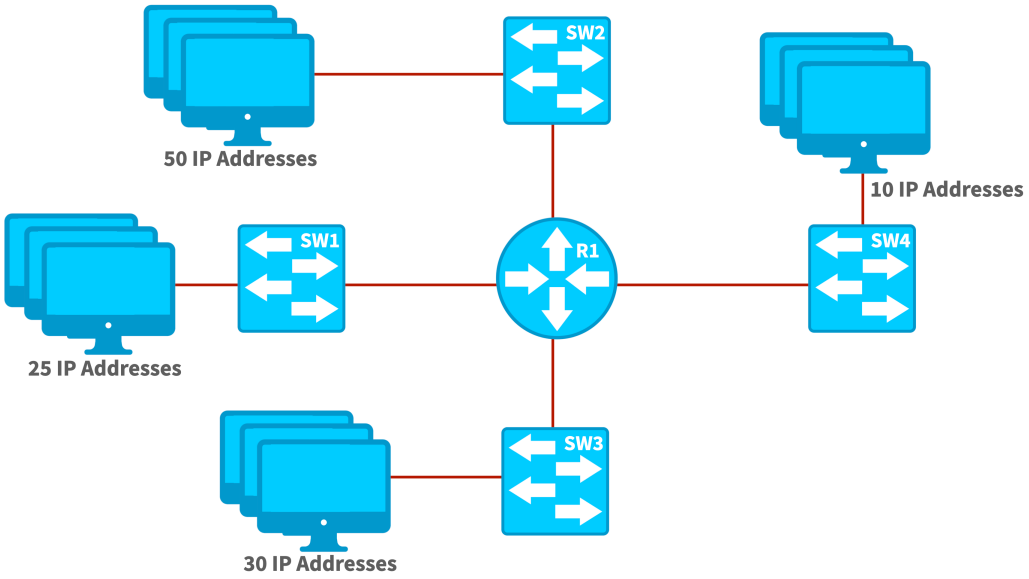
Q31. Which of the following represents the first two hexadecimal values of every IPv6 multicast address?

A) FE
B) F0
C) 0E
D) FF

Q32. Your network needs to support several link speeds. To support multiple link speeds greater than 1 Gbps, you consider using STP's Long Path Cost method to determine port cost. Under the Short Path Cost method, what is the port cost assigned to a 1 Gbps link?

A) 2
B) 4
C) 19
D) 100

Q33. What subnet mask should be used to subnet the 192.168.10.0 network to support the number of subnets and IP addresses per subnet shown in the following topology?



A) 255.255.255.0
B) 255.255.255.128
C) 255.255.255.192
D) 255.255.255.224
E) 255.255.255.240

Q34. A customer is using a Class C network of 192.168.10.0 subnetted with a 28-bit subnet mask. How many subnets can be created by using this subnet mask?

A) 32
B) 16
C) 30
D) 8
E) 14

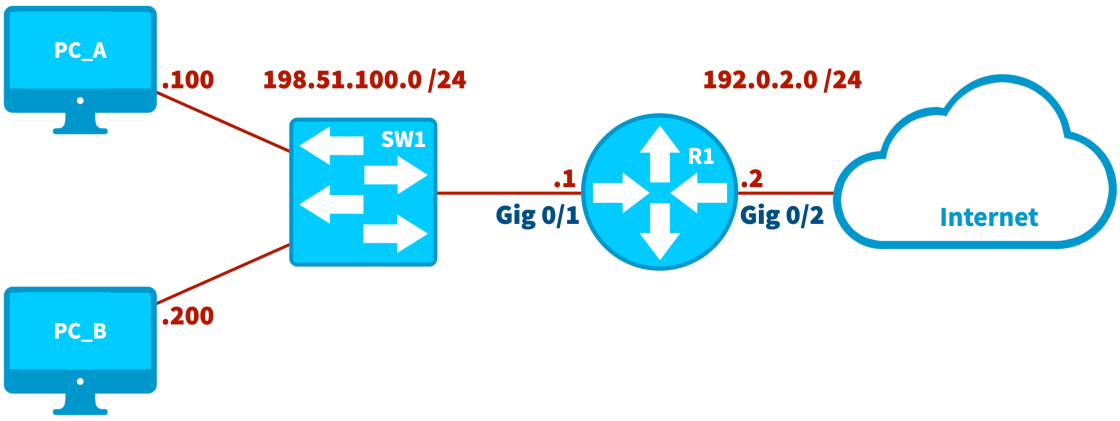
Q35. Which Port Security violation mode will disable a port completely when a violation occurs?

A) Protect
B) Restrict
C) Shutdown
D) Monitor

Q36. Which type of IPv6 address can be thought of as being similar to the IPv4 APIPA address range 169.254.0.0 /16?

A) Global Unicast
B) Loopback
C) Multicast
D) Link Local

Q37. Consider the following topology and ACL configuration. Which of the following configurations will prevent PC_A (198.51.100.100) from reaching the Internet, while permitting PC_B (198.51.100.200) to reach the Internet?



A)
R1(config)# access-list 50 permit any
R1(config)# access-list 50 deny host 198.51.100.100
R1(config)# int gig 0/2
R1(config-if)# ip access-group 50 out
R1(config-if)#

B)
R1(config)# access-list 50 deny host 198.51.100.100
R1(config)# access-list 50 permit any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 50 out
R1(config-if)#

C)
R1(config)# access-list 150 deny host 198.51.100.100
R1(config)# access-list 150 permit any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 150 out
R1(config-if)#

D)
R1(config)# access-list 50 deny host 198.51.100.100
R1(config)# access-list 50 permit any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 50 in
R1(config-if)#

Q38. Which type of wireless access point (AP) is more common in large enterprise networks?

A) Autonomous
B) Standalone
C) Master
D) Lightweight

Q39. You are diagnosing network issues in a newly set up office network and notice a device with an IP address of 169.254.1.5. Understanding the nature of this IP address, what issue is most likely present?

A) The device could not obtain an IP address from a DHCP server and assigned itself an IP address.
B) The device is configured with a static IP address intended for public Internet use.
C) The device has successfully obtained an IP address from a DHCP server.
D) The device is using a private IP address, which is causing conflicts within the network.

Q40. Which command allows us to see which IP addresses have been assigned to the interfaces?

A) R1(config)#show interface brief
B) R1#show interface assignments
C) R1(config)#show ip statistics
D) R1#show ip interface brief

Q41. With an IPv6 global unicast address, what is represented by the last 64 bits of the address?

A) Global Routing Prefix
B) Subnet ID
C) Interface ID
D) Link Local ID

Q42. In the context of emergency services, how can CDP be utilized to assist in identifying a caller's location?

A) By encrypting voice packets to secure data transmission
B) By assigning a unique identifier to each device
C) By learning an IP phone's approximate location based on the location of the switch to which the phone is connected
D) By increasing the bandwidth for emergency calls

Q43. Which fiber optic connector carries two strands of fiber?

A) MT-RJ
B) ST
C) LC
D) SC

Q44. When examining a Cisco router's routing table, you notice routes with different codes such as 'C', 'L', 'D', and 'O'. If your primary concern is identifying the next-hop for a packet destined for an internal network that your router learned via dynamic routing, which code should you look for?

A) C
B) L
C) S
D) O

Q45. Which protocol is considered more secure due to its two-way challenge-response mechanism and full packet encryption?

A) RADIUS
B) TACACS+
C) LDAP
D) AD

Q46. When examining the structure of an IPv6 link local address, which of the following is true?

A) The first 48 bits are used to specify the network prefix.
B) The first 10 bits are fixed, followed by 54 bits set to zero and the last 64 bits forming the interface ID.
C) The entire address is dynamically generated without any fixed portion.
D) It includes a global routing prefix to ensure it is routable across the Internet.

Q47. Which OSPF metric is used to determine Designated Router (DR) election?

A) Lowest Router ID
B) Highest Router ID
C) Lowest OSPF Priority
D) Highest OSPF Priority

Q48. For a data center requiring a fiber optic connection that supports 10 Gbps over a maximum distance of 300 meters, which Ethernet standard and fiber type should be used?

A) 10GBASE-SR with multimode fiber (50 micrometers core)
B) 10GBASE-LR with single mode fiber
C) 10GBASE-SR with multimode fiber (62.5 micrometers core)
D) 10GBASE-LX with single mode fiber

Q49. As a network administrator, you want to selectively prevent the transmission of a device's system name in LLDP advertisements to enhance privacy. Which command accomplishes this at the global configuration level?

A) no lldp run
B) no lldp tlv-select system-name
C) lldp tlv-select system-name
D) no lldp tlv-select all

Q50. Which prerequisite must be enabled on a switch before configuring Dynamic ARP Inspection (DAI)?

A) Port Security
B) DHCP Snooping
C) VLAN Trunking
D) Spanning Tree Protocol

Q51. Given a subnet of 172.16.56.0 /21, identify which of the following IP addresses belong to this subnet. (Select 2.)

A) 172.16.54.129
B) 172.16.62.255
C) 172.16.61.0
D) 172.16.65.255
E) 172.16.64.1

Q52. Which of the following DNS record types is used to translate a Fully Qualified Domain Name (FQDN) into an IPv4 address?

A) A record
B) CNAME record
C) MX record
D) PTR record

Q53. Which part of the fiber optic cable is used to reflect light along the data path?

A) Dopant
B) Jacket
C) Cladding
D) Core

Q54. A network administrator needs to ensure that a newly installed PoE switch can provide adequate power for several devices, including VoIP phones and surveillance cameras. The devices require up to 15.4 watts each to operate. Which IEEE standard for PoE should the administrator ensure the switch supports to meet this requirement?

A) IEEE 802.3at
B) IEEE 802.3af
C) IEEE 802.3bt
D) IEEE 802.3ab

Q55. What is the purpose of configuring the `transport input ssh` command on VTY lines?

A) To disable Telnet access and allow only SSH connections
B) To enable password encryption
C) To set up SNMP monitoring
D) To assign IP addresses to VTY lines

Q56. Which routing protocol has a default administrative distance (AD) value of 90?

A) EIGRP
B) RIP
C) OSPF
D) BGP

Q57. Which value makes up the last 24 bits of an IPv6 solicited-node multicast address?

A) Destination IPv6 address
B) Source IPv6 Address
C) Link Local IPv6 Address
D) Global Unicast Address

Q58. A network architect is implementing a Software Defined Networking (SDN). Which of the following best describes the relationship between the underlay and overlay networks in this context?

A) The underlay network is virtual, while the overlay network is physical
B) The underlay network is physical, while the overlay network is logical
C) The underlay and overlay networks are both physical
D) The underlay and overlay networks are both virtual

Q59. Which routing protocol has a default administrative distance (AD) value of 110?

A) EIGRP
B) RIP
C) OSPF
D) BGP

Q60. Considering IPv6 does not support the traditional broadcast traffic flow, which IPv6 traffic type effectively replaces the functionality provided by broadcasting?

A) Multicast
B) Unicast
C) Anycast
D) None of the above

Q61. In a GLBP configuration, how does the Active Virtual Gateway (AVG) ensure that the traffic load is distributed among different routers in a GLBP group?

A) By responding to each ARP request with the same MAC address
B) By responding to each ARP request with the one of multiple MAC addresses
C) By only responding to the first ARP request
D) By redirecting all traffic to the MAC address of the router with the least load

Q62. You are tasked with securing a server. Which of the following would you address as a vulnerability?

A) A brute force attack tool found on the network
B) An unpatched software flaw in the operating system
C) An email attempting to trick users into disclosing passwords
D) A denial of service attack targeting the server

Q63. What is the default OSPF network type for serial interfaces not configured for Frame Relay?

A) Broadcast
B) Point-to-point
C) Non-broadcast
D) Point-to-multipoint

Q64. What is the final step in a Transmission Control Protocol (TCP) 3-way handshake?

A) SYN/ACK
B) ARP
C) ACK
D) SYN

Q65. You have been tasked with influencing the DR and BDR election process in an OSPF network. Which command can you use to set the priority value for a router's interface?

A) ospf priority [value]
B) ip ospf dr-priority [value]
C) ospf dr-priority [value]
D) ip ospf priority [value]

Q66. Which of the following access control entries would correctly deny all IP traffic from a host with the IP address 172.16.5.10?

A) access-list 20 deny 172.16.5.10
B) access-list 20 deny host 172.16.5.10 0.0.0.0
C) access-list 20 deny 172.16.5.10 0.0.0.255
D) access-list 20 deny host 172.16.5.10

Q67. What is the subnet address of the IP address 192.168.5.55 with a subnet mask of 255.255.255.224?

A) 192.168.5.0 /27
B) 192.168.5.16 /27
C) 192.168.5.32 /27
D) 192.168.5.48 /27
E) 192.168.5.64 /27

Q68. When IPv6 is enabled on an interface, which type of address is automatically assigned?

A) Global Unicast
B) Loopback
C) Multicast
D) Link Local

Q69. Which IPv6 address is the equivalent of the IPv4 address 127.0.0.1?

A) ::0
B) 127:0:0:1
C) ::1
D) ::127

Q70. You are reviewing an IPv6 address that has several quartets with leading zeros (but not all zeros). What rule applies to the abbreviation of these quartets in the address?

A) You must keep all leading zeros for clarity
B) You should replace leading zeros with a single zero
C) You can omit leading zeros only if they are followed by another zero
D) You can omit all leading zeros in each quartet

Q71. What is a common use case for TFTP in a network environment?

A) Securely transferring sensitive files between servers
B) Downloading configuration files to network devices during bootup
C) Enabling encrypted remote management
D) Monitoring network traffic

Q72. What multicast address is used by Open Shortest Path First to advertise Hello messages?

A) 223.0.2.0
B) 224.0.0.5
C) 232.0.0.1
D) 225.0.0.0

Q73. Given the MAC address 0014.2201.2345, which of the following will be the IPv6 link local address?

A) fe80::14:22:01:2345
B) fe80:0014:22ff:fe01:2345
C) fe8::214:22ff:fe1:2345
D) fe80::214:22ff:fe01:2345

Q74. Which Spanning Tree Protocol (STP) port state is used to populate the CAM table during convergence after a failure?

A) Listening
B) Learning
C) Blocking
D) Forwarding

Q75. Which command configures a switch to takeover in the event that the primary root fails on VLAN 1?

A) SW2(config)#spanning-tree vlan 1 backup root
B) SW2(config)#spanning-tree vlan 1 secondary root
C) SW2(config)#spanning-tree vlan 1 root standby
D) SW2(config)#spanning-tree vlan 1 root secondary

Q76. Why is it recommended to place a standard ACL as close to the destination as possible?

A) To reduce the processing load on the route
B) To prevent premature packet dropping
C) To ensure the ACL can be modified easily
D) To improve the performance of the network

Q77. Which protocol is typically used to communicate between a wireless LAN controller and lightweight access points?

A) CAPWAP
B) WPA3
C) SNMP
D) FTP

Q78. In an Ethernet switch, how does the switch learn where to forward frames for efficient communication?

A) By using IP address tables
B) By learning MAC addresses from incoming frames
C) Through pre-configured static routes
D) Via periodic broadcast messages

Q79. Given the IPv6 address 2bcc:0a1e:fb9c:0d4c:0000:0000:07a0:76cd, which abbreviation below is a correct representation?

A) 2bcc:a1e:fb9c:d4c::7a0:76cd
B) 2bcc:0a1e:fb9c:0d4c::07a0:76cd
C) 2bcc:a1e:fb9c:d4c::7a:76cd
D) 2bcc:a1e:fb9c:d4c:0:7a0:76cd

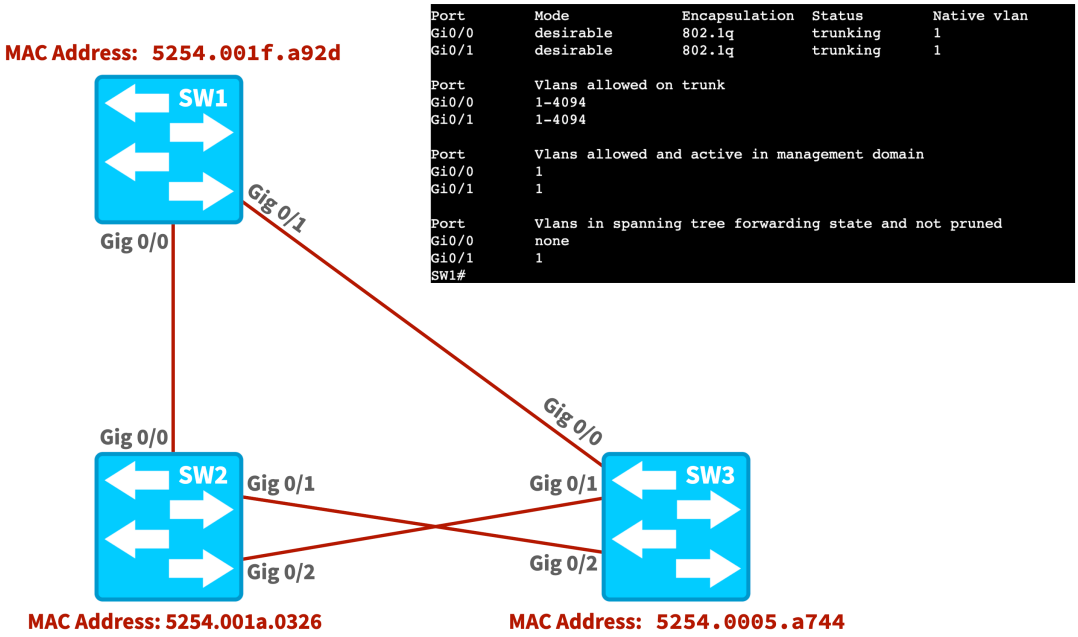
Q80. In the context of SVIs on a Layer 3 switch, what determines whether the virtual interface for a VLAN is up and able to route traffic?

A) The physical interface connected to the switch's management port must be up.
B) There must be at least one active port in the VLAN associated with the SVI.
C) A routing protocol needs to be configured and operational on the switch.
D) The SVI must be manually enabled by an administrator each time the switch restarts.

Q81. As a network architect, you are designing a virtualized network infrastructure. How can you connect virtual network interface cards (vNICs) of different virtual machines in order to organize network traffic effectively?

A) By connecting vNICs to multiple physical routers
B) By connecting vNICs to a virtual switch
C) Linking each vNIC to a separate physical network interface card
D) Assigning each vNIC to a unique subnet without VLANs

Q82. Consider the following topology and output. What command produced the output shown?




```
Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       desirable        802.1q         trunking      1
Gi0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1
Gi0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       none
Gi0/1       1
SW1#
```

A) show interfaces trunk
B) show switchport vlans allowed
C) show switchport trunk
D) show trunk

Q83. You are tasked with enhancing network security by configuring features on your switches. On switches SW1 and SW2, you configure the Root Guard feature on GigabitEthernet 0/1. What happens if a superior BPDU is received on these interfaces?

A) The port immediately shuts down.
B) The switch reboots.
C) The port transitions into a root-inconsistent state.
D) The port ignores the BPDU and continues normal operation.

Q84. Which of the following is the correct command for creating a floating static route that will be used as a backup to an OSPF route?

A) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 91
B) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 backup
C) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 ospf preferred
D) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 111

Q85. What is designated by the all-zero address 0.0.0.0/0 in a routing table?

A) Next-Hop Address
B) Default Gateway
C) Default Route
D) Unknown Route

Q86. As a network engineer, you're tasked with identifying the correct port roles and states in a RapidPVST+ enabled network. If a switch port is configured to connect to an end-user device and should bypass the usual STP convergence times, what type of port and corresponding Cisco switch feature should be applied?

A) Designated port with UplinkFast enabled
B) Root port with BackboneFast enabled
C) Edge port with PortFast enabled
D) Alternate port with Rapid Transition enabled

Q87. When using Multiprotocol Label Switching (MPLS), what information is used to make frame forwarding decisions?

A) IP Address
B) Shim Header
C) DLCI
D) MAC Address

Q88. Which port state in Rapid Per-VLAN Spanning Tree (Rapid PVST+) is a combination of the Listening and Learning port states found in traditional STP?

A) Learning
B) Discarding
C) Forwarding
D) Listening

Q89. What does the IPv6 loopback address "::1" primarily represent in network testing?

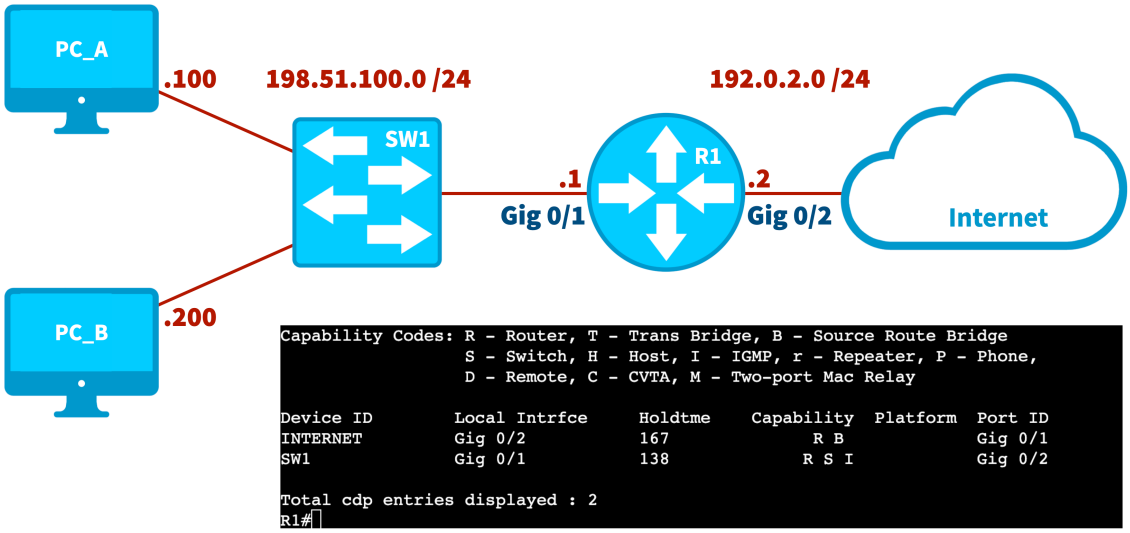
A) It is a destination address used for a host to send packets back to itself.
B) It is used to identify the machine's external IPv6 address.
C) It indicates a multicast group within the local network.
D) It represents the router's address within an IPv6 network.

Q90. How many hexadecimal quartets are found within an IPv6 address?

A) 1
B) 4
C) 8
D) 16

Questions and Answers

Q1. Consider the following topology and output. Which of the following commands produced the output?



A) show lldp neighbors
B) show cdp neighbors detail
C) show ip ospf neighbors
D) show cdp neighbors

Answer: D

Explanation: The output shown is from the `show cdp neighbors` command, which shows information about Layer 2 adjacent devices configured to run Cisco Discovery Protocol (CDP). You can optionally add the keyword of `detail` to the end of the command to get more detailed information about these neighbors. However, the output provided here only provides summary information about router R1's CDP neighbors.

Q2. Which WLAN design would you use if you need to extend wireless coverage to a remote location without direct Ethernet connectivity?

A) Infrastructure WLAN
B) Ad Hoc WLAN
C) Mesh WLAN
D) Peer-to-Peer WLAN

Answer: C

Explanation: A mesh WLAN design is ideal for extending wireless coverage to remote locations where direct Ethernet connectivity is not available. Mesh nodes (access points) can receive and regenerate wireless signals, allowing for broader coverage.

Q3. You are setting up a router that connects to the Internet but want to avoid maintaining a full Internet routing table. Which of the following should you configure?

A) Static route for each network
B) MAC address filtering
C) A default route
D) Egress interface designation

Answer: C

Explanation: To avoid maintaining a full Internet routing table, you should configure a default route. This route (often listed as the "0.0.0.0/0" network) directs packets with unknown destinations out a specific interface (typically connected to the Internet) or to a specific next-hop IP address (typically the IP address of the Internet Service Provider's router).

Q4. If a company wants to enable communication between a computer in the sales department (VLAN 10) and a computer in the engineering department (VLAN 20), which of the following components is essential?

A) A Layer 2 switch configured with VLANs 10 and 20
B) A dedicated firewall between the two VLANs
C) A router or a Layer 3 switch to route between VLANs
D) A Cisco Express Forwarding (CEF) configuration

Answer: C

Explanation: To enable communication between VLANs, a router or a Layer 3 switch is required to route packets between the different subnets associated with each VLAN. While VLANs divide a network into different broadcast domains, a routing mechanism is necessary to allow inter-VLAN communication.

Q5. Starting with which Wi-Fi standard can an access point both send and receive multiple spatial streams at the same time?

A) Wi-Fi 4 (802.11n)
B) Wi-Fi 5 (802.11ac)
C) Wi-Fi 6 (802.11ax)
D) Wi-Fi 7 (802.11be)

Answer: C

Explanation: Starting with Wi-Fi 6 (802.11ax), an access point can both send and receive multiple spatial streams at the same time. This advancement improves the overall capacity and performance of wireless networks.

Q6. You are designing a network to include EtherChannel for higher bandwidth and redundancy. Which of the following is a benefit of utilizing EtherChannel in your network design?

A) EtherChannel reduces the number of IP addresses needed for the links between switches.
B) EtherChannel can aggregate up to eight links, providing increased bandwidth and redundancy without affecting the port channel port if a single link goes down.
C) EtherChannel allows for non-contiguous links to be logically bundled together, reducing physical cabling.
D) EtherChannel eliminates the need for Spanning Tree Protocol, thereby simplifying network configuration and management.

Answer: B

Explanation: One of the primary benefits of EtherChannel is its ability to logically bundle up to eight links between switches. This aggregation increases overall bandwidth and provides redundancy, as the failure of a single link does not bring down the entire port channel. This capability enhances network performance and reliability without disabling Spanning Tree Protocol.

Q7. In the process of OSPF verification, you examine the OSPF database on a router. What would you expect to find in the Summary Net Link States section of the OSPF database?

A) Detailed topological information of all areas
B) A list of OSPF neighbors and their states
C) OSPF router IDs and their corresponding IP addresses
D) A listing of networks in other areas

Answer: D

Explanation: The Summary Net Link States section of the OSPF database, contains a listing of networks in other areas. This section is constructed using Type 3 LSAs (Link-State Advertisements), which an ABR (Area Border Router) generates to inform routers in one area about networks located in other areas. This mechanism allows OSPF to efficiently advertise routing information across different OSPF areas.

Q8. You need to configure a network device with an IP address within the subnet 10.2.4.0 /23. Which of the following IP addresses would be considered valid for a device within this subnet?

A) 10.2.4.255
B) 10.2.5.0
C) 10.2.5.254
D) All of the above

Answer: D

Explanation: The subnet mask /23 or 255.255.254.0 allows for a range of IP addresses from 10.2.4.0 to 10.2.5.255. This includes the entire range of addresses within the 10.2.4.x and 10.2.5.x network ranges, making all the options listed valid IP addresses for devices within this subnet. The network address would be 10.2.4.0, and the broadcast address would be 10.2.5.255, with all addresses in between usable for host devices.

Q9. What technology is represented by the IEEE 802.1s standard?

A) PVST
B) Rapid PVST+
C) RSTP
D) MSTP

Answer: D

Explanation: The Cisco implementation of 802.1s is referred to as Multiple Spanning Tree Protocol (MSTP). This maps multiple VLANs into the same spanning-tree instance, supporting up to 16 instances of Rapid Spanning Tree Protocol (RSTP).

Q10. Why is UDP considered an unreliable protocol compared to TCP?

A) UDP does not establish a session before data transmission
B) UDP has a larger header than TCP
C) UDP uses dynamic or private ports for communication
D) UDP traffic is always encrypted for security

Answer: A

Explanation: UDP is considered unreliable because it does not establish a session before data transmission. Unlike TCP, which uses a three-way handshake to set up a connection and ensures reliable delivery of data through acknowledgements, UDP follows a "fire and forget" approach. It sends data without establishing a connection or confirming receipt, making it less reliable but more suitable for applications where speed and low latency are more important than guaranteed delivery, such as voice over IP (VoIP) or streaming media.

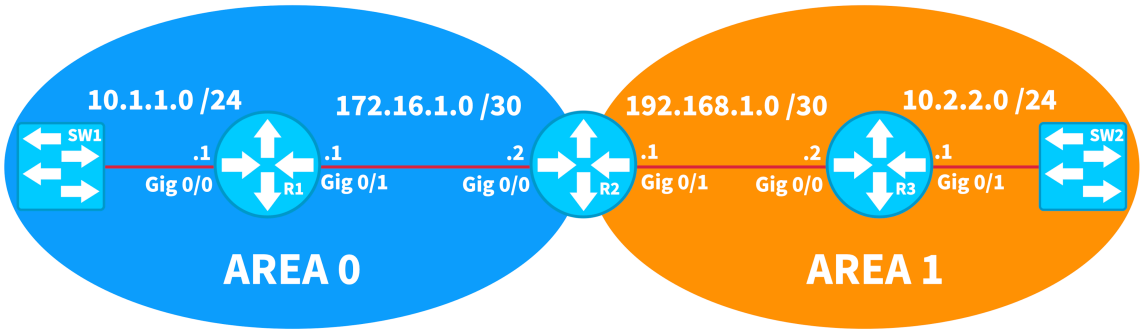
Q11. What purpose does the IPv6 solicited-node multicast address serve in the Duplicate Address Detection (DAD) process?

A) It ensures that the IPv6 address is routable on the Internet.
B) It allocates a unique MAC address to the IPv6 device.
C) It identifies the router's IPv6 address on the network.
D) It verifies that no other device on the network is using the same IPv6 address.

Answer: D

Explanation: In the Duplicate Address Detection process, the IPv6 solicited-node multicast address is used to ensure that a self-assigned IPv6 address is unique and not already in use on a network. The device sends a multicast message to the solicited-node multicast address corresponding to its potential IPv6 address. If no response is received, the address is considered unique and safe to use. This process helps in preventing IP address conflicts within a network.

Q12. Consider the following topology. How many Type 3 LSAs are present in router R3's Link State Database (LSDB)?



A) 1
B) 2
C) 3
D) 4

Answer: B

Explanation: A Type 3 Link State Advertisement (LSA) is known as a "Summary LSA." By default, an Area Border Router (ABR), which is router R2 in this topology, sends a single Type 3 LSA into an area for each network it's advertising from another area. In this example, router R3 is in Area 1, and router R2, acting as the ABR, advertises two networks from Area 0 into Area 1. Specifically, it advertises networks 10.1.1.0 /24 and 172.16.1.0 /30. Router R2 send into Area 1 a separate Type 3 LSA for each of these two networks. Therefore, router R3 will have two Type 3 LSAs in it's Link State Database (LSDB), one for each network in Area 0.

Q13. In Cisco's Collapsed Core architecture model, which two layers are combined?

A) Access and Distribution
B) Distribution and User
C) Access and Core
D) Core and Distribution

Answer: D

Explanation: For smaller topologies where less complexity is needed, this model collapses the Core and Distribution layers into a single layer. This creates a two-tier architecture with an Access layer and a Collapsed Core layer. The Collapsed Core layer performs the combined function of the Core and Distribution layers.

Q14. Which SNMP version introduced significant security improvements such as encryption, integrity checking, and authentication?

A) SNMPv1
B) SNMPv2c
C) SNMPv1c
D) SNMPv3

Answer: D

Explanation: SNMPv3 introduced major security enhancements including encryption, integrity checking, and authentication, making it much more secure than its predecessors. SNMPv1 and SNMPv2c had weaker security mechanisms that relied on community strings.

Q15. Which type of cabling issue can result in hearing part of a voice conversation from another circuit?

A) Attenuation
B) Crosstalk
C) Jitter
D) Latency

Answer: B

Explanation: Crosstalk occurs when a signal transmitted on copper medium radiates to a neighboring data channel, potentially interfere with and degrading communication. This is commonly seen in telecommunication signals, which can result in hearing part of a neighboring voice conversation from another circuit.

Q16. Which Syslog severity level is the most severe?

A) Level 0 - Emergencies
B) Level 1 - Alerts
C) Level 2 - Critical
D) Level 3 - Errors

Answer: A

Explanation: Severity level 0, or Emergencies, is the most severe level in Syslog. It indicates a condition that affects the entire system and requires immediate attention.

Q17. What is the directed broadcast address of a subnet containing an IP address of 172.16.1.10 /19?

A) 172.16.15.255
B) 172.16.31.255
C) 172.16.255.255
D) 172.16.95.255
E) 172.16.0.255

Answer: B

Explanation: To determine the subnets, assignable IP address ranges, and directed broadcast addresses created by the 19-bit subnet mask we perform the following steps:

Step #1: Identify the interesting octet (i.e., the octet that contains the first zero in the binary subnet mask).
In this question, we have a 19-bit subnet mask, which is written in binary as:
11111111 11111111 11100000 00000000
The interesting octet is the third octet, because the third octet (i.e., 11100000) is the first octet to contain a 0 in the binary.

Step #2: Identify the decimal value in the interesting octet of the subnet mask.
A 19-bit subnet mask can be written in dotted decimal notation as:
255.255.224.0
Since the third octet is the interesting octet, the decimal value in the interesting octet is 224.

Step #3: Determine the block size by subtracting the decimal value of the interesting octet from 256.
Block Size = 256 – 224 = 32

Step #4: Determine the subnets by counting by the block size in the interesting octet, starting at 0.
Placing a zero in the first interesting octet identifies the first subnet as:
172.16.0.0 /19
We then count by the block size (of 32) in the interesting octet (the third octet in this question) to determine the remaining subnets:

172.16.32.0 /19
172.16.64.0 /19
172.16.96.0 /19
172.16.128.0 /19
172.16.160.0 /19

172.16.192.0 /19
172.16.224.0 /19

Step #5: Identify the subnet address, the directed broadcast address, and the usable range of addresses.
Looking through the subnets created by the 19-bit subnet mask reveals that the IP address of 172.16.1.10 resides in the 172.16.0.0 /19 subnet.
The directed broadcast address, where all host bits are set to a 1, is 1 less than the next subnet address.
The next subnet address is 172.16.32.0. So, the directed broadcast address for the 172.16.0.0 /19 subnet is 1 less than 172.16.32.0, which is:
172.16.31.255
The usable IP addresses are all the IP addresses between the subnet address and the directed broadcast address. Therefore, in this example, the assignable IP address range for the 172.16.0.0 /19 network is: 172.16.0.1 – 172.16.31.254

Q18. When a client attempts to obtain network information through Dynamic Host Configuration Protocol (DHCP), which unicast message from the client requests network addressing information from the server?

A) REQUEST
B) DISCOVER
C) OFFER
D) ACKNOWLEDGEMENT

Answer: A

Explanation: After the OFFER message is sent from the server to the client, the client now knows the IP address of the DHCP server and is able to communicate directly through unicast. The REQUEST message requests that the DHCP server assign an IP address and other configuration values to the client.

Q19. What is the primary advantage of using Infrastructure as Code (IaC) with tools like Terraform?

A) It eliminates the need for network security.
B) It automates the creation and management of a virtual infrastructure.
C) It replaces the need for cloud service providers.
D) It physically installs and configures network hardware.

Answer: B

Explanation: The primary advantage of using Infrastructure as Code (IaC) with tools like Terraform is that it automates the creation and management of a virtual infrastructure. This approach allows administrators to define their infrastructure using code, which can then be version-controlled, replicated, and easily modified, leading to more consistent and efficient infrastructure management.

Q20. With which category of routing protocol is the Dijkstra Algorithm used?

A) Link-State
B) Distance-Vector
C) Path-Vector
D) Route-Vector

Answer: A

Explanation: The Dijkstra Algorithm is used for finding the shortest path between nodes and is used in the Open Shortest Path First (OSPF) routing protocol. This falls under the category of link-state protocols, where every node constructs a map of the connectivity in the network.

Q21. Which type of Wide Area Network (WAN) has built-in redundancy due to the ring topology used?

A) Metropolitan Area Network (MAN)
B) Multiprotocol Label Switching (MPLS)
C) Virtual Private Network (VPN)
D) Point-to-Multipoint

Answer: A

Explanation: Because a Metropolitan Area Network (MAN) is connected in a ring topology, a break in the network at any point would still allow a connection between any two points.

Q22. With IPv6 multicast communication, how many bits are dedicated to the group ID?

A) 64
B) 112
C) 107
D) 86

Answer: B

Explanation: The final 112 bits in an IPv6 multicast address are reserved for the multicast group ID. This is the address that will be joined by devices desiring to receive a particular multicast stream.

Q23. In the context of WPA2 wireless configuration, what does PSK stand for?

A) Private Secure Key
B) Public Shared Key
C) Pre-Shared Key
D) Protected Security Key

Answer: C

Explanation: PSK stands for Pre-Shared Key, which can be used in WPA2 wireless configurations for user authentication by pre-configuring a key on both an access point and a client device.

Q24. In the context of Network Address Translation (NAT), what terminology is used to describe the original, unaltered IP address of a device located inside the network, before any translation has occurred?

A) Inside Local
B) Inside Global
C) Outside Local
D) Outside Global

Answer: A

Explanation: The term Inside Local refers to the original, unaltered IP address of a device on the inside of the network, as seen from the inside network itself. It is the private IP address assigned to a device, which is not routable on the public Internet. NAT modifies this address to an Inside Global address for communication over the Internet.

Q25. Which type of cabling would be used if required to run through a raised floor or above drop-ceiling tiles?

A) Unshielded Twisted-Pair
B) Shielded Twisted-Pair
C) Plenum-Rated
D) RG-58/U

Answer: C

Explanation: Plenum-rated cable has a special insulation that has low smoke and low flame characteristics. This is mandated for any situation where cabling needs to be ran through an air handling space, such as below raised floors or inside drop-ceilings.

Q26. Which fiber optic connector is known for its straight tip design and utilizes a bayonet-style attachment mechanism?

A) ST connector
B) LC connector
C) SC connector
D) MTRJ connector

Answer: A

Explanation: The ST connector, known for its straight tip design, uses a bayonet-style attachment mechanism. To connect it, you push and twist it into a fiber receptacle, and the tension in a spring holds the connector in place. This design makes it distinct from connectors like the LC, SC, and MTRJ, with the LC connector being smaller and having a tab for release, the SC connector being square-shaped, and the MTRJ connector incorporating two fibers into one connector for increased port density.

Q27. A network administrator is implementing Cisco Catalyst Center in their enterprise network. Which of the following is NOT a primary feature offered by this SDN controller?

A) Network design and provisioning
B) Configuration monitoring and troubleshooting
C) Custom application development platform
D) Direct control of data center fabric switches

Answer: D

Explanation: Direct control of data center fabric switches is not a primary feature offered by Cisco Catalyst Center. Cisco Catalyst Center (formerly Cisco DNA Center) is designed primarily for enterprise campus and branch networks, not for data center environments. Its main features include network design, device provisioning, configuration management, monitoring, troubleshooting, and serving as a platform for custom application development through APIs. For data center fabric control, Cisco offers the APIC (Application Policy Infrastructure Controller) as part of its ACI (Application Centric Infrastructure) solution. Cisco Catalyst Center focuses on intent-based networking for enterprise environments rather than direct control of data center-specific technologies.

Q28. Which QoS mechanism, by default, drops traffic that exceeds a configured bandwidth limit?

A) Policing
B) Shaping
C) Queuing
D) Link Efficiency

Answer: A

Explanation: The two primary Quality of Service (QoS) mechanisms that can limit the amount of bandwidth used are Policing and Shaping. These are known as "traffic conditioners." Policing is more strict than Shaping and, by default, drops traffic exceeding a configured bandwidth limit (the Committed Information Rate (CIR)). Shaping, however, delays excess traffic rather than dropping it.

Q29. Which type of network connection is used in a switched network where devices are able to communicate in full-duplex mode with one another?

A) Ethernet Bus
B) Shared Media Hub
C) Direct Connect
D) Point-to-Point

Answer: D

Explanation: Ethernet switches are connected in a star topology, using a point-to-point connection to each device. Each of the connected devices are able to communicate in full-duplex, meaning they can transmit and receive data simultaneously.

Q30. Which of the following statements is true about the order of rules in an ACL?

A) The rules can be in any order, because the router processes all rules simultaneously.
B) The more specific rules should be placed at the bottom of the list.
C) The order of rules is not important as there is no implicit deny at the end of the ACL.
D) The more specific rules should be placed at the top of the list to ensure they are evaluated first.

Answer: D

Explanation: ACLs are processed in a top-down order, meaning that the first matching rule will be applied. Therefore, more specific rules should be placed at the top to ensure they are evaluated before any broader rules that might permit or deny traffic prematurely.

Q31. Which of the following represents the first two hexadecimal values of every IPv6 multicast address?

A) FE
B) F0
C) 0E
D) FF

Answer: D

Explanation: The first 8 bits in every IPv6 multicast address are set to the all 1s value of 1111 1111. This converts to the hexadecimal value FF, which is how every IPv6 multicast address begins.

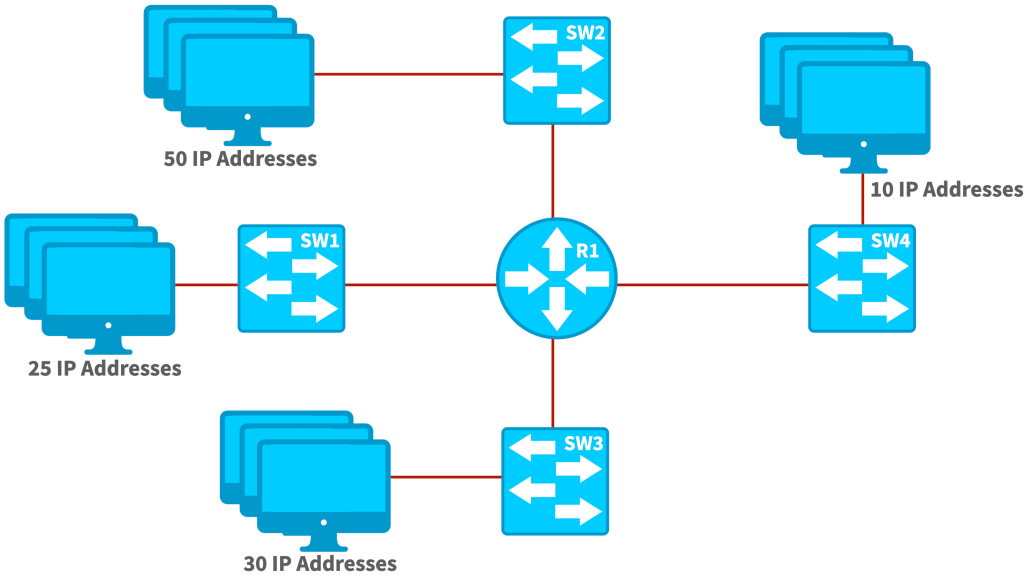
Q32. Your network needs to support several link speeds. To support multiple link speeds greater than 1 Gbps, you consider using STP's Long Path Cost method to determine port cost. Under the Short Path Cost method, what is the port cost assigned to a 1 Gbps link?

A) 2
B) 4
C) 19
D) 100

Answer: B

Explanation: In the traditional Spanning Tree port cost method (i.e., Short Path Cost method), each port speed has a predefined cost, with a 1 Gbps port assigned a cost of 4. This method allows STP to determine the most efficient path to the root bridge by comparing the cumulative port costs required to reach the root bridge.

Q33. What subnet mask should be used to subnet the 192.168.10.0 network to support the number of subnets and IP addresses per subnet shown in the following topology?



A) 255.255.255.0
B) 255.255.255.128
C) 255.255.255.192
D) 255.255.255.224
E) 255.255.255.240

Answer: C

Explanation: To meet the design requirements, four subnets must be created, and each subnet must accommodate a maximum of 50 IP addresses.
We can begin by creating a listing of how many subnets are created from different numbers of borrowed bits, using the formula:
Number of Subnets Created = 2^s, where s is the number of borrowed bits

1 borrowed bits => 2 subnets

2 borrowed bits => 4 subnets
3 borrowed bits => 8 subnets
4 borrowed bits => 16 subnets
5 borrowed bits => 32 subnets
6 borrowed bits => 64 subnets
7 borrowed bits => 128 subnets

From this, we can see we need at least 2 borrowed bits to accommodate 4 subnets. However, we need to make sure the subnet will accommodate 50 IP addresses. To determine this, we can use the formula:
Number of IP Addresses = 2^h – 2, where h is the number of host bits
If we have 2 borrowed bits (i.e., the minimum number of borrowed bits required for 4 subnets), we have 6 host bits (i.e., 8 – 2 = 6). From the above formula, we can determine the number of IP addresses supported by 6 host bits.
Number of IP Addresses = 2^6 – 2 = 62
Since 6 host bits meet our requirement of at least 50 IP addresses per subnet, we can use a 26-bit subnet mask (i.e., 2 bits added to the Class C default mask (also known as the natural mask) of 24 bits). A 26-bit subnet mask can be written as: 255.255.255.192

Q34. A customer is using a Class C network of 192.168.10.0 subnetted with a 28-bit subnet mask. How many subnets can be created by using this subnet mask?

A) 32
B) 16
C) 30
D) 8
E) 14

Answer: B

Explanation: The subnet in this question is a Class C network, because there is a 192 in the first octet. A class C network has a natural mask of 24 bits. However, this network has a 28-bit subnet mask. Therefore, we have 4 borrowed bits, which are network bits added to a network's natural mask (i.e., 2^8 – 24 = 4). The number of subnets can be calculated as follows:
Number of Subnets = 2^s, where s is the number of borrowed bits.
Therefore, in this question, the number of created subnets is 16:
Number of Subnets = 2^4 = 16

Q35. Which Port Security violation mode will disable a port completely when a violation occurs?

A) Protect
B) Restrict
C) Shutdown
D) Monitor

Answer: C

Explanation: The "Shutdown" mode of Port Security will put a port into an error-disabled state when a security violation occurs, preventing any traffic from passing through the port until the port is either manually or automatically re-enabled.

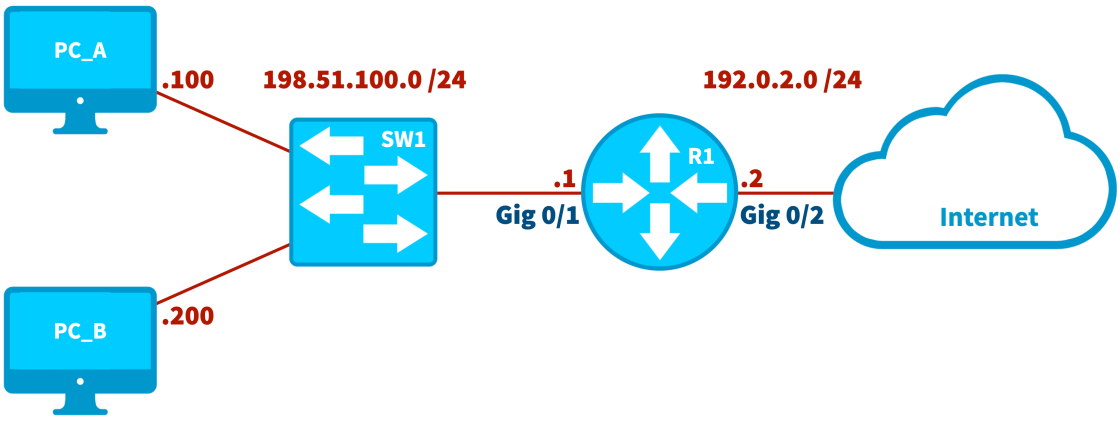
Q36. Which type of IPv6 address can be thought of as being similar to the IPv4 APIPA address range 169.254.0.0 /16?

A) Global Unicast
B) Loopback
C) Multicast
D) Link Local

Answer: D

Explanation: The link local address can only be used on the local network segment, similar to the IPv4 APIPA address range. With IPv4, an APIPA typically indicates an issue with interface communication, but this is not true with IPv6 link-local addresses. They are used by routing protocols for neighborship formation, self-assignment of IPv6 addresses, and more.

Q37. Consider the following topology and ACL configuration. Which of the following configurations will prevent PC_A (198.51.100.100) from reaching the Internet, while permitting PC_B (198.51.100.200) to reach the Internet?



A)
R1(config)# access-list 50 permit any
R1(config)# access-list 50 deny host 198.51.100.100
R1(config)# int gig 0/2
R1(config-if)# ip access-group 50 out
R1(config-if)#

B)
R1(config)# access-list 50 deny host 198.51.100.100
R1(config)# access-list 50 permit any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 50 out
R1(config-if)#

C)
R1(config)# access-list 150 deny host 198.51.100.100
R1(config)# access-list 150 permit any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 150 out
R1(config-if)#

D)
R1(config)# access-list 50 deny host 198.51.100.100
R1(config)# access-list 50 permit any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 50 in
R1(config-if)#

Answer: B

Explanation: In this example, a Standard ACL is being used, because we're not concerned about a specific destination or a port number.
Option A is incorrect, because the first Access Control Entry (ACE) will permit both PCs, before the second ACE has an opportunity to deny PC_A.
Option B is correct, because it blocks PC_A before permitting all other IP addresses. Also, the ACL is applied outbound on R1's Gig 0/2 interface. This follows the best practice of placing Standard ACLs as close to the destination as possible.
Option C is incorrect, because the ACL number is 150, which is used for an Extended ACL, not a Standard ACL.
Option D is incorrect, because the ACL is applied inbound on R1's Gig 0/2 interface, rather than outbound (i.e., going out to the Internet).

Q38. Which type of wireless access point (AP) is more common in large enterprise networks?

A) Autonomous
B) Standalone
C) Master
D) Lightweight

Answer: D

Explanation: Lightweight access points (APs) are controlled by a wireless LAN controller, which can coordinate frequencies and signal strengths between all of the managed devices from a central location.

Q39. You are diagnosing network issues in a newly set up office network and notice a device with an IP address of 169.254.1.5. Understanding the nature of this IP address, what issue is most likely present?

A) The device could not obtain an IP address from a DHCP server and assigned itself an IP address.
B) The device is configured with a static IP address intended for public Internet use.
C) The device has successfully obtained an IP address from a DHCP server.
D) The device is using a private IP address, which is causing conflicts within the network.

Answer: A

Explanation: The IP address 169.254.1.5 falls within the 169.254.0.0/16 range, which is known as the Automatic Private IP Addressing (APIPA) range. Devices with IP addresses in this rage have assigned themselves an IP address when they failed to obtain an IP address from a DHCP server. This is a common issue when a device is connected to a network but cannot communicate with a DHCP server, indicating a potential DHCP configuration or connectivity problem.

Q40. Which command allows us to see which IP addresses have been assigned to the interfaces?

A) R1(config)#show interface brief
B) R1#show interface assignments
C) R1(config)#show ip statistics
D) R1#show ip interface brief

Answer: D

Explanation: From Privileged EXEC mode, the command show ip interface brief will show IP assignments for all of the interfaces, along with the up/down status of the port.

Q41. With an IPv6 global unicast address, what is represented by the last 64 bits of the address?

A) Global Routing Prefix
B) Subnet ID
C) Interface ID
D) Link Local ID

Answer: C

Explanation: All global unicast addresses have a 64-bit interface ID, used to identify interfaces on a link. These are typically composed of a portion of the interface MAC address.

Q42. In the context of emergency services, how can CDP be utilized to assist in identifying a caller's location?

A) By encrypting voice packets to secure data transmission
B) By assigning a unique identifier to each device
C) By learning an IP phone's approximate location based on the location of the switch to which the phone is connected
D) By increasing the bandwidth for emergency calls

Answer: C

Explanation: CDP can be used to help identify the location of a caller in emergency situations by communicating the phone's location based on the location of the switch to which the IP phone is connected. This feature is particularly useful for calls to emergency services, where the physical location of the caller can be crucial for a timely response.

Q43. Which fiber optic connector carries two strands of fiber?

A) MT-RJ
B) ST
C) LC
D) SC

Answer: A

Explanation: MT-RJ connectors carry two strands of fiber, which allows for a higher port density by having transmit and receive strands in the same connector.

Q44. When examining a Cisco router's routing table, you notice routes with different codes such as 'C', 'L', 'D', and 'O'. If your primary concern is identifying the next-hop for a packet destined for an internal network that your router learned via dynamic routing, which code should you look for?

A) C
B) L
C) S
D) O

Answer: D

Explanation: In Cisco routing tables, different codes are used to identify the source of the route information. 'C' indicates a directly connected network, 'L' represents local routes (local IP addresses of the router's interfaces), 'S' is used for statically configured routes, and 'O' identifies routes learned via OSPF (Open Shortest Path First). If the primary concern is identifying the next-hop for a packet learned via dynamic routing for an internal network, 'O' would be the correct option of those listed.

Q45. Which protocol is considered more secure due to its two-way challenge-response mechanism and full packet encryption?

A) RADIUS
B) TACACS+
C) LDAP
D) AD

Answer: B

Explanation: TACACS+ is considered more secure than RADIUS because it uses a two-way challenge-response mechanism and encrypts the entire packet during transmission, whereas RADIUS only encrypts the password.

Q46. When examining the structure of an IPv6 link local address, which of the following is true?

A) The first 48 bits are used to specify the network prefix.
B) The first 10 bits are fixed, followed by 54 bits set to zero and the last 64 bits forming the interface ID.
C) The entire address is dynamically generated without any fixed portion.
D) It includes a global routing prefix to ensure it is routable across the Internet.

Answer: B

Explanation: An IPv6 link local address begins with FE80::/10, followed by 54 zeros. Therefore, since the last 2 bits in the third hexadecimal digit and all 4 bits in the fourth hexadecimal digit are zeros, we can conclude that all IPv6 link local addresses begin with FE80 in the first quartet. The last half of a link local address (i.e., the last 64 bits) represent the interface ID and are often calculated using the EUI-64 addressing process.

Q47. Which OSPF metric is used to determine Designated Router (DR) election?

A) Lowest Router ID
B) Highest Router ID
C) Lowest OSPF Priority
D) Highest OSPF Priority

Answer: D

Explanation: The router with the highest OSPF priority will win the election and become the Designated Router (DR). If there is a tie in the priority values, the router with the highest router ID will win the DR election.

Q48. For a data center requiring a fiber optic connection that supports 10 Gbps over a maximum distance of 300 meters, which Ethernet standard and fiber type should be used?

A) 10GBASE-SR with multimode fiber (50 micrometers core)
B) 10GBASE-LR with single mode fiber
C) 10GBASE-SR with multimode fiber (62.5 micrometers core)
D) 10GBASE-LX with single mode fiber

Answer: A

Explanation: 10GBASE-SR with multimode fiber (50 micrometers core) is the best choice for a data center requiring 10 Gbps connectivity over a distance of 300 meters. This standard is designed for short-range applications and, when used with higher-grade multimode fiber with a core diameter of 50 micrometers, can support distances up to 400 meters. 10GBASE-LR is designed for long-range applications using single mode fiber and supports distances much greater than 300 meters. 10GBASE-SR with a 62.5 micrometers core and 10GBASE-LX are not as well-suited for this specific requirement.

Q49. As a network administrator, you want to selectively prevent the transmission of a device's system name in LLDP advertisements to enhance privacy. Which command accomplishes this at the global configuration level?

A) no lldp run
B) no lldp tlv-select system-name
C) lldp tlv-select system-name
D) no lldp tlv-select all

Answer: B

Explanation: The `no lldp tlv-select system-name` command at the global configuration level specifically blocks a system name from being included in LLDP advertisements, enhancing privacy by not disclosing the device's identity. This selective approach allows other LLDP information to continue being transmitted, providing flexibility in controlling the scope of shared network information.

Q50. Which prerequisite must be enabled on a switch before configuring Dynamic ARP Inspection (DAI)?

A) Port Security
B) DHCP Snooping
C) VLAN Trunking
D) Spanning Tree Protocol

Answer: B

Explanation: DHCP Snooping must be enabled before configuring Dynamic ARP Inspection (DAI), as DAI uses the DHCP Snooping binding table to validate ARP messages.

Q51. Given a subnet of 172.16.56.0 /21, identify which of the following IP addresses belong to this subnet. (Select 2.)

A) 172.16.54.129
B) 172.16.62.255
C) 172.16.61.0
D) 172.16.65.255
E) 172.16.64.1

Answer: B and C

Explanation: To determine subnets and usable address ranges created by the 21-bit subnet mask we perform the following steps:

Step #1: Identify the interesting octet (i.e., the octet that contains the first zero in the binary subnet mask).
In this question, we have a 21-bit subnet mask, which is written in binary as:
11111111 11111111 11111000 00000000
The interesting octet is the third octet, because the third octet (i.e., 11111000) is the first octet to contain a 0 in the binary subnet mask.

Step #2: Identify the decimal value in the interesting octet of the subnet mask.
A 21-bit subnet mask can be written in dotted decimal notation as: 255.255.248.0
Since the third octet is the interesting octet, the decimal value in the interesting octet is 248.

Step #3: Determine the block size by subtracting the decimal value of the interesting octet from 256.
Block Size = 256 – 248 = 8

Step #4: Determine the subnets by counting by the block size in the interesting octet, starting at 0.
Placing a zero in the first interesting octet identifies the first subnet as:
172.16.0.0 /21
We then count by the block size (of 8) in the interesting octet (the third octet in this question) to determine the remaining subnets:

172.16.8.0 /21
172.16.16.0 /21
172.16.24.0 /21
172.16.32.0 /21
172.16.40.0 /21
172.16.48.0 /21
172.16.56.0 /21
172.16.64.0 /21
... SUBNETS OMITTED ...

We can stop counting after we pass the subnet we are being asked about. Specifically, in this question, we're being asked about 172.16.56.0 /21.

Step #5: Identify the subnet address, the directed broadcast address, and the usable range of addresses.
The subnet address, where all host bits are set to a 0, is given: 172.16.56.0 /24
The directed broadcast address, where all host bits are set to a 1, is 1 less than the next subnet address.
The next subnet address is 172.16.64.0. So, the directed broadcast address for the 172.16.54.0 /21 subnet is 1 less than 172.16.64.0, which is: 172.16.63.255
The usable IP addresses are all the IP addresses between the subnet address and the directed broadcast address. Therefore, in this example, the usable IP address range for the 172.16.56.0 /21 network is: 172.16.56.1 – 172.16.63.254
The only IP addresses in this question that reside in this range are:
172.16.62.255
172.16.61.0

NOTE: Many CCNA candidates look at IP addresses like these and immediately assume they are not usable IP addresses, because they have a 0 or a 255 in the fourth octet. They argue that 172.16.61.0 is a subnet address and that 172.16.62.255 is a directed broadcast address.
While that would only be true of the subnet mask were 24-bits, remember that, by definition, a subnet address has all of its host bits set to a 0, and a directed broadcast address has all of its host bits set to a 1. In this question, we have 11 host bits (i.e., 32 – 21 = 11), not 8 host bits. So, 172.16.62.255 and 172.16.61.0 are actually usable IP addresses.

Q52. Which of the following DNS record types is used to translate a Fully Qualified Domain Name (FQDN) into an IPv4 address?

A) A record
B) CNAME record
C) MX record
D) PTR record

Answer: A

Explanation: An Address (A) record is used by a DNS server to map a fully qualified domain name (FQDN) to its corresponding IPv4 address, allowing devices on the Internet to locate each other and communicate. CNAME records are used for aliases to other domain names. MX records are used for mail exchange servers. PTR records are used for reverse DNS lookups, mapping IP addresses back to their domain names.

Q53. Which part of the fiber optic cable is used to reflect light along the data path?

A) Dopant
B) Jacket
C) Cladding
D) Core

Answer: C

Explanation: The cladding layer surrounds the core and helps guide the light along the path of the core. The cladding can be made of plastic or glass and is less transparent than the core. The difference in the refraction index of the core and cladding is what causes a mirror-like surface, which helps propagate the light through the cable.

Q54. A network administrator needs to ensure that a newly installed PoE switch can provide adequate power for several devices, including VoIP phones and surveillance cameras. The devices require up to 15.4 watts each to operate. Which IEEE standard for PoE should the administrator ensure the switch supports to meet this requirement?

A) IEEE 802.3at
B) IEEE 802.3af
C) IEEE 802.3bt
D) IEEE 802.3ab

Answer: B

Explanation: The IEEE 802.3af standard for Power over Ethernet (PoE) supports delivery of up to 15.4 watts of power per port, which matches the requirement for the devices mentioned. The 802.3at and 802.3bt standards support higher power levels, while the 802.3ab standard pertains to Gigabit Ethernet over twisted pair, not PoE.

Q55. What is the purpose of configuring the `transport input ssh` command on VTY lines?

A) To disable Telnet access and allow only SSH connections
B) To enable password encryption
C) To set up SNMP monitoring
D) To assign IP addresses to VTY lines

Answer: A

Explanation: The `transport input ssh` command on VTY lines disables Telnet access and allows only SSH connections, ensuring that remote access to the router is secure and encrypted.

Q56. Which routing protocol has a default administrative distance (AD) value of 90?

A) EIGRP
B) RIP
C) OSPF
D) BGP

Answer: A

Explanation: Enhanced Interior Gateway Routing Protocol (EIGRP) has a default AD value of 90. This would be preferred by default over Open Shortest Path First (OSPF), which has a higher AD value of 110.

Q57. Which value makes up the last 24 bits of an IPv6 solicited-node multicast address?

A) Destination IPv6 address
B) Source IPv6 Address
C) Link Local IPv6 Address
D) Global Unicast Address

Answer: A

Explanation: The first 104 bits in an IPv6 solicited-node multicast are set to the hexadecimal value FF02::1:FF. The remaining bits come from the last 24 bits of the IPv6 address to which this multicast address is destined for. For example, if a solicited-node multicast message is destined for a router at 3000::2, the complete solicited-node multicast address would be FF02::1:FF00:2.

Q58. A network architect is implementing a Software Defined Networking (SDN). Which of the following best describes the relationship between the underlay and overlay networks in this context?

A) The underlay network is virtual, while the overlay network is physical
B) The underlay network is physical, while the overlay network is logical
C) The underlay and overlay networks are both physical
D) The underlay and overlay networks are both virtual

Answer: B

Explanation: In the context of SDN, an underlay network represents the physical infrastructure, including the actual switches, routers, and physical connections. An overlay network, on the other hand, is a logical network created on top of the physical underlay. This overlay network is defined in software and can contain virtual topologies that might not directly correspond to the network's physical interconnections. This allows for greater flexibility in network design and segmentation, enabling features like VXLANs (in a data center environment) to create logical network segments that span across a physical infrastructure.

Q59. Which routing protocol has a default administrative distance (AD) value of 110?

A) EIGRP
B) RIP
C) OSPF
D) BGP

Answer: C

Explanation: Open Shortest Path First (OSPF) has a default AD value of 110. By default, Enhanced Interior Gateway Routing Protocol (EIGRP) would be preferred over OSPF since it has a lower AD value of 90.

Q60. Considering IPv6 does not support the traditional broadcast traffic flow, which IPv6 traffic type effectively replaces the functionality provided by broadcasting?

A) Multicast
B) Unicast
C) Anycast
D) None of the above

Answer: A

Explanation: In IPv6, the absence of a broadcast traffic type is mitigated by the enhanced functionality of Multicast. Multicast allows for one-to-many communication, where a single packet can be sent to multiple destinations (members of a multicast group) efficiently. This serves the purposes previously fulfilled by broadcasting in IPv4, such as discovering devices or services on the network, but in a more controlled and efficient manner.

Q61. In a GLBP configuration, how does the Active Virtual Gateway (AVG) ensure that the traffic load is distributed among different routers in a GLBP group?

A) By responding to each ARP request with the same MAC address
B) By responding to each ARP request with the one of multiple MAC addresses
C) By only responding to the first ARP request
D) By redirecting all traffic to the MAC address of the router with the least load

Answer: B

Explanation: In GLBP (Gateway Load Balancing Protocol), the Active Virtual Gateway (AVG) responds to ARP requests from different devices with one of multiple (as many as 4) MAC addresses. These multiple MAC addresses belong to the different Active Virtual Forwarders (AVFs) within a GLBP group, which can contain a maximum of 4 AVFs.

Q62. You are tasked with securing a server. Which of the following would you address as a vulnerability?

A) A brute force attack tool found on the network
B) An unpatched software flaw in the operating system
C) An email attempting to trick users into disclosing passwords
D) A denial of service attack targeting the server

Answer: B

Explanation: A vulnerability is a weakness or flaw within a system that can be exploited. An unpatched software flaw in the operating system represents such a vulnerability that needs to be addressed to prevent exploitation.

Q63. What is the default OSPF network type for serial interfaces not configured for Frame Relay?

A) Broadcast
B) Point-to-point
C) Non-broadcast
D) Point-to-multipoint

Answer: B

Explanation: Serial interfaces not configured for Frame Relay use the point-to-point OSPF network type by default. This network type assumes that there are only two routers on the network segment, which eliminates the need for electing a Designated Router (DR) and Backup Designated Router (BDR).

Q64. What is the final step in a Transmission Control Protocol (TCP) 3-way handshake?

A) SYN/ACK
B) ARP
C) ACK
D) SYN

Answer: C

Explanation: The first step is when a client sends a SYN (synchronization) message to another client or server as a request to begin the 3-way handshake process. The other end will respond with a SYN-ACK (synchronization and acknowledgement) message if the SYN is accepted. The final message is an ACK (acknowledgement) message sent from the original client, which completes the establishment of the TCP session.

Q65. You have been tasked with influencing the DR and BDR election process in an OSPF network. Which command can you use to set the priority value for a router's interface?

A) ospf priority [value]
B) ip ospf dr-priority [value]
C) ospf dr-priority [value]
D) ip ospf priority [value]

Answer: D

Explanation: To influence the DR (Designated Router) and BDR (Backup Designated Router) election process, you can set the priority value for a router's interface using the `ip ospf priority [value]` command in interface configuration mode. The router with the highest priority value will be elected as the DR, and the router with the second-highest priority will become the BDR. If you want to prevent a router interface from participating in the election process, you can set its priority value to 0.

Q66. Which of the following access control entries would correctly deny all IP traffic from a host with the IP address 172.16.5.10?

A) access-list 20 deny 172.16.5.10
B) access-list 20 deny host 172.16.5.10 0.0.0.0
C) access-list 20 deny 172.16.5.10 0.0.0.255
D) access-list 20 deny host 172.16.5.10

Answer: D

Explanation: To deny all IP traffic from a specific host in a numbered standard ACL, you should use the `host` keyword followed by the host's IP address. Therefore, the correct ACE is `access-list 20 deny host 172.16.5.10`. This syntax specifies the host to be denied.

Q67. What is the subnet address of the IP address 192.168.5.55 with a subnet mask of 255.255.255.224?

A) 192.168.5.0 /27
B) 192.168.5.16 /27
C) 192.168.5.32 /27
D) 192.168.5.48 /27
E) 192.168.5.64 /27

Answer: C

Explanation: To determine subnets and usable address ranges created by the 27-bit subnet mask we perform the following steps:

Step #1: Identify the interesting octet (i.e., the octet that contains the first zero in the binary subnet mask).
In this question, we have a 27-bit subnet mask, which is written in binary as:
11111111 11111111 11111111 11100000
The interesting octet is the fourth octet, because the fourth octet (i.e., 11100000) is the first octet to contain a 0 in the binary.

Step #2: Identify the decimal value in the interesting octet of the subnet mask.
A 27-bit subnet mask can be written in dotted decimal notation as:
255.255.255.224
Since the fourth octet is the interesting octet, the decimal value in the interesting octet is 224.
Step #3: Determine the block size by subtracting the decimal value of the interesting octet from 256.
Block Size = 256 – 224 = 32

Step #4: Determine the subnets by counting by the block size in the interesting octet, starting at 0.
Placing a zero in the first interesting octet identifies the first subnet as: 192.168.5.0 /27
We then count by the block size (of 32) in the interesting octet (the fourth octet in this question) to determine the remaining subnets:

192.168.5.32 /27
192.168.5.64 /27
192.168.5.96 /27
192.168.5.128 /27
192.168.5.160 /27
192.168.5.192 /27
192.168.5.224 /27

Now that we have all of our subnets identified, we can determine the subnet in which the IP address of 192.168.5.55 resides.
Since the usable range of IP addresses for the 192.168.5.32 /27 network is 192.168.5.33 – 192.168.5.62 (because 192.168.5.32 is the network address, and 192.168.5.63 is the directed broadcast address), and since 192.168.5.55 is in that range, the subnet to which 192.168.5.55 /27 belongs is: 192.168.5.32 /27

Q68. When IPv6 is enabled on an interface, which type of address is automatically assigned?

A) Global Unicast
B) Loopback
C) Multicast
D) Link Local

Answer: D

Explanation: A link-local address is valid only on the local network segment. When enabling IPv6 on an interface a link-local address is automatically assigned, but this can also be manually configured.

Q69. Which IPv6 address is the equivalent of the IPv4 address 127.0.0.1?

A) ::0
B) 127:0:0:1
C) ::1
D) ::127

Answer: C

Explanation: This address is the specific IPv6 loopback address. The loopback interface has no hardware associated with it, and it is not physically connected to a network. It is primarily used for testing and troubleshooting.

Q70. You are reviewing an IPv6 address that has several quartets with leading zeros (but not all zeros). What rule applies to the abbreviation of these quartets in the address?

A) You must keep all leading zeros for clarity
B) You should replace leading zeros with a single zero
C) You can omit leading zeros only if they are followed by another zero
D) You can omit all leading zeros in each quartet

Answer: D

Explanation: You are allowed to omit all leading zeros in each quartet, simplifying the address and making it shorter and more readable. This technique can be used for any quartet within an IPv6 address, regardless of its position or the hexadecimal digits that follow the leading zeros.

However, if you're working with one or more consecutive quartets containing all zeros (as opposed to just having leading zeros), you can replace the entire quartet(s) with two colons.

Q71. What is a common use case for TFTP in a network environment?

A) Securely transferring sensitive files between servers
B) Downloading configuration files to network devices during bootup
C) Enabling encrypted remote management
D) Monitoring network traffic

Answer: B

Explanation: A common use case for TFTP is downloading configuration files to network devices, such as IP phones, during bootup. This allows devices to quickly obtain necessary configurations without user intervention.

Q72. What multicast address is used by Open Shortest Path First to advertise Hello messages?

A) 223.0.2.0
B) 224.0.0.5
C) 232.0.0.1
D) 225.0.0.0

Answer: B

Explanation: An OSPF-enabled router advertises Hello messages to the multicast address of 224.0.0.5 (or FF02::5 for IPv6), which is a group to which all OSPF-speaking routers belong. 224.0.0.6 (or FF02::6 for IPv6) is a group to which all OSPF DR and BDR routers belong.

Q73. Given the MAC address 0014.2201.2345, which of the following will be the IPv6 link local address?

A) fe80::14:22:01:2345
B) fe80:0014:22ff:fe01:2345
C) fe8::214:22ff:fe1:2345
D) fe80::214:22ff:fe01:2345

Answer: D

Explanation: Splitting the MAC address in the middle creates the values 0014.22 and 01.2345. Next, we insert the value FF.FE in the middle of the MAC address and change the delimiter from a decimal to a colon, giving us the value 0014:22FF:FE01:2345. We then convert the first 8 bits to binary and invert the 7th bit. Each hexadecimal value represents 4 bits, so we convert the first two hexadecimal values (00), which becomes 0000 0000. Inverting the 7th bit creates the binary value 0000 0010. We now convert back to hexadecimal, which changes the first two hexadecimal digits from 00 to 02, for the value 0214:22FF:FE01:2345. Finally, we know that all link local addresses begin with the value FE80, so we insert this value at the beginning of the address. Remembering our rules for abbreviating an IPv6 address, we can drop the leading zero on the first quartet (0214 becomes 214), creating the link local address.

Q74. Which Spanning Tree Protocol (STP) port state is used to populate the CAM table during convergence after a failure?

A) Listening
B) Learning
C) Blocking
D) Forwarding

Answer: B

Explanation: After the Blocking and Listening states, the Learning state ensures that the CAM table is populated with MAC addresses of attached clients and their corresponding switch ports. This state lasts for 15 seconds before transitioning the final operational state of Forwarding.

Q75. Which command configures a switch to takeover in the event that the primary root fails on VLAN 1?

A) SW2(config)#spanning-tree vlan 1 backup root
B) SW2(config)#spanning-tree vlan 1 secondary root
C) SW2(config)#spanning-tree vlan 1 root standby
D) SW2(config)#spanning-tree vlan 1 root secondary

Answer: D

Explanation: This command configures switch SW2 to takeover in the event that the primary root on VLAN 1 fails. Specifically, this command sets the Bridge Priority of a switch to 28672.

Q76. Why is it recommended to place a standard ACL as close to the destination as possible?

A) To reduce the processing load on the route
B) To prevent premature packet dropping
C) To ensure the ACL can be modified easily
D) To improve the performance of the network

Answer: B

Explanation: Standard ACLs only filter based on source IP addresses. If they are placed too close to the source, they might inadvertently block traffic that should be allowed to pass to other parts of the network. Placing them close to the destination minimizes the risk of prematurely dropping packets that need to traverse the network.

Q77. Which protocol is typically used to communicate between a wireless LAN controller and lightweight access points?

A) CAPWAP
B) WPA3
C) SNMP
D) FTP

Answer: A

Explanation: CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol commonly used to manage and control lightweight access points from a centralized wireless LAN controller. It allows for efficient configuration and management of multiple access points, reducing the risk of errors and administrative overhead.

Q78. In an Ethernet switch, how does the switch learn where to forward frames for efficient communication?

A) By using IP address tables
B) By learning MAC addresses from incoming frames
C) Through pre-configured static routes
D) Via periodic broadcast messages

Answer: B

Explanation: An Ethernet switch learns where to forward frames by building a MAC address table. It does this by observing the source MAC addresses of incoming frames and associating them with the corresponding switch ports. This process allows the switch to intelligently forward subsequent frames to their correct destinations without unnecessary flooding.

Q79. Given the IPv6 address 2bcc:0a1e:fb9c:0d4c:0000:0000:07a0:76cd, which abbreviation below is a correct representation?

A) 2bcc:a1e:fb9c:d4c::7a0:76cd
B) 2bcc:0a1e:fb9c:0d4c::07a0:76cd
C) 2bcc:a1e:fb9c:d4c::7a:76cd
D) 2bcc:a1e:fb9c:d4c:0:7a0:76cd

Answer: A

Explanation: The rules for abbreviating an IPv6 address are as follows: (1) Leading zeros in a quartet can be omitted. (2) Consecutive quartets containing all zeros can be represented with a double colon. (3) Only one double colon can be used per address. Given these rules, the leading zeros can be removed from the 2nd (0a1e), 4th (0d4c) and 7th (07a0) quartets. The 5th and 6th quartets consecutively contain all zeros, which can be replaced with a double colon.

Q80. In the context of SVIs on a Layer 3 switch, what determines whether the virtual interface for a VLAN is up and able to route traffic?

A) The physical interface connected to the switch's management port must be up.
B) There must be at least one active port in the VLAN associated with the SVI.
C) A routing protocol needs to be configured and operational on the switch.
D) The SVI must be manually enabled by an administrator each time the switch restarts.

Answer: B

Explanation: An SVI's operational status is contingent upon the existence of at least one active port in the VLAN associated with it. If no ports in the VLAN are up, the SVI is considered down and cannot route traffic. This design ensures that routing decisions are made only for VLANs with active, connected devices.

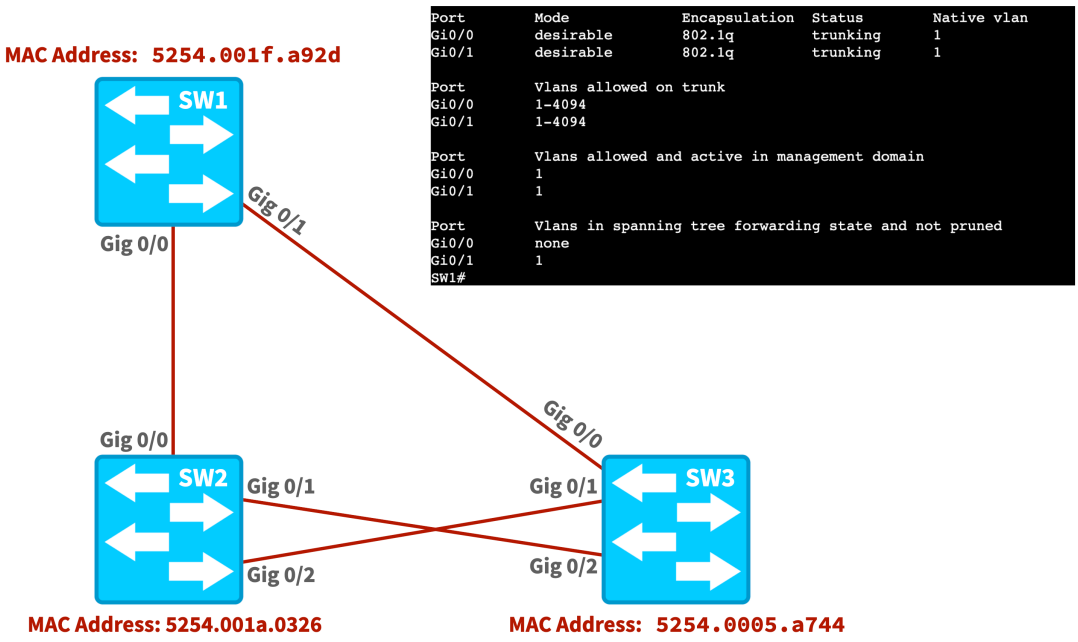
Q81. As a network architect, you are designing a virtualized network infrastructure. How can you connect virtual network interface cards (vNICs) of different virtual machines in order to organize network traffic effectively?

A) By connecting vNICs to multiple physical routers
B) By connecting vNICs to a virtual switch
C) Linking each vNIC to a separate physical network interface card
D) Assigning each vNIC to a unique subnet without VLANs

Answer: B

Explanation: Virtual network interface cards (vNICs) can be effectively connected and organized using a virtual switch, which you can create on the same hypervisor running your virtual machines. This approach allows for the creation of different VLANs for various virtual NICs, enabling sophisticated network configurations. The virtual switch can then connect to the physical network interface card of the host running the hypervisor, in order to connect with an external network.

Q82. Consider the following topology and output. What command produced the output shown?




```
Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       desirable        802.1q         trunking      1
Gi0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1
Gi0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       none
Gi0/1       1
SW1#
```

A) show interfaces trunk
B) show switchport vlans allowed
C) show switchport trunk
D) show trunk

Answer: A

Explanation: The `show interfaces trunk` command displays information for any trunks currently active on a Cisco Catalyst switch. The output also includes such information the VLANs allowed on the trunks and the VLANs that are active on the trunks.

Q83. You are tasked with enhancing network security by configuring features on your switches. On switches SW1 and SW2, you configure the Root Guard feature on GigabitEthernet 0/1. What happens if a superior BPDU is received on these interfaces?

A) The port immediately shuts down.
B) The switch reboots.
C) The port transitions into a root-inconsistent state.
D) The port ignores the BPDU and continues normal operation.

Answer: C

Explanation: When a port configured with Root Guard receives a superior BPDU, the port does not shut down or ignore the BPDU. Instead, it transitions into a "root-inconsistent" state. This state is maintained until the port ceases to receive superior BPDUs, which prevents the switch from being manipulated by potentially malicious users aiming to alter the root bridge designation.

Q84. Which of the following is the correct command for creating a floating static route that will be used as a backup to an OSPF route?

A) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 91
B) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 backup
C) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 ospf preferred
D) R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.10 111

Answer: D

Explanation: The default administrative distance (AD) value for a static route is 1, meaning that the route would be preferred over the OSPF route. If we want to make this a backup route, we must change the AD value to something larger than the AD value of an OSPF route, which is 110.

Q85. What is designated by the all-zero address 0.0.0.0/0 in a routing table?

A) Next-Hop Address
B) Default Gateway
C) Default Route
D) Unknown Route

Answer: C

Explanation: The default route is represented by an all-zero address. A static default route can be manually configured using the command ip route 0.0.0.0 0.0.0.0 followed by the IP address for the router that will be the default route.

Q86. As a network engineer, you're tasked with identifying the correct port roles and states in a RapidPVST+ enabled network. If a switch port is configured to connect to an end-user device and should bypass the usual STP convergence times, what type of port and corresponding Cisco switch feature should be applied?

A) Designated port with UplinkFast enabled
B) Root port with BackboneFast enabled
C) Edge port with PortFast enabled
D) Alternate port with Rapid Transition enabled

Answer: C

Explanation: An edge port in RapidPVST+ terminology refers to a switch port that connects to an end-user device, such as a laptop or a printer, and is not expected to contribute to network loops. By enabling PortFast on these ports, the usual Spanning Tree Protocol (STP) convergence times are bypassed, allowing the port to transition directly to the Forwarding state. This setup is essential for ports where immediate network access is required upon connection, without waiting through the usual STP Listening and Learning states.

Q87. When using Multiprotocol Label Switching (MPLS), what information is used to make frame forwarding decisions?

A) IP Address
B) Shim Header
C) DLCI
D) MAC Address

Answer: B

Explanation: When using MPLS, a 32-but shim header is inserted into a frame between the Layer 2 and Layer 3 headers. This label is used to determine the frame forwarding.

Q88. Which port state in Rapid Per-VLAN Spanning Tree (Rapid PVST+) is a combination of the Listening and Learning port states found in traditional STP?

A) Learning
B) Discarding
C) Forwarding
D) Listening

Answer: A

Explanation: The Learning state performs the combined duties of the traditional STP Learning and Listening states. When in this state, the switch is learning which MAC addresses are available off the port. This state is seen when a port is transitioning to the Forwarding state.

Q89. What does the IPv6 loopback address "::1" primarily represent in network testing?

A) It is a destination address used for a host to send packets back to itself.
B) It is used to identify the machine's external IPv6 address.
C) It indicates a multicast group within the local network.
D) It represents the router's address within an IPv6 network.

Answer: A

Explanation: The IPv6 loopback address "::1" represents a destination address used for a host to send packets back to itself. This is similar to the IPv4 loopback address (127.0.0.1) and is used for testing and configuration purposes, ensuring that the IPv6 stack is functioning correctly on the local machine. It is also commonly used by developers and network administrators to test local network setups, applications, or services running on a device.

Q90. How many hexadecimal quartets are found within an IPv6 address?

A) 1
B) 4
C) 8
D) 16

Answer: C

Explanation: There are 8 quartets found within an IPv6 address, each separated by a colon. Each of the individual quartets contains four hexadecimal digits.