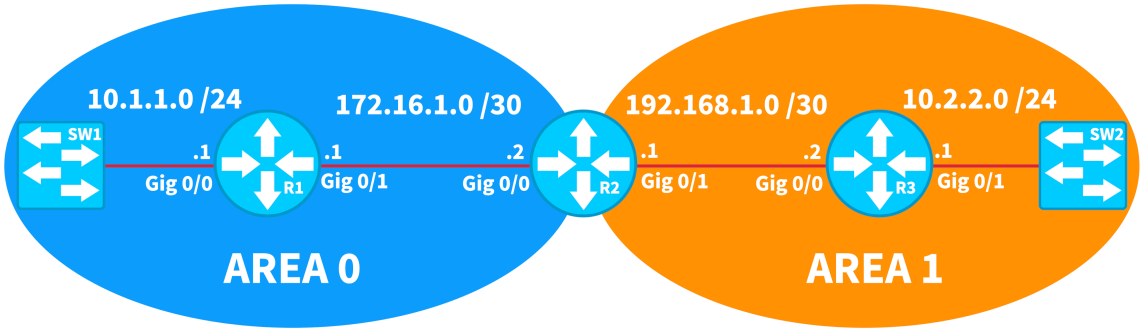
CCNA v1.1 (200-301) Video Training Series
Practice Exam #1

Questions

Q1. Consider the following topology. How many Type 1 LSAs are present in router R3's Link State Database (LSDB)?



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

Q2. What is the collection of multiple Basic Service Sets (BSS) known as?

A) WSSID
B) IBSS
C) BSSID
D) ESSID

Q3. For a data center requiring very high-speed connectivity between devices with a maximum distance of 30 meters, which category of twisted pair cabling is most suitable to support data transmission speeds up to 40 Gbps?

A) Category 6
B) Category 6A
C) Category 7
D) Category 8

Q4. After attaching a new workstation to a switch configured with STP, you observe a delay before the workstation can access the network. Assuming the port was not previously active, what is the default delay before the port becomes active?

A) 15 seconds
B) 30 seconds
C) 50 seconds
D) 20 seconds

Q5. In the context of wireless transmission, what does QAM stand for, and what is its function?

A) Quadrature Amplitude Modulation; it allows multiple bits of data to be sent per subchannel by adjusting phase and amplitude
B) Quality Assurance Method; it ensures data integrity during transmission
C) Quick Access Mode; it prioritizes urgent data packets
D) Quantum Allocation Management; it manages bandwidth allocation using quantum computing principles

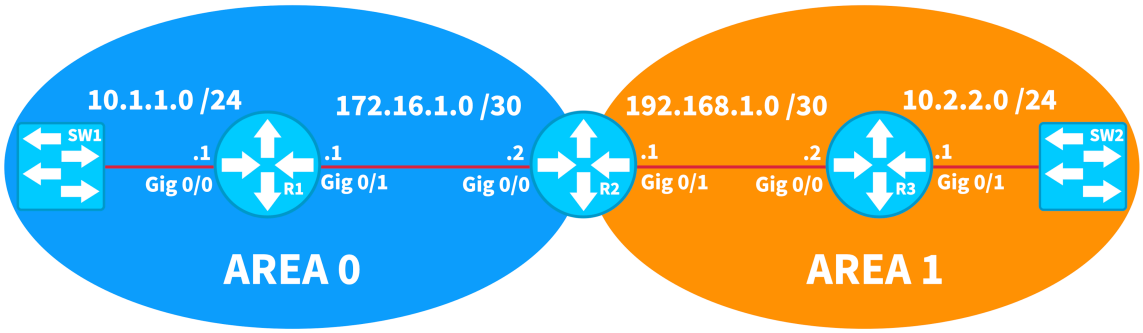
Q6. You've set up a Layer 2 EtherChannel on your Cisco switch and wish to verify the load balancing algorithm in use. Which command could you use to check the current load balancing method?

A) show etherchannel summary
B) show port-channel compatibility
C) show etherchannel load-balance
D) show spanning-tree etherchannel

Q7. An IP address of 192.168.0.100 /27 belongs to which of the following subnets?

A) 192.168.0.92
B) 192.168.0.128
C) 192.168.0.64
D) 192.168.0.96
E) 192.168.0.32

Q8. Consider the following topology. How many Type 2 LSAs are present in router R3's Link State Database (LSDB)?



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

Q9. Which routing protocol is described as being able to provide the entire path (sequence of autonomous systems) a packet will traverse to reach its destination, distinguishing it from other types of routing protocols?

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

Q10. Your network includes a subnet that does not have a DHCP server locally available. What solution allows PCs on this subnet to receive IP addresses from a DHCP server located on a different subnet?

A) Configuring a static route on the PCs
B) Upgrading to a DCHPv6 server
C) Creating an ACL on the next-hop router to permit DHCP messages
D) Implementing a DHCP relay agent on the router

Q11. Which of the following is a valid private address range for a Class C address?

A) 192.168.0.0 – 192.168.255.255
B) 10.0.0.0 – 10.255.255.255
C) 169.254.0.0 – 171.255.255.255
D) 172.16.0.0 – 172.31.255.255

Q12. What is the role of a Wireless LAN Controller (WLC) in an enterprise network?

A) To provide Internet connectivity to clients
B) To serve as a single access point
C) To increase the bandwidth of wireless connections
D) To coordinate the operation of multiple access points

Q13. In the EUI-64 method of generating an IPv6 address, why is the seventh bit of the original MAC address inverted?

A) To indicate that the address is globally unique
B) To differentiate between unicast and multicast addresses
C) To signal that the address has been modified from its original form
D) To designate the address as locally administered

Q14. What is the 48-bit address used by a switch to make frame forwarding decisions?

A) MAC address
B) CAM address
C) IP address
D) Link-local address

Q15. In SNMPv3, what is the purpose of the `snmp-server group` command?

A) To set the SNMP server location
B) To create a group for managing user permissions and encryption settings
C) To specify the contact information for the SNMP server
D) To enable SNMP traps for specific events

Q16. Which command allows us to dynamically learn MAC addresses seen on an interface, rather than using static assignments?

A) SW1(config-if)#switchport port-security mac-address smart
B) SW1(config-if)#switchport port-security mac-address dynamic
C) SW1(config-if)#switchport port-security mac-address sticky
D) SW1(config-if)#switchport port-security mac-address learn

Q17. Which command is used to enable PAT on router R1 to translate all inside local addresses matched by ACL 1 to the IP address assigned to the outside interface (which is Gig 0/2)?

A) ip nat inside source list 1 pool NAT_POOL
B) ip nat inside source list 1 interface gig0/2 overload
C) ip nat inside source static 192.168.1.0 192.0.2.0 overload
D) ip nat outside source list 1 interface gig0/2 overload

Q18. Given the 32-bit subnet mask 11111111 00000000 00000000 00000000, how many bits represent the network bits?

A) 8
B) 16
C) 32
D) 24

Q19. What is the range of assignable IP addresses for a subnet containing an IP address of 172.16.1.10 /19?

A) 172.16.0.1 – 172.16.31.254
B) 172.16.0.1 – 172.16.63.254
C) 172.16.0.0 – 172.16.31.255
D) 172.16.0.1 – 172.16.31.255
E) 172.16.0.0 – 172.16.63.254

Q20. Your team is transitioning to a DevOps model. What is the primary goal of implementing continuous feedback and iteration in the DevOps lifecycle?

A) To reduce the workload of the IT operations team
B) To eliminate the need for software testing
C) To improve quality and speed of application deployment
D) To separate development and operations responsibilities

Q21. What is the decimal equivalent of the 8-bit binary number 01100101?

A) 100
B) 102
C) 110
D) 101

Q22. Which Dynamic Trunking Protocol (DTP) mode actively generates messages on the interface in an attempt to form a trunk with a remote switch?

A) Access Mode
B) Trunk Mode
C) Dynamic Desirable Mode
D) Dynamic Auto Mode

Q23. In a typical enterprise network, where would we most likely find Layer 2 switches?

A) Campus Backbone Layer
B) Building Access Layer
C) Building Distribution Layer
D) Edge Distribution Layer

Q24. You are developing new security standards for a company. Which of the following factors would NOT typically be used in a multi-factor authentication system?

A) Something the user knows
B) Something the user has
C) Something the user is
D) Something the user believes

Q25. When determining the network and host portions of an IPv4 address, a specific value is used to identify the boundary between these two segments. What is this value called, and how does it function?

A) Network identifier, indicating the first octet as the network portion
B) Binary switch, flipping bits to distinguish between network and host parts
C) Subnet mask, using bits to differentiate network bits from host bits
D) CIDR notation, exclusively using slashes to divide network and host sections

Q26. Which EtherChannel protocol allows for the provisioning of 8 backup ports in a standby configuration, which have the ability to take over if an individual port fails?

A) EtherChannel
B) LACP
C) PAgP
D) ISL

Q27. Imagine your company operates in a large metropolitan area and requires high-speed connectivity between multiple buildings within the city. You seek a solution that offers very high bandwidth and redundancy, even in the event of a link failure. Based on these requirements, which WAN/MAN technology is best suited for your needs?

A) MPLS
B) Metro Ethernet
C) VPN over the Internet
D) Frame Relay

Q28. A security consultant is advising on the implementation of authentication for an SDN controller's REST API. Which of the following authentication methods would provide the highest level of security for this application?

A) Basic authentication over HTTP
B) API key authentication
C) OAuth 2.0 token-based authentication
D) Digest authentication

Q29. What is one advantage of using a cloud-managed solution for network management?

A) Requires less initial configuration on devices
B) Provides a single web portal for managing devices across multiple locations
C) Eliminates the need for any local IT staff
D) Ensures that all data traffic is routed through a central location

Q30. Which command tells a switch interface to passively listen for Dynamic Trunking Protocol (DTP) frames for trunk negotiation?

A) SW1(config-if)#switchport mode dynamic desirable
B) SW1(config-if)#switchport mode dynamic auto
C) SW1(config-if)#switchport mode passive
D) SW1(config-if)#switchport mode listen

Q31. You are a network administrator setting up a server for a critical application. Which of the following actions would best ensure "Availability" in the context of the CIA triad?

A) Implementing strong encryption algorithms
B) Using digital certificates for server authentication
C) Configuring redundant servers and load balancing
D) Applying strict access control policies

Q32. When examining a Power over Ethernet (PoE) topology, a wireless access point would be considered what type of component?

A) PSE
B) WAP
C) AC
D) PD

Q33. A switch port in a traditional Spanning Tree Protocol environment transitions from blocking to forwarding. Which of the following states does it NOT pass through during this transition?

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

Q34. You are assigning IP addresses to hosts in the 192.168.4.0 /26 subnet. Which two of the following IP addresses are assignable IP addresses that reside in that subnet?

A) 192.168.4.0
B) 192.168.4.63
C) 192.168.4.62
D) 192.168.4.32
E) 192.168.4.64

Q35. Which access control entry would correctly permit traffic to an HTTPS server (with an IP address of 203.0.113.1) from any host?

A) access-list 101 permit tcp any eq 443 host 203.0.113.1
B) access-list 101 permit tcp any host 203.0.113.1 eq 443
C) access-list 101 permit tcp any host 203.0.113.1 443
D) access-list 101 permit tcp any 203.0.113.1 eq 443

Q36. On a Cisco Catalyst switch, what command is used to set the MAC address table aging time to one hour?

A) mac address-table aging-time 60
B) mac address-table aging-time 1
C) mac address-table aging-time 3600
D) mac address-table aging-time 600

Q37. Which type of hypervisor runs in a traditional operating system on a server?

A) Native
B) Hosted
C) Nested
D) Installed

Q38. Which of the following reasons best explains why a company might want to implement subnetting within its Class C network infrastructure?

A) To increase the number of available public IP addresses
B) To allow for easier implementation of IPv6
C) To separate departments for security and resource allocation
D) To enable direct broadcast addresses for all devices

Q39. Which type of firewall has the ability to restrict or block packets based on source and destination addresses or other static values?

A) Proxy firewall
B) Stateful firewall
C) Stateless firewall
D) Static firewall

Q40. Which section of the Cisco DNA Center management dashboard allows us to graphically allocate pools of IP addresses?

A) Design
B) Provision
C) Platform
D) Addressing

Q41. When configuring a subinterface for VLAN 10 in a router-on-a-stick setup, which command correctly assigns the VLAN identifier using 802.1Q encapsulation?

A) ip address 192.168.1.1 255.255.255.0
B) switchport access vlan 10
C) encapsulation dot1Q 10
D) switchport mode trunk

Q42. Which command allows us to set the EtherChannel load-balancing algorithm to consider source and destination IP addresses?

A) SW1(config)#port-channel load-balance src-dst-ip
B) SW1(config)#port-channel distribute src-dst-ip
C) SW1(config)#port-channel src-dst-ip balance
D) SW1(config)#port-channel preferred src-dst-ip

Q43. In an effort to ensure continuous connectivity to the Internet, you are configuring a floating static route as a failover for your primary Internet connection via RouterA (your default gateway with an IP of 10.10.10.1). You've set up a secondary connection through RouterC, which has an IP address of 10.10.10.2. Given that your dynamic routing protocol has an administrative distance of 90, which of the following commands correctly configures the floating static route to the Internet through RouterC with an appropriate administrative distance?

A) ip route 0.0.0.0 0.0.0.0 10.10.10.2 89
B) ip route 0.0.0.0 0.0.0.0 10.10.10.1 85
C) ip route 0.0.0.0 0.0.0.0 10.10.10.2 91
D) ip route 0.0.0.0 0.0.0.0 10.10.10.1 90

Q44. Which of the following best describes a "logic bomb?"

A) Malware that encrypts a user's data until a ransom is paid
B) A code that lies dormant until triggered by a specific event
C) An attack that redirects DNS queries to malicious sites
D) A network scan for open and unprotected wireless networks

Q45. In which scenario is the IPv6 unspecified address "::" most commonly used?

A) As a destination address for multicast traffic
B) As a source address in the initial packets of an IPv6 address configuration process
C) For routing packets across the global Internet
D) As a loopback address to test local network functionality

Q46. How many available subnets are possible within the 192.168.100.0 /26 network?

A) 4
B) 2
C) 8
D) 16

Q47. You need to automate network configuration tasks at your organization. Which Cisco Catalyst Center feature would be most useful for this purpose?

A) Graphical network mapping
B) Quality of service settings
C) Application Programming Interfaces (APIs)
D) Network Time Travel feature

Q48. You are configuring a router and want to gather detailed information about devices directly connected to it via Layer 2. Which of the following commands provides detailed information, including the IP address and device type of connected CDP-speaking devices?

A) show cdp
B) show cdp neighbors
C) show cdp interface
D) show cdp neighbors detail

Q49. Which of the following is an example of a Distributed Denial of Service (DDoS) attack?

A) An attacker using a single computer to send excessive traffic to a server
B) An attacker exploiting a software vulnerability to gain control of a server
C) Multiple compromised computers simultaneously sending traffic to overwhelm a server
D) An attacker stealing user credentials through a phishing email

Q50. A host in your network has been assigned an IP address of 192.168.181.182 /25. What is the subnet to which the host belongs?

A) 192.168.181.128 /25
B) 192.168.181.0 /25
C) 192.168.181.176 /25
D) 192.168.181.192 /25
E) 192.168.181.160 /25

Q51. You are planning to deploy a subnet for a small office network that requires 28 devices to be connected. Using IPv4 addressing, what is the subnet mask you should apply to ensure all devices receive a unique IP address while minimizing the number of unused addresses?

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

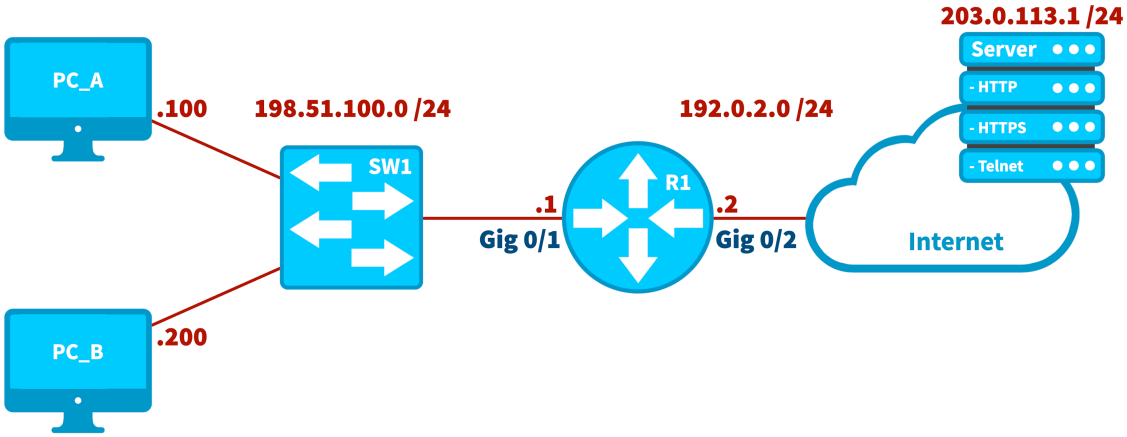
Q52. Which PAgP mode pairings will successfully negotiate an EtherChannel?

A) SW1: Desirable, SW2: On
B) SW1: Auto, SW2: On
C) SW1: Auto, SW2: Auto
D) SW1: Auto, SW2: Desirable

Q53. During a planning session for digital transformation, your company decides it needs a cost-effective solution for deploying web applications without the hassle of managing hardware. Which cloud deployment model offers this capability, along with the benefit of paying only for the resources you use?

A) Public Cloud
B) Private Cloud
C) Hybrid Cloud
D) On-Premises

Q54. Consider the following topology. Which of the following ACL configurations will block HTTP traffic and permit HTTPS traffic from the Server (at 203.0.113.1) being sent to either PC_A or PC_B?



A)
R1(config)# access-list 100 deny ip host 203.0.113.1 eq 80 198.51.100.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 in
R1(config-if)#

B)
R1(config)# access-list 100 deny tcp host 203.0.113.1 eq www 198.51.100.0 255.255.255.0
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 in
R1(config-if)#

C)
R1(config)# access-list 100 deny tcp host 203.0.113.1 eq www 198.51.100.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 out
R1(config-if)#

D)
R1(config)# access-list 100 deny tcp host 203.0.113.1 eq www 198.51.100.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 in
R1(config-if)#

Q55. A network administrator needs to ensure accurate time synchronization across all network devices to troubleshoot and correlate logs effectively. Which of the following protocols could be implemented to achieve this?

A) NTP
B) SNMP
C) FTP
D) SMTP

Q56. What is the 8-bit binary equivalent of the decimal number 112?

A) 10100100
B) 1111100
C) 1111001
D) 1110000

Q57. Which Layer 2 neighbor discovery protocol sends information to the destination multicast MAC address with an OUI of 01-80-c2-00-00-0E?

A) LLDP
B) CDP
C) ARP
D) STP

Q58. A network administrator is tasked with implementing a solution that allows rapid reconfiguration of network devices based on changing traffic patterns. Which of the following SDN components would be most directly responsible for defining these network changes?

A) The data plane of network devices
B) The southbound interface (SBI)
C) The northbound interface (NBI)
D) SDN applications

Q59. Given the network 192.168.10.0 /24, what is the usable IPv4 address range?

A) 192.168.10.1 – 192.168.10.254
B) 192.168.10.0 – 192.168.10.255
C) 192.168.10.1 – 192.168.255.255
D) 192.168.10.1 – 192.168.254.254

Q60. Imagine you want Switch SW2 to serve as the primary root bridge for VLAN 1 in a PVST+ environment, ensuring optimal traffic flow for that VLAN. Which command correctly configures this on SW2?

A) spanning-tree vlan 1 root primary
B) spanning-tree vlan 1 priority 32768
C) spanning-tree vlan 1 root bridge
D) spanning-tree vlan 1 bridge primary

Q61. Considering the routing process in a large enterprise network, what method do routers typically use to populate their IP routing tables with routes to different networks?

A) ARP requests
B) Manual configuration by network administrators
C) Automatic configuration using DHCP
D) Dynamic routing protocols

Q62. You are configuring a VPN between two office locations. Which VPN setup should you use to make the connection transparent to the end users?

A) Remote access VPN
B) SSL VPN
C) Site-to-site VPN
D) Split tunnel VPN

Q63. If you have a route to a network that was learned via OSPF, and another route to the same network learned via EIGRP, which route would a router typically prefer?

A) The OSPF route
B) The EIGRP route
C) The route with the longer prefix
D) The route learned first

Q64. What do routers reference in order to make packet forwarding decisions?

A) CAM Table
B) MAC Table
C) Routing Table
D) Memory Table

Q65. You are examining the OSPF database and notice that a transit network between two routers is not being advertised via a Type 2 LSA. What could be the reason for this?

A) The network is not a point-to-point network type
B) The network does not have a Designated Router elected
C) Type 2 LSAs are not used for advertising networks
D) The routers are in different OSPF areas

Q66. Your company wants to prevent password reuse among employees. Which policy would help enforce this?

A) Requiring passwords to be changed every 30 days
B) Using a minimum password length of 8 characters
C) Disallowing the use of previous passwords or slight variations of them
D) Mandating the use of special characters in passwords

Q67. You are working with a Class B network with the private IP address of 172.16.0.0 /16. You need to maximize the number of broadcast domains, where each broadcast domain can accommodate 1000 hosts. What subnet mask should you use?

A) /22
B) /23
C) /24
D) /25
E) /26

Q68. How many usable host addresses are found within the 172.16.0.0 /18 network?

A) 16,382
B) 65,534
C) 32,766
D) 8,190

Q69. On a Cisco Discovery Protocol (CDP) capable device, which command will display Layer 2 neighbor information?

A) SW1#show ip cdp
B) SW1#show cdp table
C) SW1#show cdp neighbors
D) SW1#show neighbors

Q70. What is the significance of the "R" bit being set to 1 in an IPv6 multicast address?

A) It indicates that the address is routable on the Internet.
B) It says that the address is reserved for future use.
C) It means the address includes an embedded IP address for a rendezvous point.
D) It designates the multicast group as restricted to the local network.

Q71. Why is it recommended not to use the CoS values 6 and 7 for production traffic in a network?

A) They are reserved for network use.
B) They are for high-priority traffic only.
C) They are deprecated values.
D) They cause increased latency.

Q72. What is the directed broadcast address for the IP address 10.10.1.48 /8?

A) 10.10.255.255
B) 10.255.255.255
C) 10.10.1.255
D) 10.10.0.255

Q73. On a Layer 2 switch, what can be used to break up broadcast domains?

A) ACL
B) VLAN
C) STP
D) FastEthernet

Q74. In a Spanning Tree Protocol (STP) implementation, the root bridge is:

A) The switch with the lowest bridge ID
B) The switch with the highest bridge ID
C) The switch closest to the designated bridge
D) The switch with the highest MAC address

Q75. Which IPv4 address class is represented by the classful mask 255.255.0.0?

A) Class A
B) Class B
C) Class C
D) Class D

Q76. In a CB-WFQ configuration, what is the maximum number of traffic classes Cisco recommends creating in order to avoid excessive complexity?

A) No more than 5
B) No more than 8
C) No more than 11
D) No more than 15

Q77. In Wi-Fi 7, what is the maximum channel width that can be achieved through channel bonding?

A) 160 MHz
B) 240 MHz
C) 320 MHz
D) 640 MHz

Q78. In the context of a campus network design, what scenario best justifies opting for a Collapsed Core architecture instead of a traditional Three-Tier model?

A) When the campus is expected to expand rapidly, requiring the addition of many new buildings
B) When each building requires a high degree of autonomy and separate network management
C) When there are a limited number of buildings, making the expense of a separate Core Layer unjustifiable
D) When network scalability is the top priority

Q79. In a Peer-to-Peer Architecture, which device is used to share resources on the network?

A) Server
B) Client
C) Proxy
D) Database

Q80. In a network that includes IP phones, which LLDP extension allows for the discovery of media endpoints and facilitates the exchange of additional information such as device capabilities and network policies?

A) LLDP-VOIP
B) LLDP-MED
C) LLDP-CAP
D) LLDP-SEC

Q81. What type of error might indicate that a network cable is damaged or experiencing interference?

A) VLAN mismatch error
B) Routing loop
C) CRC error
D) DHCP exhaustion

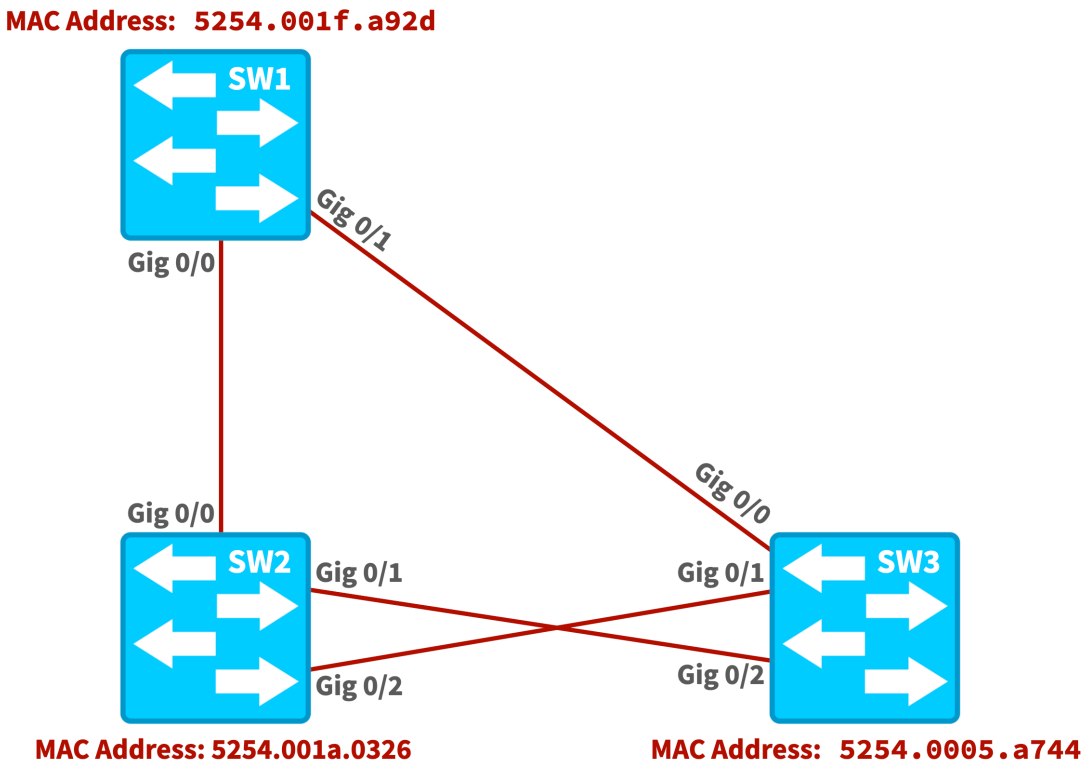
Q82. At a university with frequent construction, a network engineer wants to mitigate risks associated with unidirectional link failures due to fiber optic damage. After enabling Loop Guard on specific ports, what happens if one of these ports stops receiving BPDUs but can still transmit data?

A) The port remains in the same operational state until manually reset.
B) The port is disabled until the receipt of BPDUs resumes.
C) The port enters a loop-inconsistent state, preventing potential loops.
D) The port automatically resets itself after a predetermined timeout.

Q83. What is the network address for the IP address 172.29.20.50 /16?

A) 172.29.0.0
B) 172.29.20.0
C) 172.29.20.1
D) 172.0.0.0

Q84. Consider the following topology. Assuming all switches are configured with the default Bridge Priority for VLAN 1's Spanning Tree Protocol (STP) instance, which of the following ports will be in a Blocking state for VLAN 1? (Select 2.)



A) Gig 0/0 on SW1
B) Gig 0/0 on SW2
C) Gig 0/1 on SW2
D) Gig 0/2 on SW2

Q85. Which subnet mask can most efficiently represent all four networks listed below?

192.168.16.0 /24
192.168.22.0 /24
192.168.18.0 /24
192.168.20.0 /24

A) /21
B) /22
C) /4
D) /16

Q86. As a network administrator, you have a switch port, Gig 0/3 on switch SW3, connected to an end device that is expected to operate in full-duplex mode. You want this port to transition immediately to the forwarding state upon connection without waiting for the usual STP convergence times. How should you configure this port to meet the requirement?

A) Enable PortFast on the port.
B) Set the port as a designated port.
C) Configure the port as a trunk port.
D) Designate the port as a root port.

Q87. Which command allows us to assign a switch interface to VLAN 100?

A) SW1(config-if)#switchport vlan 100 join
B) SW1(config-if)#switchport member vlan 100
C) SW1(config-if)#switchport trunk vlan 100
D) SW1(config-if)#switchport access vlan 100

Q88. Which type of IPv4 traffic is considered to be one-to-one communication?

A) Multicast
B) Broadcast
C) Unicast
D) Transit

Q89. When converting the decimal number 241 to hexadecimal, which of the following represents the correct process and result?

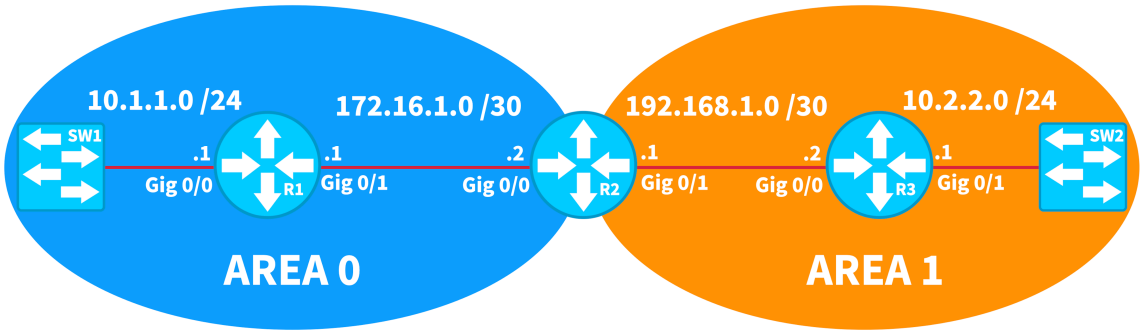
A) Convert to binary, divide into nibbles, convert nibbles to decimal, convert decimal to hex, result is 0xF1
B) Convert directly to binary, result is 0xE1
C) Divide into nibbles, convert to binary, result is 0xF1
D) Convert to binary, divide into nibbles, convert nibbles to decimal, convert decimal to hex, result is 0xE1

Q90. Which type of wireless LAN consists of clients sending and receiving radio waves directly between themselves?

A) Infrastructure Wireless LAN
B) Enterprise Wireless LAN
C) Mesh Wireless LAN
D) Ad Hoc Wireless LAN

Questions and Answers

Q1. Consider the following topology. How many Type 1 LSAs are present in router R3's Link State Database (LSDB)?



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

Answer: B

Explanation: A Type 1 Link State Advertisement (LSA) is known as a "Router LSA." A router in an area will have a Type 1 LSA entry for each network segment with that area. In this example, router R3 belongs to Area 1, and Area 1 contains two network segments, specifically: 192.168.1.0 /30 and 10.2.2.0 /24. Therefore, router R3's LSDB contains two Type 1 LSAs, one for each network segment in Area 1.

Q2. What is the collection of multiple Basic Service Sets (BSS) known as?

A) WSSID
B) IBSS
C) BSSID
D) ESSID

Answer: D

Explanation: An Extended Service Set Identifier (ESSID) is the collection of multiple Basic Service Sets (BSS) that share the same SSID. It allows seamless roaming for clients within a network, maintaining connectivity as they move between different access points.

Q3. For a data center requiring very high-speed connectivity between devices with a maximum distance of 30 meters, which category of twisted pair cabling is most suitable to support data transmission speeds up to 40 Gbps?

A) Category 6
B) Category 6A
C) Category 7
D) Category 8

Answer: D

Explanation: Category 8 twisted pair cabling is specifically designed for data center applications requiring very high-speed connectivity between devices, supporting up to 25 or 40 Gbps with a maximum distance of about 30 to 36 meters. This makes Category 8 the best choice for environments that demand the highest data transmission speeds over short distances.

Q4. After attaching a new workstation to a switch configured with STP, you observe a delay before the workstation can access the network. Assuming the port was not previously active, what is the default delay before the port becomes active?

A) 15 seconds
B) 30 seconds
C) 50 seconds
D) 20 seconds

Answer: B

Explanation: For a port that was not previously active, the default STP delay before it goes active is 30 seconds, bypassing the initial Blocking state and directly entering the Listening (15 seconds) and Learning (15 seconds) states, totaling 30 seconds. The PortFast feature can be used to eliminate this delay.

Q5. In the context of wireless transmission, what does QAM stand for, and what is its function?

A) Quadrature Amplitude Modulation; it allows multiple bits of data to be sent per subchannel by adjusting phase and amplitude
B) Quality Assurance Method; it ensures data integrity during transmission
C) Quick Access Mode; it prioritizes urgent data packets
D) Quantum Allocation Management; it manages bandwidth allocation using quantum computing principles

Answer: A

Explanation: QAM stands for Quadrature Amplitude Modulation. It allows multiple bits of data to be sent simultaneously per subchannel by adjusting the phase and amplitude of a signal and comparing the phase and amplitude differences between that signal and a reference signal to identify a point in a "constellation," which represents multiple bits.

Q6. You've set up a Layer 2 EtherChannel on your Cisco switch and wish to verify the load balancing algorithm in use. Which command could you use to check the current load balancing method?

A) show etherchannel summary
B) show port-channel compatibility
C) show etherchannel load-balance
D) show spanning-tree etherchannel

Answer: C

Explanation: To verify the load balancing algorithm currently in use for EtherChannel on a Cisco switch, the correct command is `show etherchannel load-balance`. This command provides information about the basis on which the switch distributes outbound traffic among the ports in the EtherChannel, such as source MAC address, destination MAC address, a combination of source and destination IP addresses, or other options.

Q7. An IP address of 192.168.0.100 /27 belongs to which of the following subnets?

A) 192.168.0.92
B) 192.168.0.128
C) 192.168.0.64
D) 192.168.0.96
E) 192.168.0.32

Answer: D

Explanation: To determine the subnets 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 19-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.

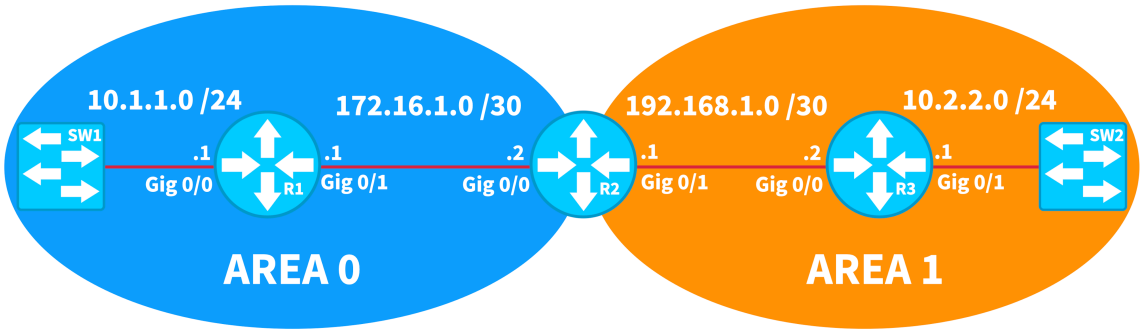
Step #3: Determine the block size by subtracting the decimal value of the interesting octet from 256.
Block Size = 256 – 224 = 32

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:
192.168.0.0 /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:

192.168.0.32 /27
192.168.0.64 /27
192.168.0.96 /27
192.168.0.128 /27
192.168.0.160 /27
192.168.0.192 /27
192.168.0.224 /27

Step #5: Identify the subnet address of the IP address 192.168.0.100 /27.
Looking through the subnets created by the 27-bit subnet mask reveals that the IP address of 192.168.0.100 resides in the 192.168.0.96 subnet.

Q8. Consider the following topology. How many Type 2 LSAs are present in router R3's Link State Database (LSDB)?



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

Answer: A

Explanation: A Type 2 Link State Advertisement (LSA) is known as a "Network LSA." An area has a Type 2 LSA for each network segment that meets two criteria: (1) The segment is a transit link (i.e., it interconnects to OSPF-speaking routers), (2) The segment is one on which a DR would be elected (e.g., on an OSPF Broadcast network type but not on an OSPF Point-to-Point network type). In this example, router R2 is in Area 1, and only one network segment in Area 1 meets both criteria. Specifically, the segment between routers R2 and R3 is an Ethernet segment, on which a DR would be elected by default. Also, that segment is a transit link, interconnecting routers R2 and R3. However, the segment between R3 and SW2 is not a transit link (i.e., it does not interconnect two OSPF-speaking routers). Therefore, we would only have one Type 2 LSA in router R3's Link State Database.

Q9. Which routing protocol is described as being able to provide the entire path (sequence of autonomous systems) a packet will traverse to reach its destination, distinguishing it from other types of routing protocols?

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

Answer: C

Explanation: BGP (Border Gateway Protocol) is unique among routing protocols as it is a path vector protocol, which provides the entire path (sequence of autonomous systems or AS hops) that packets will transit to reach their destination. This capability is crucial for routing between autonomous systems on the Internet.

Q10. Your network includes a subnet that does not have a DHCP server locally available. What solution allows PCs on this subnet to receive IP addresses from a DHCP server located on a different subnet?

A) Configuring a static route on the PCs
B) Upgrading to a DCHPv6 server
C) Creating an ACL on the next-hop router to permit DHCP messages
D) Implementing a DHCP relay agent on the router

Answer: D

Explanation: The correct solution for allowing PCs on a subnet without a local DHCP server to receive IP addresses from a DHCP server located on a different subnet is to configure a DHCP relay agent on the subnet's next-hop router. A DHCP relay agent, sometimes referred to as an "IP Helper," forwards DHCP Discover messages from clients across different subnets to a DHCP server. This enables the DHCP server to allocate IP addresses to clients on subnets where it is not directly present.

Q11. Which of the following is a valid private address range for a Class C address?

A) 192.168.0.0 – 192.168.255.255
B) 10.0.0.0 – 10.255.255.255
C) 169.254.0.0 – 171.255.255.255
D) 172.16.0.0 – 172.31.255.255

Answer: A

Explanation: The private IP address range 192.168.0.0 – 192.168.255.255 falls within the Class C IPv4 address range. The default subnet mask for a Class C address is a /24 subnet mask, or 255.255.255.0.

Q12. What is the role of a Wireless LAN Controller (WLC) in an enterprise network?

A) To provide Internet connectivity to clients
B) To serve as a single access point
C) To increase the bandwidth of wireless connections
D) To coordinate the operation of multiple access points

Answer: **D**

Explanation: In an enterprise network, a Wireless LAN Controller (WLC) coordinates the operation of multiple access points (APs). It manages client connectivity, including roaming between access points, and can perform self-healing by adjusting the power of other APs if one AP goes down.

Q13. In the EUI-64 method of generating an IPv6 address, why is the seventh bit of the original MAC address inverted?

A) To indicate that the address is globally unique
B) To differentiate between unicast and multicast addresses
C) To signal that the address has been modified from its original form
D) To designate the address as locally administered

Answer: D

Explanation: The inversion of the seventh bit in the EUI-64 process indicates that the address has been locally administered or modified from its original, universally administered state. This bit manipulation is crucial for distinguishing between globally unique MAC addresses assigned by manufacturers and those that have been locally modified or administered. It reflects a change in the address's administration scope, ensuring that the newly generated interface ID correctly represents its derivation from an altered MAC address.

Q14. What is the 48-bit address used by a switch to make frame forwarding decisions?

A) MAC address
B) CAM address
C) IP address
D) Link-local address

Answer: A

Explanation: Media Access Control (MAC) addresses are 48-bit addresses that are burned into a network interface card by the manufacturer. Switches use these addresses to make frame forwarding decisions.

Q15. In SNMPv3, what is the purpose of the `snmp-server group` command?

A) To set the SNMP server location
B) To create a group for managing user permissions and encryption settings
C) To specify the contact information for the SNMP server
D) To enable SNMP traps for specific events

Answer: B

Explanation: The `snmp-server group` command in SNMPv3 is used to create a group that defines allowable user permissions and encryption settings. This allows administrators to manage SNMP users and their access levels securely.

Q16. Which command allows us to dynamically learn MAC addresses seen on an interface, rather than using static assignments?

A) SW1(config-if)#switchport port-security mac-address smart
B) SW1(config-if)#switchport port-security mac-address dynamic
C) SW1(config-if)#switchport port-security mac-address sticky
D) SW1(config-if)#switchport port-security mac-address learn

Answer: C

Explanation: This command allows the switch to dynamically learn MAC addresses seen on an interface, which is much more scalable than static assignments. The MAC addresses are stored in the switch security table and the running configuration.

Q17. Which command is used to enable PAT on router R1 to translate all inside local addresses matched by ACL 1 to the IP address assigned to the outside interface (which is Gig 0/2)?

A) ip nat inside source list 1 pool NAT_POOL
B) ip nat inside source list 1 interface gig0/2 overload
C) ip nat inside source static 192.168.1.0 192.0.2.0 overload
D) ip nat outside source list 1 interface gig0/2 overload

Answer: B

Explanation: The command `ip nat inside source list 1 interface gig0/2 overload` is used to configure PAT by translating inside local addresses matched by ACL 1 to the IP address assigned to the outside interface (Gig 0/2) with the `overload` keyword enabling multiple translations.

Q18. Given the 32-bit subnet mask 11111111 00000000 00000000 00000000, how many bits represent the network bits?

A) 8
B) 16
C) 32
D) 24

Answer: A

Explanation: A 32-bit subnet mask separates IPv4 addresses into network bits and host bits. The mask is made by setting the network bits to all binary 1s and setting the host bits to all binary 0s. In this example, there are 8 binary 1s found, representing 8 network bits.

Q19. What is the range of assignable IP addresses for a subnet containing an IP address of 172.16.1.10 /19?

A) 172.16.0.1 – 172.16.31.254
B) 172.16.0.1 – 172.16.63.254
C) 172.16.0.0 – 172.16.31.255
D) 172.16.0.1 – 172.16.31.255
E) 172.16.0.0 – 172.16.63.254

Answer: A

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

Q20. Your team is transitioning to a DevOps model. What is the primary goal of implementing continuous feedback and iteration in the DevOps lifecycle?

A) To reduce the workload of the IT operations team
B) To eliminate the need for software testing
C) To improve quality and speed of application deployment
D) To separate development and operations responsibilities

Answer: C

Explanation: The primary goal of continuous feedback and iteration in the DevOps lifecycle is to improve both the quality and speed of application deployment. By constantly gathering feedback and making iterative improvements, teams can more quickly address issues, enhance features, and deliver better software more rapidly to meet business needs.

Q21. What is the decimal equivalent of the 8-bit binary number 01100101?

A) 100
B) 102
C) 110
D) 101

Answer: D

Explanation: The 8-bit binary number 01100101 converts to the decimal value 101. By knowing our two-base numbers, we can see that the 1s in this binary number represent the values 1, 4, 32, and 64. Adding these values together (1 + 4 + 32 + 64) gives us the solution of 101.

Q22. Which Dynamic Trunking Protocol (DTP) mode actively generates messages on the interface in an attempt to form a trunk with a remote switch?

A) Access Mode
B) Trunk Mode
C) Dynamic Desirable Mode
D) Dynamic Auto Mode

Answer: C

Explanation: A switch interface configured in Dynamic Desirable mode will generate Dynamic Trunking Protocol (DTP) messages on the interface, actively trying to convert the remote switch

interface to form a trunk. A trunk link will be formed if the remote switch interface is configured with Dynamic Desirable mode, Dynamic Auto mode or Trunk mode.

Q23. In a typical enterprise network, where would we most likely find Layer 2 switches?

A) Campus Backbone Layer
B) Building Access Layer
C) Building Distribution Layer
D) Edge Distribution Layer

Answer: B

Explanation: The Building Access Layer can be thought of as a wiring closet area. This area would typically consist of Layer 2 switches, where no routing decisions would be made. This is the area to which end user devices connect.

Q24. You are developing new security standards for a company. Which of the following factors would NOT typically be used in a multi-factor authentication system?

A) Something the user knows
B) Something the user has
C) Something the user is
D) Something the user believes

Answer: D

Explanation: In multi-factor authentication (MFA), common factors include something the user knows (password), something the user has (smartphone), and something the user is (fingerprint). The user's beliefs are not typically used in MFA systems.

Q25. When determining the network and host portions of an IPv4 address, a specific value is used to identify the boundary between these two segments. What is this value called, and how does it function?

A) Network identifier, indicating the first octet as the network portion
B) Binary switch, flipping bits to distinguish between network and host parts
C) Subnet mask, using bits to differentiate network bits from host bits
D) CIDR notation, exclusively using slashes to divide network and host sections

Answer: C

Explanation: A subnet mask is used to determine the dividing line between the network and host portions of an IPv4 address. It is a 32-bit value, similar to an IP address, and its purpose is to indicate which bits of the IP address refer to the network part and which refer to the host part. This is done by matching the subnet mask bits with the IP address bits: where the mask has a '1' bit corresponding to a bit in the IP address that is a network bit; and where the mask has a '0' bit corresponding to a bit in the IP address that is a host bit.

Q26. Which EtherChannel protocol allows for the provisioning of 8 backup ports in a standby configuration, which have the ability to take over if an individual port fails?

A) EtherChannel
B) LACP
C) PAgP
D) ISL

Answer: B

Explanation: Both Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) support a maximum of 8 active links in an EtherChannel. However, LACP can additionally designate 8 redundant backup ports in a standby manner to take over in case of a failure.

Q27. Imagine your company operates in a large metropolitan area and requires high-speed connectivity between multiple buildings within the city. You seek a solution that offers very high bandwidth and redundancy, even in the event of a link failure. Based on these requirements, which WAN/MAN technology is best suited for your needs?

A) MPLS
B) Metro Ethernet
C) VPN over the Internet
D) Frame Relay

Answer: B

Explanation: Of the options listed, Metro Ethernet is the optimal choice for high-speed connectivity within a metropolitan area, providing very high bandwidth, often up to 100 gigabits per second, depending on the service provider. It also offers redundancy, especially when configured in a ring topology, ensuring that if any single link fails, connectivity between buildings can be maintained through an alternate path. Unlike MPLS, VPNs, or Frame Relay, Metro

Ethernet is specifically designed to support the high-speed, high-reliability requirements of metropolitan area networks (MANs), making it the ideal solution for companies operating within large cities where Metro Ethernet is available.

Q28. A security consultant is advising on the implementation of authentication for an SDN controller's REST API. Which of the following authentication methods would provide the highest level of security for this application?

A) Basic authentication over HTTP
B) API key authentication
C) OAuth 2.0 token-based authentication
D) Digest authentication

Answer: C

Explanation: OAuth 2.0 token-based authentication provides the highest level of security for REST API authentication in an SDN controller. OAuth 2.0 is an industry-standard protocol for authorization that allows third-party applications to obtain limited access to an HTTP service. It generates short-lived tokens, reducing the risk of token compromise. Unlike basic authentication or API keys, OAuth 2.0 doesn't require sending credentials with each request, and it supports fine-grained access control. While digest authentication offers some advantages over basic authentication, it doesn't provide the same level of security and flexibility as OAuth 2.0.

Q29. What is one advantage of using a cloud-managed solution for network management?

A) Requires less initial configuration on devices
B) Provides a single web portal for managing devices across multiple locations
C) Eliminates the need for any local IT staff
D) Ensures that all data traffic is routed through a central location

Answer: B

Explanation: A cloud-managed solution allows administrators to log into a single web portal to manage devices across multiple locations, which simplifies the management process and provides centralized control. This approach is more scalable and efficient than managing each device individually.

Q30. Which command tells a switch interface to passively listen for Dynamic Trunking Protocol (DTP) frames for trunk negotiation?

A) SW1(config-if)#switchport mode dynamic desirable
B) SW1(config-if)#switchport mode dynamic auto
C) SW1(config-if)#switchport mode passive
D) SW1(config-if)#switchport mode listen

Answer: B

Explanation: A switch interface configured in Dynamic Auto mode will not actively try to convert the remote switch interface to form a trunk link. A Dynamic Auto mode interface becomes a trunk interface only if the remote switch interface is configured to Trunk Mode or Dynamic Desirable mode.

Q31. You are a network administrator setting up a server for a critical application. Which of the following actions would best ensure "Availability" in the context of the CIA triad?

A) Implementing strong encryption algorithms
B) Using digital certificates for server authentication
C) Configuring redundant servers and load balancing
D) Applying strict access control policies

Answer: C

Explanation: "Availability" in the CIA triad ensures that information and resources are accessible to authorized users when needed. Configuring redundant servers and load balancing helps maintain service availability even if one server fails, thereby preventing downtime.

Q32. When examining a Power over Ethernet (PoE) topology, a wireless access point would be considered what type of component?

A) PSE
B) WAP
C) AC
D) PD

Answer: D

Explanation: A wireless access point is an example of a Powered Device (PD) component. A PD is any device that requires PoE delivery, which includes IP phones, security cameras, and many more devices.

Q33. A switch port in a traditional Spanning Tree Protocol environment transitions from blocking to forwarding. Which of the following states does it NOT pass through during this transition?

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

Answer: D

Explanation: In traditional STP, a port transitions from Blocking to Listening, then to Learning, and finally to Forwarding. There is no "Filtering" state in this process. The "Discarding" state is synonymous with "Blocking" in terms of discarding user data.

Q34. You are assigning IP addresses to hosts in the 192.168.4.0 /26 subnet. Which two of the following IP addresses are assignable IP addresses that reside in that subnet?

A) 192.168.4.0
B) 192.168.4.63
C) 192.168.4.62
D) 192.168.4.32
E) 192.168.4.64

Answer: C and D

Explanation: To determine subnets and usable address ranges created by the 26-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 26-bit subnet mask, which is written in binary as:
11111111 11111111 11111111 11000000
The interesting octet is the fourth octet, because the fourth octet (i.e., 11000000) 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 26-bit subnet mask can be written in dotted decimal notation as:
255.255.255.192
Since the fourth octet is the interesting octet, the decimal value in the interesting octet is 192.

Step #3: Determine the block size by subtracting the decimal value of the interesting octet from 256.
Block Size = 256 – 192 = 64

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:
192.168.4.0 /26
We then count by the block size (of 64) in the interesting octet (the fourth octet in this question) to determine the remaining subnets:
192.168.4.64 /26
192.168.4.128 /26
192.168.4.192 /26

Step #5:
This question is asking about the 192.168.4.0 /26 subnet. From the above list of subnets, we can determine that the assignable range of IP addresses for this subnet is 192.168.4.1 – 192.168.4.62. We can also determine that 192.168.4.0 is the network address, and 192.168.4.63 is the directed broadcast address.
From the assignable range of IP addresses we have calculated, we can determine that the two assignable IP addresses given as options in this question are: 192.168.4.62 and 192.168.4.32.

Q35. Which access control entry would correctly permit traffic to an HTTPS server (with an IP address of 203.0.113.1) from any host?

A) access-list 101 permit tcp any eq 443 host 203.0.113.1
B) access-list 101 permit tcp any host 203.0.113.1 eq 443
C) access-list 101 permit tcp any host 203.0.113.1 443
D) access-list 101 permit tcp any 203.0.113.1 eq 443

Answer: B

Explanation: To permit HTTPS traffic from any source to a specific host, the correct syntax specifies the protocol (TCP), the source (any), the destination host (host 203.0.113.1), and the destination port number (eq 443). Therefore, the correct ACE is `access-list 101 permit tcp any host 203.0.113.1 eq 443`.

Q36. On a Cisco Catalyst switch, what command is used to set the MAC address table aging time to one hour?

A) mac address-table aging-time 60
B) mac address-table aging-time 1
C) mac address-table aging-time 3600
D) mac address-table aging-time 600

Answer: C

Explanation: The aging time on a Catalyst switch is set as a value in seconds. Using this command will set the aging time as desired, as 3600 seconds is equal to one hour.

Q37. Which type of hypervisor runs in a traditional operating system on a server?

A) Native
B) Hosted
C) Nested
D) Installed

Answer: B

Explanation: Also referred to as a client hypervisor, or Type-2 hypervisor, this runs within a host operating system. The underlying hardware is managed by the host OS rather than the hypervisor itself.

Q38. Which of the following reasons best explains why a company might want to implement subnetting within its Class C network infrastructure?

A) To increase the number of available public IP addresses
B) To allow for easier implementation of IPv6
C) To separate departments for security and resource allocation
D) To enable direct broadcast addresses for all devices

Answer: C

Explanation: Subnetting allows an organization to segment its network into smaller, manageable parts. This is particularly useful for separating different departments within a company, such as HR and R&D, to ensure they do not see each other's resources like printers on their local network, and to enhance security by limiting access between segments.

Q39. Which type of firewall has the ability to restrict or block packets based on source and destination addresses or other static values?

A) Proxy firewall
B) Stateful firewall
C) Stateless firewall
D) Static firewall

Answer: C

Explanation: Stateless firewalls are not aware of the state of traffic or data patterns. They use sets of static rules for packet filtering and do not keep track of the state of network connections. These rules are known as access control lists (ALCs).

Q40. Which section of the Cisco DNA Center management dashboard allows us to graphically allocate pools of IP addresses?

A) Design
B) Provision
C) Platform
D) Addressing

Answer: A

Explanation: In the Design area of Cisco DNA Center, we can graphically design networks. This includes the ability to create campus maps, import floor plans, identify IP address allocation, and more.

Q41. When configuring a subinterface for VLAN 10 in a router-on-a-stick setup, which command correctly assigns the VLAN identifier using 802.1Q encapsulation?

A) ip address 192.168.1.1 255.255.255.0
B) switchport access vlan 10
C) encapsulation dot1Q 10
D) switchport mode trunk

Answer: C

Explanation: The correct command to assign a VLAN identifier to a subinterface for VLAN 10 using 802.1Q encapsulation is `encapsulation dot1Q 10`. This command specifies the encapsulation method and the VLAN ID, allowing the router to recognize and route traffic for VLAN 10 appropriately through the subinterface.

Q42. Which command allows us to set the EtherChannel load-balancing algorithm to consider source and destination IP addresses?

A) SW1(config)#port-channel load-balance src-dst-ip
B) SW1(config)#port-channel distribute src-dst-ip
C) SW1(config)#port-channel src-dst-ip balance
D) SW1(config)#port-channel preferred src-dst-ip

Answer: A

Explanation: This command will perform an Exclusive OR (XOR) operation to add randomness to the physical links used in the EtherChannel. This will help distribute traffic more evenly over the links.

Q43. In an effort to ensure continuous connectivity to the Internet, you are configuring a floating static route as a failover for your primary Internet connection via RouterA (your default gateway with an IP of 10.10.10.1). You've set up a secondary connection through RouterC, which has an IP address of 10.10.10.2. Given that your dynamic routing protocol has an administrative distance of 90, which of the following commands correctly configures the floating static route to the Internet through RouterC with an appropriate administrative distance?

A) ip route 0.0.0.0 0.0.0.0 10.10.10.2 89
B) ip route 0.0.0.0 0.0.0.0 10.10.10.1 85
C) ip route 0.0.0.0 0.0.0.0 10.10.10.2 91
D) ip route 0.0.0.0 0.0.0.0 10.10.10.1 90

Answer: C

Explanation: This command is correct because it sets a default route through RouterC with an administrative distance of 91, slightly higher than the primary routing protocol's administrative distance of 90. This ensures the route through RouterC will be used as a backup if the primary path via RouterA fails. The administrative distance is crucial in determining the preference of routing information; in this case, the slightly higher value of 91 ensures the route serves as a floating static route, acting as a failover route rather than overriding the primary route.

Q44. Which of the following best describes a "logic bomb?"

A) Malware that encrypts a user's data until a ransom is paid
B) A code that lies dormant until triggered by a specific event
C) An attack that redirects DNS queries to malicious sites
D) A network scan for open and unprotected wireless networks

Answer: B

Explanation: A "logic bomb" is a piece of malicious code that remains dormant within a system until it is triggered by a specific event or condition, such as a certain date or the removal of an employee from a database.

Q45. In which scenario is the IPv6 unspecified address "::" most commonly used?

A) As a destination address for multicast traffic
B) As a source address in the initial packets of an IPv6 address configuration process
C) For routing packets across the global Internet
D) As a loopback address to test local network functionality

Answer: B

Explanation: The IPv6 unspecified address "::" is primarily used as a source address in the initial packets when a device is undergoing the IPv6 address configuration process. This includes scenarios such as sending Neighbor Solicitation messages or Router Solicitation messages when the device does not yet have a configured IPv6 address.

Q46. How many available subnets are possible within the 192.168.100.0 /26 network?

A) 4
B) 2
C) 8
D) 16

Answer: A

Explanation: We first determine the classful mask for the given network. This particular network falls within the Class C address space, which has a default classful mask of /24 (or 255.255.255.0). In order to determine the available subnets, we need to use the formula 2^s, where s = the number of borrowed bits. The borrowed bits are the number of bits beyond the

default classful mask for a network. Since we are using a /26 subnet mask and the default classful mask is /24, this means we have 2 borrowed bits (26 – 24 = 2). Now we put that number into our formula as 2^2, which gives us the value of 4. Therefore, by using a /26 subnet mask, we have the potential for 4 different subnets on this network.

Q47. You need to automate network configuration tasks at your organization. Which Cisco Catalyst Center feature would be most useful for this purpose?

A) Graphical network mapping
B) Quality of service settings
C) Application Programming Interfaces (APIs)
D) Network Time Travel feature

Answer: C

Explanation: Cisco Catalyst Center's Application Programming Interfaces (APIs) are most useful for automating network configuration tasks. These APIs allow network administrators to programmatically configure a network, set policies, and gather troubleshooting information using scripts, such as those written in Python.

Q48. You are configuring a router and want to gather detailed information about devices directly connected to it via Layer 2. Which of the following commands provides detailed information, including the IP address and device type of connected CDP-speaking devices?

A) show cdp
B) show cdp neighbors
C) show cdp interface
D) show cdp neighbors detail

Answer: D

Explanation: The `show cdp neighbors detail` command provides detailed information about each directly connected CDP-speaking device, including device IDs, port identifiers, capabilities, and IP addresses. This detailed view is crucial for administrators needing to map the network topology or troubleshoot connectivity issues, offering insights beyond the basic connectivity and device type information provided by summarized `show cdp neighbors` command output.

Q49. Which of the following is an example of a Distributed Denial of Service (DDoS) attack?

A) An attacker using a single computer to send excessive traffic to a server
B) An attacker exploiting a software vulnerability to gain control of a server
C) Multiple compromised computers simultaneously sending traffic to overwhelm a server
D) An attacker stealing user credentials through a phishing email

Answer: C

Explanation: A Distributed Denial of Service (DDoS) attack involves multiple compromised computers (often part of a botnet) simultaneously sending traffic to overwhelm a server, making it unavailable to legitimate users.

Q50. A host in your network has been assigned an IP address of 192.168.181.182 /25. What is the subnet to which the host belongs?

A) 192.168.181.128 /25
B) 192.168.181.0 /25
C) 192.168.181.176 /25
D) 192.168.181.192 /25
E) 192.168.181.160 /25

Answer: A

Explanation: To determine subnets and usable address ranges created by the 25-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 25-bit subnet mask, which is written in binary as:
11111111 11111111 11111111 10000000
The interesting octet is the fourth octet, because the fourth octet (i.e., 10000000) 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 25-bit subnet mask can be written in dotted decimal notation as:
255.255.255.128
Since the fourth octet is the interesting octet, the decimal value in the interesting octet is 128.

Step #3: Determine the block size by subtracting the decimal value of the interesting octet from 256.

Block Size = 256 – 128 = 128

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:
192.168.181.0 /25
We then count by the block size (of 128) in the interesting octet (the fourth octet in this question) to determine the remaining subnets, or in this case just a single additional subnet.
192.168.181.128 /25
Now that we have our two subnets identified, we can determine the subnet in which the IP address of 192.168.181.182 resides.
Since the usable range of IP addresses for the 192.168.181.128 /25 network is 192.168.181.129 – 192.168.181.254 (because 192.168.181.128 is the network address, and 192.168.181.255 is the directed broadcast address), and since 192.168.181.182 is in that range, the subnet to which 192.168.181.182 /25 belongs is: 192.168.181.128 /25

Q51. You are planning to deploy a subnet for a small office network that requires 28 devices to be connected. Using IPv4 addressing, what is the subnet mask you should apply to ensure all devices receive a unique IP address while minimizing the number of unused addresses?

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

Answer: A

Explanation: The 255.255.255.224 subnet mask can be written in slash notation as /27, which indicates 5 host bits (i.e., 32 - 27 = 5). According to the formula: "Available Hosts = (2^h - 2), where h is the number of host bits," the number of available hosts in this instance = (2^5 - 2) = 32 - 2 = 30. (NOTE: Keep in mind that the order of operations says we need to perform exponentiation before subtraction.) If we had used 4 host bits, the number of available hosts would have only been 14. Therefore, 5 host bits (corresponding to a subnet mask of 255.255.255.224) is the minimum number of host bits that can be used to meet the design criteria.

Q52. Which PAgP mode pairings will successfully negotiate an EtherChannel?

A) SW1: Desirable, SW2: On
B) SW1: Auto, SW2: On
C) SW1: Auto, SW2: Auto
D) SW1: Auto, SW2: Desirable

Answer: D

Explanation: If one side of an EtherChannel is configured with PAgP Auto mode, the only way a successful EtherChannel can be formed is when the other end is set to PAgP Desirable mode. The auto option passively listens for PAgP frames, while the desirable option actively sends PAgP frames in an attempt to form an EtherChannel.

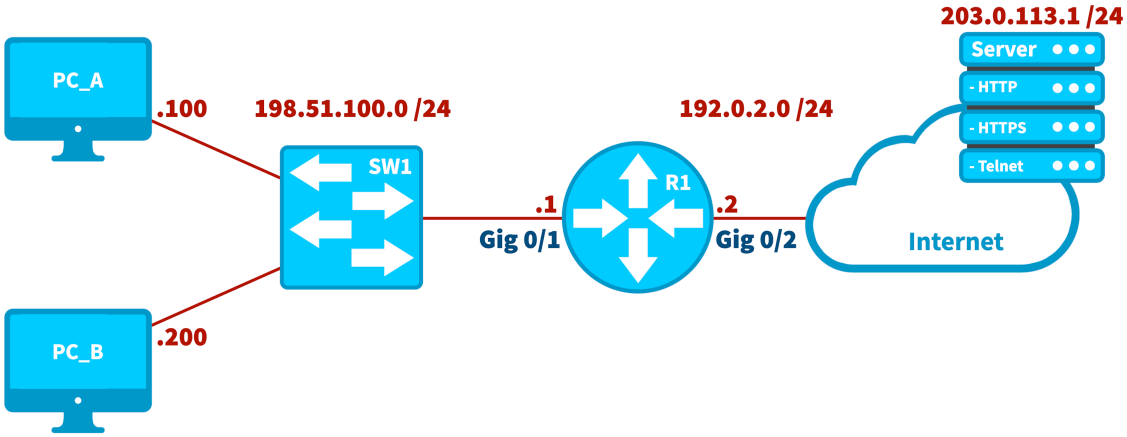
Q53. During a planning session for digital transformation, your company decides it needs a cost-effective solution for deploying web applications without the hassle of managing hardware. Which cloud deployment model offers this capability, along with the benefit of paying only for the resources you use?

A) Public Cloud
B) Private Cloud
C) Hybrid Cloud
D) On-Premises

Answer: A

Explanation: The Public Cloud deployment model is designed to deliver computing resources over the Internet, provided by cloud service providers. This model enables organizations to deploy web applications without the need to purchase, manage, or maintain any hardware, as all the infrastructure is managed by their cloud provider. Additionally, it operates on a "pay-as-you-go" basis, ensuring that organizations only pay for the resources they consume. This can make the public cloud an exceptionally cost-effective and scalable solution for deploying web applications.

Q54. Consider the following topology. Which of the following ACL configurations will block HTTP traffic and permit HTTPS traffic from the Server (at 203.0.113.1) being sent to either PC_A or PC_B?



A)
R1(config)# access-list 100 deny ip host 203.0.113.1 eq 80 198.51.100.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 in
R1(config-if)#

B)
R1(config)# access-list 100 deny tcp host 203.0.113.1 eq www 198.51.100.0 255.255.255.0
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 in
R1(config-if)#

C)
R1(config)# access-list 100 deny tcp host 203.0.113.1 eq www 198.51.100.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 out
R1(config-if)#

D)
R1(config)# access-list 100 deny tcp host 203.0.113.1 eq www 198.51.100.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)# int gig 0/2
R1(config-if)# ip access-group 100 in
R1(config-if)#

Answer: D

Explanation: In this example, we're blocking traffic from the Server to the PCs. Therefore, the source IP address is the Server's IP address (203.0.113.1), and the source port is TCP port 80 for the HTTP traffic we wish to block. Also, since the traffic is traveling from the Server into interface Gig 0/2 on router R1, the access list needs to be applied in the inbound direction on interface Gig 0/2. Alternately, the ACL could have been applied in the outbound direction on interface Gig 0/1, but in keeping with best practices, we're applying the Extended ACL as close to the source (i.e., the Server) as possible.
Option A is incorrect, because the first line is denying "ip" traffic rather than "tcp" traffic, and will therefore not allow us to specify a port number.
Option B is incorrect, because a subnet mask (255.255.255.0) is being used for the destination network (i.e., the network on which the PCs reside) rather than a wildcard mask (0.0.0.255).
Option C is incorrect, because the ACL is being applied outbound on interface Gig 0/2 rather than inbound.
Option D, however, is correct. Specifically, it blocks TCP port 80 traffic (i.e., www traffic) from the server (with a host IP address of 203.0.113.1) to PCs in the 198.51.100.0 /24 network.

Q55. A network administrator needs to ensure accurate time synchronization across all network devices to troubleshoot and correlate logs effectively. Which of the following protocols could be implemented to achieve this?

A) NTP
B) SNMP
C) FTP
D) SMTP

Answer: A

Explanation: Network Time Protocol (NTP) is designed to synchronize the clocks of network devices. Accurate time synchronization helps in correlating logs and troubleshooting network issues effectively. SNMP is for network management, FTP is for file transfer, and SMTP is for email communication.

Q56. What is the 8-bit binary equivalent of the decimal number 112?

A) 10100100
B) 1111100
C) 1111001
D) 1110000

Answer: D

Explanation: By knowing our two-base numbers, we can calculate the corresponding 8-bit binary value as 01110000. The 1s in this binary number represent decimal values 16, 32, and 64. Adding these values together (16 + 32 + 64) give us the decimal value 112.

Q57. Which Layer 2 neighbor discovery protocol sends information to the destination multicast MAC address with an OUI of 01-80-c2-00-00-0E?

A) LLDP
B) CDP
C) ARP
D) STP

Answer: A

Explanation: Link Layer Discovery Protocol (LLDP) sends information to this address, known as the LLDP Multicast address. This address is defined within a range of addresses reserved by the IEEE for protocols that are to be constrained to an individual LAN.

Q58. A network administrator is tasked with implementing a solution that allows rapid reconfiguration of network devices based on changing traffic patterns. Which of the following SDN components would be most directly responsible for defining these network changes?

A) The data plane of network devices
B) The southbound interface (SBI)
C) The northbound interface (NBI)
D) SDN applications

Answer: D

Explanation: Software Defined Networking (SDN) applications are most directly responsible for defining network changes in an SDN environment. These applications communicate with the

SDN controller through northbound interfaces (NBIs) using REST APIs. They express the desired state of the network, such as quality of service configurations or traffic routing patterns. The SDN controller then translates this high-level intent into specific device configurations and communicates these changes to network devices through southbound interfaces (SBIs). This approach allows for rapid, programmatic reconfiguration of a network based on changing requirements or traffic patterns.

Q59. Given the network 192.168.10.0 /24, what is the usable IPv4 address range?

A) 192.168.10.1 – 192.168.10.254
B) 192.168.10.0 – 192.168.10.255
C) 192.168.10.1 – 192.168.255.255
D) 192.168.10.1 – 192.168.254.254

Answer: A

Explanation: Using the formulas to find the network and directed broadcast addresses, we can determine that the network address is 192.168.10.0 and the directed broadcast address is 192.168.10.255. The usable IPv4 address range will fall inside here, with the first available host address being one address higher than the network address, and the last being one address lower than the directed broadcast address. This means the usable IPv4 address range is 192.168.10.1 – 192.168.10.254

Q60. Imagine you want Switch SW2 to serve as the primary root bridge for VLAN 1 in a PVST+ environment, ensuring optimal traffic flow for that VLAN. Which command correctly configures this on SW2?

A) spanning-tree vlan 1 root primary
B) spanning-tree vlan 1 priority 32768
C) spanning-tree vlan 1 root bridge
D) spanning-tree vlan 1 bridge primary

Answer: A

Explanation: The command `spanning-tree vlan 1 root primary` dynamically adjusts a switch's bridge priority to ensure the switch becomes the primary root for VLAN 1. This command is part of Cisco's PVST+ enhancements, allowing network administrators to directly influence which switch serves as a root bridge for a specific VLAN, optimizing traffic flow.

Q61. Considering the routing process in a large enterprise network, what method do routers typically use to populate their IP routing tables with routes to different networks?

A) ARP requests
B) Manual configuration by network administrators
C) Automatic configuration using DHCP
D) Dynamic routing protocols

Answer: D

Explanation: Routers can populate their IP routing tables through various methods, including manual configuration (static routing) and dynamic routing protocols. Dynamic routing protocols allow routers to automatically discover and maintain routes to different networks, providing scalability and the ability to route around link failures. Examples of dynamic routing protocols include OSPF and EIGRP.

Q62. You are configuring a VPN between two office locations. Which VPN setup should you use to make the connection transparent to the end users?

A) Remote access VPN
B) SSL VPN
C) Site-to-site VPN
D) Split tunnel VPN

Answer: C

Explanation: A site-to-site VPN connects two office locations, allowing routers to handle encryption and decryption transparently. This makes the connection seamless for end users, who do not need to initiate the VPN themselves.

Q63. If you have a route to a network that was learned via OSPF, and another route to the same network learned via EIGRP, which route would a router typically prefer?

A) The OSPF route
B) The EIGRP route
C) The route with the longer prefix
D) The route learned first

Answer: B

Explanation: EIGRP (Enhanced Interior Gateway Routing Protocol) has a lower administrative distance (AD) of 90 compared to OSPF (Open Shortest Path First), which has an AD of 110. Since routers prefer routes with lower ADs, the route learned via EIGRP would be preferred over the OSPF route.

Q64. What do routers reference in order to make packet forwarding decisions?

A) CAM Table
B) MAC Table
C) Routing Table
D) Memory Table

Answer: C

Explanation: A router maintains and references a routing table for packet forwarding decisions. This table contains a list of its ports, along with the network that is connected to each port. This allows the router to intelligently forward packets to their intended destination.

Q65. You are examining the OSPF database and notice that a transit network between two routers is not being advertised via a Type 2 LSA. What could be the reason for this?

A) The network is not a point-to-point network type
B) The network does not have a Designated Router elected
C) Type 2 LSAs are not used for advertising networks
D) The routers are in different OSPF areas

Answer: B

Explanation: For a network to be advertised via a Type 2 LSA (network LSA), two criteria must be met. First, the network must be a transit network interconnecting OSPF neighbors. Second, a Designated Router (DR) must be elected on that network segment. If no DR is elected, such as on point-to-point network types, the network will not be advertised using a Type 2 LSA.

Q66. Your company wants to prevent password reuse among employees. Which policy would help enforce this?

A) Requiring passwords to be changed every 30 days
B) Using a minimum password length of 8 characters
C) Disallowing the use of previous passwords or slight variations of them
D) Mandating the use of special characters in passwords

Answer: C

Explanation: Disallowing the reuse of previous passwords or slight variations of them helps prevent employees from using the same passwords repeatedly, thereby enhancing security by reducing the likelihood of compromised passwords being reused.

Q67. You are working with a Class B network with the private IP address of 172.16.0.0 /16. You need to maximize the number of broadcast domains, where each broadcast domain can accommodate 1000 hosts. What subnet mask should you use?

A) /22
B) /23
C) /24
D) /25
E) /26

Answer: A

Explanation: In addition to testing your knowledge of subnetting, this question is also making sure you understand that a subnet is a broadcast domain. This should not be confused with a collision domain (i.e., each port on a switch is in its own collision domain).

To determine how many host bits are required to support 1000 hosts, we can create a table from the following formula:
Number of Hosts = 2^h – 2, where h is the number of host bits
From this formula, we can create the following table:

1 Host Bit => 0 Hosts
2 Host Bits => 2 Hosts
3 Host Bits => 6 Hosts
4 Host Bits => 14 Hosts
5 Host Bits => 30 Hosts
6 Host Bits => 62 Hosts

7 Host Bits => 126 Hosts
8 Host Bits => 254 Hosts
9 Host Bits => 510 Hosts
10 Host Bits => 1022 Hosts

This table tells us that a subnet with 10 host bits will accommodate the requirement of 1000 hosts. If we have 10 host bits, then we have a 22-bit subnet mask (i.e., 32 – 10 = 22). Also, by not using more host bits than we need, we are maximizing the number of subnets that can be created.

Q68. How many usable host addresses are found within the 172.16.0.0 /18 network?

A) 16,382
B) 65,534
C) 32,766
D) 8,190

Answer: A

Explanation: To calculate the number of usable host addresses within a network, we use the formula 2^h – 2, where h = the number of host bits in the subnet mask. Two is subtracted in order to preserve a network address and a directed broadcast address. We know that subnet masks are 32 bits in length, so given a /18 mask we can determine that there are 14 host bits (32 – 18 = 14). Inserting this into the formula gives us 2^14 – 2, which comes to 16,382. Therefore, we have 16,382 usable host addresses in this network.

Q69. On a Cisco Discovery Protocol (CDP) capable device, which command will display Layer 2 neighbor information?

A) SW1#show ip cdp
B) SW1#show cdp table
C) SW1#show cdp neighbors
D) SW1#show neighbors

Answer: C

Explanation: This command displays information about Layer 2 adjacent neighbors that are also running CDP. Information displayed includes the port ID on the neighboring device, the local interface, and the type of neighboring device.

Q70. What is the significance of the "R" bit being set to 1 in an IPv6 multicast address?

A) It indicates that the address is routable on the Internet.
B) It says that the address is reserved for future use.
C) It means the address includes an embedded IP address for a rendezvous point.
D) It designates the multicast group as restricted to the local network.

Answer: C

Explanation: When the "R" bit in an IPv6 multicast address is set to 1, it indicates that the address includes an embedded IP address of a rendezvous point (RP). This feature is part of multicast addressing that allows for efficient distribution of multicast traffic by directing it to a specific router (rendezvous point) from which it can be sent out to all subscribing nodes.

Q71. Why is it recommended not to use the CoS values 6 and 7 for production traffic in a network?

A) They are reserved for network use.
B) They are for high-priority traffic only.
C) They are deprecated values.
D) They cause increased latency.

Answer: A

Explanation: CoS values 6 and 7 are reserved for network use, such as control traffic, and should not be used for regular production traffic to avoid potential conflicts and ensure network reliability.

Q72. What is the directed broadcast address for the IP address 10.10.1.48 /8?

A) 10.10.255.255
B) 10.255.255.255
C) 10.10.1.255
D) 10.10.0.255

Answer: B

Explanation: With a /8 subnet mask (or 255.0.0.0), we know that there are 8 network bits and 24 host bits. In order to find the network address, we first convert the IP address into binary, which in this case is 00001010.00001010.00000001.00110000. Since there are 8 network bits in

the subnet mask, this means we take the first 8 bits of this converted address and keep them the same. The remaining 24 bits are set to a 1 value, giving us the binary value 00001010.11111111.11111111.11111111. Converting this back to decimal gives us the address 10.255.255.255, which is the network address for this IP address.

Q73. On a Layer 2 switch, what can be used to break up broadcast domains?

A) ACL
B) VLAN
C) STP
D) FastEthernet

Answer: B

Explanation: A virtual LAN (VLAN) allows for broadcast domain separation on a Layer 2 switch, giving separation to sensitive traffic. It's common to place different enterprise employee groups on their own VLAN, such as separating the Sales department from the Engineering department.

Q74. In a Spanning Tree Protocol (STP) implementation, the root bridge is:

A) The switch with the lowest bridge ID
B) The switch with the highest bridge ID
C) The switch closest to the designated bridge
D) The switch with the highest MAC address

Answer: A

Explanation: The bridge ID (BID) is made up of the bridge priority (2 bytes) and the MAC address (6 bytes). Combines, that created the BID value. By default, all Cisco Catalyst switches have a priority value of 32768, so the MAC address value will be the tie breaker (lowest MAC wins).

Q75. Which IPv4 address class is represented by the classful mask 255.255.0.0?

A) Class A
B) Class B
C) Class C
D) Class D

Answer: B

Explanation: In IPv4 classful network addressing, the classful mask 255.255.0.0 represents a Class B address. This means that values in the first octet of the IPv4 address will range from 128 to 191. This can also be represented in prefix notation with a /16.

Q76. In a CB-WFQ configuration, what is the maximum number of traffic classes Cisco recommends creating in order to avoid excessive complexity?

A) No more than 5
B) No more than 8
C) No more than 11
D) No more than 15

Answer: C

Explanation: Cisco recommends creating no more than 11 traffic classes in a Class-Based Weighted Fair Queuing (CB-WFQ) configuration in order to avoid excessive complexity and help ensure the classes are treated with the appropriate levels of priority.

Q77. In Wi-Fi 7, what is the maximum channel width that can be achieved through channel bonding?

A) 160 MHz
B) 240 MHz
C) 320 MHz
D) 640 MHz

Answer: C

Explanation: In Wi-Fi 7 (802.11be), the maximum channel width that can be achieved through channel bonding is 320 MHz. This is accomplished by combining two 160 MHz channels, allowing for significantly higher data rates and improved performance, as compared with previous standards.

Q78. In the context of a campus network design, what scenario best justifies opting for a Collapsed Core architecture instead of a traditional Three-Tier model?

A) When the campus is expected to expand rapidly, requiring the addition of many new buildings
B) When each building requires a high degree of autonomy and separate network management
C) When there are a limited number of buildings, making the expense of a separate Core Layer unjustifiable
D) When network scalability is the top priority

Answer: C

Explanation: A Collapsed Core architecture, where the Core and Distribution Layers are combined, is most suitable for scenarios with a limited number of buildings. This is because the complexity and expense of maintaining a separate Core Layer with high-end switches might not be justified in smaller environments with only one to three buildings. In such cases, collapsing the Core and Distribution Layers simplifies the network structure and can reduce costs, while still meeting the network's performance and connectivity requirements. This choice focuses on practicality and cost-effectiveness for smaller-scale networks.

Q79. In a Peer-to-Peer Architecture, which device is used to share resources on the network?

A) Server
B) Client
C) Proxy
D) Database

Answer: B

Explanation: In a Peer-to-Peer Architecture, the clients themselves are serving resources to the network. This allows clients on the network to access local files or attached printers directly from another client, without the use of a central server.

Q80. In a network that includes IP phones, which LLDP extension allows for the discovery of media endpoints and facilitates the exchange of additional information such as device capabilities and network policies?

A) LLDP-VOIP
B) LLDP-MED
C) LLDP-CAP
D) LLDP-SEC

Answer: B

Explanation: LLDP-MED (Media Endpoint Discovery) is an extension of the LLDP standard specifically designed for network devices like IP phones. It enhances the basic capabilities of LLDP by allowing for the communication of additional information related to media endpoints, such as device type, location information, and network policies, facilitating more effective network management and policy application.

Q81. What type of error might indicate that a network cable is damaged or experiencing interference?

A) VLAN mismatch error
B) Routing loop
C) CRC error
D) DHCP exhaustion

Answer: C

Explanation: CRC (Cyclic Redundancy Check) errors often point to physical layer issues such as a bad cable or electromagnetic interference (EMI) affecting traffic flowing over the cable. CRC is a method used to detect errors in transmitted frames by comparing a calculated value to an expected value. If these values don't match, it indicates that the data has been corrupted during transmission.

Q82. At a university with frequent construction, a network engineer wants to mitigate risks associated with unidirectional link failures due to fiber optic damage. After enabling Loop Guard on specific ports, what happens if one of these ports stops receiving BPDUs but can still transmit data?

A) The port remains in the same operational state until manually reset.
B) The port is disabled until the receipt of BPDUs resumes.
C) The port enters a loop-inconsistent state, preventing potential loops.
D) The port automatically resets itself after a predetermined timeout.

Answer: C

Explanation: When Loop Guard is enabled on a port, and that port stops receiving BPDUs (potentially due to a unidirectional link failure), the port automatically transitions into a loop-inconsistent state. This state helps prevent the port from moving into a Forwarding state, which could cause a Layer 2 loop, particularly in scenarios like construction damage to cables. The port remains in this state until it resumes receiving BPDUs, providing an effective safeguard against network disruptions caused by physical link issues.

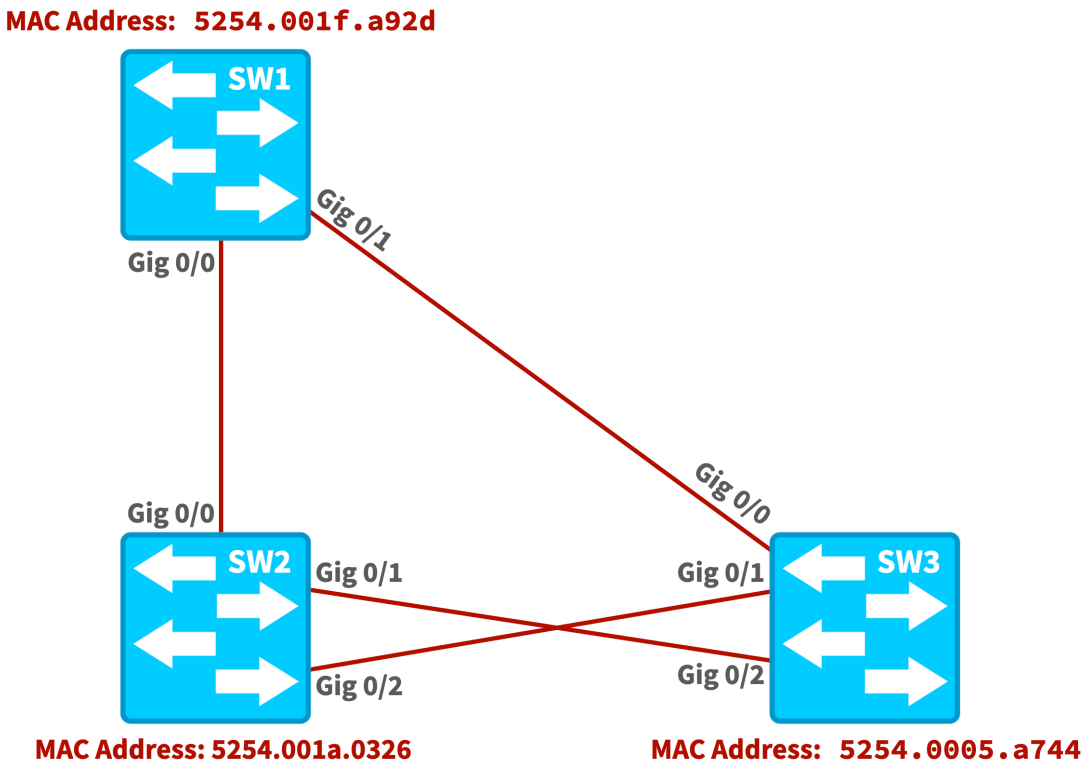
Q83. What is the network address for the IP address 172.29.20.50 /16?

A) 172.29.0.0
B) 172.29.20.0
C) 172.29.20.1
D) 172.0.0.0

Answer: A

Explanation: With a /16 subnet mask (or 255.255.0.0), we know that there are 16 network bits and 16 host bits. In order to find the network address, we first convert the IP address into binary, which in this case is 10101100.00011101.00010100.00110010. Since there are 16 network bits in the subnet mask, this means we take the first 16 bits of this converted address and keep them the same. The remaining 16 bits are set to a 0 value, giving us the binary value 10101100.00011101.00000000.00000000. Converting this back to decimal gives us the address 172.16.0.0, which is the network address for this IP address.

Q84. Consider the following topology. Assuming all switches are configured with the default Bridge Priority for VLAN 1's Spanning Tree Protocol (STP) instance, which of the following ports will be in a Blocking state for VLAN 1? (Select 2.)



A) Gig 0/0 on SW1
B) Gig 0/0 on SW2
C) Gig 0/1 on SW2
D) Gig 0/2 on SW2

Answer: A and C

Explanation: Since the Bridge Priorities for VLAN 1 are all at their default value on the switches, the lowest switch MAC address determines which switch is the Root Bridge. In this topology, SW3 has the lowest MAC address and is therefore the Root Bridge.
SW2 has two connections to the Root Bridge. To prevent a loop, STP will cause one of those ports to be blocking. Since both of SW2's Gig 0/1 and Gig 0/2 ports connect to SW3, the deciding factor for which port becomes the Root Port is which port is connected to the lowest far end Port ID. The far end of the link connected to SW2's Gig 0/1 interface is Gig 0/2 on SW3. The far end of the link connected to SW2's Gig 0/2 interface is Gig 0/1 on SW3. Therefore, the Root Port on SW2 is Gig 0/2, because it connects to the lowest far end Port ID (i.e., Gig 0/1 on SW3 as opposed to Gig 0/2 on SW3). And, to prevent a loop, Gig 0/1 on SW2 will be Blocking.

For the link between SW1 and SW2, Gig 0/0 on SW1 is blocking. The cost to get back to the Root Bridge is the same for each end of that link. So, the tie breaker is to determine which end of the link connects to a switch with the lowest Bridge ID. Since the MAC address of SW2 is less than the MAC address of SW3, Gig 0/0 on SW2 is the Designated port for that link and Gig 0/0 on SW1 is Blocking.

Q85. Which subnet mask can most efficiently represent all four networks listed below?

192.168.16.0 /24
192.168.22.0 /24
192.168.18.0 /24
192.168.20.0 /24

A) /21
B) /22
C) /4
D) /16

Answer: A

Explanation: If we convert all four IP addresses to binary, we will discover that they share the same values in their first 21 bits. This tells us that we should use a /21 subnet mask, or 255.255.248.0 in dotted decimal.

Q86. As a network administrator, you have a switch port, Gig 0/3 on switch SW3, connected to an end device that is expected to operate in full-duplex mode. You want this port to transition immediately to the forwarding state upon connection without waiting for the usual STP convergence times. How should you configure this port to meet the requirement?

A) Enable PortFast on the port.
B) Set the port as a designated port.
C) Configure the port as a trunk port.
D) Designate the port as a root port.

Answer: A

Explanation: Enabling PortFast on a switch port allows it to immediately transition to the forwarding state, bypassing the usual Listening and Learning states of STP. This configuration is ideal for ports connected to end devices like PCs or IP phones, where immediate network access upon connection is preferable, and there is no risk of creating network loops. PortFast should be

used with caution and only on ports that are confirmed to connect to an end device, in order to prevent potential loop conditions in the network.

Q87. Which command allows us to assign a switch interface to VLAN 100?

A) SW1(config-if)#switchport vlan 100 join
B) SW1(config-if)#switchport member vlan 100
C) SW1(config-if)#switchport trunk vlan 100
D) SW1(config-if)#switchport access vlan 100

Answer: D

Explanation: This command designates the interface as a switchport (rather than a trunk port) and assigns the interface to VLAN 100. Interfaces can be added on an individual basis, or as a group under interface-range configuration mode.

Q88. Which type of IPv4 traffic is considered to be one-to-one communication?

A) Multicast
B) Broadcast
C) Unicast
D) Transit

Answer: C

Explanation: Unicast is the term used to describe communication where data is sent from one point to another point, with a single source and a single destination. This is the predominant form of data transmission on LANs and the public Internet.

Q89. When converting the decimal number 241 to hexadecimal, which of the following represents the correct process and result?

A) Convert to binary, divide into nibbles, convert nibbles to decimal, convert decimal to hex, result is 0xF1
B) Convert directly to binary, result is 0xE1
C) Divide into nibbles, convert to binary, result is 0xF1
D) Convert to binary, divide into nibbles, convert nibbles to decimal, convert decimal to hex, result is 0xE1

Answer: A

Explanation: The process involves converting a decimal number to binary (11110001 for 241), dividing the binary number into nibbles (1111 and 0001), converting each nibble to its decimal value (15 and 1), and then converting each decimal value into its corresponding hexadecimal value (F and 1). Therefore, the correct hexadecimal representation of 241 is 0xF1. Recall that a hexadecimal value is prepended with "0x" to identify the value as a hexadecimal value.

Q90. Which type of wireless LAN consists of clients sending and receiving radio waves directly between themselves?

A) Infrastructure Wireless LAN
B) Enterprise Wireless LAN
C) Mesh Wireless LAN
D) Ad Hoc Wireless LAN

Answer: D

Explanation: An Ad Hoc Wireless LAN is a de-centralized type of network which does not rely on devices such as wireless routers or access points. These networks are very limited, but still may be useful in certain cases. The Apple iOS AirDrop feature is a modern example of an Ad Hoc network, which creates a secure device-to-device connection for data transfer.